Foundational and Systems Support for Quantitative Trust Management (QTM)

Insup Lee (PI)
Computer and Information Science
University of Pennsylvania

ONR MURI N00014-07-1-0907
Review Meeting
June 10, 2010
Project Team

Principal Investigators

- **Sampath Kannan** (Ph.D 89, Berkeley)
  Stream Algorithms, Run-time monitoring, Cryptography
- **Insup Lee** (Ph.D. 83, Wisconsin)
  Real-time and cyber-physical systems, Run-time monitoring
- **Matt Blaze** (Ph.D. 93, Princeton)
  Network security, Cryptography, Trust Management
- **Oleg Sokolsky** (Ph.D. 96, SUNY-SB)
  Formal methods, Real-time and hybrid systems
- **Jonathan Smith** (Ph.D. 89, Columbia)
  Networking, Security and privacy, Mobility
- **Angelos Keromytis** (Ph.D. 01, Penn)
  Computer security, Cryptography, Networking
- **Wenke Lee** (Ph.D. 99, Columbia)
  System and network security, Applied cryptography, Data mining

• Students
  - Adam Aviv, Jian Chang, Nikhil Dinesh, Zhiyi Huang, Andrew West, David Dagon, Manos Antonakakis, Yacin Nadji, Matt Burnside, Vasilis Pappas, Stelios Sidiropoulou

• Postdocs
  - Daniel Luo, Roberto Perdisci, Vinayak Prabhu, Krishna Venkatasubramanian

• Collaborators
  - Nick Feamster, Boon Loo, Aravind Joshi, Jason Nieh
Trust

- Webster’s Dictionary: TRUST, -noun:
  - (1) Assured reliance on the character, ability, strength, or truth of someone or something.
  - (2) One in which confidence is placed.

- Our Definition:
  - Trust is the expectation of a trustor with respect to certain properties of a trustee or her actions under a specified context and time, considering the risks, incentives, and historical information.
Policy-Based Trust Mgmt. (PTM)
- Effective for delegated credentials and access enforcement
- Can’t handle uncertainty and partial information

Rep-Based Trust Mgmt. (RTM)
- Quantifies trust relationships
- No delegation (i.e., reputation no-transferable)
- No enforcement

QUANTITATIVE TRUST MANAGEMENT (QTM)
- Combine PTM and RTM
- Dynamic interpretation of authorization policies for access control decisions based on evolving reputations of the entities involved
QTM Challenges

• What are some metrics for effectiveness of TM systems?
• How do we incorporate uncertainty in policy-based TM’s?
• How do we incorporate dynamism in policy-based TM’s?
• How can we model adversaries as economic agents and develop a game-theoretic view of trust management?
• Can we build new reputation management systems based on sound principles?
• What is the proper way to mathematically combine reputations?
  – Involves integration of logical/quantitative/probabilistic reasoning
  – Is there a means to build consensus from distributed observations?
• How do we integrate policy-based and reputation-based TMs?
• What are some important applications of TM systems?
Quantitative Trust Management (QTM)

[Diagram showing the process of QTM with various components including Local Policy, Policy Evaluation Engine, TDG Extractor, TDG, Policy-Based Trust Manager, Trust Quantifier, TV, Context Information, Decision Maker, Decision Manager, Action, Request & Credentials, Reputation Database, Reputation-Based Trust Manager, Feedback, Re却uation Engine, and Decision Manager.]

6/10/10
Policy-based Trust Management (PTM)
Collaboration

Reputation-based Trust Management (RTM)

Evaluating RTM Systems

Blacklist as Feedback of Reputation Management
Collaboration

Policy-based Trust Management (PTM)

- Local Policy
- TDG Extractor
- Reputation Algorithm
- TDG
- Reputation Database
- Reputation Quantifier
- Request & Credentials
- Policy Evaluation Engine

Reputation-based Trust Management (RTM)

- Context Information
- TV
- Decision Meta-Policy
- Decision Manager
- Action

Quantitative Trust Management (QTM)

- Decision Maker
- TDG
- Metapolicy

Contributors:

- Oleg Sokolsky: formal methods, hybrid systems
- Insup Lee: cyber-physical systems
- Sampath Kannan: algorithms, cryptography
- Matt Blaze: trust management
- Jonathan Smith: network security and privacy
- Angelos Keromytis: network security, cryptography
- Wenke Lee: intrusion detection, data mining
- Insup Lee: cyber-physical systems
- Angelos Keromytis: network security, cryptography

6/10/10
Team Efforts

• Several Research Collaborations
  – Distributed TM, Dynamic TM, Spatio-Temporal Reputations, …
  – Keynote-based QTM (QuanTM)
• Many Tele-conferences and Student Visits
  – Penn -> GA Tech, Columbia -> Penn, GA Tech -> Penn
• Collaborative case studies
  – SPAM list and BGP security as QTM application
• PhD Dissertation Committees
  – Matt Burnside (Columbia)
  – David Dagon (GA Tech)
  – Andrew West (Penn)
Education

- **Courses**
  - Integrated material into COMS W4180 course (Columbia)
  - CIS 125 new course on understanding of existing and emerging technologies, along with the political, societal and economic impacts of those technologies (Penn)
  - Integrated material into CIS 551 (Penn)
  - Material on botnet detection added to Network Security classes: undergraduate cs4237, and graduate cs6262 (GA Tech)
  - 3 senior design projects (Penn)

- **Workforce training**
  - 3 post-docs
  - 10 Ph.D. students
  - 1 Masters and 1 undergraduate
Publication

• Publications
  – 7 journal articles
  – 2 book chapter
  – 33 conference papers

• Selected papers
Dissemination & Tech transfer

• Beyond conference talks
  – 7 invited and 2 keynote talks, 6 panels
• Working with Symantec to determine modus operandi of rogue Antivirus sites (and why users trust them)
  – Interim Symantec Threat Report (ISTR), Oct 09
• Working with Damballa to deliver botnet detection and mitigation technologies to government and enterprise customers
  – Botnet detection system such as BotMiner malware analysis technologies, and the DNS-based monitoring technologies
  – Several Ph.D. students did summer internship
  – Several Damballa researchers were former students at Georgia Tech, and still participate in some of the research meetings at Georgia Tech
• Matt Burnside now working for NSA
• QTM ideas used in ONR-supported "Networks Opposing Botnets" (NoBot) project, with Penn, Harvard and Princeton
Updates since Nov 2009

- **Award**
  - Georgia Tech Sigma Xi Faculty Best Paper Award

- **Publications**
Publications (con’d)


• Book Chapters


Research highlights

- Project Overview, Insup Lee (PI)
- QuanTM Architecture for Web Services, Insup Lee
- Reflections on Trust Evidence, Jonathan M. Smith
- Distributed Trust Management and Rogue AV Software, Angelos Keromytis
- Dynamic IP Reputations from DNS, Wenke Lee
- Detecting Wikipedia Vandalism via Spatio-Temporal Analysis of Revision Metadata, Andrew West
- AS-CRED: Reputation based Trustworthy Inter-domain Routing, Krishna Venkatasubramanian
- Permission to Speak: A Novel Formal Foundation for Access Control, Oleg Sokolsky
- Reputations and Games, Sampath Kannan
- Demo Session
- Future Work and Discussion, Insup Lee