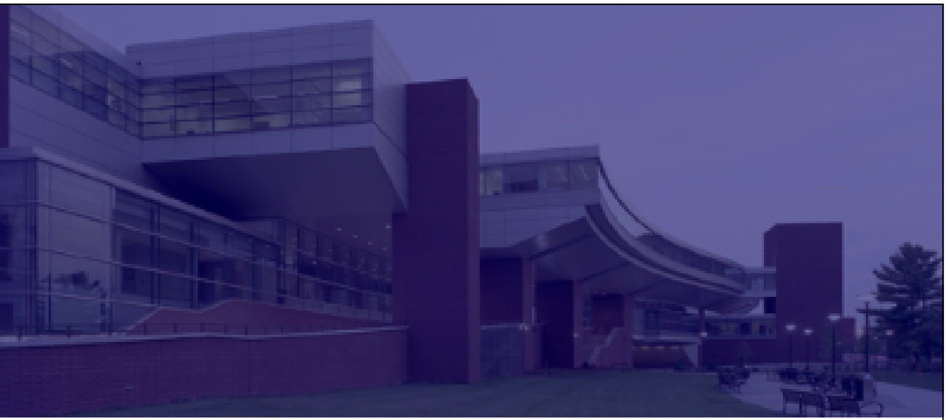
Systems and Internet Infrastructure Security

Network and Security Research Center
Department of Computer Science and Engineering
Pennsylvania State University, University Park PA



1st Workshop on Telecommunications Infrastructure Protection Security: Supply Chain Impact on Security and Information Communications Technology

Patrick McDaniel, Tom La Porta, Karl Rauscher, Jun Li

December 4th, 2009

Supply Chain

- Any non-trivial technology is critically dependent on a huge number of diverse designers, manufacturers, resellers, enablers to be *secure*/efficient/reliable.
    - Relationships in supply chain are complex and fluid.
    - Dependencies hidden by organizational and market forces.
    - Consequence: security assessment is difficult ...

Microsoft

Globalization

- Globalization changes the calculus of security in potentially harmful ways ...
  - ... relationships become more complex ...
  - ... cultural challenges ...
  - ... governance becomes murky ...
  - ... political influence possible.

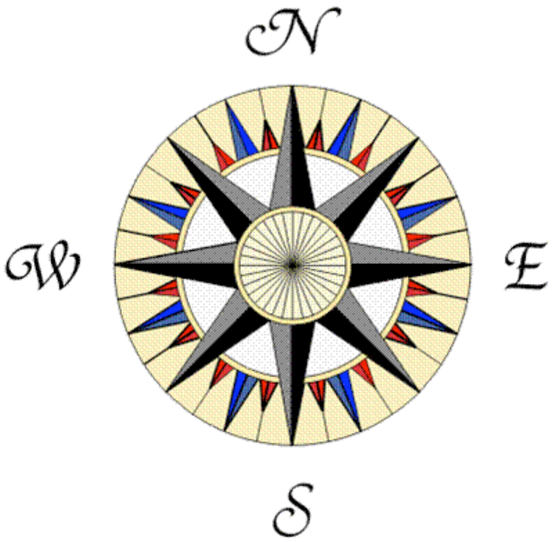
A Computer Scientist's Perspective

"Reflections on Trusting Trust", Ken Thompson, Turing Award Lecture, 1983.

- *Axiom*: In computer security, you can't trust anything you did not build yourself.
  - Understand your TCB!!
- *Consequence*: assessment is not about managing trust, but about proper recognition of risk and opportunity,
- E.g., define and understand
  - Participant capabilities
  - Misalign/disconnected incentives
  - Think Columbo: everyone must be assessed ...

Studying the Supply Chain

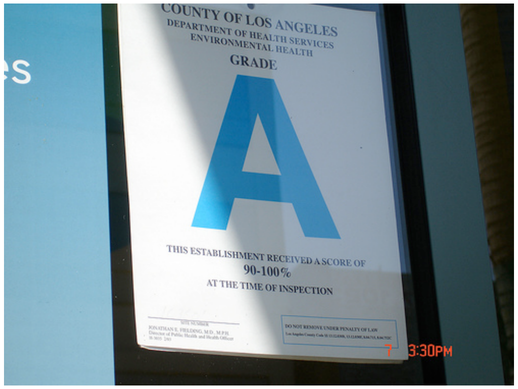
- "8 ingredient" methodology attempts to identify the intrinsic risks associated with a domain
  - See, Karl Rauscher coming up ...
- Lucent/PSU - identify the supply chain risks and impacts on "hard" elements of the 8I framework
  - Hardware
  - Software
  - Networks
  - Payload
- Q: *What to look for?*



Breaking down the challenge?

- What do the technology consumers want to know?
  - Risk?
  - Mitigation?
  - Traceability?
  - Detection?

- What would useful information look like?
  - Risk/dependency maps?
  - Process analysis?
  - Bad actors?



COUNTY OF LOS ANGELES
DEPARTMENT OF HEALTH SERVICES
ENVIRONMENTAL HEALTH
GRADE

A

THIS ESTABLISHMENT RECEIVED A SCORE OF
90-100%
AT THE TIME OF INSPECTION

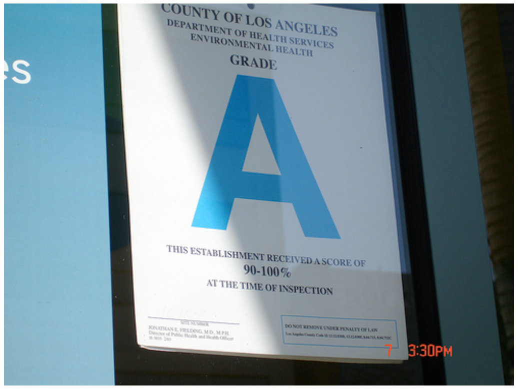
SITE NUMBER
JONATHAN E. FIELDING, M.D., M.P.H.
Director of Public Health and Health Officer

DO NOT REMOVE UNDER PENALTY OF LAW
Los Angeles County Code [illegible]

Breaking down the challenge?

- What would customers do with that information
  - Planning?
  - Process?
  - Punitive?

- What would validation look like?
  - Design validation?
  - Acceptance testing?
  - Operational evidence?



COUNTY OF LOS ANGELES
DEPARTMENT OF HEALTH SERVICES
ENVIRONMENTAL HEALTH
GRADE
A
THIS ESTABLISHMENT RECEIVED A SCORE OF
90-100%
AT THE TIME OF INSPECTION