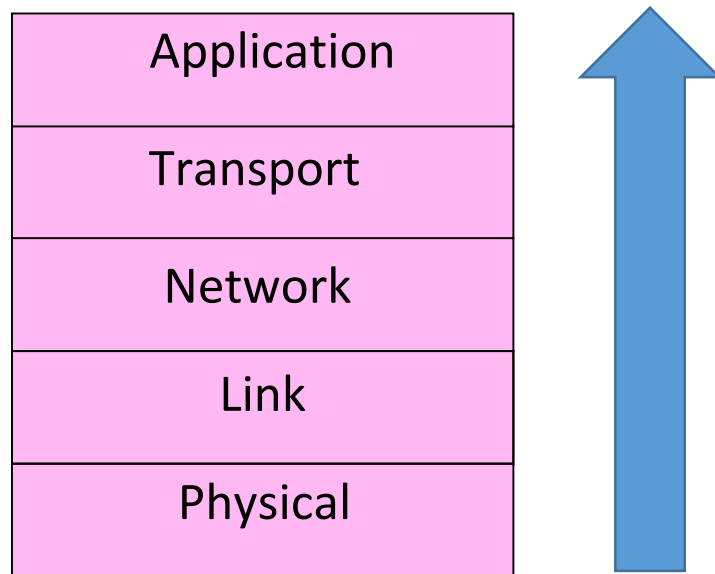


Network Security

Where we are in the Course

- Security crosses all layers



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

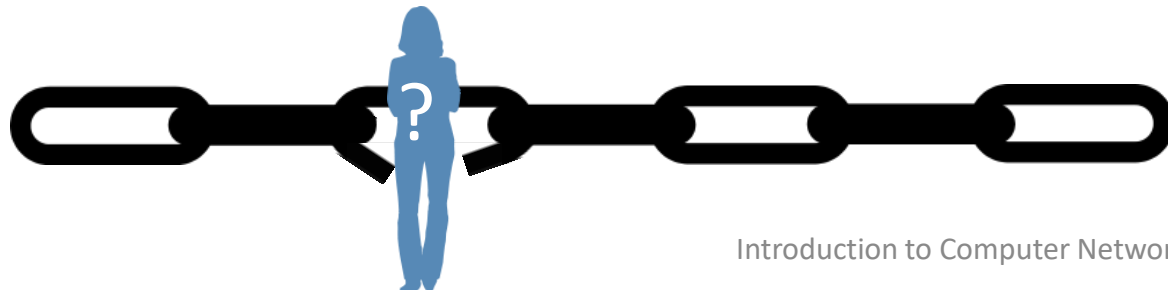
Security Threats (2)

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

Attacker	Ability	Threat
Eavesdropper	Intercept messages	Read contents of message
Observer	Inspect packet destinations	Collect conversations
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 and don't let anything bad happen!
- End-to-end principle in action (can't trust network!)
- 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

Cryptography

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

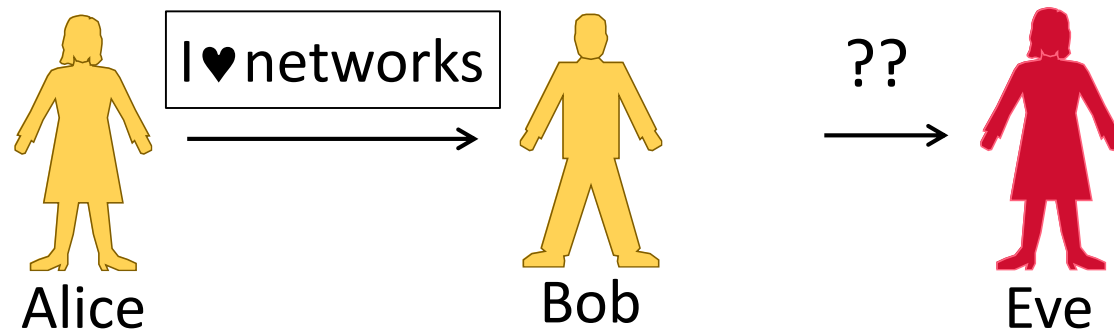
- Encrypting information is useful for more than deterring eavesdroppers
 - Prove message came from real sender
 - Prove remote party is who they say
 - Prove message hasn't been altered
- Designing secure cryptographic scheme tricky!
 - Use approved design (library) in approved way

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!

Goal and Threat Model

- Goal is to send a private message from Alice to Bob
 - This is called confidentiality
- Threat is Eve will read the message
 - Eve is a passive adversary (observes)



Encryption/Decryption Model

- Alice encrypts private message (plaintext) using key
- Eve sees ciphertext but not plaintext
- Bob decrypts using key to get the private message

