Exposing Trust Assumptions in Distributed Policy Enforcement

Angelos D. Keromytis
Columbia University
DTM – Motivation

• Distributed system defenses built as “islands”
  – Forced to make assumptions re: topology, other defenses …
    • Locally correct, globally incorrect security enforcement
  – Assumptions fail or are exploited by attackers!

• Our work is motivated by real security incidents experienced first hand
  – “Pushing Boulders Uphill: The Difficulty of Network Intrusion Recovery”

• DTM forces these assumptions in the open, allowing systems to verify them continuously
Dynamic Trust Management

- **A COOPERATIVE and DYNAMIC policy evaluation infrastructure that will enable such critical capabilities as:**
  - Adaptation to dynamic service availability
  - Complex situational dynamics (e.g., differentiating between bot-net and physical attacks on infrastructure).
- **BENEFITS of a Dynamic Trust Management approach**
  - Flexible and robust control of authorizations in complex distributed systems such as the DoD/IC GIG
  - The ability to define policies for scalable decentralized defense against emergent cyber-threats by rapid adaptation of resource access limits.
Specific Tasks (Years 1-3)

- Develop language for expressing DTM policies
  - "Arachne: Integrated Enterprise Security Management"

- Design DTM architecture
  - "Asynchronous Policy Evaluation and Enforcement"

- Collaborative/Distributed policy enforcement
  - "F3ildCrypt: End-to-End Protection of Sensitive Information in Web Services"
  - "Path-based Access Control for Enterprise Networks"

- Medium-size case study
  - In progress at Columbia CS Department
Contributions

• Framework for integrating all types of defenses
• Proof of feasibility
  – Prototype, preliminary performance, security analysis
• Initial exploration of design options
• Education (GRA training, coursework integration)
• Outreach (collaboration with Symantec)
Overall Approach

• Define policies that take into consideration system-wide context
  – Extend security mechanisms to emit contextual information (continuous or event-based)
  – Distribute information to interested components
• Integrate IDS/ADS, access control, reaction
• Challenges:
  – Accuracy (extracting data from noise)
  – Complexity (defining policies)
  – Performance (scale with users, system, events)
**Arachne**

- **ARACHNE** is a system for the coordinated distribution and evaluation of a system-wide policy on different nodes
  - Several prototype systems for enterprise-level security have been developed
- **GOAL:** Integrate a variety of different, diverse security mechanisms and policy expression methods
  - Achieve enhanced protection over any individual method
  - Allow exchange of information between different mechanisms (Eliminate the possibility of “locally correct” but globally wrong decisions)
  - Capture trade-offs between amount of global context, scalability, etc.
Arachne

- Simple publish-subscribe backend
  - Policies consume and produce events, may revisit decisions based on new information
  - “Sessions” group related components
  - Graph-based policies, can be learned and refined
Other work

• Path-based policy enforcement
  – Simplification of Arachne (weaker properties, higher performance), well suited for web SOAs

• Selective data protection in web SOAs
  – Limit data theft/leakage risks by using web client as vantage point that encrypts data to specific SOA components

• Study of Rogue Antivirus sites (with Symantec)
Lessons Learned

• Coordinated defenses appear to be feasible
• Writing policies from scratch is hard
  – Exposing assumptions requires people to think about what assumptions they are making
    • Not always obvious!
• Learning interaction policies is promising
  – Someone still needs to define component policies
• Performance does not appear to be show-stopper
• Accuracy remains to be seen (current focus)
Outreach and Education

• Integrated material into COMS W4180 course
• 2 invited talks (beyond conference talks) and 1 panel
• Main Ph.D. GRA now working for NSA
• Working with Symantec to determine modus operandi of rogue AV sites (and why users trust them)
  – Preliminary results published in the October 2009 Interim Symantec Threat Report (ISTR)

Future Directions

• Continue work on refining architecture and system
  – Explore performance/scalability, effectiveness, overhead tradeoffs

• Integrate with QTM
  – Particularly important in federated systems (e.g., dynamically composable SOAs)

• Large-scale case study
Future Directions

• Investigate the use of reactive mechanisms
  – Global coordination of dynamic defenses

• Investigate the use of active deception
  – Possible integration into NCR
Expected Contributions in Years 4 & 5

- Proof of feasibility
  - Experimentation in real environment
- Exploration of design and implementation space
- Use of active defenses and deceit
  - Can we challenge attackers’ (trust) assumptions?
Summary

• Exploring systems that allow (and require) explicit assumption (trust) declarations
• All deliverables on track (or done) for Years 1-3
• Interesting new directions and capabilities to be explored in Years 4-5