

Auto Theft Today

A PROFESSIONAL E-NEWSLETTER BY THE INTERNATIONAL ASSOCIATION OF AUTO THEFT INVESTIGATORS

VOLUME 3 ♦ ISSUE 5 ♦ MAY 2016

this issue

IAATI Websites	p.2
Branch and Chapter News	p.3
64th International Seminar	p.8
Sponsor Spotlight: Regula Forensics	p.19
Member's Articles	p.20
In the News	p.36
Training Seminars	p.74



Common themes are emerging

With a large number of training events having been conducted all around the globe during the last two months a couple of themes have emerged. Firstly, many jurisdictions are reporting significant increases in the dismantling and distribution of stolen parts either locally, or via export to areas such as Africa and the Middle East. This theme was strong in presentations at both the Interpol conference in Thailand, and last month's Australasian Branch Seminar. It is also reinforced in a number of the articles in this issue of Auto Theft Today as well as a recent article titled "The Sum of All Parts" by UK President Justin Powell (Justin's article will be published in the next issue of APB).

On the one hand the shift of focus to the laundering of stolen parts has been brought about by: increased demand for vehicles and parts in developing countries; cheap container freight costs; and the introduction of the internet and related technologies to remotely source, market and distribute goods.

It is also partly due to the increased professionalism of authorities in detecting re-identified vehicles, and improved registration and inspection regimes in many Western Countries. These successes have helped force offenders to find alternative methods of turning a stolen vehicle into cash.

This shift in modus operandi comes at a critical time. Not only are we now entering a potential new era of vehicle hacking and electronic attacks, it is also a time when many Auto Theft Units are struggling to survive under budget constraints and increased pressure to direct resources to other crime categories. Only today I read about the Arizona Automobile Theft Authority battling to retain \$3 million of its funding. These pressures on Auto Theft Units are discussed in an article by the UK Branch Board (see page 28) and is the second theme emerging around the world.

To fight these two trends we all need to continue to work smarter. Specifically we need to embrace a partnership approach with related organizations and we need to continue to learn and adapt. This is one area where we have an advantage over offenders. IAATI's low cost training seminars and resources allow members to update their knowledge, skills and develop new contacts that will prove invaluable. This is one of the best investments you and your organization can make.

Chris McDonold, Editor

Auto Theft Today



Editor: Chris McDonald

Editor: Christopher T. McDonald

Email: enews@iaati.org

Auto Theft Today is an official e-newsletter of The International Association of Auto Theft Investigators (IAATI).

Any articles included in this newsletter express the views and opinions of the authors and do not necessarily represent the views and opinion of IAATI.

All rights reserved worldwide.

No portion of this publication can be reproduced, in whole in or part, without the express written permission of IAATI.

This newsletter is designed to provide the reader with links to the related information. Click on pictures or links to see more information. The inclusion of a link does not imply the endorsement of the site.

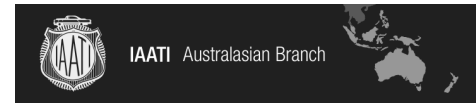


IAATI's Branch and Chapter Websites

Branches:

Australasian Branch

iaatiaus.org



European Branch

eb-iaati.org



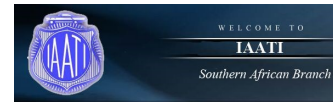
Latin American Branch

iaatilatam.org



Southern African Branch

iaatisab.co.za



United Kingdom Branch

<http://www.iaati.org.uk/>



Chapters (North America/Canada)

North Central Regional Chapter

ncrc-iaati.org



North East Regional Chapter

neaati.org



South Central Regional Chapter

tavti.org



South East Regional Chapter

seiaati.squarespace.com



Western Regional Chapter

wrciaati.org



BRANCH & CHAPTER NEWS

Latin American Branch:

- In February President Daniel Beck and Ana Laura Brizuela, Secretary of the Branch, attended as speakers at the 2nd Interpol Global Conference on Vehicle Theft, on behalf of the LatAm Branch. The event took place in the city of Bangkok, Thailand, from the 16th to the 18th February and our representatives spoke about: "The impact of illicit spare parts trade in Latin America". Carlos Alberto Betancur Ruiz, Director on behalf of Brazil, was also there, and lectured about: "Regulations of the use of jammers in the world".

- **1st Annual Training Seminar**

During the 9th, 10th and 11th March, we developed the 1st Annual Training Seminar of the IAATI LatAm Branch, at the city of Tigre, Buenos Aires Argentina.

There were representatives from the USA, Brazil, Uruguay, Chile, Paraguay, Colombia and the United Kingdom.

Also attended: members from the Ministry of Security of Argentina and the Province of Buenos Aires, other armed forces, specialists from the judiciary system, important enterprises, among others.

According to a survey carried out, the most interesting presentations were: "Detection of vehicle trafficking in South America: MO between Colombia and Ecuador", developed by María Cristina Torres González, Prosecutor at the Direction of the National Prosecutor's Office, Specialized in Organized Crime from Colombia.

Also, the audience has found very interesting the lecture about "Keyless System", presented by John Abounader.

Another praised speaker was Cora Smolianski, who is in charge of the National Antifraud Office in Argentina and who spoke about the reality and prevention of insurance fraud.

The Seminar took place at the city hall of Tigre city, where 272 people attended, exceeding our expectations by far.

At the end of each day, the attendees were able to visit different cultural icons of the city, as well as in the last day, a visit to the Tigre Surveillance Center –a model to follow in Latin America-, was carried out.



Last day visit to the Tigre Surveillance Center.

BRANCH & CHAPTER NEWS

Latin American Branch:

- 1st Annual Training Seminar - photos

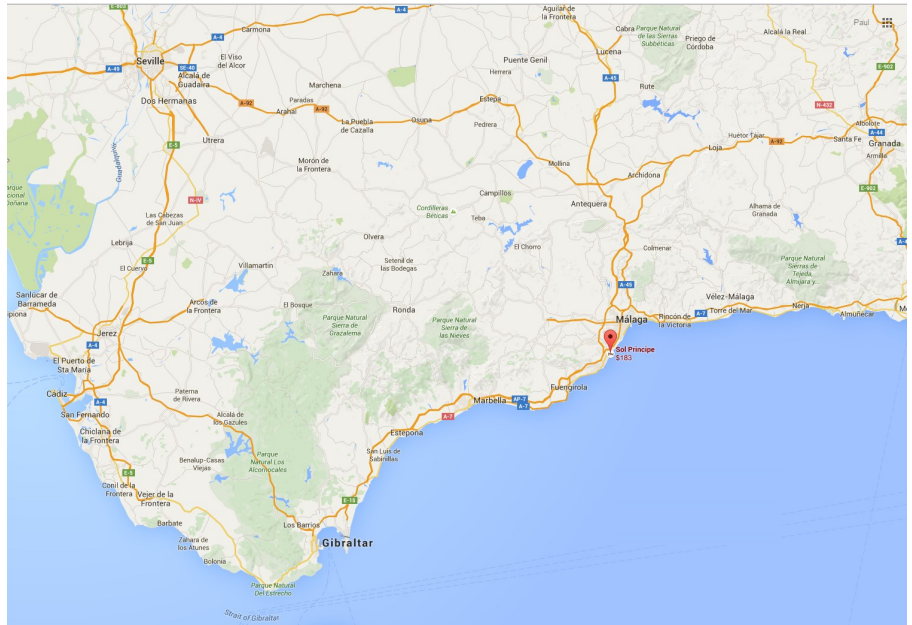


Above: Presenting a recognition to Executive Director John Abounader for his support to the LatAm Branch.

BRANCH & CHAPTER NEWS

European Branch:

- The European Branch Committee have announced that due to circumstances beyond their control the venue and dates of their 2016 Seminar has changed. It will now be held on 5—7 October at the Hotel Sol Principe, Paseo Colorado 26 - 29620 Torremolinos, - the southern coast of Spain.
- The Sol Príncipe Hotel is located in Malaga, on the way in to the resort of Torremolinos on the Costa del Sol. It has a fantastic beachfront location with direct access to the magnificent Playamar Beach, and enjoys an excellent Mediterranean climate 365 days a year (normally from 25 to 30° C in early October) The facilities cover 27,000 m2 and make the Sol Príncipe Hotel a spectacular theme hotel with a huge range of daytime and evening activities for children and adults - ideal for family vacations.
- The Sol Príncipe Hotel provides 799 rooms in different categories with magnificent views of the sea or the pool area, all set in beautiful gardens. The hotel is adapted for disabled guests and has a private car park. The Hotel is located just:
 - 2 km from Torremolinos town centre
 - 15 km from Malaga
 - 8 km from Malaga airport and Malaga coach station
 - 15 / 20 minutes from María Zambrano - AVE high speed train station



Western Regional Chapter:

- The WRC is also coordinating with the WSATI Southern Chapter, for the planning of their annual Auto Theft Training Seminar, to be held October 17-20th, 2016 in San Diego, California. The WRC will be holding their Annual Membership Meeting at the Seminar, and assist WSATI Southern Chapter with training and Seminar logistics. WSATI Southern Chapter President Brian Yori and his Board, has agreed to include IAATI membership fees in their registration costs for attendees to support WRC - IAATI. http://www.wsati.org/2016conference_begin.html

Did you know?

That as a financial member you can always access past issues of Auto Theft Today or APB in our f the IAATI **File Library**.

The File Library also contains a range of other important documents including our Constitution and By-laws, SOPs, our 2015-20 Strategic Plan, Legislation Update, Corporate Partner Program plus training material from past seminars and Certification reading materials.

Just log into the member only section of the website and search the file library.



BRANCH & CHAPTER NEWS

Australasian Branch:

- The Australasian Branch has recently hosted its 23rd Annual Training Seminar in Melbourne, Australia. The seminar was held over three days with two days of classroom presentations and a final day which included a workshops at the Automotive Centre of Excellence and a tour of the Fox Classic Car Museum.

The delegates heard from a range of high quality presenters including from our international President Todd Blair and John Rusted from the UK. Other highlights included a presentation by Stephen Tully about the examination of tyres and wheels, and a fascinating presentation by Mark Borlace on the “The next generation of motor vehicles – their risks and opportunities for vehicle crime investigations” that had everyone talking.

On a social side the President’s Networking included some visits by Australasian Motor rating champions John Bowe and Steven Richards who gave some there entertaining insights into their careers. During the Seminar and Awards Dinner the delegates raised \$1,600 from the raffle which will be donated to Victoria Police Legacy.

The Annual Seminar also celebrates the presentation of the Australasian Branch Awards. The 2016 winners were:

- Investigation of the Year: Strike Force Granite 15, New South Wales Police
- Insurance Industry Investigation of the Year: Mathew McKee
- President’s Award: Police Initiative ‘Refocuss’, New South Wales Police
- Forensic and Supporting Services Award: Det Sgt. Callum McNeill, Operation Maloo, New Zealand Police
- Member of the Year: Det Sgt. Brett Florence, Victoria Police

Summaries of each of the Australian Branch award winners will be published in the next issue of APB.

Selected presentations and photographs from the seminar are available via: www.iaatiaus.org/images/uploads/documents/Seminars/2016_Seminar_Melbourne/2016_Presentations_and_Photos.docx



International President, Todd Blair and Sandi Blair with 2016 Australasian Branch President, Mark Pollard



BRANCH & CHAPTER NEWS

South East Regional Chapter:

- In 2016 the South East Chapter is hosting IAATI's International Seminar in Murfreesboro, Tennessee during the 7-12 August. The international Seminar is IAATI's premier event each year and attracts 200-3000 delegates. Members are encourage to start planning their travel arrangement now as this is a not to be missed event. More details about the International Seminar are included on **pages 8 - 18**, and further updates will be available on the website when they are available.
- The IAATI community was sadden to learn of the recent passing of immediate past SERC Present Dave Dempsy. Aged 58, Dave passed away on March 29, 2016, after a brief illness. He was a proud member of Florida law enforcement for over thirty five (35) years and a hard working contributor to IAATI. Our thoughts are with his wife Emily and his family. See pages 20—22 as 2015/16 current SERC President Rusty Russell, recalls a font memory of his friend and colleague.

North East Regional Chapter:

- The NERC all set for 10 -12th May at the Ottawa Conference and Event Centre in Ottawa, Canada. This is their NERC's 44th Annual Training Seminar and is being held in conjunction with the Ottawa Police Service at the Ottawa Conference and Event Centre.
- Opening ceremonies will be May 10th at 8:30 am with remarks from Ottawa Police Chief Bordeleau, NEIAATI President Burke and a keynote speaker to be announced soon. There will be a president's reception the evening of May 10th and a 3-course dinner at the Awards Banquet on May 11th. Entertainment provided by the Floyd Hutchinson Quartet. The event venue is flanked by 2 hotels which both have blocks of rooms reserved for this event at a discounted rate. Bookings are open so register now through the links on the right.
- Registration is open to all auto theft investigators - \$225 (CAD) for IAATI members. Non-members will be required to pay for membership at the time of registrations. Fee includes all sessions, reception, banquet, lunches and coffee breaks. To register visit: <https://www.neiaati.com/index.php/seminar>

Southern African Branch:

- Planning and preparation is well underway for our annual SAB training seminar which will again be held end October 2016 at the usual venue, the South African Police Resort & Conference Centre Weesgerus in the Limpopo Province. For more information contact Daan Nel, via email: dnel@tracker.co.za

UK Branch:

- The UK Branch's 2016 National Vehicle Crime Conference is being held on the 8th and 9th June at Holywell Park, Loughborough, Leicestershire, LE11 3GR Please **see pages 51 & 52** of this issue of Auto Theft Today for more details.

July Issue of Auto Theft Today — Publication deadline

The next issue of Auto Theft Today will be released in the first week of July 2016. If you have any articles, photographs, member news, or anything else you would like included in the next issue please email it to: PThomas@iaati.org by **Friday 24th June 2016**

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	Notes	

64th INTERNATIONAL SEMINAR

This year's International Seminar will be held in **Murfreesboro, Tennessee, 7-12 August, 2016** and the Seminar Committee, is developing an exciting program for all delegates. Presenters for the training classes are almost finalised, social events are being organized and registrations are open via the IAATI website.

2016 Course Schedule: (Classes Subject to Change)

Sunday August 7, 2016

- 1300-1700 hours Registration Opens
- 1800-2000 hours President's Reception – Ballroom A

Monday August 8, 2016 (Plenary Session)

- 0800-0945 hours Opening Ceremonies:
President Todd Blair, IAATI
Chief Glenn Chrisman, Murfreesboro Police Dept.
CEO Joe Wehrle, NICB
- 0945-1000 hours Break
- 1000-1145 hours International Panel:
U.S. Chapters
European Branch
UK Branch
Australian Branch
South African Branch
Latin America Branch
- 1145-1300 hours Lunch (on your own)
- 1300-1445 hours Vendor Presentations:
- 1445-1500 hours Break
- 1500-1645 hours VBIED Case Presentation: Times Square Bombing
- 1700-2000 hours BBQ
- 2000-2300 hours Hospitality Room 1800-2000 hours

Tuesday August 9, 2016 (Concurrent Session)

- 0800-0945 hours Salon A *Basic Vehicle Identification*
Salon B Vessel Identification & HIN Restoration
Salon C Using NMVTIS Law Enforcement Access Tool to battle Vehicle-related Crimes to include Terrorism
Salon D Cargo Theft & Intermodal Identification
- 0945-1000 hours Break
- 1000-1145 hours Salon A *Chop Shop Investigations*
Salon B Vessel Identification & HIN Restoration (continued)
Salon C Odometer Fraud
Salon D Officer Safety
- 1145-1300 hours Lunch (on your own)
- 1300-1445 hours Salon A *ATV Identification*
Salon B Interview & Interrogation
Salon C GPS Decryption
Salon D Vehicle-Borne IED's (US LE only)
- 1445-1500 hours Break

It's time to book your travel
and accommodation.

95

Days left until the

64th Annual Training
Seminar, Murfreesboro
(Nashville),
Tennessee, USA

Early bird registrations
end 30 June 2016

64th INTERNATIONAL SEMINAR

2016 Course Schedule: (Classes Subject to Change)

Tuesday August 9, 2016 (Concurrent Session)

- 1500-1700 hours Salon A *Sport Bike Identification*
Salon B Interview & Interrogation (continued)
Salon C GPS Decryption
Salon D Vehicle-Borne IED's (US LE only)
- 1900-2300 hours Hospitality Room 1700-2000 hours

Wednesday August 10, 2016 (Concurrent Session)

- 0800-0945 hours Salon A RISSNET & RISS Center Services
Salon B Interview & Interrogation
Salon C GPS Decryption
Salon D Cargo Theft & Intermodal Identification
- 0945-1000 hours Break
- 1000-1145 hours Salon A Surveillance Technology
Salon B Interview & Interrogation
Salon C GPS Decryption
Salon D Officer Safety
- 1145-1300 hours Lunch (on your own)
- 1300-1445 hours Salon A Vehicle Arson: Beyond Cause & Origin
Salon B Vessel Identification & HIN Restoration
Salon C Odometer Fraud
Salon D Vehicle-Borne IED's (US LE only)
- 1445-1500 hours Break
- 1500-1700 hours Salon A Vehicle Fires: Investigating Beyond Cause & Origin
Salon B Vessel Identification & HIN Restoration (continued)
Salon C Using NMVTIS Law Enforcement Access Tool to battle Vehicle-related Crimes to include Terrorism
Salon D Vehicle-Borne IED's (US LE only)
- 1900-2300 hours Hospitality Room 1000-1145 hours

Thursday August 11, 2016 (Concurrent Session)

- 0800-0945 hours Salon A Vehicle Arson: Beyond Origin & Cause
Salon B *Corvette Identification*
Salon C RISSNET/RISS Center Services
Salon D *Abandoned Vehicles in Latin America*
- 0945-1000 hours Break
- 1000-1145 hours Salon A Vehicle Fires: Investigating Beyond Origin & Cause
Salon B *Corvette Identification (continued)*
Salon C Surveillance Technology
Salon D *Carfax*
- 1145-1300 hours Lunch (on your own)
- 1300-1445 hours Salon A Mapping & Analyzing Historical Cell Phone Records
Salon B *GM Onstar Updates*
Salon C *FBI LEEP/LEO System Overview*
Salon D *Insurance Fraud*



64th INTERNATIONAL SEMINAR

2016 Course Schedule: (Classes Subject to Change)

Thursday August 11, 2016 (Concurrent Session)

- 1445-1500 hours Break
- 1500-1700 hours Salon A IAATI Business Meeting
- 1800-2000 hours Banquet
- 2000-2400 hours Hospitality Room 1000-1145 hours

Friday August 12, 2016 (Concurrent Session)

- 0800-0945 hours Salon A Mapping & Analyzing Historical Cell Phone Records
Salon B *Rental Car Theft*
- 0945-1000 hours Break
- 1000-1145 hours Conference Closing Ceremonies

Classes bracketed by asterisks (e.g., *Chop Shop Investigation*) occur only once during program. All other classes repeat at least once during the program. Check schedule for times/location.

Course Descriptions:

Course: Basic Vehicle Identification

This is an entry level overview of the concepts and methodologies used to identify vehicles. This course will cover vehicle identification number (VIN) formats and public Vehicle Identification Number attachment methods. The course will also cover how to identify altered vehicles (i.e. vehicles on which the public vehicle identification number plate has been switched/altered) utilizing alternative points of identification. Case examples will be provided. This course is provided in conjunction with Chop Shop Investigations to provide new investigators with the tools necessary to recognize key identifiers of stolen vehicles on which their identification numbers have been altered or obliterated.

Course: Chop Shop Investigations

This is an entry level overview of the concepts and methodologies used to identify and investigate organized rings involved with the theft, dismantling, re-numbering, and concealment of stolen vehicles. This course is provided in conjunction with Basic Vehicle Identification to provide new investigators with the tools necessary to recognize the key identifiers of chop shop activities.

Course: Cargo Theft Concepts

A 45 minute course that describes the basic concepts of cargo theft, the seriousness of the problem, general information on how cargo crimes are perpetrated, things to look for, how to respond to the problem and suggestions to follow in responding to cargo crimes occurring in your area.

Course: Intermodal Theft Investigation

A 1 hour course that defines intermodalism, the components associated with it, identifiers found on intermodal components, the location of container confidential numbers, common reporting problems and suggestions on how to properly further the investigation after the initial report has been taken.

64th INTERNATIONAL SEMINAR

Course Descriptions: (continued)

Course: Corvette Identification

This class will encompass advanced methods on how to identify all years of the Chevrolet Corvette. The main focus will be on identification by secondary numbers which include grease pencil markings, pin stamping and sequence numbers cross referenced by the vehicles build sheet. This presentation will be supported by power point instruction and practical exercise. On hand will be a Chevrolet Corvette donated by General Motor Company to use as example for this class.

Course: Using the NMVTIS Law Enforcement Access Tool to battle Vehicle-related Crimes to include Terrorism

Automobile fraud and theft negatively affect public safety and cost consumers and insurance companies \$8 billion per year. In addition to auto theft, vehicle cloning has become a lucrative illegal activity for organized criminals with profits often used to fund additional criminal activities, including terrorism. The National Insurance Crime Bureau estimates vehicle cloning profits annually exceed \$12 million, with criminals netting an average of \$30,000 per cloned vehicle. Vehicle auctions have grown into multi-million-dollar enterprises and international criminals have found ways to exploit vehicle auctions for illegal activities, especially those in which the buyer does not have to be physically present. In an effort to facilitate law enforcement investigations and public safety, several enhancements have been made to the National Motor Vehicle Title Information System (NMVTIS) Law Enforcement (LE) Access Tool. This workshop will provide vehicle-related crimes trends, an overview of the NMVTIS and the NMVTIS Law Enforcement Access Tool (LEAT), examples of how the tool has facilitated investigations, and instructions for accessing the tool.

At the end of this workshop, participants will learn:

- Vehicle-related crime trends
- The purpose of the NMVTIS LE Access Tool
- Information included in the NMVTIS LE Access Tool
- Benefits of the NMVTIS LE Access Tool
- Specific examples of how the tool facilitated investigations
- Instructions for accessing the tool

Course: CDR Analysis and Mapping

Historical cellular telephone records (CDRs) are being used more often in various types of investigations. CDRs are more readily available to investigators, and provide another method of determining the possible whereabouts of an individual. Analysis can also be done to determine with whom an individual was engaged in communication with during a specific time of interest. Multiple software applications can be used to aid in the analysis and mapping of CDRs.

The NICB can provide analytical support to investigations where CDRs have already been obtained. Analysis includes research, mapping of cell towers captured during phone use, and reports detailing findings. The NICB has access to various software platforms, including GeoTime, which can be used to create a geo-temporal animated mapping of cell towers captured during calls.

Course: Vehicle Fires: Investigating Beyond Origin & Cause

This course will primarily focus on investigative practices and strategies when investigating a vehicle fire beyond determination of the origin and cause of the fire. Specifically, this course is designed to identify the available insurance claim file information and resources in order to complete a full investigation, both in the criminal and civil arena. The lecture will also include a case study presentation.

64th INTERNATIONAL SEMINAR

Instructor Biographies:

Senior Tactical Analyst Anna Kotsovos, National Insurance Crime Bureau Identification

Course: Cell Phone Analytics

Anna Kotsovos is a Senior Tactical Analyst with the National Insurance Crime Bureau (NICB) in Des Plaines, Illinois. Anna provides analytical support for NICB case investigations, creating products for local and federal law enforcement agencies and prosecutors. She is the lead instructor for the NICB Analyst Academy which provides training to insurance and law enforcement analysts. She has provided cellular telephone record mapping analysis for various types of cases from vehicle give-ups to homicides.

Anna holds an associate's degree in computer networking, a bachelor's degree in psychology, a master's degree in clinical psychology, and a graduate certificate in intelligence analysis. Anna completed the Introductory Intelligence Analyst Training Program through the Office of State and Local Training of the U.S. Department of Homeland Security.

Anna was a college adjunct instructor for seven years teaching psychology and criminal justice courses, and maintains licensure as an EMT, currently volunteering with the Medical Reserve Corps.

Anna is the Immediate Past-President of the North Central Regional Chapter of the International Association of Auto Theft Investigators (IAATI).

Anna was awarded the 2011 Analyst of the Year award by the International Association of Special Investigation Units (IASIU).

Anna achieved the Certified Insurance Fraud Analyst designation from the IASIU in 2012.

Anna has presented at various training seminars to members of the insurance industry, law enforcement, arson investigators, and prosecutors.



Special Agent Bill Shiver, CSXT Railroad Police

Course: Cargo Theft & Intermodal Identification

CSXT Special Agent Bill Shiver began his career in law enforcement with the Florida Highway Patrol in May, 1970. He retired in December 2006 as a Lieutenant assigned to the Florida Highway Patrol Bureau of Investigations.

During the last 12 years of his career with the Florida Highway Patrol, S/A Shiver focused on the little known problem of cargo theft in Florida. He established the Fax Alert Anti-Theft System which provided a means for law enforcement and transportation industry members to alert State law enforcement of recent commercial vehicle and cargo theft

incidents. Statistical data received from the Fax Alert System provided a means to track the cargo theft problem throughout Florida and attack it in pro-active ways.

In mid-year 2005, the Fax Alert System transitioned to the Electronic Freight Theft Management System (EFTMS); a web based system which remains operational and serving the transportation industry and law enforcement community today. When a theft incident is reported to the EFTMS by law enforcement or an industry member, within 5 minutes an alert is delivered to the e-mail accounts of all State Troopers, Weigh Stations and Agricultural Inspection Stations throughout Florida.

After retiring from F.H.P., S/A Shiver joined the CSXT Police Department as a member of their Cargo Theft Unit. The CSXT Police Department continues to contribute man power and equipment resources to the Florida Cargo Theft Task force effort. S/A Shiver remains active in those efforts.

64th INTERNATIONAL SEMINAR

Instructor Biographies: (continued)

Detective BJ Caudill, Kentucky State Police

Course: Corvette Identification

Detective Caudill began his law enforcement career in 2001 as a Deputy for the Floyd County Sheriff Department. During this time he completed DOCJT training academy and was assigned to general patrol from 2001-2003.

Detective Caudill graduated Kentucky State Police Academy in 2004, upon graduation was assigned to KSP Pikeville Post as a uniformed trooper. During this time I had responsibilities of answering calls of service, enforcing traffic laws, investigating collisions and criminal complaints. In 2006 Trooper Caudill was recognized and honored by The Senate of the Commonwealth of Kentucky for his service and awarded The Justice and Public Safety Cabinet, Secretary's Award.

In 2007 he was placed in general investigations as a detective, where he successfully prosecuted homicides, robberies, sex abuse and other major crimes. During this assignment Detective Caudill was named Trooper of the Year for Pikeville Post 2010.

In 2010 Detective Caudill was assigned to Vehicle Investigations Branch where he still assigned today. Serving as detective in Vehicle Investigations, he is tasked in investigating crimes related to major auto, heavy equipment, boat and ATV thefts with emphasis on conducting confidential inspections when the true identity is obscured. Detective Caudill also active in cargo theft related crimes.

Additional Responsibilities: KLEC (Kentucky Law Enforcement Council) certified instructor responsible for composing a 32 hour yearly in-service course for the Kentucky State Police Academy. Provide additional blocks of instruction related to vehicle investigations, KSP Telecommunications Academy, KSP Arson Investigator in-service and Kentucky Transportation Cabinet Vehicle Inspector Certification class.

Detective Israel Slinker, Kentucky State Police

Course: Corvette Identification

Post 7 Richmond: Joined the KSP in May 1998 and served as a dispatcher for 2 ½ years

Kentucky State Police Academy: Graduated June 2001

Post 2 Madisonville / Post 15 Columbia: Worked as a uniformed Trooper for 5 ½ years with responsibilities of answering calls for service, enforcing traffic laws, investigating collisions and criminal complaints.

Post 15 Columbia: Assigned as a general investigations detective for 4 years. During this time conducted investigations into and successfully prosecuted a variety of cases to include bank robberies, physical and sexual abuse cases, murder for hire, and homicide cases.

KSP Vehicle Investigations Branch: For the past 4 ½ years serving as a detective tasked with investigating crimes related to auto, heavy equipment, boat, and ATV thefts with emphasis on conducting confidential inspections when the true identity of an item has been obscured. Also active in many cargo theft investigations across the eastern United States that involve organized Eastern European and Cuban based criminal enterprise groups, loosely organized local based groups, and opportunistic thieves working alone.

Additional Responsibilities: KLEC (Kentucky Law Enforcement Council) certified instructor responsible for composing a 32 hour yearly in-service course for the Kentucky State Police Academy. Provide additional blocks of instruction related to vehicle investigations and cargo theft to cadets in the KSP Academy, KSP Telecommunications Academy, KSP Arson Investigator in-service, Drug Interdiction training, KSP Drug Enforcement Special Investigations in-service, Kentucky Transportation Cabinet Vehicle Inspector Certification class, and cargo theft awareness trainings for law enforcement and private industry.

64th INTERNATIONAL SEMINAR

Instructor Biographies: (continued)



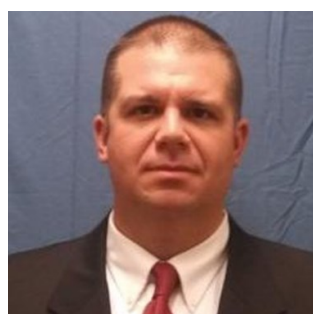
Joseph H. Wehrle, Jr. President and Chief Executive Officer, National Insurance Crime Bureau Police

Joseph H. Wehrle, Jr., serves as President and Chief Executive Officer for NICB.

From 2003 – 2007, Mr. Wehrle was Senior Vice President, then President of USAA Property and Casualty Insurance Group. As President of USAA, Mr. Wehrle led nearly 11,000 employees located in six national and two international locations catering to over five million members. He had overall responsibility for an \$8 billion book of business, which experienced record growth for auto, property and homeowners insurance during his tenure.

Mr. Wehrle completed a distinguished 33-year career in the United States Air Force having risen to the rank of lieutenant general. He served in various leadership positions with the U.S. Air Force and retired in 2003 as the Air Force Assistant Vice Chief of Staff.

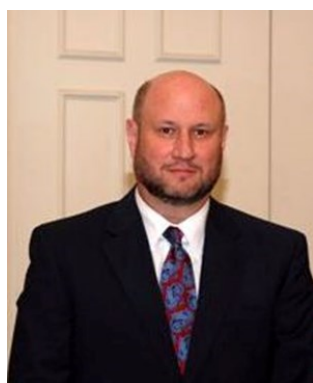
Mr. Wehrle holds a Bachelor of Science degree in engineering from the U.S. Military Academy, West Point, New York (1970), and a Masters Degree in business administration and management from the University of Utah, Salt Lake City, Utah (1979). He is also a graduate of the Air Force Air Command and Staff College (1983) and the National War College (1987).



Investigator Ian Tedder, North Carolina Department of Insurance-Criminal Investigations Division

Ian has a B.S. degree in Criminal Justice and Criminology from Mount Olive College and a Master of Justice Administration degree from Methodist University. Ian is also a graduate of the Criminal Investigations Certificate Program from the North Carolina Justice Academy and he is a North Carolina Certified Fire Investigator. Ian is currently employed a criminal investigator with the North Carolina Department of Insurance – Criminal Investigations Division, where he also serves on the Davidson County Fire Investigation Task Force. Prior to coming to NCDI-CID, he has served as a captain with the Wilmington (NC) Fire Department – Fire Marshal's Office and a police detective with the

King (NC) Police Department. Ian also currently serves on the board of directors for the North Carolina Chapter of the International Association of Arson Investigators. He is also a past president and board officer for the North Carolina Insurance Crime Information Exchange. Ian has conducted presentations on fire and insurance fraud investigations for NCICIE, IASIU, and SE-IAATI.



Lane Roberson, North Carolina Farm Bureau Insurance

Lane has a B.S. Degree in Physical Education from UNC Greensboro, 1982. Lane has earned insurance designations of Fraud Claims Law Specialist and Certified Insurance Fraud Investigator. He worked as a Greensboro Police Officer from 1984 until 1989 in the patrol division. He began his insurance career as a claims adjuster with Integon Ins. in 1990 and became Integon's first special investigator in 1992 through 1997. Lane then worked as a senior special investigator with Atlantic Causality Ins. which became Guaranty National Ins. and Orion Auto Ins. Since 1999 to the present he has worked as a senior special investigator for N.C. Farm Bureau Insurance. Lane has worked insurance investigations in 32 states. He has held offices in the North Carolina Insurance Crime Information Exchange and is currently a state board officer for the NCIAAI. He is also a member of IAATI and IASIU.

64th INTERNATIONAL SEMINAR

Instructor Biographies: (continued)

Senior Policy Advisor David P. Lewis, Bureau of Justice Assistance

David P. Lewis is a Senior Policy Advisor for the Bureau of Justice Assistance responsible for a number of successful justice information sharing projects like the, the National Motor Vehicle Title Information System (NMVTIS) Law Enforcement Access Tool (LEAT), the Nationwide SAR (Suspicious Activity Reporting) Initiative (NSI), and was the lead in the development of National Sex Offender Public Registry (NSOPR). His oversight portfolio includes the Regional Information Sharing Systems (RISS), the National White Collar Crime Center (NW3C) and is BJA's lead on several cybercrime initiatives and numerous field initiated information sharing projects.

Before joining BJA, David served as the Project Director for both the Ohio Justice Information Network (OJIN) and the Ohio Juvenile Justice Information System (JJIS) at the Ohio Office of Criminal Justice Services, a Governor's Cabinet Agency. Prior to moving to Columbus, Ohio, he served 24 years in law enforcement retiring from the Cranberry Township Police Department, Pennsylvania, as the Support Services Commander in charge of training, community programming, D.A.R.E., Internet/high tech investigations, media relations, and the department's computer projects.

David is a respected practitioner, presenter, and author in the areas of school safety, Internet awareness, computer crimes, justice information sharing, community policing, and media relations. He holds a Bachelor's Degree in Criminal Justice from the University of Dayton, a Master's Degree in Regional Planning from the California University of Pennsylvania, and a dual MBA in Business Management and Information Systems from Point Park University, Pittsburgh, PA.



John Bull, North Carolina Farm Bureau Insurance

Currently lives in Winston-Salem, NC. Upon High School graduation, served in the Army's 82nd Airborne Division (3rdBn. 504th PIR - 1st. Brigade) Fort Bragg, NC and as a Drill Sergeant at Fort Jackson, SC. Earned Combat Infantry Badge (CIB) and Expert Infantry Man's Badge (EIB).

Graduate of NC State University with a B.A. in Sociology (Criminal Justice) & Minor in Political Science.

Agent with NC Alcohol Law Enforcement & Vice Narcotics Officer with Stokes County Sheriff's Office.

Began Insurance Career with Integon/GMAC Insurance before leaving for NC Farm Bureau Insurance. Currently serving as a Senior Special Investigator for the last 11 years with North Carolina Farm Bureau Insurance.

North Carolina Insurance Crime & Information Exchange Investigator of the Year, Certificates/letters of Commendation from North Carolina Dept. of Insurance & National Insurance Crime Bureau (NICB).

Professional Organizations: International Association of Special Investigation Units (IASIU), North Carolina Insurance Crime & Information Exchange (NCICIE), International Association of Auto Theft Investigators (IAATI), International Association of Arson Investigators (IAAI) & National Association of Bunco Investigators (NABI)

Certifications/Designations: Certified Insurance Fraud Investigator (CIFI), Senior Claims Law Associate (SCLA), (I-CAR) Gold Class Certified, Completed BATF Advanced Arson Investigation Techniques.

Additional Instructor Biographies will be published in the July issue of Auto Theft Today

64th INTERNATIONAL SEMINAR



64th ANNUAL IAATI SEMINAR

August 7 – August 12, 2016

EARLY REGISTRATION FEE \$275.00 (USF) Prior to July 1, 2016

LATE REGISTRATION FEE \$300.00 (USF) AFTER JULY 1, 2016

PLEASE PRINT OR TYPE:

Name:	Rank/Title:			
Department:	Phone:			
Address:	City:			
State:	Zip:			
Email:	IAATI Membership # (required if paying member registration fee) \$40.00			
Seminar Tuition:	Early Regis- tration	\$275.00	Late Regis- tration	\$300.00
Companion Banquet Tickets Companion Name:	Guest Wel- come	\$50.00		
Total Fees Enclosed:				

******ON-LINE REGISTRATION THROUGH PAYPAL IS ENCOURAGED*******

If you are paying online, please submit this form via the email button on the top of this page and make payment through the PayPal button on the IAATI conference webpage. Non Members please submit an IAATI membership application with your registration form available at www.iaati.org.

If you are paying by check/mail, please mail this form and a check made payable to: "IAATI 2016" to the following address: IAATI 2016 Seminar P.O. Box 223 Clinton, NY 13323-0223 USA (PLEASE DO NOT MAIL CASH)

Lodging Information/Host Facility:

Embassy Suites Nashville SE- Murfreesboro

1200 Conference Center Blvd Murfreesboro, Tennessee 37129

Phone: (615)-216-5363 or (800) 228-9290

Room Rates: King or Double - \$143.00 Triple or Quad - \$153.00 (includes breakfast and parking)

www.murfreesboro.embassysuites.com

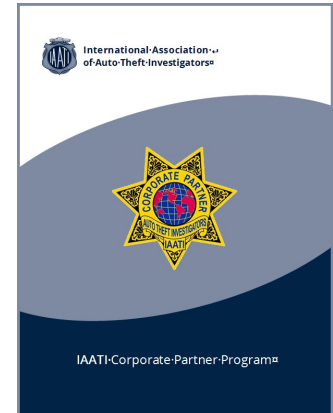
Use reservation code: AAATI for conference rate

64th INTERNATIONAL SEMINAR

- The 64th Training Seminar will be the year's major event and something not to be missed. It is also a great opportunity for companies to join us in Murfreesboro as a sponsor and/or exhibitor and promote their products and services. The **Sponsorship Committee** is keen to work with any interested parties and has released its **Corporate Partnership brochure** which offers companies the unique opportunity to:
 - support IAATI's activities in the development and education of professionals involved in the fight against vehicle crime
 - assist with the provision of face to face and on-line training,
 - facilitate the development of local, national and international networks across agencies and industries.

In addition the Corporate Partner program also offer opportunities for you to forge special relationships with IAATI members and create a dialogue with the membership through an array of marketing and promotional elements.

IAATI relies heavily on the generous support of our Corporate Partners so please consider partnering with us. For full details download the brochure by clicking on the image on the right [or using this link:](#)



	Diamond	Platinum	Gold	Silver
Package Costs (\$US)	\$7,500	\$5,000	\$3,500	\$2,500
General Advertising/Promotional Benefits				
Use of IAATI Corporate Partner Logo	✓			
One email blast to the entire membership sent by IAATI on your behalf	✓			
Advertising on IAATI website (includes placement of logo and link to website and link to your company website)	12 months	6 months	6 months	3 months
Inclusion of company profile in <i>Auto Theft Today</i>	✓	✓		
Opportunity to have any company specific training material (videos, publications, PowerPoint presentations, reference guides, links to website tools, etc.) included in the Member's only area of the IAATI file library.	✓	✓	✓	✓
Annual International Training Seminar Benefits				
Seminar Banquet Sponsor	✓			
Break Sponsor		✓		
Complimentary tickets to the Annual Training Seminar	4	3	3	2
Complimentary tickets to the President's Reception	4	3	3	2
Complimentary tickets to the Seminar Banquet Dinner	4	3	3	2
Exhibitor Booth 8 x 10	✓ Double booth	✓	✓	✓
Electricity to exhibitor booth	✓	✓	✓	✓
Signage	✓	✓	✓	✓
Wi-fi	✓	✓	✓	✓
Logo and contact information published in seminar handbook	✓	✓	✓	✓
Inclusion of company logo and links to your website in the IAATI Mobile Seminar App	✓	✓	✓	✓
Entry to nightly networking Hospitality events	✓	✓	✓	✓
Opportunity to present to the delegates during the 'Sponsors Presentations' session	✓	✓	✓	✓
Opportunity to include promotional material in Seminar delegates registration packs	✓	✓	✓	✓

SPONSOR SPOTLIGHT



**HAVE YOU TAGGED
YOUR VALUABLES YET?**

FORTUNATELY WE USE ADVANCED MICRODOT TECHNOLOGY

Recoveri Dot provides an advanced on line asset registration and tracing solution through innovative technology and microdot integration. Valuable assets can now be tagged with permanent and nearly invisible microdots that can be read physically with a Recoveri Microscope and identified with an ultraviolet light for ease of detection. Assets are registered in a secure online database where ownership of goods can be traced locally and internationally. The HOTDOT® feature provides quick feedback on stolen assets, which has made it popular with Police and law enforcement agencies.

For more information contact 719 357-5717 or visit www.usa.recoveri.net

RECOVERI
TAG WHAT'S YOURS

MEMBERS ARTICLES

In memory of Dave Dempsey, Immediate Past President of Southeast Regional Chapter

The following article has been submitted by Rusty Russell, 2015/16 SERC President in fond memory of his buddy and colleague Dave Dempsey who passed away on 29 March 2016. Dave was a proud member of Florida law enforcement for over thirty five years. He was a devoted husband, brother, father and colleague and a friend to all he met. Dave was a very active member of IAATI having served as the 2014/15 President of SERC. He was a great friend and mentor to many and will be sadly missed.

On March 29, 2016, the immediate past President of the Southeast Chapter Dave Dempsey, passed away at the early age of 58. For most people Dave's passing came as an unexpected shock. In fact, most people didn't know that just several months earlier he had been diagnosed with a terminal illness. Even the few of us who knew about his diagnosis were surprised to discover that his death had been hastened after he contracted pneumonia like symptoms. That was the essence of Dave Dempsey, what you saw on the surface was only a small part of the person underneath. So what can you say about someone you consider a close friend and who departs this world far too early? While I could tell you about all of his great strengths I'd rather tell you about one brief moment in time that I believe signifies the kind of guy he was. First, it's important to know that for one reason or another Dave always seemed to be the target of some form of harassment. Second, whether he was entertaining us with one of his true, but hilariously funny tales of adventures on their farm or something else he had done, he was always quick-witted and amusing. Funny, as I write this I can almost hear him saying "why you gotta tell them all that..."

Dave and I were both members of the Florida Highway Patrol's Statewide Cargo Theft Taskforce. As such, we often worked cargo theft sting operations across the State deploying decoy trailers. At the time, Dave was a Special Agent with the National Insurance Crime Bureau (and reserve deputy with Gadsden County Sheriff's Office) and I was an auto theft detective with the Saint Lucie County Sheriff's Office. The nature of work often meant downtime during the daytime hours as we generally worked nightshifts. Dave and I shared a kindred spirit in so much that neither of us spent our days sleeping, rather off somewhere trying to find a way to pass the time.

Early one Sunday I called Dave and asked he if would like to accompany me on an overflight mission to look for stolen vehicles. Without hesitation he was ready to go. In south Florida one common way of disposing of stolen vehicles is to submerge them in nearby canals or bodies of water in hopes they will never be found. The submersion eliminates many of the common methods of processing for evidentiary purposes as well as accomplishes the goal of concealing the location of the vehicle. What the criminals fail to realize is that all of those oil based fluids eventually end up escaping from the vehicle and leave behind a tell-tale trail of evidence that is easily seen from the air.



Continued on the next page

MEMBERS ARTICLES

In memory of Dave Dempsey, Immediate Past President of Southeast Regional Chapter (cont.)

We loaded up in the helicopter, lifted off, and began our search of area canals for stolen vehicles. After about 45 minutes it appeared our efforts were all for nothing, and we were almost finished with our overflight, when Dave's voice yelled over the intercom "I see it, I see it." Sure enough there it was, the distinct sheen of oil bubbling up from the depths of the murky brown water. Several slicks were strung out along the flow of the current. Dave was so excited I thought he might fall out of the helicopter as he craned his neck out the open door to inspect his findings. We made note of the location and headed back to the hangar. I explained to Dave that I would get the dive team out first thing Monday morning to recover the still unknown vehicle. Our cargo theft operation was set to end on Monday and everyone was scheduled to head home, but not Dave. He quickly explained to me there was no way he was going to leave for home (which was about a six-hour drive for him) until he saw that vehicle pulled out of the water.

That Monday morning was unseasonably cold and not exactly the type of weather you prefer when scuba diving. When I picked Dave up he was wearing a raid jacket emblazoned with the "NICB" initials on the back of the jacket. We drove out and met the dive team at the location. After some grumbling and complaining about the weather the dive team suited up in full wetsuits, grabbed their tanks, and made their way into the murky abyss of the canal. To document the recovery of the vehicle Dave decided to photograph the event. He took photos of the dive team preparing to enter the water, and I took one of him standing on the edge of the bank in anticipation of his next vehicle recovery. After several minutes of searching, we saw the bright yellow float buoy break the surface of the water. The dive team had located a late model sport utility vehicle sitting on the bottom of the canal. The divers retrieved the cable from the waiting rotator wrecker and we watched as the wrecker slowly winched up Dave's find and plucked the vehicle from its watery grave. The vehicle turned out to be a late model Volkswagen Touareg. The gas pedal had been wedged down with a broom stick and the vehicle was still in drive. The vehicle had been reported stolen out of Palm Beach County. Dave seemed almost giddy at the fact that his observation had led to the recovery of this stolen vehicle.

In the days following that photograph of the divers on the edge of the canal bank, and Dave wearing his NICB raid jacket, just seemed to beckon a Photoshop moment. So the NICB logo found its way onto the back of one of the diver's wetsuit. I sent the 8 x 10 photo to Dave. I can almost hear Dave now saying "You rat bastard, why you gotta do me like that!" That seemed to be one of his favorite sayings, perhaps because he was always on the receiving end of some sort of prank. Yet in quintessential Dave fashion he knew immediately what he intended to do with that photo. During a performance review he retrieved the photo, presented it to his supervisor, and explained "there are no depths I won't go to make a recovery." Dave said that for just a few moments his supervisor looked perplexed, as if he



MEMBERS ARTICLES

In memory of Dave Dempsey, Immediate Past President of Southeast Regional Chapter (cont.)

actually thought that Dave had been the diver who recovered the vehicle, and that he couldn't figure out where Dave had gotten a wetsuit emblazoned with the NICB logo. Dave said they both enjoyed a good laugh about the photo.

Throughout our lives we occasionally are lucky enough to meet, and make friends with, people who affect the destiny of our own lives. Dave Dempsey was one of those people. I can honestly say that he was a great friend, mentor, and someone I always could rely on. In large part, he's the reason that I became a Special Agent with NICB. So what can you say about someone you consider a close friend and who departs this world far too early? I'm not certain exactly what one should say, but I think it's as simple as; I'll miss you buddy, thanks for everything!

Lawrence "Dave" Dempsey 1957—2016

Lawrence "Dave" Dempsey, 58, passed away on March 29, 2016, after a brief illness. He was born in Staten Island, NY and resided in Daytona Beach, Ft. Lauderdale, and Georgia before moving to Tallahassee, FL in 2002.

He is survived by his wife and best friend of over twenty-five (25) years Emily Beyer of Tallahassee, FL, sister Jill Dempsey Arner of Palm Coast, FL, sister Debbie Pensiero of Ijamsville, MD, and daughters Megan Dempsey, Amanda Royer, and Kayla Dempsey of Palm Coast, FL.



Dave was a proud member of Florida law enforcement for over thirty five (35) years. He was a devoted husband, brother, father, and colleague. He was a friend to all he met. Dave was an estate auction enthusiast who was always on the hunt for that special treasure. If not at an auction, he could be found at Lake Talquin or at St. George Island fishing. Dave will be deeply missed by everyone whose lives he has touched over the years.

MEMBERS ARTICLES

Your Witness Was Right in Front of You

By Brook T. Schaub

In my previous career in law enforcement, a portion of it was in the Auto Theft Unit, and as a member of IAATI. I even had the privilege of coordinating the IAATI conference when it came to Saint Paul, MN. As an IAATI member, many of the good ideas learned were brought back to St. Paul and put into use. We initiated a CAT program, and we were one of the first to use a bait car, albeit with very primitive technology available at the time.

My career eventually led to computer forensics and writing a grant that started the Minnesota Internet Crimes Against Children Task Force. When I retired, a national accounting firm reached out to drag me off the lawn tractor to perform computer forensics for business litigation in their forensic accounting unit. Some of my cases are for insurance SIU units. Evidence related to arson cases and suspected insurance fraud.

I received a call from an SIU agent one day asking about what information could be obtained from a motor vehicle. The car was reported stolen by the owner, after it was involved in an accident with a parked car a few blocks from the owner's residence. The owner's boyfriend had possession of the vehicle at the time. The occupant(s) had fled the vehicle. We were not talking about the Event Data Recorder evidence, but something new, the Infotainment and Telematics system.

Lacking the knowledge, I forced myself to attend a conference in Las Vegas, during a Minnesota winter, where a presentation of vehicle forensics was made by the company Berla (www.berla.co). I have been doing computer forensics for 20 years, and never had heard of vehicle resources for evidence other than the EDR. I eventually attended their software class. I have since started to spread the word to local law enforcement and others about what is being missed in vehicle evidence. The vehicle evidence value is just too good not to share immediately.

Since 2008, most American made cars have an Infotainment system. If you ever opened your car door and saw the "drivers door ajar" light, this was logged into the Infotainment System (IS). Turned on the lights? Put the gear in drive? Sync your cell phone? Plug in an iPod? All this, and more is documented in modules within the vehicle (time/date stamped) with odometer readings. If the vehicle has a Navigation system, even more information is available.

So let's take the scenario provided by our SIU agent above, and match it with computer forensics. First we will assume that the vehicle can be forensically examined, not all vehicles can, but most American brands, and some foreign brands can. We pull the modules from the console or behind the dash, hook them up to specialized circuit boards, and run them through the software on our laptop.

At the time of the accident, our examination shows that the boyfriend's cell phone was synced to the vehicle at the time it hit the parked car Figure 1. The cell serial number, and cell brand are documented from the time it is synced to the vehicle, until it is un-synced. His phonebook, call logs Figure 2, and text messages are present in the exam Figure 3. Just before the accident, he sent a text to the vehicle owner saying he was on his way home, or made a phone call. Either example is documented with time/date stamps in the modules. Even longitude and latitude may be present. If a navigation system is present, log files of the vehicle's travels are recorded Figure 4. The driver had a few friends with him that night, information on their phones syncing to the IS might also be available, as well as their doors being "ajar" when opened Figure 5. Slim Whitman's Greatest Hits was playing on the IS at the time of the crash and the module time/date stamped an iPod plugged into the USB and documented the drivers lack of taste in music Figure 6. The screen shots in the Figures are not based upon this exact case, but only as examples of the data available.

Think of the value of this information (and much more) on not only your cases, but homicide cases, abductions, being able to show the suspect's car trunk being opened 5 minutes before and two blocks away from a drive-by shooting.

MEMBERS ARTICLES

Your Witness Was Right in Front of You (continued)

Figure 1.

The screenshot shows the 'iVe - Infotainment & Vehicle System Forensics' application. The left sidebar contains a 'CONTENT' tree with categories like Applications, Connections, Devices, Events, Call Logs, Media, and Navigation. The main window displays a grid of Bluetooth connections with the following data:

Device Name	Device Type(int)	Device Type	Unique Number	Unique Number Type
Erin's iPhone	3	Phone-3	A888083AE07F	Bluetooth Address
Ben's iPhone	3	Phone-3	B8E85688ED20	Bluetooth Address
T7380	3	Phone-3	38E7D825E758	Bluetooth Address
rola	3	Phone-3	E89C43E8A97	Bluetooth Address

Figure 2.

The screenshot shows the 'iVe - Infotainment & Vehicle System Forensics' application with the 'Call Logs' view selected. The main window displays a grid of call log entries with the following data:

Start Time	Phone Number	Contact Name	Call Type	Device Identifier	Flags
04/24/2014 07:09:08 PM	4102539074	Ken Case	Outgoing	88E85688ED20	None
04/25/2014 06:47:19 PM	+14102539085	Erin LeMere	Outgoing	88E85688ED20	None
04/25/2014 07:08:09 PM	18003913000		Outgoing	88E85688ED20	None
04/25/2014 07:10:40 PM	18002662278		Outgoing	88E85688ED20	None
04/25/2014 10:09:32 PM	+14342841315	Darin	Outgoing	88E85688ED20	None
04/27/2014 02:47:33 PM	4102539085	Erin LeMere	Outgoing	88E85688ED20	None
04/28/2014 05:44:09 PM	3013957309		Outgoing	88E85688ED20	None
04/28/2014 09:12:08 PM	+14342841315	Darin	Outgoing	88E85688ED20	None
04/13/2014 11:08:32 PM	8002662278		Missed	88E85688ED20	None
04/14/2014 10:22:02 PM	4109231425	Erin LeMere	Missed	88E85688ED20	None
04/16/2014 04:58:34 PM	2526861552	Tiffany Lozada	Missed	88E85688ED20	None
04/17/2014 10:29:05 PM	3107684185		Missed	88E85688ED20	None
04/18/2014 11:05:33 PM	4342841315	Darin	Missed	88E85688ED20	None
04/20/2014 11:52:53 PM	4102126566	Gene Olmo	Missed	88E85688ED20	None
04/21/2014 02:27:24 PM	4102539085	Erin LeMere	Missed	88E85688ED20	None
04/21/2014 04:20:49 PM	4342841315	Darin	Missed	88E85688ED20	None
04/22/2014 05:09:49 PM	8004633339		Missed	88E85688ED20	None
04/22/2014 07:14:16 PM	4102539085	Erin LeMere	Missed	88E85688ED20	None
04/22/2014 10:42:14 PM	4438711316	Buzzy	Missed	88E85688ED20	None
04/23/2014 05:13:38 PM	4102539085	Erin LeMere	Missed	88E85688ED20	None
04/23/2014 09:21:54 PM	4342841315	Darin	Missed	88E85688ED20	None
04/23/2014 10:38:29 PM	8473726777		Missed	88E85688ED20	None
04/24/2014 05:45:14 PM	4102539085	Erin LeMere	Missed	88E85688ED20	None
04/24/2014 09:38:08 PM	4342841315	Darin	Missed	88E85688ED20	None
04/25/2014 06:45:57 PM	4102539085	Erin LeMere	Missed	88E85688ED20	None
04/28/2014 08:38:48 PM	6303184762		Missed	88E85688ED20	None

MEMBERS ARTICLES

Your Witness Was Right in Front of You (continued)

Figure 3.

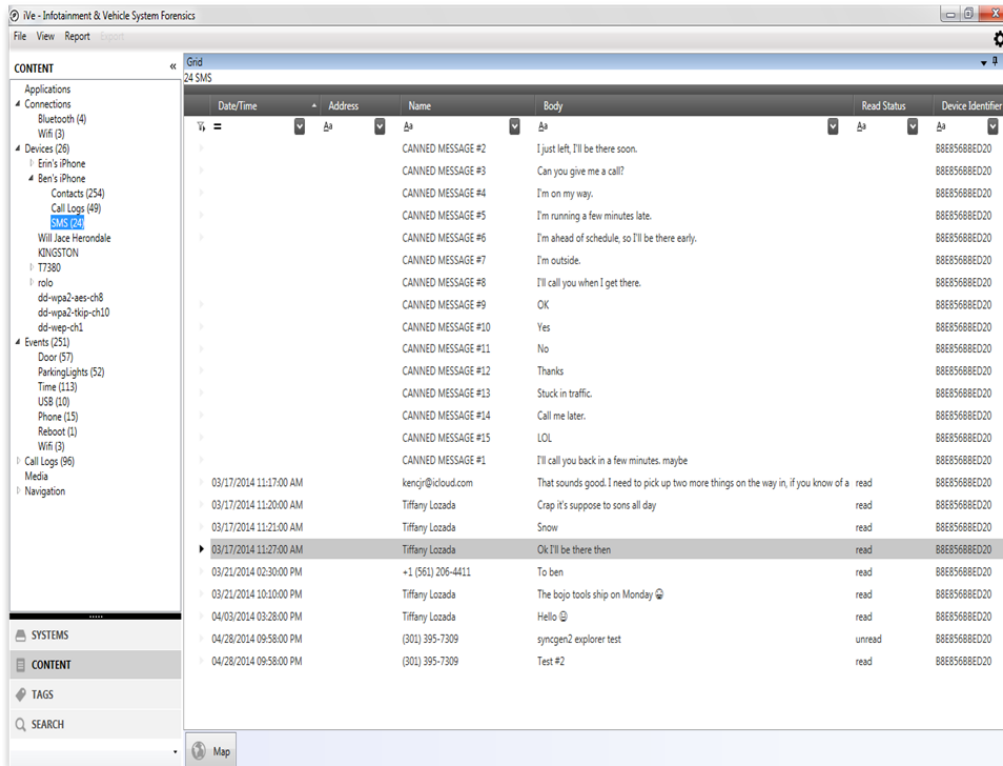
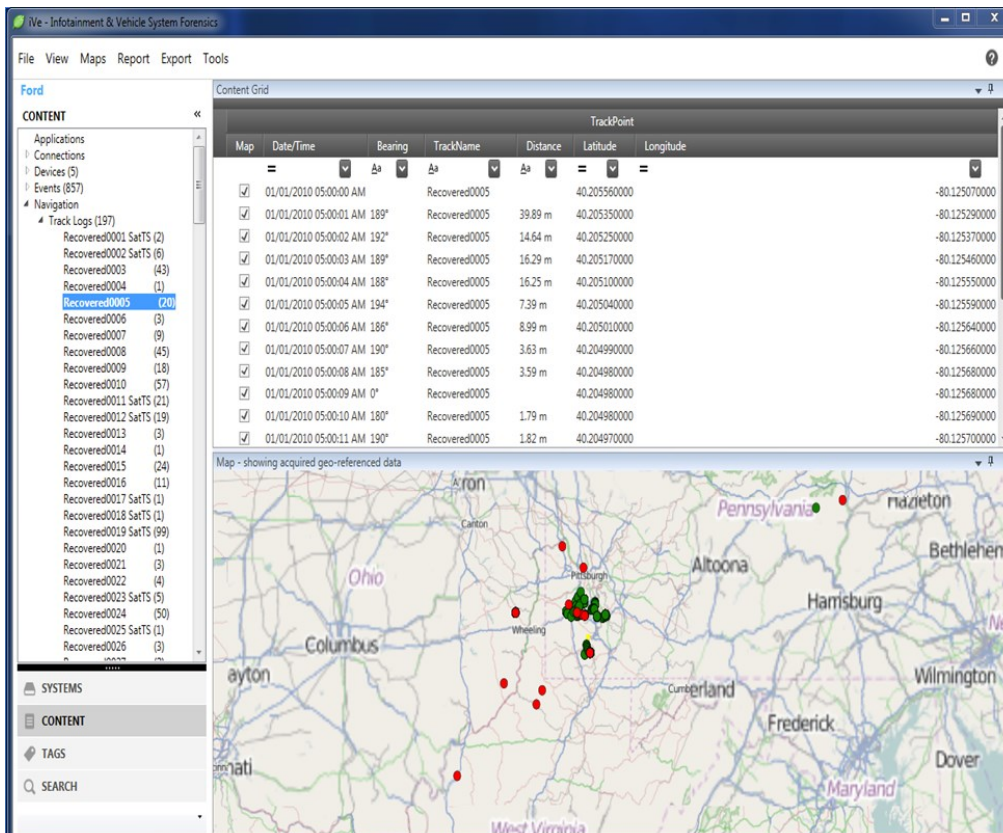


Figure 4.



MEMBERS ARTICLES

Your Witness Was Right in Front of You (continued)

Figure 5.

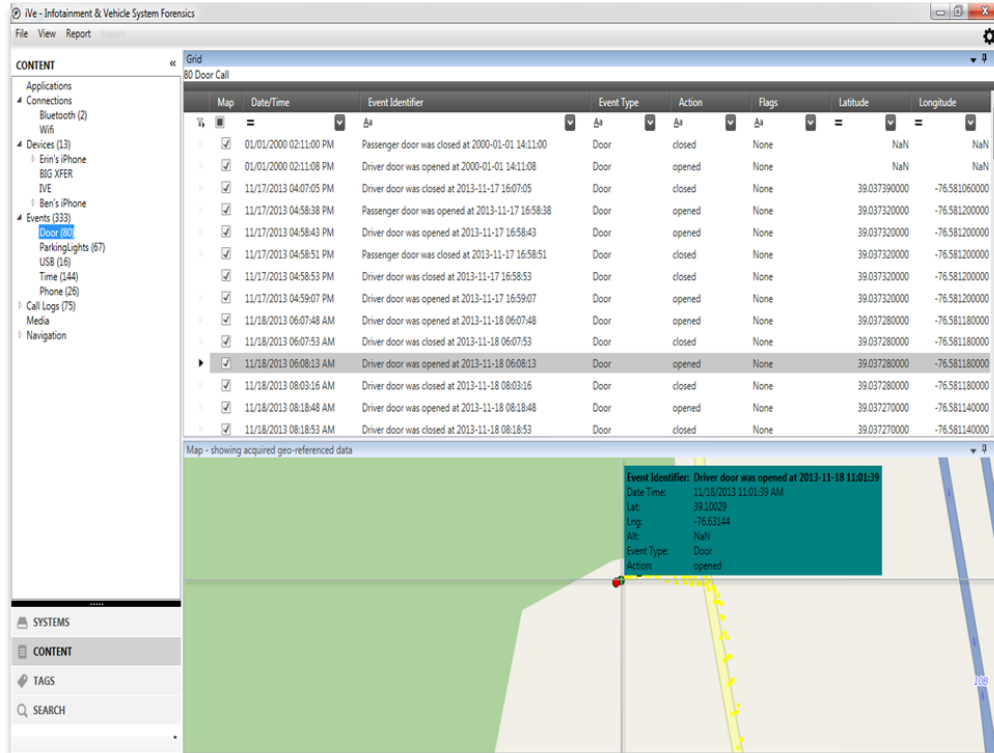
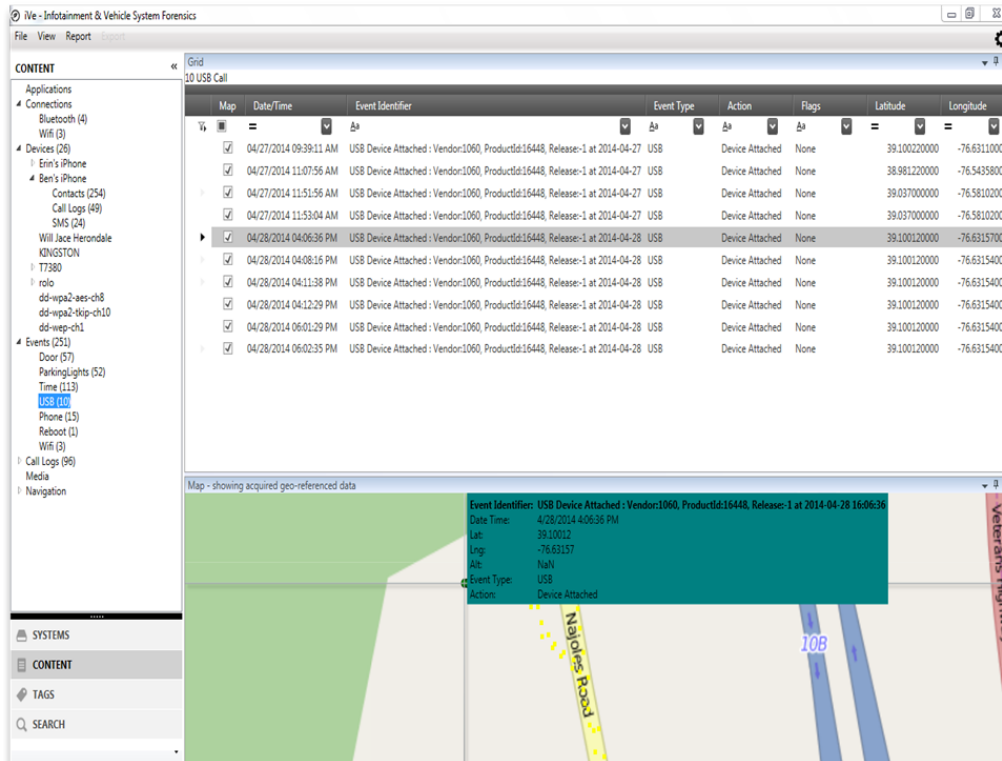


Figure 6.



MEMBERS ARTICLES

Your Witness Was Right in Front of You (continued)

So, we now know the value, we now know the technology is there, we just need to know how to get it. To my knowledge, Berla is the only company at this time providing the software, hardware, training, etc. I have no connection to Berla, in fact I really can't use the knowledge on behalf of my company. We would have to charge too much to clients, e.g. insurance companies, to make any money.

The advantage of IAATI, and NICB pushing to obtain the resources, either by enhancing the existing computer forensic cops already employed at an agency, having NICB take the lead, or other avenues, is that many states have auto theft prevention grant programs that would pay for the training, software, hardware, and yearly subscriptions. Nothing prevents the skills learned from being used for a larger range of crimes outside of auto theft cases.

Brook T. Schaub (Retired Saint Paul Police)
Manager Computer Forensics/eDiscovery
Eide Bailly LLP
800 Nicollet Mall Suite 1300
Minneapolis, MN 55402
bschaub@eidebailly.com

(All Screen Shots courtesy of Berla.co)

Request for assistance: International Association of Chiefs of Police, Vehicle Crimes Committee

The International Association of Chiefs of Police (IACP) is a dynamic organization that serves as the professional voice of law enforcement. One of the IACP's committees is the Vehicle Crimes Committee. This Committee studies, considers, and determines the various methods and means by which vehicle crimes are committed, including the make and type of vehicles most commonly stolen; surveys, investigates, and evaluates the techniques and methods employed by the police and other agencies in solving and reducing the incidence of vehicle crimes cases; and reports to this Association for the dissemination to all interested agencies all pertinent information and recommendations that will reduce the incidence of this major crime.



The Vehicle Crimes Committee is currently working on an initiative to show the chiefs'/sheriffs the importance of having (or keeping) a dedicated auto theft unit. Stolen vehicles are routinely used in the commission of other, and often times, more serious offenses. The committee is wanting to show the chiefs/sheriffs the connection between auto theft and the other crimes committed as a way to impress upon them if there is any way possible, they should have an auto theft unit.

This endeavor is quite difficult as the current reporting methods do not provide the data we would like to see. The Vehicle Crimes Committee is asking for everyone's help by providing examples of cases they have investigated where a stolen vehicle was used in the commission of other crimes. **Please respond directly to Nathaniel McGanty (IACP Vehicle Crimes Committee Member) at nmcganty@cityofchesapeake.net**

The article on the next page was authored by Justin Powell and Board members of the UK Branch in response to this request.

MEMBERS ARTICLES

Why We Need Stolen Vehicle Units

Overview

It is a shame we now live in a world where budgets and cost saving having become a key focus for all, said austerity measures have now caused a knowledge gap and loss of specialist areas tackling vehicle criminality. This is certainly the case in the UK when it comes to budget spends in public sector services and has been for some years now. With this in mind it is inevitable that the wheels will eventually come off and large gaps in knowledge and skills have widened already. This is certainly the case when it comes to the demise of mostly all of the UK's Stolen Vehicle Units (SVU's).

Crime methodologies have changed over this period and is the biggest threat we now globally face is managing the international trading arena of the internet and policing of it.

This was apparent at the recent Interpol Global Vehicle Crime conference in Bangkok. It highlighted many of us are seeing the same methods of crime involving vehicles. It is just our geographic locations that cause issue in us all joining the dots.

Another issue we have is global trading commodities; vehicles, metal, drugs and people can all be trafficked. If it has value over here, move it over there... it can still fetch the same financial return and if you paid nothing for it here, the result is almost pure profit. If 'your' goods are intercepted, what have you lost? This IS a real problem.

Most crime is geared for serious financial gains. In the examples, all can and do return serious amounts of revenue although the one through-line, the common denominator, for all is vehicles; they are the 'enabler' to facilitate all.

Stop or at least track the vehicles stolen or involved in crime and we may stand a better chance to curb not just vehicle crime but also many other types of crime. We need more joined up and collaborative thinking between law enforcement and private sector tackling all areas of vehicle crime across the globe. **'A Partnership Approach'** IS seriously required in order to achieve this and I believe that anyone reading this now would agree, we are now dealing with more sophisticated, organised, tech savvy and ruthless types of criminal. My belief is opportunistic crimes may be on the demise but a new 'Migratory' criminal has now emerged. This criminal has no disregard for law enforcement, is acutely aware that cross border, cross countries or continents hides their activities much better. It may take more organisation and thought but when stolen vehicles can fetch £100,000 plus per unit and you can fit 2 in a 40 foot shipping container and ship it anywhere for approx £2,000 you will see the serious ROI (Return on Investment) crime now offers. I would offer that whoever came up with quote **'Crime Doesn't Pay'** clearly did not come from the times we live in now.

Criminals have been a lot quicker to adopt current technologies, why wouldn't they? The internet is a perfect tool for the criminals. It gives anonymity, the ability to present oneself as something they are not, vaster resource to purchase tools and kit without detection, a global audience in which to sell on their stolen commodities and again global online portals help them facilitate this perfectly. How is law enforcement ever going to tackle and track brown parcel deliveries? Does your average consumer vet or scrutinise the online seller when they can buy vehicle parts for much less than a genuine seller? I doubt it.

A fellow IAATI UK member summed it up better than I can, many years ago now. *'You can bet that 99% of the vehicle drivers on the road are just your average Joes going about their daily lives. You can also bet that 99% of criminals will use vehicles to commit or enable other crimes'*. It has never left me this quote. It is one of the reasons that convinced me to become a member in the IAATI family. This organisation has taught me so much over the years but what I am seeing now is a very current and real threat in all areas of vehicle criminality. Trouble is many people I could've gone to for help, advice and guidance have now moved on with the demise of all our SMU's in the UK. We appear to have painted ourselves into a corner and removed the collective knowledge on the subject we once held. Criminals are not stupid, they are acutely aware of this also and I think this factor goes a long way to explaining why we all have such a problem now and it will continue to grow.

Continued over the page

MEMBERS ARTICLES

Why We Need Stolen Vehicle Units (continued)

Vehicle Crime has taken me all over the world in the last few years to discuss the subject. I have never stolen a vehicle in my life but the simple math is; I and others cannot all be as busy as we are right now if there was not a real global problem involving vehicles, theft of and enabled crimes. Think on.

Now is the time to act. Forget what we think we know about vehicle crime, that it simply causes inconvenience, some distress and hardship for the owner and that an insurer will return the victim to the situation they were before. Do not be lulled into the false sense of security brought about by post-2000 vehicle security improvements. We are in a new age; that of the 'connected-car'.

At a time when technology engulfs us and packed into vehicles, we find it bizarre that SVU's are diminishing. This is the time to invest in such departments. Law enforcement is notorious for playing catch-up, with criminals being ahead of the game as they spot the opportunities. How long before we will be so far behind that catch-up will be impossible or require incredible resourcing? We do not believe the idiom 'a stitch in time saves nine' is archaic, irrelevant

We are not standing still, we are going backward. As each SVU is closed, so the gap in our expertise and knowledge widens. It is these holes that criminals exploit.

SVU's need to exist and need to evolve. The crime is specialist, the subject matter (vehicles) are specialist. SVU's require support and training to address the growing trend in vehicle crime and to support most other investigative law-enforcement departments whose crime have a vehicle, if only on the periphery i.e. as a get-away, to transport illicit items or to assist in funding. Few crimes occur without the involvement of a vehicle and some crimes are committed to fund a vehicle purchase or use funds from vehicle crime to fund other crimes.

A vehicle is at the centre of an individual's daily life providing them with freedom of movement, the ability to socialise, work or just for 'fun'. They are status symbols for some, necessity for others. But most have at least one. This applies to the criminal fraternity ... so why would we ignore this asset that unlikely many which are kept behind locked doors (home, work or bank as examples), is identifiable and on public display?

Look about you, how many vehicles do you see? What value of cars do you believe sit on the street where you live? These cars are ripe targets and there are many who look to exploit them.

An SVU also represents a deterrent. In the absence of a deterrent, is vehicle crime more or less likely to flourish?

This is a rhetorical question; obviously criminals have no concern for our budget cuts, that we lack resources. Sympathy is the last thing we can expect and to think otherwise is to be deluded. Criminals exploit weaknesses. Maximum return for minimum investment is the approach coupled with a desire to retain their freedom. In the UK we had a TV series called 'Porridge' (slang for imprisonment). The opening credits included the main character, a small time crook stating that being caught was an 'occupational hazard'. We need to make this a reality for criminals rather than provide them an opportunity.

Justin Powell

President – IAATI UK

A Police Perspective

There has now for a number of years been a reduction of specialist vehicle crime units throughout the UK due to financial cutbacks and amalgamations. Many forces have centralised units and closed police stations in order to fit into the yearly fiscal budget imposed upon them by the government. In order to maintain front line policing, specialist unit have borne the brunt of cutbacks.

Having served for 30 years in London's Metropolitan Police and for the last 8 in the Stolen Vehicle Unit part of New Scotland Yard's specialist crime command I have seen the direct correlation between this reduction and criminal trends.

MEMBERS ARTICLES

Why We Need Stolen Vehicle Units (continued)

Back in the 1990's this unit was 30 strong, now there are less than 10.

Having had to report to the industry concerning crime trends and crime figures it was well noted that although crime reporting had reduced over the last few years, vehicle crime was one of the only recorded crimes that had actually increased. Criminals know Police procedure, they have for many years and in this age of transparency they know it even more so. They know the problems with cross border crime, they understand that resources are strained and they know that specialist knowledge is getting less and less. To this end, they then take every advantage of this and expand their criminal enterprises.

Vehicle crime in the UK has reduced since the 1980's but, this is only due to greater security being placed on vehicles as a direct working relationship and knowledge sharing between Police Forces and the industry; working to understand how criminals behave and what weaknesses they exploit to steal vehicles. The theft of vehicles that we see today is organised criminality; this is a huge business for those involved. A large amount of money is to be made from stealing vehicles, whether it is being used as a getaway car to out run the police, commit burglaries or to break for parts, to ring and resell, or pay for other goods and debts.

A large amount of high value stolen vehicles taken within the UK are destined for other countries throughout the world. Police forces have in recent years been able to look at and seize criminal's money and assets under the Proceeds of Crime Act. Financial institutions automatically alert the authorities if suspicious or large amounts of money are moved around the banking system.

What better way to hide money and pay for goods than by stolen vehicles. On the black market particular vehicles command particular amounts and with the ever increasing recommended retail price of these vehicles edging towards 100,000 GBP mark, the black market value increases. It is well known, although hard to evidence, that vehicles are traded for drugs, guns and human cargos. Stolen vehicles are the best way to hide money and pay your debts. It is estimated that for every stolen vehicle found being exported out of the UK at least 4 get through. Many markets like Africa, Cyprus, and Trinidad and the Far East welcome UK stolen vehicles. Without mentioning specific people or operations I know that 2 specific joint operations conducted when I was a serving officer targeted family members of well known terror suspects. The vehicles stolen were taken out of the country and the sale of those vehicles fuelled terror campaigns.

I was involved with many successful operations against organised criminal networks stealing vehicles and exporting them. The networks were, and still are, extremely organized and targeted in what they want to take. The vehicles would be taken to feed certain markets in countries all over the world. These successful operations would normally lead to a jail sentence, it would frustrate the network, damage profits and cause fall outs. Dealing with those criminals who deal in vehicle theft, they are well organised and specialise in what they do and they make a great deal of money from the business. With the many 'off the record' conversations it is clear they have a great knowledge of Police units, police powers and police numbers. We cannot defeat them alone; Police Units with specialist knowledge needs to work with the industry to defeat them. A great example of this is the Construction Equipment Security And Registration (CESAR) Scheme. It was an idea from The Metropolitan Police Stolen Vehicle Unit, a specialist unit, a unit that knew the weaknesses of the products but also knew how, what and most importantly, why the criminals targeted certain plant equipment. Working with the plant industry it is now in its ninth year and it has reduced plant and agricultural thefts by 60%. This remarkable result only came from specialist knowledge and specialist understanding.

Certain forces within the UK have had specialist vehicle crime units axed and this has had a direct result of increasing the criminal activity in those areas. As mentioned, vehicle theft is one of the only crimes that has seen an increase in recent years. It is imperatively important to keep up this pressure on the criminal networks, to send a message to them that they run a high chance of being caught, and if caught, sent to prison and their assets taken. We slow them down and frustrate their operations. Through knowledge and experience specialised units get to know the criminal exploits and behaviors of these networks and in doing so continue to frustrate them and their business. Without this pressure they will be free to keep business as usual.

MEMBERS ARTICLES

Why We Need Stolen Vehicle Units (continued)

Simon Ashton

Metropolitan Police - Vehicle Industry Liaison Officer (Retired)
2nd Vice President – IAATI UK

Private Sector Funded Policing Model in the UK – NaVCIS

NaVCIS is the National Vehicle Crime Intelligence Service, a small Police Unit dedicated to the prevention and detection of vehicle crime and supporting our law enforcement colleagues both home and abroad. As part of the National Police Chiefs Council portfolio, we represent UK policing and provide support to National Crime Agency, UKBF and HM Government.

NaVCIS is at the heart of national vehicle crime related issues and is steadily growing its footprint in both public and private sectors, not only running its own operations and investigations but also disseminating key data, intelligence and advice to Police Forces, Industry, Government, Partners, Public and foreign enforcement agencies.

There are various strands to our work each working towards reducing vehicle-related crime. These are NaVCIS Fraud, NaVCIS Ports, NaVCIS Leisure, NaVCIS Agricultural, NaVCIS Freight and NaVCIS Intelligence (More information is provided in the attached PDF document).

Our primary task is to help reduce vehicle and vehicle-enabled crime by building knowledge in prevention, detection and monitoring techniques. Although theft of and from vehicles has fallen over the past 10 years, the use of vehicles in acquisitive crimes, such as burglary, serious and organised crime, cannot be overlooked. NaVCIS incorporates a number of specialist services working together to reduce vehicle crime and vehicle-enabled crime.

A few notable successes

- Through the work of NaVCIS and our partners, vehicles valued in excess of £17 million have been recovered in the last two and half years by NaVCIS Ports and nearly £34 million worth of vehicles have been recovered as a result of the work conducted by the NaVCIS Fraud team and their colleagues.
- Operation Britcar 2 day operation (28/29th April 2015) was led by the UK National Vehicle Crime Intelligence Service (NaVCIS) and supported by the INTERPOL Stolen Motor Vehicle (SMV) Task Force. During the operation, police inspected vehicles at the ports of Felixstowe, Dover and Portsmouth, identified as routes used by organized criminal groups to smuggle stolen vehicles to Southern Europe and Africa. Police recovered 18 stolen vehicles, including a caravan which had been reported just 40 minutes earlier, and arrested two individuals.

In June 2015, officers from the UK's, National Crime Agency (NCA) and National Vehicle Crime Intelligence Service (NaVCIS), working with the Uganda Police Force, carried out a number of searches at bonded warehouses across Kampala. Together they discovered a total of 36 high value cars stolen from the UK with a value in excess of £1 million.

It's worthy of note the number of specialist vehicle examiners has reduced across a number of forces in the UK therefore specialist resources like NaVCIS bring expertise that can add really value to local police forces/wider partners. Investment in analysis capability has been central to our growth working to understand regional/national threats in particular from organised crime groups towards promoting an evidence-based approach to both vehicle and vehicle enabled criminality.

References and UK Crime examples

All of the links below are aimed to support the above theories. All of the links below have been taken from UK Press on completion of many operations and investigations by UK Law enforcement. It is worth noting that all reference

MEMBERS ARTICLES

Why We Need Stolen Vehicle Units (continued)

examples compiled are collated from over the last 12 to 24 months. Take time to look through these, the images contained are very powerful representation of the threat we now face in the vehicle theft and vehicle 'enabled' crime arenas.

Follow the vehicles, you WILL find the other crimes;

Drugs:

<http://www.birminghammail.co.uk/news/midlands-news/70-years-drugs-gang-involved-10585866>

<http://www.bbc.co.uk/news/uk-england-29260777>

Murders and Drive-bys:

<http://www.standard.co.uk/news/crime/detective-london-gangs-using-stolen-mopeds-to-carry-out-murders-and-driveby-shootings-a3215281.html>

<http://www.liverpoolecho.co.uk/news/liverpool-news/policeman-killed-wallasey-hit-run-10197559>

Stripping and shipping:

<http://www.hamhigh.co.uk/news/crime-court/>

[hampstead car theft led police to lithuanian gang that stole 400 cars worth 10million 1 2261690](http://www.nation.co.ke/counties/mombasa/luxury-cars-import-racket/-/1954178/3139012/-/3jb8gi/-/index.html)

<http://www.nation.co.ke/counties/mombasa/luxury-cars-import-racket/-/1954178/3139012/-/3jb8gi/-/index.html>

<http://metro.co.uk/2016/03/24/head-of-3m-luxury-car-stealing-ring-told-to-pay-back-less-than-100000-5773510/>

<http://www.dailyecho.co.uk/>

[news/14375972.PHOTOS_The_1m_luxury_cars_stolen_and_found_in_a_car_lot_in_Uganda_are_back_in_Southampton/?ref=twtrrec](http://www.dailyecho.co.uk/news/14375972.PHOTOS_The_1m_luxury_cars_stolen_and_found_in_a_car_lot_in_Uganda_are_back_in_Southampton/?ref=twtrrec)

<http://www.westerndailypress.co.uk/Land-Rover-Defender-owners-warned-gangs-stripping/story-28829692-detail/story.html>

Burglary or 'Key enabled crime':

<http://www.dailymail.co.uk/news/article-2314843/Brazen-luxury-car-thieves-pictures-cash-sandwich-Facebook-jailed-series-raids.html>

<http://www.dailymail.co.uk/news/article-2564660/Dim-thieves-caught-police-posting-pictures-posing-luxury-stolen-cars-bikes-Facebook.html#ixzz458hDDkeb>

Simple Theft and disposal:

<http://www.autoevolution.com/news/motorcycle-theft-in-london-up-a-staggering-44-in-2014-105526.html>

<http://www.itv.com/news/calendar/update/2016-02-26/six-arrests-in-investigation-into-2-million-car-cloning-ring/>

Vehicle 'Enabled' Crime – Fraud:

<http://www.theguardian.com/uk-news/2016/jan/29/cash-for-crash-81-sentenced-easifix-garage-blackwood>

People trafficking and illegal immigrants:

<http://www.telegraph.co.uk/news/uknews/law-and-order/11619090/Suspected-illegal-immigrants-found-hiding-in-Maseratis.html>

Notes

Document compiled by Board members of IAATI UK. For further questions or comment the report authors can be contacted at: iaati@iaati.org.uk

MEMBERS ARTICLES

Interpol 2nd Global Crime Conference

By Justin Powell, UK Branch President



This was the 2nd time I had attended this event with Interpol and global stakeholders all tackling vehicle theft and vehicle enabled crime. I do love these events and feel privileged to have attended both now. The news is not good though; when I attended the 1st global conference at Interpol's HQ in Lyon, France in November 2013 we were discussing that Interpol had 7.2 million stolen vehicles recorded on the Stolen Motor Vehicle (SMV) database from 127 supplying countries. When I attended the second conference in February 2016 the figure is now in excess of 7.4 million. So despite all our efforts globally we are still seeing an increase. I believe there are a number of reasons for this;

- The closure or downsizing of Stolen Vehicle Units from police forces.
- Austerity or budget cuts in public sector spending both here in the UK and further afield.
- Vehicle crime and departments to deal with vehicle crime are not an area many in law enforcement get the opportunity to go into these days let alone specialise in.
- We are losing the 'knowledge' to tackle vehicle crime and vehicle 'enabled' crime.
- Attack methods have seriously evolved with electronics, the level of anonymity the internet provides to criminals and the 'connected car' manufacturers are always pushing towards.
- Criminals are more organised, tech savvy and aware country borders cause issues for all in chasing down.



Group photo of participants who attended the Interpol Conference in Bangkok in February 2016

Continued over the page

MEMBERS ARTICLES

Interpol 2nd Global Crime Conference (continued)

Much of the above may appear stating the obvious but it is worth highlighting in such a fashion because it clearly highlights the 'good guys' are getting a tougher time and the criminals are exploiting this fact massively and have better tools, better communication and with the money that current vehicles fetch makes it a highly lucrative business with lesser chance of detection than ever before.

The through-line at the conference for me was the sale of stolen or illicit parts. There were presentations from many countries and this MO (Modus Operandi) featured in all. Some stand-out presentations were given by Maximillian Weidmann of Bavarian State police, Peter De Santos from Victoria police, Australia and Torbjörn Serrander from Larmjanst in Sweden. All highlighted cases worked on, all highlighted the problematic nature of trying to piece back together the vehicles themselves on the discovery of such operations.

The other reflective thing for me was how we need to encourage 'A Partnership Approach' to tackling vehicle criminality as much as possible and I envisage Interpol and IAATI being two routes to encourage this logic as much as possible in the years ahead. Interpol need to be involved to pull together the law enforcement side but equally IAATI need to play a large part by pulling together private industry, solution makers, insurance and lender industries and providing training and awareness of the problems faced.

The IAATI community worldwide continues to amaze me in how far and wide our organisation reaches. This was apparent and we had a real show of force at the conference. In the days ahead we need to encourage the networking part of our organisation more and more.

The fact we are in excess of 3,500 members worldwide should not be overlooked and seeing as vehicle crime is becoming more 'migratory' we need this global network to build ever closer working relationships to counter the threats faced. The knowledge gained at the conference, many of which was presented by IAATI members was also testament to how perfectly placed we are in order to aid organisations such as Interpol and others country specific agencies with vehicle theft and other vehicle 'enabled' crimes.

An IAATI colleague said it best many years ago now and is probably one of the main



International President, Todd Blair, Latin American Branch Secretary, Ana Laura Brizuela and Latin American Branch President, Daniel Beck.



International President, Todd Blair, and International Past President Chris McDonold.

MEMBERS ARTICLES

Interpol 2nd Global Crime Conference (continued)

reasons I joined IAATI.

'You can bet that 99% of people driving around in vehicles will just be your average Joes going about their daily lives. You could also bet that 99% of criminals will use vehicles as the 'enabler' to facilitate so many other crimes. Follow the vehicles we may have a chance to uncover and disrupt so much more'.

It has never left me this quote and still holds true; maybe even more today.

The event overall was a great success and had in excess of 150 delegates in attendance from 47 countries represented. I would suspect the 3rd Global Crime conference pencilled in for November 2017 will exceed this number still and another educated guess would be we will see further rises in vehicle crime still between now and then globally.

IAATI is perfectly placed to help aid law enforcement worldwide tackle this area of crime and my belief is we will continue to do so through the global network that is truly unique.



Chris McDonold (International Past President), Todd Blair (International President), Daniel Beck (Latin American Branch President) and Hans Kooijman (1st International Vice-President).

Photographs supplied by Justin Powell and Ana Laura Brizuela

IN THE NEWS

Tests uncover major security risk to keyless cars

By Martin Saarinen, *AutoExpress.co.uk*, 18 Mar, 2016

New tests by German vehicle experts show 24 cars from 19 different manufacturers vulnerable to an 'easily built' electronic device.

Owners of cars with keyless technology are being warned to stay more vigilant after German vehicle experts showed thieves could bypass the central locking and start the engine of 24 different cars and vans with an 'easily built' electronic device.

The German automotive organisation ADAC - the German equivalent to organisations like the AA - tested 24 different vehicles with keyless technology from 19 different manufacturers like Audi and SsangYong, and found every single one could be broken into using a simple homemade electronic device.

Keyless technology allows drivers to enter and start their vehicle without using the key - the car using sensors to communicate with the key in proximity and authorise start-up. A feature commonly found in premium makes like BMW and Audi, it's slowly trickling down to more mainstream brands, and even vans like the Renault Trafic now feature the technology.

One way the thieves operate is by following the owner and using an electronic device to extend the range of the owner's key. A second thief then waits by the car and uses the signal to access the vehicle and start it.

Auto Express previously reported on how criminal gangs in London are taking advantage of the technology. In 2014, thieves managed to steal up to 17 cars a day in London, netting over 6,000 cars over the course of the year. A study last year also found electronic immobilisers used by 26 manufacturers are vulnerable to hacking, putting over 100 models at risk.

Although carmakers are coming up with new countermeasures to tackle thieves, ADAC says, "Owners of cars with keyless locking systems should exercise increased vigilance in the storage of the key."

The organisation added: "It's the duty of all car manufacturers to get rid of this problem. It makes no sense that this more expensive locking system is way easier to break into than the normal one."

Source: <http://www.autoexpress.co.uk/car-news/consumer-news/94918/tests-uncover-major-security-risk-to-keyless-cars>

Which keyless cars failed the ADAC security test?

The below table shows the test results from ADAC's findings in Germany:

Make	Model	Model Year	Able to illegally open doors	Able to illegally start engine
Audi	A3	2015	Yes	Yes
	A4	2015	Yes	Yes
	A6	2015	Yes	Yes
BMW	730d	2015	Yes	Yes
Citroen	DS4 Crossback	2014	Yes	Yes
Ford	Galaxy	2015	Yes	Yes
	Eco-Sport	2015	Yes	Yes
Honda	HR-V	2015	Yes	Yes
Hyundai	Santa Fe	2015	Yes	Yes
Kia	Optima	2015	Yes	Yes
Lexus	RX 450h	2015	Yes	Yes
Range Rover	Evoque	2015	Yes	Yes
Renault	Trafic	2015	Yes	Yes
Mazda	CX-5	2015	Yes	Yes
Mini	Clubman	2015	Yes	Yes
	Outlander	2013	Yes	Yes
Mitsubishi	Qashqai+2	2013	Yes	Yes
	Leaf	2012	Yes	Yes
Nissan	Leaf	2012	Yes	Yes
Vauxhall	Ampera	2012	Yes	Yes
SSangYong	Tivoli XDi	2015	Yes	Yes
Subaru	Levorg	2015	Yes	Yes
Toyota	RAV4	2015	Yes	Yes
	Golf GTD	2013	Yes	Yes
VW	Touran 5T	2015	Yes	Yes

IN THE NEWS



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



This PSA is a joint product by the Federal Bureau of Investigation, the Department of Transportation and the National Highway Traffic Safety Administration.

March 17, 2016 - Alert Number: I-031716-PSA
<http://www.ic3.gov/media/2016/160317.aspx>

Motor Vehicles Increasingly Vulnerable to Remote Exploits

As previously reported by the media in and after July 2015, security researchers evaluating automotive cybersecurity were able to demonstrate remote exploits of motor vehicles. The analysis demonstrated the researchers could gain significant control over vehicle functions remotely by exploiting wireless communications vulnerabilities. While the identified vulnerabilities have been addressed, it is important that consumers and manufacturers are aware of the possible threats and how an attacker may seek to remotely exploit vulnerabilities in the future. Third party aftermarket devices with Internet or cellular access plugged into diagnostics ports could also introduce wireless vulnerabilities.

Modern motor vehicles often include new connected vehicle technologies that aim to provide benefits such as added safety features, improved fuel economy, and greater overall convenience. Aftermarket devices are also providing consumers with new features to monitor the status of their vehicles. However, with this increased connectivity, it is important that consumers and manufacturers maintain awareness of potential cyber security threats.

Vehicle hacking occurs when someone with a computer seeks to gain unauthorized access to vehicle systems for the purposes of retrieving driver data or manipulating vehicle functionality. While not all hacking incidents may result in a risk to safety – such as an attacker taking control of a vehicle – it is important that consumers take appropriate steps to minimize risk. Therefore, the FBI and NHTSA are warning the general public and manufacturers – of vehicles, vehicle components, and aftermarket devices – to maintain awareness of potential issues and cybersecurity threats related to connected vehicle technologies in modern vehicles.

How are computers used in modern motor vehicles?

Motor vehicles contain an increasing number of computers in the form of electronic control units (ECUs). These ECUs control numerous vehicle functions from steering, braking, and acceleration, to the lights and windshield wipers. A wide range of vehicle components also have wireless capability: from keyless entry, ignition control, and tire pressure monitoring, to diagnostic, navigation, and entertainment systems. While manufacturers attempt to limit the interaction between vehicle systems, wireless communications, and diagnostic ports, these new connections to the vehicle architecture provide portals through which adversaries may be able to remotely attack the vehicle controls and systems. Third-party devices connected to the vehicle, for example through the diagnostics port, could also introduce vulnerabilities by providing connectivity where it did not exist previously.

Continued on the next page

IN THE NEWS

Motor Vehicles Increasingly Vulnerable to Remote Exploits (Continued)

What are some of the ways an attacker can access vehicle networks and driver data?

Vulnerabilities may exist within a vehicle's wireless communication functions, within a mobile device – such as a cellular phone or tablet connected to the vehicle via USB, Bluetooth, or Wi-Fi – or within a third-party device connected through a vehicle diagnostic port. In these cases, it may be possible for an attacker to remotely exploit these vulnerabilities and gain access to the vehicle's controller network or to data stored on the vehicle. Although vulnerabilities may not always result in an attacker being able to access all parts of the system, the safety risk to consumers could increase significantly if the access involves the ability to manipulate critical vehicle control systems.

Example: Recently Demonstrated Remote Exploits

Over the past year, researchers identified a number of vulnerabilities in the radio module of a MY2014 passenger vehicle and reported its detailed findings in a whitepaper published in August 2015.^a The vehicle studied was unaltered and purchased directly from a dealer. In this study, which was conducted over a period of several months, researchers developed exploits targeting the active cellular wireless and optionally user-enabled Wi-Fi hotspot communication functions. Attacks on the vehicle that were conducted over Wi-Fi were limited to a distance of less than about 100 feet from the vehicle. However, an attacker making a cellular connection to the vehicle's cellular carrier – from anywhere on the carrier's nationwide network – could communicate with and perform exploits on the vehicle via an Internet Protocol (IP) address.

In the aforementioned case, the radio module contained multiple wireless communication and entertainment functions and was connected to two controller area network (CAN) buses in the vehicle. Following are some of the vehicle function manipulations that researchers were able to accomplish.

- In a target vehicle, at low speeds (5-10 mph):
 - Engine shutdown
 - Disable brakes
 - Steering
- In a target vehicle, at any speed:
 - Door locks
 - Turn signal
 - Tachometer
 - Radio, HVAC, GPS

What did the manufacturer in the recent case do to fix or mitigate the identified vulnerabilities?

In this case, NHTSA believed the vulnerability represented an unreasonable risk to safety based on a number of critical factors: once exploited, the vulnerability allowed access to and manipulation of critical vehicle control systems; the population of vehicles potentially at risk was huge; and the likelihood of exploitation was great given that the researchers were scheduled to publish the bulk of their work product. As a result, almost one and a half million vehicles were recalled (NHTSA Recall Campaign Number: 15V461000). Before the researchers' report was released, the cellular carrier for the affected vehicles blocked access to one specific port (TCP 6667) for the private IP addresses used to communicate with vehicles. However, the recall was still necessary to mitigate other, short-range vulnerabilities.

Continued on the next page

IN THE NEWS

Motor Vehicles Increasingly Vulnerable to Remote Exploits (Continued)

The manufacturer and cell service provider have provided a remedy to mitigate the specific vulnerabilities. The manufacturer announced it would notify owners of vehicles affected by the recall and would mail them a USB drive containing the update and additional security features for the vehicle software. Alternatively, the manufacturer announced that owners could visit a Web site to check if their vehicle was included in the recall and to download the software update to a USB drive. Owners who did not wish to install the update via USB to their own vehicles were given the option to have their vehicle dealer install the update.

Cybersecurity Recalls and Consumer Action

How can consumers determine whether their vehicle has been recalled for a vehicle cybersecurity issue?

When a vehicle is included in a recall, the manufacturer sends a notification to vehicle owners informing them of the issue and how to obtain a free remedy to address the problem.

In general, it is important that consumers maintain awareness of the latest recalls and updates affecting their motor vehicles. This can be done by following the instructions on NHTSA's [safercar.gov](http://www.safercar.gov) Web site, media and news announcements of recalls, contacting your nearest vehicle dealership, or checking the vehicle manufacturer's Web site for recall-related information. Vehicle owners should check the vehicle's VIN for recalls at least twice per year using this Web link: <http://vinrcl.safercar.gov>

Consumers can also look for other related information for their vehicles at the following Web links:

<http://www-odi.nhtsa.dot.gov/owners/SearchSafetyIssues>

<http://www.recalls.gov/nhtsa.html>

How can consumers help minimize vehicle cybersecurity risks?

1. Ensure your vehicle software is up to date

If a manufacturer issues a notification that a software update is available, it is important that the consumer take appropriate steps to verify the authenticity of the notification and take action to ensure that the vehicle system is up to date.

As a note of caution, if manufacturers regularly make software updates for vehicles available online, it is possible that criminals may exploit this delivery method. A criminal could send socially engineered e-mail messages to vehicle owners who are looking to obtain legitimate software updates. Instead, the recipients could be tricked into clicking links to malicious Web sites or opening attachments containing malicious software (malware). The malware could be designed to install on the owner's computer, or be contained in the vehicle software update file, so as to be introduced into the owner's vehicle when the owner attempts to apply the update via USB. Additionally, an attacker could attempt to mail vehicle owners USB drives containing a malicious version of a vehicle's software. To mitigate potential risks, vehicle owners should always:

- Verify any recall notices received by following the steps for determining whether a vehicle has been recalled for a vehicle cyber security issue, as outlined above.
- Check on the vehicle manufacturer's Web site to identify whether any software updates have been issued by the manufacturer.
- Avoid downloading software from third-party Web sites or file-sharing platforms.
- Where necessary, always use a trusted USB or SD card storage device when downloading and installing software to a vehicle.

IN THE NEWS

Motor Vehicles Increasingly Vulnerable to Remote Exploits (Continued)

- Check with the vehicle dealer or manufacturer about performing vehicle software updates.

If uncomfortable with downloading recall software or using recall software mailed to you, call your dealer and make an appointment to have the work done by a trusted source.

2. Be careful when making any modifications to vehicle software

Making unauthorized modifications to vehicle software may not only impact the normal operation of your vehicle, but it may introduce new vulnerabilities that could be exploited by an attacker. Such modifications may also impact the way in which authorized software updates can be installed on the vehicle.

3. Maintain awareness and exercise discretion when connecting third-party devices to your vehicle

All modern vehicles feature a standardized diagnostics port, OBD-II, which provides some level of connectivity to the in-vehicle communication networks. This port is typically accessed by vehicle maintenance technicians, using publicly available diagnostic tools, to assess the status of various vehicle systems, as well as to test emissions performance. More recently, there has been a significant increase in the availability of third-party devices that can be plugged directly into the diagnostic port. These devices, which may be designed independent of the vehicle manufacturer, include insurance dongles and other telematics and vehicle monitoring tools. The security of these devices is important as it can provide an attacker with a means of accessing vehicle systems and driver data remotely.

While in the past accessing automotive systems through this OBD-II port would typically require an attacker to be physically present in the vehicle, it may be possible for an attacker to indirectly connect to the vehicle by exploiting vulnerabilities in these aftermarket devices. Vehicle owners should check with the security and privacy policies of the third-party device manufacturers and service providers, and they should not connect any unknown or un-trusted devices to the OBD-II port.

4. Be aware of who has physical access to your vehicle

In much the same way as you would not leave your personal computer or smartphone unlocked, in an unsecure location, or with someone you don't trust, it is important that you maintain awareness of those who may have access to your vehicle.

What should you do if you suspect you are a victim of vehicle hacking?

In much the same way as you would not leave your personal computer or smartphone unlocked, in an unsecure location, or with someone you don't trust, it is important that you maintain awareness of those who may have access to your vehicle.

1. Check for outstanding vehicle recalls or vehicle software updates

It is important that you check to identify whether there are any outstanding recalls related to your vehicle. This can be done by following the steps outlined above. You may also check on the manufacturer's Web site to determine whether there are any software updates that may need to be applied.

2. Contact the vehicle manufacturer or authorized dealer

An important step is being able to diagnose whether any anomalous vehicle behavior might be attributable to a vehicle

Continued on the next page

IN THE NEWS

Motor Vehicles Increasingly Vulnerable to Remote Exploits (Continued)

hacking attempt. Contact your vehicle manufacturer or authorized dealer and provide them with a description of the problem so that they can work with you to resolve any potential cyber security concerns.

3. Contact the National Highway Traffic Safety Administration

In addition to contacting the manufacturer or authorized dealer, please report suspected hacking attempts and perceived anomalous vehicle behavior that could result in safety concerns to NHTSA by filing a Vehicle Safety Complaint.

- <https://www-odi.nhtsa.dot.gov/VehicleComplaint/>.

4. Contact the FBI

In addition to the above steps, please reach out to your local FBI field office and the Internet Crime Complaint Center (IC3).

- FBI field office contacts can be identified at <https://www.fbi.gov/contact-us/field>.
- You can file a complaint with the IC3 at <http://www.ic3.gov>. Please provide any relevant information in your complaint.

Agency and Industry Action

What is NHTSA doing on vehicle cyber security?

NHTSA is the regulatory agency that sets and enforces the federal motor vehicle safety standards for new vehicles. They are actively working on several initiatives to improve the cyber security posture of vehicles in the United States. More information about their vehicle cyber security activities can be found at:

http://www.nhtsa.gov/staticfiles/administration/pdf/presentations_speeches/2015/NHTSA-VehicleCybersecurity_07212015.pdf

What are automakers doing on vehicle cyber security?

In addition to the steps taken by individual automakers to address vehicle safety and security, the auto industry has established an Information Sharing and Analysis Center (ISAC) to provide a trusted mechanism for exchanging cyber security information. The Auto ISAC will act as a central hub for gathering intelligence to help the industry analyze, share, and track cyber threats. Automakers are also collaborating on best practices for enhancing the cyber resiliency of motor vehicle electronics and associated in-vehicle networks.

a Online research paper; Chris Valasek, Charlie Miller; IOActive Security Services Technical Whitepaper; "Remote Exploitation of an Unaltered Passenger Vehicle"; 10 August 2015; http://www.ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf; 17 September 2015. IOActive is a computer security services company. Authors have researched vehicle vulnerabilities for several years.

Source: <http://www.ic3.gov/media/2016/160317.aspx>

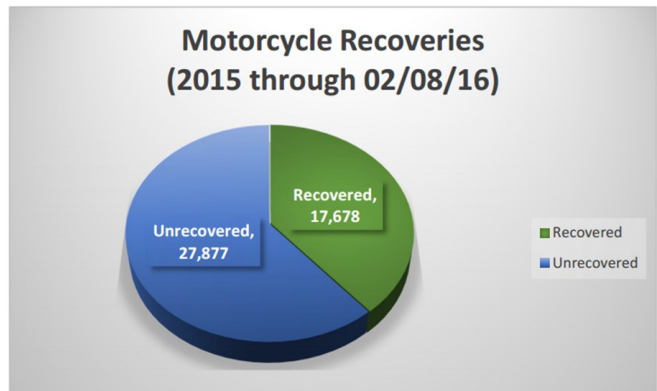
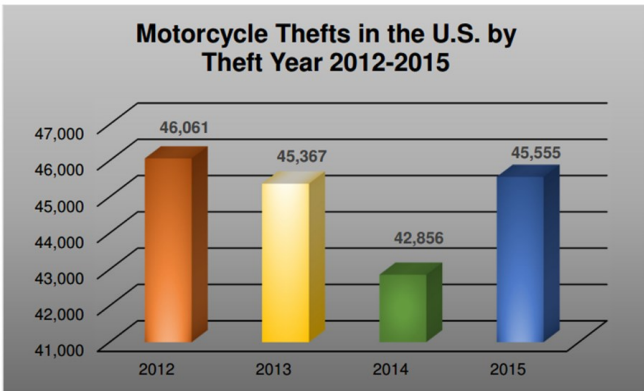
IN THE NEWS

USA: NICB—Motorcycle Thefts Post Increase in 2015

2015 thefts up 6 percent from 2014

DES PLAINES, Ill., April 14, 2016 — The National Insurance Crime Bureau (NICB) today released a report on motorcycle thefts in the United States for 2015. A total of 45,555 motorcycles were reported stolen in 2015 compared with 42,856 reported stolen in 2014—an increase of 6 percent.

Motorcycle thefts have been on a consecutive, nine-year decline going from 66,774 thefts in 2006 to 42,856 in 2014 for a drop of 36 percent. When we include 2015's number, the decline is still a healthy 32 percent for the period.



The top 10 states with the most reported motorcycles thefts in 2015 were California (7,221), Florida (4,758), Texas (3,403), South Carolina (2,160), New York (1,902), North Carolina (1,866), Nevada (1,408), Georgia (1,393) Indiana (1,333), and Virginia (1,253).



Continued on the next page

IN THE NEWS

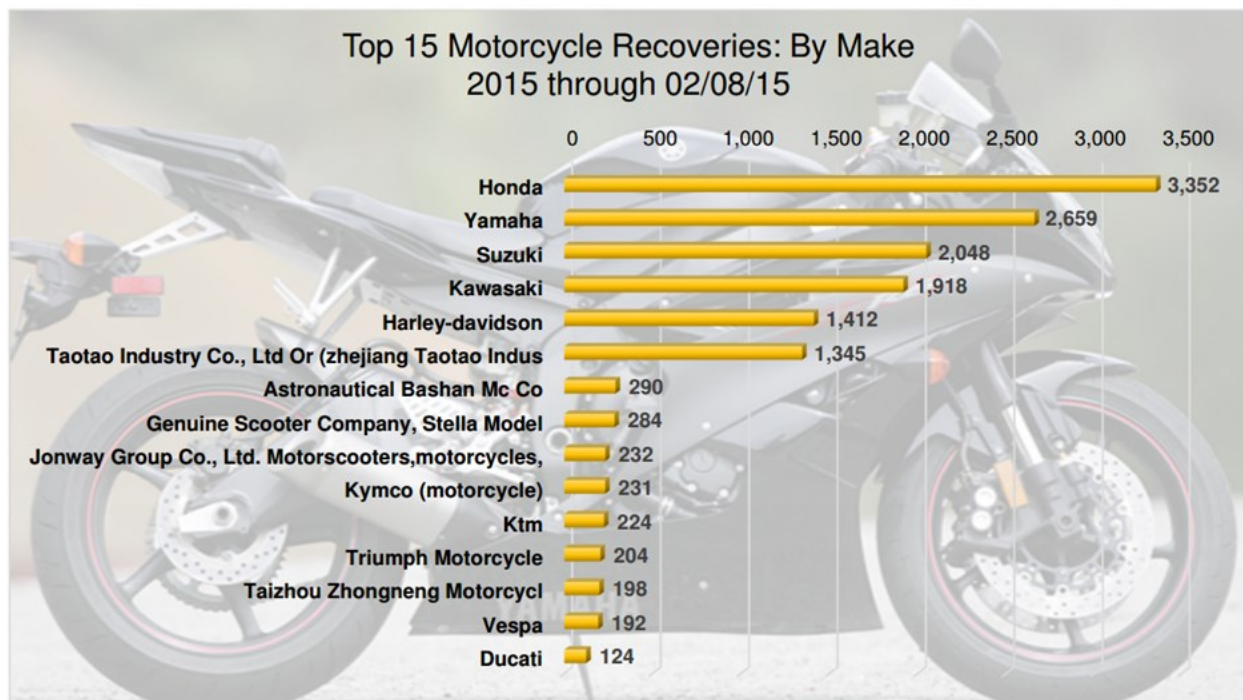
USA: NICB—Motorcycle Thefts Post Increase in 2015 (continued)

The top 10 cities for motorcycle thefts in 2015 were New York (1,340), Las Vegas (1,042), San Francisco (729), San Diego (717), Miami (713), Houston (517), Los Angeles (486) San Antonio (431), Indianapolis (375), and Albuquerque (373).

The top 10 most stolen motorcycles in 2015 by manufacturer were American Honda Motor Co., Inc. (8,674 thefts), Yamaha Motor Corporation (7,214), American Suzuki Motor Corporation (6,065), Kawasaki Motors Corp., U.S.A. (4,920), Harley Davidson, Inc. (4,416), Taotao Group Co. Ltd (2,757), KTM Sportmotorcycle AG (630), Astronautical Bashan (620), Jonway Group Co., Ltd. (520) and Kymco U.S.A., Inc. (512).

The most motorcycle thefts occurred in August (5,269) and the fewest in February (2,093) which continues to reflect a weather-influenced pattern that is consistent with previous years.

The complete report is available [here](#) or by pasting www.nicb.org/File%20Library/Public%20Affairs/2015-Motorcycle-Theft-ForeCAST.PDF into your browser.



Source: <https://www.nicb.org/newsroom/news-releases/motorcycle-thefts-post-increase-in-2015>

IN THE NEWS

USA: Stolen 1982 Ferrari 308 GTSi Found After 28 Years

Robert Moore, TopSpeed, 15 April 2016

Auto theft has always been a serious problem, and today manufacturers are combating it more than ever with disabling devices, laser cut keys, and even biometrics. Of course, California has always hosted a number of metro areas that rank the highest for auto theft. Being on the west coast, it's pretty easy for a professional car thief to jack-move a car, load it on a container ship, and send it across the big blue. Well, not all stolen cars make it to their destination. A prime example is this Ferrari that was stolen 28 years ago and has just now resurfaced as it was about to be shipped out of the Long Beach Seaport.

The car is a 1981 Ferrari GTSi that was stolen from a consignment lot in Orange County, California on July 19th, 1987. The only reason the car caught the attention of customs agents was because the vehicle identification number (VIN) recorded on the export paperwork was used previously on a 1982 Ferrari 208 GTS that was shipped off to Norway back in 2005. The California Highway Patrol, National Insurance Crime Bureau, and a Ferrari factory expert were able to determine what this car really was.

Back in the 1980s, when the car was stolen, the owner was compensated by his insurance company, and now wishes to remain anonymous. The car has probably been parked the entire time it has been missing, as it only has 45,000 miles on the clock. What happens to the car next is a bit of a mystery, and officials have remained quiet about who was shipping the car or who was receiving it.

It is pretty crazy that a car that was stolen 28 years ago was just now being shipped out of the country. It really makes one wonder just what the car has been doing, or where it has been at for the better part of three decades. Who knows, maybe it was Memphis Raines and his crew who stole it way back when. Okay, it's obviously not, but a stolen Ferrari did show up at the Longbeach Seaport, so you can bet it was a team of professional thieves that stole the car.

Considering the previous owner was compensated by insurance, the car will probably go back to the insurance company, or Customs will hold it and eventually auction it off. Either way, it's a \$50,000 car, and somebody will eventually auction it off the legal way. Can you imagine getting a phone call and finding out someone found your Ferrari 28 years after it was stolen? That had to make for an interesting day.

Source: <http://www.topspeed.com/cars/car-news/stolen-1982-ferrari-308-gtsi-found-after-28-years-ar173023.html>



IN THE NEWS

UK: Wave of Land Rover Defender thefts in North Yorkshire and North-East sparks security appeal

Stuart Minting, The Northern Echo, 14 April 2016

Insurers and police have urged owners of a Land Rover Defenders to increase security measures after a 69 per cent rise in thefts of the vehicle in the North-East.

Police believe the vehicles, which have recently risen in value due to production ceasing after 68 years, are being stolen to order and exported out of the country.

NFU Mutual said the North-East had been by far the hardest hit region over the past year, with claims totalling £760,000.

The appeal comes weeks after police forces highlighted how one gang that tried to steal a Defender in Bainbridge, in the Yorkshire Dales, being chased for more than 40 miles before being stopped near Knaresborough and that a long wheelbase Defender had been stolen from Hetton, also in the Dales.

Cleveland Police said its cars had got stuck in mud while trying to follow a stolen Land Rover off-road in Stockton, while Durham Constabulary said a green model was stolen from outside the Piercebridge Organic Farm Shop & Café and a black Defender was taken from Startforth, near Barnard Castle.

PC Garry Dunn said: "I urge owners of Defenders in Teesdale to consider fitting extra security – mechanical devices such as steering and pedal locks, have alarms and immobilisers activated and tracking devices installed."

He added: "Owners of Defenders looking for spare parts should also seriously consider where they buy them from.

"Paying a pittance for commonly stolen parts such as doors and bonnets should set your alarm bells ringing."

Sergeant Nick Hill, of North Yorkshire Police, added: "It appears an organised group of criminals is specifically targeting this make and model of vehicle.

"Of greatest concern to us is that it is evident these thieves have knowledge of this particular vehicle's factory-fitted security and electrical systems."

Clive Harris, agricultural vehicle specialist at NFU Mutual, said Land Rover ending production of the Defender in January had made the vehicle a bigger target for thieves.

A recent auction saw three rare Land Rovers, including one of the last Defenders - a 2016 110 Heritage Edition - fetch nearly £140,000.

He said: "I urge Land Rover Defender owners to be vigilant and be on their guard.

"When not in use Defenders should be parked in a garage or a secure area which is well lit if possible.

"Never leave keys in the ignition and keep keys out of sight at home and when out in public areas; it's essential that easy opportunities are taken away from thieves."

Source: http://m.thenorthernecho.co.uk/news/14417611.Wave_of_Land_Rover_Defender_thefts_in_North_Yorkshire_and_North_East_sparks_security_appeal/



IN THE NEWS

UK: One in 12 cars 'have cloned number plates'

By Paul Hudson, The Telegraph, 30 March 2016

Highly organised vehicle crime gangs are using falsified car registrations to avoid detection by the police

One in 12 of the 37 million vehicles on UK roads could have cloned registration plates, according to new research.

The vast number of cloned plates, in which a car's identity is disguised by the false use of an authorised registration or characters amended to a registration that does not exist, are associated with serious criminal activity.

Dr Ken German, a director of the International Association of Auto Theft Investigators (IAATI), who collated figures from various official sources, said that according to the police there are thousands of cloned plates spotted every day by their automatic number plate recognition (ANPR) and CCTV cameras clearly in an attempt (they suggest) to avoid detection when stealing petrol, parking illegally, speeding or committing more serious offences such as burglary or robbery.

About 1.75 million of the 37 million vehicles of all types in the UK (about 32 million of those being cars) are estimated to be wearing cloned registration plates.

This is made up of 250,000 vehicles of all types - including cars, motorcycles, HGVs, vans, caravans, motor homes, plant and agricultural machinery - reported stolen last year, plus the 500,000 vehicles written off by insurers.

There are also about a million vehicles still unrecovered from the last decade.

The remainder of the one-in-12 total - about 1.25 million vehicles - is made up of legitimate registrations that have been doctored so they read differently.

More than 100,000 sets of number plates are stolen every year but many more will have been altered with paint, a felt tip pen or black tape to deceive ANPR cameras or witnesses to a crime.

Dr German said that the IAATI has identified that thefts of registrations are carried out by highly organised vehicle crime gangs who not only continue to make huge profits from auto crime but who are now almost solely responsible for ensuring less than half of those stolen are ever seen again.

"The police rely heavily on ANPR cameras and don't have the time to investigate. If they spot, say, a bus number plate on a Mercedes saloon they just have to make a note on the computer flagging the anomaly," said Dr German.

How to prevent car theft

"This flag might be triggered if the same registration crops up in connection with a burglary, or worse, but the criminals - or innocent motorists whose car wears a cloned registration - have to be very



ANPR and CCTV cameras detect false plates but overstretched police forces are often unable to act CREDIT: ALAMY

Continued on the next page

IN THE NEWS

UK: One in 12 cars 'have cloned number plates' (continued)

unlucky to be stopped because the police don't have the manpower."

This has left many legitimate owners both angry and bemused when they receive letters from the police suggesting that they in their vehicle have committed an offence to which they have no knowledge.

Dr German said that most innocent purchasers of vehicles with a cloned identity are cash buyers who think they are getting a bargain.

"There are lots of rung [false identity] cars. It's only after the purchase that buyers find out that a car has been cloned, when they contact the DVLA to register the change of keeper," he said.

The tricks of the criminals' trade include forged or stolen V5 vehicle registration documents and different or doctored chassis number identification plates

TOP 10 MOST STOLEN AND RECOVERED CARS IN 2015

1. Range Rover Sport
2. BMW X5
3. Range Rover Vogue
4. Mercedes C-class
5. BMW 3-series
6. Mercedes C63 AMG
7. BMW 5-series
8. Audi RS4
9. Audi Q7
10. Range Rover Autobiography

Source: <http://www.telegraph.co.uk/cars/news/one-in-12-cars-have-cloned-number-plates/>

HOW TO AVOID BUYING A CAR WITH CLONED NUMBER PLATES

The police will seize vehicles, and the innocent buyer has no redress, according to Dr German.

He recommends that buyers thoroughly research a potential purchase, including an identity check with firms such as HPI or Equifax to also find out whether it has finance owing, is stolen, written off or clocked.

He also suggests establishing that a private seller actually lives where he claims, and not paying in cash. "There are some real experts now," he said. "They mainly target cash buyers and use all sorts of reasons, such as leaving the country for a new job and having to sell 'their' car quickly.

"If it looks too good to be true, it probably is."

Buyers can easily check the legitimacy of a car's registration by studying its number plates. The writing on the bottom of the registration plate should bear a dealer or plate manufacturer's name; if it doesn't, the plate is likely to have come from an unregistered source, Dr German said.

Australia: Warning over online scammers targeting car buyers and sellers

By Matt Watson, ABC news, 2 April 2016

Australians are being warned that scammers are stepping up their attacks on people who are selling goods via online classifieds. So far in 2016, 544 people have fallen victim to classified scams and lost a combined \$260,000. In 2014, there were more than 3,200 reports of classified scams that cost Australians almost \$2,000,000.

A spokesperson for the Australian Competition and Consumer Commission (ACCC) said people who used websites to buy and sell goods must be vigilant. The ABC has seen several emails purportedly from genuine buyers and sellers who are using a car retail website. The scammers initially send a text, asking if the car is still available, and ask the seller to contact them only by email.

Once the seller makes contact by email, the scammer sends an email similar to this one:

Thanks for getting back, I'm cool with the price likewise the condition, I work with New Zealand Oil and Gas (NZOG) and we are presently offshore in New Zealand Taranaki Basin.

We do not have access to phone at the moment and that's why I contacted you with internet messaging facility. I will be paying you through PayPal linked up with my Westpac bank account, please get back to me with your Paypal details, I have also contacted my courier who will come for pick up and deliver it to my place in Darwin after the whole fund has been cleared into your acct.

Manager of operations and security at the Carsales.com.au website, Dimitri Kulshitsky, said if the seller agreed and provided payment or banking details, the scammer would then send a fake transaction report. The scam then works one of three ways.

- A courier comes and picks up the car and it is effectively stolen
- The buyer suddenly demands a refund on the fake transaction
- They "accidentally" pay extra on the fake transaction and demand to be reimbursed

"We see those scams periodically," Mr Kulshitsky said. "They will use all those usual stories like the oil rig, some kind of remote location or pretend to be a soldier. It is very fascinating to watch what the bad guys will do to try to get through and look like Australian public"

"Usually they don't have access to the internet or the phone, they can use only email and text message. The idea is usually to take you out of normal channels of communication."

Mr Kulshitsky said another scam involved a car being advertised and the scammer wanting to make a quick sale. They will promise to courier the car as soon as payment has been deposited into an account. But once payment is made, the car is never dispatched.

Staying one step ahead of the bad guys

Mr Kulshitsky said retail websites constantly updated their security systems to ensure customers were protected. "To stay ahead of the game, one step ahead of those bad guys," he said. "If you initiate direct conversation with those guys you're on your own."

He said most of the scammers lived overseas, but they could have partners in Australia who were able to provide Australian phone numbers to prove they were real buyers and sellers.

"It's a cat and mouse kind of game," Mr Kulshitsky said. "It is very fascinating to watch what the bad guys will do to try to get through and look like Australian public. If it is too good to be true then think twice. It's your money so be really careful when you're paying people or how you're paid."

Source: <http://www.abc.net.au/news/2016-04-02/scammers-targeting-car-buyers-and-sellers-online/7293160>

IN THE NEWS

UK: Crazy for Cortinas: The 80s cars targeted by thieves

By Bethan Bell, BBC News, 13 March 2016



They were the cars in every driveway, as symbolic of the 1980s as big hair, yuppies and Duran Duran. But now the once ubiquitous Cortinas, Escorts and Novas are sought after. So much so that they are increasingly being targeted by organised criminals.

It is big business - a couple of vinyl seat covers for a Cortina can sell for £300, while an Escort door can go for £500.

Other than retro-fitting alarms and immobilisers, demand is such that there is little owners can do to protect their vehicles.

Classic car collector and motorway police officer Alan Colman goes as far as to compare the spare parts industry to the drugs trade.

"You need parts for a restoration and get them from an internet auction site," he says. "You pick them up from an 'Aladdin's cave' of rare parts at good prices.

"You think it's downright dodgy and the seller is cagey about the origins of those parts. What do you do? After all, it could be your parts they are selling one day.



Image Copyright: IAATI

IN THE NEWS

UK: Crazy for Cortinas: The 80s cars targeted by thieves (Continued)

"Just like the drugs market, if the supply of buyers dries up then the thefts diminish."

Dave Bailey, a spare parts dealer from Gloucestershire, said he buys cars at auction whole and breaks them himself to sell on, "easily tripling" his profit.

But he admitted there are some people in the trade who turn a blind eye to where their parts come from, and it is that willingness to "sort of wink at jacked goods" which fuels the black market.

Is there a solution to the problem? Mr Bailey thinks not.

"It's second-hand car parts. There's no registry or anything like that. It's up to the buyer - if you think it's dodgy, it probably is. But you don't have to buy it.

"And of course there's a risk to the seller - I've known lads fined or even jailed for selling parts they've got by unconventional means, if you know what I'm saying."

The victims of the black market are people like Martin Isitt. His pride and joy, a red Mk5 Cortina Crusader was taken from the driveway outside his home in Chatham, Kent, on New Year's Eve.

"It's like I lost a part of me," said Mr Isitt, who had spent the past three years working on it.

The car, which had no battery and was missing bumpers and a Ford badge, was reportedly seen on the back of a pick-up truck.

Bob and Tracy Tobin were similarly distraught when their Cortina disappeared from outside their home in Kent. Mr Tobin rescued the car 30 years ago after hearing a friend was planning to send it to a scrapyard. Mrs Tobin said her husband was "absolutely devastated" at the theft.

If going to the effort of arranging a truck to steal a car sounds extreme, it is nothing out of the ordinary, according to Neil Armstrong who runs Stolen Oldskool Fords - a group dedicated to publicising the theft of, and finding, Fords from the 1970s and 80s.

The models only fetched a few hundred pounds as recently as a decade ago but are increasingly popular with thieves.



Image Copyright: IAATI



Martin Isitt's pride and joy, a red Mk5 Cortina Crusader

Continued on the next page

IN THE NEWS

UK: Crazy for Cortinas: The 80s cars targeted by thieves (Continued)

When Mr Armstrong set up the group in 2008, just 15 thefts were reported to him. Last year there were 34. Thieves are going to increasingly extreme lengths to steal the cars.

A Mk1 Ford Escort Mexico was taken from a garage in south London in 2008 after thieves removed tiles from a garage roof, cut the roofing felt, dropped someone inside who removed the steering lock from the car and opened the garage door.

A recent government report found that, although newer cars make up a far higher proportion of stolen vehicles than older cars, vehicles made in the 1980s were still proportionally more likely to be stolen.

"I've heard theories they might be being stolen for banger racing or parts, but I suspect it's all about the resale value," says Dr Ken German, a former police officer and rally driver.

"Enthusiasts and collectors will pay thousands, sometimes tens of thousands of pounds, for a nice example."

One attraction of targeting 1970s and 80s cars is their lack of sophisticated security.

"No cars had alarms or immobilisers back then, unless they were fitted after-market. So they are easy to steal by anyone with a coat-hanger and a screwdriver," says Tom Bell, owner of a Mk2 Golf.

Perhaps most importantly, however, these cars evoke a nostalgia for the earliest "hot hatches", which allowed speed freaks to go from 0 to 60 in 12 seconds without the expense of buying a sports car.

Now, the children of the 1980s have grown up and can recreate their - or their dad's - youth with their own Cortina or early Golf.

The cars are fast and fun to drive, relatively economical and easy for amateur mechanics to tinker with.

But with a roaring black market spare parts trade, the cars of the 1980s are becoming increasingly rare on the streets, and increasingly popular on the car thief's to-do list.

Source: <http://www.bbc.com/news/uk-england-35716456>



This Cortina Lotus was stolen from an enthusiast who had owned it for 27 years



IN THE NEWS

Turkey: Syria jihadists buy 2,000 cars stolen from Turkey

Fevzi Kızılkoyun ANKARA, *Hurriyet Daily News*

About 2,000 vehicles that have been stolen in Turkey have been sent to Syria in the last two years, most of them having been sold to jihadists fighting in the neighboring country.

According to figures from the Police Department and the Gendarmerie Command, the 2,000 vehicles stolen in 2013 and 2014 were smuggled to Syria via using cloned license plates. Most of the vehicles were either pick-up vans or panel vans which have been sold to fighter groups in the region, primarily the Islamic State in Iraq and the Levant (ISIL). Such vehicles have been used by fighter groups for carrying ammunition and fighters.



Reuters Photo

According to figures from the Public Security Department of the Police Department, approximately 63 vehicles are stolen every day in Turkey. Istanbul is the province where the most vehicles are stolen, with 26 vehicles stolen a day. In 2014, 23,000 vehicles were stolen across Turkey.

The newest models of luxury vehicles are also often stolen and smuggled to northern Syria and Iraq, according to data obtained by the police.

Car bomb attacks are frequently conducted in the Middle East, often with stolen vehicles. In February 2013, a bombing at Turkey's Cilvegözü border gate with Syria killed 14 people, with Turkish authorities blaming Damascus for the attack.

Car bomb in town near Syrian border

The deadliest terror attack in Turkey's history took place, which claimed more than 50 lives, in the Reyhanlı district in the southern province of Hatay on the border with Syria in 2013.

At the time, authorities insisted the suspects being tried for the attack are linked to Syrian President Bashar al-Assad, not Islamist rebels, but some leaked documents cast doubt on the government's claims, suggesting al-Qaeda-linked groups committed the attack.

Turkey faced four car bomb attacks in central Istanbul on Nov. 15, 2003, and Nov. 20, 2003, which left 57 people dead and hundreds wounded. Al-Qaeda claimed responsibility for the attacks on the Beth Israel and Neve Shalom synagogues, the HSBC bank headquarters and the British Consulate. British Consul-General Roger Short was among the victims.

There are around 3,000 people linked to ISIL in Turkey, official reports have suggested. The number is in addition to between 700 and 1,000 Turkish fighters in the group, whose potential return has concerned Turkey, Foreign Minister Mevlüt Çavuşoğlu recently said.

Source: <http://www.hurriyetdailynews.com/syria-jihadists-buy-2000-cars-stolen-from-turkey.aspx?pageID=238&nID=77428&NewsCatID=352>

IN THE NEWS

USA: Tustin man charged with defrauding owners out of \$2 million worth of luxury cars

By Scott Schwebke, The Orange County Register, Nov. 11, 2015

The California Attorney General's office has filed 68 felony charges against a Tustin man accused of engaging in identity theft to defraud victims out of luxury vehicles worth more than \$2 million.

Minhchau "Mike" Pham II, 46, is being held in the Los Angeles County Jail in lieu of \$1.7 million bail. He is slated to appear in Los Angeles Superior Court on Monday.

Pham was arrested in Burlingame on Oct. 29 and faces multiple counts of grand theft auto, identity theft, financial fraud and white-collar crime enhancements, California Highway Patrol Investigator Todd Wolf said.

"This is a very sophisticated crime," Wolf said. "Pham is well-spoken, knows cars and the car business.

He was able to con his victims to believe he was a legitimate businessman with a successful dealership that can assist them in finding a third party to assume their vehicle leases or clients who were ready to purchase the vehicle outright."

Pham's attorney, Heena Patel, declined to comment on the charges against him.

Pham is accused of taking more than 20 luxury vehicles, including a BMW, a Bentley, a Mercedes-Benz and a Rolls-Royce.

He may have made at least \$300,000 from victims in Orange, Los Angeles, San Diego, San Bernardino and Kern counties, and Pham may have victimized people in other parts of the nation, Wolf said.

The CHP and Tustin Police Department began investigating Pham in 2013, according to Wolf.

Pham is accused of using aliases and representing fraudulent vehicle dealerships to make contact with victims who advertised their leased vehicles on a website looking for someone to either assume the lease or buy their cars, he said.

Pham also set up a website, majesticmotoring.com, to lure customers, Wolf said.

The website, which was still in operation Wednesday, touts Majestic Motoring as an "award-winning dealership" specializing in the sale of preowned luxury vehicles with a state-of-the-art showroom in Las Vegas.

However, the showroom address is actually for a UPS store in Las Vegas, Wolf said.



2014 BMW M6 that investigators say Minhchau "Mike" Pham II of Tustin obtained through fraud. Photo courtesy of California Highway Patrol

Continued over the page

IN THE NEWS

USA: Tustin man charged with defrauding owners out of \$2 million worth of luxury cars (cont.)

The voicemail message for a telephone number on the Majestic Motoring website identifies the business, but a message seeking comment was not returned.

Wolf said that after many emails and text messages, Pham would gain the victims' trust, and contracts were signed with the promise to have a buyer assume the lease or purchase the vehicle.

"Once Pham was in possession of the vehicles, he would either use the vehicles as his own or rent them out to individuals not known to the victim," he said.

According to a February search warrant filed by Wolf for Pham's residence in Tustin, the subleasing scam operated like this:

Once Pham took possession of a vehicle, he placed a GPS tracking device on the car. Pham then rented the vehicles to third parties for a large down payment plus monthly payments, which he pocketed.

Pham used the GPS system to take vehicles back and start the process over again with another third party.

Monthly payments Pham collected from renting vehicles were supposed to be forwarded to the original owner's finance company, the search warrant says.

Monthly payments to the finance companies would ultimately stop and the vehicles would disappear, said Wolf.

Some vehicles were recovered by the owners, others were abandoned in public parking lots and several were found in private garages, he added.

Authorities interviewed victims and entered information about their cars into the Stolen Vehicle System, a law enforcement database, and all but one of the stolen vehicles has been recovered, Wolf said.

Many of the vehicles sustained damage and required several thousand dollars in repairs, he said.

Pham pleaded guilty in Santa Clara Superior Court in 2012 for subleasing-related crimes. He was sentenced to house arrest along with three years of probation, according to the search warrant. X

Source: <http://www.ocregister.com/articles/pham-691654-vehicles-wolf.html#fancy-1>



2014 Jaguar F Type that investigators say Minhchau "Mike" Pham II of Tustin obtained through fraud.. Photo courtesy of California Highway Patrol

IN THE NEWS

Nissan Leaf cars vulnerable to remote hacking - via unsecured APIs

By Allie Coyne, IT News, February 25, 2016

The world's best-selling electric car, the Nissan Leaf, can be remotely hacked thanks to unsecure application programming interfaces (APIs) supplied by the car maker, two security researchers have found.

Security researchers Troy Hunt and Scott Helme have demonstrated that the unsecured APIs combined with the VIN number of a car - which is easily visible through a car's windshield - could allow attackers to remotely control features like the air conditioning and heated seating.

The vulnerability exists in Nissan's Connect app for iOS and Android, which allows users to control their car.

Attackers could also access the username of the car's owner, which - despite not being "personally identifiable information such as the individual's address" Hunt wrote - wouldn't take "too much effort to fill that gap".

The researchers also said the car's telematics system leaked historic driving data - the time and distance of every trip made - which they said could be used to predict when the driver would be away from home.

"This kind of data should be collected and secured with the utmost respect for my privacy," Helme said.

Hunt demonstrated the flaw by accessing Helme's Nissan Leaf, located in England, from Australia.

Hunt said while attackers could not exploit the vulnerabilities to create a life-threatening situation, they could do things like run down a vehicle's battery.

"If your car is parked on the drive overnight or at work for 10 hours and left running, you could have very little fuel left when you get back to it ...you'd be stranded," Helme wrote.

Nissan Leaf owners who use the Connect app are at risk, the researchers warned.

While it is good that the hack "doesn't impact the driving controls of the vehicle ... the [process] of gaining access to vehicle controls in this fashion doesn't get much easier - it's profoundly trivial," Hunt wrote.

"As car manufacturers rush towards joining on the internet of things craze, security cannot be an afterthought."

Hunt said he notified Nissan first about the issue a month ago as part of responsible disclosure, with several subsequent attempts to discuss the problem, but did not hear back.



Last year researchers revealed the Jeep Cherokee could be remotely controlled by hackers who were able to turn off a car's engine while it was driving.

Fiat Chrysler recalled 1.4 million Cherokees in the US as a result, and later recalled almost 8000 sport utility vehicles to update their radio software in order to prevent hacking.

Source: <http://www.itnews.com.au/news/nissan-leaf-cars-vulnerable-to-remote-hacking-415612>

IN THE NEWS

UK: Police officers uncover large-scale theft of plant machinery

By Simon Mulligan, St Helens Star, 2 March 2016

Police officers have been commended with an international award after helping undercover large-scale theft of plant machinery worth more than £1.5 million.

Merseyside Police was asked to carry out enquiries after the DVLA raised concerns over the authenticity of a vehicle registration certificate for a forklift truck, a JCB Telehandler, in St Helens as it appeared that the vehicle was already registered in Northern Ireland.

Constable Chris Kelleher and vehicle examiner Geoff McKeown were allocated the enquiry and it was found by the Merseyside Police team that the truck in St Helens was an outstanding stolen vehicle.

Further investigation revealed the same firm had bought more plant machinery which turned out to be stolen and that the company who had supplied them had bought them together, with approximately 14 other machines from a London-based organisation.

This led to the Plant and Agriculture National Intelligence Unit (PANIU) taking over the investigation and warrants were executed at the London premises, where a number of organised crime groups were arrested.

Enquires are currently ongoing and it is believed that stolen machinery, worth in excess of £1.5 million, has had its identity altered and subsequently sold by the London company.

Merseyside Police's Vehicle Crime Group were subsequently presented with the 'Peter Leigh Plant Award' by the International Association of Auto Theft Investigators (IAATI) which is presented to an "individual, group, association or company who have shown distinction in the investigation, prevention or detection of plant theft."

Sergeant David Williams from Merseyside Police said: "The IAATI have recognised the diligent and professional manner in which the Vehicle Crime Group has investigated the incident, working closely with our partners to break up a major source of stolen plant equipment."

Source: http://www.sthelensstar.co.uk/news/14312631.Police_officers_uncover_large_scale_theft_of_plant_machinery/

Start planning now for the TAVTI/SCRC Annual conference

The 2016 TAVTI/SCRC (Texas Association of Vehicle Theft Investigators/ South Central Regional Chapter – IAATI) Annual Conference will be held in San Antonio, Texas at the Marriott Northwest Hotel, 3233 NW Loop 410, San Antonio, TX, 78213. The conference will begin on Monday, October 24, 2016, and run through Friday, October 28, 2016. The conference is certified for approximately 24 hours of TCOLE credit. Registration for the seminar is \$200. The Marriott Northwest Hotel room rate is \$115 for a single room or \$120 for a double room. For more information please contact:

Kat Anderson, SCRC treasurer, at 806-787- 5133 / texkat52@yahoo.com, or **Michelle Snyder** at 254-757-0701 / adminattf@burnetcountytexas.org. or visit: <http://tavti-org.secure46.ezhostingserver.com/conference/>

**2016 TAVTI/SCRC
Annual Conference**

24 - 28 October, 2016

Marriott Northwest Hotel,
San Antonio, Texas

IN THE NEWS

Motor Mouth: Ransomware is the future of car theft

Imagine hackers remotely locking you out of your own car and holding it for ransom. It could very well be the next big thing in auto theft

By David Booth, April 22, 2016

Imagine your car has been stolen. It's brand new, you've barely made your third payment and it's your first luxury car, a Mercedes or BMW with all the bells and whistles. You held onto the old Taurus until the fenders almost rusted off, got pre-approved credit at the bank and cross-shopped online so assiduously that you could probably start writing for [Driving.ca](#).

Now it's gone, the thrust of that turbocharged engine – more power and better fuel economy, promised the salesperson – no longer making the daily commute at least a little entertaining. In fact, how are you going to get to work this morning? And, damn, I think the kid left her homework in the back seat. Crap, Bob's coming back from his business trip tonight: How will I pick him up? Now, here's the final insult, the kicker that makes you feel just that much more helpless: Your car is still in the driveway.

It's called ransomware and it could well be the future of car theft. Already the scourge of computer servers, small businesses and now hospitals, security experts, the FBI and even Interpol are predicting that automotive ransom is the next big thing in auto theft.

Here's how it works: "Black hat" hackers — that's the bad kind — install a worm that disables people's most precious files. Then they let them stew helplessly for a couple of hours, so that, when they finally send a malicious little email demanding money in return for control of the hard drive, the ransom demand is almost welcomed.

The average amount extorted, according to experts, is about \$500. But when you consider Forbes magazine estimates that just one "exploit" — Locky, which scrambles and renames all your important files — tries to extort as many as 90,000 victims around the world each and every day, you get an idea of how widespread ransomware already is. Now, throw in the ubiquity of bitcoin — its untraceable nature is blamed for encouraging ransomware exploits around the globe — and then target industries with products notoriously lax in cyber-security. Like, say, cars.

It might be the easiest money a high-tech gangsta will ever make. Think about it — it's the perfect crime. The thief gets the payout of holding something valuable for ransom, yet never has to take possession of it. Why bother with all the fuss of actually stealing a car when "virtual" theft is so much easier and more profitable?

Even the most enterprising car thief is going to have a hard time "liberating" more than two or three Benzes a day, what with the plotting required, waiting around for the "target" to be isolated and, perhaps most time-consuming of all, disposing of two tons of steel and leather.

On the other hand, how many emails can an ambitious cyber-thief pump out? Once a specific operating system has been compromised, it's comparatively simple to repeat the same exploit over and over again. And although there have been no cases of mass automotive ransoms yet, it would appear to be a case of when, not if. Corey Thuen of Digital Bond Labs told Forbes that any American taking advantage of Progressive Insurance's discounts for "safe" driving is vulnerable to getting hacked. According to Thuen, the company's Snapshot "dongle" — a cellular-equipped device that plugs into a car's onboard diagnostic port to relay your driving habits back to Progressive — has "basically no security technologies whatsoever," making more than two million Progressive clients vulnerable to anything from auto theft to "road carnage."

Continued on the next page

IN THE NEWS

Motor Mouth: Ransomware is the future of car theft (continued)

And that's not even the worst-case scenario! What if some particularly diabolical crypto-nerd was to infect all cars of a certain model and then hold the manufacturer for ransom? Andy Rowland, head of Customer Innovation, Energy, Resources and Automotive at BT Technology posited just such a doomsday scenario to idgconnect.com, noting the "infection" could start in any number of seemingly innocent ways: a compromised app that drivers download, "a batch of components with embedded malware" not detected on the production line, or by giving USBs to franchised workshops so that malware "gets onto diagnostic PCs, which then infect all of the vehicles brought in for servicing."

In fact, hacks of the not-so-distant future could prove even more widespread. According to William Largent, a researcher at Talos Security Intelligence and Research Group, "the age of self-propagating ransomware, or 'cryptoworms,' is right around the corner." Completely self-sufficient, once a cryptoworm gains access to a system, it can navigate through a network semi-autonomously, determining how to best invade other subsystems without programmer input.

In other words, skillful hackers, if they could get access to one car's central nervous system, might be able to design malware that infects any car connected to it. Now factor in the fact that the future of automotive safety is supposed to be vehicle-to-vehicle communication (V2V), which requires all cars be connected to one another via Dedicated Short Range Communication — a form of short-range Wi-Fi — and you have the recipe for an automotive apocalypse.

Think such a doomsday scenario is a little too far-fetched? Think again. "Until cars equipped with V2V are available and we can determine the strength of their security systems," says Stephen Cobb, a senior security researcher at ESET, an Internet security company, "we won't know that such exploits can't be done." He goes on to note that "so far, the auto industry doesn't have a good record of building in protection before technology gets compromised; it's always, 'Let's see what happens.'"

Small comfort if you're staring at a \$70,000 Mercedes-Benz "bricked" in your driveway until you fork over the required ransom — with no guarantee it won't happen again next week.

Vehicular cyber-attacks could be terrorism's next frontier

Although most current hacking is still plain, ordinary extortion, the possibilities of cyber-attacks as terrorism is still a clear and present danger. In fact, just last week, John Carlin, U.S. Assistant Attorney General for national security, told the Society of Automotive Engineers' 2016 World Congress that "if you were able to do something that could affect a large scale of an industry – like 100,000 cars – you could see that being in the arsenal of a nation-state's tool kit as a new form of warfare." In other words, the fact that Fiat Chrysler sat on a security flaw in its Jeeps – that Charlie Miller and Chris Valasek famously exposed for Wired magazine – is now a security problem. And when Leonid Bershidsky, a Berlin-based Bloomberg View columnist, says "not worrying about car hacking is like living with a '12345' email password," we're looking at something more serious than just a couple of offshore accounts being exposed or naked selfies being passed around.

Related stories:

[Motor Mouth: Hacking a car is far easier than you might think](#)

[Top 10 ways to avoid getting your car hacked](#)

Source: <http://www.independent.ie/irish-news/news/gardai-seize-14-stolen-vehicles-as-part-of-a-carjack-mob-probe-34540761.htm><http://driving.ca/auto-news/news/ransomware-is-the-future-of-car-theft>

IN THE NEWS

Ireland: Gardai seize 14 stolen vehicles as part of a carjack mob probe

By Cathal McMahon, 15/03/2016

GARDAI have struck a major blow against a criminal gang suspected of stealing vans in the UK and selling them in Ireland.

Searches led by officers from Granard, Co Longford on Monday uncovered 13 Ford Transit vans and one caravan.

Independent.ie has learned that the seizures in Longford, Cavan and South Dublin were targeting a traveller gang and their associates under Operation Butler.

The criminal outfit are believed to be behind a sophisticated scam where badly damaged vehicles are bought for scrap in the UK. A senior source explained that members of the gang then steal a similar car or van and clone the number plates of the damaged vehicle onto it before importing them into Ireland with the bogus documentation.

Officers suspect that the gang is also 'clocking' the mileage on vehicles in a bid to get a better price from customers.

A senior source explained: "This is a local criminal gang based around a family and their associates. They have been running this multi-million euro operation for some time and it is for this reason that authorities moved."

Gardai from the Granard and Longford districts were joined on Monday afternoon by officers from Department of Social Welfare and officers from Revenue Custom and Excise at six simultaneous raids on Monday afternoon.

Members of the Gardai Stolen Motor Vehicle Investigation Unit (SMVIU) are also involved in Operation Butler.

In total 60 officers took part in the simultaneous searches at six different premises. Three commercial premises, believed to be garages and car dealerships, were searched in Granard and Longford.

A considerable amount of documents, laptops, mobile phones and other supporting information was seized as part of Operation Butler. A number of engines were also taken for examination.

A garda spokeswoman explained that during the course of the searches a total of 14 suspected stolen vehicles were seized, they consisted of 12 Ford transit vans, one Ford camper van and one caravan.

The vehicles include Ford Transit flatbed vans and minibuses. The vans range in age from 2010 to 2014.

The mileage had been altered on a number of the vehicles in order to drive up the price.

No arrests were made during Monday's raids but further operations targeting the gang are expected in the coming months.

This is the second raid targeting the gang. Earlier this year gardai seized six vehicles from the owners.

The vehicles are being advertised on DoneDeal.ie, carzone.ie and other websites. And even while gardai were searching a premises in Granard on Monday prospective customers were asking about the vehicles.

A senior source explained: "I don't know whether it is greed or naivety but people were coming in and asking to buy vehicles they had seen online while gardai were swarming around the place on Monday."

Last week it was revealed that 6,128 vehicles were stolen in 2015. A total of 3,838 (63pc) were recovered.

Source: <http://www.independent.ie/irish-news/news/gardai-seize-14-stolen-vehicles-as-part-of-a-carjack-mob-probe-34540761.html>

IN THE NEWS

South America: Organized crime networks targeted in INTERPOL-coordinated operation in Tri-Border area

Interpol, 15 April 2016



"Guns, drugs and stolen cars were seized during an INTERPOL-coordinated operation targeting organized crime networks in the tri-border area between Argentina, Brazil and Paraguay, which also saw the arrest of a fugitive wanted for murder.

Throughout the operation, the first of its kind involving all three countries, more than 300 officers were deployed to key locations at and around the border control points. Frontline officers carried out some 25,000 checks against INTERPOL's global databases during the eight-day (1 – 8 April) operation, which resulted in 25 arrests, the seizure of 750 kg of drugs including marijuana and cocaine, and the recovery of 14 stolen vehicles.

Key locations were the Tancredo Neves International bridge between the Argentine city of Puerto Iguazú and Foz do Iguazú in Brazil, and the Amistad International Bridge which joins Foz to Ciudad del Este in Paraguay and is crossed by more than 15,000 vehicles and 40,000 people every day.

Experts in drug trafficking, document security, counterfeit medicines, trafficking in human beings and stolen vehicles from the INTERPOL General Secretariat headquarters in Lyon and the INTERPOL Regional Bureau for South America in Buenos Aires were also deployed to provide on-site support. An Italian man wanted in connection with a murder in Argentina in 2015 and who was the subject of an INTERPOL Red Notice was identified and arrested as he attempted to cross into Paraguay from Brazil. Some 400 kg of marijuana were discovered in a single car after the driver abandoned the vehicle at a police checkpoint and fled on foot.

A car recorded in INTERPOL's Stolen Motor Vehicles database as stolen from Spain in June 2013 was recovered by federal police in Brazil. Further investigation revealed it was among nearly 100 cars smuggled into Paraguay and enquiries into the network involved are continuing. Three men were arrested for firearms trafficking after eight automatic weapons were discovered hidden their car as they travelled into Brazil. "Although we have been exchanging information on organized crime networks in the triple frontier area, this operation was the first time we coordinated our efforts on the ground," said Argentine Federal Police Comisario Inspector Fabian Zabala. "INTERPOL's support and coordination played an integral part in the operation's success."

"These results are as a result of the dedicated work of the officers on the ground and the excellent coordination and cooperation between the involved law enforcement agencies," said Brazilian Federal Police Commissioner Fabiano Bordignon.

"The access to INTERPOL's databases played an important role in the success of the operation and again has shown the need for international information exchange. Operations like this show what can be achieved when law enforcement agencies collaborate in the fight against organized crime," said the Head of INTERPOL Brasilia, Commissioner Valdecy Urquiza Junior.

"This operation has resulted in a valuable exchange of experience and knowledge and will provide a strong platform for even closer cooperation to target organized crime networks in the future," said Luis Arias Navarro, Head of INTERPOL Asuncion.

"Operations such as this are not just about arrests and seizures, they are also about the added value that INTERPOL brings to its member countries to strengthen national and regional law enforcement cooperation," said Tim Morris, INTERPOL's Executive Director for Police Services. "When frontline officers have access to INTERPOL's global network and databases, they can join the dots between investigations around the world which would otherwise go unnoticed, and we will continue to work with our member countries to encourage this model worldwide," added Mr Morris.

In addition to the INTERPOL National Central Bureaus (NCBs) in Asuncion, Brasilia and Buenos Aires, the operation was supported by the Federal Police, National Gendarmerie, Airport Police and Navy Prefecture in Argentina, the Federal Police, Highway Police and Federal Revenue Service in Brazil, and the Paraguay National Police.

Source: <http://www.interpol.int/News-and-media/News/2016/N2016-047>

IN THE NEWS

Auto industry turns to 'bug bounties' to find security holes

By Chad Halcom, Crain's Detroit Business, March 21, 2016

"Bug bounty" reward programs, for hackers to responsibly identify and help correct automotive software weaknesses, may be on their way for the top automakers, much as they have been adopted already in other industries.

General Motors has had an internal "Collaborative Disclosures" program running since January to interact with software researchers, or "white hat" hackers, and could soon expand the program to offer financial rewards or incentives for finding vulnerabilities before they create problems.

Tesla Motors Inc., the California-based electric car maker headed by CEO Elon Musk, has sponsored a bug bounty program since last June offering rewards of \$100 to \$10,000 per error or software flaw. That program has issued 106 awards as of March, according to Tesla's website.

Ford Motor Co. and Fiat Chrysler Automobiles have yet to announce any internal collaboration with hackers, but both companies are part of a new automotive Information Sharing and Analysis Center, or a collaborative industry program to share intelligence on software attacks and bolster cybersecurity, also launched in January.

Ford spokesman Alan Hall said the automaker "routinely monitors the security environment" and is reviewing possible strategies like a software bug disclosure program in the future, to mitigate threats. FCA spokesman Michael Palese said the automaker would not discuss its future plans for software disclosures.

But industry experts told Crain's Detroit Business, an affiliate of Automotive News, that other automakers are likely to follow GM and Tesla, with new cybersecurity initiatives of their own.

Automotive security executives and others are expected to attend the third annual Automotive Cyber Security Summit this week at the Baronette Renaissance Detroit-Novati Hotel, hosted by New York-based Penton Learning Systems LLC or International Quality & Productivity Center.

GM program

Jeff Massimilla, chief product cybersecurity officer at GM who sits on the board of directors at the new ISAC, said earlier this month that the internal GM program has been primarily vetting and talking with researchers for sharing findings on auto vulnerabilities, since it launched at the start of the year.

A rewards program is likely to follow, but he declined to estimate when that might be.

"I don't think it is ready for that yet, because right now we're in a "crawl" program phase. That would be more of a "run" phase -- to have a bug bounty, or be sponsoring a participatory and reward program for researchers," he said.

But Scott McCormick, president of the Connected Vehicle Trade Association, said he expects bug bounties and open collaboration with white hat hackers to become a standard industry practice.

Saving millions

If FCA had already had a bug bounty or collaborative program up in place when researchers hacked a Jeep Cherokee using Uconnect software in its entertainment system last summer, it likely could have saved millions in software fixes, he said.

Tesla's program was pretty restrictive on researchers, and GM will probably work in a similar way, McCormick said.

"There are often ground rules like the research can't harm GM or its customers, you can't risk the safety of others, and researchers have to keep private the details of their findings until an automaker has a period of time to review and confirm it. I'm expecting the other companies will model that," he added.

IN THE NEWS

Auto industry turns to 'bug bounties' to find security holes (continued)

Barbara Ciaramitaro, professor of information technology and cybersecurity and director of the newly-formed Decision Science program at Walsh College, said administrators at the school have been meeting with Ford and other local automakers in recent months about possible ways to collaborate on training new professionals in cybersecurity. But those talks are still preliminary.

The college added a new cybersecurity concentration within its master of science in information technology degree program, also in January.

"The automotive engineer community has to interact with the hacker and software engineer community to understand the whole mindset that goes into cyber attacks, and building your program to withstand attacks. There are cultural differences between" the software and auto industries, she said.

"It's a learning process for everyone, and even though there's progress this is still going to take a couple more years."

Talent competition

Even when automakers do understand the world of hackers and cyber threats, they are often competing for the top software talent with Silicon Valley firms and other industries, so collaborating with specialists outside the industry might be more convenient than building and training a workforce to tackle the challenges of cybersecurity, she said.

The new ISAC for auto cyber defense is one of about two dozen such centers nationwide, some industry-specific and others that cross industries but focus on specific infrastructure or threats that various businesses have in common, as part of the National Council of ISACs.

President Barack Obama three years ago signed new executive orders to direct the U.S. Department of Homeland Security to encourage and cooperate with ISACs to address cyber threats affecting critical infrastructure.

Experts expect automotive cyber defense is going to be a priority focus for at least the next year or two. Ciaramitaro and McCormick both said connected vehicles can have as much as 100 million lines of code across their various systems -- more than some airplanes -- and if even one in 4,000 lines contains a code error or vulnerability that could be 25,000 points of potential access.

Legislation and executive orders to facilitate ISACs or information exchange can be vital for automakers and suppliers, who might otherwise run afoul of federal antitrust laws on collusion or conspiracy by sharing too much, said Claudia Rast, an attorney at Detroit law firm Butzel Long. She also said ground rules can be important in working with white hats.

She said: "In a sense, working with one is not too dissimilar from hiring an external consultant or an expert, they would all be an outside party, and there are a couple of entrance legal issues to settle like confidentiality, and the aspect of whether there's an existing agreement in procurement for the service.

Source: <http://www.autonews.com/article/20160321/OEM06/160329987/auto-industry-turns-to-bug-bounties-to-find-security-holes?platform=hootsuite>



Cyber security researchers Charlie Miller, left, and Chris Valasek helped Jeep identify security weaknesses in its software.

IN THE NEWS

USA: - Car theft rate starts to rise

By Matt Schmitz, Cars.com February 16, 2016

Despite declines for property crime overall, car theft was on the rise early last year, according to new national crime figures from the FBI.

The number of stolen car cases rose 1% in the first half of 2015, compared to the same period the year before, the latest FBI Uniform Crime Report says.

That's despite an overall drop in property crimes in all other categories of the database, as calculated from local and regional crime stats submitted to the FBI by thousands of law-enforcement agencies across the nation. Burglary was down nearly 10% and larceny theft by more than 3% versus the same period a year earlier.

While all categories of violent crime also saw a surprising uptick, a surge in car theft wasn't completely unexpected. The crime-stats crunchers at the Des Plaines, Ill.-based National Insurance Crime Bureau previously projected an increase in auto theft of as much as 9% for the first half of 2015. The NICB said anti-theft technologies that had been keeping car thieves at bay in recent years have led criminals to become more clever. For instance, some have figured out how to prey on rental-fleet car fleets or use falsified ownership titles.

Moreover, motor vehicle theft over the past decade has not fallen as dramatically as the rates for other crimes. While property crimes overall during the past 10 years dipped by about 19%, auto theft went down less than 2%.

Still, it is possible that the trend could reverse: The figures from the first six months of last year still are preliminary and subject to change. As of 2014 — the most recent full year of available data — auto theft rates were still sliding across the nation.

Based on each state's number of incidents per 100,000 residents, as calculated by the FBI's annual report for 2014, the states (including the District of Columbia) with: the highest auto-theft rates are:

The highest auto-theft rates per 100,000 residents	The states with the lowest auto-theft rates per 100,000 residents
1. District of Columbia; 3,783 thefts; 574.1	1. Vermont; 244 thefts; 38.9
2. Washington; 30,647 thefts; 434.0	2. Maine; 799 thefts; 60.1
3. California; 151,852 thefts; 391.3	3. New Hampshire; 857 thefts; 64.6
4. Nevada; 10,185 thefts; 358.7	4. New York; 15,736 thefts; 79.7
5. New Mexico; 6,290 thefts; 301.6	5. Virginia; 7,665 thefts; 92.1
6. Hawaii; 3,879 thefts; 273.3	6. Idaho; 1,661 thefts; 101.6
7. Oklahoma; 10,583 thefts; 272.9	7. Pennsylvania; 13,040 thefts; 102.0
8. Missouri; 16,357 thefts; 269.8	8. West Virginia; 1,896 thefts; 102.5
9. South Carolina; 12,902 thefts; 267.0	9. Wyoming; 603 thefts; 103.2
10. Georgia; 26,854 thefts; 266.0	10. South Dakota; 1,007 thefts; 118.0

Source: <http://www.usatoday.com/story/money/cars/2016/02/16/car-theft-rate-starts-rise/80445860/>

IN THE NEWS

Securing connected-car tech will take 1 to 3 years, survey says

By John Irwin, Automotive News, March 1, 2016

Automakers and suppliers believe it will take one to three years to secure connected-car technology, according to a new study.

The survey of manufacturers, parts makers and European drivers by International Data Corp. and commissioned by security company Veracode found that while the auto industry is aware of potential privacy and safety problems and is working to resolve them, it is unclear how quickly the potential problems can be addressed.

Veracode Chief Technology Officer Chris Wysopal said that in the wake of last year's hacking of a Jeep Cherokee by a pair of professional computer hackers, manufacturers and suppliers have a greater understanding than ever of cyberthreats. But survey respondents -- including Fiat Chrysler, Bosch and Delphi -- said on average that it will be one to three years before connected-car technology will be secure.

"They're admitting that everything they built today wasn't built with security in mind," Wysopal said.

The security of connected-car technology likely will become more prevalent, Wysopal said. The study found that half of European drivers are concerned about security and privacy in connected cars, while about two-thirds say they would hold the manufacturer and app developers liable for security.

Wysopal said manufacturers would be wise to keep a car's performance and infotainment systems separate to reduce the risk of "contamination" from the possibility of hackers gaining control of infotainment system software and being able to affect a vehicle's engine, braking or steering systems, compromising driver safety.

"The more you can separate the systems, the more secure it'll be," he said.

He said the best way to do that is to let Apple, Google and others develop the infotainment systems separately and to use their systems. He said that will require more cooperation on security from manufacturers and Apple and Google, who all compete with each other.

Source: <http://www.autonews.com/article/20160301/OEM06/160229867/securing-connected-car-tech-will-take-1-to-3-years-survey-says>



Too good to miss!

The 2016 International Training Seminar in Murfreesboro is likely to be the most valuable five days you can spend enhancing your career.

You will also have a great time and make new friends from around the world. So block out **7-12 August, 2016** in your diary and register now.

Register now at:

https://www.iaati.org/seminar/2016/seminar_app.asp

IN THE NEWS

UK: Motorcycle Theft in London Up a Staggering 44% in 2014

By John Irwin, *Automotive News*, March 1, 2016



Being a motorcycle owner in the London area does not look too pretty after the Metropolitan Police in UK's capital revealed some of the figures for 2014. Motorcycle thefts went up a mind-blowing 44 percent in 2014 compared to what the records for 2012 showed, and this does not bode well.

In numbers, around 2,900 additional motorcycles were stolen in 2014 compared to 2012, and it appears that the phenomenon is on the rise. According to sources in the UK, this growth cannot be attributed to the increase of two-wheelers present on the road. The number of motorcycles has only registered minor fluctuations since the economic crisis in 2008, so the increase in bike thefts is an authentic one.

The Metropolitan Police also says that the number of cars being stolen in the area has decreased, and this triggers the "need" that criminals steal other vehicles. The drop in stolen cars could be attributed to the increasingly sophisticated theft-deterrent technologies that are built into cars nowadays.

Namely, stealing a car became much harder, and this could be one of the reasons thieves turn more onto stealing motorcycles. Obviously, taking off with a stolen bike or hiding it is much easier than concealing a car. A bike can be loaded into a van even if locked and impossible to start, whereas a car would have to be driven or towed, if you fancy action movies more.

Media in the UK also links the theft of motorcycles and committing other crimes, as visordown reports. This means that criminals are stealing motorbikes for the sole purpose of using them as getaway vehicles and not necessarily for dismantling them and selling the parts.

Unfortunately, the London Metropolitan Police does not offer a comparison with previous years regarding crimes committed by suspects riding scooters or motorcycles. So far, they only revealed that 1,240 such crimes were recorded between January 2014 and February 2015. More data is expected from the law enforcement organizations.

As for what motorcycle owners can do to prevent theft, it looks like keeping these bikes in their garages behind locked doors might be the safest bet, albeit not accessible to everyone. Strong chains and padlocks, better alarm systems and GPS tracking beacons are also worth considering. Also, there's Datatag and other anti-theft solutions.

We haven't done the math, but we could not help remembering that "one scooter is stolen every 8 minutes in France."

Source: <http://www.autoevolution.com/news/motorcycle-theft-in-london-up-a-staggering-44-in-2014-105526.html#ixzz4310nNy8V>

IN THE NEWS

Australia: Vic police want to shoot GPS trackers at fleeing cars

By Allie Coyne, IT News, February 9, 2016

Police officers in Victoria have put forward a case for GPS tracking devices to be shot onto cars speeding away from officers in order to reduce the risk involved in high-speed chases.

Officers also asked for remote vehicle disabling technology that would cut off a car's fuel supply and take control of its brakes.

The ideas arose from a survey of almost 3000 officers by the Victorian Police Association, which found 93 percent of the surveyed officers were unhappy with the force's current pursuit policy.

Police wanted their superiors to invest in technology that would allow them to avoid or bring pursuits to a safe end.

A "fleeing vehicle tagging system", as termed in the survey, would allow a "laser guided projectile" to be fired at a fleeing vehicle so police can track its movements via GPS.

Police could then follow and monitor the tagged vehicle at a safe distance and avoid a high-speed chase.

Officers also suggested implementing a remote disabling system that would cut off a car's fuel and control its braking capabilities.

"Remote vehicle disabling technologies" would send signals to a vehicle that would restrict its fuel supply and take control of its braking system to bring it either to a walking pace or complete stop.

Police suggested using the General Electric OnStar system as a starting point for the development of such a capability.

"[We need] investment in new/emerging technologies to assist tracking/stopping stolen vehicle involved in serious offending," the report quoted police officers as saying.

"If we are going to keep the [current pursuit] policy let's be a flagship police force for new methods of stopping/tracking these stolen vehicles who evade ground units."

While the report noted that such suggestions had previously been dismissed by the 2012 Victoria Police Inspectorate Review as "too risky, difficult and costly to operate and execute", it argued that many of the suggested technologies were at the time in their infancy, limited, and expensive.

"Given the pace of technology and the four years that has elapsed since these supplementary options were last considered, the Association supports a reconsideration of these options – a task beyond the scope of this review – and cautions against a summary dismissal of member's ideas," the Police Association argued.

"It is imperative that these options not be superficially dismissed by Victoria Police as being too dangerous, or too expensive as to date no genuine assessment is known to have been conducted using reliable data or rigorous assessment."

The call to change the existing pursuit policy follows the death of two innocent bystanders within three weeks last year after police chose not to chase stolen cars.

Source:

<http://www.itnews.com.au/news/vic-police-want-to-shoot-gps-trackers-at-fleeing-cars-414804>

IN THE NEWS

South Africa: Reasons why some vehicles continue to be stolen

Police inform why certain vehicles remain criminal favourites

rekordeast.co.za , March 24, 2016

Garsfontein police spokesperson Dave Miller said there were two main reasons why certain vehicles remained popular among criminals. Re-usable and durable parts to be stripped and exporting certain brands to neighbouring countries.

"The perpetrators steal some cars to sell off the parts for profit. Some vehicle parts remain in high demand for vehicle thieves because they sell off the parts to bidding buyers," Miller said. "After suspects are arrested in possession of a stolen vehicle, you'll find hijackings or vehicle thefts in those areas often die down."

Miller said this would often be the case because criminals avoided a particular area after an arrest had been made.

Private investigator Mike Bolhuis said he strongly believed a syndicate for certain brand vehicles was controlling theft operations. He said he believed a special 'order syndicate' targeted certain vehicles and provided lucrative rewards for the theft of particular bakkies. "The parts are easily separated and chopped, to make a profit," Bolhuis said.

Miller said police special units were investigating this the probability of syndicates. Bolhuis said engines were taken out of stolen bakkies only to be used in a different bakkie.

"Engine numbers are changed because syndicate is usually professional enough to avoid capture," Bolhuis said.

Miller said bakkies were not the only vehicles targeted. VW, Ford and many older version cars were targeted. He said knowing crime hotspots helped to reduce the chances of becoming a victim of vehicle theft. "Checking that the vehicle is locked after pressing the remote lock button could prevent thefts," Miller said.

Vehicle owner Gawie Wolmarans who found his Hilux bakkie after it had been stolen a month earlier said police found the dashboard ripped apart. "Unfortunately, most of the dashboard of the Hilux was stripped while the thieves were making a getaway," Wolmarans said. "The bonnet was also cut open to gain access to the immobiliser before it was stolen," Wolmarans said.

Miller said police were aware of this method of disengaging vehicle immobilisers. "In a situation such as with Wolmarans, it was safe to assume the vehicle would have been stripped for parts," Miller said.

The stolen Hilux of Wolmarans was found by police after a high-speed chase that ended with the Hilux crashing after skipping a red light.

Source: <http://rekordeast.co.za/86870/reasons-why-some-vehicles-continue-to-be-stolen/>



Dashboard ripped apart Toyota Hilux in theft



Stolen Hilux bonnet sawed open in theft.

IN THE NEWS

Trinidad & Tobago : Thieves target Tiida owners

Jensen La Vende, Trinidad & Tobago Guardian, April 14, 2016

The Nissan Tiida is the number one vehicle targeted by car thieves and the police is urging owners to install anti-theft devices to make it easier to recover.

Speaking at yesterday's weekly media briefing of the Police Service, Sgt Christopher Swamber, of the Stolen Vehicles Squad, disclosed that for the first three months of the year 211 cars have been stolen and only 61 have been recovered. Swamber said the Nissan Tiida, particularly those white and silver grey, were easy to blend in on the roads.

Also at the briefing was public information officer ASP Michael Pierre who said for the year 39 Nissan Tiidas were stolen compared to 48 last year and overall 211 cars were stolen so far this year while 200 were stolen for the same period last year.

Statistics from the Crime and Problem Analysis Branch of the Police Service reveal that for the period January 1 to March 31 there has been a total of 163 cars were stolen as compared to 178 for the corresponding period 2015. The figures also reveal that for the same period 48 motorists were victims of car jacking as opposed to 22 for the corresponding period last year.

Swamber said the police believed the car-stealing ring comprised criminal deportees who have perfected the art of stealing vehicles in under five minutes and locating the global position system (GPS) devices and other car-theft devices and dismantling them. An official of the stolen vehicle recovery provider, CarSearch, said the majority of cars stolen were Nissan models followed by Toyota and Ford brands.

The official, who spoke on the condition of anonymity, said for the past two years the majority of the vehicles stolen were along the East/West Corridor and they have also recovered most of the vehicles in that area. Second to the East/West Corridor is the Port-of-Spain Division for stolen cars, the information provided showed.

Swamber said the Nissan Tiida is considered a "poor man's vehicle" and as such it is targeted for both resale and spare parts. He added that the car-stealing ring in the country was a multi-million dollar business and it was difficult to infiltrate.

The men added that drivers should be careful of where they parked and get anti theft devices and GPS tracking in the event the car was stolen, making it easier for the vehicle to be retrieved.

Swamber said some car parts outlets, referred to as "chop shops", that sell parts of stolen vehicles operated as legitimate businesses and therefore advised car owners to place marking on their vehicles that they alone would be able to identify, making it easier for police to charge the businessmen.

Both Swamber and Pierre advised garage owners as well to be cautious of people bringing vehicles for repairs and suggested that garage owners get proper identification from customers and if they refused, that should be an automatic red light.

Swamber said often the stolen car's chasis numbers are changed and registered as a new vehicle and put back on the roads. He advised car rental agencies to take photographs of customers.

Source: <http://www.guardian.co.tt/news/2016-04-14/thieves-target-tiida-owners>



IN THE NEWS

UK: London gangs using stolen mopeds to carry out murders and drive-by shootings owners

Jamie Bullen, The Evening Standard, 3 April 2016

Theft of mopeds and scooters is on the rise in London because gangs are increasingly using them to carry out serious violent crimes like murder and drive-by shootings, a top detective has said.

The number of mopeds and motorbikes stolen across London rose by 12 per cent last year despite a police operation to crack down on the problem.

Scotland Yard broadened its crackdown on scooter thefts, codenamed Operation Venice, last April as a result of its success in Camden, Islington and Westminster.

Its aim is to combat moped and motorbike theft and more serious crime associated with it, like drive-by shootings, stabbings and robbery.

It comes days after a youth was found guilty of manslaughter of Stefan Appleton, 17, who was stabbed to death with a "zombie killer" knife.

The killer, who cannot be identified due to his age, killed him after using a stolen moped.

However, despite these efforts, more than 11,000 vehicles were stolen in the capital last year – about a 30 a day.



Police are trying to clamp down on scooter gangs but they have been told they can't chase them

Continued over the page.

IN THE NEWS

UK: London gangs using stolen mopeds to carry out murders and drive-by shootings owners (continued)

More than half of the stolen vehicles were not recovered.

The figure is a 12 per cent rise compared to the previous year but the detective leading the investigation insisted "London was safer" because of breakthroughs in tackling organised crime.

Detective superintendent Raffaele D'Orsi, head of Operation Venice, told the Standard: "There is more theft of mopeds or powered two wheelers than there was last year. However we have detected more offenders across the majority of the boroughs than ever before and there is a more organised approach to deal with these offenders.

"Stolen bikes are being used in significant criminality which is why it is a threat to us here in London and that is why we are responding.

"London is safer because of the individuals we have managed to lock up."

He added more people were now likely to report a theft, which contributed to more recorded offences.

Mr D'Orsi said gang leaders were paying youngsters up to £50 a time to move stolen motorbikes across the capital.

Since the operation was launched, more than 600 people have been arrested for vehicle theft but many more have been held for other associated crimes.

He added: "What we find is mopeds are being used in robbery, burglary, smash and grab, drive-by shootings, attempted murders, murders and drug dealing.

"It has been within London for a number of years, whether it's a smash and grab raid or making off from police on a moped. This is serious criminality and often it is organised."

He added officers were risking their lives on a daily basis during high speed pursuits on streets across the capital.

One police officer suffered a broken ankle while another was on the back of a moped when it was driven off by an offender.

Last year, Scotland Yard estimated the value of stolen motorbikes and mopeds to be £28 million but a new estimate by The Motorcycle Industry Association claims the cost is closer to £100 million.

Police said they are working closer with the industry to make it harder for thieves to steal the bikes.

Source: <http://www.standard.co.uk/news/crime/detective-london-gangs-using-stolen-mopeds-to-carry-out-murders-and-driveby-shootings-a3215281.html>

Register now for UK Conference

The delegate cost for attending will be £80 for both days or £45 for the Wednesday only and £40 for the Thursday only. This includes Conference lunches and all day refreshments. Wi-Fi is free and available throughout the venue

For more information: <http://www.iaati.org.uk/conference-2016/>

2016 National Vehicle Crime Conference

8 - 9 June May, 2016

Holywell Park, Loughborough,
Leicestershire, LE11 3GR

IN THE NEWS

Cargo Theft: Not Just a US Problem

Supply chain security issues plague multiple countries around the world.

Bill Turner, LPC, March 24, 2016

Mexico's number of cargo thefts grew 73% in 2015. According to Freight Watch International's supply chain report, 1087 incidents were reported. Northern Mexico's cargo thefts rose significantly, although the central zone states of Puebla, Guanajuato and the State of Mexico remain the highest risks. Food and drink continue to be the most stolen items, accounting for 18% of all cargo theft. Fuel cargo was subject to multiple hijackings in transit. Warehouse robberies were also a common theft method. Mexico reports at least three cargo theft incidents per day, versus two in the U.S., and the Mexican trucking industry is miniscule compared to that of the U.S. August through September continue to be months with the most supply chain security issues in Mexico.



But Mexico is not alone. There has been a sharp increase in thefts from moving trucks in China, according to BSI's 2015 annual report on supply chain security. This type of theft, which has also been seen recently in Europe, is known as "open sunroof thefts" because thieves in these incidents drive cars behind cargo trucks, jump on to the moving vehicles, cut a hole in the top of the soft-sided trailer and toss cargo back to the car behind. BSI reported moving cargo theft incidents in numerous Chinese provinces. Examples included \$55,000 worth of pharmaceuticals and a \$40,000 theft of leather goods. A key issue that prevents effective response to cargo theft in China is confusion over which police force or enforcement agency has jurisdiction. This complicates reporting of cargo theft incidents and allows gangs to operate longer before capture.

Meanwhile, in India, the prevailing trend is toward more sophisticated cargo theft techniques. These include the diversion of shipments to locations where the contents of the truck are removed – generally by cutting panels, leaving the cargo security seals intact. Thieves are increasingly relying on corrupt supply chain employees to facilitate their crimes.

Other trends in supply chain security around the world include a reduction in incidents in some western European countries, including the Netherlands and the UK.

In South Africa, cargo robberies are increasingly violent. Last year, most of their incidents were believed to be perpetrated by current or former police or security officers, often involving sophisticated tactics to carry out high-value cargo thefts, according to BSI. In Latin America, thefts have decreased in some countries—notably Columbia—and markedly increased in others, such as Chile, where an average of three trucks are stolen every day. In Argentina, there has been a shift from targeting full-sized trucks to smaller vehicles such as vans. Incidents in Peru reveal the perils of relying on too much technology to thwart thieves. Thieves recently stole a loaded container of electronics after reportedly using a falsified copy of a supposedly impossible-to-forgo electronic document, thereby allowing them to pick up the container from the port.

In the United States, 86 percent of cargo thefts are still reported from unsecured parking spots at truck stops. But it's only a matter of time before other methods, now threatening supply chain security around the world, become more prevalent here.

Supply chain security: No Loss Prevention pro can afford to overlook it anymore. Start learning with our [FREE Special Report, Trailer and Warehouse Theft: Cargo Theft Security, Investigations, and Prevention Tips from the Experts](#)

Source: http://losspreventionmedia.com/insider/supply-chain-security/cargo-theft-not-just-a-us-problem/?mqsc=E3830389&utm_source=WhatCountsEmail&utm_medium=LPM%20List+LPM%20Insider+LPM%20Insider&utm_campaign=Insider%20Daily%20032416

IN THE NEWS

Suspect accidentally turns himself in by ditching stolen vehicle in police parking lot

Calgary Herald, April 13, 2016



From a video released by the Calgary Police showing an alleged car thief ditching a stolen car in a parking lot that happened to be in front of a Calgary police station. Officers from the district office apprehended the suspect.

Calgary police officers didn't have to go far to chase down the suspect in a vehicle theft Tuesday, after the offender unwittingly abandoned the stolen car in the parking lot of the District 1 office.

According to a post on the Calgary Police Service Facebook site, a Chevrolet Blazer was taken from the 3900 Block of Manchester Road S.E. after the owner left the keys in the ignition of the running vehicle.

Officers on patrol in the area quickly spotted the vehicle, as the suspect drove away at high speed.

A description of the car was broadcast to all District 1 officers — some of whom were busy doing paperwork and preparing to start their shift at the district office.

Moments later, the vehicle showed up on their doorstep, and the suspect didn't make it far before he was nabbed by several sprinting police officers.

"Officers gave chase and the offender was apprehended a short distance from the office without incident," a post on the Calgary Police Service website reads.

A 42-year-old suspect is facing several charges, including motor vehicle theft and dangerous operation of a motor vehicle.

Follow the link to watch the video.

Source: <http://wpmedia.calgaryherald.com/2016/04/police.gif?w=840&h=630&crop=1>

IN THE NEWS

USA: ISIS runs fish farms, car dealerships to compensate for lost oil revenues

Homeland Security News Wire, 29 April 2016

The U.S.-led coalition's air strike have crippled the ISIS oil-smuggling-based economy, forcing the organization to rely on fish farming and car dealing as alternative money generating resources, a new report has revealed. In order to close a yawning gap in the organization's once-lucrative \$2.9 billion oil trading scheme, ISIS has now increasingly turned to other revenue streams.

The U.S.-led coalition's air strike have crippled the ISIS oil-smuggling-based economy, forcing the organization to rely on fish farming and car dealing as alternative money generating resources, a new report has revealed.

CNBC reports that in order to close a yawning gap in the organization's once-lucrative \$2.9 billion oil trading scheme, ISIS has now increasingly turned to operating network of fishing farms in hundreds of lakes north of Baghdad, generating millions of dollars a month. The information is contained in a report by Iraq's central court of investigation. Another source of income is the many car dealerships and factories which once belonged to the Iraqi government, but which have been captured by ISIS.

"After the armed forces took control of several oil fields Daesh was using to finance its operations, the organization devised non-traditional ways of paying its fighters and financing its activities," a report by Iraq's central court of investigation said, according to Reuters.

The latest figures released by market research firm IHS show that ISIS revenue has fallen by around a third since last summer, to about \$55 million a month.

CNBC notes that operating fish farms is not new for extremists in the region. ISIS predecessor, Al-Qaeda in Iraq, operated fish farms since 2007. The Islamists either take over operations at the abandoned farms or coerce the locals to share their profits.

ISIS has also begun to impose a 10 percent tax on agricultural products or any other food stuffs that enters the territory under their control.

"Recently there has been reliance on agricultural lands in areas outside the control of the (Iraqi) security forces through taxes imposed on farmers," the Iraqi court report says..

"Daesh [ISIS] treats its northern Baghdad province as a financial center; it is its primary source of financing in the capital in particular," Judge Jabbar Abid al-Huchaimi said in the report.

Another form of financing for ISIS comes from car dealerships and factories. "In the recent period, Daesh has gone back to using government factories in the areas it controls – like Mosul – for financial returns," Huchaimi said.

Huchaimi notes, though, that oil smuggling from Syrian refineries is still ISIS primary source of financing.

All of the money generated by ISIS various money-making schemes is channeled to Mosul, where the organization's equivalent of a finance ministry is located. The money is then distributed to its fighters and their family members.

"The organization distributes money to areas outside its control through hawala (transfer) offices first in Erbil and from there to Iraq's other provinces," Huchaimi said.

Source: www.homelandsecuritynewswire.com/dr20160429-isis-runs-fish-farms-car-dealerships-to-compensate-for-lost-oil-revenues

TRAINING & TOOLS

Training is one of the most important areas that we as auto theft investigators need to continually seek out. With the trends in auto theft changing on a daily basis, we need to stay on top of these new developments that can assist us with prevention, identification, investigation, and prosecution. If you know of any other auto theft courses that are being offered, please contact Denny Roske at: iaatidenny@aol.com



2016/17 Conferences and Training Seminars

National Insurance Crime Bureau	Continuous	on line training web site, click on: courses	www.NICBTraining.org
North East Regional Chapter	May 9th – 12th	Ottawa, Ontario, Canada	Trevor Archibald archibaldt@ottawapolice.ca
National Odometer & Title Fraud Enforcement Association	May 15th – 19th	Park City, Utah	Holly Mertz Holly.Mertz@iowa.gov
Florida Auto Theft Intelligence Unit	May 19th – 20th	Ocala, Florida	Sheri Taynor staynor@cfl.rr.com
NICB Auto Theft School	May 31st – 2 June	San Antonio, Texas	Steve Amerson samerson@Bexar.org
United Kingdom Branch	June 8th – 9th	Hollywell Park, Loughborough Leicestershire, UK	Ian Platt platt.ian@btinternet.com
64th Annual IAATI International & South East Chapter Seminar	Aug. 7th – 12th	Murfreesboro, Tennessee	Rusty Russell DRussell@nicb.org
Florida Auto Theft Intelligence Unit	Sep 8th – 9th	Ft. Myers, Florida	Sheri Taynor staynor@cfl.rr.com
NICB Auto Theft School	Sept 13th – 15th	Greenville, Texas	Daniel Looney dlooney@huntcounty.net
Miami Dade Auto Theft Symposium	Oct 3rd – 7th	Miami, Florida	Rosa Holtz rholtz@mdpd.com
European Branch Annual Seminar	Oct 5th – 7th	Torremolinos, Spain	Arne Knippel akn@forsikringogpension.dk
South Central Regional Chapter	Oct. 25th – 28th	San Antonio, Texas	Bill Skinner bskinner4309@gmail.com
South African Branch Seminar	Oct. 26th – 28th	Weesgerus Police Resort Modimole, Limpopo	Daan Nel dnel@tracker.co.za
Australasian Branch Annual Training Seminar	March 2017	Brisbane, Australia	Mark Pollard mpollard@iaatiaus.org

TRAINING & TOOLS



International Association of Auto Theft Investigators (UK Branch) (I.A.A.T.I.)
2016 National Vehicle Crime Conference
Holywell Park, Loughborough, Leicestershire, LE11 3GR
8th & 9th, June 2016

National Vehicle Crime Conference	 www.iaati.org.uk
2016	The Current Face Of Vehicle Crime
holywell park	
dedicated conference centre	
Holywell Park Conference Centre Loughborough, LE11 3GR	
8th and 9th June 2016	
Sponsored By: Trade Vehicle Locks Ltd other sponsors TBA	

I.A.A.T.I. partners with trusted organisations who are service providers in products, intelligence, opinion formers and a healthy cross section of key players from the motorcycle, road haulage, leisure, plant, and the insurance and motor industry as a whole. The Conference is being reformatted to include 'training / awareness presentations in the areas highlighted below.

I.A.A.T.I. UK will play host to the National Vehicle Crime Conference at the Holywell Park Conference Centre at Loughborough, on the 8th and 9th June 2016. This is a one day and a half event attracting senior practitioners, opinion formers, law enforcement, intuitive projects, vehicle examiners and a healthy cross section of key players from the plant, agricultural, haulage, leisure, salvage, I.T., insurance and motor manufacturer industries. This event, unlike previous Conferences, will focus on classroom Training (Awareness) sessions covering Electronic, Physical, Marking, insurance fraud and other aspects of vehicle crime.

Along with classroom training / awareness presentations, there will be keynote speakers from leading organisations across the sector. The event attracts up to 150 delegates and is the focus of both industry and media attention. A number of Sponsors will have exhibition stands, each bringing state-of-the-art solutions and best practice to the attention of delegates.

SPONSORSHIP OPPORTUNITIES ARE AVAILABLE IN THE CATEGORIES:-

ELECTRONIC (Including Tracking and electronic intrusion / product substitution)

MARKING (all types)

PHYSICAL (attack / intrusion methods and their deterrence / prevention)

Gold Sponsorship - (3 at £4000 - 2 Remaining – Categories ELECTRONIC including Tracking, and MARKING – The Category of PHYSICAL has been taken by Trade Vehicle Locks Ltd.

Silver Sponsorship - (3 at £2500 - All 3 Categories Remaining).

Bronze Sponsorship - (which includes Exhibitors) - First come first served up to a maximum of 20

TRAINING & TOOLS



International Association of Auto Theft Investigators (UK Branch) (I.A.A.T.I.)
2016 National Vehicle Crime Conference
Holywell Park, Loughborough, Leicestershire, LE11 3GR
8th & 9th, June 2016

INTRODUCING OUR FIRST 2016 CONFERENCE GOLD SPONSOR (CATEGORY PHYSICAL)

Trade Vehicle Locks Ltd [TVL] is the UK's Premier Supplier of designer vehicle security products. Based in Grays, Essex, with 40 years in the industry, TVL also has a nationwide network of fitters and provides world leading vehicle security products and is the UK specialist for commercial vehicle security. TVL boasts a combined experience of more than 40 years designing, building and installing advanced locking systems for vans and goods vehicles.

Trade Vehicle Locks pride itself on supplying the largest and most bespoke range of commercial vehicle security products available, giving our customers the choice of products to satisfy their customers needs. Most products available on the market today have originated from TVL in one shape or form. Our R&D department is the most proactive of any supplier in our industry, allowing our product portfolio to constantly expand. We are able to design, build and quickly bring to market countermeasures for the latest vehicle specific criminal methods employed by thieves.

TVL believes knowledge is key and as such we offer Installation and Product training courses where we will be showing first hand the benefits of each products and application, giving you the confidence to properly advise your customers on the best products and applications to suit their needs. Technical support is offered by experienced installers and engineers. You can have peace of mind that the person answering the phone knows what they are talking about and will provide you with the very best advice to assist you if required.

The Delegate cost for attending will be £80 for both days or £45 for the Wednesday only and £40 for the Thursday only. This includes Conference lunches and all day refreshments. Wi-Fi is free and available throughout the venue

- Delegate registration is available online at: <http://www.iaati.org.uk/conference-2016/>
- Directions can be found on :- <http://www.holywell-park.co.uk/imago/directions>
- For SatNav, type in LE11 3GR
- Details of Holywell Park can be seen on: www.holywell-park.co.uk
- The Hotel is the on-site 4* Burleigh Court Hotel.
- For Sponsorship Opportunities contact the Organiser

The Event Organiser is : Ian Platt (IAATI) – 07899 967322 / platt.ian@btinternet.com

TRAINING & TOOLS



The International Association of
Auto Theft Investigators



2016 IAATI EB SEMINAR TORREMOLINOS - SPAIN

Hotel: SOL PRINCIPE - Paseo Colorado 26 - 29620 TORREMOLINOS (Malaga)



Seat & Treasurer's office European Branch – Bergstraat 50 – B-9820 Merelbeke –
website www.eb.iaati.org

TRAINING & TOOLS

The region lends itself to extended stay for visits to Malaga, Cordoba, Ronda and Granada.

MALAGA:



RONDA



GRANADA



As the hotel lies straight to the beach it also invites to enjoy the sun (normal from 25 to 30° C begin October)

TRAVEL INFORMATION:

Nearby Airport: MALAGA (Malaga - Torremolinos = 8 km)

From Airport to hotel best take a taxi (costs: 12 to 15 €)

or

Rental car: several traditional rental companies rent you a car for good prices. For the moment it seems that Malagacar.com gives good price and conditions (full insurance) with very quick shuttle-service at airport (3min)(own experience). Also other companies give similar conditions.



Registration form

IAATI - EB TRAINING SEMINAR

October 05 - 07, 2016

TORREMOLINOS - PLAYAMAR - SPAIN

PLEASE FILL IN WITH COMPUTER - FOR EACH SEMINAR VISITOR 1 FORM

WE DO NOT ACCEPT REGISTRATIONS LATER THAN ON 21th SEPTEMBER

Step 1: Your personal information

Name :

Address :

City :

Country :

E-mail address :

Phone number :

IAATI membership number:

Profession :

Law enforcement : yes / no

T-shirt size : S M L XL XXL (please circle).

Companion (non attendee of the seminar)

Name :

Address :

Place :

Country :

Phone number :

EXTRA INFORMATION FOR THE ORGANISERS?

.....

.....

TRAINING & TOOLS

PRIVACY

Do you want your name and information to be mentioned on the participants list which will be spread during the seminar?

Yes

No

(When not filled in = yes)

Step 2: Your hotel and seminar fees

ROOMS ARE TO BE RESERVED VIA IAATI EB SECRETARIAT. WE BOOK ONLY ON BASE OF ROOM+BREAKFAST.

a. Standard room - single use 85€ / night
Check-in date:..... Check-out date..... Total nights:.....

b. Standard room - double use 95€ / night
Check-in date:..... Check-out date..... Total nights:.....

c. Standard room - triple use 135,40 € / night
Check-in date:..... Check-out date..... Total nights:.....

d. Junior suite *** Pool view 1pax 105€ / night
Check-in date:..... Check-out date..... Total nights:.....

e. Junior suite *** Pool view 2pax 115€ / night
Check-in date:..... Check-out date..... Total nights:.....

f. Junior suite *** Pool view 3pax 155,40€ / night
Check-in date:..... Check-out date..... Total nights:.....

g. Junior suite *** Pool view 4pax 195€ / night
Check-in date:..... Check-out date..... Total nights:.....

NET RATES PER ROOM PER NIGHT. VAT 10% INCLUDED
BASIS: B&B: Bed & Breakfast (buffet style)
WI-FI CODE: Included

REDUCTIONS POLICY

1 Child 0-2 years (baby cot) -100% (GRATIS)
1 Child 3-11 years sharing twin room or Junior suite Pool View -50% over
95€/2=47.50€

To pay:x.....=.....€ (Quantity X price)

TRAINING & TOOLS

CANCELLATION POLICY:

Until **31 August, 2016** without costs.

Note: In case of a “no-show” or any other cancellations after Aug 31, 2016, IAATI has to charge you for the total amount of your registration !

Step 4: Send us your reservation form!

We do not accept registrations without a completed registration form !!!!

Return the registration form to:

Franky Dedeurwaerder

E-mail : franky.dedeurwaerder@telenet.be

And CC to : davy.borysiewicz@baloise.be
: ukraned3@live.nl