I Don't Trust ICT: Research Challenges in Cyber Security

Félix Gómez Mármol[1], Manuel Gil Pérez[2(✉)], and Gregorio Martínez Pérez[2]

[1] NEC Europe Ltd., Kurfürsten-Anlage 36, 69115 Heidelberg, Germany
felix.gomez-marmol@neclab.eu
[2] Departamento de Ingeniería de la Información y las Comunicaciones, University of Murcia, 30071 Murcia, Spain
{mgilperez,gregorio}@um.es

Abstract. Can we trust ICT (Information & Communication Technology) systems? Every single day a handful of previously unknown security vulnerabilities on these environments are published, dangerously feeding the lack of trust feeling that many end users already exhibit with respect to ICT. In order to disrupt and even invert such a perilous tendency (hindering the wide adoption of ICT and all its associated benefits), a number of research challenges in the field of cyber security need to be addressed. This paper presents some of these key challenges, offering initial thoughts on how to tackle each of them.

Keywords: Trustworthy ICT · Cyber security · Research challenges

1 Introduction

The numerous benefits brought by Information and Communications Technologies (ICT) are unquestionable today. Yet, a non-negligible amount of end users feel often reluctant to enjoy those advantages, since they distrust such ICT. And this lack of confidence is mainly due to the perception of insecurity that the ICT systems pose. Despite the large amount of works and efforts mainly done by the research community, government agencies and industry, oriented to provide security solutions for the ICT systems [1], everyday we observe fateful news regarding the proliferation of new cyber attacks, thefts, threats and other potential cyber crimes. Thus, we state that such mistrust will persist while the aforementioned perception of insecurity in ICT systems remains [2].

In this context, this paper presents some of the main challenges in the cyber security field that must be first addressed and solved in order to increase the trustworthiness of the end users in the ICT systems, in a way that the former may benefit from the latter. It is noteworthy that this paper does not merely list a number of challenges, but it also provides a pool of initial ideas on how to manage each of them. Therefore, the main contribution of the paper is to bring together a number of challenges in order to foster and encourage research in the

S.M. Habib et al. (Eds.): IFIPTM 2016, IFIP AICT 473, pp. 129–136, 2016.
DOI: 10.1007/978-3-319-41354-9_9

field of cyber security, with the ultimate goal of increasing the trustworthiness deposited by end users in ICT systems.

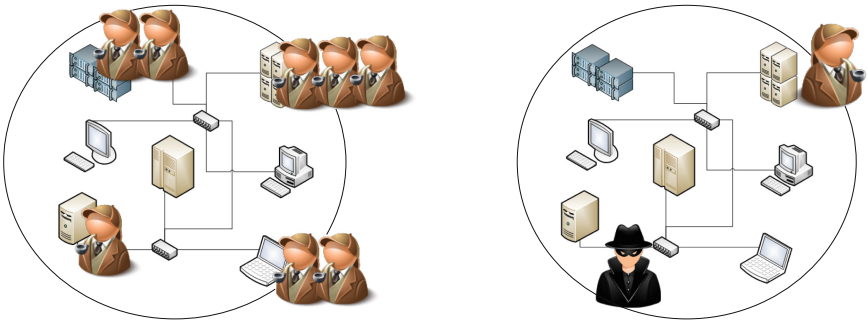
As stated before, cyber security entails a large list of challenges, where the most critical ones can be grouped in the following four main research trends. They have to be treated adequately in order to provide greater trustworthiness of the end users when using the ICT systems.

- **Dynamic risk management**. The organizations' operational needs have to be continuously tackled to update the risk level of any change happening in the corporation on its assets: changes in threats, new vulnerabilities, new response actions or countermeasures, or even modification of the assets themselves [3]. A dynamic risk management or treatment system requires a continuous feedback mechanism to monitor threats in a real-time basis, and so allowing a quick reaction to minimize the exposure time in front of potential risky situations and events for the organization being protected.
- **Attack and defense graphs**. One of the main ways of providing risk assessment is supporting the implementation of attack and defense graphs [4]. With them, the dynamic risk management systems pretend to estimate the level of risk of the assets through the definition of attack patterns to capture dynamics of a threat and stages it has to go through.
- **Incidents correlation**. The correlation mechanisms are a required feature to reach a holistic view about the cyber security of any organization. All the sensors, strategically deployed in the underlying network, should share their monitoring information in an orchestrated way with the aim of correlating the individual evidences detected by each of them in different locations [5]. With this information, the dynamic risk assessment engines will subsequently compute the instantaneous risk level of the organization at any time.
- **Information sharing**. In the current distributed systems, it is necessary to define an information model with which to exchange the corresponding information between the different stakeholders in order to detect distributed threats [6]. This will require the design and deployment of context-aware security and privacy models protecting the process of sharing information among the different actors of the dynamic risk management system: how to securely share the information, which one can be shared and which one cannot. Furthermore, the risk information sharing conveys the use of standard formats and protocols to reach a common assurance model between stakeholders in a trustworthy way.

All these challenges can be summarized as follows, where the text in bold corresponds to the previous main four research trends and the italic text represents the properties of each of them:

> *Dynamic* **risk management** over *large systems* using *adaptive* **attack/defense graphs** with *privacy-preserving* **incidents correlation** and *encouraging* **information sharing**

In the next sections, we present the main research challenges in the cyber security field regarding the four research trends enumerated earlier.



(a) RC1: Resources allocation (b) RC2: Insider attack

Fig. 1. Resources allocation and insider attack cyber attacks

2 Dynamic Risk Management

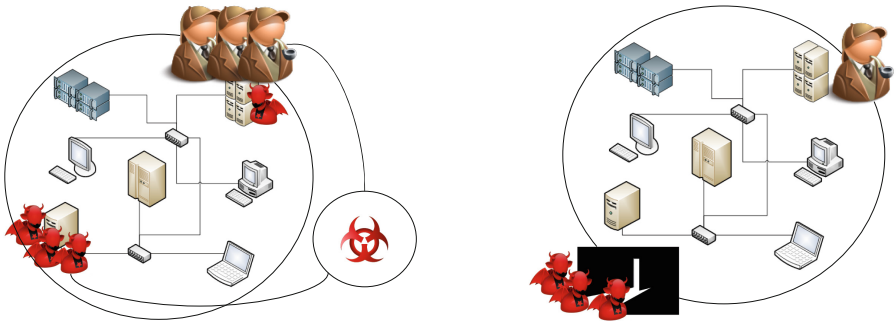
Despite the plethora of works aimed at designing accurate dynamic risk management in ICT systems, there are still unresolved research challenges (**RC**) that should not be neglected. Among them, we highlight the following main challenges that, in our opinion, represent initial ideas to be firstly addressed them.

RC1. ***How to estimate how much effort (resources) to put on monitoring/protecting each asset?*** In an ICT system the assets are limited, but so are the resources to protect them too. Hence, there is a need to smartly allocate resources to protect each asset (see Fig. 1a). Moreover, such assignment can be dynamic throughout time. To this end, dynamic risk management can become a powerful tool to influence such resources allocation decision.

RC2. ***How to minimize the impact of unexpected advantages in a cyber attack (e.g., an insider attack)?*** One of the most potentially harmful attacks is the one coming from an insider within the system to be protected (see Fig. 1b). In those cases, where a trust relationship between the insider and the organization is violated, it is critical to minimize the damage inflicted by the attacker. Thus, an appropriate risk management could promptly raise a flag when a suspicious behavior is detected from a user within the system.

RC3. ***How to detect cyber attacks trying to divert the victim's attention to protect non-critical assets, while actually compromising critical ones?*** Attackers might pretend to be interested in a given asset, trying to force the system to allocate more resources to protect it, while their true interest lies in another asset (see Fig. 2a). These so called reverse honeypots can be effectively combated with an accurate and dynamic risk management, indicating at each time which are the assets under real attack and which not.

RC4. ***How to detect back doors inadvertently installed on the system?*** Another advanced type of attack consists of surreptitiously installing a so called back door (see Fig. 2b). This intends to be undetectable by the victim, which will be subsequently used to perform an actual attack on the system.



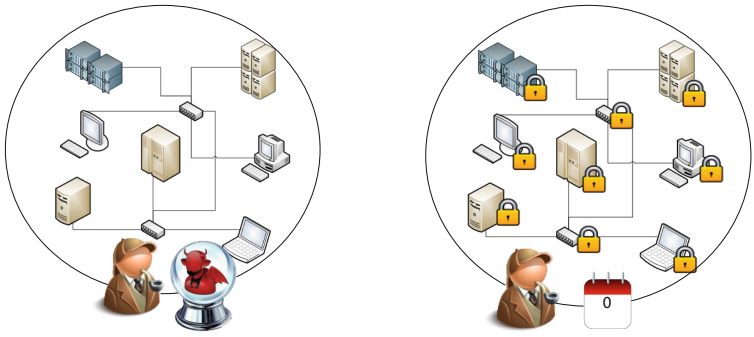
(a) RC3: Reverse honeypot (b) RC4: Back door

Fig. 2. Reverse honeypot and back door cyber attacks

A comprehensive penetration test can help out to assess the current risk of each asset in the system and, consequently, unveil hidden back doors.

RC5. ***How to predict a potential cyber attack over a given asset?*** Ideally, every system administrator would like to predict an attack before it actually happens (see Fig. 3a). In this case, a smart combination of dynamic risk management, attack graphs, incidents correlation and information sharing can be extremely effective to make accurate guesses about imminent attacks.

RC6. ***How to protect assets against zero-day exploits, while preserving usability/availability?*** Similarly to RC2, zero-day exploits, by definition, cannot be avoided (see Fig. 3b). Nevertheless, we can (and must) minimize the potential impact that such attacks might have on the system. And here the real challenge is to do so while preserving usability/availability of the protected assets. Again, dynamic risk management can be extraordinarily helpful to achieve such balance between assets protection and availability.



(a) RC5: Attack prediction (b) RC6: Zero-day exploits

Fig. 3. Attack prediction and zero-day exploits cyber attacks

3 Attack and Defense Graphs

Both attack and defense graphs have captured the attention of many researchers and security experts worldwide. Yet, their notable complexity and modest scalability are still refraining their wide acceptance and deployment [4]. Next we introduce some research challenges regarding attack and defense graphs.

RC7. ***How to effect a tailored and adaptive response to a cyber weapon?*** Whereas sophisticated attacks are often tailored to the system they are targeting, the countermeasures applied to defeat them are usually rather generic. To maximize the effectiveness of the response given to an attack, the remedies should be tailored to the specific threat they are facing. To this end, defense graphs, for instance, can constitute an essential aiding tool.

RC8. ***How to detect the target of a cyber weapon?*** Some generic cyber weapons do not have a specific target and act on an indiscriminate fashion over ICT systems. Yet, some others actually focus on particular environments such as critical infrastructures or enterprises, for example. Promptly identifying the specific ecosystem targeted by an attacker is extremely helpful in deciding how to counter such threat. Thus, attack graphs are capable of indicating which is the most plausible victim of a given cyber weapon.

RC9. ***How to detect a dormant/latent cyber weapon in our domain?*** Related to RC4, a cyber weapon can remain on a dormant state, waiting for remote instructions to wake up and perform the actual attack. While in this latent state, it will try to go unnoticed to the administrator of the victim's system. In this regard, attack graphs can assist those administrators to identify both a cyber weapon getting into the dormant state, as well as a latent one receiving commands to wake up imminently.

RC10. ***How to detect the self-destroy capability in a cyber weapon and how to prevent it?*** Some advanced cyber weapons are equipped with a self-destruction capability, leaving no trace when they realize they have been detected by the target system. In those cases, it is many times a cumbersome task to try to get information about the source of the attack or to learn how to fight against such threat. Again, attack graphs can effectively help to identify the initiation of this self-destruction procedure and abort it.

RC11. ***How to avoid an attacker to snoop into a victim's domain in preparation for a cyber attack?*** One of the first things an attacker does is to carefully study the victim's domain, seeking for vulnerabilities or weaknesses. Being able to detect such pre-analysis enough in advance gives a very valuable advantage to the administrators when defending against the actual attack. Attack graphs, together with dynamic risk management and incidents correlation, can help in unveiling suspicious behaviors considered as actions conducted by potential attackers in preparation for a cyber attack.

4 Incidents Correlation

Sophisticated attackers no longer play alone. An advanced attack usually consists of multiple steps, either subsequently or concurrently executed that, isolated,

might not be detected as a harmful action, but when combined, they deploy all their damage on the target system. In this regard, incidents correlation can constitute a very effective tool to accurately spot these situations [5].

RC12. ***How to detect cyber weapons capable of smartly colluding with other cyber weapons?*** A sophisticated cyber weapon might be able to detect other cyber weapons in the victim's domain and, even more, collude with them to provoke a bigger harm. Here, an appropriate incidents correlation could reveal such perilous collusion with potential devastating consequences.

RC13. ***How to discern whether a cyber attacker is controlling certain infrastructure (devices, networks,...) to perform the attack?*** Some attackers do not hit their final target directly, but they rather first compromise other systems (known as *botnet*) and then use those to perform the actual attack over the real victim's domain. Such strategy hinders the identification of the real source of the attack. Yet, a smart combination of incidents correlation and information sharing can ease such identification.

RC14. ***How to detect a "composite" cyber weapon smartly split into (apparently) innocuous parts?*** Another sign of sophistication in a cyber weapon consists of partitioning it into several (apparently) innocuous pieces. Each of these parts, isolated, is usually harmless (and therefore undetectable by defensive mechanisms), but when combined all together the real damage is inflicted. Again, an intelligent combination of attack graphs and incidents correlation can help in diminishing this specific threat.

RC15. ***How to discern whether a cyber weapon is autonomous or being remotely controlled by an attacker?*** While certain cyber weapons only react upon a given command from the attacker, others are rather autonomous in their malicious behavior. Being able to detect the first case can help to neutralize the attack by blocking command and control channels used by the cyber weapon to receive its orders. And to achieve that, again a coherent mix of attack graphs and incidents correlation can be of extreme utility.

RC16. ***How to detect a multi-vector cyber weapon?*** Complex and advanced cyber weapons might not take advantage of just one single approach with the aim of assaulting the victim's domain, but rather try various entry points. That weapon is known as a multi-vector one, and an appropriate incidents correlation can be crucial to unmask this type of attackers.

5 Information Sharing

It is unrealistic to think of securing ICT systems without sharing relevant data devoted to their protection. Many entities feel reluctant to share certain information that they might consider sensitive arguing privacy concerns [6], as well as other issues like current regulations, as thoroughly discussed in [7].

RC17. ***How to detect whether a cyber attack is becoming epidemic?*** Often, when a system is under attack, its administrators are unable to see

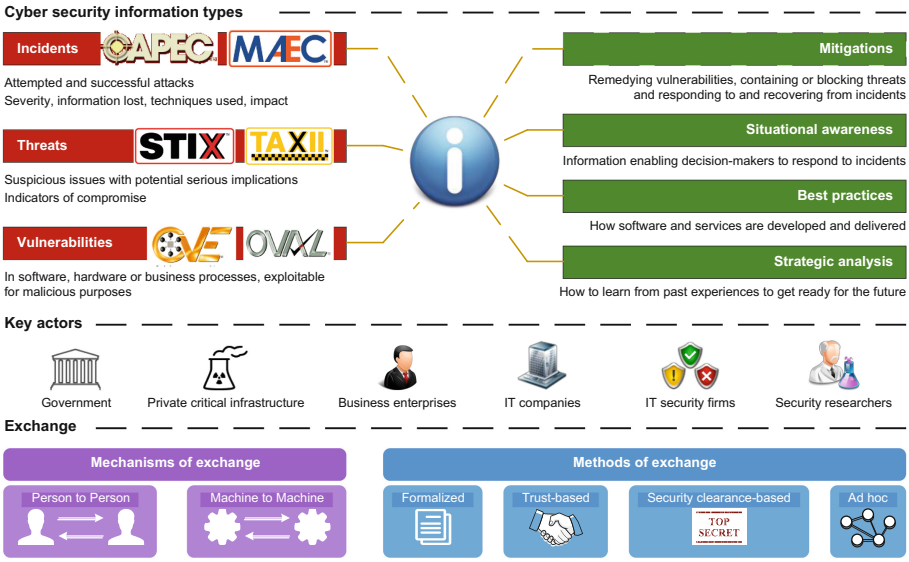


Fig. 4. A framework for cyber security information sharing and risk reduction

beyond the borders of their domain, having thus a constrained view of the overall spreading of a particular cyber weapon. By sharing specific information amongst different realms, it is possible to detect whether a cyber attack is becoming epidemic and, if so, prioritize on battling it back (see RC1).

RC18. ***How to effectively and promptly (maybe also automatically and in a standardized way) communicate and share the remedy to a given cyber attack amongst allies?*** Nowadays we still face (too often) systems exposed to rather old vulnerabilities for which there is even a patch (maybe also old). The challenge, therefore, is on how to disseminate or propagate these mitigations, patches or bug fixes so that they reach every vulnerable system in a timely fashion.

RC19. ***How to incentive information sharing to boost collaborative intrusion detection?*** One of the main impediments to a successful information sharing is precisely the reluctancy of the participating entities to distribute certain information that, in many cases, might be considered as sensitive or confidential. Hence, an appropriate incentives mechanism should foster such collaboration in detecting cyber attacks.

RC20. ***How to identify, with a certain level of confidence, the attacker in a cyber attack?*** The so called attribution problem, or how to reliably identify the source of a cyber attack, might be in many cases quite a tough task for administrators. To aim them in overcoming this difficulty, a consistent information sharing strategy, together with the most advanced incidents correlation mechanisms could be enforced.

RC21. ***How to measure whether a given domain is susceptible of having cyber weapons or being producing cyber weapons?*** Similarly to RC11, if the administrators of a system get to know well in advance that another domain contains or is producing cyber weapons targeting such given system, they can better get ready to counter back such threat.

A number of secure measures, standard formats and potential actors are depicted in Fig. 4 for sharing information, as well as how to lessen the exposure risk by making use of the research challenges identified earlier.

6 Conclusions

This paper has proposed an initial number of research challenges that need to be tackled in order to increase trustworthiness of the end users with respect to the ICT systems. All these challenges deal with cyber security threats that appear everyday incessantly, which we grouped and analyzed into four main research trends, namely: dynamic risk management, attack and defense graphs, incidents correlation and information sharing. With the aim of increasing the trustworthiness of these end users in the ICT systems, we have also provided some initial thoughts on how to deal with each of the aforementioned challenges.

Acknowledgment. This work has been partially supported by the European Commission under grant agreements FP7-ICT-2013.1.4/609062 - SMARTIE (*Secure and Smarter Cities Data Management*) and H2020-ICT-2014-2/671672 - SELFNET (*Framework for Self-Organized Network Management in Virtualized and Software Defined Networks*).

References

1. Gil Pérez, M., Gómez Mármol, F., Martínez Pérez, G., Gómez Skarmeta, A.F.: RepCIDN: a reputation-based collaborative intrusion detection network to lessen the impact of malicious alarms. J. Netw. Syst. Manage. **21**(1), 128–167 (2013)
2. Robinson, M., Jones, K., Janicke, H.: Cyber warfare: issues and challenges. Comput. Secur. **49**, 70–94 (2015)
3. Poolsappasit, N., Dewri, R., Ray, I.: Dynamic security risk management using bayesian attack graphs. IEEE Trans. Dependable Secure Comput. **9**(1), 61–74 (2012)
4. Abraham, S., Nair, S.: A predictive framework for cyber security analytics using attack graphs. Int. J. Comput. Netw. Commun. **7**(1), 1–17 (2015)
5. Zuech, R., Khoshgoftaar, T.M., Wald, R.: Intrusion detection and big heterogeneous data: a survey. J. Big Data **2**(1), 1–41 (2015)
6. Goodwin, C., Nicholas, J.P.: A framework for cybersecurity information sharing and risk reduction. Technical report, Microsoft Corporation, January 2015
7. Skopik, F., Settanni, G., Fiedler, R.: A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing. Comput. Secur. **60**, 154–176 (2016). http://dx.doi.org/10.1016/j.cose.2016.04.003