Cryptography in the Cyber Trainer project

Francesco Tarquini, Ph.D.
Department of Information Engineering, Computer Science and Mathematics
University of L'Aquila
francesco.tarquini@univaq.it

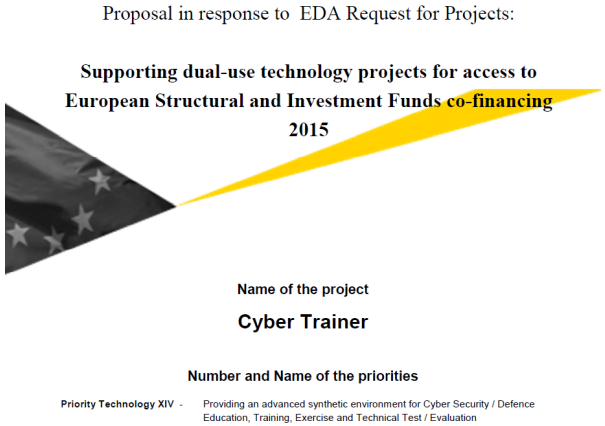
Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica
Università degli Studi dell'Aquila

The Cyber Trainer project

- is based on research and experimentation activities to build a nationwide infrastructure dedicated to the operational training of IT security staff
- helps the creation of services in favor of critical infrastructures and large national, public and private networks.
- the project was referenced in an initiative launched by the European Defense Agency in the field of R&D for Dual Use technologies

UNIVERSITA' DEGLI STUDI DELL'AQUILA

EUROPEAN DEFENCE AGENCY



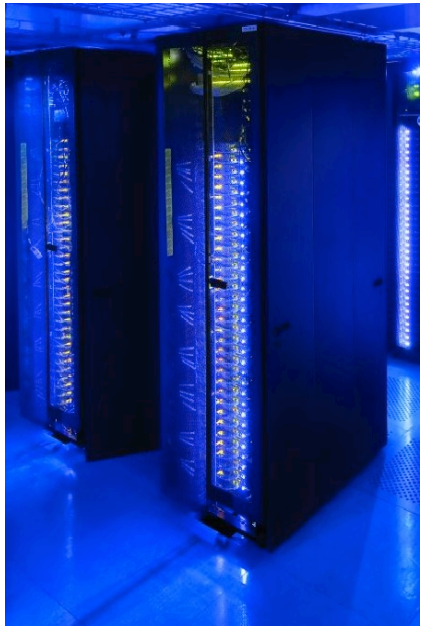
Cyber Trainer features

UNIVERSITA' DEGLI STUDI DELL'AQUILA

- Create an environment dedicated to the study of ICT network security based on modeling, simulation and emulation techniques
- flexibly reproduce different cyber defense / attack scenarios
- sharing of operational experience of personnel, for technological, organizational and procedural aspects
- security of large networks, both civil and military, and critical infrastructure protection.

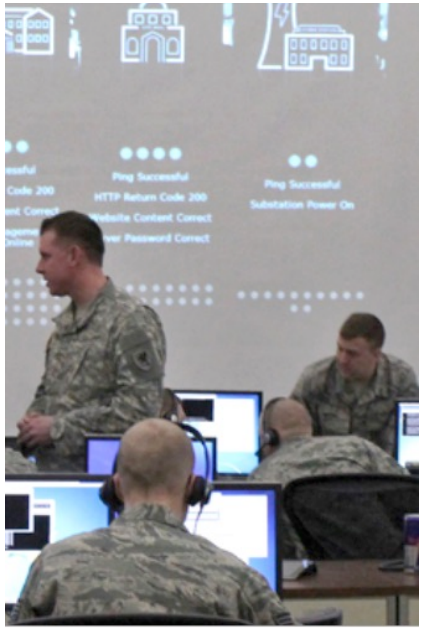
UNIVERSITA' DEGLI STUDI DELL'AQUILA

Distinctive features of the Cyber Trainer project



TECHNOLOGY

- Modeling
- Simulation
- Emulation



APPLICATION

- Formazione
- Pianificazione
- Testing
- Supporto alle decisioni

DUAL USE

CIVIL / DEFENSE

not *dual technology*
for *dual market*,
but *single technology*
for *multiple market*

Cyber Trainer Partners

The Cyber Trainer project can count on a system of territorial, multidisciplinary and complementary skills focused on:

- advanced training in network technologies
- cybersecurity
- ICT
- IoT
- Automotive

An environmental situation that offers excellent guarantees for the transformation of research results into real industrial growth

UNIVERSITA' DEGLI STUDI DELL'AQUILA

LEONARDO
SECURITY & INFORMATION SYSTEMS

UNIVERSITA' DEGLI STUDI DELL'AQUILA

REISS ROMOLI

TEKNE

G & A Engineering
Microelectronics for Space

The Cyber Trainer Case studies

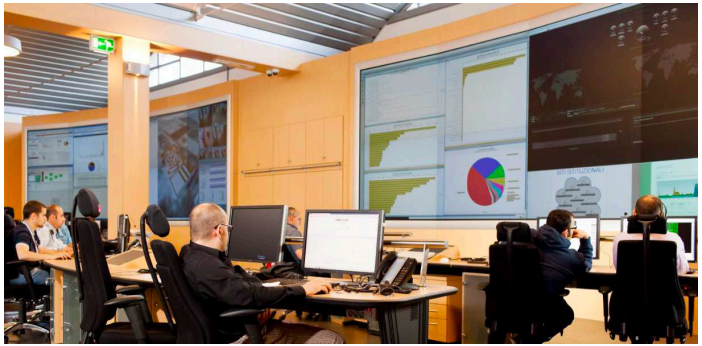
UNIVERSITA' DEGLI STUDI DELL'AQUILA

- training service for Security Operation Centre (SOC) operators
- training of forensic analysis and cryptanalysis specialists
- security and vulnerabilities in IoT devices
- Safety testing of vehicle electronics (Automotive safety)

Use case: training of operators SOC

UNIVERSITA' DEGLI STUDI DELL'AQUILA

- To test a team of a large SOC (Security Operation Center) it is essential to have a particularly complex training scenario
- In particular, if the objective is to train operators (blue team) in the defense of an infrastructure towards a team of attackers (red team), it is necessary to have a real network from transform into "battlefield".
- Training in the physical environment would limit training to the technologies and architectural solutions already present in the organization.
- The use of a virtualized Cyber Training platform, on the other hand, will allow to train the SOC staff in a manner more complete, since it will be possible to deliver virtualized scenarios that include very quickly various technologies and security solutions.



Use case: training of forensic analysis and cryptanalysis specialists

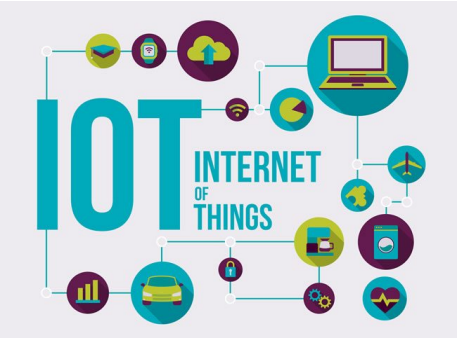
UNIVERSITA' DEGLI STUDI DELL'AQUILA

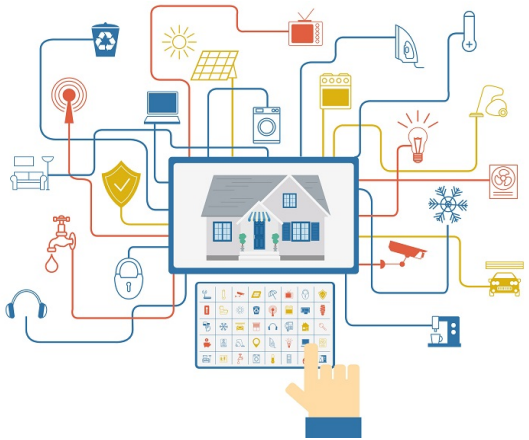
- specificity of this activity, mainly aimed at training in techniques for examining
- digital devices following the processes of forensic analysis, such as identification, preservation and the
- recovery of evidence related to incidents and crimes
- reconstruction of a multiplicity of related events in which it would be possible to insert the practice known as Open Source Intelligence (OSINT).
- training activities will be performed in the following areas specialization of forensic analysis:
  - **Computer Forensics**
  - **Network Forensics**
  - **Mobile Forensics**

Use case: safety and vulnerabilities in IoT devices

UNIVERSITA' DEGLI STUDI DELL'AQUILA

- The security problems in the IOT are a serious concern as they have the power to cause, in addition to potentially huge financial damage, physical destruction, loss of life human resources and non-recoverable environmental damage.
- The risk factor related to the IoT is unique in that brings together many cutting-edge technologies, including cloud, mobility, big data, as well as interconnected micro-sensors, gateways and management platforms.
- The project is focusing on two widely used protocols
- Bluetooth low energy (BLE)
- Zigbee



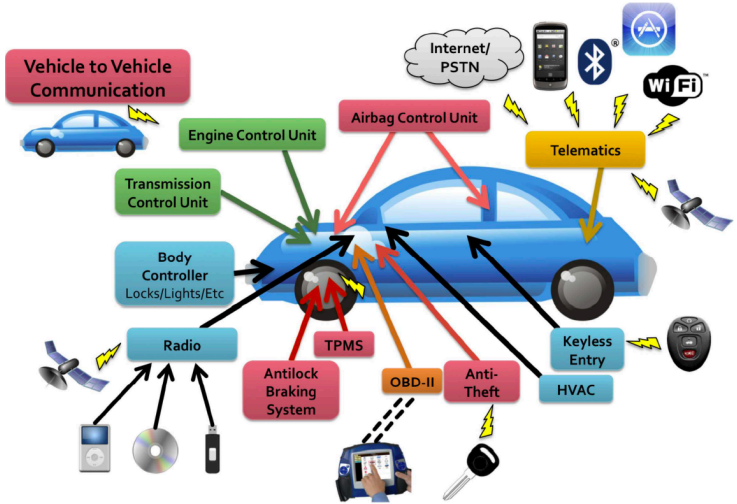


Use case: Vehicle electronics safety test

UNIVERSITA' DEGLI STUDI DELL'AQUILA

- Up until 20 years ago, automotive safety was limited to locks and other mechanical devices (steering wheel lock, pedal lock), or small isolated electronic devices;

- Today, vehicles use powerful digital "infotainments" and distributed control and "safety" functions, which include up to 100 million lines of code, and up to 100 Electronic Control Units (ECUs) per each vehicle and multiple heterogeneous and interoperating buses. At the same time, wireless interfaces connect the car with the surrounding environment, turning the vehicle into an Internet node almost online 24 hours. This situation exposes the modern vehicle to the risk of possible hacker attacks aimed at obtain information on passengers (for example, the traceability of the car's position and interception of communications), or attacks on the safety of the moving vehicle itself.



Where is cryptography in the project?

- short answer: Everywhere! ☺
- Let's have a glimpse of two application in the project
  - digital signature
  - lightweight cryptography

Digital signature: what is it?

UNIVERSITA' DEGLI STUDI DELL'AQUILA

- A *digital signature* is a string of bits associated to a message that allows the authentication of the signer of the message using his public key, independently from the content of the message.

- A digital signature is typically based on:
  - Hash functions + public key algorithms

Digital signature: what is it?

UNIVERSITA' DEGLI STUDI DELL'AQUILA

A digital signature satisfies 3 properties:

1. Authentication: the receiver can verify the identity of the signer.
2. Non-repudiation: the signer cannot deny to have signed a message having his signature
3. Integrity: the enemy cannot alter the message signed by the sender without invalidating the signature.

Digital signature: what is it?

UNIVERSITA' DEGLI STUDI DELL'AQUILA

A digital signature scheme consists of three algorithms:

1. Key generation algorithm

   The algorithm selects a private key, and the corresponding public key, uniformly at random from a set of possible private keys.

2. Signing algorithm

   Given a message and a private key, this algorithm produces a signature.

1. Verification algorithm

   Given a message, a public key and a signature, this algorithm returns "true" or "false" depending on whether the signature is valid for the message.

Digital signature: Eve ("eavesdropper")

UNIVERSITA' DEGLI STUDI DELL'AQUILA

If an attacker is able to construct a valid message-signature pair (m, s), we say that Eve has found a forgery.

The problem is that the verification algorithm returns "true" even if the

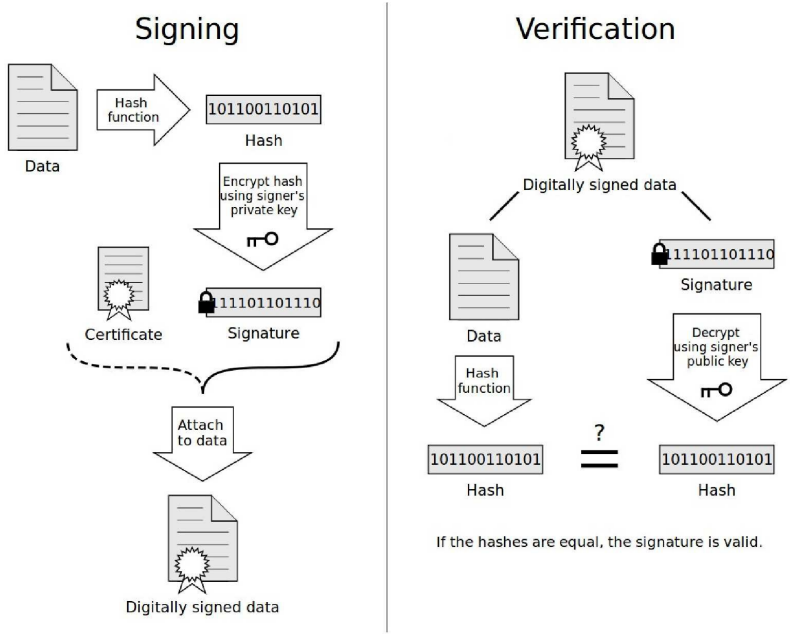
message was not signed by the sender ().

There are different types of attack that are commonly considered:

- total break: Eve is able to determine Bob's private key, therefore she can create valid signatures on any message.
- selective forgery: Eve is able, with some non-negligible probability, to create a valid signature for a class of messages.
- existential forgery: Eve is able, with some non-negligible probability, to forge a signature for at least one message.

Digital signature

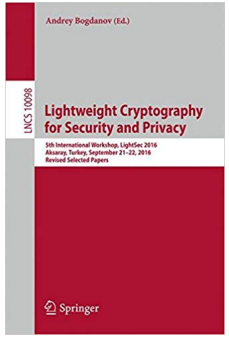
To avoid these types of attacks, digital signature commonly combines hash functions and public key cryptosystems.

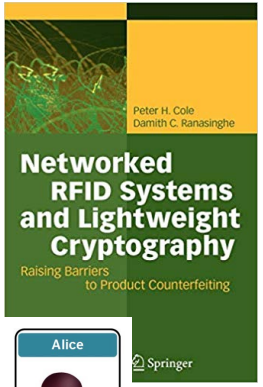


Lightweight cryptography

UNIVERSITA' DEGLI STUDI DELL'AQUILA

- It is easy to misunderstand "lightweight" as less secure. Although devices to be protected are constrained in resources, but attackers are not. So we need security techniques and mechanisms that are lightweight in resource consuming, but NOT in security weight.
- On August 27, 2018 NIST (U.S. National Institute of Standards and Technology) has published a call for algorithms to be considered for lightweight cryptographic standards.





Light-weight Crypto:
Asymmetric Encryption

CYBER ACADEMY

WHAT IS LIGHTWEIGHT CRYPTOGRAPHY?

- Lightweight cryptography has been a very important for the last few years, driven by the lack of primitives capable to run on devices with very low computing power.
- We can think for instance of RFID tags, sensors in wireless sensor network or, more generally, small internet-enabled appliances expected to flood the markets as the Internet of Things (IoT) arises.
- At the core of lightweight cryptography is a trade-off between Lightweightness and
  security.
- Many cryptographers have addressed these issues by suggesting lightweight stream ciphers, block ciphers, hash function and recently one-pass authenticated encryption.

Lightweight Cryptographic Mechanisms

Embedded devices often have inherent limitations in terms of processing power, memory, storage and energy. The cryptographic functionality that ESs utilize to provide tamper resistant hardware and software security functions has direct impact on the system's:

- **Size:** Memory elements constitute a significant part of the module's surface.
- **Cost:** Directly linked to the surface of the component.
- **Speed:** Optimized code provides results faster.
- **Power Consumption:** The quicker a set of instructions is executed, the quicker the module can return to an idle state or be put in sleep mode where power consumption is minimal.

LIGHTWEIGHT CRYPTOGRAPHY LOUNGE

- Lightweight Block Ciphers
- Lightweight Hash Functions
- Lightweight Stream Ciphers
- Lightweight One-pass Authenticated Ciphers

Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica
Università degli Studi dell'Aquila

UNIVERSITA' DEGLI STUDI DELL'AQUILA

Ing. Francesco Tarquini – francesco.tarquini@univaq.it