Funded by the European Commission
Seventh Framework Programme

Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

Cyber Threat Awareness

Author(s): Davide Ariu (UNICA), Giorgio Giacinto (UNICA), Fabio Roli (UNICA), Enrico Frumento (CEFRIEL), Federica Freschi (CEFRIEL)

CC RG-5 & CT RG-2 – New awareness methodologies with a human touch
CC RG-20 & CT RG-17 - Training methodology (anti-phishing and social engineering) to increase security awareness for critical infrastructures.
CC RG-56 & CT RG-56 - New ways to alert users of ongoing attacks or increased risks because the device become a disappearing device and thus perceiving the related threats is also difficult.
CC RG-58 - Techniques and strategies for raisin user awareness towards the sensitivity of health data. Methods for providing the social component of such networks, while still providing anonymity.
CC RG-63 - Research into effective awareness training methods
CT RG-68 - Process awareness embedded in security tools

ABSTRACT

Nowadays, Social Engineering (SE) attacks are posing one of the most significant risks for cybersecurity. Indeed, the analysis of the new attack strategies clearly shows how cybercriminals increasingly tend to exploit vulnerabilities introduced by human factors to perform cyber-attacks. While SE is a well-known method for deception used for a very long time, its evolution in the past years has been dramatically changing the current attack landscape, and it will heavily influence future scenarios. The evolution of SE attacks is rooted in socio-economic and technological factors. On the one hand, current society transformations are characterized by a model of "immersed humans", where physical and virtual meetings seamlessly merge, thanks to mobile and ubiquitous terminals. In working contexts, employees can complete a task in any possible place, leading to an inevitable blending between private and professional lives. Furthermore, the advent of online social networks has been heavily affecting people-sharing habits, creating a proliferation of digital identities available on the Internet. On the other hand, new technologies have been enabling more sophisticated SE attacks, i.e. advanced automatic methods to gather and elaborate information needed to carefully select the "victims". All these factors contributed to the evolution of SE into a new multifaceted phenomenon that goes under the name of Social Engineering 2.0, which increases the number of potential victims directly exposed on the Internet.

People's vulnerability to SE attacks is based primarily on their naivety and lack of cybersecurity awareness. Hence, SE attacks (e.g. stealing bank codes and passwords) exploit the behavioural habits and trusting nature of users. The unsafe behaviour of users is also worsened by the poor design in many human-computer interfaces that do not provide any feedback on the increased exposure to cyber threats. Since the crucial phase of these attacks leverages on vulnerabilities introduced by users' behaviour, it is of the utmost importance to extend the governance of security to include human element among the risk factors in order to implement appropriate and effective countermeasures. The most effective measure against SE attacks is the development of awareness through specific training courses. Such training should be aimed at increasing the security culture within a specific domain. The crucial point is to create awareness programs that have a real impact on people's attitudes with the result of an effective increase in the level of security to be maintained over time. In general, it is necessary to develop intervention strategies that encourage the active involvement of people, where security features are not perceived as an "enemy", but as an ally to cooperate with in avoiding the bad consequences of falling victims of SE attacks.

RESEARCH ACTION #1

Improvement of awareness mechanisms for data and information sharing in personal and wearable devices and in the trend of disappearing computer

DISTANCE TO THE MARKET: **TRL 3**
COST OF THE TOPIC: **5 STREPs + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **3**
TIME SPAN FOR ADDRESSING THE ACTION: **36 months**
ACTORS: **Research institutions, Industry**

Personal devices, such as smartphone, wearables, and the whole category of disappearing computer, are capable to sense, store, and share a large variety of environmental, physical, and health data, as well as textual and visual information. Often this happens without users' awareness and knowledge. The new European General Data Protection Regulation (GDPR) legislation foresees to radically change most of these problems, but the awareness of the users in terms of understanding what the systems propose or want to do with the data is still lagging behind.

For these reasons, there are some important directions that should be investigated to improve the informed use, and the market penetration of these solutions.

- Raising user's awareness through effective feedback mechanisms from the connected devices that let the user clearly perceive privacy and security risks related to improper data sharing behaviour.
- Interactive and adaptive alerting mechanisms that allow users to cooperate with the machine in detecting the characteristics of potentially unsecure websites, cloud and online social services.
- Informed processing of data along its lifecycle, so that users can control the whole chain, from the acquisition phase, to data storage and destruction, with the possibility for the users to revoke permissions.

RESEARCH ACTION #2

Improving the awareness of cyber threats for workforces in critical infrastructures

DISTANCE TO THE MARKET: **TRL 4**
COST OF THE TOPIC: **3 STREPs + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **30 months**
ACTORS: **Industry, research institutions**

- Effective detection of phishing web sites, and spear phishing emails based on the correlation of open source intelligence, textual and visual analysis.
- Enable the user to naturally interact with the phishing and spear phishing detection mechanisms in a feedback loop to iteratively improve the detection capabilities, and raise the awareness level of the workforces.
- Threat modelling paradigms for critical infrastructures that include indirect threats based on social engineering attacks.
- Involvement of users in defence solutions, by keeping the humans in a feedback loop with the modern learning-bases threat intelligence systems, to match the users' awareness tracks with the learning curves of the defence system. Despite some early products appeared on the market the research is still at its beginning. For example, a crowd idea generation based approach that rewards humans to participate into human sensors networks signalling phishing samples, could be used to feed analyst-driven predictive analysis.

RESEARCH ACTION #3

Detection of attempts of tampering with manufacturing processes in industrial plants

DISTANCE TO THE MARKET: **TRL 3**
COST OF THE TOPIC: **5 STREPs + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **36 months**
ACTORS: **Industry, Research Institutions**

- Novel paradigms for security information and event management to correlate network and computer system events with process control events.
- SCADA devices and algorithms to self-detect any modifications in manufacturing process execution.
- Encryption and obfuscation mechanisms for the exchange of data and command and control instructions in the internal network connecting the remote controlled production systems.
- Insertion of humans in the loop: most of nowadays threats involve humans as their main vector of infection. Humans became a relevant and integrated part both in the attack and protection mechanisms: this changed the landscape of IT security, because the humans have been added in the protection mechanisms as sensors (sensing what is happening in the enterprise, via for example human sensors networks), or feeding the machines (for example analyst-driven solutions). Integrated human-technological protection systems are appearing on the market, but the research area is still evolving.

Creation of ad-hoc awareness experiences

DISTANCE TO THE MARKET: **TRL 4**
COST OF THE TOPIC: **4 STREPs + 0 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **30 months**
ACTORS: **Industry, Research Institutions**

The number of awareness mechanisms available in the ICT Security market for training users is increasing, ranging from printed leaflets, courses, infographics, videos, audio courses, and gamification. However, each of the available method showed its effectiveness in specific environments (e.g., video and posters in enterprises, gamification with citizens etc.), but there is neither a winning approach, nor some guidelines to allow the selection of the best approach for a given scenario. Nevertheless, the most interesting recipes for new awareness strategies in security are all involving the following three elements:

- Gamification: traditional ICT security trainings do not present particular appealing characteristics. In contrast, gamification frames such trainings as hacking games of different formats (e.g., attack-defence capture the flag, jeopardy), fostering competitiveness and promoting problem-solving activities.
- Incidental learning: partial yet continuous learning and knowledge improvement, for example through mini-sessions during the day, trying to avoid monolithic tracks.
- Personalization: adapt the learning experience to individuals' attitudes, habits and mind-sets.

What is important to investigate is how to tailor the awareness experience around each single person, according to his/her psychological profile and personality and match these findings against the costs to produce the material.