

Student Presentations

CS6V81-002: Language-based
Security

January 16, 2008

Presentation Specs

- Length: ~45 min.
 - 10 min. for quiz, 20 min. for discussion
 - some discussion during talk
 - plan to be interrupted
- Media
 - use slides (I will put them on website)
 - handouts too, if desired
 - whiteboard too, if you wish
- Topics
 - cover mandatory reading (first paper listed)
 - supplemental readings too, if you wish
 - use material from related work (e.g., cited references) to explain, but don't expect prior knowledge

Presentation Structure

- Explain the problem
 - What are traditional solutions?
 - Why are they insufficient / suboptimal?
- Explain the solution in a nutshell
 - What was implemented?
 - What conceptual breakthroughs?
 - How does it improve upon traditional solutions?
 - What are the limitations?
- Technical content (majority of talk)
 - should prepare student to do a project
 - explain important notational conventions
 - teach MAIN technical points (don't attempt everything!)
- Conclusions
 - explain limitations
 - pose interesting discussion questions
 - propose future work

Slide Tips

- Avoid...
 - animated bullet lists
 - full sentences (keep slide text brief!)
 - graphical backgrounds that obscure the text
 - huge diagrams that nobody can read
- Prefer...
 - pictures / diagrams / graphs
 - elucidating animations
- Citations
 - always cite!
 - include all last names, year, journal/conference acronym
 - no “et al.”
 - full citations for major works referenced on last slide

Pitfalls

- No suspense, no surprise endings
- Don't over-philosophize
- Timing
 - you won't have enough time
 - rehearse your timing at least once
 - be flexible (have a plan B)
- Educate, don't obfuscate
 - usually more of an issue when presenting your own work...
- Use Correct Terminology
 - security terminology is well-established and specific
 - making up new words to replace established terms is bad

Terminology

- Security Goals
 - integrity – trustworthiness of data/resources (no unauthorized changes permitted)
 - confidentiality – concealment of data/resources (“need to know” vs. “need to share”)
 - availability – ability to use data/resources desired
- Security Policies
 - safety – some “bad thing” doesn’t happen
 - liveness – some “good thing” eventually happens
 - information flow – secret inputs do not flow to public outputs
 - non-interference – public outputs do not depend upon secret inputs
 - access control – read/write/execute permission based on user privs
 - discretionary – privileges defined by certain users (e.g., root)
 - mandatory – privileges hardcoded into system
 - “end-to-end” security policies

Attacks

- Attacks and Attacker Models
 - threat – a potential violation of security
 - attack – actions intended to violate security
 - attacker – entity performing an attack
 - attacker model – capabilities of an attacker
 - vulnerability – flaw which could be exploited to violate security
 - principal – entity with security privileges (person, code, etc.)
 - man-in-the-middle – attacker who intercepts messages
- Varieties of Attacks
 - virus – malware that propagates by user action (e.g., email)
 - worm – malware that propagates automatically
 - denial-of-service (DoS) – attack that violates availability
 - flood attack – DoS attack that overloads victim with junk data
- The Gold Standard: Authentication, Authorization, Audit

Cryptography

- Public Key Encryption (asymmetric encryption)
 - public key (K) is disclosed
 - private key (k) withheld
 - $M = \langle \langle M \rangle_K \rangle_k = \langle \langle M \rangle_k \rangle_K$
 - Secure communication: Receive $\langle M \rangle_K$
 - Digital Signature: Disclose $\langle M \rangle_k$
- Secure Hash Functions
 - maps large plaintext to smaller hashcode
 - one-way (hard to recover plaintext from hash)
 - few collisions (but not usually one-to-one)
 - hard to find any plaintext that hashes to a particular hashcode

Next Time

- Monday no class (MLK Day)
- Wednesday
 - quiz on SFI paper
 - first student presentation (Scott)