Critical Information Infrastructure Protection: Urgent vs. Important

Miguel Correia

2012 Workshop on Cyber Security and Global Affairs
and Global Security Forum

UPC – Barcelona – Jun. 2012

Critical Information Infrastructure

- July 15th 96 American president signed Executive Order 13010
  - introduced (or popularized?) the term **critical infrastructures**
- Identifies 8 classes of critical infrastructures:
  - telecommunications, electrical power systems, gas/oil storage and transportation, banking/finance, transportation, water supply systems, emergency services, continuity of government
- Critical information infrastructures – the ICT part of these infrastructures

federal register

Part III

The President

2

Power grid

- Recent past:
  - Power grid undergone significant computerization and interconnection
  - Improved operation, but became exposed to cyber-threats
- Present/future:
  - Smart grid: smart metering, distributed generation… - ICT is core
  - More computerization and interconnection, higher exposure to cyber-threats

Power grid is under siege

- 2003: Davis-Besse nuclear power plant's control systems blocked by the Slammer/Sapphire worm
- 2007: experimental DHS-sponsored cyber-attack destructs a power generator
- 2009: US electrical grid allegedly penetrated by spies from China, Russia and others
- 2010: Stuxnet damages centrifuges in Iranian nuclear enrichment center

URGENT: REDUCING RISK

Risk is high

$$\textit{risk} = \underbrace{\textit{level of threat} \times \textit{degree of vulnerability}}_{\textit{likelihood of successful attack}} \times \textit{impact}$$

- Level of threat is high – nation states, random threats, extortion
- Degree of vulnerability is high – as shown by the previous cases
- Impact is high – think of a city without power for hours/weeks

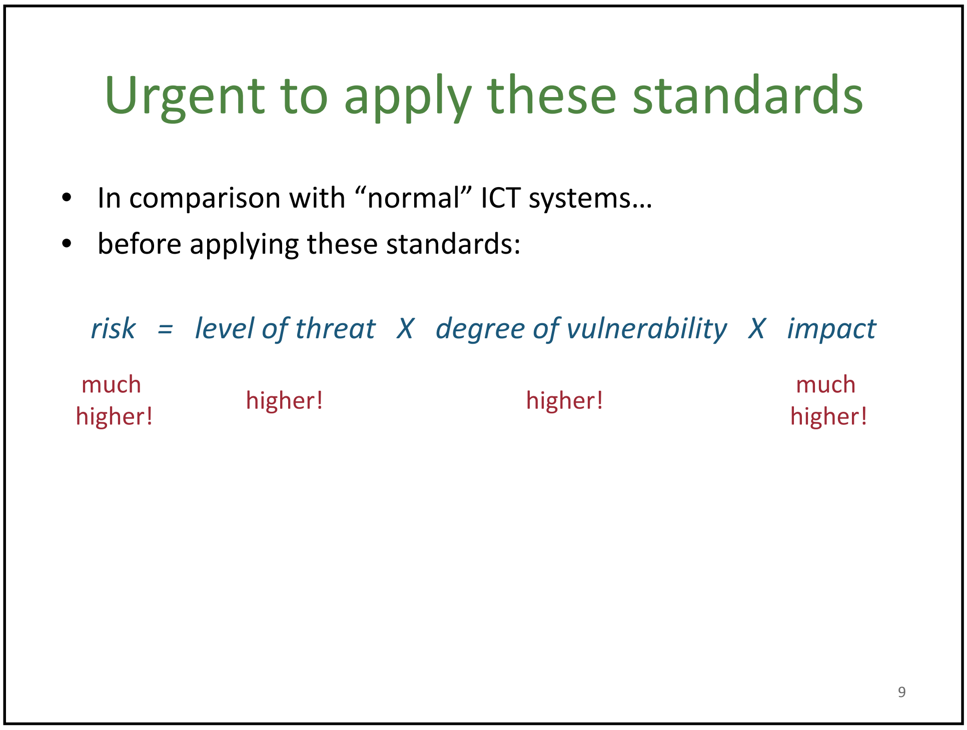
It is urgent to reduce this risk
By reducing the degree of vulnerability

NIST SP 800-82

- “Guide to Industrial Control Systems (ICS) Security”, Jun. 2011
- Recommendations about
  - Network architecture – firewall usage, network segregation,…
  - Management controls – planning, risk assessment,…
  - Operational controls – personnel security, contingency planning, configuration management,…
  - Technical controls – authentication, access control, systems and communication protection,…
- ICT security applied to CIIP

IEC 62351

- “Power systems management and associated information exchange – Data and communications security”, May 2007
- Recommendations about the security of TC57 protocols
  - protection from eavesdropping, man-in-the-middle, spoofing, and replay
- ICT security applied to CIIP

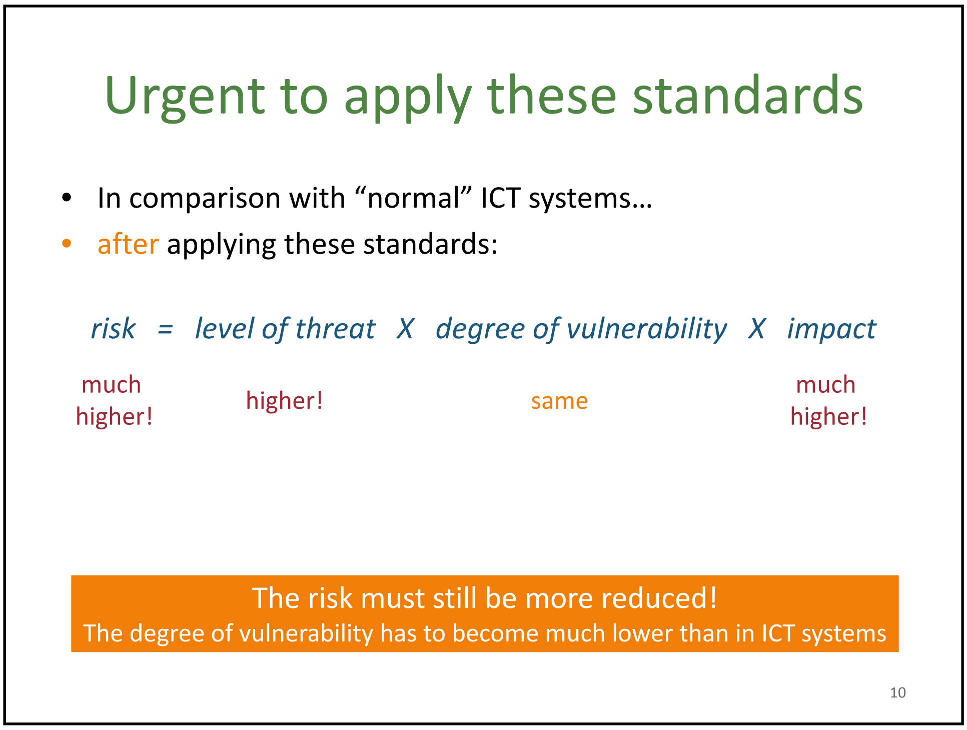


Urgent to apply these standards

- In comparison with "normal" ICT systems…
- before applying these standards:

risk	*=*	*level of threat*	*X*	*degree of vulnerability*	*X*	*impact*
much higher!		higher!		higher!		much higher!

9



Urgent to apply these standards

- In comparison with "normal" ICT systems…
- after applying these standards:

risk	*=*	*level of threat*	*X*	*degree of vulnerability*	*X*	*impact*
much higher!		higher!		same		much higher!

The risk must still be more reduced!
The degree of vulnerability has to become much lower than in ICT systems

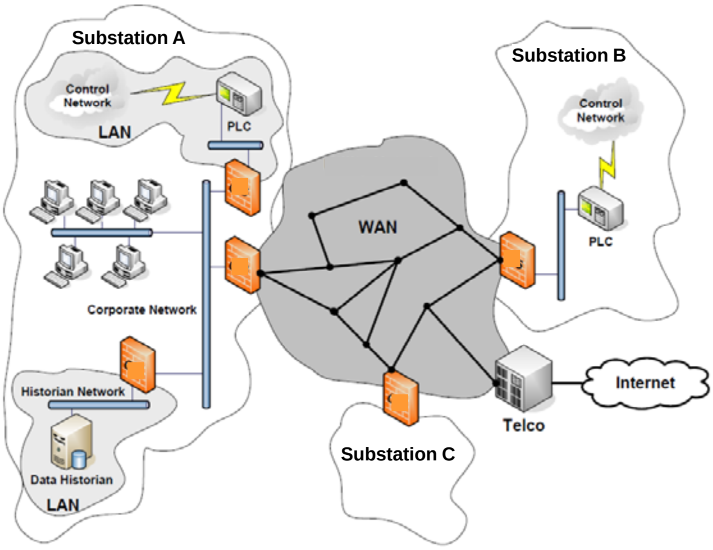
10

CRUTIAL
CRitical UTIlity InfrastructurAL resilience

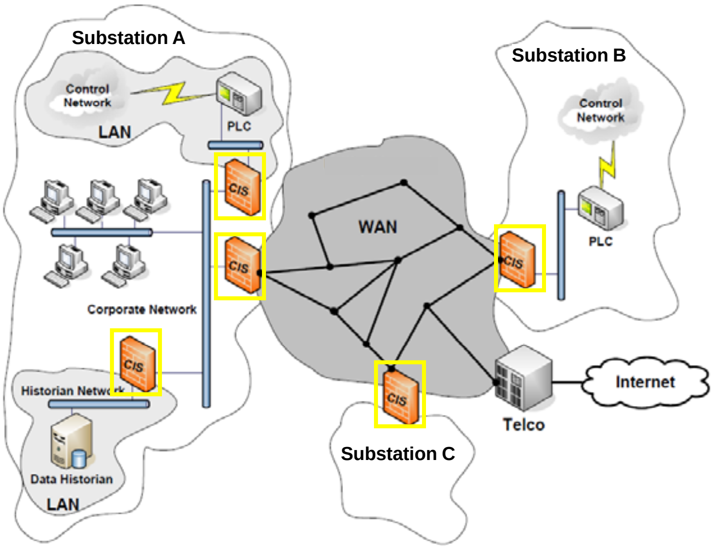
Information Society Technologies

IMPORTANT: RESEARCH ABOUT REDUCING RISK MUCH MORE

Architecture – WAN-of-LANs

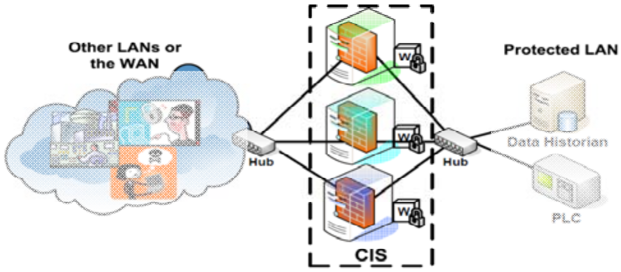


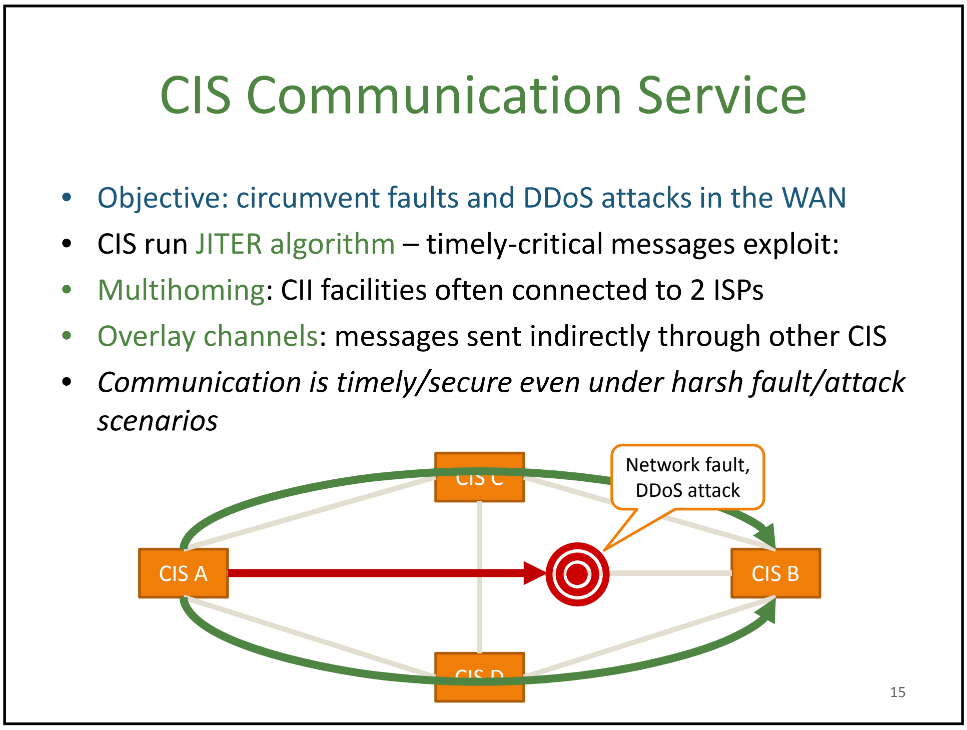
CIS - CRUTIAL Information Switch



CIS Protection Service

- Objective: effectively block incoming attacks
- CIS-PS works at application layer and is a distributed firewall
- It is intrusion-tolerant thanks to replication and diversity
- It is self-healing thanks to replica rejuvenation
- *It cannot be attacked even if there are 0-day vulnerabilities*



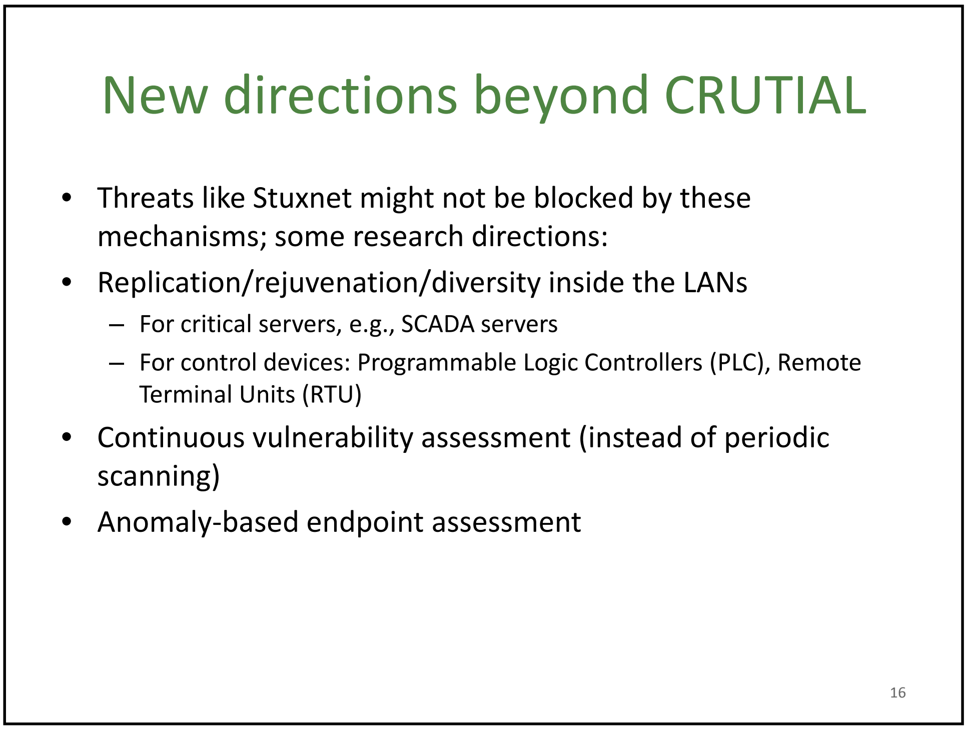


CIS Communication Service

- Objective: circumvent faults and DDoS attacks in the WAN
- CIS run JITER algorithm – timely-critical messages exploit:
- Multihoming: CII facilities often connected to 2 ISPs
- Overlay channels: messages sent indirectly through other CIS
- *Communication is timely/secure even under harsh fault/attack scenarios*

CIS C
Network fault,
DDoS attack
CIS A
CIS B
CIS D

15



New directions beyond CRUTIAL

- Threats like Stuxnet might not be blocked by these mechanisms; some research directions:
- Replication/rejuvenation/diversity inside the LANs
  - For critical servers, e.g., SCADA servers
  - For control devices: Programmable Logic Controllers (PLC), Remote Terminal Units (RTU)
- Continuous vulnerability assessment (instead of periodic scanning)
- Anomaly-based endpoint assessment

16

Conclusions

- The power grid and other critical information infrastructures are vulnerable to cyber-attacks
- It is urgent to do the urgent: apply standards and recommendations
- But ICT-like security mechanisms are not enough: the threat level and impact of CII failure is high, so risk remains high
- So it is important to do what is important: to investigate novel protection mechanisms that greatly reduce the degree of vulnerability

17

More info at my web page: google miguel correia inesc-id