# Challenges in Critical Infrastructure Security

**Corrado Leita**

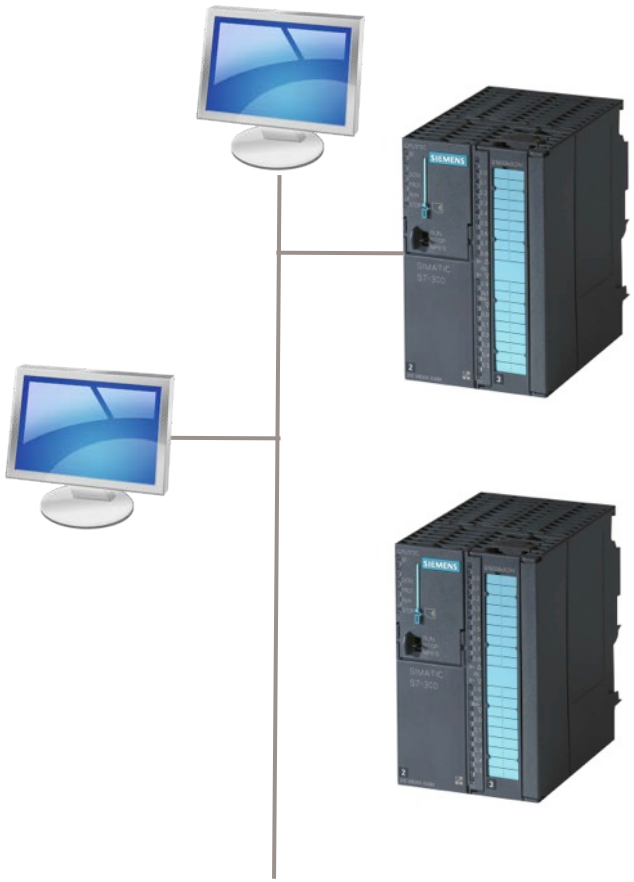
Symantec Research Labs

# Symantec Research Labs

- CARD (Collaborative Advanced Research Department) group
  - Sophia Antipolis, FR
  - Culver City, CA
  - Herndon, VA
- Relevant recent work:
  - **SGNET**: distributed honeypot deployment for the study of code injection attacks based on ScriptGen
  - **HARMUR:** dataset providing a historical perspective on client-side threats
  - **TRIAGE:** multi-criteria decision analysis for the study of security datasets (Olivier Thonnard)
  - **WINE:** Worldwide Intelligence Network Environment (http://www.symantec.com/WINE)

# Convergence between IT and OT technologies

- Interconnection of standard computer systems with industrial control systems
- An **opportunity**?
  - Lower costs and increased system efficiency
  - Opportunity to leverage standard IT techniques (intrusion detection, file scanning, standard hardening techniques, …)
  - Opportunity to enable OT suppliers to manage and support OT devices at scale
- A **threat**?
  - Enable attacks and incidents that are typical of standard IT environments
  - Enable attacks on critical infrastructures and environments such as energy, gas, medical
  - Privacy violations from data being more widely available



# What are the challenges in the protection of ICS environments?

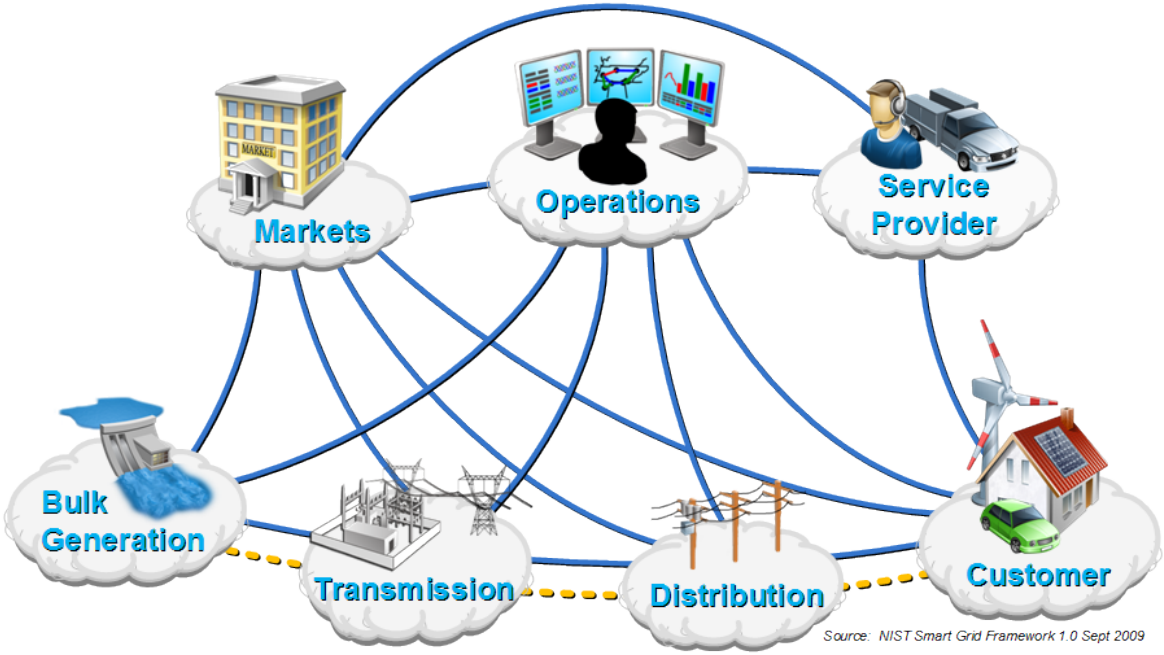

**Off-the-shelf suitability to ICS**

**Challenges**

IT VS OT culture

Threat economy

# Smart Grid as a complex ecosystem

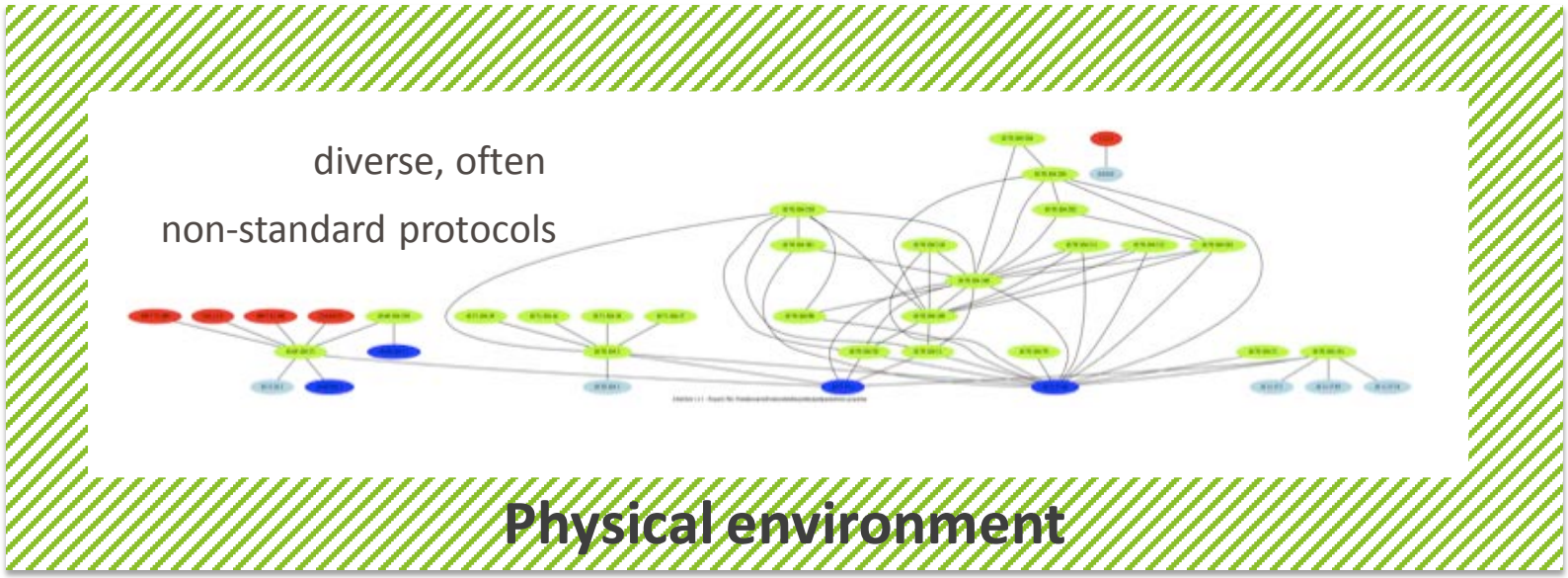



Our focus

SCADA → AMI

# A composition of complex environments

flow datagram generated from the analysis of one hour of operation of a water pump control system

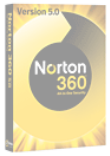



servers

gateways

clients in main network

clients in separate network




Off-the-shelf suitability to ICS


IT VS OT culture

Threat economy

The Washington Post

# NATIONAL

Corrections | Energy & Environment | Health & Science | Higher Educa

In the News | Super Bowl commercials | Madonna | Josh P

## Checkpoint Washington

Reporting on diplomacy, intelligence and military affairs

On Twitter | E-Mail Checkpoint | More national security news | RSS Feed

**ABOUT THIS BLOG**

Checkpoint Washington is produced by the national security staff of The Washington Post.

**E-mail us**
Follow us on Twitter:
**@checkpointwash**

**SUBSCRIBE**

Posted at 12:44 PM ET, 11/18/2011

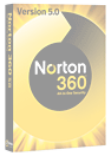
### Foreign hackers targeted U.S. wa apparent malicious cyber attack,

*By Ellen Nakashima*

Foreign hackers caused a pump at an Illinois week, according to a preliminary state report attack, if confirmed, would be the first known the systems that supply Americans with wate essentials of modern life.

# The interesting lesson

Is it possible to burn-out a water pump by solely interfacing with the SCADA layer? Fail-safe mechanisms exist to prevent physical damage!




Off-the-shelf suitability to ICS

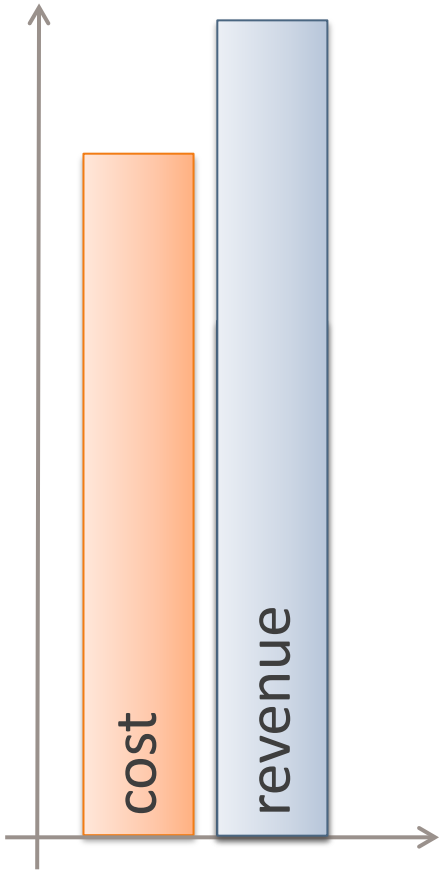
Challenges

IT VS OT culture

Threat economy

# Threat economy

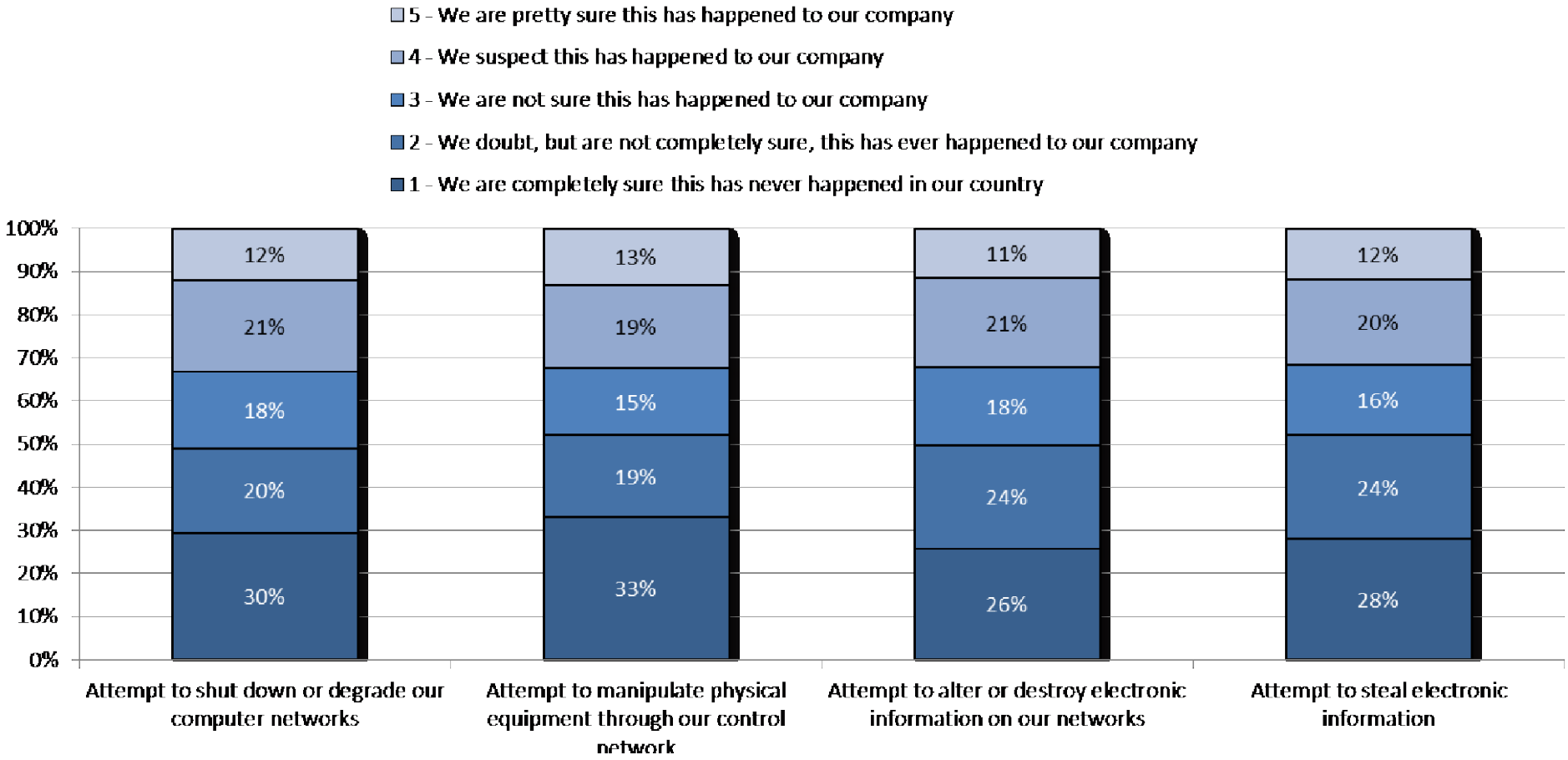
- Security mechanisms often aim at rendering an intrusion “difficult enough”
- Their effectiveness depends on the value of the target!
  - Requiring a signed certificate to inject a kernel driver
  - Keeping valuable resources in a private network
  - Storing a certificate in a secure room
  - …



# The threats are real

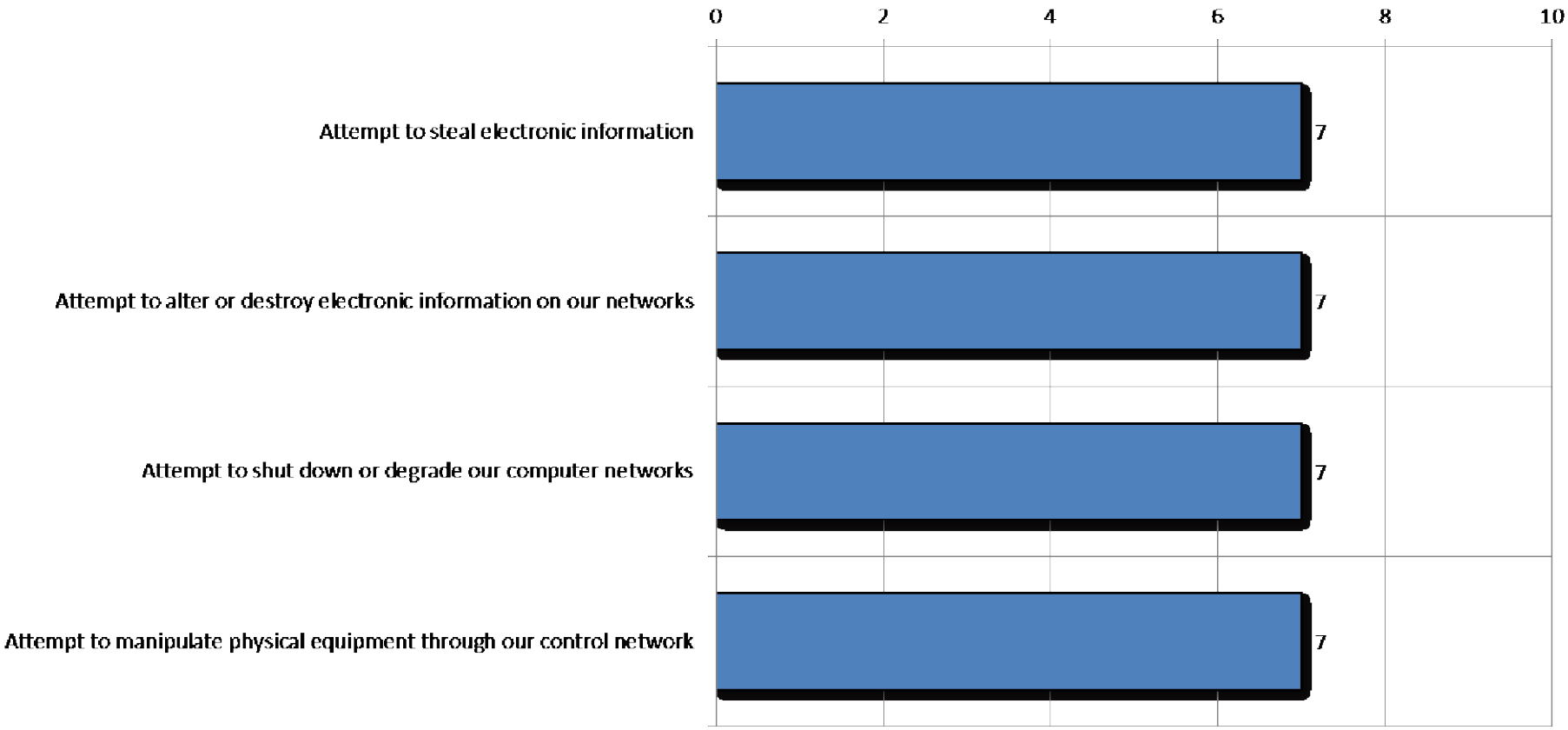
# What is your experience with each of this type of attacks? (1580 industries contacted, 2010)

Symantec 2010 Critical Infrastructure Protection Study - **http://bit.ly/bka8UF**



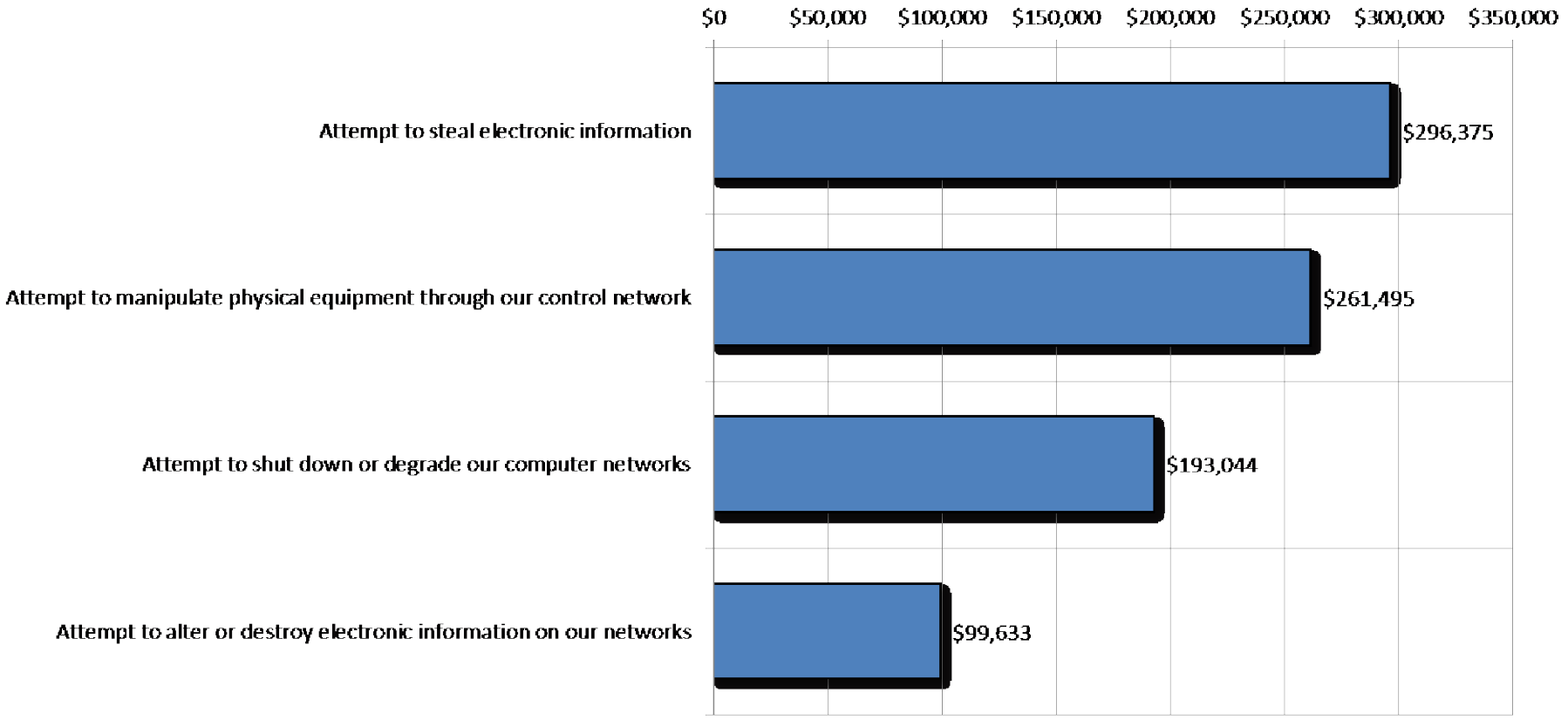
# How many times have you suspected or been sure each of the following has occurred in the last 5 years?

Symantec 2010 Critical Infrastructure Protection Study - **http://bit.ly/bka8UF**



# Cost estimations of all the attacks over the 5 years

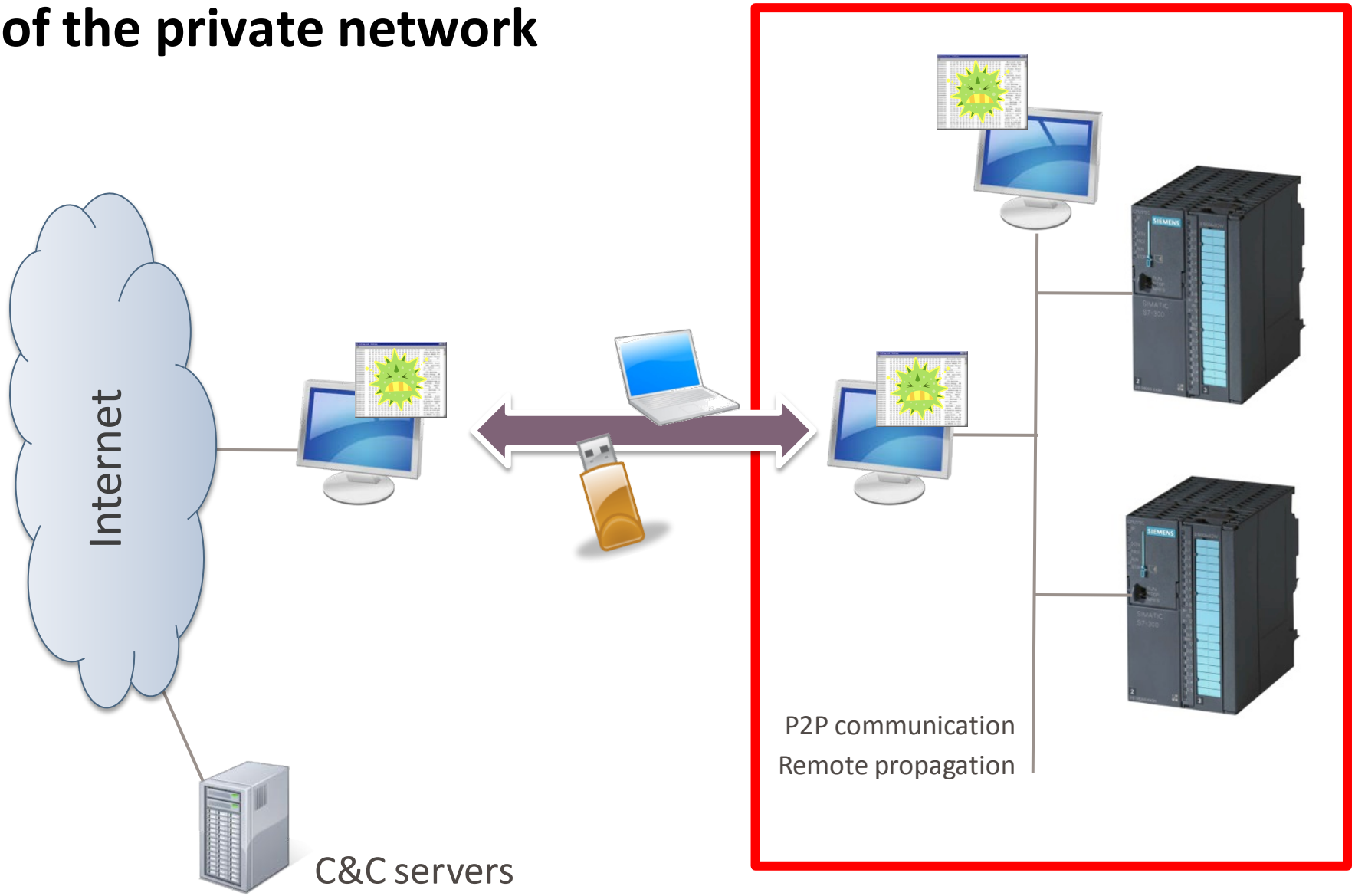
Symantec 2010 Critical Infrastructure Protection Study - **http://bit.ly/bka8UF**



# Stuxnet

- Windows worm discovered in **July 2010**
- Uses **7** different self-propagation methods
- Uses **4** Microsoft 0-day exploits + **1** known vulnerability
- Leverages 2 Siemens security issues
- Contains a Windows rootkit
- Used **2 stolen digital certificates** (second one introduced when first one was revoked)
- Modified code on Programmable Logic Controllers (PLCs)
- First known PLC rootkit

# Stuxnet and the myth of the private network



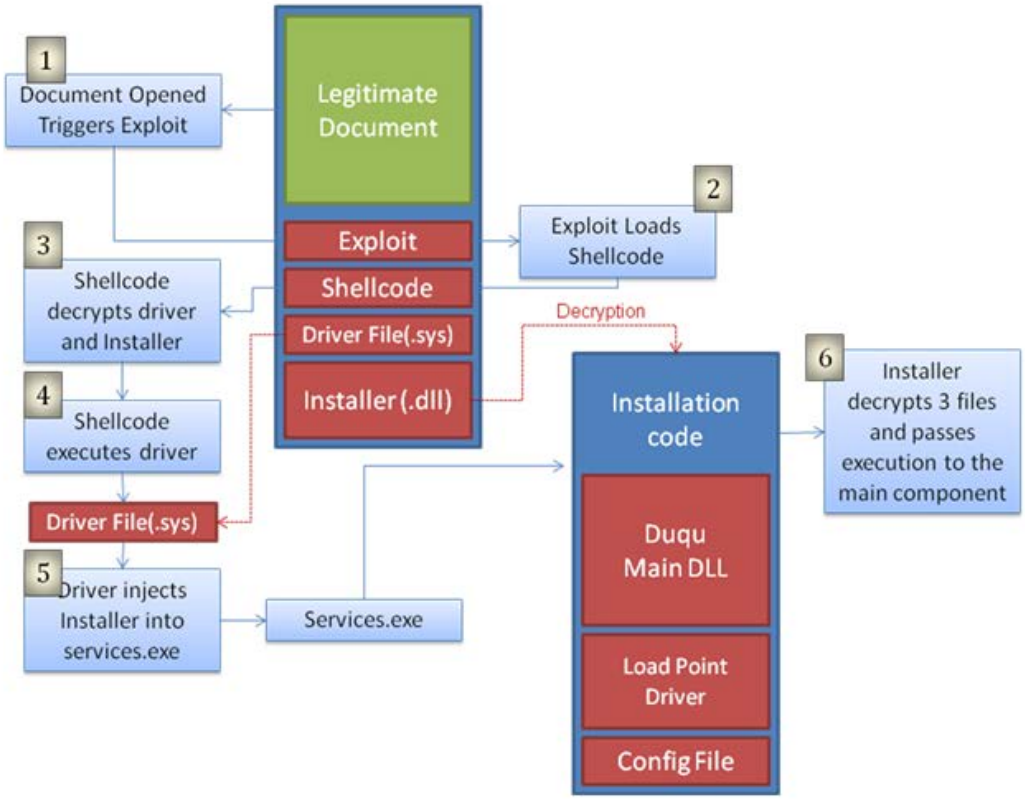
# Stuxnet: an isolated incident?

- **September 2011:** a European company seeks help to investigate a security incident that happened in their IT system, and contacts CrySyS labs (Budapest University of Technology and Economics)
- **October 2011:** CrySyS labs identifies the infection and shares information with major security companies
  - Duqu: named after the filenames created by the infection, starting with the string "~DQ"
  - A few days later, Symantec releases the first report on Duqu malware sample with the help of the outcomes of the original CrySyS investigators

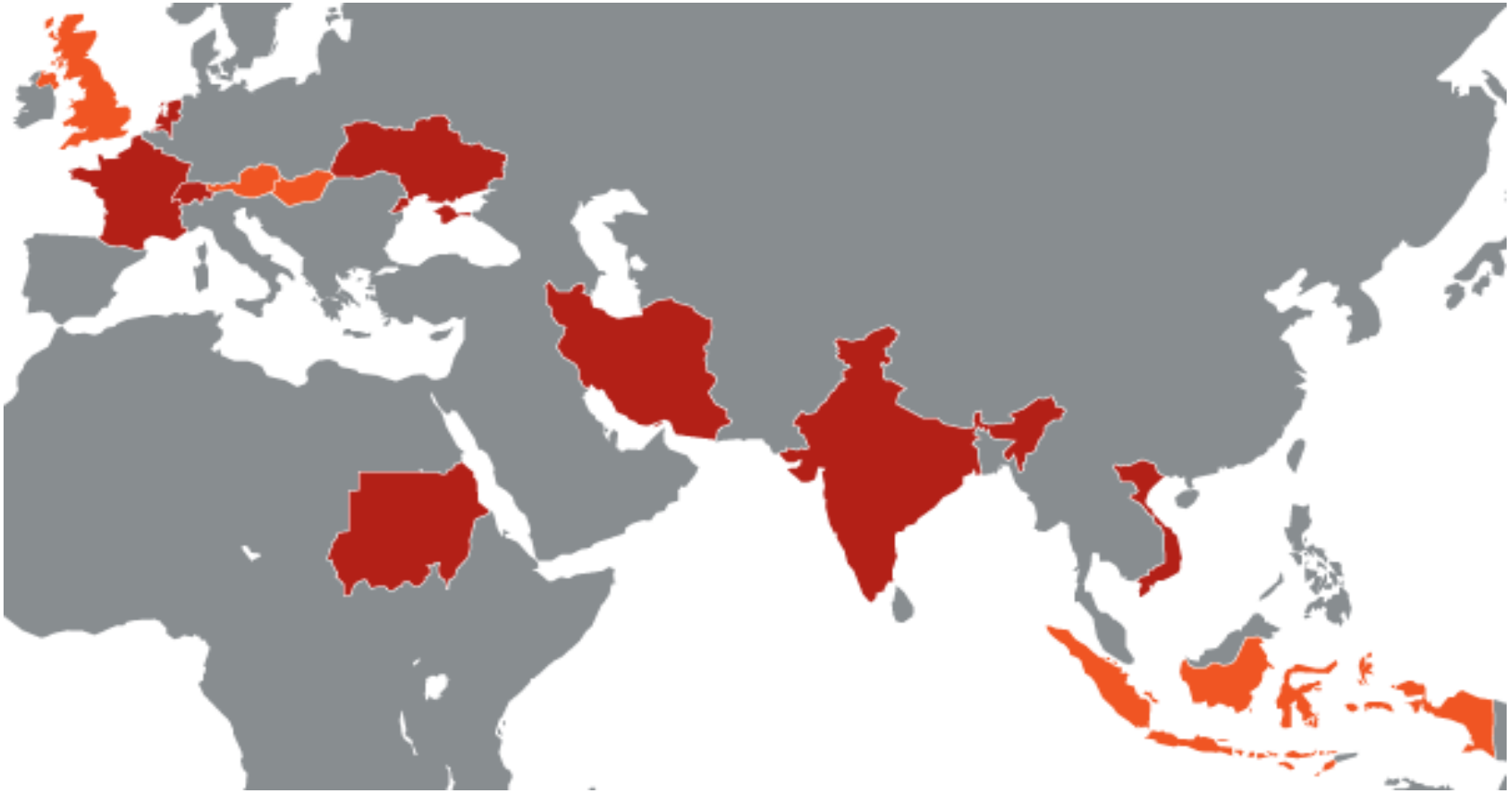
# Extremely stealthy and targeted infection

Infection leaves almost no trace on hard drive: only the driver file is stored in stable storage!

- 0-day vulnerability in TTF font parser
- Shellcode ensures infection only in an 8 days window in August
- No self-propagation, but spreading can be directed to other computers through C&C
  - Secondary target do not communicate with C&C, communicate instead through P2P

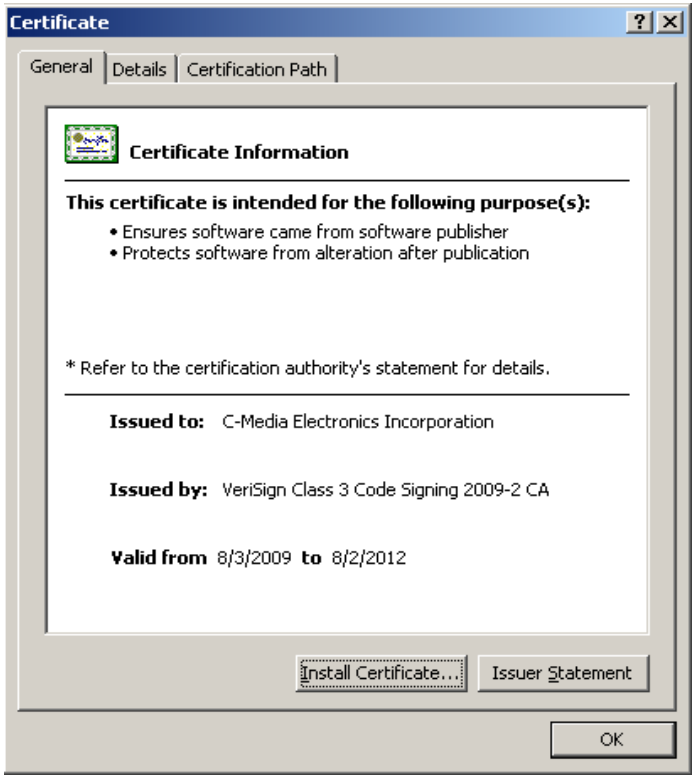


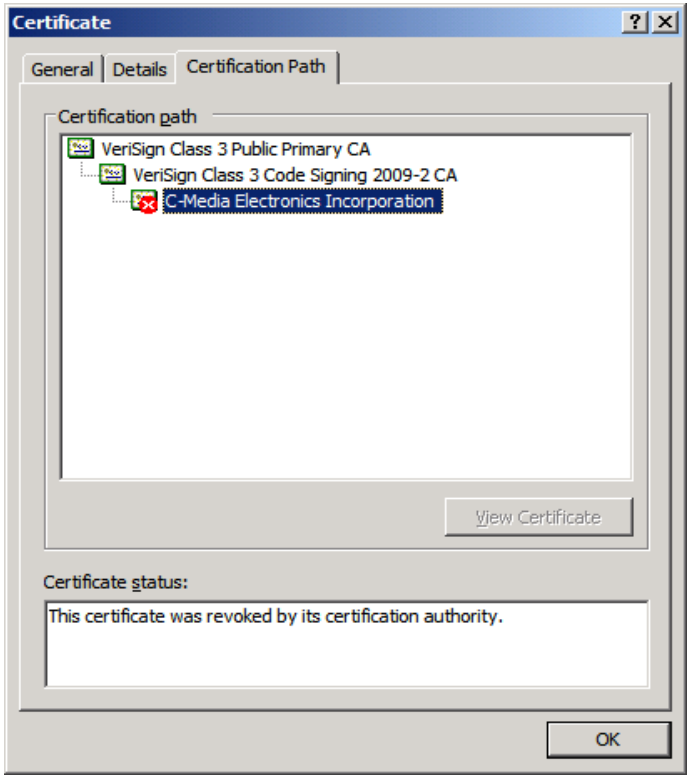
# Targets



6 organizations in 8 countries confirmed infected

# Signed Drivers




- **Some** signed (C-Media certificate)
- Revoked immediately after discovery

# Command & Control Complexity

- Communication over TCP/80 and TCP/443
  - Embeds protocol under HTTP, but not HTTPS
  - Includes small blank JPEG in all communications
  - Basic proxy support
- Complex protocol
  - TCP-like with fragments, sequence and ack. numbers, etc.
  - Encryption AES-CBC with fixed Key
  - Compression LZO
  - Extra custom compression layer
- CnC server hidden behind a long sequence of proxies

# Duqu “strange clues”

- TTF Exploit
  - Font name “Dexter Regular” from “Showtime Inc.”
  - Only two characters defined:

: )

- Inside the keylogger component is a partial image
  - “interacting Galaxy System NGC 6745”

# Stuxnet and Duqu

- Stuxnet: first publicly known malware to cause public damage
- Duqu: shares many similarities, used for cyber espionage (a new Stuxnet?)
- High complexity
  - Require resources at the level of a nation-state
  - The attackers are not gone: new binary found compiled in February 2012

- **Cyber warfare is not a myth**

# CRISALIS

# What have we learned so far?

1. **Attacker motivation:** no security practice is likely to make the intrusion **difficult enough**. New motivations for attackers (crime, cyber warfare) mean more resources and incentives to conduct attacks.
2. **Myth of the private network:** also because of 1. , relying on network isolation from the Internet as main security protection is ineffective. Physical security cannot be enforced in practice, and network isolation renders cloud-based security technologies impossible to apply (e.g. reputation, data analysis, signatures, …).
3. **From Intrusion Prevention to Intrusion Tolerance:** a layered approach is required with several safety nets and managerial procedures to handle fallback modes.

# The CRISALIS project

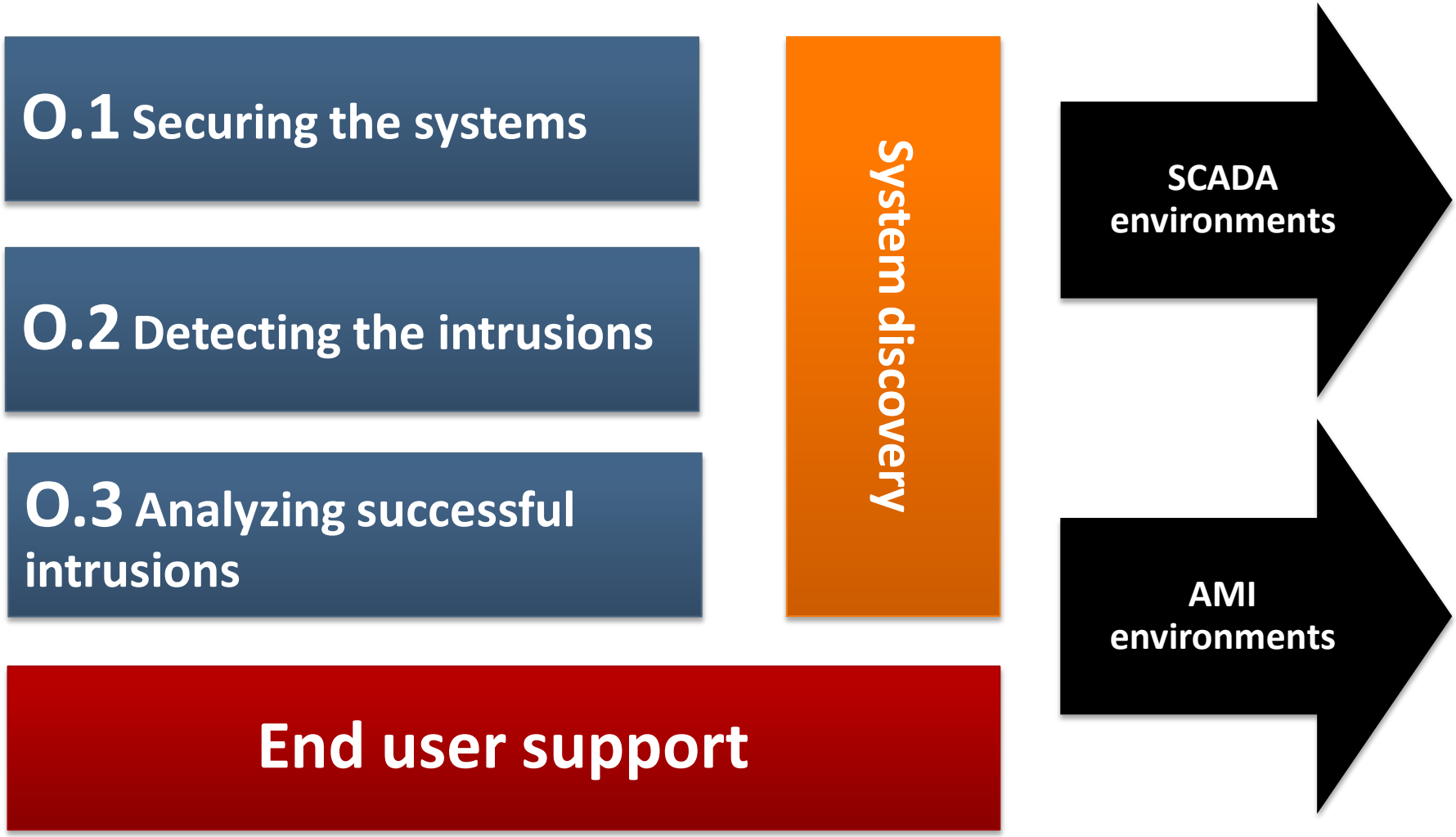
- 3-year collaborative project (funded by FP7-SEC)
- Participants:
  - Symantec (Ireland)
  - Siemens (Germany)
  - Security Matters (Netherlands)

  Industry
  - EURECOM (France)
  - Chalmers (Sweden)
  - University of Twente (Netherlands)

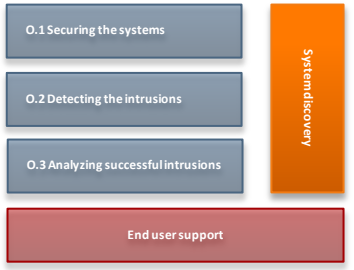
  Academia
  - ENEL (Italy)
  - Alliander (Netherlands)

  End users

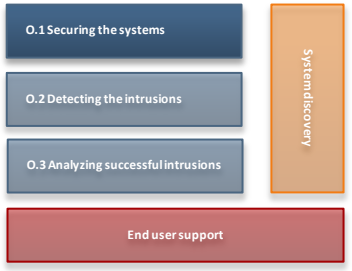
# The CRISALIS approach



# System discovery: the foundation of the CRISALIS project



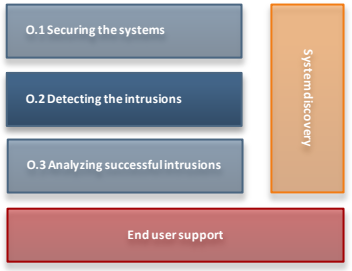

- Understand the environment being monitored
  - Devices
  - Interconnections among devices
  - Semantics of the interactions
- Challenges
  - Proprietary devices and protocols
  - Lack of protocol parsers




# O.1 Securing the systems

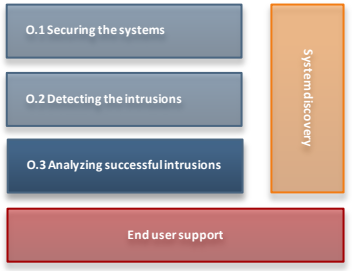
- Penetration testing
  - Globally accepted methodologies in ICT infrastructures
  - Methodology needs to be carefully revisited to be applicable to ICS (dangerous!)
- Vulnerability discovery
  - Attention to the **automated** discovery of vulnerabilities in ICS devices
    - Static analysis of the binary code
    - Dynamic analysis
  - Drive the vulnerability discovery process through information on the protocol specification

# O.2 Detecting the intrusions



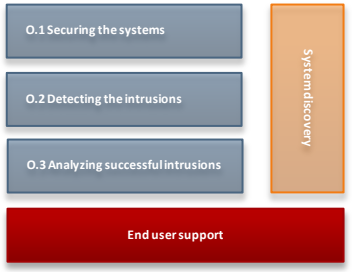

- Vulnerability discovery is unlikely to exhaustively identify all the possible threat vectors. How to identify and block a successful intrusions?
- Targeted attacks: we need to avoid a-priori assumptions on the threat vector
  - Traditional assumptions on the threat model are likely to not hold
  - Signature-based technologies are not appropriate
  - Revisit behavior-based detection in ICS environments
  - Revisit host-based monitoring techniques

# O.3 Analyzing successful intrusions



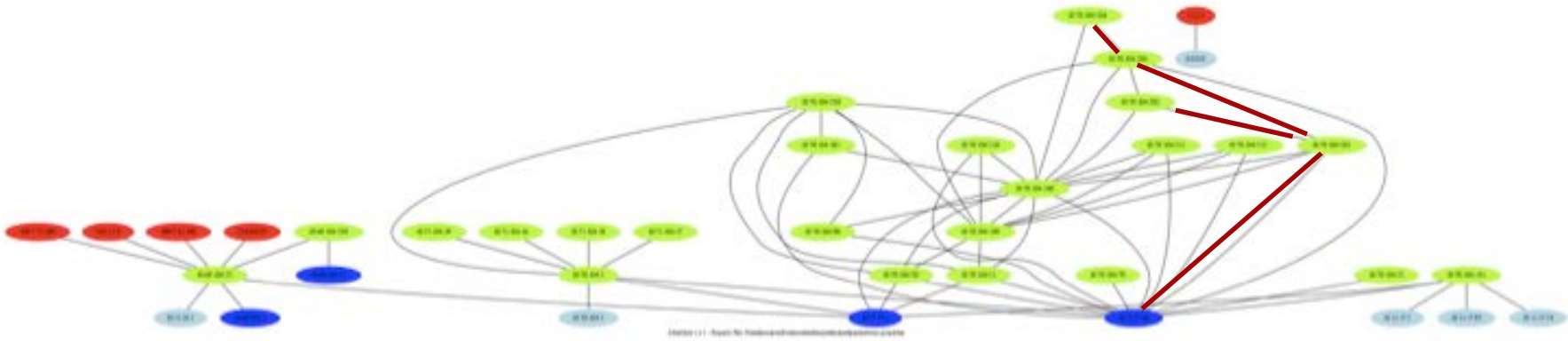

- Be ready to fail: provide instruments to detect suspicious modifications to the devices and analyze their effects
  - Forensic analysis of industrial devices: how can we understand if a PLC device has been compromised? How can we understand the impact of the modifications?
- Challenges
  - Perceived absence of real threats by the industry
  - Deployment of proprietary components and protocols
  - Lack of persistent storage capabilities

# Validation environment




- How can we validate the soundness of the obtained results? What is the performance of an intrusion detection methodology in real world environments?
- Validation environments:
  - ENEL Security Lab (Livorno, Italy): replica of a real-world SCADA system used in power generation
  - Alliander Testing deployment (Netherlands): testing AMI deployment

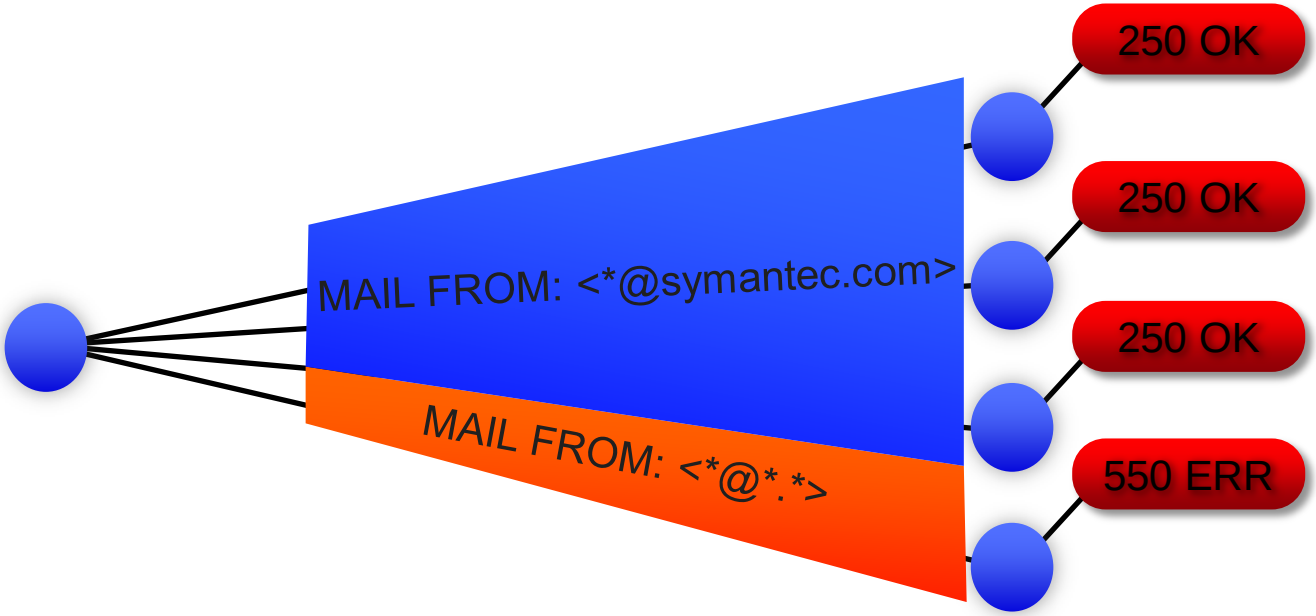
# An example: CRISALIS and protocol learning



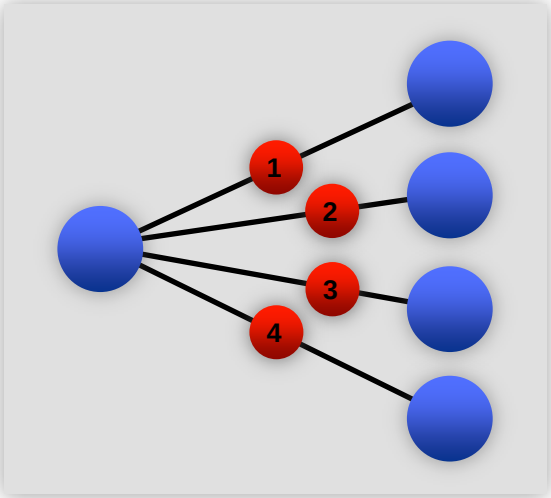
- Can we try to attach semantics to the different edges with no a-priori knowledge on the protocol structure?
- Can we infer causality…?

# ScriptGen

- Protocol-agnostic algorithm
- Observe conversation samples between a client and a real server
- Infer semantics using bioinformatics algorithms
- Proved good results in handling deterministic exploit scripts



# Region analysis




Multiple alignment
Clustering

Region synthesis

Micro clustering

| | |
|---|---|
| 1 | |
| 2 | MAIL FROM:<*@eurecom.fr> |
| 3 | |
| 4 | MAIL FROM:<*@*.*> |

# Thank you!

Corrado Leita
corrado_leita@symantec.com