Funded by the European Commission
Seventh Framework Programme

Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

SCADA & CIP

Author(s): Javier Martínez-Torres (INDRA), Jorge López Hernández-Ardieta (INDRA)

CC RG- 14 and CC RG- 16 - Tamper-proof sensors and controllers
CT RG-21 Develop techniques for monitoring and control of parameters and status of pipeline in order to detect deviations and misbehaviour
CT RG-22 - Research into improving integrity and confidentiality of heterogeneous smart grid networks.
CT RG-24 - Physical-layer authentication
CT RG-27 - Research on efficient and secure communication protocols for wide area power systems
CC RG- 28 and CT RG-28 - Research on secure routing and aggregation protocols
CC RG- 30 and CT RG-30 - Research into securing large scale (Open) Demand Response environments
CC RG- 35 and CT RG-35 - Challenging to provide protection to a large number of components in the entire railway/aviation system
CC RG- 37 and CT RG-37 - Identify integrity of messages, support designated capacity per radio link, identify jammers
CC RG- 45 and CT RG-46 - Enhance robustness in existing geo-localization systems
CT RG-49 - Assess the performance of GNSS receivers in a broad range of channels under different attack schemes to provide a framework for risk and vulnerability assessment
CC RG- 90 and CT RG-86 - Design of banking system solutions that are resilient to DDoS attacks

ABSTRACT

The modernization, interconnectedness and increasing complexity of Critical Infrastructure and the underlying technology have made that new attack vectors are available for offenders. Thus, in order to protect Critical Infrastructures effectively is mandatory to leverage various new approaches. This challenge is especially relevant in national security and the fight against cybercrime and cyber terrorism.

Addressing Advanced Secure Mobile Computing for the protection of Critical Infrastructure

DISTANCE TO THE MARKET: **TRL 4-5**
COST OF THE TOPIC: **3 STREPs + 3 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **1**
TIME SPAN FOR ADDRESSING THE ACTION: **50 months**
ACTORS: **Governments, Critical Infrastructure Organizations, Research Institutes**

Smart phones and other types of smart devices, such as wearables, IMD (Implantable Medical Devices) and Internet-enabled appliances are now widely adopted. They offer pervasive user connectivity through various wireless communication means, powerful sensing capabilities and easy install-and-use of third party applications. Altogether, it is reasonable to think that they will become the main user platform for managing Critical Infrastructure in near future.
The architecture of smart devices, the existing security models and the prolific mobile malware market make current commercial solutions highly ineffective. Recent studies show that traditional signature-based antimalware techniques for smart phones detect only between 20.2% and 79.6% of analysed malware. Other approaches, such as dynamic analysis, seem promising but are unaffordable when executed on the device due to resource consumption rates.
On the other hand, the inherent architecture of the smart phones, enables potential attacks at device or application level by subverting the security of "goodware" installed on the device. To deal with these threats, completely novel approaches that consider the whole ecosystem of apps installed on the device are required. Such approaches should highlight the level of security the apps exhibit, to support making informed decisions about whether executing certain actions (e.g. managing power plants, water treatment plants, etc.) that might have an impact not only on the citizens but also at business level.

Ensuring a secure execution environment brings a number of challenges that are particular to smart devices:

- Efficient and effective real-time, dynamic risk assessment for making informed decisions with a clear impact on personal and business assets. Recent advances suggest that the optimal approach lies in a combination of market, platform and cloud-based defensive strategies that overcome the inherent limitations of current devices. Transforming this into practical, cost-effective solutions remains an open challenge for the industry.
- Identifying and detecting polymorphic and metamorphic malware, as well as repackaged malware apps (the most common distribution and infection vector) regardless the presence of any security measure implemented at market level (open/unofficial markets).

None of the above will succeed against our adversaries if the human analyst still plays a role in the process, neither when supported by automated tools. Fully automation becomes a must-have requirement, both for malware/attack detection

and remediation/response actions. Considering the figures of the malware market and its daily growth, it is obvious that the human analyst must move from a link in the operational chain to a valuable asset in pre and post operational phases, such as the design of new tools (analysis strategies, expert knowledge, algorithms, patterns) and the post-analysis of automatically-generated information.

Training platforms able to replicate real Critical Infrastructures

DISTANCE TO THE MARKET: **TRL 6-7**
COST OF THE TOPIC: **3 STREPs + 2 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **1**
TIME SPAN FOR ADDRESSING THE ACTION: **42 months**
ACTORS: **Governments, Universities, Critical Infrastructure Organizations**

Although figures vary between reports, there is a general agreement over the fact that current and former employees are amongst the main causes of cybersecurity incidents suffered by the Critical Infrastructures. Their lack of awareness is one of the most significant threats any organisation has to face. Likewise, the lack of qualified and trained IT/security staff aggravates the situation.
It has been largely proved that conducting training and awareness activities is a winning bet for reducing exposure to cyber threats at a reasonable cost.
Traditional training approaches, namely class-room sessions, e-learning and b-learning (as we know them today) do not suffice to keep our workforce up-to-date and ready to respond in such an overwhelming changing scenario. Punctual training sessions, however they are provided, continue to lag behind the rapid rate of change of technology and cyber threats. But, worst of all, current approaches cannot accommodate, in a cost-effective and timely manner, the particularities of a customer's security problem, neither the technologies nor networks they use in their operational environments. In other words, the effectiveness of the training is very limited.

Even though training is currently considered a fundamental prerequisite for the adequate protection of Critical Infrastructures, there is still a need for innovative technology capable of providing realistic, flexible, evolutionary and tailored training able to reach a large-scale audience in a cost-effective way. As of today this remains a great challenge both for the academy and the industry.
In recent years, the training concept has been reshaped with the introduction of cyber ranges. A cyber range is a virtual environment typically built on top of standard hardware and used for multi-tenant hands-on training, experimentation, test and research in cybersecurity.

Some of the aforementioned required properties (realism, flexibility, etc.) are already met by current cyber range solutions. For example, a standard cyber range is usually designed to provide realistic settings where the user interacts with real (virtual) systems and networks that may, to some extent, reproduce real-world scenarios with real-time feedback and operation.
However, much research and innovation is still needed to accommodate and combine in a single solution all of the properties above. For instance, combining the capability to tailor a hands-on training course for a specific customer is, considering current cyber range solutions, impractical if large-scale and cost-effective properties also need to be provided. With this regard, a smart and

automated trainee supervision and assessment system that guided them through the exercise, providing automated hints when needed, would permit to deploy the solution for thousands of trainees concurrently without the need of a single instructor. Also, a cyber range capable of easily deploying on-demand configurations of new tailored exercises would provide a significant improvement to better tackle with particular needs, specific situations, and representing new and emerging threats.

If there is one common limitation in current cyber ranges is that, even when commercialised under the label of training platforms, they support test, experimentation and research activities (even capture-the-flag competitions) but without any pedagogical features. Current solutions hardly incorporate metrics and functionality to measure the actual performance of the trainee and manage their progress along the time. At the most, we observe that some solutions incentivize and motivate the trainee using quantitative scoring systems or gamification approaches. A more comprehensive and systematic view is needed. The foundations underlying the learning process should be considered by design. This may imply implementing different and complementary approaches, such as formal learning, observational learning, trial and error approach, etc.
Related to this, the complexity of the training exercises should be scaled to the trainee's level, customising the level of automated guidance and support in each exercise. This is particularly important when targeting individuals at introductory level. A significant break-through innovation would be that this adaptation – including the difficulty of the training – is automatically readjusted along the lifespan of the training, an even dynamically during an exercise, according to the trainee's performance. The system could, for example, propose new challenges/objectives, reinforce certain attitudes or improve the adversary skills for highly proficient trainees.

Expected Impact:

1) Increased competiveness of European Critical Infrastructure security to the needs of citizen, national public administrations and organizations.
2) Increased resilience against widespread cyber security threats facing Critical Infrastructure Organizations.

Information Sharing Systems to support Critical Infrastructure protection

DISTANCE TO THE MARKET: **TRL 6-7**
COST OF THE TOPIC: **4 STREPs + 2 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **3**
TIME SPAN FOR ADDRESSING THE ACTION: **36-45 months**
ACTORS: **Governments, Critical Infrastructure Organizations**

The efforts and initiatives towards encouraging the information sharing amongst the stakeholders in Critical Infrastructure protection are significant and continue to grow in number and intensity. The European Cybersecurity Strategy and the NIS Directive are possibly the most relevant examples at European level, identifying information sharing as one of the main pillars for building cohesive and resilient infrastructures and services in Europe.

However, in spite of the achievements made so far, which were undoubtedly necessary, there is still a long road ahead if we really want to fight cyber threats effectively and be at the forefront of this never ending battle. Cyber-attacks execute and succeed in computer time, so we need information sharing mechanisms that operate within the same order of magnitude. Contrary to this, we regret to observe that current real-life implementations for information sharing still heavily depend on the human factor.

In addition to this, the intrinsic flawed and highly vulnerable nature of technology leads us to conclude that absolute trust cannot be achieved in Critical Infrastructure. We should not rely, in absolute terms, on any information independently of who is the source. This demolishes the principle which current real-life implementations are based on, mandating full trust in the peers that are part of an information sharing community. This problem is aggravated by the fact that we cannot foresee who will have the knowledge needed to prevent or respond to certain incident. So, it seems that creating rather static, rigid procedure-based information sharing communities, as suggested by current political and industry initiatives, will not work as effectively as we require.

In order to really make information sharing a truly useful tool that eventually redresses the imbalance between attackers and defenders we need an urgent shift in the way we approach it. In particular, we need (near) real-time information sharing that relies on suitable trust and risk-aware models at the same time that leverages existing standards (data formats, exchange protocols) and infrastructures. Creating novel mechanisms and models for information sharing would benefit the whole community. We recognize that the human-factor is possibly the main impediment for the wider adoption of not only novel ways of sharing information automatically without the human intervention, but also "de facto", more traditional information sharing practices that have not managed to prosper.

Expected Impact:

1) Improved cooperation among Critical Infrastructure Organizations across the EU and Associated Countries.
2) Lower cyber operating costs for European CERTs teams
3) Improved description of incidents and characteristics of the various types of cyber-attacks frequently carried out by cyber terrorist.