Funded by the European Commission
Seventh Framework Programme

Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

New objects and disappearing computing

Author(s): Davide Andreoletti (SUPSI), Angelo Consoli (SUPSI)

CC RG- 31 and CT RG- 31 - Difficulty to find updating mechanisms that scale to large and heterogeneous networks
CT RG-90, CC RG-93, CC RG-10, CT RG-11, CT RG-81 - Absence of a reliable and holistic security mechanism
CC RG- 8, CT RG- 16, CT RG-44 - Absence of a systemic view of the correlation among security, privacy and safety

ABSTRACT

Since the proliferation of the Internet of Things (IoT) paradigm, the use of tiny and interconnected devices has seen an enormous growth in several fields. Examples of application areas are monitoring systems and e-banking services.

Networks that are established on the basis of such devices differ from traditional ones, which makes them difficult to secure. Here we identify three key research gaps:

1) difficulty to find updating mechanisms that scale to large and heterogeneous networks
2) absence of a reliable and holistic security mechanism
3) absence of a systemic view of the correlation among security, privacy and safety.

Difficulty to find updating mechanisms that scale to large and heterogeneous networks

DISTANCE TO THE MARKET: **TRL 4**
COST OF THE TOPIC: **0 STREPs + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **12 months**
ACTORS: **Universities and academic actors; electronic industry**

The use of IoT devices is increasingly pervasive. Their adoption is common in several areas, ranging from wearable health-care devices to tiny sensors that monitor the level of water poisoning.

The scenarios where IoT networks work are continuously evolving, both in terms of computational requirements and in security complexity. Thus, it is of paramount importance to define hardware and software upgrading mechanisms that are as simple as possible.

Devices must be built in order to ease extension in memory, computation capabilities and performance in general. The same applies for software components, for which a reliable updating/patching mechanism has to be clearly defined (and standardized).

While the replacement/upgrade of hardware components requires a physical access to the network, this is not necessarily true as far as software is concerned. In fact, the feasibility of a remote upgrading mechanism which is secure and reliable is worth investigating.

More specifically, an ideal updating mechanism should discover and provide patches to new security flaws in a way that notifies the owner of the devices in a timely manner or that, alternatively, is automatic.

The former option is not always possible, since the interaction between users and devices is not as user-friendly as in a traditional scenario (e.g., devices often do not have a input/output capabilities).

As far as the latter option is concerned, it is necessary that some trusted authority (e.g., the manufacturer) get constantly notified about the status of the network, i.e., the type of devices and the software they currently run.

This requirement is difficult to meet due to two main reasons:

1) these network are heterogeneous and continuously evolve (i.e., it is easy to add and remove devices)
2) devices have generally limited connection capabilities, which make the interaction with an external entity harder.

Additionally, limited resources prevent a traditional updating mechanism to be properly implemented, since firmware and patches should be distributed with minimal overhead and stored in a very limited memory. A possible approach consists in optimizing the distribution of the updates, for example by proposing peer-to-peer solutions (i.e., a small set of nodes initially receive the updates and then deliver them to the rest of the network). Other security requirements (e.g., integrity, updates authentication, etc.) have to be satisfied in the IoT scenario. The aforementioned constraints force researchers to find lightweight solutions.

RESEARCH ACTION #2

Absence of a reliable and holistic security mechanism

DISTANCE TO THE MARKET: **TRL 3**
COST OF THE TOPIC: **0 STREPs + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **24 months**
ACTORS: **Research institutes and security related industries**

The presence of a centralized mechanism that distributes patches to the network nodes opens the door to the definition of a reliable IoT network management system. The goal is to implement monitoring/reaction procedures, in order to realize security mechanisms, analogous to those used in traditional networks (e.g., intrusion detection systems, firewalls, etc.).

The adoption of techniques commonly used in traditional network requires significant reengineering to address the constraints posed by resource-limited devices. For instance, if the processing power is limited, it is not possible to implement robust encryption and alternative lightweight solutions must be found. Analogous considerations hold as far as authentication mechanisms are concerned: due to the highly dynamism that characterize IoT networks, it is necessary to find a way to easily authenticate the sensors.

Generally, in IoT networks it is possible to identify very simple devices connected to a more powerful device, which often acts as a gateway. Being the gateway the most powerful device within the IoT ecosystem, it may be used to implement several monitoring functions that give a global view of the network. The global view also allows to correlate the events observed in all the devices, helping to identify malicious activities better than an approach based on single devices. Moreover, this approach is also more feasible due to the well-known energy issues (i.e., most of the security operations are off-loaded to the gateway). Thus, a completely distributed approach in realizing, for example, an intrusion detection system, seems to be not possible. However, it is possible to investigate hybrid solutions, where the network is divided in clusters for which head nodes are defined. The role of the cluster-head is to monitor the nodes under its supervision, measuring, for instance, their energy consumption. If the consumed energy is above a given threshold, security countermeasures should be triggered (e.g., because flooding attacks have likely happened).

Moreover, given that IoT devices are often used to gather very personal information, another key issue is the definition of mechanisms and procedures through which it is possible to understand when there is leakage of sensitive information. Thus, a holistic approach that can face both security and privacy issues in a centralized fashion seems to be a viable route to take.

Finally, an extensive standardization on how things should be secured by design is urgently required.

RESEARCH ACTION #3

Absence of a systemic view of the correlation among security, privacy and safety

DISTANCE TO THE MARKET: **TRL 4**
COST OF THE TOPIC: **3 STREPs + 0 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **18 months**
ACTORS: **Research institutes and security related industries**

Information gathered by IoT devices can be very different in nature. Some examples are: very sensitive and context-dependent information, such as those collected by wearable health-care devices; information vital for a community, such as those collected by sensors that monitor the level of poisoning of the water-supply network or information that are extremely important for an industrial process, such as those collected by generic monitoring sensors employed in a factory.

In all the aforementioned scenarios security has an impact on privacy, safety (these devices may act also in physical space) or both. Thus, a necessary step in the definition of reliable IoT system is the creation of a framework with the goal of assessing in a systemic way the correlation among these three key aspects, namely security, privacy and safety. The framework should include the definition of suitable metrics, which must measure security/safety potential risks, as well as the level of sensitiveness of the gathered information. In this way it will be easier to evaluate the type of network, and consequently implement ad-hoc design principles.

In fact, Security, Privacy and Safety by design principles must be followed and adapted to the particular situation. For example, if a network that monitors a mine field is compromised, safety of people is the first concern. If a home IoT network is compromised, the main concern is shifted to privacy. A possible design principle could be the automatic disabling of the devices that collect the most sensitive information whenever an intrusion is detected (i.e., disable certain sensors as soon as the environment is under attack).