CSE543 - Introduction to Computer and Network Security
Module: Final review

Professor Trent Jaeger
Fall 2012
Since Midterm

- Firewalls
- Intrusion Detection
- Malware
- Botnets
- Web Security
- Virtualization
- Cloud
- Trusted Computing
Before Midterm

- Cryptography (Algorithms)
- Applied Cryptography (Protocols)
- Authentication
- PKI
- Access Control
- OS Security
Know from 1st Midterm

- Cryptography (Algorithms)
- Applied Cryptography (Protocols)
  - Cookies, Trusted Computing
- Authentication
  - SSL
- PKI
  - DAA, SSL
- Access Control
  - Firewalls, Virtualization
- OS Security
  - Web Security, Virtualization, Cloud
Stuff from Before Midterm

- Cryptography (Algorithms)
- Applied Cryptography (Protocols)
  - Hash functions, signatures, ...
- Authentication
  - Kerberos
- PKI
  - PKI
- Access Control
  - Concepts and Models
- OS Security
  - Multics, Capability Systems
Since Midterm

• Firewalls
  • Policy spec, Wool study, iptables (concepts)

• Intrusion Detection
  • Host and network, misuse and anomaly, Forrest, Bayes

• Malware
  • types, propagation, DoS, Defenses

• Botnets
  • Definition, Botnet cycle, Botnet size estimation

• Web Security
  • Cookies, SSL, Dynamic content attacks, Server security, OP
Examples

• Firewalls
  • Given a set of requirements, write a sufficient set of firewall rules
  • Allow some access
  • Prevent others
  • Don’t forget the “stealth rule”
Examples

• Intrusion Detection
  • What does the Base-Rate Fallacy tell us about false positives in intrusion detection systems? State your answer in terms of the probability of key events.
Examples

• Intrusion Detection

• What does the Base-Rate Fallacy tell us about false positives in intrusion detection systems? State your answer in terms of the probability of key events.

answer: BRF states that if the probability of an accurate detection is high, the number of false positives may still be high. The false positive rate depends on the probability of a detection and the probability of an intrusion. If the latter is very low, even a very accurate detection will not be effective.
Examples

• Malware
  • Design a puzzle to stop a DoS attack

• Cost of puzzle
• Cost of checking
• Relate via a formula
Examples

- Botnets
  - Methods for botnet size estimation
  - See so many DNS blacklist requests
  - What is the infection footprint?
  - What is the effective botnet size?
Examples

• Web security
  • Implement single-signon using cookies

• Design cookie
Examples

• Virtualization

• Why must a “sensitive” instruction be “privileged” in a secure virtualized environment?

• Complete mediation. The VMM must be mediate all security-sensitive instructions to implement security checks comprehensively.
Examples

• Cloud
  • Why do cloud insiders create additional security problems when deploying in cloud?
  • What additional threats do users of pre-configured instances care about?
  • What additional threats are caused by co-hosting?
  • Can you prevent/mitigate those threats?

• What’s a side channel?

• Stakeholders
  • What do service providers care about?
  • What do clients care about?
  • What to cloud admins care about?
Examples

• Trusted Computing
  • Extend
  • Seal
  • Build an Attestation
  • Obtain a Public Key via DAA

• Mostly crypto
  • Also need to show how validation works
  • What does validation mean under prescribed circumstances
Deeper Papers

• Key issues? How do they prove? Why convinced or not?

• OP
  • Reference monitor
  • Attack analysis
  • Security analysis

• AmazonIA
  • Attacks, yes, but what about defense?
  • 4 attack types (flaws) in AMIs
  • What was proof for defense for X? Why convinced or not?
    What is missing that would convince you?