CyberROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

Grant Agreement N. **607642**

D 4.4 Profiles of Cyber-Criminals and Cyber-Attackers

Date of deliverable: 01/12/2015
Actual submission date: 01/12/2015

Start date of the Project: 1st June 2014. Duration: 24 months
Coordinator: UNICA – University of Cagliari, PRA Lab - Pattern Recognition and Applications Lab
Version: 1.0

Project funded by the European Commission Directorate-General Home Affairs in the Prevention of and Fight against Crime Programme		
Restriction Level		
PU	Public	✓
PP	Restricted to other programme participants (including the Commission services)	no
RE	Restricted to a group specified by the consortium (including the Commission services)	no
CO	Confidential, only for members of the consortium (including the Commission)	no

Revision history

Version	Object	Date	Author(s)
0.1	Initial draft Table of Contents.	01/07/2015	INDRA
0.2	Structure Changes.	01/08/2015	INDRA
0.3	Multiple changes in the structure. Content added to section 1 and 2.	03/08/2015	INDRA
0.4	Review of attributes for characterization.	07/08/2015	INDRA
0.5	Attacks to Postal and Logistic Services.	28/08/2015	INDRA
0.6	Attacks to Social Networks, Unmanned Systems, Mobile Biometry, ICS, Automotive, IoT, Transport Critical Infrastructure, Virtualization, Cloud Computing.	01/09/2015	INDRA
0.7	Attacks to Smart Grids.	11/09/2015	INDRA
0.8	Attacks to BYOD, Smart Cities.	07/10/2015	INDRA
0.9	Drafting Conclusions.	07/11/2015	INDRA
1.0	Adding References.	07/12/2015	INDRA

D4.4
Profiles of Cyber-Criminals and Cyber-Attackers

Responsible

INDRA

Contributor(s)

NASK
SM
NCSRD
SBA
PROPRS
CEFRIEL
VITROCISET

Summary:

According to RFC494, the attack potential is defined as perceived likelihood of success should an attack be launched, expressed in terms of the attacker's ability (i.e. expertise and resources) and motivation. In this deliverable, the knowledge and resources required to commit a crime or terrorist act in the cyberdomain will be studied and assorted in categories.

Keywords: attacker, profile, attack, categories, security

TABLE OF CONTENTS

1 INTRODUCTION 8

1.1 PURPOSE OF THE DOCUMENT 8

1.2 STRUCTURE OF THE DOCUMENT 8

2 DEFINITIONS AND SCOPE 10

3 PROFILES OF CYBER-CRIMINALS AND CYBER-ATTACKERS 13

3.1 ATTACKS TO POSTAL AND LOGISTIC SERVICES 13

3.1.1 Profiling a Reported attack 13
3.1.2 Potential Attack In the Future 14
3.2 ATTACKS TO SOCIAL NETWORKS 18

3.2.1 Profiling a Reported attack: Information Elicitation via Social Engineering [CAPEC] 18
3.2.2 Potential Attack In the Future: Automatic Social Network Attacks (ASE) 19
3.3 ATTACKS TO UNMANNED SYSTEMS 21

3.3.1 Profiling a Reported attack: UAVs Hijacking by jamming and GPS signal spoofing 21
3.3.2 Potential Attack In the Future: Eavesdrop on telecommunications networks by UAVs 22
3.4 ATTACKS TO MOBILE BIOMETRY 24

3.4.1 Profiling a Reported attack 24
3.4.2 Potential Attack In the Future: Stole of personal health records and data 26
3.5 ATTACKS TO INDUSTRIAL CONTROL SYSTEMS 28

3.5.1 Profiling a Reported attack: Stuxnet 28
3.5.2 Potential Attack In the Future 28
3.6 ATTACKS TO SMART TRANSPORT (AUTOMOTIVE) 30

3.6.1 Profiling a Reported attack: Remotely Controlled Car 30
3.6.2 Potential Attack In the Future: Automatic Social Network Attacks (ASE) 31
3.7 ATTACKS TO INTERNET OF THINGS, QUANTIFIED SELF 34

3.7.1 Profiling a Reported attack: ThingBots 34
3.7.2 Potential Attack In the Future: Emotional Intelligence War 34
3.8 ATTACKS TO TRANSPORT CRITICAL INFRASTRUCTURE 36

3.8.1 Profiling a Reported attack: jamming of telecommunication by mean of GPS Jammers 36
3.8.2 Potential Attack In the Future: Intentional Electromagnetic Interference Attacks 36
3.9 ATTACKS TO VIRTUALIZATION TECHNOLOGIES 38

3.9.1 Profiling a Reported attack: Hyperjacking [CAPEC] 38
3.9.2 Potential Attack In the Future: VM-specific malware 39
3.10 ATTACKS TO CLOUD COMPUTING 40

3.10.1 Profiling a Reported attack: Cloud Leak 40
3.10.2 Potential Attack In the Future: Smart Cloud Attack 41
3.11 ATTACKS TO SMART GRIDS 43
3.11.1 Profiling a Reported attack: Blackout in New York 43
3.11.2 Potential Attack In the Future: Burgling Homes by means of Smart Meters 43
3.12 ATTACKS TO SMART CITIES 45
3.12.1 Profiling a Reported attack: Spying on citizens using home/building automation systems 45
3.12.2 Potential Attack In the Future: Disruption and causing of accidents through controlling traffic lights and systems 46
3.13 ATTACKS TO SMART BORDERS 47
3.13.1 Profiling a Reported attack: Sharing too much information 47
3.13.2 Potential Attack In the Future: Insufficient border control 47
3.14 ATTACKS TO BRING YOUR OWN DEVICE 49
3.14.1 Profiling a Reported attack: Employee-owned mobile devices 49
3.14.2 Potential Attack In the Future: BYOD Attack Vector 49
3.15 ATTACKS TO TELECOMMUNICATION SERVICES 52
3.15.1 Profiling a Reported attack: Bypass encryption of mobile device communication 52
3.15.2 Potential Attack In the Future: Mobile Attack of NGN-based Telco Systems 52
4 CONCLUSIONS 54
4.1.1 The main Attack Channel: Interconectedness 54
4.1.2 People are the "Weak Link": Unwise Implementations, Weak Configurtaitons, etc. 54
5 REFERENCES 55

Glossary

EC	European Commission
EU	European Union
CI	Critical Infrastructure
CIA	Confidentiality, Integrity and Availability
CPD	Cyber Physical Systems
D4.1	Deliverable 4.1 Technology Landscape Report
DoS	Denial of Service
DDoS	Distributed DoS
DoW	Description of Work
HW	Hardware
MITM	Man In The Middle
LEA	Law Enforcement Agency
LIS	Lawful Interception Systems
LEMF	Law Enforcement Monitoring Facilities
WP	Work Package

1.1 PURPOSE OF THE DOCUMENT

The technological landscape (Deliverable 4.1), and the security challenges depicted in deliverables 4.2 and 4.3 must face the threats posed by a wide spectrum of attacker profiles. These offenders (criminals and terrorist) are increasing their knowledge, coordination, sophistication and resources.

This deliverable is aimed at analyzing the map of offender profiles in order to relate each of them with the scenarios depicted in deliverable 4.1. That way, the picture of the technological scenario will enrich finally the viewpoint of the reader by mean of providing the offensive point of view.

1.2 STRUCTURE OF THE DOCUMENT

This report is the deliverable for "D4.4. Profiles of Cyber-Criminals and Cyber-Attackers" of the CyberROAD Project (www.cyberroad-project.eu). It includes the following sections:

1. *INRODUCTION:* This section, the introduction. The topic covered by the document is presented following the guidelines established in Description of Work (DoW)
2. *DEFINITIONS AND SCOPE:* The scope of this section is to define the concepts needed to develop the rest of the document.
3. *ATTACK CATEGORIES*: the attack are assorted in diferent categories based on diferent features, such as complexity, direction, knowledge and resources of the attackers, etc.
4. *TECHNOLOGICAL SCENARIOS*: to place the canonical attacks in the depicted scenarios in deliverable 4.1 is the culmination of the report. The detailed information of the offender will be encompassed in the emerging trends, such as BYOD, Smart Grid, Smart Cities, etc. The result of the analysis will provide a clear understanding of the technologies and techniques that attackers put into practice to commit their acts but also the technological problems underlying such attacks.

The main input for this document is the "D4.1 Technology Landscape Report" (D4.1) that conjointly with "D4.2. Security Challenges of Future and Emerging technologies" and "D4.3 Security Challenges in Critical Infrastructure" comprises the outcomes of technological aspects in Cyber Crime and Cyber Terrorism of the reserch roadmap.

The following Table lists that document and other key documents that help in understanding the background of this deliverable.

ID	Deliverable title	Dissemination level
D4.1	Technology Landscape Report	PU
D4.2	Security Challenges of Future and Emerging technologies	RE

Additional input documents are provided in the References section and cited within the document where appropriate.

The following template is applied for two different types of attacks. Firstly, for a relevant attack in the present or the past. Secondly, for a potential attack in the future. An overview is given for each of these attacks. Besides, a brief explanation for certain concepts is given.

Below, a list of concepts is available in order to identify the domain space of cybercrime / cyber security. (Please note: the following lists and subsequent related sections and subsections are for illustrative purposes only; they are not exhaustive and may be adapted and extended at any time):

Possible attacker categories [D2.1]:

- criminal groups, organized crime
- espionage groups
- insider
- phisher
- spammer
- malware attacker
- terrorist
- activist
- military
- intelligence agency

Source Sectors [Miller & Rowe, 2012]

Source of the incident if explicitly identified:

- Com – Denotes a commercial source (including consumer products, industry, small business).
- Gov – Denotes local or national government (including buildings/housing, emergency services, public benefits, social services, state and federal government, taxes, tribal governments, worker protections, environment, military).
- User – Denotes an individual user.

Types of attack [D2.1]:

- spam: the use of electronic messaging systems to send unsolicited bulk messages, especially advertising, indiscriminately.
- phishing scheme: the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication
- spyware: is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.
- malware: Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems

- exploit: is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized)
- botnet: a botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks.
- backdoor: a backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected.
- ransomware: is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed
- social engineering: in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information
- clumsy behavior: is the conception that some people might have predisposition, or that they might be more likely to suffer accidents, such as car crashes and industrial injuries, than other people
- misinformation: is false or inaccurate information that is spread unintentionally
- physical damaging: -
- insider attacks: Attacks perpetrated internally. Given the natural view of a conventional firewall on the networks topology as consisting of an inside and outside, problems can arise, once one or more members of the policy network domain have been compromised by internal staff.

The fundamental motivations of cyber attacks [D2.1]:

- financial drivers: Monetary gain, financial advantages, insider information
- governmental reasons: Sabotage of critical infrastructures, ideological and political activism, terrorism
- vengeance
- reputation
- stalking
- verification of systems to improve them
- unintentional: Unintentional damaging

Targets [D2.1]:

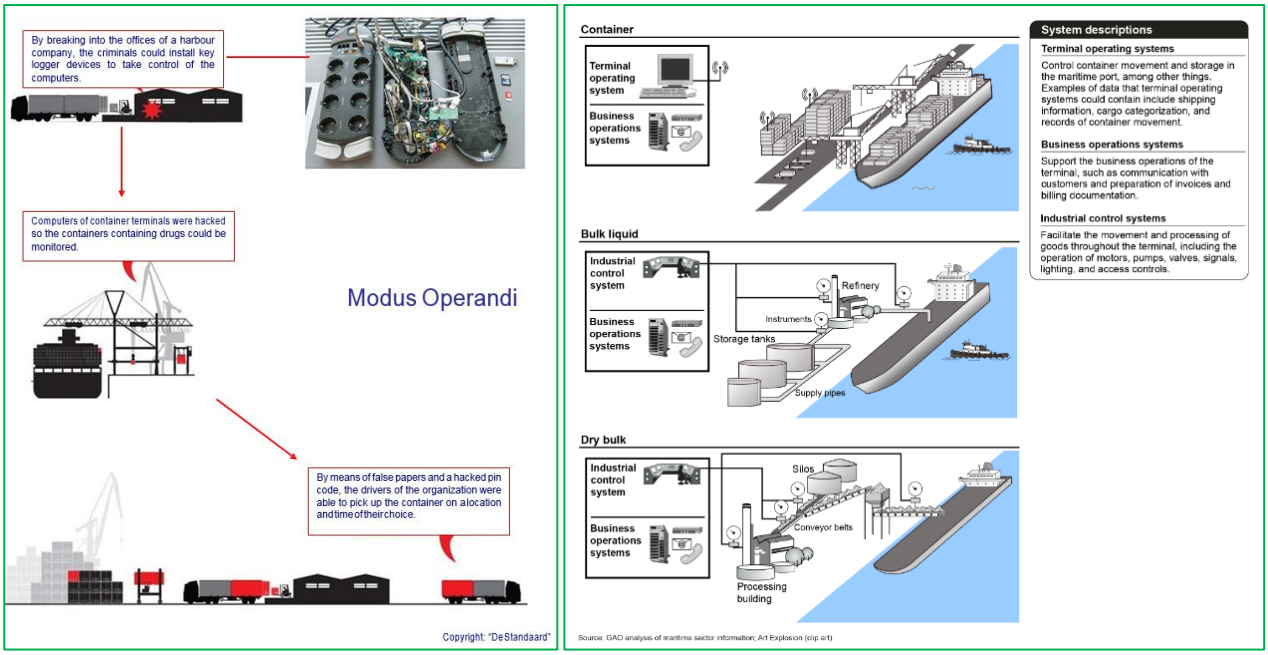
- industry
- finance
- government
- military
- private

Relevant Attack In the Present or the Past		
Attack Name		
Attacker	□ Organized group □ Espionage group □ Insider □ Phisher □ Spyware/malware attacker □ Terrorist □ Activist □ Others (please indicate, if any):	
Resources to commit the attack	[ ] Very High [ ] High [ ] Medium [ ] Low [ ] Very Low	Explanation
Knowledge of attacker(s)	[ ] Very High [ ] High [ ] Medium [ ] Low [ ] Very Low	Explanation
Source Sectors	[ ] Com – Denotes a commercial source. [ ] Gov – Denotes local or national government Edu [ ] User – Denotes an individual user [ ] Others	
Type of attack	[ ] spam [ ] phishing scheme [ ] spyware [ ] malware [ ] exploit [ ] botnet [ ] backdoor [ ] ransomware [ ] social engineering [ ] clumsy behavior [ ] misinformation [ ] physical damaging [ ] insider attacks [ ] Others	
Fundamental Motivation of attack	[ ] financial drivers [ ] governmental reasons [ ] vengeance [ ] reputation [ ] stalking [ ] verification of systems to improve them [ ] unintentional [ ] Others	
Target	[ ] industry [ ] finance [ ] government / national [ ] military [ ] private [ ] Others	

3.1 ATTACKS TO POSTAL AND LOGISTIC SERVICES

3.1.1 PROFILING A REPORTED ATTACK

Europol EC3 [Europol, 2013] reports that on June 2013, the members of a criminal group smuggled drugs through the Belgian harbor of Antwerp to The Netherlands. The criminal group used cyber-experts and took control of the computer systems of harbor logistic companies and container terminals. The intrusion started with a phishing attack: the criminals sent mail to staff members containing Trojans as attachments. Then they also physically penetrated into offices to install key logging devices to capture passwords. Once the computers were under their control, the group could follow "their" container and upon arrival, unload it to a location and at a time of their choosing. This in return enabled the criminal group's drivers to access the container before the normal harbor staff would.



3.1.1.1 *Resources to commit the attack*

Attacker: Organized group, phisher

- Resources to commit the attack: MEDIUM. Europol says the criminal group was professional and well-connected as demonstrated by the amounts of drugs seized; Some members of the criminal gang were cybercriminals; Some specific malicious tools and malware were used to perpetrate the attack.
- Knowledge of attacker(s): MEDIUM. Criminals knew where to buy, how to install and operate key logging devices; Criminals knew Social Engineering techniques and how to buy/use phishing kits (phishing attack); Criminals were able to buy/build a malware and to control it remotely; As specific knowledge of the logistic system that

has been violated was probably necessary to execute the cyber-attack; It is one of the first times this modus operandi has been revealed.

- Source sectors:
  - Others – Criminal Organization.
- Type of attack:
  - Phishing scheme
  - Spyware
  - Malware
  - Social engineering
  - Physical damaging
  - Others- Keylogging
- Fundamental motivation of attack:
  - Financial drivers
  - Drug smuggling
- Target:
  - Industry
    - Logistics sector

3.1.2 POTENTIAL ATTACK IN THE FUTURE

According to an authoritative report [PwC, 2014]:

"[…] *the transportation and logistics industry already relies heavily on Information and Communication* Technology *(ICT) and the trend is upwards. Virtual threats need to be taken just as seriously as physical ones. Cyber-attacks designed to induce physical damage will be an increasing threat for the transportation and logistics industry*".

Reuters reports [Wagstaff, 2015] that (in 2014):

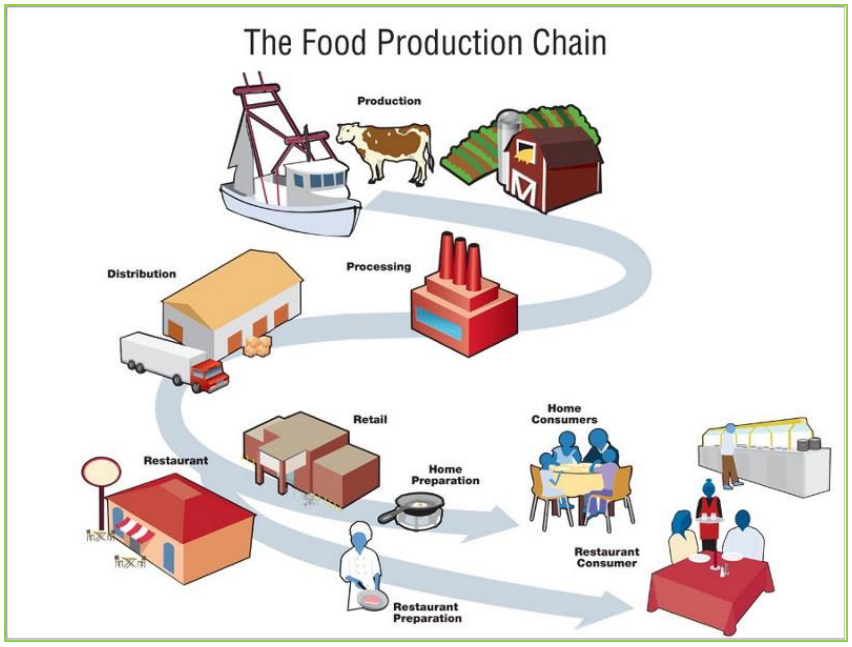
"[…] *hackers shut down a floating oil rig by tilting it, while another rig was so riddled with computer malware that it took 19 days to make it seaworthy again; Somali pirates help choose their targets by viewing navigational data online, prompting ships to either turn off their navigational devices, or fake the data so it looks like* they're *somewhere else".*

"[…] *already €570m is lost annually* within *the UK gas and oil industry alone due to cyber theft. Globally, it estimated that cyber-attacks against oil and gas infrastructure will cost energy companies close to €1.8 billion by 2018*".

Transportation and Logistics IT support systems (especially the oldest ones) are not designed with security in mind and it is quite common that operational security (SOCs, CERTs) does not take them into proper consideration.

The birth of strongly financed cyber-armies [ArcCyber] [BBC] and the rise of state-sponsored cyber-attacks [Brownlee, 2015] makes plausible attack scenarios so far considered impossible to carry out. Therefore, both critical infrastructures and the supply chain (including logistic infrastructures and services) are now attractive targets for cyber-criminals (e.g. frauds, thefts), terrorists (e.g. cyber-terror, service/physical disruption), hacktivists (e.g. service/physical disruption, data theft) and governments (e.g. cyberwarfare, cyber-espionage). A description of a potential attack to logistic infrastructures follows:

A politically motivated attack, targets the food production chain of a country that strongly relies on road transportation for regional and last-mile distribution.



(source: medium.com)

The attackers intend to create a chaotic situation affecting the greatest possible number of citizens and workers in the supply chain, in order to damage country's reputation and to cause substantial economic damage.

The attackers start hacking the accounts of journalists working in or more press agencies of high reputation (for example using a *targeted phishing attack*);

Using the hacked accounts, a coordinated attack starts with the publication of news regarding a really unpopular decision the government is going to take (for example the introduction of a new heavy tax on regional and local transportation with high impact on primary goods' price - *misinformation attack*);

At the same time, using hundreds of fake social network accounts, the news are spread and compounded, adding other false details and using angry expressions in order to incite unrest among the population (*social engineering*);

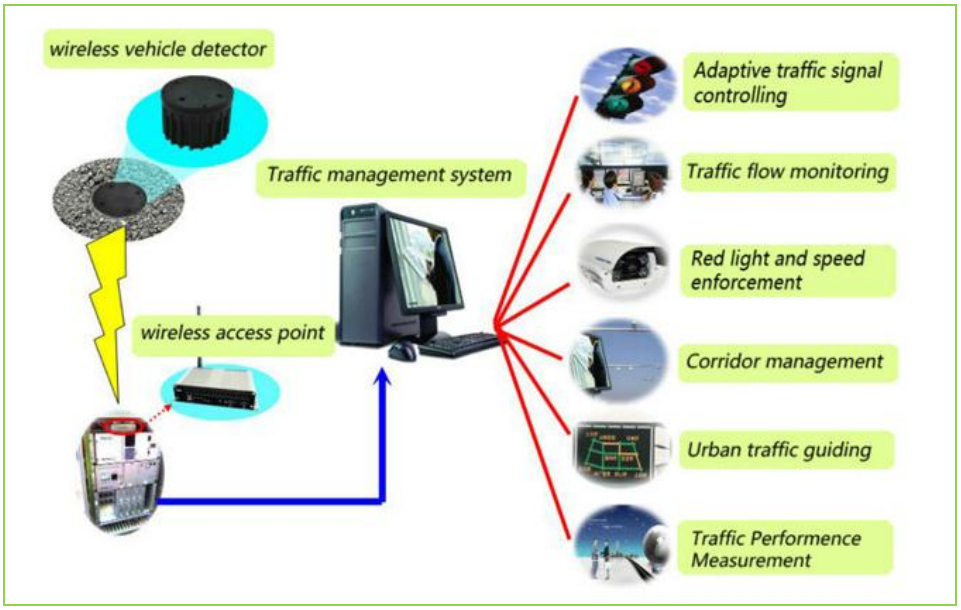
The attackers preventively selected and silently compromised the business operations systems of several important players in logistics operations at national and local level. In particular they focused on the ones involved in primary goods transportation (e.g. perishable goods, medicines, live animals and fuel) (*malware infection*);

A coordinated action disrupts the business operations of the compromised logistic players, affecting communication with customers, scrambling, altering and deleting data needed for the preparation of invoices and billing documentation. This action causes big delays in shipments that in a short time generates a primary goods shortage in wholesale, retail and institutional markets; The shortage of fuel exacerbates the problems (*malware infection*);

(source: www.wholesomewave.org)

The major highway toll booth management systems are infected by malware randomly creating long queues and affecting cars and trucks circulation (*malware infection*);

Traffic management systems in major cities falls under control of the attackers, randomly creating big traffic jams and provoking car incidents (*malware infection*);



(source: www.rosimits.com)

The coordinated execution of such a complex attack is now plausible, considering the resources available to a state-sponsored cyber-army or to an international terrorist organization.

3.1.2.1 *Resources to commit the attack*

Attacker: Organized group, Terrorist.

- Resources to commit the attack: VERY HIGH. Different and coordinated attack teams should be set-up, each team consisting of a significant number of members; The teams should operate long before the attack execution in order to penetrate the various systems and to compromise them persistently; Sophisticated, maybe customized attack tools should be developed and used; Several zero-day vulnerabilities should be exploited; Reliable and untraceable support infrastructures should be available;
- Knowledge of attacker(s): VERY HIGH. A deep knowledge of different attack techniques are needed; Psychological and communication skills are needed to support the social engineering campaign; Various technical skills and abilities are needed; A specific knowledge of the attacked management systems is needed;
- Source sectors:
    - Gov – Denotes local or national government
- Type of attack:
    - Phishing scheme
    - Spyware
    - Malware
    - Exploit
    - Social engineering
    - Misinformation
    - Physical damaging
- Fundamental motivation of attack:
    - Governmental Reasons
    - Reputation
    - Vengeance
    - Others - Cyber-warfare, Retaliation, Sabotage, Diversion
- Target:
    - Industry
    - Government
    - Private
    - Others - Logistic chain, Supply chain

3.2 ATTACKS TO SOCIAL NETWORKS

3.2.1 PROFILING A REPORTED ATTACK: INFORMATION ELICITATION VIA SOCIAL ENGINEERING [CAPEC]

Social Engineering attacks through Social Media sites have been common and widely observed in the past years [Gohel, 2015] . According to the major security companies, Social Media accounts – for example – are heavily targeted by cybercriminals and cyberterrorists as the attacks have a surprisingly high success rate and the attack outcomes are rewarding. The depicted situation is becoming a major concern in particular for enterprises. In 2010, a controversial security expert created a fake character (Robin Sage) and several false profiles on the most common social networks (Facebook, Twitter, LinkedIn, etc.).

"Robin Sage" as she appeared on social networking pages.

Robin Sage was depicted as a young but experienced cyber-threat analyst. Her pictures shown a good-looking young woman. Using this fake account, the security expert befriended men and women of all ages during a short time period (about 1 month). Almost all of them were working for the US military, government or companies (including CIA and the FBI). Abusing the trust relationship established with these contacts, the expert "…gained access to email addresses and bank accounts as well as learning the location of secret military units based on soldiers' Facebook photos and connections between different people and organizations. He was also given private documents for review and was offered to speak at several conferences." [Robin Sage] The security expert concluded that similar findings could have compromised national security if a terrorist organization had employed similar tactics

3.2.1.1 *Resources to commit the attack*

Attacker: Organized group, Espionage group, phisher, Spyware/Malware attacker, Terrorist, Activist.

- Resources to commit the attack: MEDIUM. The initial setup of fake social media accounts requests limited resources, but to keep the attack credible, persistent and sustainable over time, the accounts needs to be managed and monitored according to a pre-defined strategy that should be coherent to the attackers' objectives.
- Knowledge of attacker(s): LOW. To be effective, Social Engineering attacks on Social Media does not require specific technical knowledge other than being masters in the "art of deception". Psychological and communication skills are an obvious advantage for the attackers.
- Source sectors:
  - Com – Denotes a commercial source.
  - Gov – Denotes local or national government

- User – Denotes an individual user
- Others – Military, Activists, Criminal Organizations, Terrorists, etc.

- Type of attack:
  - Social engineering
  - Misinformation
- Fundamental motivation of attack:
  - Financial drivers
  - Governmental reasons
  - Vengeance
  - Stalking
  - Verification of systems to improve them
- Target:
  - Industry
  - Finance
  - Government / national
  - Military
  - Private
  - Others

3.2.2 POTENTIAL ATTACK IN THE FUTURE: AUTOMATIC SOCIAL NETWORK ATTACKS (ASE)

In the last few years, the appearance of some new technologies (including Social Networks) allowed to greatly automate most of the Social Engineering steps against a large number of people/victims at the same time [Huber et al., 2009]. This phenomenon that we call Social Engineering 2.0 (SE 2.0) greatly uses advanced automatic methods to gather and elaborate the information needed to select precisely the "victims". SE 2.0 includes many renewed and new technologies such as Open Source Intelligence (OSINT) and Social Network Analysis (SNA), psychological profiling (for example through personality profiling to identify most vulnerable persons), memetics [Blackmore, 1999] and sentiment analysis.

Overview of the main characteristics of Social Engineering 2.0 (source: CEFRIEL)

The modern social engineers use a large and complex mix of different competences (technological, cyber-sociology, psychological, marketing, design, etc.) to create a complete attack. One of the most important trends characterizing the SE 2.0 are the Automatic Social Network Attacks (ASE): automation of SE attacks through information collection and mining and through the sentiment analysis from Social Networks.

3.2.2.1 Resources to commit the attack

Attacker: Organized group, Espionage group, Terrorist, Activist.

- Resources to commit the attack: MEDIUM. For the purpose of carrying out such kind of attacks, it is necessary to use automated tools for massive information collection, mining and sentiment analysis. Appropriate computational and storage resources should be also available
- Knowledge of attacker(s): HIGH. Psychoanalytic skills proficiency is necessary to monitor the victims and induce them to do things they do not want to do, e.g. to reveal personal information or habits. Furthermore, it is vital to have a full knowledge of tools for massive information collection, mining and sentiment analysis. Depending on the type of Cyberattack being used, further specific skills are needed (e.g. a viral cyberattack through a video, needs video editing and graphics skills);
- Source sectors:
    - Com – Denotes a commercial source.
    - Gov – Denotes local or national government
    - User – Denotes an individual user
    - Others – Military, Activists, Criminal Organizations, Terrorists, etc.
- Type of attack:
    - Social engineering
    - Misinformation
- Fundamental motivation of attack:
    - Financial drivers
    - Governmental reasons
    - Vengeance
    - Stalking
    - Verification of systems to improve them
    - Others - Espionage, Cybercrime, Terrorism, etc
- Target:
    - Industry
    - Finance
    - Government / national
    - Military
    - Private
    - Others - Everyone who owns a social media account is a potential target

3.3 ATTACKS TO UNMANNED SYSTEMS

3.3.1 PROFILING A REPORTED ATTACK: UAVS HIJACKING BY JAMMING AND GPS SIGNAL SPOOFING

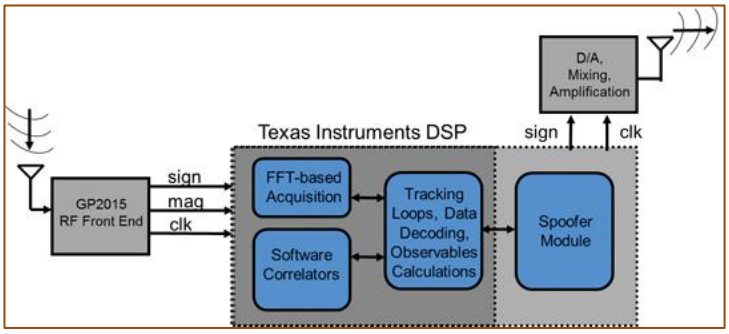
Currently UAVs (Unmanned Aerial Vehicles) are used for a wide range of purposes such as transportation, border surveillance, reconnaissance, and armed attacks. By 2012 the U.S. military only, had increased its investment in research and production of unmanned aerial vehicles (UAVs) from $2.3 billion in 2008 to $4.2 billion [True, 2014] .

Events such as the loss of an RQ-170 Sentinel drone to Iranian military forces on 4th December 2011 show that the efforts of the past to identify risks and harden UAVs are insufficient, but researchers in this field are "up in arms" [CyCon, 2013] .

UAV's Ground Control Station (source: www.militaryaerospace.com)

Details on the Iranian attack are not disclosed but an Iranian engineer claimed in an interview that "Iran managed to jam the drone's communication links to American operators" causing the drone to shift into an autopilot mode that relies solely on GPS to guide itself back to its home base in Afghanistan. With the drone in this state, the Iranian engineer claimed that "Iran spoofed the drone's GPS system with false coordinates, fooling it into thinking it was close to home and landing into Iran's clutches." [GPSWorld]

In February of 2012, the US Congress passed the FAA Modernization and Reform Act of 2012. Such civilian UAVs would be primarily guided by civil GPS, which has been shown to readily spoofable in the lab. On invitation of the Department of Homeland Security (DHS), unclassified spoofing tests against a UAV were performed at White Sands Missile Range (WSMR) on June 19, 2012 during the DHS GYPSY test exercise. The civil GPS spoofer used for these tests is an advanced version of the spoofer reported in 'Assessing the Spoofing Threat' .



Spoofing Schema (source: gpsworld.com)

3.3.1.1 *Resources to commit the attack*

Attacker: Organized group, Espionage group, Terrorist, Activist.

- Resources to commit the attack: VERY HIGH. To execute such kind of attack it is necessary to have resources to track an UAV during its travel (e.g. radar stations), to be able to jam radio signals and interrupt communication between the UAV and its Ground Control Station and to be ready to spoof GPS signals.
- Knowledge of attacker(s): VERY HIGH. Very high skills are needed to run such an attack. The attacker has to know which kind of UAV is going to attack and its technical specifications. Deep engineering skills are needed.
- Source sectors:
  - Gov – Denotes local or national government
  - Others – Military, Activists, Criminal Organizations, Terrorists, etc.
- Type of attack:
  - Physical damaging
  - Misinformation
  - Others - Denial of Service
- Fundamental motivation of attack:
  - Financial drivers
  - Governmental reasons
  - Vengeance
  - Reputation
  - Others - Espionage, Cybercrime, Terrorism, etc.
- Target:
  - Industry
  - Government / national
  - Military

3.3.2 POTENTIAL ATTACK IN THE FUTURE: EAVESDROP ON TELECOMMUNICATIONS NETWORKS BY UAVS

The air space is destined to become soon a highly sophisticated surveillance area for non-military purposes. In the U.S., there are already hundreds of public bodies, universities and departments that own a specific license from the FAA (Federal Aviation Administration) allowing them to pilot UAVs (Unmanned Aerial Vehicles) over the country [De Medici, 2013]. The same FAA predicts that in twenty years no less than twenty thousand devices will be in

operation in the United States of America (world's largest producer of devices UAV) on behalf of public and commercial entities.

Security specialists predicts [Globalsecuritymag] "*that it will not be long before reports start to circulate that drones are being used in cyber-attacks on businesses and individuals, where the devices eavesdrop on wireless computer and telecommunications networks*".

"*Drones readily available on the consumer market can be easily adapted to carry electronic eavesdropping equipment. It is clear that over the coming few years, countries, organizations and businesses will have to re-think their security strategies to combat this new potential cyber threats*".

3.3.2.1 Resources to commit the attack

Attacker: Organized group, Espionage group, Terrorist, Activist.

- Resources to commit the attack: LOW. UAVs are getting cheaper and cheaper and easy to buy while electronic eavesdropping equipment cannot be bought "off the shelf" but have a relatively affordable price.
- Knowledge of attacker(s): HIGH. Piloting UAVs and assembling and using electronic eavesdropping equipment are still activities that require specific knowledge and advanced technical skills.
- Source sectors:
  - Others – Eavesdropping, Communication Hijacking, Malicious Traffic Injection.
- Type of attack:
  - Social engineering
  - Misinformation
- Fundamental motivation of attack:
  - Financial drivers
  - Governmental reasons
  - Vengeance
  - Reputation
  - Stalking
  - Verification of systems to improve them
  - Others - Espionage, Cybercrime, Terrorism, etc
- Target:
  - Industry
  - Finance
  - Government / national
  - Military
  - Private
  - Others - Even single users are a potential target

3.4 ATTACKS TO MOBILE BIOMETRY

3.4.1 PROFILING A REPORTED ATTACK

As reported in D4.1 in general the so called "Mobile Biometry" is a new branch of biometry whose characteristics are:

- Tight integration with mobile terminals such as smartphones or wearable Internet of things devices
- Low cost of sensors
- Typical usage for personal authentication either locally or for remote services (e.g., m-banking) in heterogeneous contexts[1, 2] (The first paper surveys 160 cases where biometric identification has been used for economic, political, and social purposes in developing countries, the second one surveys 121 banks in the world which use biometrics in their operations)
- Data fusion and integration of different biometric data

The most relevant attacks when dealing with mobile biometry, beside all those already known for "classic" biometry[3], arise from the heterogeneous diffusion of sensors, produced with different quality criteria and accessible to vulnerable targets, like smartphones, which could become a Trojan horse for the biometric devices.

This threat model customizes the more generic one of IoT, where the attacker could gain physical control over the node. This is probably the most important difference because the attacker can dissect the stolen node at home privately without any disturb and has full access to the hardware (e.g. mobile biometry is vulnerable to physical attacks such as chip-off, de-soldering of components to reverse the firmware etc., which are not common in normal biometry).

This threat has also renewed thanks to recent exploits in wearable sensors connected to vulnerable terminals, or even with weak communication channels[4] or unprotected on-board firmware[5].

The general attack chain is the following one:

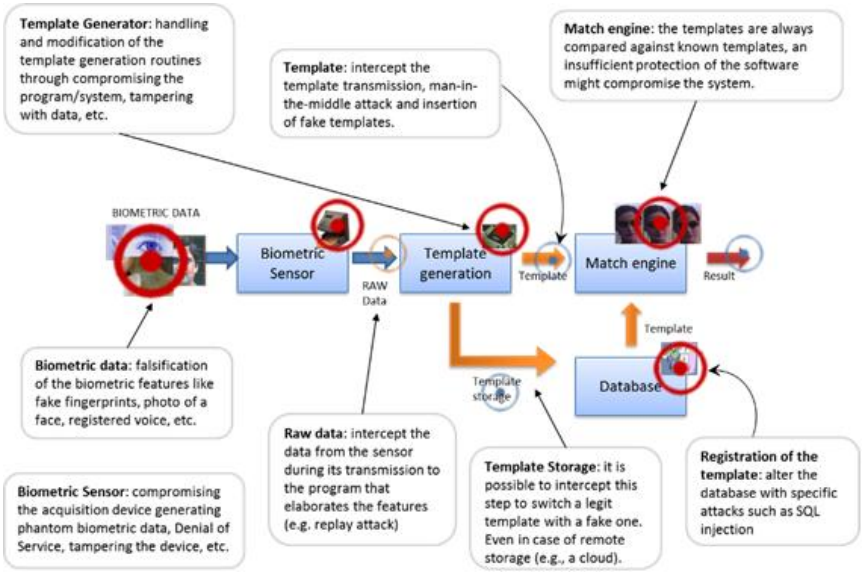
[1] Gelb and J. Clark, 'Identification for Development: The Biometrics Revolution', SSRN Electronic Journal.

[2] Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System, J of Basic and Applied Scientific Research, issue 2(9) p. 9152-9160, 2012.

[3] Singh, Y. N. and Singh, S. K. (2013) 'A taxonomy of biometric system vulnerabilities and defences', International Journal of Biometrics, 5(2), p. 137.

[4] Why Links Between Smartwatches and Phones Could be Vulnerable to Attacks - http://mcaf.ee/c2nmaf

[5] Wearables May Be Vulnerable to Cyberattack | Pure Situation Room - http://mcaf.ee/6vewrf



And the general threats could be grouped in the following five categories[6]:

- Lack of transport encryption
- Insecure Interfaces
- Insufficient User Authentication/Authorization
- Insecure Software/Firmware
- Privacy Concerns

3.4.1.1 Resources to commit the attack

Attacker: Organized group, phisher, Spyware/Malware attacker.

- Resources to commit the attack: MEDIUM. The overall security level of most products is relatively poor, being the market extremely competitive now and in an important expansion phase, the security features are not among those attracting the investors. A poor implementation of the security features is the result of this situation also for trending products[7].
- Knowledge of attacker(s): MEDIUM. The generic knowledge required to attack such terminals is generally averaged and available on the black market. The only complexity is that this type of terminals are not often exposed themselves, but though a bridge terminal such as the smartphone. Therefore, a new class of infecting vectors uses the smartphones as a trampoline for the final wearable target.
- Source sectors:
  - User – Denotes an individual user
  - Others – Criminal Organizations.
- Type of attack:
  - Spyware

[6] Internet of Things Security Study: Smartwatches, HP, Available at: http://go.saas.hp.com/l/28912/2015-07-20/325lbm/28912/69038/IoT_Research_Series_Smartwatches.pdf

[7] PoC hack on data sent between phones and smartwatches (updated) | Ars Technica - http://mcaf.ee/lunyf5

    - Malware
    - Exploit
    - Botnet
    - Backdoor
    - Ransomware
    - Social engineering
    - Physical damaging
- Fundamental motivation of attack:
    - Financial drivers
    - Stalking
    - Others – Drug Smuggling
- Target:
    - Industry
    - Private
    - Others – Logistic sector

3.4.2 POTENTIAL ATTACK IN THE FUTURE: STOLE OF PERSONAL HEALTH RECORDS AND DATA

For a long time the threats of mobile biometry and wearable will be more or less those described by HP into their whitepaper[8]:

1. Lack of transport encryption
2. Insecure Interfaces
3. Insufficient User Authentication/Authorization
4. Insecure Software/Firmware
5. Privacy Concerns

These threats are nowadays mostly tied to the release of new, but faulty, products and a solution could be the adoption of standardized secure methodologies, as also suggested by the Cloud Security Alliance[9]. However, with the increasing obsolescence of the products on the field, there are some other problems arising. The problematic updating of devices that are not autonomous may for example lead to usage of old or faulty crypto suites.

Beside this mobile biometry is good for local authentication: if the biometric data is transmitted over a network it could be easily stolen and used with a MITM attack-schema to authenticate an attacker. This scenario becomes more problematic considering also that, if a biometric data is stolen it cannot be substituted or replaced.

---

[8] Internet of Things Security Study: Smartwatches, HP, Available at: http://go.saas.hp.com/l/28912/2015-07-20/325lbm/28912/69038/IoT_Research_Series_Smartwatches.pdf

[9] VV, AA. 'Security Guidance for Early Adopters of the Internet of Things (IoT).' CSA Cloud Security Alliance, Mobile Working Group. N.p., 20 Apr. 2015. Web. 26 Apr. 2015. https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

The future of mobile biometry is anyway extremely interesting also for the increasing interest in the behavioral security solutions: increasingly the security industry is looking for alternatives to the hard to manage and all too easily compromised password.[10]

3.4.2.1 *Resources to commit the attack*

Attacker: Organized group, Phisher, Spyware/Malware Attacker, Terrorist.

- Resources to commit the attack: HIGH. The type of threat is highly exploitable because of the mass nature of mobile biometry nowadays: once a system is vulnerable, it becomes easily exploitable by Trojans or other malevolent vectors thanks to the indirect connectivity of these gadgets (e.g. via the smartphone's connectivity).
- Knowledge of attacker(s): VERY HIGH. The behavioral security is a concrete application of mobile biometry that is leading the market as an alternative to the too weak password based systems, or in general the "you're in/you're out" authentication systems. This application will lead the mobile biometry industry toward more secure products pushing up the resources required to successfully attack a system. Another complication is the adoption of behavioral biometry thanks to the integration of multiple values.
- Source sectors:
  - User – Denotes an individual user
- Type of attack:
  - Spyware
  - Malware
  - Exploit
  - Botnet
  - Backdoor
  - Ransomware
  - Social engineering
  - Physical damaging
- Fundamental motivation of attack:
  - Reputation
  - Stalking
  - Others - Cyber-warfare, Retaliation, Sabotage, Diversion
- Target:
  - Industry
  - Government / national
  - Private
  - Others - Logistic chain, Supply chain

[10] How behavioral biometrics can help secure systems - http://mcaf.ee/h5g827

3.5 ATTACKS TO INDUSTRIAL CONTROL SYSTEMS

3.5.1 PROFILING A REPORTED ATTACK: STUXNET

In June 2010, it was discovered that a worm dubbed Stuxnet had struck the Iranian nuclear facility at Natanz. Stuxnet used four 'zero-day vulnerabilities' (vulnerabilities previously unknown, so there has been no time to develop and distribute patches). The worm employs Siemens' default passwords to access Windows operating systems that run WinCC and PCS7 programs. The worm would hunt down frequency-converter drives made by Fararo Paya in Iran and Vacon in Finland. These drives were used to power centrifuges used in the concentration of the uranium-235 isotope. Stuxnet altered the frequency of the electrical current to the drives causing them to switch between high and low speeds for which they were not designed. This switching caused the centrifuges to fail at a higher than normal rate [Farwell & Rohozinski, 2011].

3.5.1.1 *Resources to commit the attack*

Attacker: Organized group.

- Resources to commit the attack: VERY HIGH. Although Stuxnet details are uncertain, the offenders went to great lengths to commit the attack. Several big companies were involved to develop the most famous cyberweapon so far. "*The level of effort to create Stuxnet has been estimated to cost millions of dollars*" [TERR]
- Knowledge of attacker(s): VERY HIGH.
- Source sectors:
  - Com – Denotes a commercial source.
  - Gov – Denotes local or national government
- Type of attack:
  - Malware
  - Exploit
  - Backdoor
  - Social engineering
  - Physical damaging
- Fundamental motivation of attack:
  - Governmental Reasons
- Target:
  - Industry
  - Government / national

3.5.2 POTENTIAL ATTACK IN THE FUTURE

Industrial Control Systems will not be out of the grasp of a total interconnectedness world. In the following paragraph an hypothetical situation will be explained:

The employees of a Nuclear Plant usually bring their smart phones to work place; the Chief Information Security Officer ignores the threat since nothing happened so far.

Meanwhile the terrorist group is using social engineering to convince an employee of installing a game in his smartphone. They researched *the possibility for every employee, two of them have*

enabled "root user" in their smartphones. Finally one of them has installed the game with malicious behavior.

The malware misuses the camera, microphone and Bluetooth to provide sensitive information to the terrorist group. Later this information will be studied by terrorists for carry out a second phase of the attack.

3.5.2.1 Resources to commit the attack

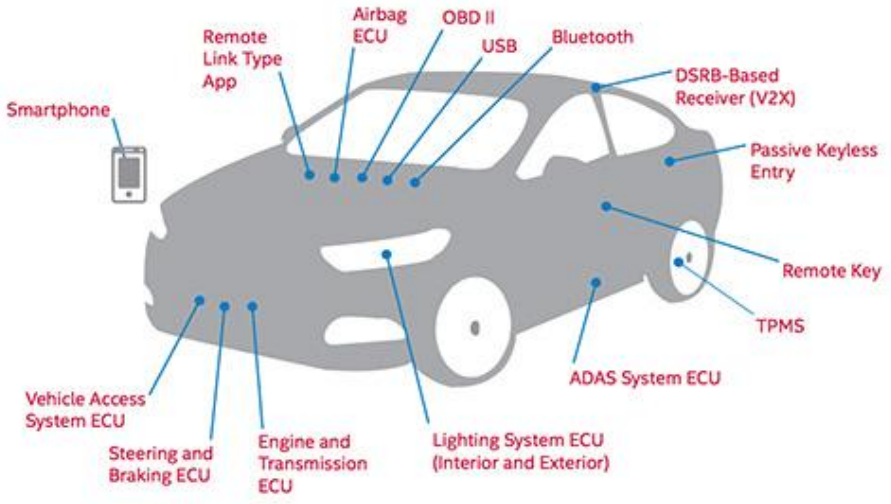
Attacker: Terrorist.

- Resources to commit the attack: VERY HIGH.
- Knowledge of attacker(s): VERY HIGH.
- Source sectors:
  - Com – Denotes a commercial source.
  - Gov – Denotes local or national government
- Type of attack:
  - Spyware
  - Malware
  - Social engineering
- Fundamental motivation of attack:
  - Governmental Reasons
  - Reputation
- Target:
  - Industry

3.6 ATTACKS TO SMART TRANSPORT (AUTOMOTIVE)

3.6.1 PROFILING A REPORTED ATTACK: REMOTELY CONTROLLED CAR

In July 2015 hacker successfully took control of a Jeep Cherokee probably it is the most famous sample of a successful attack to a Smartcar, to date [WIRED]. In general anyway Intel recently created a big consortium specifically meant to address these threats [Intel] within the automotive industry. The following figure shows all the possible channels through which an attack may come.



Sample of hacking unsecure and badly implemented solutions for smartcars are nowadays very common, despite at research level due to the limited diffusion in the real live of this type of vehicles [THEHACKERNEWS]. On the other hand modern nowadays mainstream cars are still partially not really "smart" and the attack surface is often still limited [Thestack]

3.6.1.1 *Resources to commit the attack*

Attacker: Organized group, phisher.

- Resources to commit the attack: MEDIUM. There's still not real evidence of large scale attacks and most of the proof of concepts (some of them more than a proof of concept) require a lot of specific knowledge. Despite this the attacked targets proven to be very weak and this poses the pre-condition that crime will appear in this area as soon as there will be relevant asset to steal. At the current state of art most of the cases were meant to physically steal the car (e.g. weakness of some smartkey systems).
- Knowledge of attacker(s): MEDIUM. The leading security model is security by obscurity, because most of the current threats come from the research area and not from the underground. The lack of standards hacking a car still requires a lot of specific knowledge, but on the other hand the targets proven often weak.
- Source sectors:
  - Criminal Organizations.
- Type of attack:
  - Spyware
  - Malware

    - Exploit
    - Botnet
    - Backdoor
    - Ransomware
    - Social engineering
    - Physical damaging
    - Others - Keylogging
- Fundamental motivation of attack:
    - Financial drivers
    - Others - Drug Trafficking
- Target:
    - Industry
    - Others – Logistics sector

3.6.2 POTENTIAL ATTACK IN THE FUTURE: AUTOMATIC SOCIAL NETWORK ATTACKS (ASE)

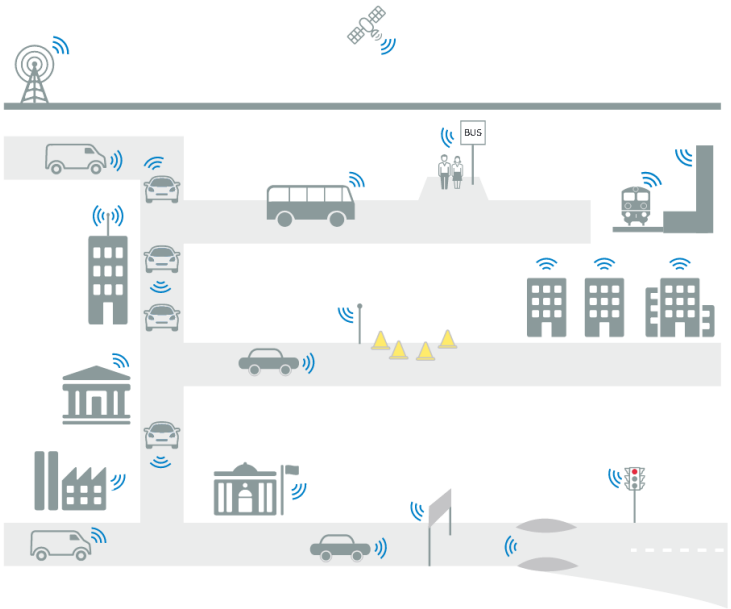
Both the market share of smart cars and the complexity of in-vehicle data exchange services are increasing. The samples seen so far are just early challenges posed by security. By this point of view, the smart-car's market grew rapidly, but in most cases without much attention to the security. In general terms these are the most challenging threats

- **Security & Privacy for context aware systems.** The automotive is expected to increasingly see the adoption of Context aware systems and immersive interfaces (e.g. augmented reality) where the IT complexity is disappearing. This poses new threats and approaches to security which are largely to be investigated.
- **Secure IT Architectures:** The modern cars are increasingly becoming complex IT systems and are moreover always connected. This faces these systems to all the security problems already known for online systems (malware, DoS, attacks). The software and IT architectures must be developed from scratch using a proper approach. One reasonable solution is to re-think them with a trusted platform approach, like Apple is also doing with their "iOS in the car" system.
- **Secure development of onboard software:** In almost any modern software system, exposed to external menaces the Secure Software Development Lifecycle (SSDL) is a stable and well known best practice, which has still largely not been adopted in the automotive world. This could lead to change the development methodologies with the final result of having more robust software with security in mind from the early development steps.
- **Secure deploy of updates (OTA or wired):** Like any other complex IT system, also in-car software needs to be updated. Nowadays used solutions are either OTA or tokens (e.g. USB sticks or pen-drives), but whatever solution it is used there are specific security problems that must be deeply faced and solved. A wrong or malevolous update of the onboard systems could lead to serious problems.
- **eTrust of the communication channels:** Any communication channel in complex IT services must be properly secured, this means proof of the source and the destination, privacy of the channel and data integrity. All these requirements can and must be embodied in the way the car communicates with external data sources, to prevent leaks or damages. Modern solutions derived from mobile applications, can be adopted in automotive world.

Moreover, existing standards are not really tested against real threats and attacks, often no real assessment have been done on the existing protocols. For example this is exactly nowadays problem of the vehicle-to-road and vehicle-to-vehicle interactions standards which are still to come on the market and yet not fully tested against security and are an huge source of data exchange between uncontrolled hosts the road and potentially the cars which can be either source of malicious exploits (actually mostly the roads)

- V2X gateway and related security policies are still at prototype solution
    - Specifications and first security solutions by PRESERVE, EVITA, SeveCom FP7 projects
    - Early implementation exists, but are far from market (http://www.darkreading.com/attacks-breaches/car-hacking-prototype-passes-crash-test/d/d-id/1319794)
- Intrusion Detection (IDS) for automotive interfaces and gateways is missing
    - Anomaly detection on ECU's and other SW/HW components
    - Attack signature-based detection on network (over V2X or CAN protocols, via the CAN Hacking Tool for example[Thehackernews, 2014] [INFOSECInstitute])

Thanks to V2X protocols the cars are foreseen to increasingly exchange data with the surrounding environment, within what is called an ecosystem. The most used term in this are is ecosystem because there are different elements concurring to create an extensive and capillary system of data and information exchange among vehicles and surrounding roads and infrastructures. This problem naturally interface with the world of IoT and Smart-Cities and inherits from these worlds the most challenging security issues [Wired, 2012] [CloudSecurityAlliance, 2015] [Thehackernews, 2015]



Another interesting threat recently underlined by Europol [Zdnet] is about the ransomware attacks to smartcars, eg. against the Smart locking systems [Thehackernews, 2015].

3.6.2.1 Resources to commit the attack

Attacker: Organized group, Phisher, Malware, Terrorist.

- Resources to commit the attack: HIGH. The foreseen availability of IoT nodes in the cities is so huge that it will be impossible to control all the functioning elements. The most challenging issues of the IoT world are:
  - Some unique problem for security like, the single node can be stolen and "dissected" at home by the attacker without being noticed by anyone.
  - Smart cities are a result of different actors not all equally approaching the security problems
- Knowledge of attacker(s): VERY HIGH. A deep knowledge of different attack techniques are needed; Various technical skills and abilities are needed; A specific knowledge of the attacked management systems is needed.
- Source sectors:
  - User – Denotes an individual user
- Type of attack:
  - Spyware
  - Malware
  - Ransomware
  - Exploit
  - Botnet
  - Backdoor
  - Physical damaging
- Fundamental motivation of attack:
  - Vengeance
  - Reputation
  - Others - Cyber-warfare, Retaliation, Sabotage, Diversion.
- Target:
  - Industry
  - Government / national
  - Private
  - Others - Logistic chain, Supply chain.

3.7 *Attacks to Internet of Things, Quantified Self*

3.7.1 Profiling a Reported attack: ThingBots

In January 2014 Proofpoint disclosed their spam and phishing campaigns monitoring results. Statistical data they provided revealed that many of the devices compromised in order to send e-mail were in fact what is called "internet of Things". These included a fridge, set-top boxes, or "smart" television sets. They were exploited and became a part of botnet used by the attackers to endanger other Internet users.

3.7.1.1 *Resources to commit the attack*

Attacker: Organized group, Espionage group, phisher, Spyware/Malware attacker, Terrorist, Activist.

- Resources to commit the attack: LOW. Usually IoT devices have unpatched, publicly known vulnerabilities and, in some cases, cannot be patched. Attackers can use open sourced tools and common devices (e.g. WiFi card) to exploit them.
- Knowledge of attacker(s): LOW. Due to the number of unpatched devices, publicly available exploits should work on most of them. These exploit require a fairly low level of knowledge, as they are even incorporated in standard pentesting frameworks.
- Source sectors:
  - User – Denotes an individual user
- Type of attack:
  - Spam
  - Phishing scheme
  - Spyware
  - Malware
  - Exploit
  - Botnet
  - Misinformation
- Fundamental motivation of attack:
  - Reputation
  - Stalking
  - Unintentional
- Target:
  - Private

3.7.2 Potential Attack In the Future: *Emotional Intelligence War*

In the future, more and more people will join the Quantified Self movement and use that technology to track their health status and sports achievements. By doing so, they expose data about themselves to the devices that are untrusted and hard to update. A targeted attack on CEO or government official, that extracts all of that data can expose their secrets or be used to gain advantage. Attackers know when the target is happy or aroused and what his current health condition is. They can use that knowledge to threaten the target or, when the target does not know about the attack, steer him or her to making a decision benefiting the attacker.

3.7.2.1 *Resources to commit the attack*

Attacker: Organized group.

- Resources to commit the attack: MEDIUM. Attackers have to observe the target to know which devices he or she uses and to confirm that they indeed have access to them. This requires some resources dedicated to surveillance.
- Knowledge of attacker(s): HIGH. While the devices are usually left unpatched, targeting a specific device can be challenging and may require some research.
- Source sectors:
  - Com – Denotes a commercial source.
  - Gov – Denotes local or national government
- Type of attack:
  - Social engineering
  - Spyware
- Fundamental motivation of attack:
  - Financial drivers
  - Governmental reasons
  - Reputation
  - Stalking
- Target:
  - Finance
  - Government / national

3.8 ATTACKS TO TRANSPORT CRITICAL INFRASTRUCTURE

3.8.1 PROFILING A REPORTED ATTACK: JAMMING OF TELECOMMUNICATION BY MEAN OF GPS JAMMERS

There have been recorded cases where illegal GPS jammers interfered with critical infrastructures and specifically with telecommunication components. For example, a GPS jammer disrupted the installation and operation of communications equipment in Newark Airport (New York, US). GPS jammers are considered illegal but can easily be purchased online, and have the ability to disrupt GPS receivers and other telecommunications equipment nearby.

Example: Accidental jamming of Newark Airport as reported by CBS New York: http://newyork.cbslocal.com/2013/08/09/n-j-man-in-a-jam-after-illegal-gps-device-interferes-with-newark-liberty-operations/

3.8.1.1 Resources to commit the attack

Attacker: Accidental.

- Resources to commit the attack: LOW. Jamming equipment is necessary to perform a disruption. Such equipment (e.g. GPS Jammers) is already illegal in many EU member states although it can be purchased online.
- Knowledge of attacker(s): LOW. Some basic knowledge is necessary to setup jamming equipment, although specialized skill is not required.
- Source sectors:
  - Com – Denotes a commercial source.
  - User – Denotes an individual user
- Type of attack:
  - Clumsy behaviour
- Fundamental motivation of attack:
  - Unintentional
- Target:
  - Industry
  - Government / national
  - Military
  - Private
  - Others

3.8.2 POTENTIAL ATTACK IN THE FUTURE: INTENTIONAL ELECTROMAGNETIC INTERFERENCE ATTACKS

In 1999, URSI Commission E defined criminal activities based on the use of electromagnetic tools [URSI] as the:

"intentional malicious generation of electromagnetic *energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes".*

In order to differentiate such actions from accidental interference, the term "Intentional Electromagnetic Interference" (IEMI) was proposed. In [Sabath, 2011] presents cases of IEMI attacks along with the motivations and technical skills of the offenders. Although examples of such attacks already exist, there has not been extensive work on risk analysis, detection and

mitigation measures, especially in terms of safeguarding Critical Infrastructures from such attacks. Therefore, this case can be generalized to include multiple sectors and not just Transport.

3.8.2.1 Resources to commit the attack

Attacker: Organized group, Espionage group, Insider, Terrorist, Criminals.

- Resources to commit the attack: MEDIUM. Electronic equipment needs to be used as an IEMI source.
- Knowledge of attacker(s): LOW - HIGH. From Low to High: Some technical knowledge is required to handle the IEMI equipment although very specialized knowledge is not necessary. Future and more complex scenarios might require higher level of knowledge.
- Source sectors:
  - Com – Denotes a commercial source.
  - User – Denotes an individual user
- Type of attack:
  - Exploit
  - Physical damaging
  - Others: Attackers exploit the inherent weakness of electronic systems to withstand electromagnetic interference. For higher (transmission) power IEMI can disrupt electronics or damage them completely.
- Fundamental motivation of attack:
  - Financial drivers
  - Governmental reasons
  - Vengeance
  - Unintentional
- Target:
  - Industry
  - Finance
  - Government / national
  - Military
  - Private
  - Others - Any electronic equipment can be targeted.

3.9 ATTACKS TO VIRTUALIZATION TECHNOLOGIES

3.9.1 PROFILING A REPORTED ATTACK: HYPERJACKING [CAPEC]

Hyperjacking is a term used to refer to the hypervisor stack jacking, an attack that targets virtual environments. In a virtual environment, the hypervisor is the software that creates and runs virtual machines. If an attacker manages to take control over the hypervisor, he can control everything running on the machine to carry out dangerous actions like stealing sensitive information, attack guest VMs but also installing back doors for maintaining the access to the hypervisor. Regular security measures are ineffective because the OS will not even be aware that the machine has been compromised.

For a Hyperjacking attack to be successful, an attacker would need a processor capable of doing hardware-assisted virtualization, something that is still rare nowadays. For this reason, the risk of being victim of such an attack are still currently low. However, Hyperjacking is considered a real-world threat, and administrators should take this into account. In addition, [King and Chen, 2006] created VMBR (Virtual Machine Based Root kit), a proof-of-concept to show the feasibility of a Hyperjacking attack and how it can be used to spread malicious services that corrupt the virtual environment.

3.9.1.1 Resources to commit the attack

Attacker: Espionage group, Spyware/malware attacker.

- Resources to commit the attack: MEDIUM. Hyperjackings are rare due to the difficulty of directly accessing hypervisors, so most of the effort might go in that direction (e.g. corrupting an administrator).
- Knowledge of attacker(s): MEDIUM. The most difficult part of the attack would be to gain access to the hypervisor (e.g. by corrupting an insider or by installing initial malware). Once access has been gained misusing the system by installing malicious services or stealing data does not require very high skills.
- Source sectors:
    - Com – Denotes a commercial source.
    - Gov – Denotes local or national government
- Type of attack:
    - Spyware
    - Malware
    - Backdoor
    - Insider attacks
- Fundamental motivation of attack:
    - Financial drivers
- Target:
    - Industry
    - Finance
    - Government / national

3.9.2 POTENTIAL ATTACK IN THE FUTURE: VM-SPECIFIC MALWARE

Virtualization is set to become more and more popular. Today, most of the Fortune 500 companies use some sort of virtualization. The efficient usage of resources guaranteed by virtualization will make possible that an increasing number of industries will rely on it to provide their services. In healthcare industry, where there is abundancy of legacy systems, the adoption of virtualization might be a game changer. However, because the healthcare industry deals with extremely sensitive information it can easily become a target of cyber criminals, hence there are some concerns about the security of virtual environments.

A possible way for cyber criminals to attack virtual environment is the creation of specific malware able to infect a virtual machine (VM). Typically, can be configured by acting on the image file with no need of rebooting the system. These characteristics (that enhance flexibility) can be exploited by malware to install spyware that can record and collect all the action taking place while the VM is running. In case of a VM dealing with sensitive data such as in healthcare, this attack might lead to costly data breaches.

3.9.2.1 Resources to commit the attack

Attacker: Espionage group, Spyware/malware attacker.

- Resources to commit the attack: HIGH.
- Knowledge of attacker(s): HIGH.
- Source sectors:
  - Com – Denotes a commercial source.
  - Gov – Denotes local or national government
  - User – Denotes an individual user
- Type of attack:
  - Spyware
  - Malware
- Fundamental motivation of attack:
  - Financial drivers
  - Governmental reasons
  - Reputation
- Target:
  - Industry
  - Finance
  - Government / national

3.10 ATTACKS TO CLOUD COMPUTING

3.10.1 PROFILING A REPORTED ATTACK: CLOUD LEAK

On August the 31st in 2014, a voluminous amount of private information (commonly images) of various celebrities, mostly women, were leaked from iCloud and later disseminated on the web by a viral re-posting and diffusion. Apple later confirmed that the hackers responsible for the leak obtained the images by compromising the cloud service through phishing and brute force techniques guessing iCloud usernames and passwords. Some further investigation revealed that a piece of computer code that repeatedly guesses passwords has been found online. Also a piece of software called iBrute has been linked to the alleged attack because of its ability to exploit a vulnerability in Apple's Find My iPhone service. Apple had no limit on the number of password guesses, which allowed the malicious script to make multiple attempts at a fast rate until the correct password was identified. Actually the flaw has been patched by a 5-attempt limit. On September 2, 2014, Apple reported that the leaked images were the result of compromised accounts, using a very targeted attack on user names, passwords and security questions.

3.10.1.1 Resources to commit the attack

Attacker: Blackmailer. The chief hacker who organized the theft of private information is referred as 'original guy' by other but it seems that the hacking was a conspiracy involving more than just one individual and 'the result of several months of long and hard work'.

Gawker, the anonymous hacker said that “original guy” asked for bitcoin (BTC) donations from those willing to pay to see.

- Resources to commit the attack: HIGH. There is still no concrete evidence that the images were stolen from iCloud and some commentators and investigators evidences sustain the theory of multiple breaches that may have been used to access the photographs from the mobile phones of celebrities. It seems that the leaked celebrity images weren't the result of a single hack but were instead hoarded over a period of months by one well-connected figure in underworld specialized forums.
- Knowledge of attacker(s): HIGH. Even if the kwowledge of attacker’s seems to be high in order to execute this leakage, nowadays some on line resources are available to facilitate similar leakages. In fact, The /stol/ board on AnonIB (short for "Stolen" or "Obtained Photos") serves as a global meeting hub for iCloud hackers. Using specialist password-cracking tools and guessing targets' security questions through Apple's iForgot password reset form, AnonIB hackers are consistently able to gain access to iCloud accounts with only an email address. Once inside, the hackers get to work to extract photographs as quickly as possible, using file-retrieval software to download photo backups.
- Source sectors:
  - User – Denotes an individual user
- Type of attack:
  - Phishing scheme
  - Brute force
- Fundamental motivation of attack:

- Financial drivers
- Target:
  - Private

3.10.2 POTENTIAL ATTACK IN THE FUTURE: SMART CLOUD ATTACK

A Cloud is a pool of hardware (e.g. network, storage etc) and software resources (e.g.: applications). Resources are virtualized and automated so that they can be easily accessible to use on line services. Cloud services are shared by multitenant using internet channel which is a vulnerable to attacks. Each of the multiple resources can be a target of an attach, both singularly and all together. Whatever the type of service is available and accessible from the cloud (space allocation memory, remote services, applications) an hypothetical scenario may consider a combination of techniques that use an initial phishing attack (retrieving personal information from unsuspecting user through sending emails, webpage linker and instant message to acquire passwords) or Audio Steganography Attack (embedding malware within an audio files to execute it during file listing from the user) oriented to inoculate malware in a wide number of devices (pc, firewall, router, IOT devices) so that all together may act as a botnet. When a botnet attack (stepping stone attach) is executed, attackers intrudes in to target victims host, by a series of other hosts (called stepping stone) and at the appropriate time (the final phase of the attack) the DDOS attack is accomplished. At this final phase of the scenario, each botnet device begins to request for resources until the cloud servers are overloaded and their performances begin to decrease progressively, until all the infrastructure is so full of request that no more requests are manageable and accepted. Users at that time won't obtain any service from the cloud infrastructure that appear in a "denial of services" state. If a cloud infrastructure was public or if it was directed to deliver public services, then the cloud infrastructure would be considered as critical infrastructures and the disruption of services would cause serious harm to the public life of the users themselves, especially in the case of healthcare services. (gov, millitary targets). This final motivation is suitable in case of terroristic attack.

An eventual cybercrime scenario motivation can be considered if a request of money is claimed to solve the "denial of service" and return to normal performance activity. (finance, industry targets)

Another attack scenario that can appear more traditional, passes through network attack strategies but can be oriented to harass three layers of cloud. A web browser attacks can be used to exploit the authentication, authorization, and accounting vulnerabilities of cloud systems. Malicious programs (e.g.virus and Trojan) can be uploaded to cloud systems and can cause damage. Malicious operations (e.g. metadata spoofing attacks)can be embedded in a normal command, passed to clouds, and executed as valid instances. In IaaS, the hypervisor(e.g. VMware vSphere and Xen) conducting administrative operations of virtual instances can be compromised by zero day attack. Again the final user may experiment services not accessible or various miswoking.

3.10.2.1 Resources to commit the attack

Attacker: Organized group, Terrorist.

If a cloud infrastructure was public or if it was directed to deliver public services, then the cloud infrastructure would be considered as critical infrastructures and the disruption of services would cause serious harm to the public life of the users themselves, especially in the case of healthcare services. This final motivation is suitable in case of terroristic attack.

An eventual cybercrime scenario motivation can be considered if a request of money is claimed to solve the "denial of service" and return to normal performance activity. Attacker in this second case can be an organized group linked to organized crime.

- Resources to commit the attack: HIGH. Hackers could rent the virtual machines, analyze their configurations, find their vulnerabilities, and attack other customers 'virtual machines within the same cloud. IaaS also enables hackers to perform attacks, e.g. brute-forcing cracking, that need high computing power. Since IaaS supports multiple virtual machines, it provides an ideal platform for hackers to launch attacks (e.g. distributed denial of service (DDoS)attacks) that require a large number of attacking instances.
- Knowledge of attacker(s): HIGH. Hackers need to know each of the attack techniques previously described but also they may know traditional network attack strategies. Cloud computing do not differ from other hardware and software resources in technological terms, but heavily differ for the dimension of the enabling infrastructure. Therefore whatever is the motivation hacker need to know, understand and be able to execute attack on a large scale of resources otherwise the impact of the attack would be negligible.
- Source sectors:
    - Com – Denotes a commercial source.
    - Gov – Denotes local or national government
    - User – Denotes an individual user
- Type of attack:
    - Phishing scheme
    - DDOS
    - Network attack
- Fundamental motivation of attack:
    - Financial drivers
- Target:
    - Industry
    - Finance
    - Government / national
    - Military

3.11 ATTACKS TO SMART GRIDS

3.11.1 PROFILING A REPORTED ATTACK: BLACKOUT IN NEW YORK

As a large system of distributed and interconnected systems, the smart grid offers an exceptionally large attack surface. The smart grid cyber security challenge is about protecting the ever-growing number of smart grid assets and their communication channels from fast-growing and continuously evolving cyber threats. The most important accidental attack to Smart Grid happened in August 2003:

"*… on Aug. 14, 2003, the electricity grid in the U.S. Northeast was stressed close to the limit. This wasn't unusual; summer is a period of high demand in the Northeast, as air conditioners run overtime to compensate for the heat, and a number of older power plants were already offline for maintenance. As power lines became overloaded, they began sagging because of the high temperatures, until one line south of Cleveland touched an overgrown tree limb and short-circuited. What followed was a cascade of disaster due to a mix of human error and equipment failure, until by 4:10 p.m. E.T. that day more than 50 million people had lost power in parts of Ontario and eight U.S. states. New York City looked like this, and power wasn't fully restored for two days. At the time it was the second most widespread power blackout in history, after a 1999 disaster in Brazil.*" [Walsh, 2013]

3.11.1.1 *Resources to commit the attack*

Attacker: Accidental.

- Resources to commit the attack: LOW. In reality the attack is due to an overloaded in the electricity grid.
- Knowledge of attacker(s): LOW. In fact the attack could be producedd by coordination of activist in order to draw the attention about global warming.
- Source sectors:
  - User – Denotes an individual user
- Type of attack:
  - Denial of Service
- Fundamental motivation of attack:
  - Unintentional
- Target:
  - Industry
  - Finance

3.11.2 POTENTIAL ATTACK IN THE FUTURE: BURGLING HOMES BY MEANS OF SMART METERS

In near future the smart meters will be in every home, sending data that contains information on our requirements, habits, timetables, etc. A malicious manufacturer of smart meters intentionally implements the electronic devices with vulnerability. The vulnerability is exploited for criminals groups to monitor people with high standard of living in order to gain access to their properties when they are on holidays.

3.11.2.1 Resources to commit the attack

Attacker: Organized group, Espionage group, Criminal.

- Resources to commit the attack: LOW. The vulnerability is exploited using Bluetooth communication, the criminals just visit the victims properties regularly to collect information stored locally in the smart meters. The device to extract the information is a standard smartphone with a malicious component to exploit the vulnerability in smart meter.
- Knowledge of attacker(s): LOW. The attacker knows perfectly how to stimulate the smart meter in order to extract information. The code and the app to install in the smartphone are available in the *deep web*.
- Source sectors:
  - Com – Denotes a commercial source.
- Type of attack:
  - Phishing scheme
  - Malware
  - Exploit
  - Backdoor
  - Spyware
  - Social engineering
- Fundamental motivation of attack:
  - Financial drivers
  - Vengeance
  - Stalking
- Target:
  - Industry
  - Finance

3.12 ATTACKS TO SMART CITIES

3.12.1 PROFILING A REPORTED ATTACK: SPYING ON CITIZENS USING HOME/BUILDING AUTOMATION SYSTEMS

In many smart cities approaches and models, the automation of apartment buildings is a vital part: This not only includes central heat and energy management, but issues like building security, safety in case of threats (e.g. fire), central control over building access, waste management down to usage optimization like it is done in elevators.

While these systems might be uncritical and not used for actual control over the resources, but just for monitoring usage and condition, this information could be used to gather intelligence on the individuals and families living in these houses. While related issues have been discussed in the political arena regarding the (further) development of smart grids with smart meters, discussing the issue of loss of user privacy and the resulting attack vectors through criminals, home automation systems and the resulting, even more detailed, information on citizen behavior has been neglected throughout most of the literature. Still, as is discussed in [1], in case of adding security (e.g. access) features to a home automation system, the security of this system itself gains importance.

Weaknesses in smart building concepts cannot only be used for gaining access, information on the end user can help single out interesting targets and gain intelligence on their availability, their day plans and so forth, making the planning of burglaries far more simple and riskless. Unfortunately, privacy has been neglected in the home automation concepts [Brush et al., 2011] [Kaur, 2010] in many commercial systems.

3.12.1.1 *Resources to commit the attack*

Attacker: Espionage group, criminal.

- Resources to commit the attack: HIGH. Depending on the actual system implemented, some possess security features; some require only physical access to the bus which is rather simple in large buildings.
- Knowledge of attacker(s): HIGH. Typically knowledge of the system, which can be derived easily from the Internet. Some systems have security measures in place that need to be circumvented.
- Source sectors:
  - User – Denotes an individual user
- Type of attack:
  - Spyware
- Fundamental motivation of attack:
  - Financial drivers
- Target:
  - Industry
  - Private

3.12.2 Potential Attack In the Future: Disruption and causing of accidents through controlling traffic lights and systems

One vital part of the smart city concept is constituted by intelligent traffic control systems, especially the dynamic optimization of traffic flow. One vital aspect of the latter lies in the control of traffic lights that are centrally controlled in a smart city to be able to be easily adapted to changes in traffic volume, as well as other related side parameters like construction sites, accidents or simply optimizations on other parts of the road/rail system that propagate throughout the system through dependencies. One main interest of a terrorist attacker here does not lie in disturbing the traffic making it less efficient, but especially in provoking accidents: Setting traffic lights from two exclusive traffic lights to green, especially considering streets with higher speed levels or intersections with urban train systems. With 25.700 road deaths [EUCommission, 2015], even a low percent increase would cause a serious impact, still, we estimate that even in case of no accidents the inconvenience cause together with the demonstration of power over a field that directly relates to normal citizens lives would result in serious impact on political decisions, thus catering for terrorist needs (relating to the fact that terrorist do not need to target human casualties as their target, but often want to achieve political effects). Related to this is the topic of gaining control on other traffic-related systems like tunnel lights. But even when not considering the topic of provoking accidents, control over the traffic system could result in serious financial damage, since many modern countries would have to step back to regulating the traffic lights by hand, thus resulting in high costs, not including the damage caused by jamming the traffic of a city through rush hour (the effects of unreliable traffic control on behavior have been studied in [Kantowitz, 1997]).

3.12.2.1 Resources to commit the attack

Attacker: Organized group, Espionage group, Insider, Terrorist.

- Resources to commit the attack: MEDIUM. Knowledge and interface to traffic control system. Low resources in case of having an insider.
- Knowledge of attacker(s): From HIGH to Low. The specifications are typically easy to get depending on the product and the vendor, access to the system depends on this too. High complexity in case the attacker needs to get control over the central system.
- Source sectors:
  - Com – Denotes a commercial source.
  - User – Denotes an individual user (lowers the bar)
- Type of attack:
  - Misinformation
  - Physical damaging
- Fundamental motivation of attack:
  - Governmental reasons
  - Vengeance
  - Unintentional
- Target:
  - Industry
  - Government / national
  - Private

3.13 ATTACKS TO SMART BORDERS

3.13.1 PROFILING A REPORTED ATTACK: SHARING TOO MUCH INFORMATION

Nowadays, it is very common to find on the Internet personal information that should not be shared. An excellent example of an attack to smart borders is related to the problem of sharing too much information through social networks.

Due to the excitement of travelling abroad, some people share photographs of their boarding pass. At first sight, it should not pose a problem. However, the boarding pass contains personal information and some data that allows changing data of the booking.

As a result, an attacker retrieved personal information from the shared photograph of the boarding pass uploaded to a known social network. Making use of this information, the attacker changed the flight and even personal information of the traveller. After that, the attacker travelled without problems and the victim could not do anything but regreting not having uploaded the photograph.

Impersonation was possible due to the lack of awareness and the relaxed control of changes on the information of the booking.

3.13.1.1 *Resources to commit the attack*

Attacker: Organized group, Espionage group, Terrorist.

- Resources to commit the attack: LOW. Once the personal information is shared, the attacker could retrieve it and use it for personal interests.
- Knowledge of attacker(s): LOW. In order to complete the attack it is only necessary to retrieve the information and to access into the system to modify the information related to the traveller.
- Source sectors:
  - User – Denotes an individual user
  - Others – Military, Activists, Criminal Organizations, Terrorists, etc.
- Type of attack:
  - Social engineering
  - Clumsy behavior
  - Misinformation
- Fundamental motivation of attack:
  - Vengeance
  - Stalking
  - Verification of systems to improve them
- Target:
  - Private

3.13.2 POTENTIAL ATTACK IN THE FUTURE: INSUFFICIENT BORDER CONTROL

Even though border control measures have considerably improved in the last years, some potential attacks are still possible.

Given that some border controls are based only on the traveler identification through official documents, attackers could use fake passports to cross the border. In contrast, a second

authentication factor like biometric controls is used for some border controls. Using a second authentication factor in border controls reduces the success rate of such attacks.

Attacks are becoming more sophisticated and effective, that is why some biometric controls have been already bypassed. It might be an insufficient border control.

3.13.2.1 Resources to commit the attack

Attacker: Organized group, Espionage group, Terrorist, Activist.

- Resources to commit the attack: HIGH. Given that the border control is a physical control, the attacker must build a system to bypass the control.
- Knowledge of attacker(s): HIGH. Attackers must know how the border control works to try to bypass it.
- Source sectors:
  - User – Denotes an individual user
  - Others – Military, Activists, Criminal Organizations, Terrorists, etc.
- Type of attack:
  - Social engineering
  - Misinformation
- Fundamental motivation of attack:
  - Financial drivers
  - Verification of systems to improve them
  - Others - Espionage, Cybercrime, Terrorism, etc
- Target:
  - Industry
  - Military
  - Private

3.14 ATTACKS TO BRING YOUR OWN DEVICE

3.14.1 PROFILING A REPORTED ATTACK: EMPLOYEE-OWNED MOBILE DEVICES

In May 2014 the insurance company Aviva was attacked with the employee-owned mobile devices (in particular iPhones) as the main target [THEREGISTER]. The attacker was compromising Aviva's third party contractor MobileIron that was providing a BYOD service to manage over thousand Apple-based devices such as iPhones and iPads that were given to the employees on behold of Aviva. After the attacker compromised MobileIron's administration server, he was able to take full control of every single iPhone that was part of Aviva's BYOD fleet. In turn, the attacker wiped the contents of the entirety of the mobile devices causing a millions in damages.

3.14.1.1 *Resources to commit the attack*

Attacker: Activist.

- Resources to commit the attack: MEDIUM. The actual infiltration of MobileIron's admin server was based on the Heartbleed bug that was disclosed publicly some month before the attack happened. To that time public tools to perform perimeter scans and thus could indicate a potential vulnerability were publicly available. Furthermore, public exploits for the Heartbleed bug were available as well. The actual attack of the BYOD devices was possible since they were under control of MobileIron's remote administration tools and services.
- Knowledge of attacker(s): MEDIUM. The attacker must have been able to understand the basics of the Heartbleed attack as at the time of the attack there were public exploits available that would automatically mount attacks based on the Heartbleed vulnerability.
- Source sectors:
  - User – Denotes an individual user
- Type of attack:
  - Exploit
- Fundamental motivation of attack:
  - Financial drivers
  - Reputation
  - Others
- Target:
  - Industry
  - Finance

3.14.2 POTENTIAL ATTACK IN THE FUTURE: BYOD ATTACK VECTOR

Mobile devices will become an increasingly important building stone in the future way that employees will interact and share information amongst each other as well as with other departments of the company. Already there is the trend that employees are working more often either from home office or while there are away on business. This way of working requires for mobile devices. Furthermore, by equipping employees with mobile devices the

employer is able to create a communication channel that is available even if the employee is not physical present at the company.

Thus, the BYOD trend could be exploited by attackers in various ways. The initial attack vector might by i) a phishing attack that lures the victim into downloading malware (camouflaged as a genuine mobile application or update package) ii) some vulnerability in a installed software component or iii) a drive-by download exploiting vulnerabilities of the in-built browser or its media components (such as the flash player etc.). Once the device is brought to the company and connects to the internal network, the malware could start to retrieve information by scanning the infrastructure, running services, installed applications or gathering login credentials by launching MITM attacks. To get a broader view upon the network, the malware could use Bluetooth or NFC to scan for nearby devices to further spread. Once the malware has identified valuable targets and critical parts of the infrastructure it might load applicable exploits and launch targeted attacks against the services to obtain complete control of admin servers and such a like.

3.14.2.1 Resources to commit the attack

Attacker: Organized group, Espionage group, Insider, Phisher, Terrorist, Activist.

- Resources to commit the attack: HIGH. Depending upon the infrastructure of the company and the level of stealthiness that should be kept throughout the attack, the attackers must have very good knowledge on how to create mobile malware that is able to spread using different communications protocols (Bluetooth, ZigBee, NFC). Furthermore, the malware must be designed in such a way that it can perform various tasks including reconnaissance, worm-like behavior to further spread, downloading of 2nd stage payload and performing further attacks on identified targets. This asks for a well-written malware.
- Knowledge of attacker(s): HIGH. As mentioned already, the attackers must be very skillful in terms of creating malware and furthermore they must have detailed information about employees or the infrastructure to perform the initial attack that would infect the first mobile device.
- Source sectors:
    - Com – Denotes a commercial source.
    - Gov – Denotes local or national government
- Type of attack:
    - Phishing scheme
    - Malware
    - Exploit
    - Backdoor
    - Social engineering
    - Insider attacks
- Fundamental motivation of attack:
    - Financial drivers
    - Governmental reasons
    - Vengeance
    - Reputation

- Target:
    - Industry
    - Finance
    - Government / national
    - Military

3.15 ATTACKS TO TELECOMMUNICATION SERVICES

3.15.1 PROFILING A REPORTED ATTACK: BYPASS ENCRYPTION OF MOBILE DEVICE COMMUNICATION

In summer 2012 an attack dubbed 'Operation Socialist' was identified against the Belgium Telecom provider Belgacom. The attack was conducted with a highly-advanced malware identified as Regin, which is suspected to be developed by government-sponsored intel agencies. The attack was launched in phases between 2010 and 2011. It is believed to be perpetrated by the GHCQ. The goal was to bypass encryption of mobile device communication by extracting roaming data before it is getting encrypted in the first place. Furthermore the idea was to conduct a man-in-the-middle attack on mobile devices. The attack was conducted using a technique dubbed "Quantum Insert" where profile pages of the victims (in particular members of the Belgacom with broad access to internal systems) were modified such that they would redirect to malicious website that would download and execute the Regin malware [THEINTERCEPT] [SPIEGEL].

3.15.1.1 Resources to commit the attack

Attacker: Organized group.

- Resources to commit the attack: VERY HIGH. The Regin malware is a state-sponsored malware that was potentially developed by several intel agencies such as the NSA as well as the GHCQ. Furthermore the attack was planned over a long time and in great detail and was conducted in several phases spanning several years. The attack required good knowledge about personal details of the attacked victims as well as the information about the internal network of Belgacom. Furthermore, to be stealthy and provide long-term access the attackers launched an APT using one of the most advances cyberweapons (Regin) known so far.
- Knowledge of attacker(s): VERY HIGH. Published information about the incident show that Britain's GHCQ is the main force behind the attack. Without any doubt the skills of the attackers can be regarded as very high.
- Source sectors:
  - Com – Denotes a commercial source.
  - Gov – Denotes local or national government
- Type of attack:
  - Malware
  - Backdoor
  - Social engineering
- Fundamental motivation of attack:
  - Governmental reasons
- Target:
  - Industry
  - Government / national

3.15.2 POTENTIAL ATTACK IN THE FUTURE: MOBILE ATTACK OF NGN-BASED TELCO SYSTEMS

In the future critical components of the PSTN network will be increasingly merged with the packet-based Next Generation Network (NGN). Thus, software will replace the role of traditional telco operators to administer main components of the network. However, this

exposes interfaces to the user that were previously shielded by the operator. With this increasing trend consider the following scenario.

A state-sponsored attacking group explores vulnerability in an IP-based service that directly interfaces a critical component or functionality of the network of the Telco provider. The attacker is able to exploit this vulnerability remotely without the requirement for a social-engineering or physical attack. In order to cover his tracks, the attacker launched his attack by accessing a hardly documented switch that is located at an abandoned underground place beneath the city. Using his smartphone the attacker can interface the switch and implant a malware. Given the fact that the overall network is using heterogeneous hardware, protocols and interfaces at some points the monitoring of the security of the system is insufficient such that the attack can be mounted to be an APT. Thus, the existence of malware spreading through the network is only detected years after the initial attack. During this time the attacker is able to extract any message operated by the Telco provider in plain text as he is able to access the messages before they are being encrypted.

3.15.2.1 Resources to commit the attack

Attacker: Organized group, Espionage group, Insider, Terrorist.

- Resources to commit the attack: MEDIUM. Once a vulnerability of the Telco's system is identified, conducting the actual attack is within the means of advanced adversaries.
- Knowledge of attacker(s): HIGH. The attacker must have a thorough understanding of the internals of the Telco system as well as potential vulnerabilities existent in the internal protocols or applications. However, given the fact that the Telco uses IP-based protocols as well, the attacker might apply a generic vulnerability of IP to the Telco network.
- Source sectors:
  - Gov – Denotes local or national government
- Type of attack:
  - Malware
  - Exploit
  - Backdoor
  - Insider attacks
- Fundamental motivation of attack:
  - Governmental reasons
- Target:
  - Industry
  - Government / national

4 CONCLUSIONS

This section ends the document by summarizing the main identified trends related to Cyber-Criminals and Cyber-Attackers profiles.

In section 3 all the scenarios have been profiled based on a reported attack in present or past and another effort has been made to profile a potential attack in the future. Many of these profiles reveal common patterns, below some of the main features of the attacks are summarized in two aspects:

4.1.1 THE MAIN ATTACK CHANNEL: INTERCONECTEDNESS

Smart devices, wearables, smart TVs, are, by and large, present in many of the profiled attacks. Firstly, the more emerging the technology is, the more exposed are their users. That is due to the rapid evolution of the needs claimed by the users, this fast movement push the IT companies to develop the product without any concern of security aspects.

Secondly, many of the scenarios traditionally isolated, are now opening some new communication means in order to manage some features remotely. This is especially trending for small Critical Infrastructures such as, water treatment systems, local electricity facilities, etc. In this process the Internet of Things is playing a key role. The decision maker should take actions to protect these devices (smartphones, wearables, etc.) against current and future threats.

4.1.2 PEOPLE ARE THE "WEAK LINK": UNWISE IMPLEMENTATIONS, WEAK CONFIGURTAITONS, ETC.

For an effective implementation of cyber security, the organizations must have qualified personnel as well as have the capability to test and experiment with new technology before going into production environment.

Traditional cybersecurity training platforms, such as those supporting individual computer-based training or e-learning, have long been the only way to implement training programmes in cybersecurity. More recently, the introduction of cyber ranges has redefined how cybersecurity training is to be approached. A cyber range is a virtual environment typically built on top of standard hardware that is used for hands-on training, experimentation, test and research in cybersecurity, and that is intended to support multitenant activities. Cyber range solutions are gaining attention as a key ally to support cost-effective training programs in different civil and military contexts. Actually, during the last few years a number of cyber ranges for cybersecurity training have been developed, both from the academy and the industry, as a response to meet the market demand.

However, the results to date show that current cyber ranges still present limitations that leave most challenges unanswered. Consequently, there is still an urgent need for innovating new approaches that solve the open problems.

BBC, 'The Internet Is the New Frontline as UK Sets up Army Cyber-Unit' (*BBC*, 2015) <http://www.bbc.co.uk/newsbeat/article/31074227/the-internet-is-the-new-frontline-as-uk-sets-up-army-cyber-unit> accessed 30 November 2015

Blackmore SJ, *The Meme Machine* (Oxford University Press 1999)

Brownlee L, 'China-Based Cyber Attacks on US Military Are "Advanced, Persistent and Ongoing": Report' *Forbes* (17 September 2015) <http://www.forbes.com/sites/lisabrownlee/2015/09/17/chinese-cyber-attacks-on-us-military-interests-confirmed-as-advanced-persistent-and-ongoing> accessed 30 November 2015

Brush AJB and others, 'Home Automation in the Wild' [2011] Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11

CAPEC, 'Â Information Elicitation via Social Engineering Definition in a New Window' (*Capec-410*) <https://capec.mitre.org/data/definitions/410.html> accessed 1 December 2015

Cycon, 'CyCon2013' <https://ccdcoe.org/publications/2013proceedings/CyCon_2013_Proceedings.pdf> accessed 1 December 2015

'European Commission - PRESS RELEASES - Press Release - How Safe Are Your Roads? Commission Road Safety Statistics Show Small Improvement for 2014' (24 March 2015) <http://europa.eu/rapid/press-release_IP-15-4656_en.htm> accessed 4 December 2015

Europol, 'Cyber Bits - Hackers Deployed to Facilitate Drugs Smuggling' (*Europol*, 30 June 2013) <https://www.europol.europa.eu/content/cyber-bits-hackers-deployed-facilitate-drugs-smuggling> accessed 30 November 2015

Farwell JP and Rohozinski R, 'Stuxnet and the Future of Cyber War' (2011) 53 Survival 23

Globalsecuritymag, 'Drones Could Be the next Cyber Threat' (*globalsecuritymag*) <https://www.globalsecuritymag.fr/Drones-could-be-the-next-cyber,20150423,52486.html> accessed 2 December 2015

Huber M and others, 'Towards Automating Social Engineering Using Social Networking Sites' [2009] 2009 International Conference on Computational Science and Engineering

Kantowitz BH, Hanowski RJ and Kantowitz SC, 'Driver Acceptance of Unreliable Traffic Information in Familiar and Unfamiliar Settings' (1997) 39 Human Factors: The Journal of the Human Factors and Ergonomics Society 164

Kaur I, 'Microcontroller Based Home Automation System with Security' (2010) 1 International Journal of Advanced Computer Science and Applications

King ST and Chen PM, 'SubVirt: Implementing Malware with Virtual Machines' [2006] 2006 IEEE Symposium on Security and Privacy (S&P'06)

Miller B and Rowe D, 'A Survey SCADA of and Critical Infrastructure Incidents' [2012] Proceedings of the 1st Annual conference on Research in information technology - RIIT '12

ONLINE S and Hamburg, 'Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm - SPIEGEL ONLINE' (20 September 2013) <http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html> accessed 2 December 2015

PricewaterhouseCoopers, 'Transportation & Logistics 2030, Volume 4: Securing the Supply Chain' (*PricewaterhouseCoopers (PwC)*, 2014) <http://www.pwc.com/gx/en/industries/transportation-logistics/publications/security-transport-systems.html> accessed 30 November 2015

'Robin Sage', , *Wikipedia* (Wikimedia Foundation 2015) <https://en.wikipedia.org/wiki/Robin_Sage> accessed 1 December 2015

Sabath F, 'What Can Be Learned from Documented Intentional Electromagnetic Interference (IEMI) Attacks?' [2011] 2011 XXXth URSI General Assembly and Scientific Symposium

'Security Guidance for Early Adopters of the Internet of Things (IoT) Mobile Working Group Peer Reviewed Document' (2015) <https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf> accessed 2 December 2015

'The inside Story of How British Spies Hacked Belgium's Largest Telco' (15 October 2015) <https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/> accessed 2 December 2015

True D, 'Disciplining Drone Strikes' [2014] Transforming Conflict, Law, and Policy 285

'US Army Cyber Command' (*ArcCyber*) <http://www.arcyber.army.mil/index.html> accessed 30 November 2015

Wagstaff J, 'All at Sea: Global Shipping Fleet Exposed to Hacking Threat' (*Reuters*, 2015) <http://www.reuters.com/article/2014/04/24/us-cybersecurity-shipping-idUSBREA3M20820140424> accessed 30 November 2015

Walsh B, '10 Years after the Great Blackout, the Grid Is Stronger — but Vulnerable to Extreme Weather | TIME.com' (13 August 2013) <http://science.time.com/2013/08/13/ten-years-after-the-great-blackout-the-grid-is-stronger-but-vulnerable-to-extreme-weather/> accessed 3 December 2015

'Winning Strategies: Software Development for the Internet of Things' (9 October 2012) <http://insights.wired.com/profiles/blogs/winning-strategies-software-development-for-the-internet-of> accessed 2 December 2015

'Http://resources.infosecinstitute.com/future-Now-Car-Hacking/' <http://mcaf.ee/u4bl3y> accessed 2 December 2015

'Http://www.intel.com/content/www/us/en/automotive/automotive-Overview.html' <http://mcaf.ee/n5zq32> accessed 2 December 2015

'Http://www.zdnet.com/article/europol-Warns-of-Iot-Murder-and-Ransomware-for-Smart-Cars/' <http://mcaf.ee/1ujwbr> accessed 2 December 2015

'http://thehackernews.com/2014/02/hacking-Car-Remotely-with-20-Iphone.html' <http://mcaf.ee/szwdxg> accessed 2 December 2015

'http://thehackernews.com/2014/03/tesla-Cars-Can-Be-Hacked-to-Locate-And.html' <http://mcaf.ee/m8d6ic> accessed 2 December 2015

'http://thehackernews.com/2015/07/smart-City-Cyber-Attack.html' <http://mcaf.ee/06h293> accessed 2 December 2015

'http://thehackernews.com/2015/08/ransomware-Android-Smartwatch.html' <http://mcaf.ee/huewdm> accessed 2 December 2015

'http://www.wired.com/2015/07/hackers-Remotely-Kill-Jeep-Highway/' <http://mcaf.ee/oly3rw> accessed 2 December 2015

'https://thestack.com/security/2015/11/19/how-Susceptible-Are-Modern-Cars-to-Hacking/' <http://mcaf.ee/xgsnoj> accessed 2 December 2015

De Medici M, 'L'ambiguo Futuro Dei Droni Fra Uso Militare E Sviluppo Civile' (25 November 2013) <http://www.artapartofculture.net/2013/11/25/lambiguo-futuro-dei-droni-fra-uso-militare-e-sviluppo-civile> accessed 2 December 2015

staff GW, 'Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle' (1 August 2012) <http://gpsworld.com/drone-hack> accessed 1 December 2015

'"Heartbleed-Based BYOD Hack" Pwns Insurance Giant Aviva's iPhones' <http://www.theregister.co.uk/2014/06/23/aviva_heartbleed_hack/> accessed 2 December 2015

- End of Document -