RESCUE IN UNDERGROUND FACILITIES

NEW TECHNOLOGY NEW RISKS IN TRANSPORT FACILITY

Roma, 3 Marzo 2011

MINISTERO dell'INTERNO
Corpo Nazionale dei Vigili del Fuoco
DIPARTIMENTO dei VIGILI del FUOCO
del SOCCORSO PUBBLICO
e della DIFESA CIVILE

a cura di

Dr. Pistilli Marcello

BU Information Security
Eustema Spa

Intelligent Transport Systems

On february 27, 2012, the european directive on **Intelligent Transport Systems** (ITS) will be operative

Intelligent Transport Systems are used to manage:

- Public and private transportation
- Fleet and freight
- Automatic payments
- Veichles control
- Emergencies

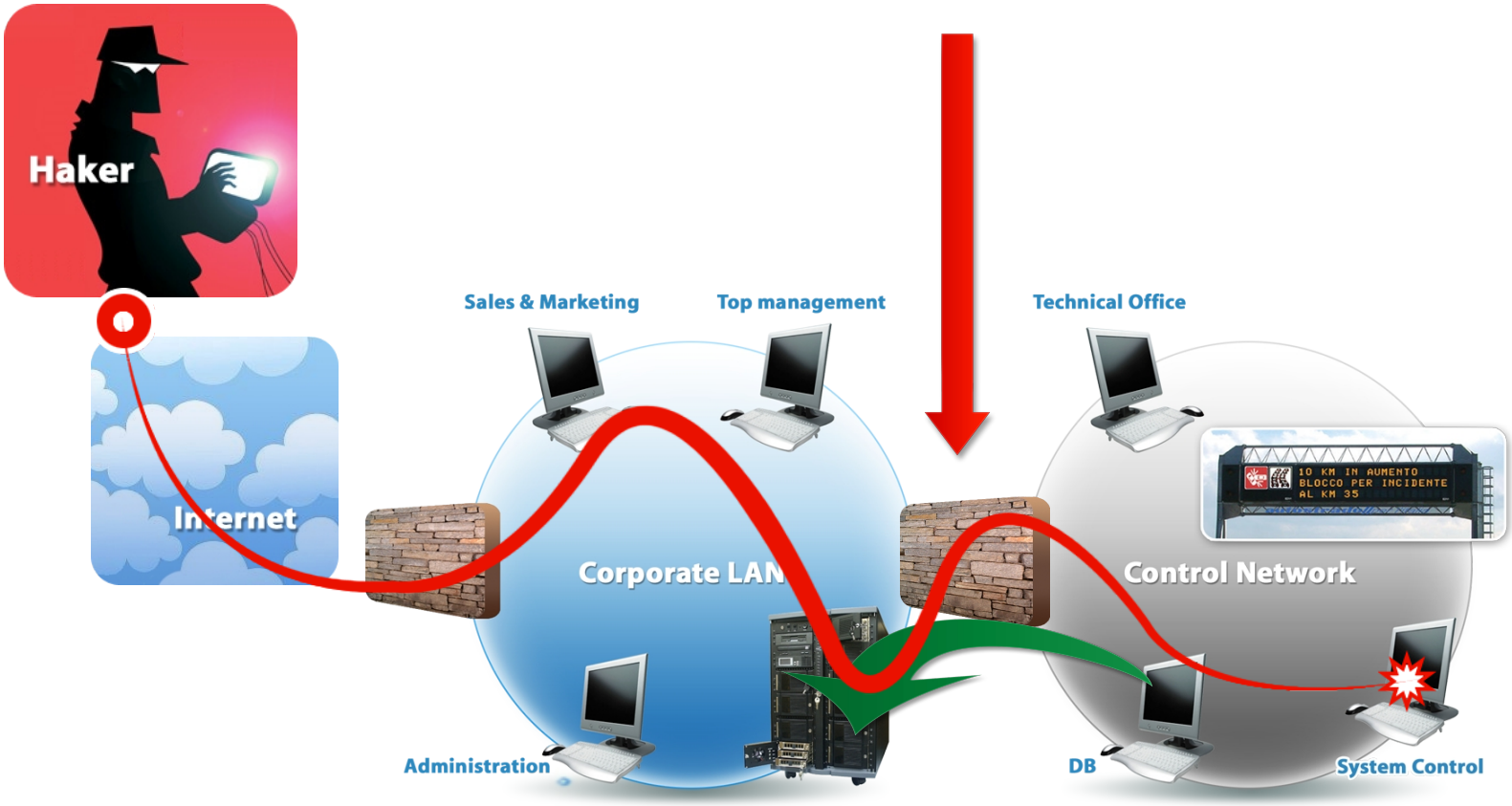
EUSTEMA

Control systems are increasingly connected to local networks of firms, mainly public companies, and from these to Internet

In most of the case
they run on Windows OS,
often with obsolete software

end of security by obscurity!

Network



EUSTEMA

Hacker Vs. Cars

Often, new generation cars have smartphone connectivity and diagnostic systems managed by satellite

Experts are aware of information security problems into the car for at least five years (cyber attacks, viral infections…)

EUSTEMA

Hacker Vs. Cars

Connecting to a diagnostic system, a remote-controlled device allows to outrage the onboard's information systems…

CAESS researchers (Center for Automotive Embedded Systems Security - University of Washington/California) were able to:

- Turn off the brakes
- Put the engine out
- Send false alerts to the dashboard
- Lock the car doors with passengers inside

EUSTEMA

Hacked the Dutch Railways

http://www.youtube.com/watch?v=9WxOo5u2dkM&feature=related

Utrecht central station hack

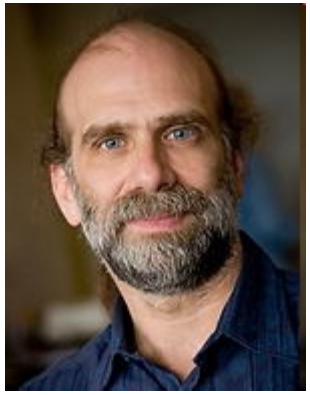
http://www.youtube.com/watch?v=zcmmFQGxMNU&feature=channel

Hacked Dutch road

http://www.youtube.com/watch?v=ZR0U1nyQlD0&feature=channel

"If authentic, it's awesome..."

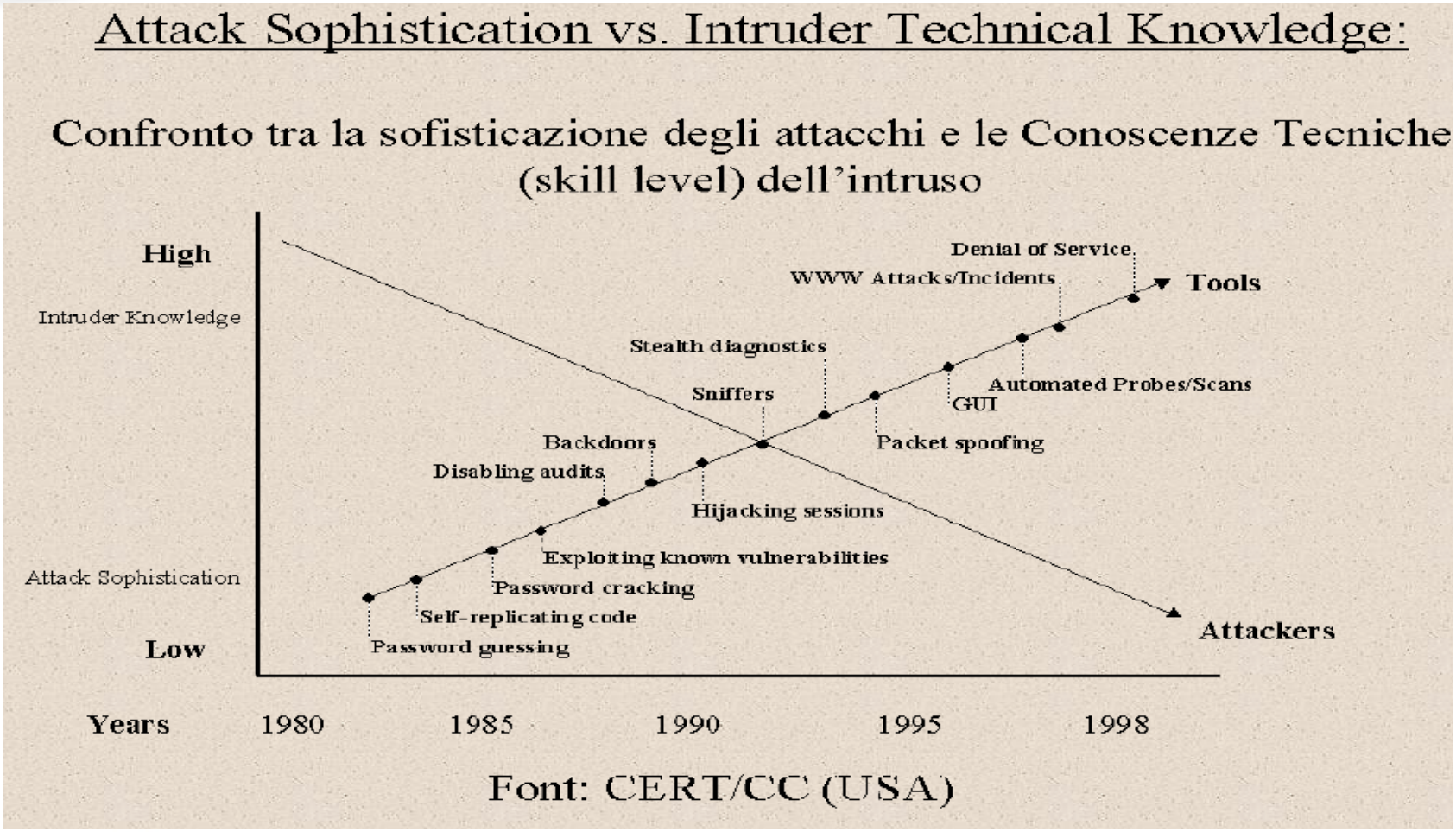
by Schneier on Security, a blog covering security and security technology



Internet offers **a lot** of informations in order to get the best tools to attack websites, databases…

At the same time it offers useful tips to identify configurations errors, security holes…

This leads to the proliferation of unethical people



Fonte Raul Chiesa

Hackers are becoming day by day real **criminals**…

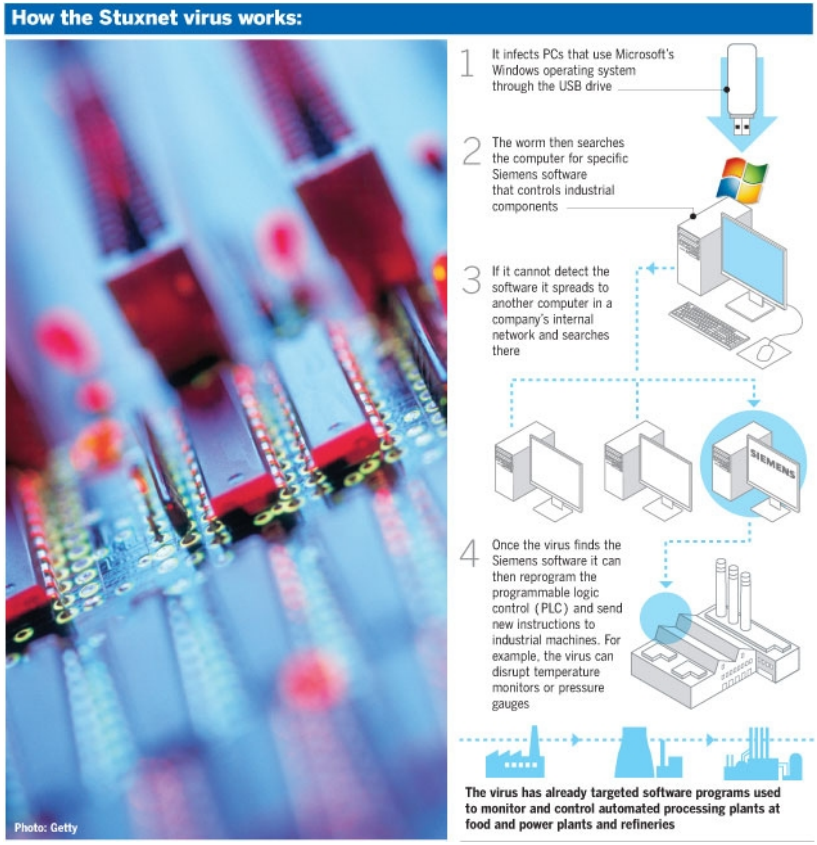
The expert Raul Chiesa divided them into three categories:

- **Low level hackers** – who exploit known or specific vulnerabilities
- **High level hackers** – who conduct more sophisticated attacks and have ties to organized crime
- **Industrial espionage and terrorism**

Fonte Raul Chiesa

Stuxnet **is not** just 'another' run of the malware…

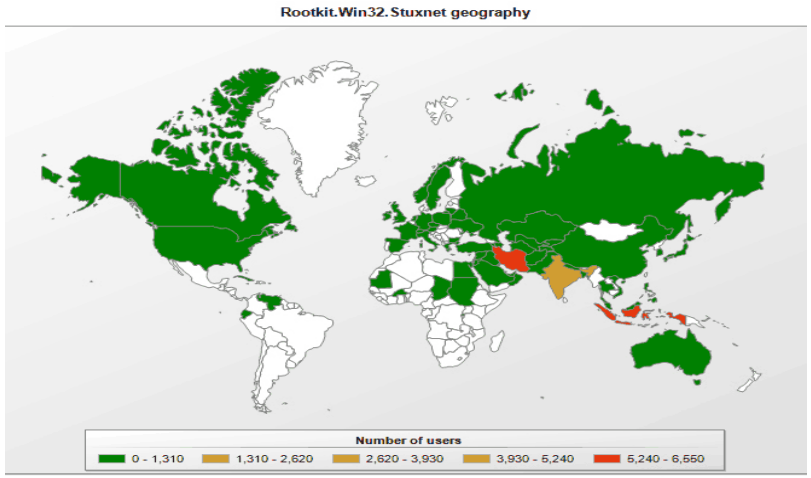
but a highly specialized malware designed to target only Siemens ***Supervisory Control And Data Acquisition*** (SCADA), systems that are configured to control and monitor specific industrial processes



Discovered in July 2010, **Stuxnet** is the first known malware that spies on and subverts industrial systems, and the first to include a programmable logic controller (PLC) rootkit

Stuxnet infects **PLCs** by subverting the **Step-7**, software application used to reprogram these devices.

Other malware may be developed under the rootkit Stuxnet, making **USB attacks** more and more dangerous and hard to eradicate



USB attacks

Source of dangers

A CSI Computer Crime and Security Survey, based on the responses of 494 information security and information technology professionals in United States corporations, government agencies, financial institutions, showed that:

- ***59% of respondents had at least one security problem due to carelessness of an employee (Insider)***
- Only 52% of security problems are due to malware and spyware

Damage due to insider:

- theft of computer data secrets
- use of illegal software
- downloading pornography, copyrighted music and programs
- malware infections

EUSTEMA

Knowing the Insider

In most of cases (73%), the Insider is an employee who has suffered a pay cut or was fired. Usually the Insider subtracts confidential data before being removed from company

Fonte RSA Security

Wikileaks

"The new modern face of censorship is to prevent leaks of confidential information. But as far as to invent new protections, you can always devise schemes to circumvent"

Julian Assange

EUSTEMA

A successful attack

5 USB keys
left in the parking lot
of a bank

person
who finds
the USB key

...and even
the ATTACK starts!

the same person
uses the key
on his own netbook
(Corporate LAN)

the remote control starts

EUSTEMA

The human factor plays a key role in every computer process:

- It affects every software design and development process
- Without adequate skill, it can itself become a risk
- It influences compliance with corporate security policies
- It affects network devices control and security systems

…It's the **focus** of information security

A proper security policies management is not possible without a **careful acceptation** by top executives and employees

In order to that, the most critical areas are:

- Vulnerability assessment – Infrastructure compliance
- Legacy applications and web assessment
- Endpoint security
- Security policies compliance

Eustema is a consultancy company specialized in software engineering operating since 1989 in Italian marketplace

Leading supplier of IT software solutions, including:

- **business intelligence**
- **business process management and workflow**
- **system integration**
- **information security**
- **web site**
- **apps and interactive**

Dr. Marcello Pistilli

BU Information Security

m.pistilli@eustema.it

EUSTEMA

Via Carlo Mirabello, 7
00195 Roma
Tel. +39.06.37.49.31
Fax +39.06.37.49.33.51
www.eustema.it

AZIENDA CON SISTEMA QUALITÀ
CERTIFICATO DA RINA
ISO 9001 - SA 8000 - ISO 20000 - 1