With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

Development of the Cybercrime and Cyberterrorism Research Roadmap

Why Cyber Security Research Matters

Cyber criminal activities are reported to be continuously growing and are negatively impacting the development of the European society and economy, and are pervasively affecting all the aspects of our daily lifes. Even though the level of awareness of cyber threats has increased, and Law Enforcement acts globally to fight against them, illegal profits have reached unsustainable figures. In addition to the economic reasons, however, cyber crime often hides other political and social motivations.

What is CyberROAD?

CyberROAD is a 24-month research project funded by the European Commission under the Seventh Framework Programme (with a total budget of 1.300.000 €).
In order to help coordinate the European efforts in the fight against cyber crime and cyber terrorism, **the CyberROAD project has identified 19 research topics** on which Europe should concentrate resources to increase its security and resilience, **organizing them in strategic roadmap** for Cyber Security Research.
In the next pages a **short selection of these research topics** and of their related current threaths and defences is briefly presented.

This handbook focuses on four very common aspects of our daily "digital" life:

- **Social Sharing**
- **Life Logging**
- **E-Health**
- **Online Banking**

Roadmapping Cybercrime

The roadmap developed within the project encompasses all the aspects which may contribute to reach this goal, from the development of better and more robust technologies for prevention, detection and mitigation of the attacks, to the legal and forensics aspects concerning the fight against cyber crime and cyber terrorism, up to the need of developing better methods to measure and to analyse the phenomenon and make the citizens more aware of it.
The roadmap is the final outcome of a process of information collection and analysis, during which the existing literature has been deeply analysed, public events and interviews with the relevant stakeholders have been organized in order to grasp the future challenges which our society will be called to face in the forthcoming years. A ranking methodology has been also applied to the devised research topics which allows to obtain different views of the research roadmap tailored on the needs of the different stakeholders which may be interested in the project outcomes.

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

WHO PARTICIPATES IN CYBERROAD?

The CyberROAD consortium is led by the University of Cagliari and consists of **20 international partners**, involved in the fight against Cyber Crime and Cyber Terrorism. Members include representatives from Academia and Research, Industry, Government and NGOs across Europe:

- PRA Lab, University of Cagliari, Italy (Project coordinator).
- CEFRIEL - Forcing Innovation, Italy.
- CyberDefcon, UK.
- National Centre for Scientific Research "Demokritos", Greece.
- FORTH - Institute of Computer Science, Greece.
- Governo de Portugal - Ministério da Justiça, Portugal.
- Hellenic Republic - Ministry of National Defence, Greece.
- Indra, Spain.
- INOV - Inesc Inovação, Portugal.
- McAfee, UK.
- MELANI - Reporting and Analysis Centre for Information Assurance, Switzerland.
- NASK, Poland.
- Poste Italiane, Italy.
- PROPRS - Professional Probabilistic Risk Solutions, UK.
- Royal Holloway - University of London, UK.
- SBA Research, Austria.
- Security Matters, Netherlands.
- SUPSI - Scuola Universitaria Professionale della Svizzera Italiana, Switzerland.
- Technische Universitaet Darmstadt, Germany.
- Vitrociset, Italy.

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

Social Sharing

Social Networks are Internet-based services that allow people to share information with a community. Websites like Twitter, Facebook, LinkedIn and Google+ became the most popular sites on the Internet, and every day millions of users use them to create connections with other people.

The huge spread of social networking sites allows them to collect a fair amount of personal data about the users and their communities. Unfortunately, this wealth of information, related to the ease with which it is possible to reach a large number of people, is a factor of attraction for malicious parties.

Current threats

Cybercriminals attempt to use social media sites as a delivery method for malware:

Creating fake news sites which somehow attempt to exploit unsuspecting users' browsers and their plugins. Links to those sites are advertised on social networks in an aggressive way - forcing users who click on a link and to share the link with all their contacts.

Establishing click farms: sets of users profiles, which can be used to abuse advertisement systems by creating a false sense of popularity of products or topics. Click farms are either made up of fake profiles or from profiles of unsuspecting users who "liked" a popular social network page or profile in the past.

Sharing illegal content: hate speech, advertisement of goods and services which are illegal to sell (drugs, gambling, counterfeit goods, illicit materials), paedophilia. This problem is underlined by differences in legislation regarding what is considered legal in different countries.

Current defenses

Content filters and "report spam/malicious software" are the only automated methods of eradicating malware, scams and other illegal content from social media. These methods set only a good baseline for other, manual forms of protecting social media websites, mainly because easy access to details of personal lives is still a problem and one that cannot be solved easily. People simply do not use privacy options, because they lack the awareness of the possible consequences of sharing private information online, and thus see no incentive in the effort to protect it.

Future threats and future defenses

All this information sharing makes it easier than ever for attackers to assume your identity or an identity of your relatives or close ones. Sending fake, highly personalized "help needed" messages has also became a rather simple task. Moving from a broader, spam-like distribution of malware to a more personalized way of providing malware/phishing disguised as a useful and meaningful service for a particular individual is also simpler and, as always, more effective. In response to current defences, attacks have to become more personalized and the defences have to adapt to that threat model.

Impersonation could become a serious problem - it is increasingly easier to get information about a specific person and to impersonate him or her. This could lead to the surge of different "identity protection/identity theft insurance" schemes. These schemes will be a business incentive for ordinary people to care about their privacy and consider what to make public.

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

LIFE LOGGING

Life Logging, also known as Life Archiving or Quantified Self, is the process of capturing and recording (logging) data generated by one's bodily (physiological) activities. Typical life logging includes recording activities related to sleeping, eating, walking, moods, emotions, through smart digital/wearable devices, able to automatically monitor and capture data. Life logging, by its nature generates tremendous amount of data that must be stored, processed and transmitted.

CURRENT THREATS

One of the top security challenges facing life logging is the possible attack on various components of the system resulting in violation of any of the key components of information security – availability, confidentiality and integrity. Most of these components were designed with low attention to security.

Using specially crafted malware and social engineering skills life logging data can be breached and used for nefarious activities such as **blackmailing, cyber stalking or extortion**.

Data being processed or stored as part of life logging activity can be changed or replaced through various means by the criminal to achieve specific ends. This type of attack can have far-reaching consequences especially for applications relating to health and wellbeing. As an example, a few well-publicized privacy breaches involving fitness trackers could lead to a sharper focus from governmental agencies on wearable security. **Information transfers** from wearables to insurance companies could lead to a big data dystopia that few consumers want. The benefits of life logging include memory recall and retrieving documents, among others.

CURRENT DEFENSES

Current defences include employment of various security measures inherent in other areas to protect availability of life logging systems and integrity and confidentiality of data being acquired, processed and stored by the system. Such security measures include physical protection, encrypting data end-to-end; multi-factor authentication, enforcement of data protection laws and regulations, and user awareness training.

FUTURE THREATS AND FUTURE DEFENSES

Future security threats to life logging include: accidental loss of device by users or individuals, intentional and unintentional destruction or misuse of user's data, equipment/communication failure or malfunction, malicious physical or logical attacks on logging infrastructure, hearing or recording beyond the scope intended by the logging system, profiling of individuals, spamming activities of criminals, peer pressure to share data. All these threats will present themselves in new and emerging technologies (IoTs), people's sharing of data via mobile networks, Online social networking and other complex chains of trusts and relationships. To defend against future cybercrime threats on life logging, the critical stakeholders need to consider the adoption of secure-by-design philosophy in the implementation of different components that make up a life logging system. A situation where systems are designed and security fitted after-the-fact, creates security loopholes in systems that are often exploited by cybercriminals; security awareness training for users; review of existing laws and enactment of new ones to make up the gaps in laws governing use of logging systems.

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

eHealth

Until a few years ago, healthcare ecosystems were understood as limited within the hospital walls. An evolution of the healthcare systems started, thanks to the evolution of information technology and mobile services/wellness solutions, knocking down the localization attribute, in favour of an outsourced network of services. Therefore, hospitals evolved from a place of care to a network of care services, developing Assisted Living systems and Patient Ecosystems. The main motivation for cybercriminal activities in healthcare is financial profit from stolen data. The modern healthcare ecosystems can be abused in different ways. Hospitals became digitalized often with complex and still largely unsolved security problems tied to the used standards, lack of harmonization of services and problems with either roles in the hospitals and harmonizing laws among different countries (especially in Europe).

Current Threats

Health is a simpler target than banks, the hospitals security landscape is jeopardized and their employees are much less trained. This problem is getting even harder with the rise of mobile Health. **Physical theft/damage/loss** is maybe one of the most usual cases in areas where there is the presence of very sensitive data, such as health and government. **Information theft** is another important element of incidents in the medical/healthcare industry. **Identity theft** in this sector has received particular attention. **Targeted Attacks** are among those that more efficiently exploit Social Engineering techniques to facilitate data breaches. Social engineering is hard to identify, especially in larger organizations where workforce members do not always know their fellow co-workers. Threatening of hospital patients and infiltration through the external nodes. The problem of a distributed informative system like Hospitals 2.0 is that the security of the overall ecosystem is equal to the security of the weakest nodes, which, in a distributed system are several: patients, wearable devices, peripheral ambulatories, etc. Modern hospitals still suffer the problem of standardisation in the eHealth world; interoperability standards to allow semantically correct interoperability should be defined and adopted, to allow a proper interchange of data, transactions, messages and document structures, adopted terminologies, code systems.

Current Defenses

After significant financial costs incurred by migrating to electronic health records, the health care industry now is looking to beef up its spending on data security, innovative user awareness programs involving the victims into the attack tactics (social engineering), innovative mobile terminal management systems which mix perimeter defence with pervasive awareness.

Future Threats and future defenses

The personal information space is getting larger, more complex, and it is opening to an increasing number of patients and operators, also thanks to the diffusion of personalized healthcare services offered through ecosystems, while the general awareness of what data sharing implies is not increasing. The Deployment EU research priorities in healthcare underlined some priority areas including legitimization of mobile Health solutions and data; healthcare delivery and connecting healthcare professionals; Mobile Health for patient engagement and empowerment; Mobile Health for wellbeing and prevention; and adoption of specific security certifications in the health-care sector.

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

Online Banking

Online Banking is an ICT payment system which enables a bank customer to effect transactions on his account from anywhere and at any time. An online banking customer receives his banking credentials (ID and password) and, additionally, he could receive a token (hardware or software). A variant of the online banking system described above is Mobile Banking in which the bank customer uses mobile devices to effect banking transactions on his accounts. While online banking has contributed to making life easy for bank users and building a truly global village, it has equally provided new platforms for criminals to attack users to dispossess them of their funds.

Current Threats

One of the greatest threats currently faced by online banking is the existence of many sophisticated and difficult to fight malicious software tools. This software uses various techniques to steal banking credentials from users, which are then exploited by the criminals to withdraw money from the online banking users. An example for such malicious tools are **keyloggers** that hide in the background of an infected system to record keystrokes typed by the system users, which may include their banking transactions and user IDs and passwords. **Phishing** is also commonly used, whereby attackers use various social engineering techniques such as spoofing of banks' websites to obtain users' bank credentials.

Current Defenses

Login ID and password is a common security measure used by banks to protect their customers from cyber-attacks on online systems. Overtime, login ID / password turned out to be weak means of authentication as they are easily broken due to poor password management practices by users and availability of many password cracking tools. An alternative measure, the **One-time password (OTP)**, is a password used on a computer system, which is valid for only one login session or transaction. OTPs are more secure than static passwords, which are susceptible to replay attacks.

Most current banking applications use a system of two- factor authentications and TANs, i.e. one-time PINs that a user has to provide before executing transactions. Typically, these TANs are sent to the legitimate user of the bank account beforehand via mobile phone or bank token. Thus, most banking applications currently provide a form of two-factor authentication, where the attacker either has to possess access to the victims TAN-list.

Future Threats and future defenses

ICT is moving to a stage where every common device will be connected to the Internet. This drive into digitalization of everything is called Internet of Things (IoT). Our everyday-use devices may all have digital components connected to the Internet. It would be possible for financial institutions, equipment manufacturers and system integrators to enable such devices for financial transactions and payments. In such a scenario, we expect cybercriminals in pursuit of financial gains to attack such systems using current and emerging tools and technologies.

The first form of defence against future cybercrime attacks on online banking platform is user awareness training. Other forms of defence include multi-factor authentication and strong encryption technologies on online and mobile banking devices and platforms.

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

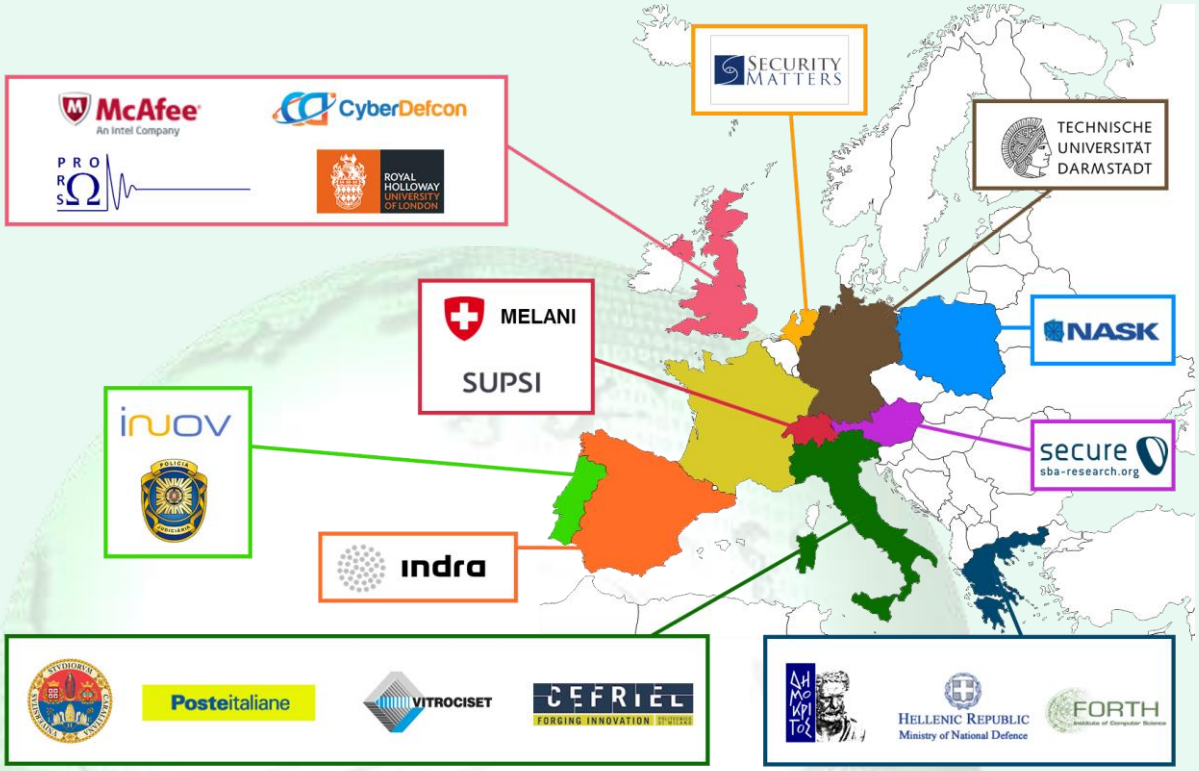
With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

The electronic version of this document is available on the official CyberROAD project's website
www.cyberroad.eu

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

The CyberROAD Consortium



Visit our Website

http://www.cyberroad-project.eu/en/

Join us in Social Media

https://twitter.com/cyberroad_eu

https://www.facebook.com/cyberroadproject

https://www.linkedin.com/groups/CyberROAD-8184478

Contact the Coordinator

Prof. Fabio Roli
Department of Electrical and Electronic Engineering
University of Cagliari - Piazza d'Armi 09123, Cagliari, Italia.
E-mail: roli@diee.unica.it, **Phone:** +39 070 675 5779, **Fax:** +39 070 675 5782

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.