An Adversarial Experimental Platform for Privacy and Anonymity

Ben Zhao, U. C. Santa Barbara

NSF GENI Security Workshop, January 2009

Disclaimer

- This sounds a lot like Nikita’s ideas on testing Tor on GENI
  - Independent idea, similar in some ways, different in others
- Key difference
  - Focus on general privacy/anonymization techniques
  - Focus on fine grain data collection and data measurement, tracing, and replay
- Clearly, he and I will talk ☺

A Need for Experimental Privacy

- Internet privacy an increasingly important topic
  - Anonymity relevant to new popular applications
  - E.g. VoIP, content sharing, remote machine control, secure data access, social networks
- Experimental evaluation critical, but challenging
  - Real world often different from analysis of idealized protocols
    - Assumptions often unrealistic
    - Real world factors key to breaking secure protocols
    - E.g. network/node dynamics, resource heterogeneity
  - Challenging to setup and deploy
  - Thorny legal issues w/ deployed services

Dream for Privacy Experimentalists

- What would we really like to have?
  - Experiments on popular privacy protocols with real users
    - What are real traffic patterns and user behavior patterns?
    - How do users react to attacks/DoS in real time?
  - Publicly available traces for repeatable, realistic experimentation
  - Adversarial evaluation of anonymity protocols and attacks

An Adversarial Measurement Platform

- Outcomes
  - Real users, waived legal rights (naïve?)
  - Re-evaluation of commonly accepted assumptions
  - Real-time anonymity attacks and defenses
  - Detailed, anonymized traces for public consumption

What Do We Need / Questions

- Possible requirements from GENI
  - Detailed traffic capture/logging at routers
  - Well-instrumented VMs for user-controlled network dynamics
  - IP- and DNS-level firewalls to enforce AUPs
  - Central directory for privacy-enhanced/anonymous applications and services
- Questions and issues
  - Timers, time synchronization, accuracy
  - Access or access control to external sites
  - Preventing pollution by legally questionable content
  - Isolating/identifying anonymous traffic