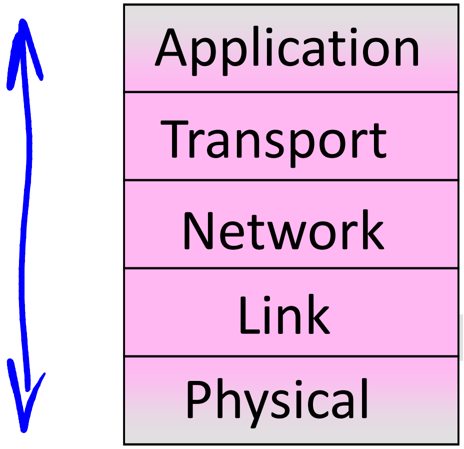
Introduction to Computer Networks

Network Security Introduction

David Wetherall (djw@uw.edu)
Professor of Computer Science & Engineering
UNIVERSITY of WASHINGTON

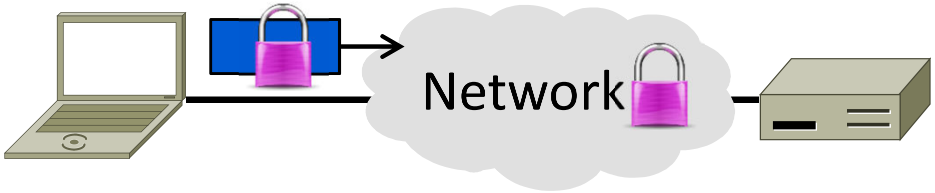
Where we are in the Course

- Revisiting the layers
  - Network security affects all layers because each layer may pose a risk



Topic

- Network security designs to protect against a variety of threats
  - Often build on cryptography
  - Just a brief overview. Take a course!



Security Threats

- "Security" is like "performance"
  - 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 attacker's abilities
  - Can't assess risk otherwise

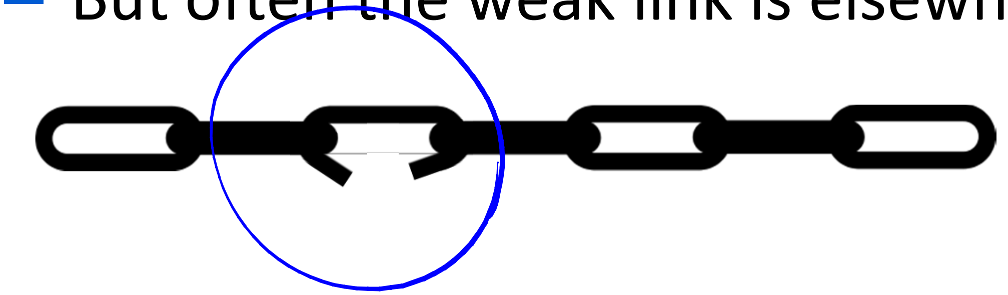
Security Threats (2)

- Some example threats
  - It’s not all about encrypting messages

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

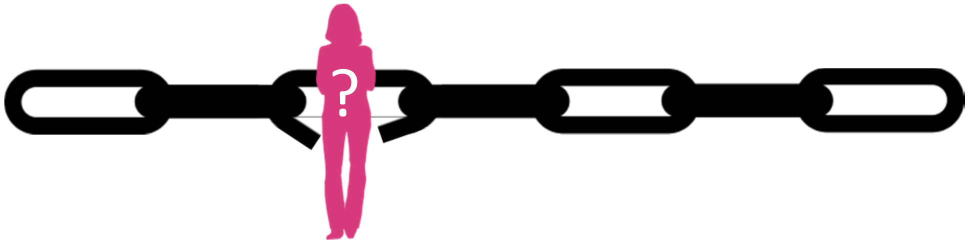
Risk Management

- Security is hard as a negative goal
  - Try to ensure security properties that don't let anything bad happen!
- Only as secure as the weakest link
  - Could be design flaw or bug in code
  - But often the weak link is elsewhere …



Risk Management

- Security is hard as a negative goal
  - Try to ensure security properties and don’t let anything bad happen!
- Only as secure as the weakest link
  - Could be design flaw or bug in code
  - But often the weak link is elsewhere …



Risk Management (2)

- 802.11 security … early on, WEP:
  - Cryptography was flawed; can run cracking software to read WiFi traffic
- Today, WPA2/802.11i security:
  - Computationally infeasible to break!
- So that means 802.11 is secure against eavesdropping?

Risk Management (3)

- Many possible threats
  - We just made the first one harder!
  - 802.11 is more secure against eavesdropping in that the risk of successful attack is lower. But it is not “secure”.

Threat Model	Old WiFi (WEP)	New WiFi (WPA2)
Break encryption from outside	Very easy	Very difficult
Guess WiFi password	Often possible	Often possible
Get password from computer	May be possible	May be possible
Physically break into home	Difficult	Difficult

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 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

This time

Crypto

Applied crypto

Connectivity

END