

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

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 10 JUN 2010		2. REPORT TYPE		3. DATES COVERED 00-00-2010 to 00-00-2010	
4. TITLE AND SUBTITLE Cyberwarfare, botnets and trust				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) University of Pennsylvania, Computer and Information Science, 3451 Walnut St, Philadelphia, PA, 19104				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES MURI Review, June 2010. U.S. Government or Federal Rights License					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 20	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

What is cyberwarfare?

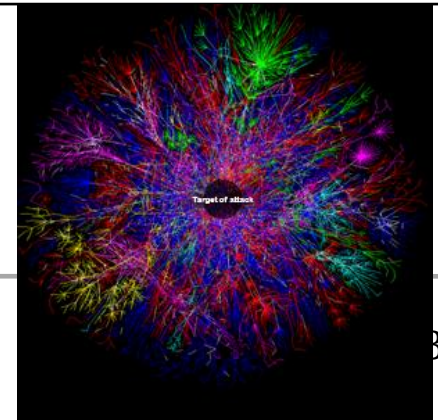
- Attacks against adversary using computers as weapons
 - And, defense against such attacks
- Goal is attack/defense of nation(s)
 - Issues are scale, capabilities, willingness



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



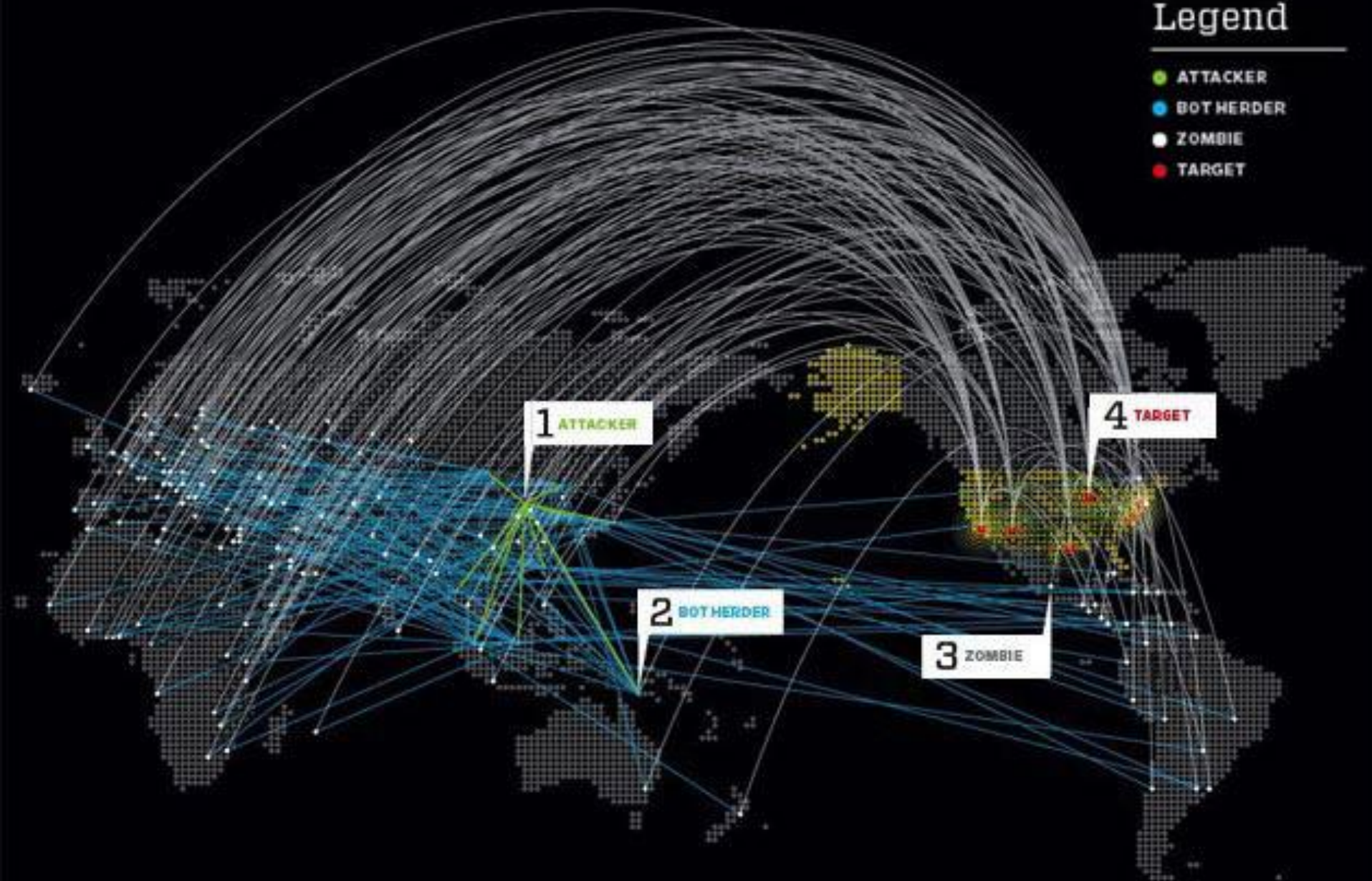
Review

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

Legend

- ATTACKER
- BOT HERDER
- ZOMBIE
- TARGET



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."

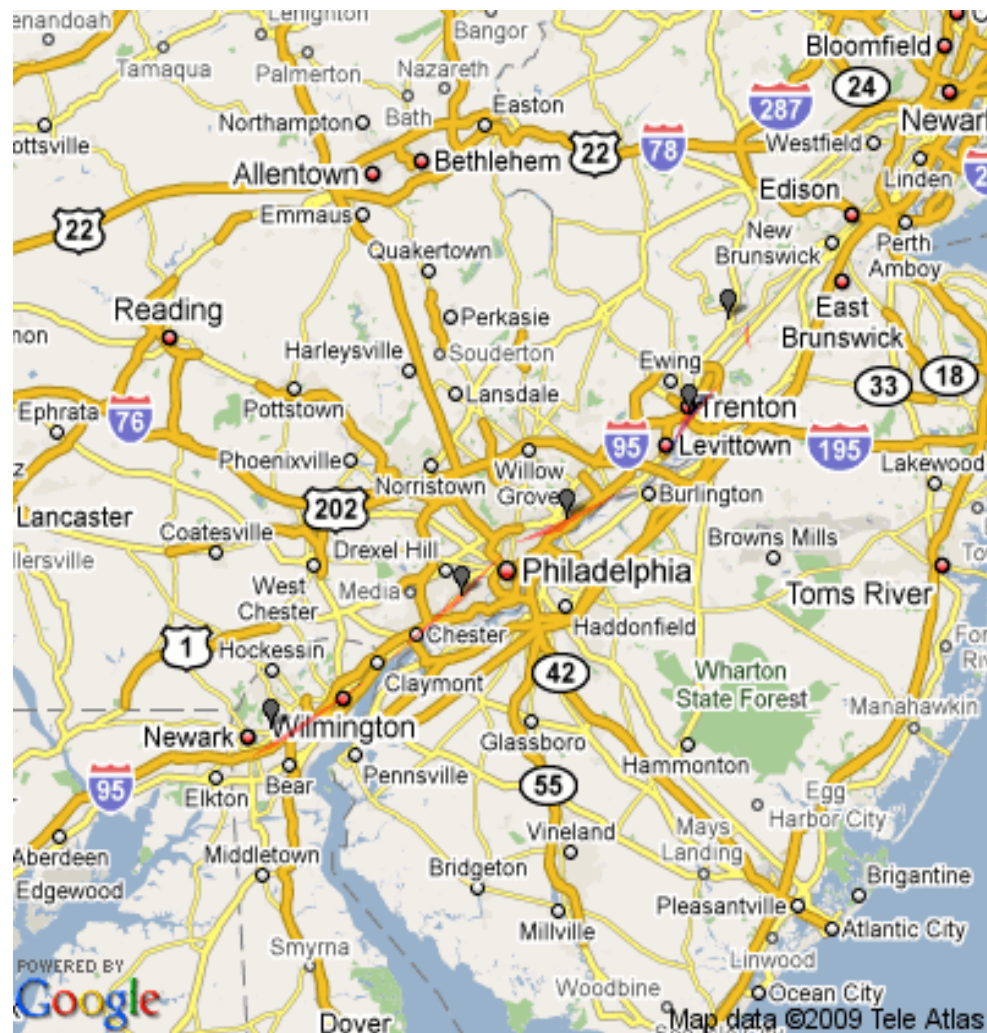
Botnets

- 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

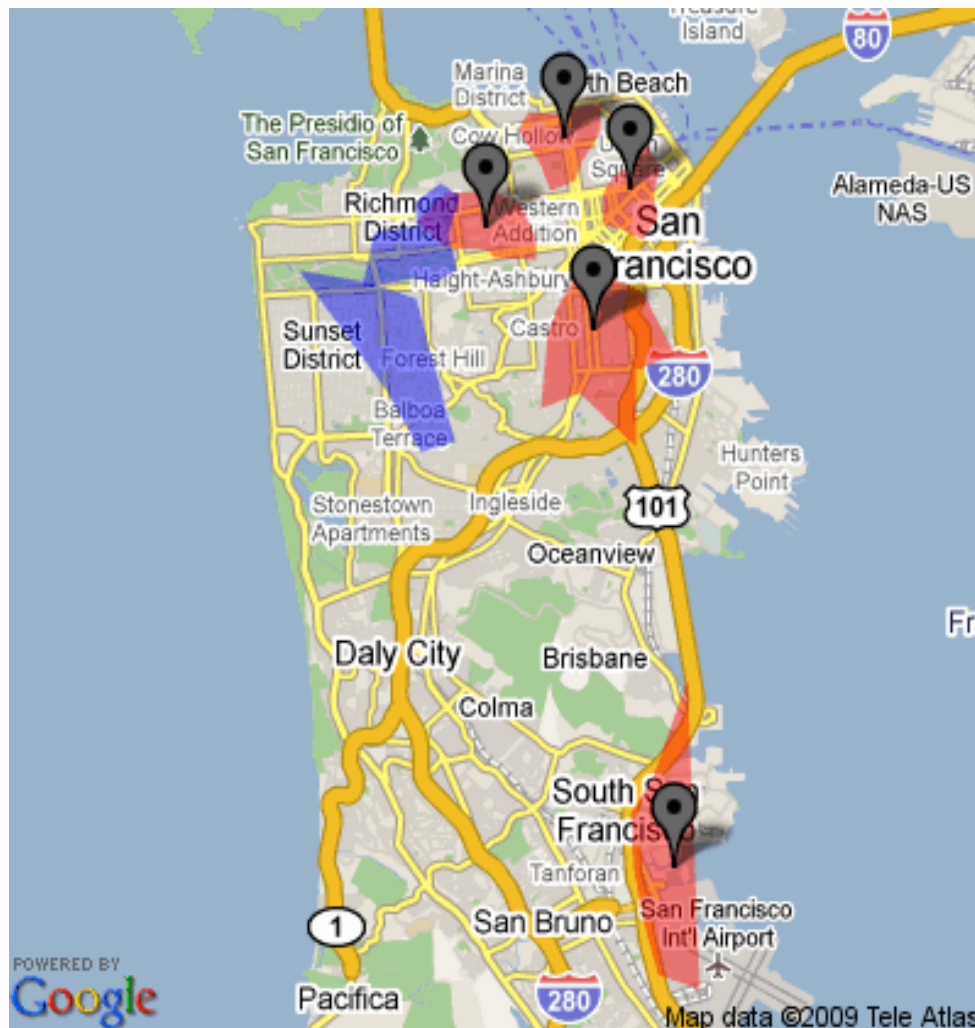
Humanets

- 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?

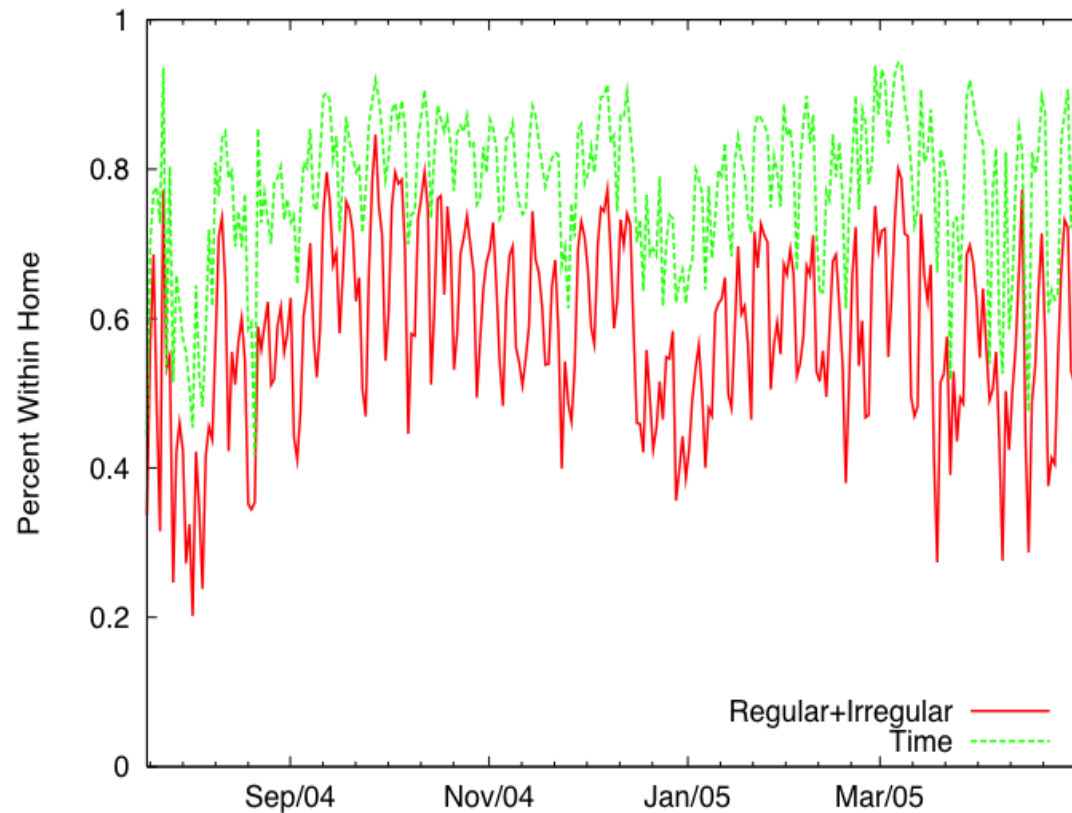
Capture data from G-1



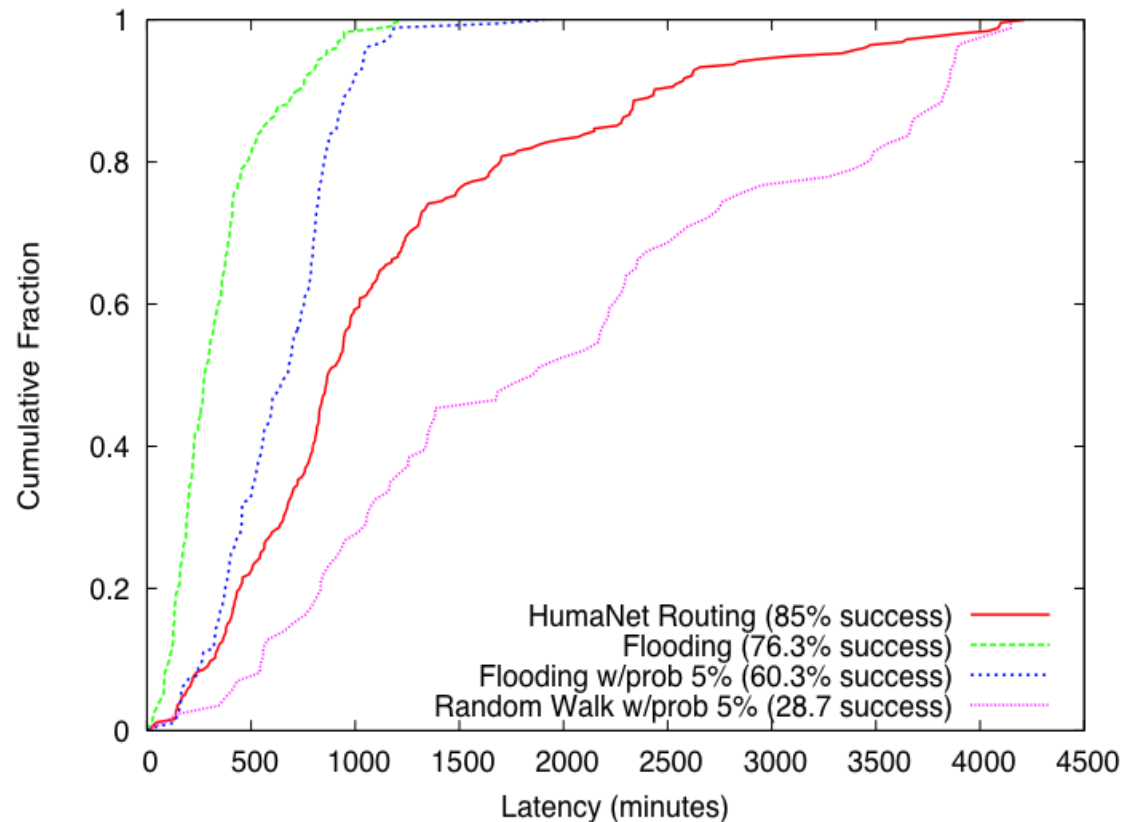
Location data from S.F. Cabs



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?

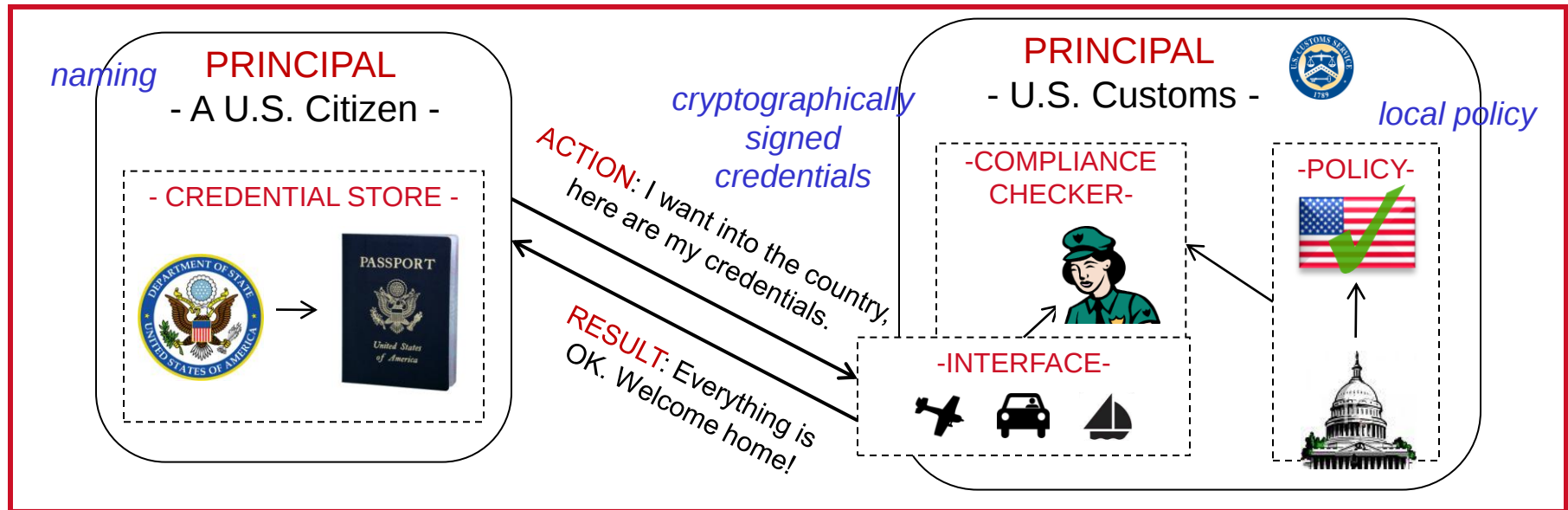
Reasoning about Trust

- 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: $\Pr(\text{good}) = 1 - \Pr(\text{bad}_1) * \Pr(\text{bad}_2) * \dots$

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

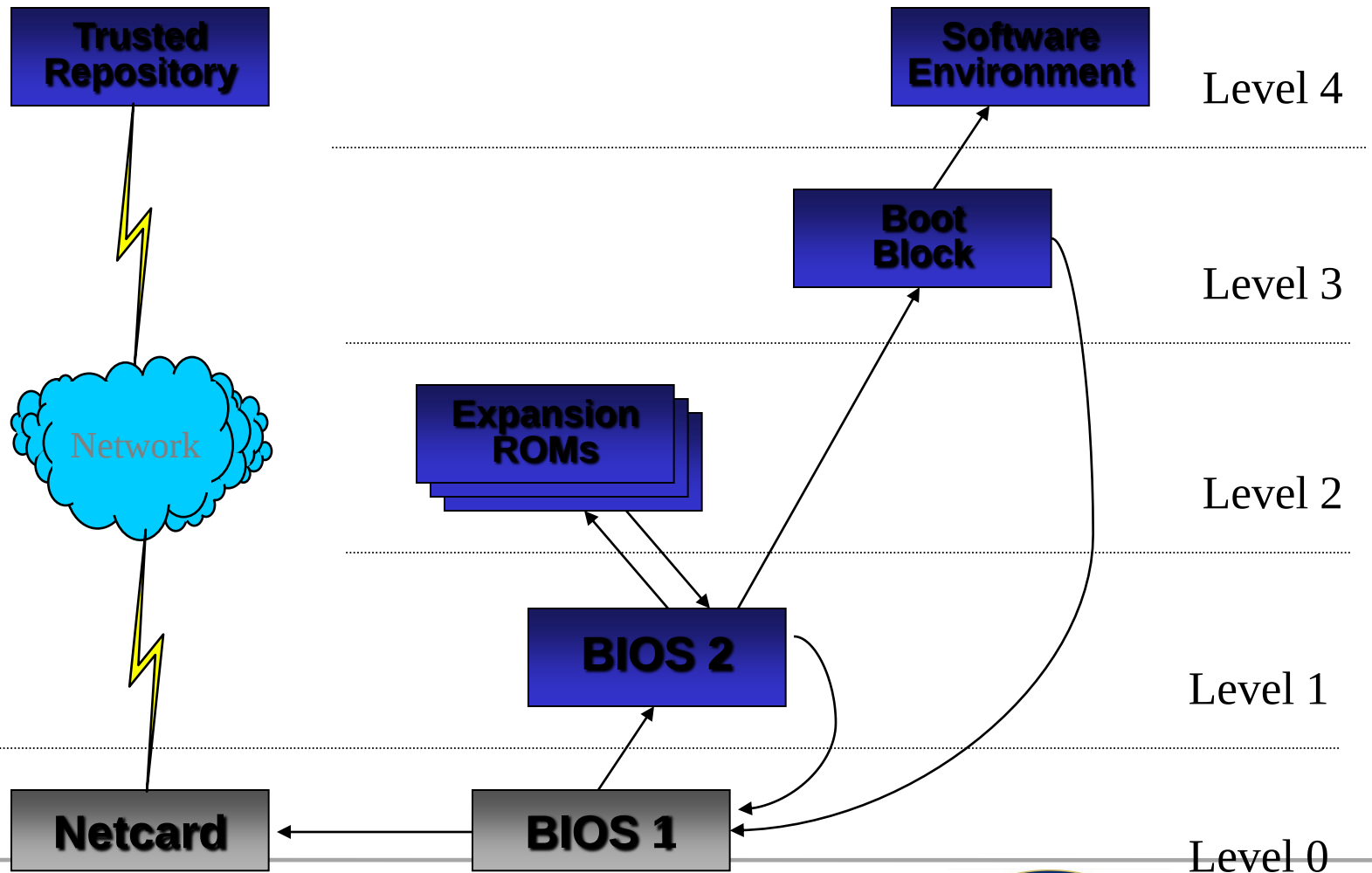
Jonathan M. Smith, University of Pennsylvania

Angelos D. Keromytis, Columbia University

Wenke Lee, Georgia Institute of Technology

W

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)

