INTRODUCTION TO NETWORK SECURITY

COMP 30650: NETWORKS AND INTERNET SYSTEMS

Dr. Gavin McArdle
Email: gavin.mcardle@ucd.ie
Office: A1.09 Computer Science

RECAP

- Application Layer
  - Http
  - Improving Performance – Page Load Time
    - Persistent Connections
    - Caching
    - CDN

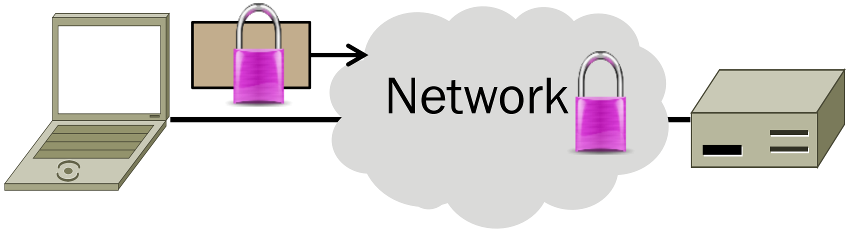
TODAY’S PLAN

- The Bigger Picture
  - From a web Perspective
  - Application to Application Communication across the Internet
- Security
  - Risk Management
  - Cryptology
  - Confidentiality
    - Encryption

NETWORK SECURITY

Network security designs to protect against a variety of threats

- Often build on cryptography



SECURITY THREATS

- Means many things to many people
- Must define the properties we want

Key part of network security is clearly stating the threat model

- The **dangers** and attackers' **abilities**
- Can't assess risk without this key information.

SECURITY THREATS

Some example threats that we need to secure against.

Attacker	Ability	Threat
Eavesdropper	Intercept messages	Read contents of message
Intruder	Compromised host	Tamper with contents of message
Impersonator	Social engineering	Trick party into giving information
Extortionist	Remote / botnet	Disrupt network services

RISK MANAGEMENT

Only as secure as the weakest link

- Could be design flaw or bug in code
- But often the weak link is elsewhere…
  - Passwords shared
  - Unlocked Nodes/Machines

CRYPTOLOGY

Rich history, especially spies / military

- From the Greek “hidden writing”

Cryptography

- Focus is encrypting information

Cryptanalysis

- Focus is how to break codes

Modern emphasis is on codes that are “computationally infeasible” to break

- Takes too long compute solution

USES OF CRYPTOGRAPHY

Encrypting information is useful for more than deterring eavesdroppers

- Prove message came from real sender
- Prove remote party is who they say
- Prove message hasn’t been altered

Designing a secure cryptographic scheme is full of pitfalls

- Use approved design in the approved way

INTERNET REALITY

Most of the protocols were developed before the Internet grew popular

  - It was a smaller, more trusted world

- So protocols lacked security …

We have strong security needs today

  - Clients talk with unverified servers
  - Servers talk with anonymous clients

Security has been retrofitted

  - This is far from ideal!

TOPICS

- Threat models
- Confidentiality
- Authentication
- Wireless security (802.11)
- Web security (HTTPS/SSL)
- DNS security
- Virtual Private Networks (VPNs)
- Firewalls
- Distributed denial-of-service

Crypto

Applied crypto

Connectivity