Speech : Francesco Arruzzoli
Cyber Security Analyst

CMC Lugano 2016 - Anatomy of a Cyber Attack : the new level of breach

We have connected our economy and society using platforms designed for ***sharing*** *information… **not protecting** it..*

… and organizations must trust people every day.

States rapidly embrace new technology to better serve constituents, efficiently

Cloud

Social Media

Mobile

Online

State agencies continue to be a target

States collect, share and use large volumes of the most comprehensive citizen information.

The large volume of information makes states an attractive target for both organized cyber criminals and hacktivists.

Innovations that drive growth also create cyber risk

Speech : Francesco Arruzzoli
Cyber Security Analyst

Threat actors exploit weaknesses that are byproducts of business growth and innovation.

- New citizen service models
- New sourcing and supply-chain models
- New applications and mobility tools
- Use of new technologies for efficiency gains and cost reduction

Perfect security is not feasible. Instead, reduce the impact of cyber incidents by becoming:

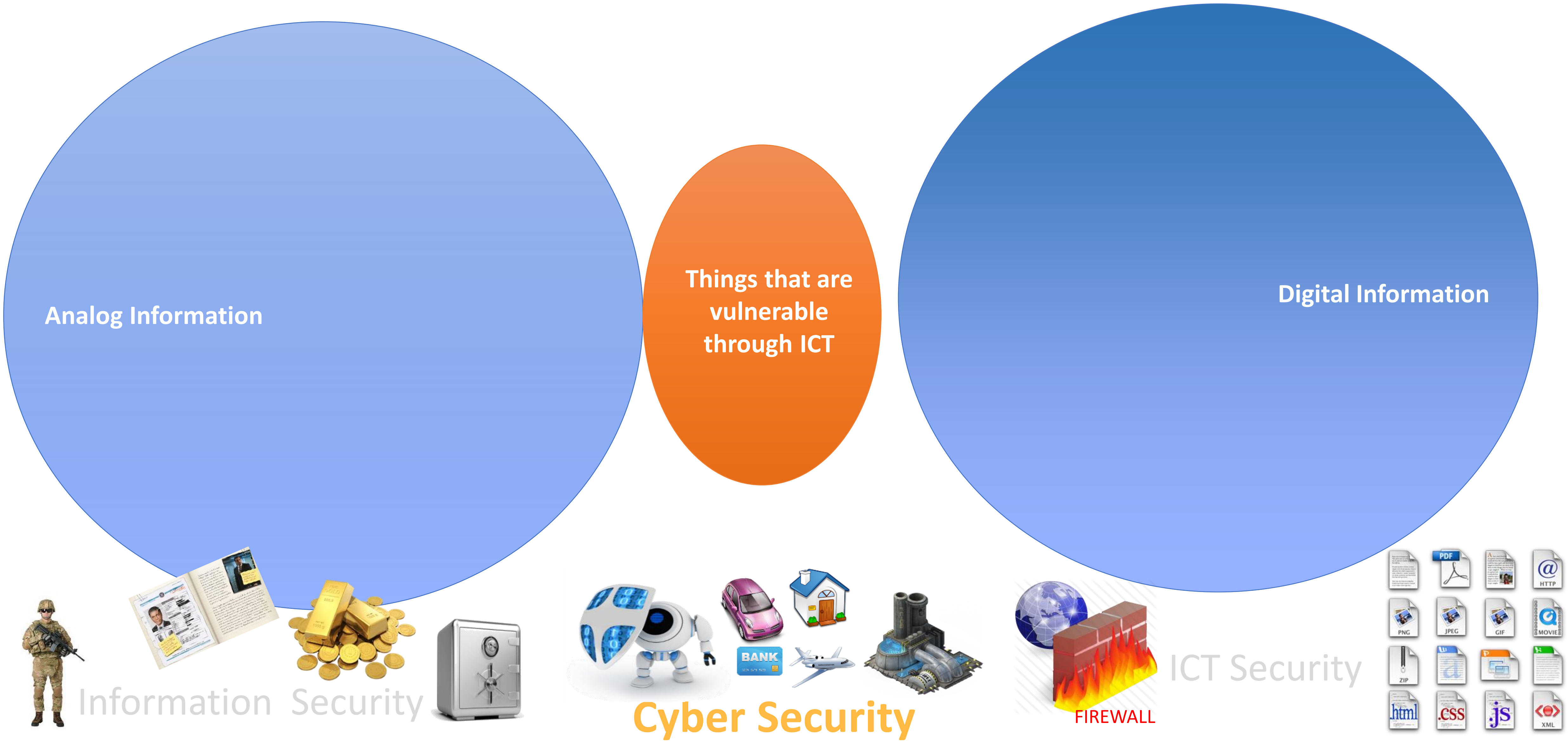
SECURE — Enabling business innovation by protecting critical assets against known and emerging threats across the ecosystem

VIGILANT — Gaining detective visibility and preemptive threat insight to detect both known and unknown adversarial activity

RESILIENT — Strengthening your ability to recover when incidents occur

Cyber risk management is a positive aspect of managing business performance.

Our Vision



Analog Information

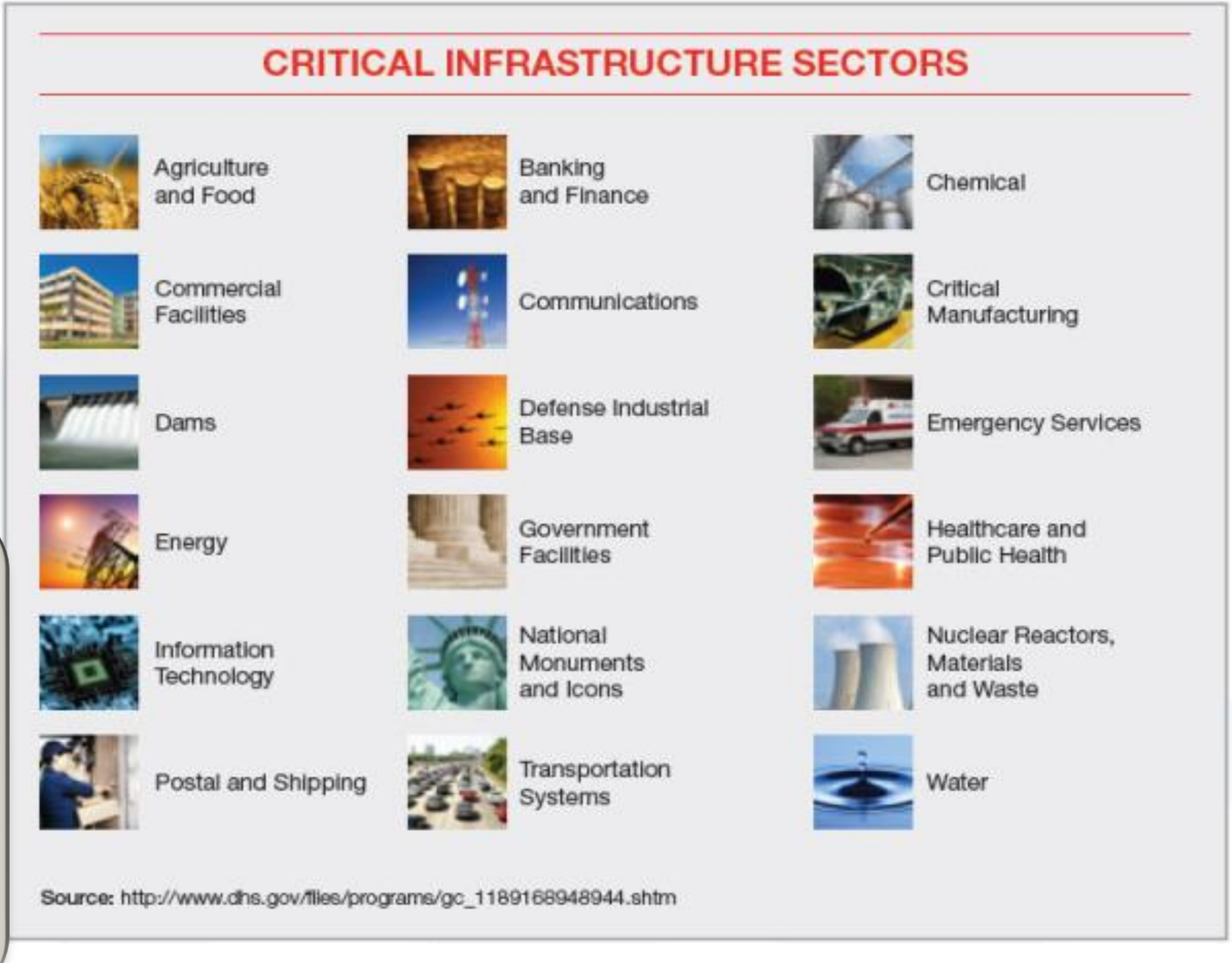
Things that are vulnerable through ICT

Digital Information

Information Security

Cyber Security

ICT Security



CRITICAL INFRASTRUCTURE SECTORS

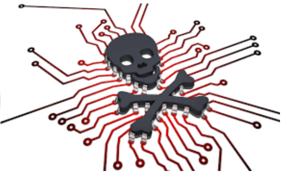
- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Healthcare and Public Health
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials and Waste
- Postal and Shipping
- Transportation Systems
- Water

Source: http://www.dhs.gov/files/programs/gc_1189168948944.shtm

Understand threats and motives relevant to your environment

Who might attack?

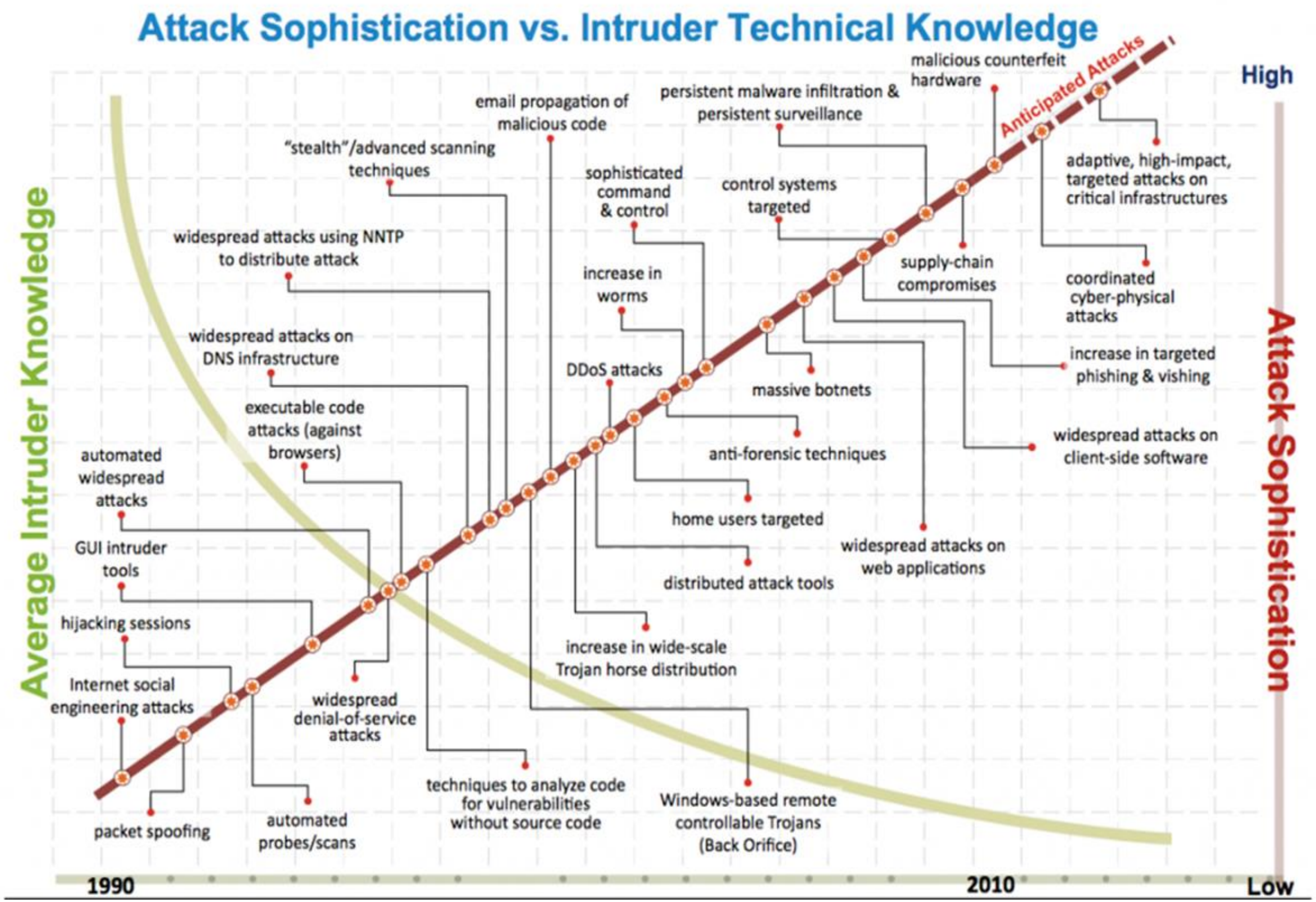
What are they after, and what are the key business risks we need to mitigate?



What tactics might they use?

IMPACTS / ACTORS	Financial theft/fraud	Theft of IP or strategic plans	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life safety	Regulatory
Organized criminals	🟥	□	□	□	🟨	□	🟦
Hactivists	□	□	■	□	■	□	🟦
Nation states	□	□	■	■	□	■	🟦
Insiders/ partners	■	□	🟨	□	🟨	□	🟦
Skilled individual hackers	▨	□	🟨	□	🟨	□	🟦

KEY 🟥 Very high 🟨 High ▨ Moderate □ Low



Source: Software Engineering Institute & Carnegie Mellon

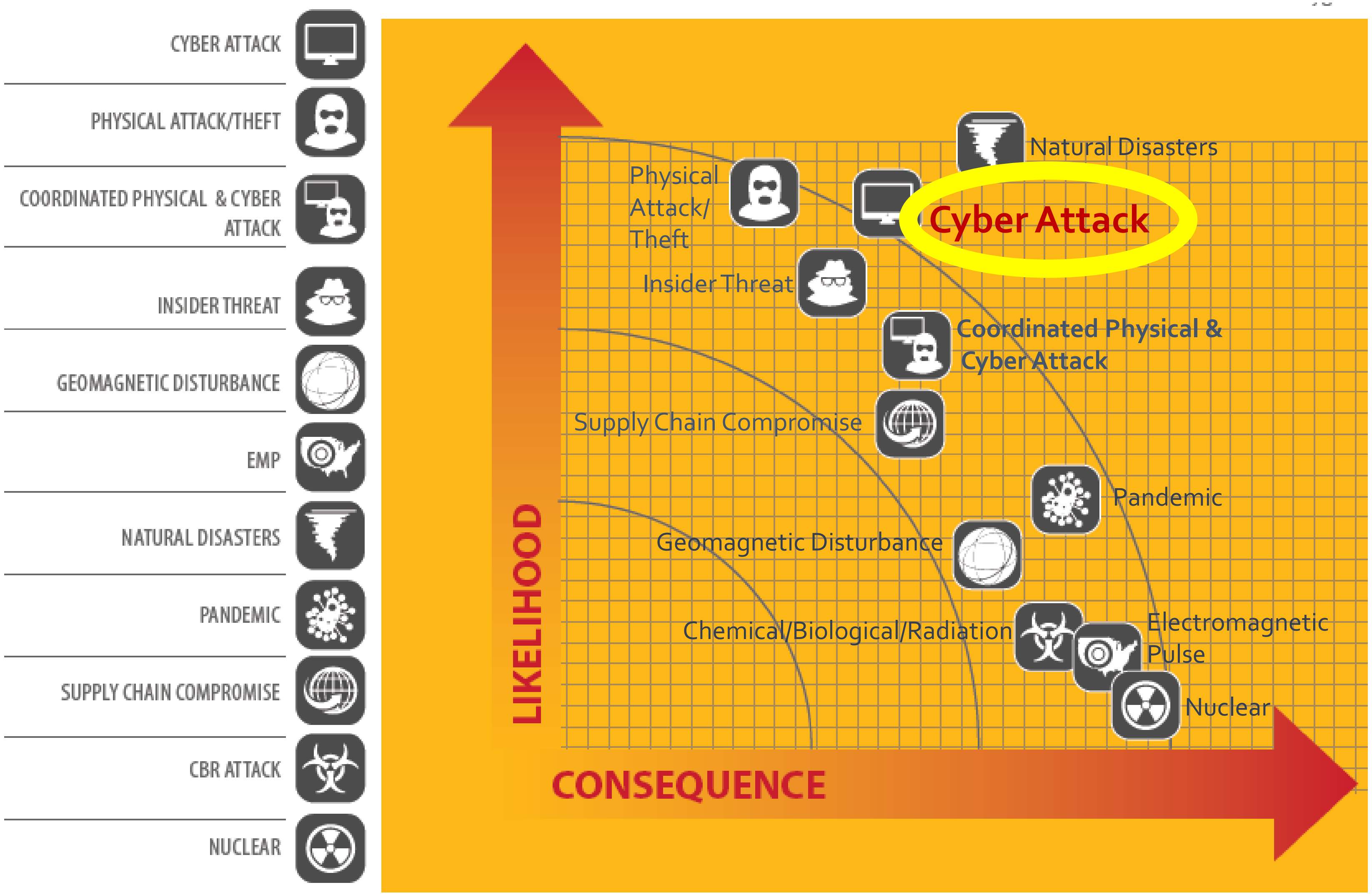
«THE POWER WITHOUT KNOWLEDGE PRODUCES EVIL»

Socrate

An example: Attack Road Signs

Speech : Francesco Arruzzoli
Cyber Security Analyst

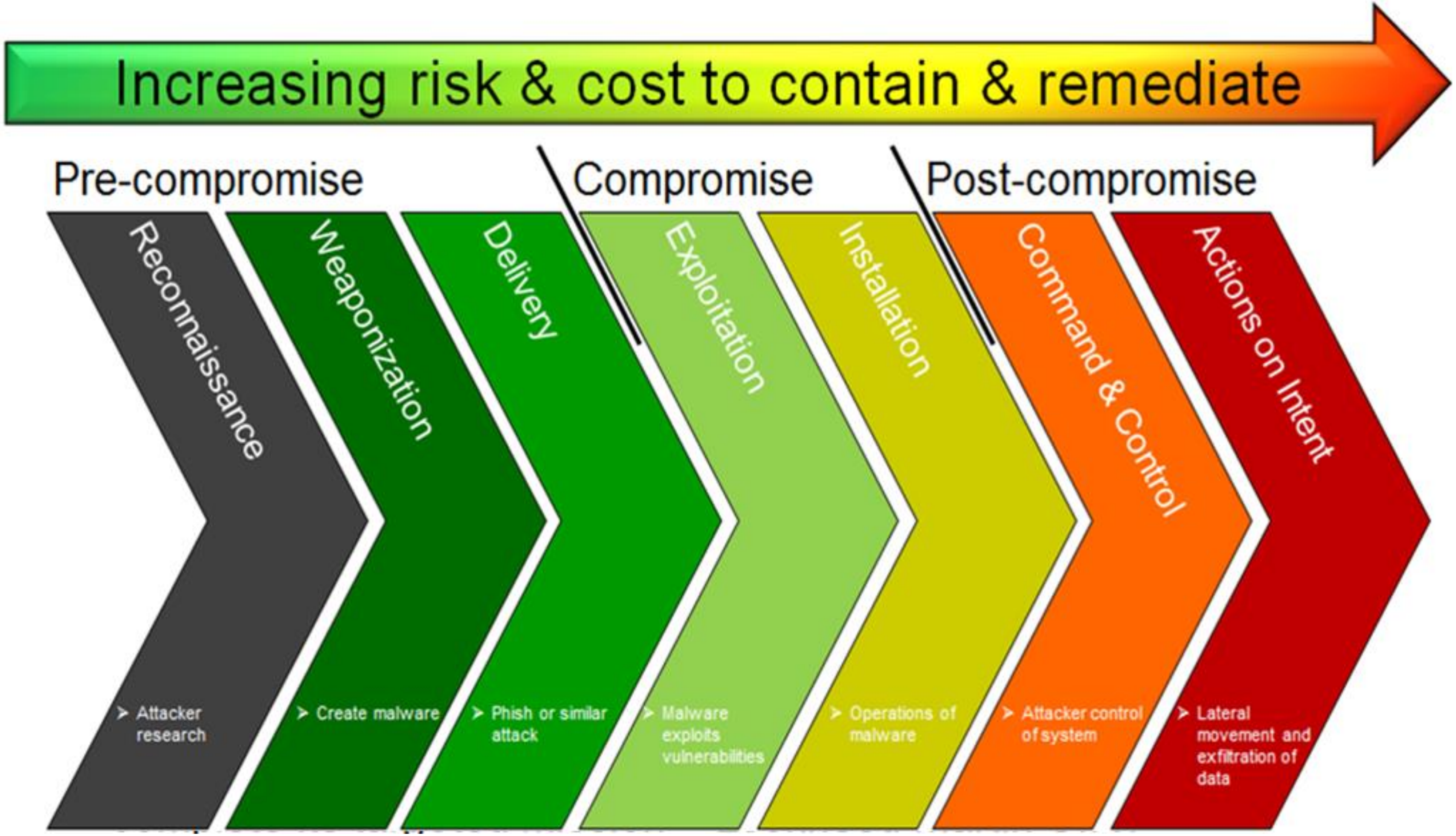
Threat Landscape Example : Electric Utility Sector



Source: The Chertoff Group

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

Sun Tzu, *The Art of War*



Increasing risk & cost to contain & remediate

Pre-compromise

Compromise

Post-compromise

Reconnaissance
- Attacker research

Weaponization
- Create malware

Delivery
- Phish or similar attack

Exploitation
- Malware exploits vulnerabilities

Installation
- Operations of malware

Command & Control
- Attacker control of system

Actions on Intent
- Lateral movement and exfiltration of data

Speech : Francesco Arruzzoli
Cyber Security Analyst

Anatomy of a Cyber Attack : the new level of breach

The AXAN CASE

Anatomy of a Cyber Attack : the new level of breach

ACTIVITY: PENETRATION TEST

PLACE : LONDON

CUSTOMER: AXAN TECHNOLOGY LTD

MISSION : **SHUTDOWN DATACENTER AND STEAL CONFIDENTIAL FILES**

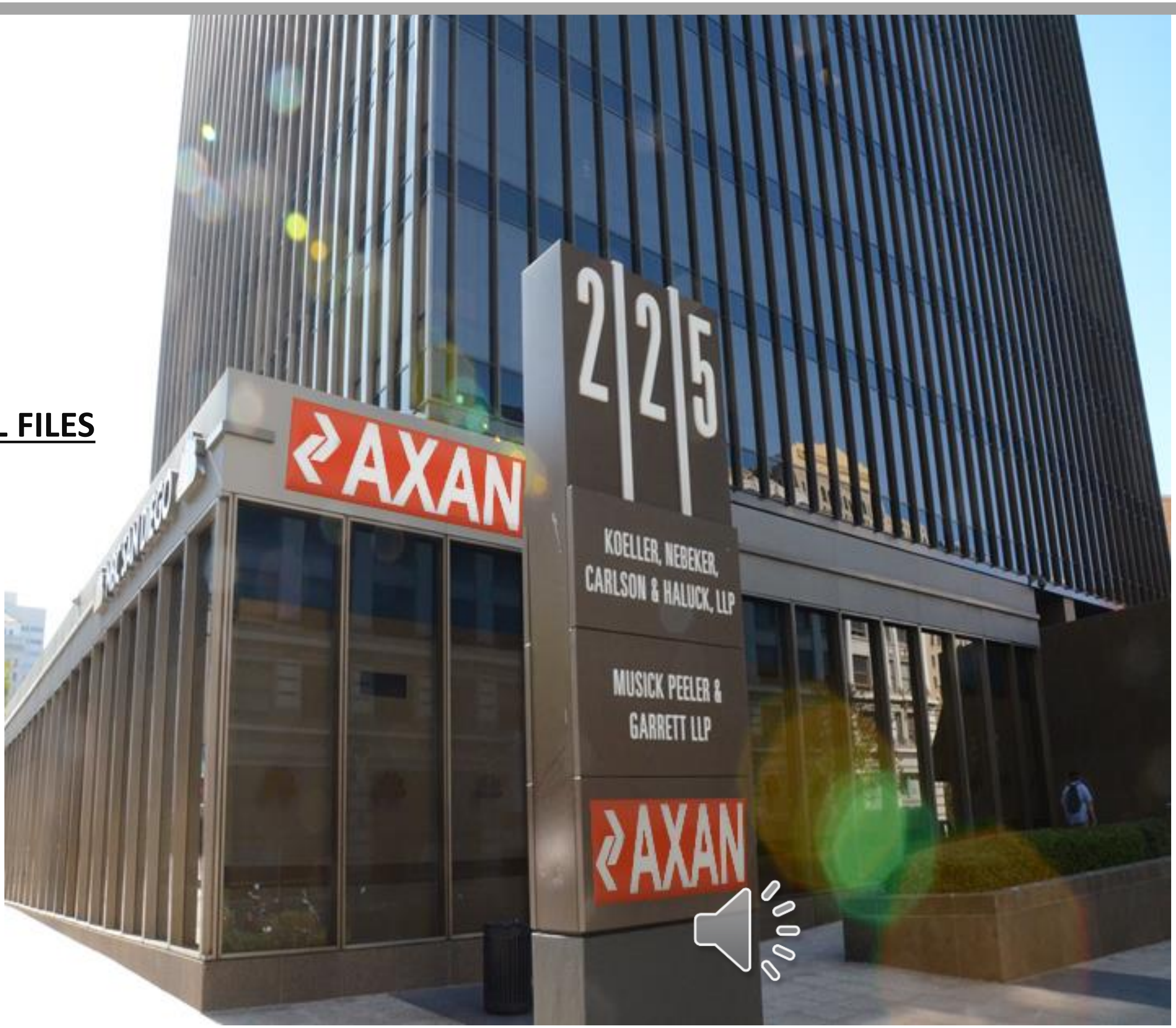
ACTIVITY STATUS:

EXTERNAL PENETRATION TEST
FAILED

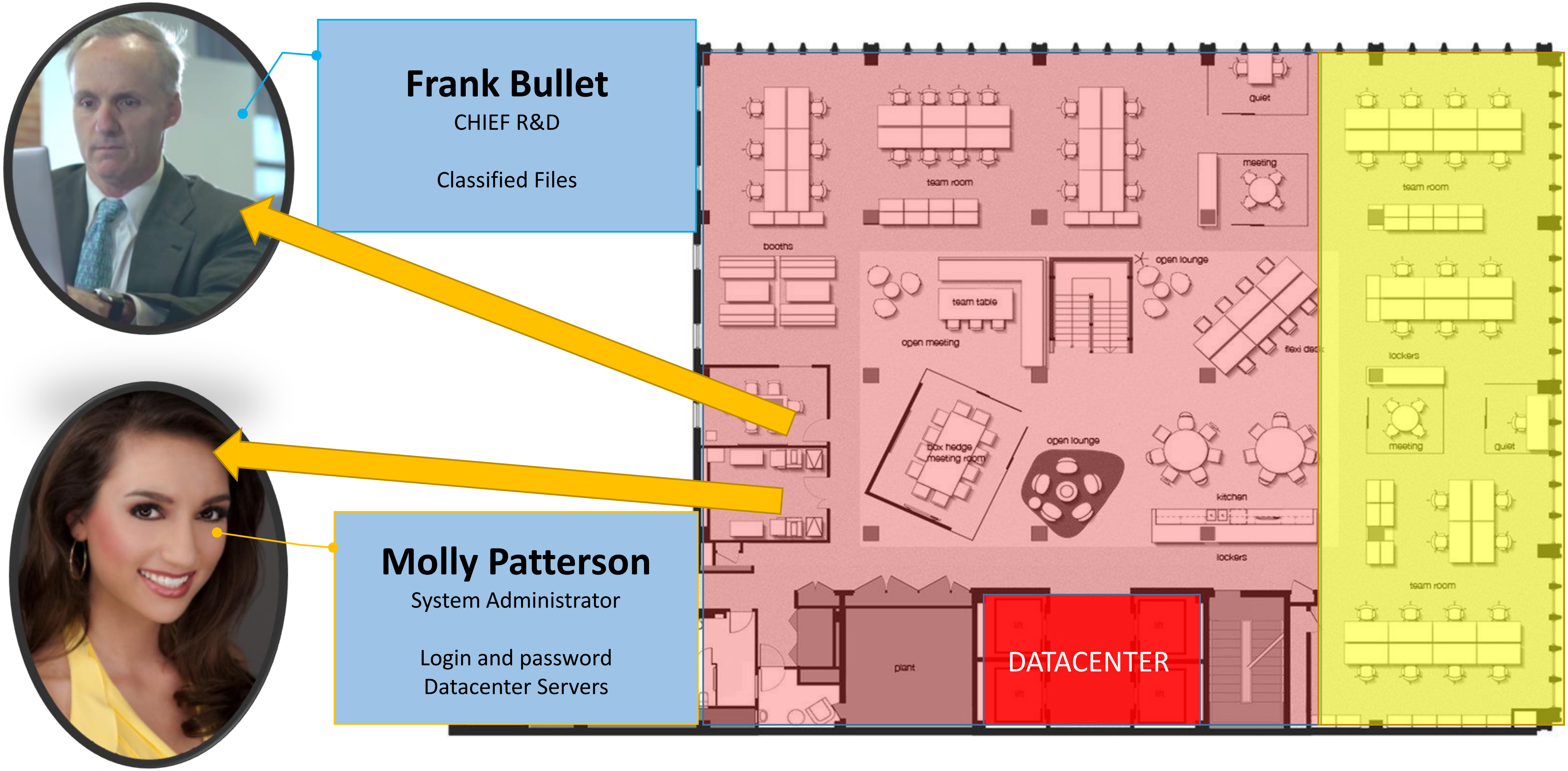
INTERNAL PENETRATION TEST
FAILED

SOCIAL ENGINEERING
FAILED

ACTIVITY IN PROGRESS..


AXAN
2|2|5
KOELLER, NEBEKER, CARLSON & HALUCK, LLP
MUSICK PEELER & GARRETT LLP
AXAN

AXAN



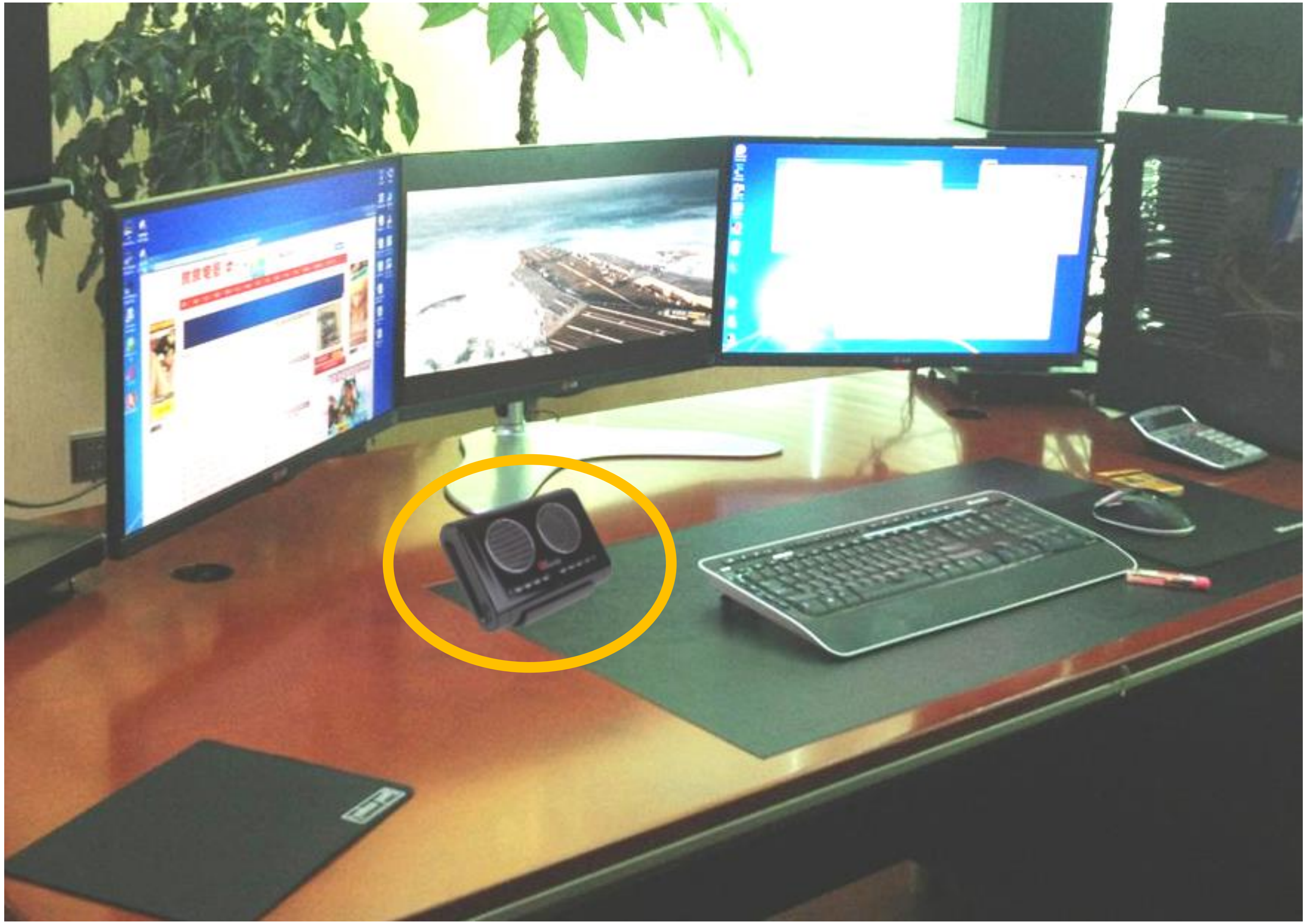
Frank Bullet
CHIEF R&D

Classified Files

Molly Patterson
System Administrator

Login and password
Datacenter Servers

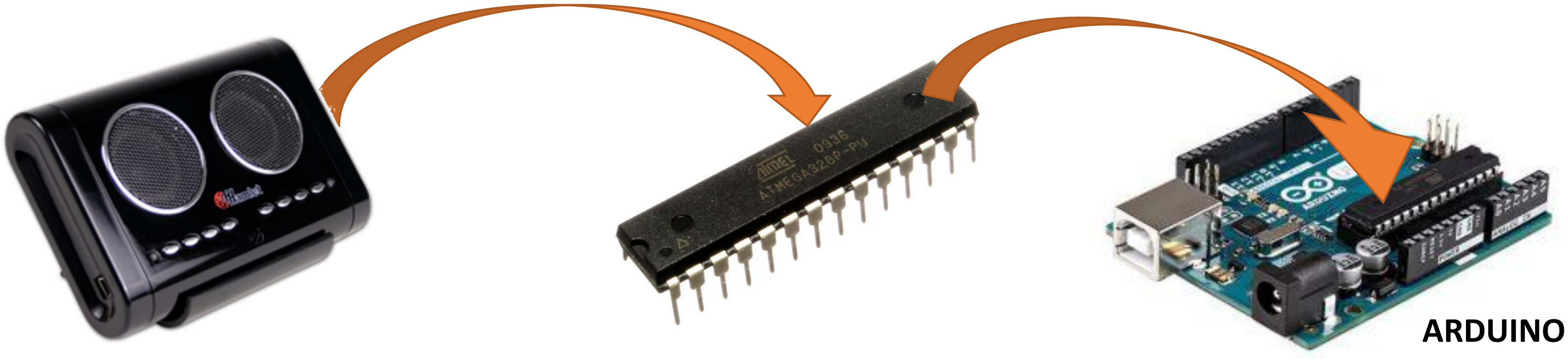
Molly Desktop



the art of deception

USB Speakerphone

ATmega328 microcontroller

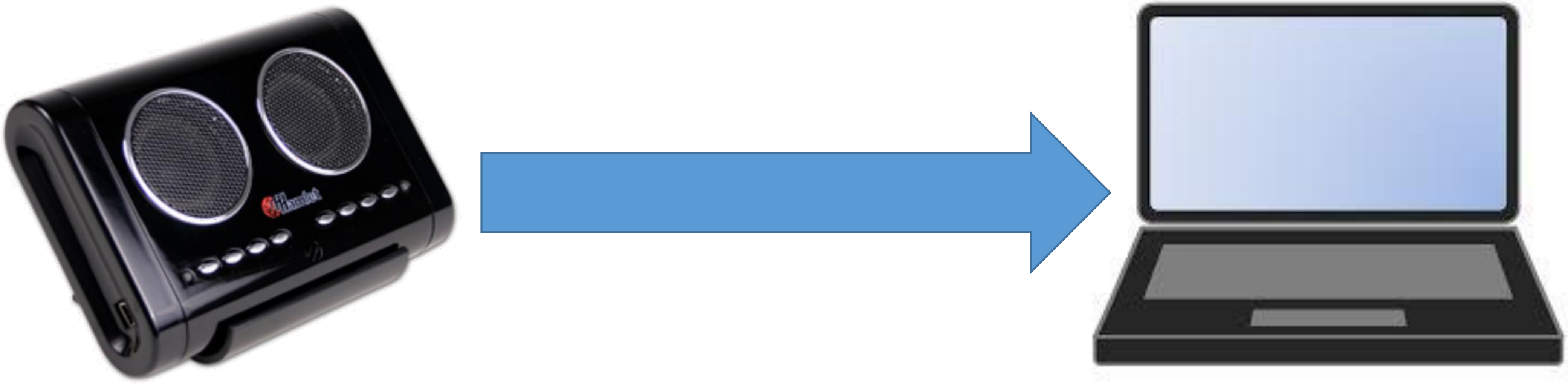


ARDUINO UNO

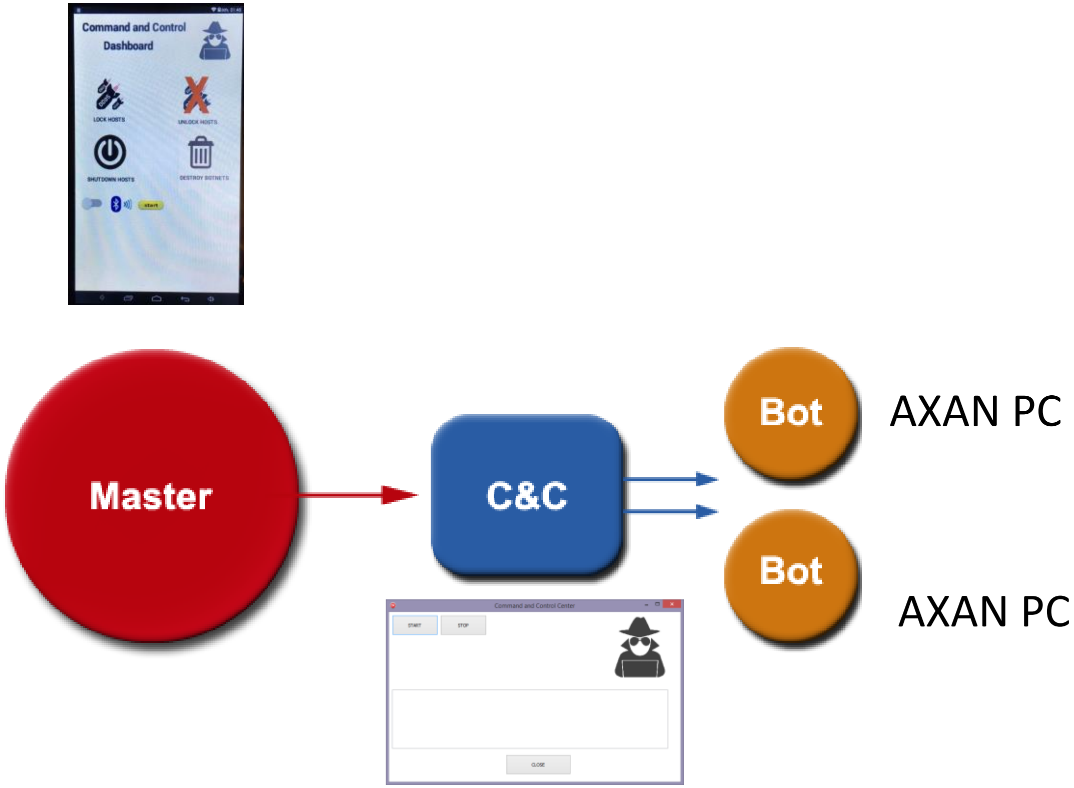
*"If it quacks like a keyboard
and types like a keyboard,
it must be a keyboard."*

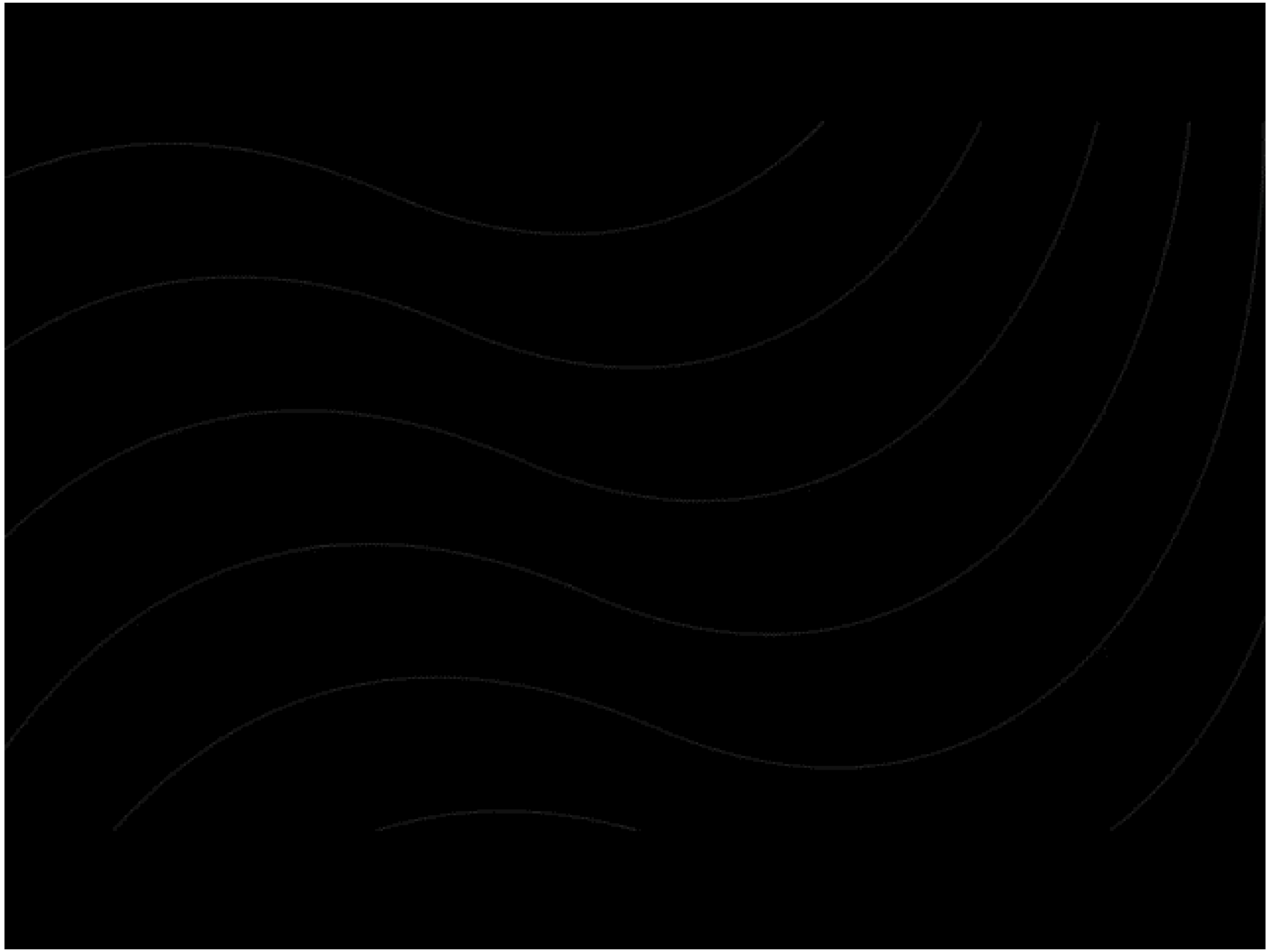
*"Humans use keyboards.
Computers trust humans."*

A very bad USB Speakerphone to inoculate a Botnet



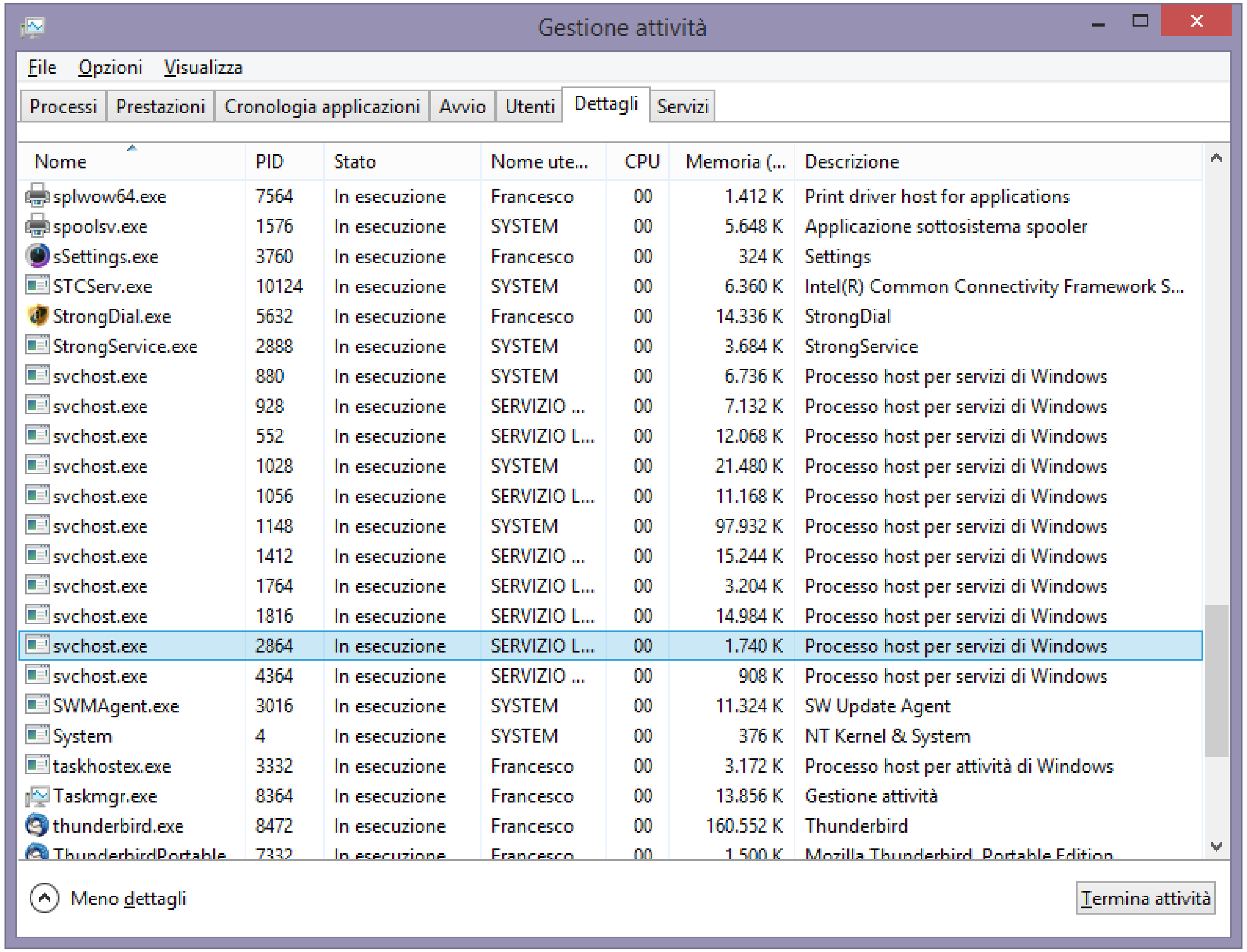
BotNet Architecture





..three days after…

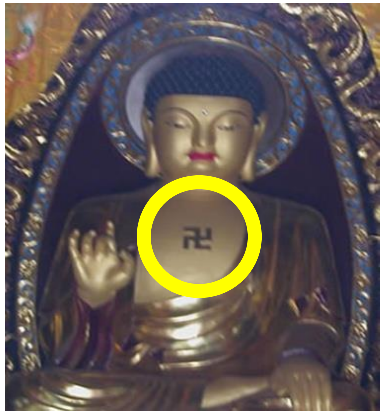
What you see is NOT always what you get



Nome	PID	Stato	Nome ute...	CPU	Memoria (...	Descrizione
splwow64.exe	7564	In esecuzione	Francesco	00	1.412 K	Print driver host for applications
spoolsv.exe	1576	In esecuzione	SYSTEM	00	5.648 K	Applicazione sottosistema spooler
sSettings.exe	3760	In esecuzione	Francesco	00	324 K	Settings
STCServ.exe	10124	In esecuzione	SYSTEM	00	6.360 K	Intel(R) Common Connectivity Framework S...
StrongDial.exe	5632	In esecuzione	Francesco	00	14.336 K	StrongDial
StrongService.exe	2888	In esecuzione	SYSTEM	00	3.684 K	StrongService
svchost.exe	880	In esecuzione	SYSTEM	00	6.736 K	Processo host per servizi di Windows
svchost.exe	928	In esecuzione	SERVIZIO ...	00	7.132 K	Processo host per servizi di Windows
svchost.exe	552	In esecuzione	SERVIZIO L...	00	12.068 K	Processo host per servizi di Windows
svchost.exe	1028	In esecuzione	SYSTEM	00	21.480 K	Processo host per servizi di Windows
svchost.exe	1056	In esecuzione	SERVIZIO L...	00	11.168 K	Processo host per servizi di Windows
svchost.exe	1148	In esecuzione	SYSTEM	00	97.932 K	Processo host per servizi di Windows
svchost.exe	1412	In esecuzione	SERVIZIO ...	00	15.244 K	Processo host per servizi di Windows
svchost.exe	1764	In esecuzione	SERVIZIO L...	00	3.204 K	Processo host per servizi di Windows
svchost.exe	1816	In esecuzione	SERVIZIO L...	00	14.984 K	Processo host per servizi di Windows
svchost.exe	2864	In esecuzione	SERVIZIO L...	00	1.740 K	Processo host per servizi di Windows
svchost.exe	4364	In esecuzione	SERVIZIO ...	00	908 K	Processo host per servizi di Windows
SWMAgent.exe	3016	In esecuzione	SYSTEM	00	11.324 K	SW Update Agent
System	4	In esecuzione	SYSTEM	00	376 K	NT Kernel & System
taskhostex.exe	3332	In esecuzione	Francesco	00	3.172 K	Processo host per attività di Windows
Taskmgr.exe	8364	In esecuzione	Francesco	00	13.856 K	Gestione attività
thunderbird.exe	8472	In esecuzione	Francesco	00	160.552 K	Thunderbird
ThunderbirdPortable	7332	In esecuzione	Francesco	00	1.500 K	Mozilla Thunderbird, Portable Edition

Adolf Hitler

Nazism



The swastika is a symbol universally known and very old , has vanished in Asia , Mongolia , India and also in Central America . The symbolism of the swastika you can ' observe the large golden statues of Buddha in the center of his chest The symbolism of the swastika is derived from the Sanskrit language and is found in ancient Indian and Chinese scriptures and is part of the symbols representing wisdom .

Homograph attack

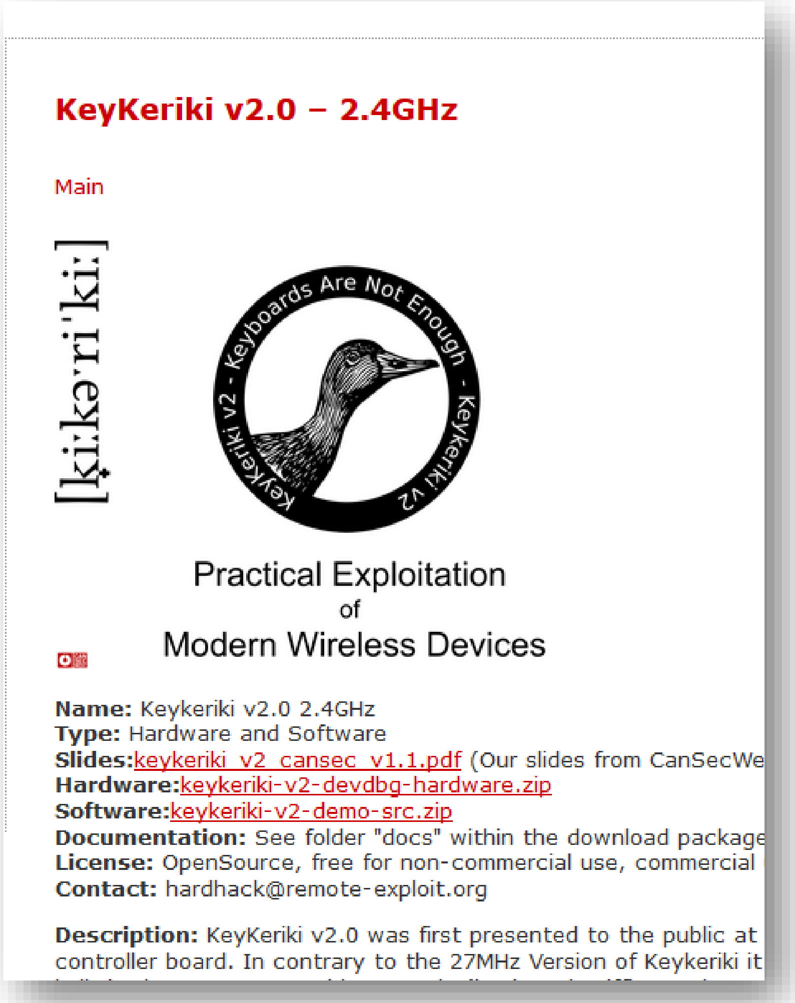
A homograph (from the Greek: ὁμός, homós, "same" and γράφω, gráphō, "write") is a word that shares the same written form as another word but has a different meaning. The **internationalized domain name (IDN) homograph attack** is a way a malicious party may deceive computer users about what remote system they are communicating with, by exploiting the fact that many different characters look alike.

An Example Is Worth a Thousand Words..

URL : www.microsoft.com

Homograph URL : www.microsoft.com

The magnitude of the threat



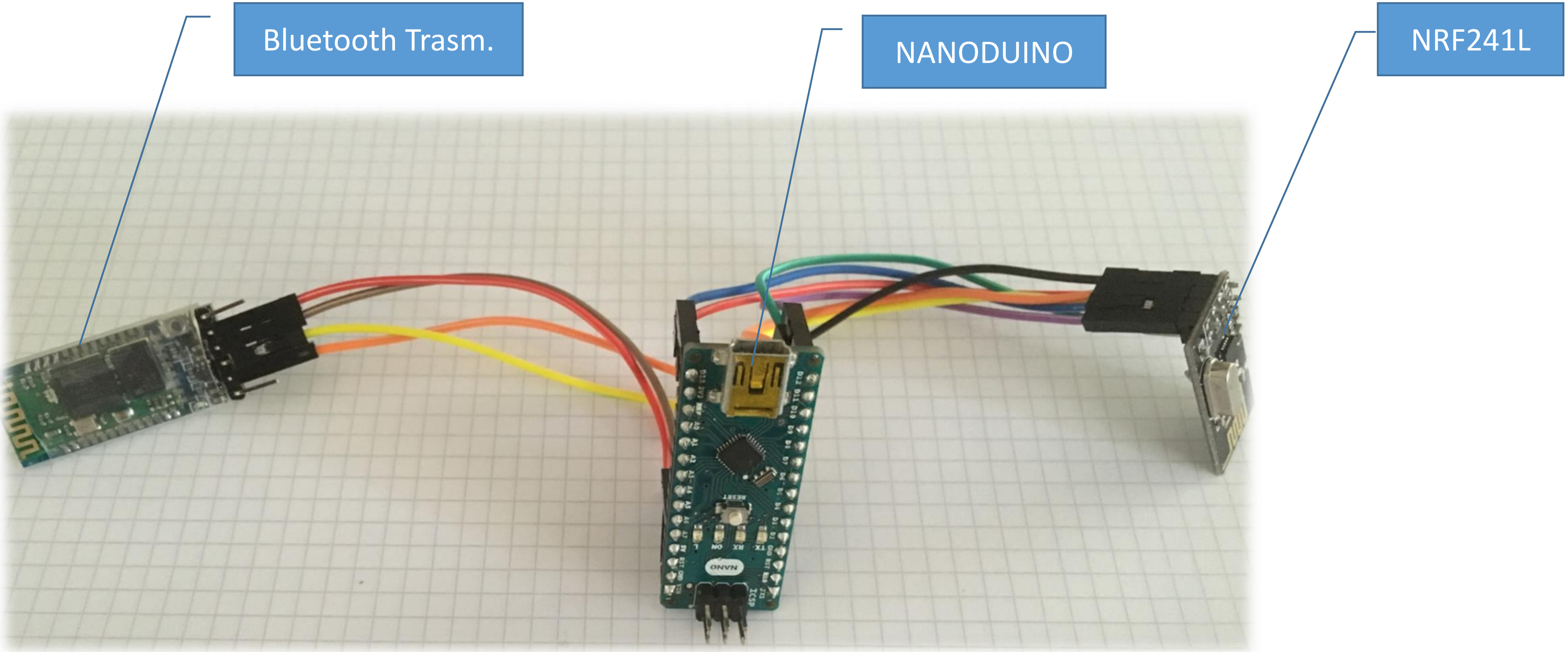
KeyKeriki v2.0 – 2.4GHz

Main

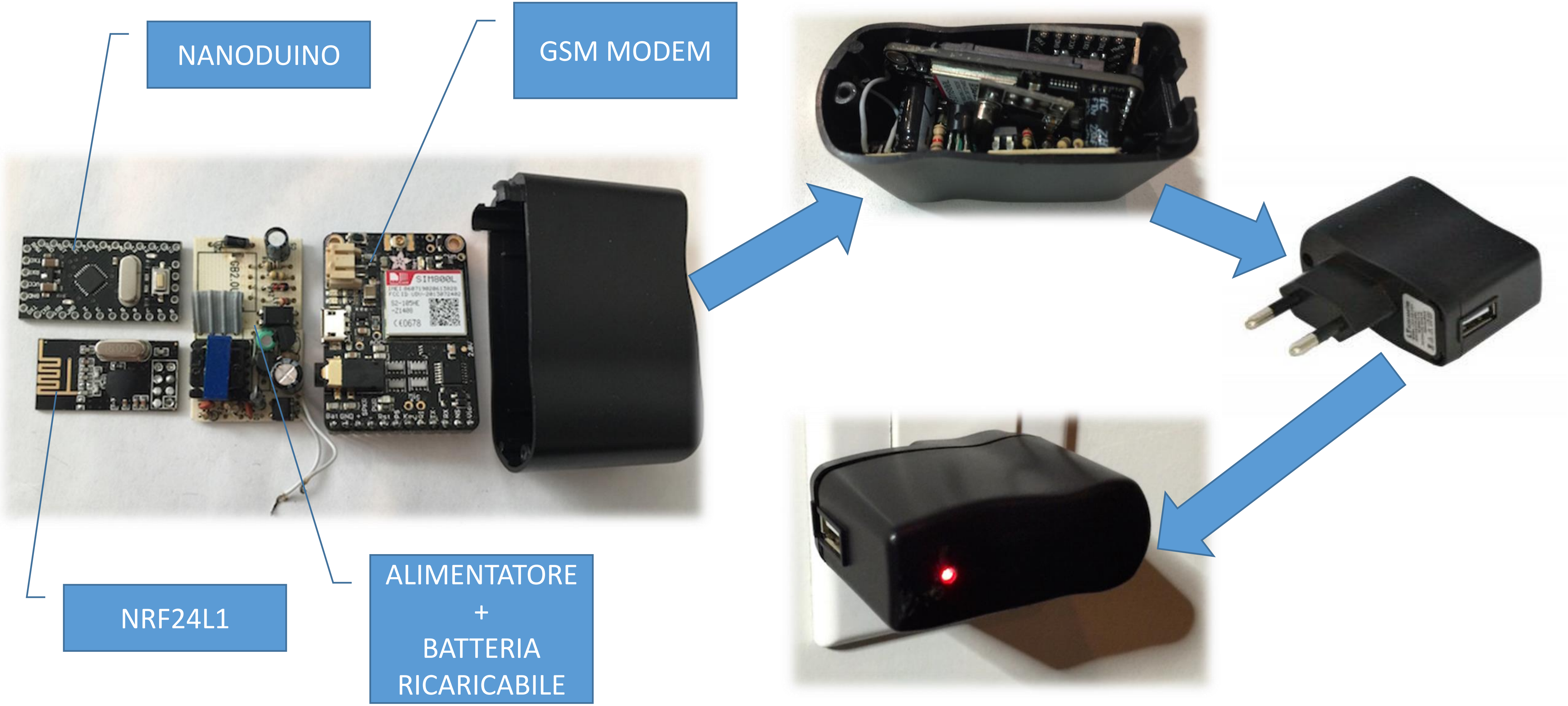
Practical Exploitation
of
Modern Wireless Devices

Name: Keykeriki v2.0 2.4GHz
Type: Hardware and Software
Slides:keykeriki_v2_cansec_v1.1.pdf (Our slides from CanSecWe
Hardware:keykeriki-v2-devdbg-hardware.zip
Software:keykeriki-v2-demo-src.zip
Documentation: See folder "docs" within the download package
License: OpenSource, free for non-commercial use, commercial
Contact: hardhack@remote-exploit.org

Description: KeyKeriki v2.0 was first presented to the public at
controller board. In contrary to the 27MHz Version of Keykeriki it


Bluetooth Trasm.
NANODUINO
NRF241L

The magnitude of the threat



NANODUINO

GSM MODEM

NRF24L1

ALIMENTATORE
+
BATTERIA
RICARICABILE