Foundations of Network and Computer Security

John Black

Lecture #27
Dec 9th 2004

CSCI 6268/TLEN 5831, Fall 2004
Announcements

• Last Class Today
  – Final Review

• Final Exam on Monday
  – Dec 13th
  – In this room
  – 10:30am – 1:00pm
  – Calculators allowed
  – Closed “book”, closed notes, etc.
About the Final

• Same format as Midterm
  – Short answers, extended topic questions, Justified True/False
  – 11 pages
    • Twice as much time as the midterm, but the final is not twice as long
  – Far fewer “thought problems” than the midterm
    • ie, it’s an easier test
Coverage

• Everything
  – Lectures (incl Ryan’s guest lecture)
  – Quizzes and Midterm
    • Know the answers!
  – Readings
  – Projects

• But does not include:
  – Material I said you were specifically not responsible for
    • Eg, coupon collecting
  – Reading on the web page that was not “assigned reading”
What to Study

• Blockciphers
  – Definition, Security Notions, Feistel, Attacks, DES, AES, DDES, TDES

• Modes of Operations
  – ECB, CBC, CTR
  – One-time-pad
  – Attack models
    • COA, KPA, CPA, CCA
Review (cont)

- **MACs**
  - Syntax, ACMA model
  - CBC MAC, XCBC, UMAC, HMAC

- **Hash Functions**
  - Syntax, applications, MD paradigm, MD theorem, security notions (inversion resistance, $2^{nd}$-preimage resistance, collision resistance), SHA-1, MD5
  - Birthday problem
    - Bounds, how to apply to hash functions
Review (cont)

• Groups
  – Definition, examples
    • $\mathbb{Z}_m$, $\mathbb{Z}_m^*$, $\mathbb{Z}_p^*$
  – Euler’s $\phi$ function, Lagrange’s theorem

• RSA Cryptosystem
  – Key generation, encryption
  – Security
    • Basic RSA bad, factoring is best known attack, factoring technology
  – Implementation
    • Not much…, know the diff between primality testing and factoring!
    • Prime number theorem
      $\pi(n) \sim n/\ln(n)$
Review (cont)

- Digital Signatures
  - Definition, ACMA model, RSA sigs, hash-then-sign
- SSL
  - Outline of protocol, CAs, Man-in-the-middle attacks
- OpenSSL
  - Symmetric key and IV derivation
    - Salt, passphrase, base64 encoding
  - Certificates, administration
  - Structure of projects 1 and 2
Review (cont)

• Networking Basics
  – Routing, basic protocols (IP, UDP, TCP, Eth, ARP, DHCP, DNS, ICMP, BGP), packet formatting
  – IP addresses, subnetting, NAT boxes

• Viruses
  – High-level history (Morris worm, Windows worms, macro viruses)
  – Propagation methods
    • How to own the Internet
Review (cont)

• Trojans
  – Thompson’s Turing Award lecture
  – Rootkits
  – Phishing

• Denial of Service
  – Gibson story
    • Bandwidth saturation, filtering, zombie armies
  – SYN Floods
    • Mechanics, SYN Cookies
  – Reflection attacks, smurfing
  – Backscatter, Traceback, Ingress Filtering
Review (cont)

• Session Hijacking
  – Technique, prevention

• ICC Talk
  – Architecture, network issues, timing, key exchange, mode of operation, blockcipher flaws

• Vulnerabilities
  – Buffer overruns
    • Idea, techniques, machine architecture, calling conventions, stack layout, shellcode
Review (cont)

• Overruns, cont
  – Prevention
    • Non-executing stack, canaries
  – Ways around them
  – Static Analysis

• Off-by-One

• Format String Vulnerabilities
  – What they look like
  – How to exploit
  – Prevention

• Heap Overflows
  – Basic idea only
Review (cont)

- Password Crackers
  - `/etc/passwd`, salt, shadowed password files
- Web Security Overview
  - PHP
  - Disguised URLs
  - XSS
- Wireless Security
  - War driving, SSIDs, MAC Filters
Review (cont)

• WEP
  – Protocol problems
    • Dictionary attack on pads, authentication doesn’t work
  – RC4 problems
    • Uses RC4 in a bad way
    • Details of FMS attack

• Protocol Attacks
  – ARP cache poisoning (ettercap), DNS spoofing, prevention (AuthARP, DNSSEC)
Review (cont)

• Intrusion Detection
  – Static vs Dynamic
  – Profiling
    • Statistical, ML, etc
  – pH-type systems
    • Tracking system calls for each app
  – Mimicry Attacks
    • Nops, building a FSM, finding a sequence
  – Escaping from chroot jail