Cyberwarfare, botnets and trust

Jonathan M. Smith

jms@cis.upenn.edu

Computer and Information Science

University of Pennsylvania

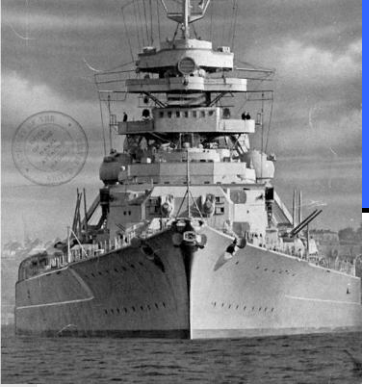
ONR MURI N00014-07-1-0907

Review Meeting

June 10, 2010

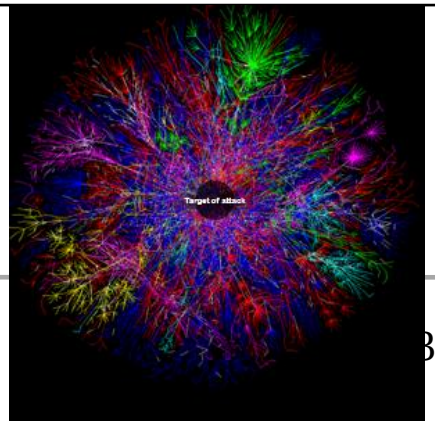
What is cyberwarfare?

- Attacks against adversary using computers as weapons
  - And, defense against such attacks
- Goal is attack/defense of nation(s)
  - Issues are scale, capabilities, willingness



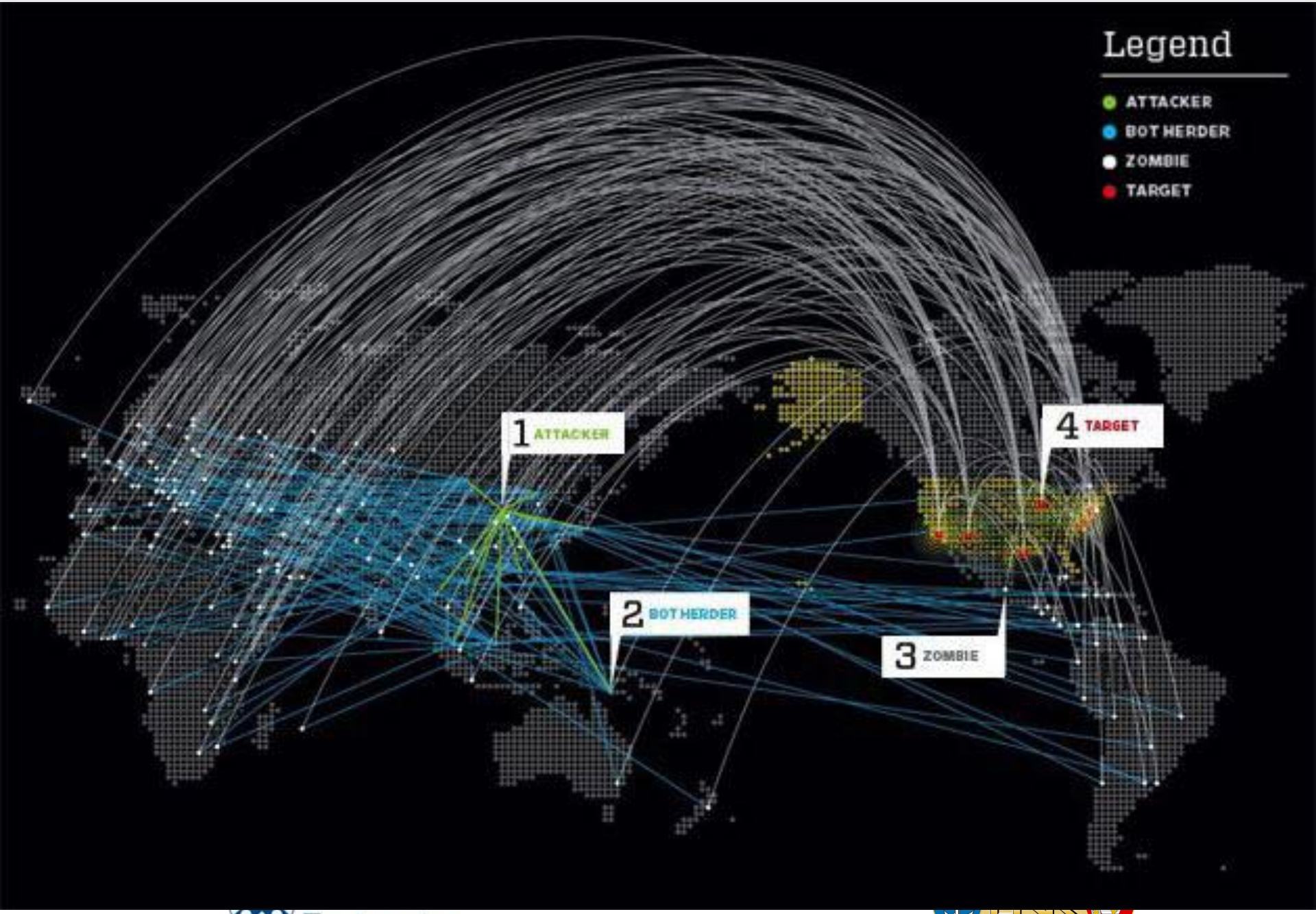
Kinetic versus Cyber

Attribute	Kinetic	Cyber
Effects	Variable (largely known, e.g., guns, bombs)	Variable (largely unknown)
Coverage	Limited by materiel	Global
Speed	Limited by transport	Possibly instantaneous
Cost (as %GDP)	Significant	Insignificant
Industrial base important?	Yes	No
Attributable	Yes, at scale	Not clear, at any scale



Example: Estonia

- http://www.nytimes.com/2007/05/29/technology/29estonia.html
- Affected government, banks, newspapers
- Example of “Denial of Service” attack
- If you depend on the net
  - Availability: your packets get through
  - “Best effort” (IP service) not enough
  - 1M machines send one 1KB packet/second
    - 8 Gbits/second – overwhelms most links



Engineering

Science & Technology

Attribution (who did it?)

- Kinetic weapons: easy
- Internet: source addresses not needed for routing, anonymity tools

"On the Internet, nobody knows you're a dog."

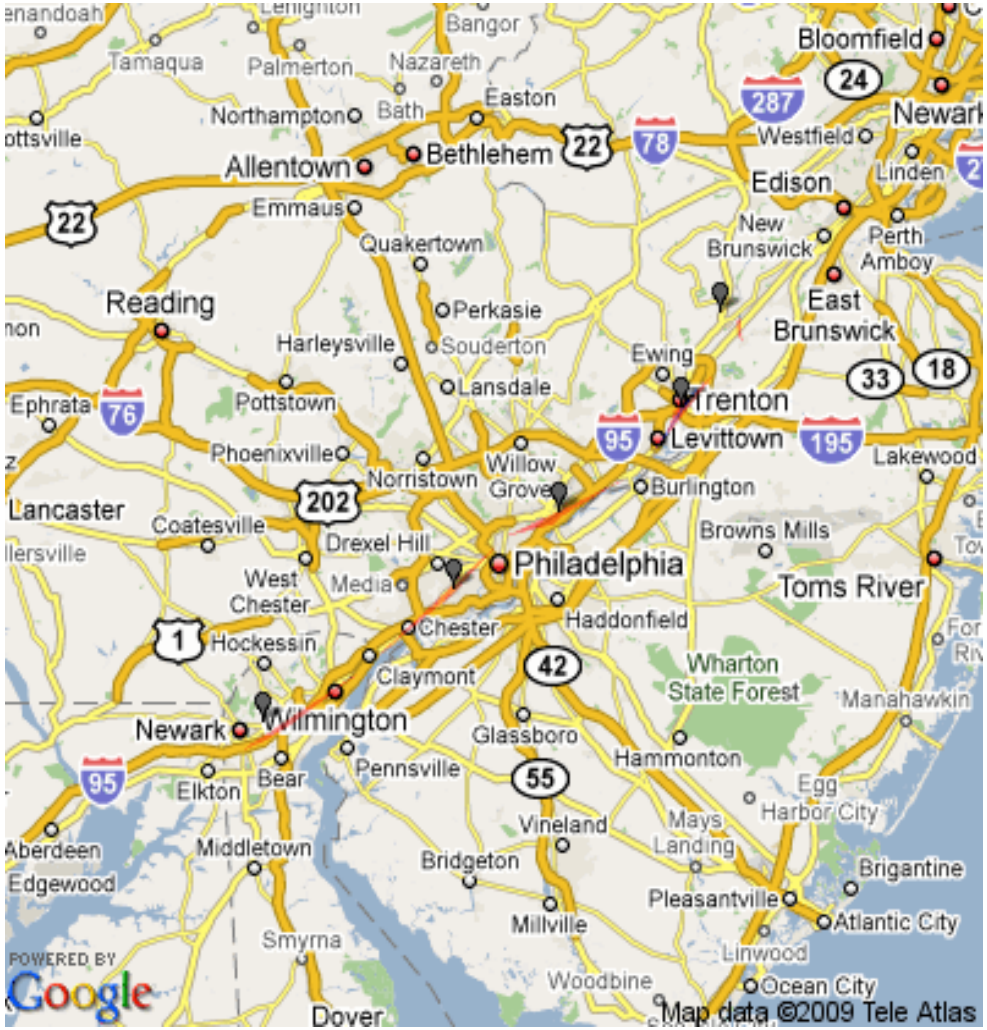
Botnets

- Can botnets be eliminated at the host?
  - Same question as “can hosts be made secure” ☺
- Can they be detected and defended against?
  - DDoS major threat
- We demonstrate detection of the command and control is hard

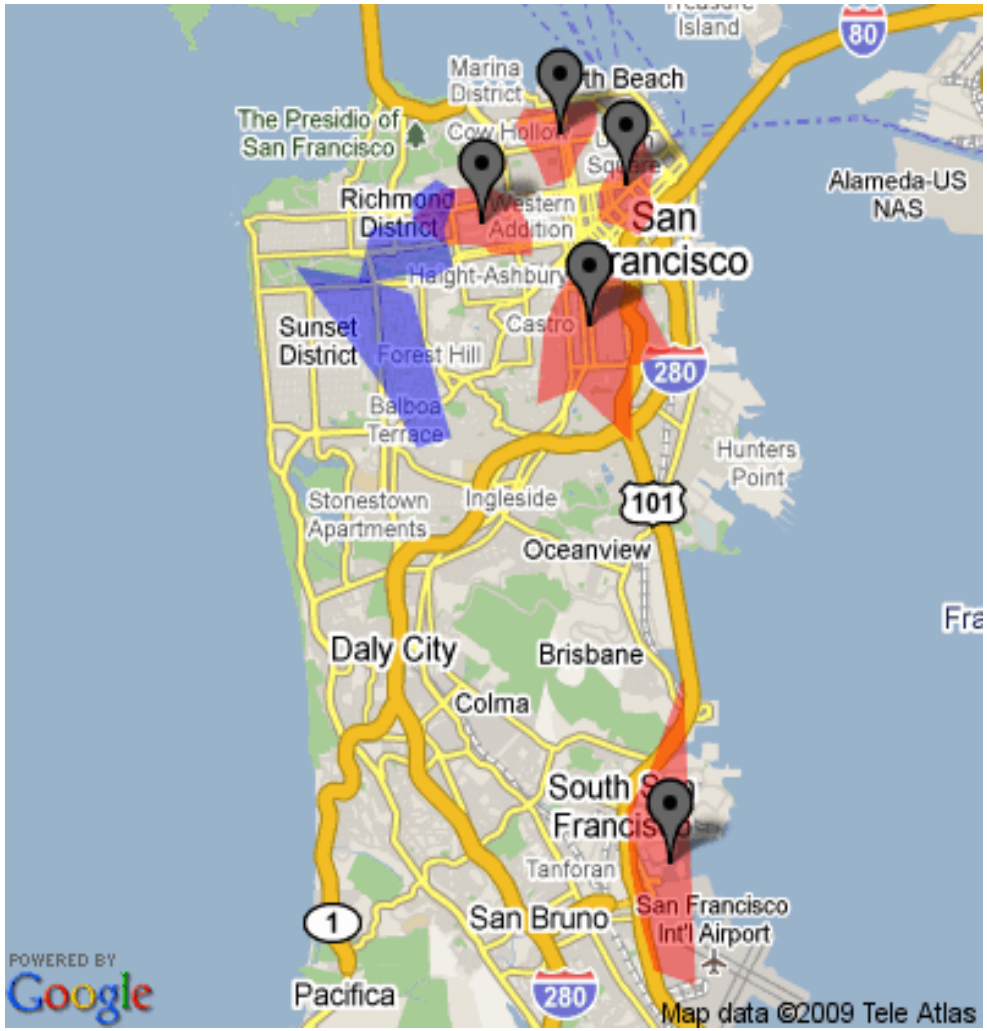
Humanets

- Routing via smartphone wireless LAN ports
- Could do epidemic routing
  - Overloads network
- Smarter use of smartphones
  - Look for “promiscuous” host …
  - That is also likely to move towards destination
- Does it work?

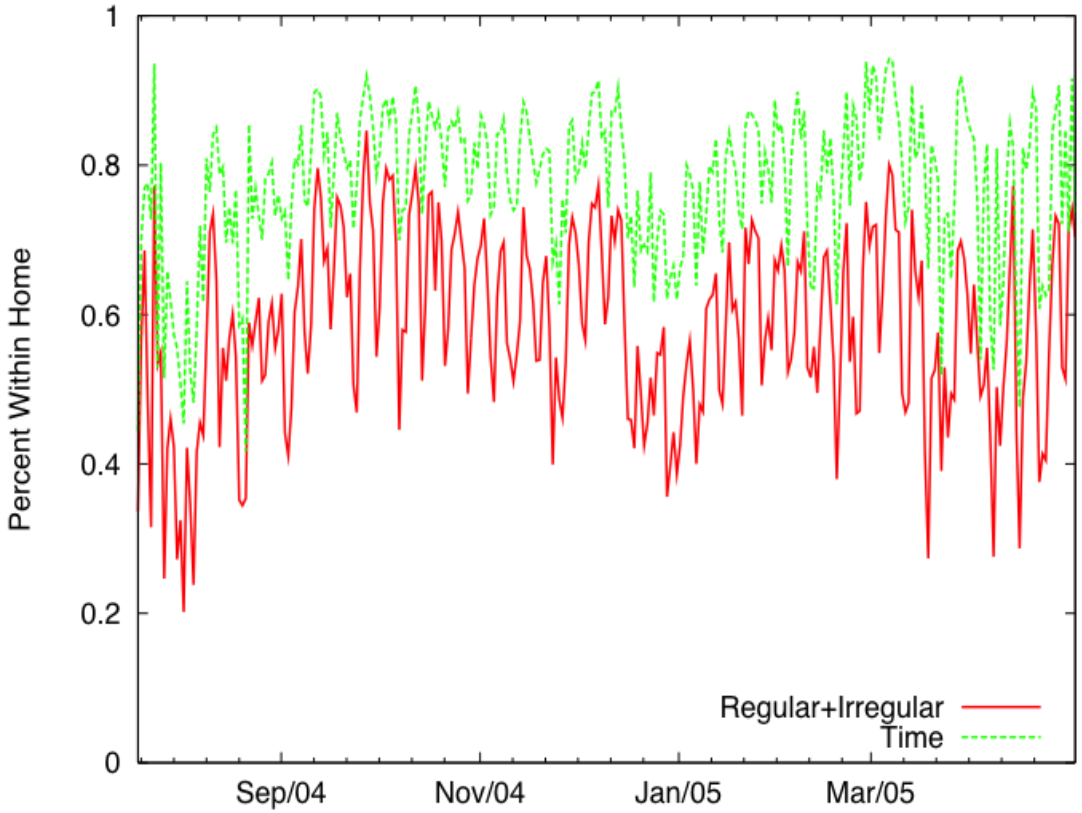
Capture data from G-1



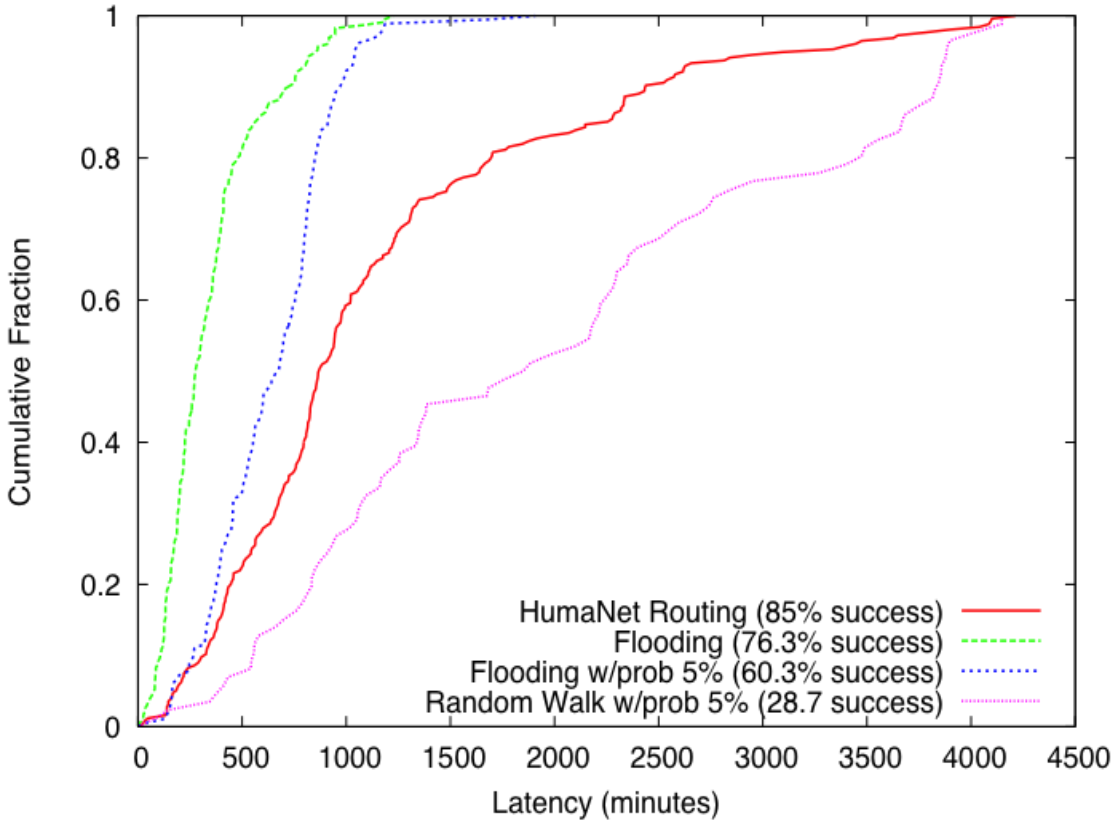
Location data from S.F. Cabs



Are locations predictable?



It works pretty well on the data…



Impact?

- Completely decentralized C&C net
  - 85% delivery in 12 hours
- Easy to use for botnet or …
  - Wherever short commands are enough
- Hard to detect (you have to be local)
- Hard to block

Trust: What is it?

- **Trust** is the *expectation* that the right thing will happen for the right person at the right time and at the right place
- Various factors can increase or decrease this expectation
  - Unknowns (and unknowables?)
  - Adversaries
- 100% and 0% not achievable, but how close?

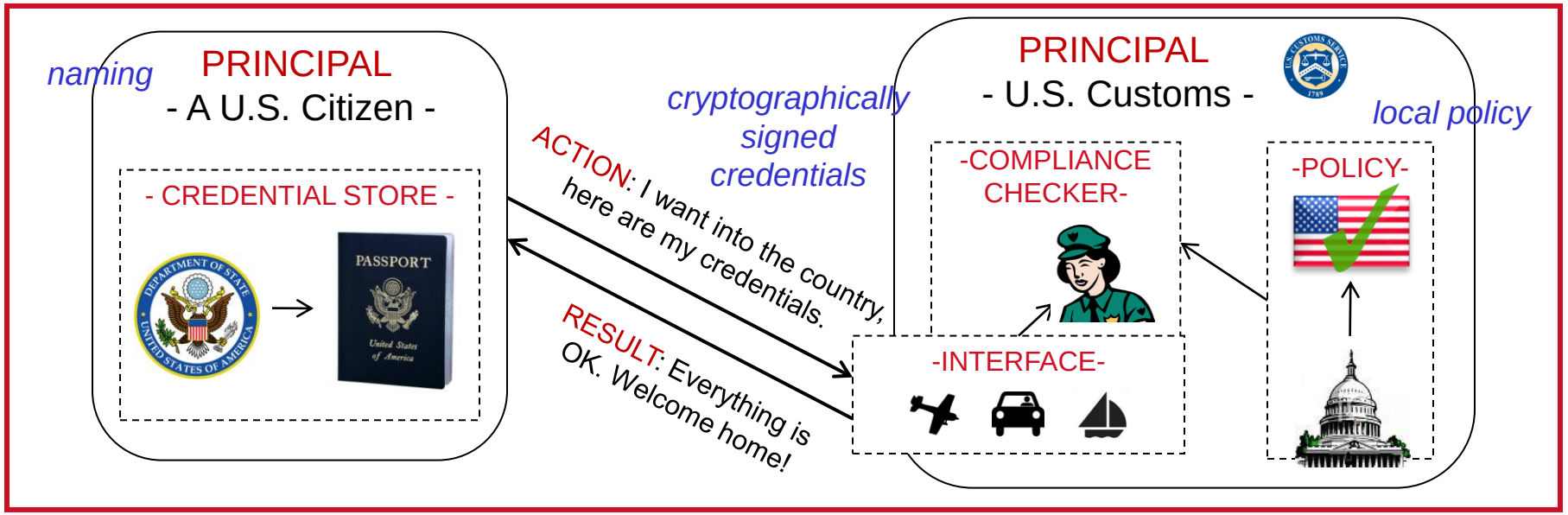
Reasoning about Trust

- Trust is often based on *transitive* trust
  - I trust Alice since I trust Bob and Bob trusts Alice
- But *degree* of trust is more subtle
  - I trust Alice less than Bob, with whom I vacation (*i.e.*, my knowledge of Bob is better, and direct)
- Trust is dynamic
  - More experience with Alice, Bob cheats me, …
  - As examples show, increases *and* decreases

Dependencies and Independence

- Trust is often based on *assumptions* of trust
  - This creates a chain of dependencies
  - See Thompson, "Reflections on Trusting Trust"
- Most SW systems assume HW trusted
  - "FPGA Viruses", Hazdic, Udani, Smith, FPL '99
  - "Overcoming an Untrusted TCB", Hicks, Finnicum, King, Martin, Smith, S&P '10
- Desiderata: Independent attestation
  - Thinking Bayes: Pr(good) = 1-$Pr(bad_1)*Pr(bad_2)*\ldots$

Blaze, *et al.*, "Trust Management" supports *dependent and independent trust*



DISTRIBUTED authorization and compliance checking

Policies may be dynamically introduced by multiple authorities

Computer

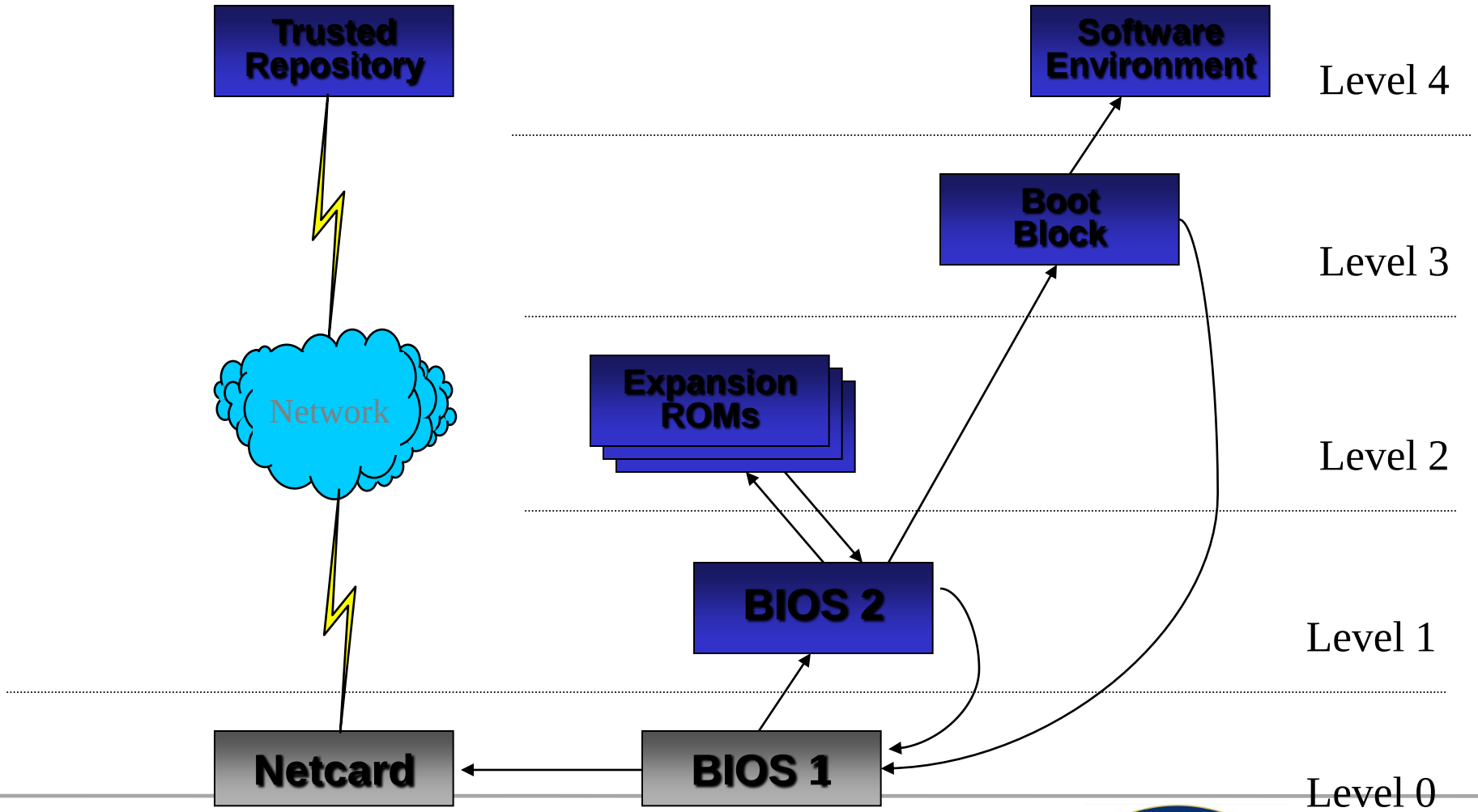
Dynamic Trust Management

February 2009 (vol. 42 no. 2)

pp. 44-52

Matt Blaze, University of Pennsylvania
Sampath Kannan, University of Pennsylvania
Insup Lee, University of Pennsylvania
Oleg Sokolsky, University of Pennsylvania
Jonathan M. Smith, University of Pennsylvania
Angelos D. Keromytis, Columbia University
Wenke Lee, Georgia Institute of Technology

Root of Trust – Arbaugh's AEGIS (Oakland '97)



Evidence of Trust

- Multiple independent sources for attestation
  - E.g., voting TPMs with secured access (crypto)
- Minimal dependent sources
  - Rely as much as possible on differential integrity
  - Secure Boot on TPM
- Robust integrity checks
  - Chaining Layered Integrity Checks
- Dynamics – situational awareness
- Recovery strategies using independence

Quantitative Trust Management (Eurosec '09)