CS118 Discussion 1A, Week 10

Zengwen Yuan
Dodd Hall 78, Friday 10:00—11:50 a.m.
Logistics

- Final Exam: Thursday, 6/14 11:30am – 2:30pm in Humanities Building A65
  - Roughly 20% before midterm, 80% after midterm
  - Closed book & notes, allow up to 2 double-sided cheat sheets
- Sign up for Project 2 demo!!

- Please complete course evaluation on MyUCLA, thanks!
Network security principles

- Confidentiality
- Authentication
- Integrity
- Access and availability
Corresponding security threats

- Eavesdropping
- Impersonation
- Hijacking/MITM Attack (Man-in-the-middle attacks)
- DoS (Denial of Service)

Courtesy: Alex Afanasyev
Key-based cryptography

• Symmetric key crypto: DES, AES

• Asymmetric key crypto:
  • Diffie-Hellman [2015 Turing Award], RSA [2002 Turing Award]
  • pubkey, private key
Authentication: digital signatures

- Verifiable, non-forgable
- Hash functions:
  - MD5
  - SHA-1
- Digital signature: *signed* message digest
- CA (certificate authority)
SSL: Secure Sockets Layer

- A transport layer protocol (it sits between TCP and Application)
  - variation: TLS protocol
- Benefit: confidentiality, integrity, authentication
- Main steps
  - handshake
  - key derivation
  - data transfer
  - connection closure
More things to know

• IPSec (network layer), VPN, Firewall, IDS …

• How to achieve:
  • Encryption
  • Authentication
  • Digital signature
  • Message integrity
Exercise

• What are the security mechanisms to defend against the following network attacks?
  • Data sniffing & interception
  • IP address spoofing
  • Replay attack
  • Man in the middle attack
  • (Distributed) denial of service attack
  • Email spam
  • Illegal access to UCLA networks
  • Network virus
Study guide & sample final solutions & Project 2