Security in Critical Infrastructures Challenges and the Road ahead

Martín Ochoa
Singapore University of Technology and Design

2do Foro Nacional de Seguridad de TI
Desafíos y oportunidades de la Seguridad de la Información en la era del postconflicto
Bogotá, Junio 21 - 2016

About me

- Assistant Professor at SUTD, interested in:
  - Information flow analysis
  - Security testing
  - Security in Cyber-physical systems

- Past:
  - Post-doc at the TU Munich.
  - Researcher and consultant at Siemens CT in Munich.
  - PhD in Computer Science at TU Dortmund.
  - Mathematics in Munich and Rome.
  - Systems Engineering in CR.

martin_ochoa@sutd.edu.sg

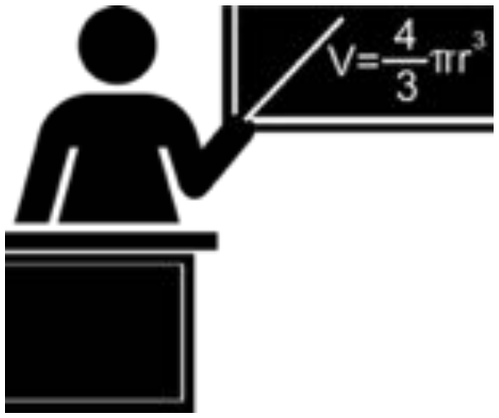
State of affairs

- Increasingly interconnected, software dependent critical infrastructures.
  - Electricity distribution, Water treatment and distribution, Financial services, Healthcare etc.

http://invensyscustomersuccess.blogspot.sg/2013/09/web-hmi-and-mobile-scada-rocks.html

State of affairs

- Evidence of attacks in the wild
  - Highly sophisticated malware (Stuxnet and co.)
  - Increase of sophisticated attacks agains CI.



Role of academia

- In general, topic on its own (philosophy of science)
- In my view, in the context of cyber security of CI:
  - Understand reality
    - What is going on? What is being attacked? Who is attacking? How are they attacking?
  - Propose solutions
    - How can we solve existing problems? Can we make CI more secure?

Critical infrastructures

- Historically CI engineering had focused on <u>safety</u> as opposed to <u>security</u>.
- Assumption was that an adversary had to bypass certain <u>physical</u> security to attack.
- Many CIs not built by computer scientist but by electric/electronic engineers.
- Proprietary systems, designs usually <u>secret</u>.

Security as a science

- On the positive side, some lessons learned in security:
  - Kerckhoff's principle: security by design vs. security by obscurity [Kerckhoff].
  - Selected Secure Development principles [Viega & McGraw]
    - Secure the weakest link.
    - Practice defence in depth.
- Security is often not a boolean property, but is relative to capacity of adversary

Risk analysis for security?

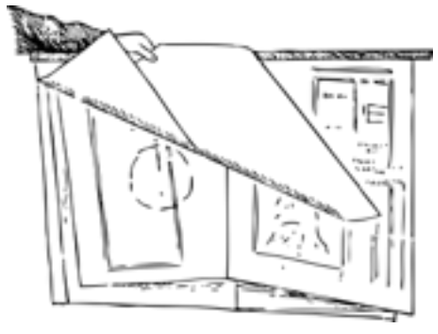
- Risk notions
  - Impact: in some cases clear.
  - Likelihood?
- Security vs. Safety:
  - Intelligent threat vs. pure chance
- Cost vs. Risk?

Security as a science

- Security != cryptography
- But cryptography offers fundamental building blocks
- P vs NP?
  - Formulation of the problem is from the 1970's
  - Solution guarantees 1M USD (Millenium problem).
  - Tightly linked to rigorous foundations of modern crypto. [Arora & Barak]

Challenges

- What do we mean by security?
  - Research challenges:
    - What exactly should be secured in critical infrastructures?
    - What are good attacker models?
    - Is the cost of countermeasures justified?



Challenges

- For historical reasons, in most CIs security is an after-thought (if at all).
- Research challenges:
  - Short term: how can we make running systems (more) secure without having to rebuild them?
  - Future: how should we design secure CIs from scratch?

Challenges

- Even if CIs have security element by design, how should we cope with changes in the threat landscape?

- 0-days.

- broken primitives (hash functions, encryption functions).

Challenges

- How can we evaluate the security of CI designs?
- Formal proofs?
- Simulations?
- What is the “correct” attacker model?

Challenges

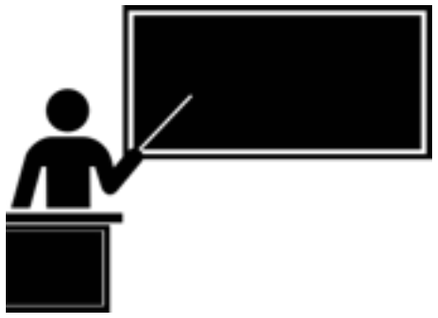
- How can we evaluate the security of CI implementations?
- Automated testing based on design?
- Pen-testing?
- Again, what is the “correct” attacker model?

Road ahead

- What we are doing at SUTD
  - Considering all of the above.
  - Interdisciplinary approach.
  - Testing attacker models and defence mechanism against state of the art test-beds.
  - Deriving designs for secure CIs.

SWaT Testbed at SUTD

http://itrust.sutd.edu.sg/research/testbeds/



Road ahead

- Awareness is critical!
  - Teaching at undergrad and graduate levels.
  - Theory and practice of security.
  - Next generations need to thoroughly understand challenges and existing solutions, and be able to cope with upcoming challenges.

Conclusions

- Many challenges but exciting research ahead.
- Interdisciplinary research is critical.
- Awareness and training are key.
- Security is (most likely) an infinite game!

References

[Kerckhoff] A. Kerckhoff, ”La cryptographie militaire" Journal des sciences militaires, vol. IX, pp. 5–83, January 1883, pp. 161–191, February 1883.

[Viega & McGraw] Viega, J., & McGraw, G. (2001). Building Secure Software: How to Avoid Security Problems the Right Way, Portable Documents. Pearson Education.

[Arora & Barak] Arora, S., & Barak, B. (2009). Computational complexity: a modern approach. Cambridge University Press.