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

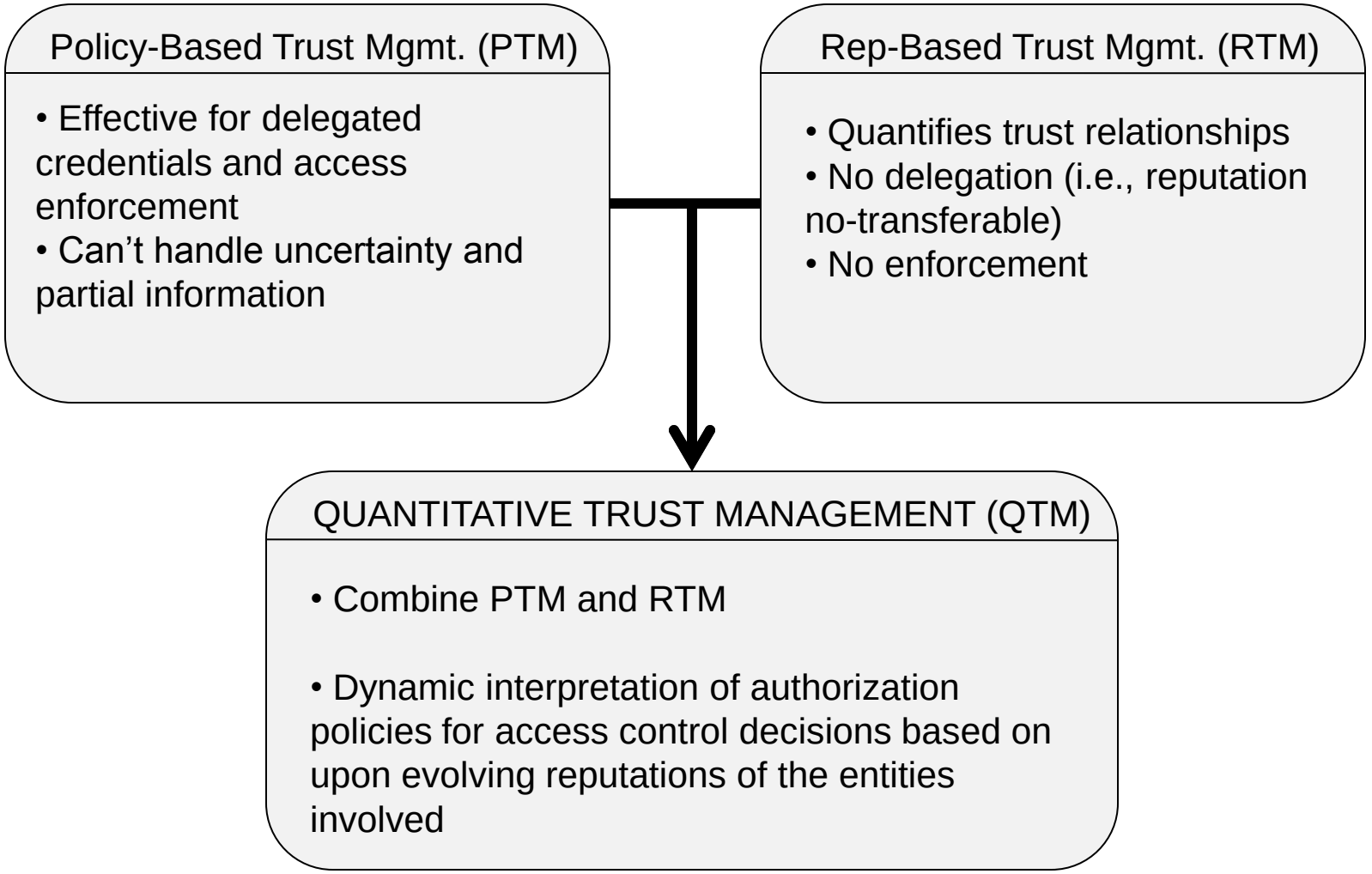
- Students
  - Adam Aviv, Jian Chang, Nikhil Dinesh, Zhiyi Huang, Andrew West, David Dagon, Manos Antonakakis, Yacin Nadji, Matt Burnside, Vasilis Pappas, Stelios Sidiroglou
- Postdocs
  - Daniel Luo, Roberto Perdisci, Vinayak Prabhu, Krishna Venkatasubramanian,
- Collaborators
  - Nick Feamster, Boon 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**.

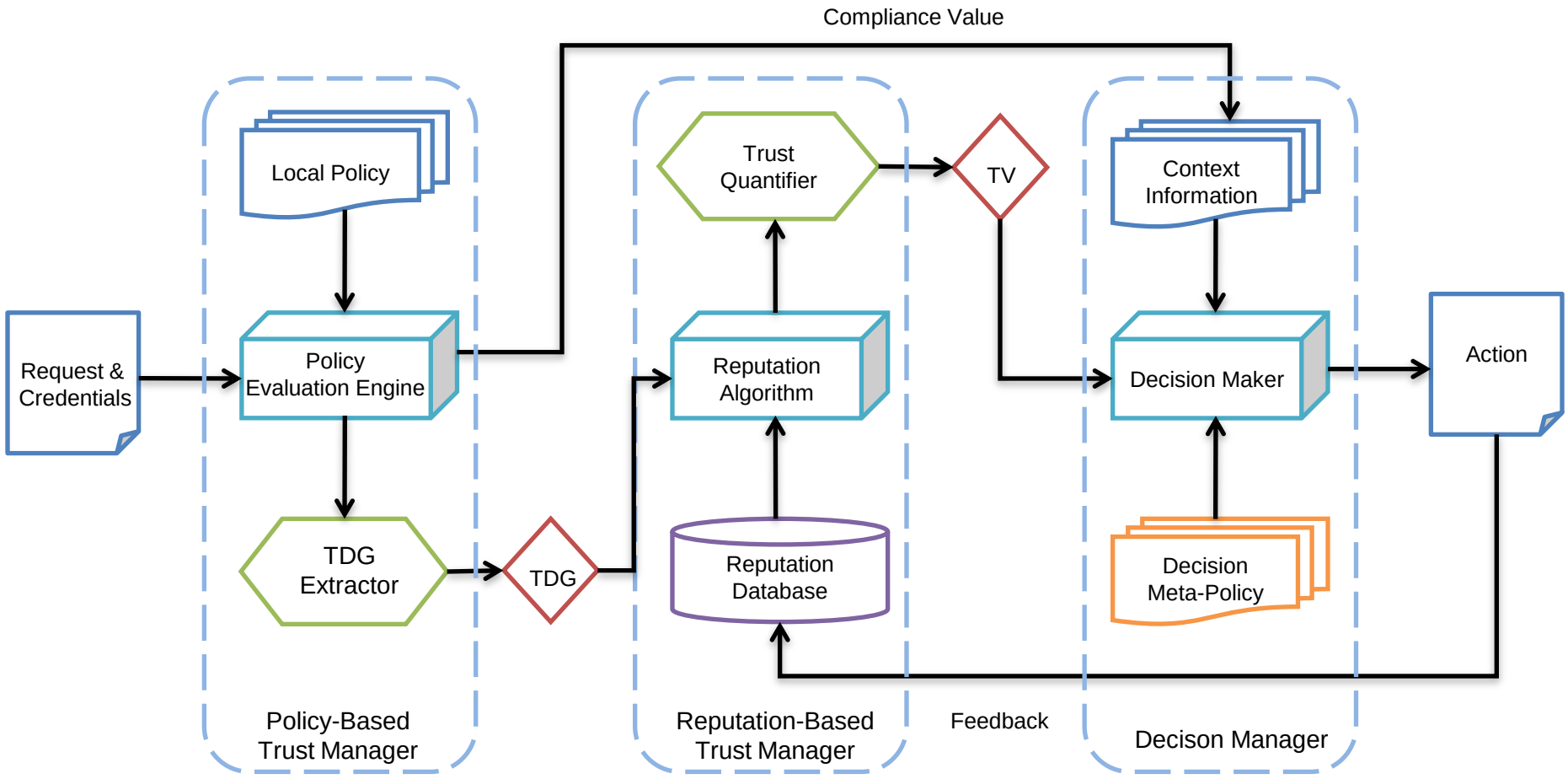
Trust Management



QTM Challenges

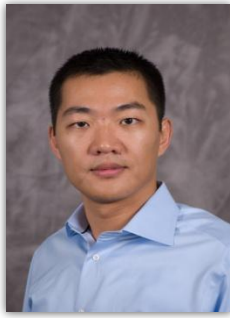
- What are some metrics for effectiveness of TM systems?
- How do we incorporate uncertainty in policy-based TM's?
- How do we incorporate dynamism in policy-based TM's?
- How can we model adversaries as **economic agents** and develop a **game-theoretic view** of trust management?
- Can we build new 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)



Collaboration

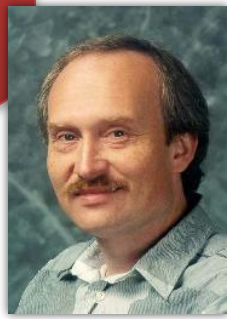
Policy-based Trust Management (PTM)



- KeyNote PTM Systems
- Permission-to-Speak
- Dynamic Trust Management Arachne

Collaboration

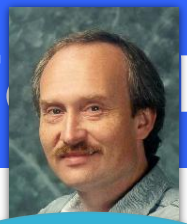
Reputation-based Trust Management (RTM)



Evaluating RTM Systems

Blacklist as Feedback of Reputation Management

Collabor n



Oleg Sokolsky
formal methods, hybrid systems

Insup Lee
cyber-physical systems

Sampath Kannan
algorithms,cryptography

Policy-based Tru gement (PTM)

Reputation-based T t M ent (RTM)

Quantitative Trust ment (QTM)

Local Policy

TDG Extractor

TV

Context Information

Request & Credentials

Policy Evaluation Engine

Reputation Algorithm

Decision Maker

Action

Reputation Quantifier

TDG

Reputation Database

Decision Meta-Policy

Matt Blaze
trust management

Policy-Based Trust Manager

Reputation-Based Trust Manager

Decison Manager

Jonathan Smith
network security and privacy

Angelos Keromytis
network security, cryptography

Wenke Lee
intrusion detection, data mining

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
  - M. Blaze, S. Kannan, I. Lee, O. Sokolsky, J.M. Smith, A.D. Keromytis, and W. Lee. Dynamic Trust Management, In IEEE Computer Magazine, vol. 42, no. 2, pp. 44 - 52, February 2009.
  - A.G. West, A.J. Aviv, J. Chang, V. Prabhu, M. Blaze, S. Kannan, I. Lee, J.M. Smith, and O. Sokolsky. QuanTM: A Quantitative Trust Management System. EUROSEC 2009, pp. 28-35.
  - A.G. West, I. Lee, S. Kannan, and O. Sokolsky. An Evaluation Framework for Reputation Management Systems. In *Trust Modeling and Management in Digital Environments: From Social Concept to System Development* (Zheng Yan, ed.), 2009.

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, withPenn, Harvard and Princeton

Updates since Nov 2009

- Award
  - Georgia Tech Sigma Xi Faculty Best Paper Award
- Publications
  - J. Chang, K. Venkatasubramanian, A. G. West, S. Kannan, I. Lee, B. T. Loo, O. Sokolsky "AS-CRED: Reputation Service For Trustworthy Inter-Domain Routing", University of Pennsylvania Technical Report, CIS-MS-10-17, April, 2010
  - "An Analysis of Rogue AV Campaigns"Marco Cova, Corrado Leita, Olivier Thonnard, Angelos D. Keromytis, and Marc Dacier. To appear in Proceedings of the 13th International Symposium on Recent Advances in Intrusion Detection (RAID). September 2010, Ottawa, Canada.
  - Detecting Malicious Flux Service Networks through Passive Analysis of Recursive DNS Traces. Roberto Perdisci, Igino Corona, David Dagon, and Wenke Lee. In Proceedings of *The 25th Annual Computer Security Applications Conference (ACSAC 2009), Honolulu, HI, December 2009.*
  - *On the Incoherencies in Web Browser Access Control Policies. Kapil Singh, Alexander Moshchuk, Helen J. Wang, and Wenke Lee. In Proceedings of The 2010 IEEE Symposium on Security and Privacy, Oakland, CA, May 2010.*
  - *Building a Dynamic Reputation System for DNS. Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee, and Nick Feamster. In Proceedings of the 19th USENIX Security Symposium, Washington DC, August, 2010 (to appear).*
  - J. Chang, K. Venkatasubramanian, A. G. West, S. Kannan, I. Lee, B. T. Loo, O. Sokolsky "AS-CRED: Reputation Service For Trustworthy Inter-Domain Routing", Submitted for publication, 2010.

Publications (con'd)

- "Detecting Wikipedia Vandalism via Spatio-Temporal Analysis of Revision Metadata". Andrew G. West, Sampath Kannan, and Insup Lee. In EUROSEC '10: Proceedings of the Third European Workshop on System Security, pp. 22–28, Paris, France. April 2010.
- Book Chapters
- "An Evaluation Framework for Reputation Management Systems". Andrew G. West, Insup Lee, Sampath Kannan, and Oleg Sokolsky. Book chapter in Trust Modeling and Management in Digital Environments: From Social Concept to System Development (Zheng Yan, ed.), pp. 282–308. Information Science Reference, Hershey, PA, USA, 2010.
- "Detecting Wikipedia vandalism via spatio-temporal analysis of revision metadata". Andrew G. West, Sampath Kannan, and Insup Lee. Technical Report MS-CIS-10-05, University of Pennsylvania, Dept. of Computer and Information Science, February 2010.
- "Mitigating spam using spatio-temporal reputation". Andrew G. West, Adam J. Aviv, Jian Chang, and Insup Lee. Technical Report MS-CIS-10-04, University of Pennsylvania, Department of Computer and Information Science, February 2010.Demonstrations, Tutorials, and Posters
- "STiki: An anti-vandalism tool for Wikipedia using spatio-temporal analysis of revision metadata". Andrew G. West, Sampath Kannan, and Insup Lee. Formal demonstration. To appear in WikiSym '10: Proceedings of the Sixth International Symposium on Wikis and Open Collaboration, Gda´nsk, Poland. July 2010.
- "Spatio-temporal analysis of Wikipedia metadata and the STiki anti-vandalism tool". Andrew G. West, Sampath Kannan, and Insup Lee. Poster. To appear in WikiSym '10: Proceedings of the Sixth International Symposium on Wikis and Open Collaboration, Gda´nsk, Poland. July 2010.Talks (without associated proceedings)
- "STiki: An anti-vandalism tool for Wikipedia". Andrew G. West, Sampath Kannan, and Insup Lee. Talk. To be presented at WikiMania '10, Gda´nsk, Poland. July 2010.

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