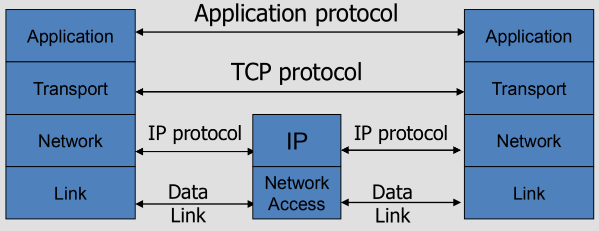
CSE 433S: Introduction to Computer Security

Midterm Review

Washington University in St. Louis

Slides contain content from Professor Dan Boneh at Stanford University

TCP Protocol Stack



Security Issues in IP

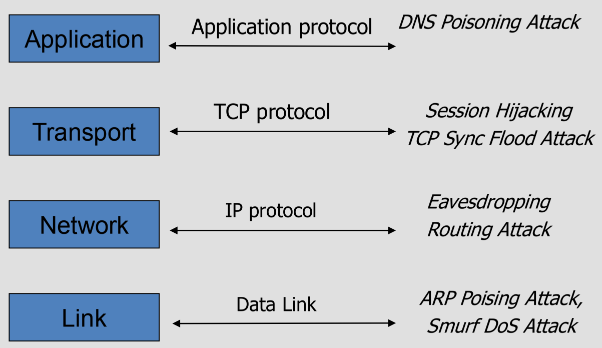
- Source spoofing
- Replay packets
- No data integrity or confidentiality

- DOS attacks
- Replay attacks
- MiTM attack
- Interleaving attacks
- Eavesdropping
- and more…

Fundamental Issue:

Networks are not fully secure

Network Attacks



Application — Application protocol — *DNS Poisoning Attack*

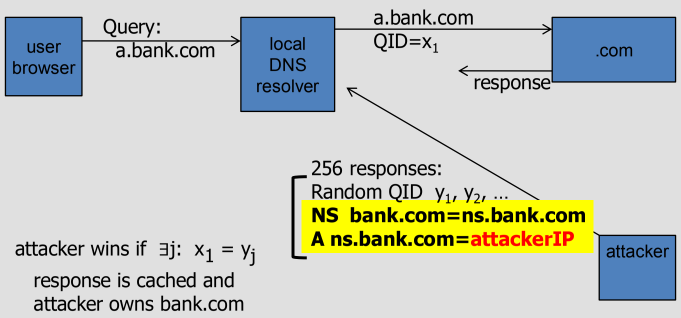
Transport — TCP protocol — *Session Hijacking*, *TCP Sync Flood Attack*

Network — IP protocol — *Eavesdropping*, *Routing Attack*

Link — Data Link — *ARP Poising Attack,* *Smurf DoS Attack*

DNS cache poisoning (a la Kaminsky' 08)

- Victim machine visits attacker's web site, downloads Javascript



Summary of Threats

- Confidentiality
  - Packet sniffing
- Integrity
  - ARP poisoning
  - UDP spoofing
  - TCP Session hijacking
- Availability
  - Denial of service attacks
- Common
  - Address translation poisoning attacks (DNS, ARP)
  - Packet Spoofing

Summary

- Core protocols not designed for security
  - Eavesdropping, Packet injection, Route stealing, DNS poisoning
  - Patched over time to prevent basic attacks
- More secure variants exist :

  IP ⟶ IPsec

  DNS ⟶ DNSsec

  BGP ⟶ sBGP

Network Attacks

- Can you sniff packet in the network? Why or Why not?
- Can you spoof packet in the network? Why or Why not?
- What is smurf attack?
- What is TCP sync flood attack?
- Will Sync flood on ssh affect telnet ? (Yes)
- Is increasing the buffer the right approach to defend against TCP sync flood?
- What level of network stack is Ping operating on? (Network)

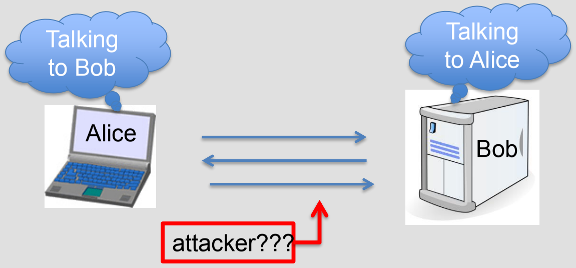
Importance of Cryptography

Quiz Questions

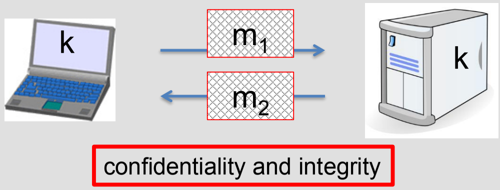
- What are the three principles of secure system
- Systems should always be password (or biometric) protected
- If we take all the right steps to construct the system, we can continue to rely on the security mechanisms for years to come, why or why not?
- What does C.I.A stand for, can you give one example of each, and the techniques to accomplish them
- What are the differences between ciphertext only attack and known plaintext attack threat model?

Crypto core

Secret key establishment:



Secure communication:



Symmetric vs Asymmetric

- Symmetric
  - Assuming we have some share secret, k
  - Focus on protecting information – confidentiality and integrity
- Asymmetric
  - Key exchange
  - Certificate – authenticity
  - PKI

Summary – Classic and Stream Cipher

Stream Cipher : you XOR a random byte sequence with unencrypted message (plaintext) to get the encrypted message (ciphertext)

- Caesar Cipher, Substitution Cipher
- Frequency attack XOR with uniform random variable
- Perfect Secrecy - One time pad
- What does it take to have perfect secrecy?
- Attack on Stream Cipher
  - Two time pad
  - Integrity attack

Quiz Questions

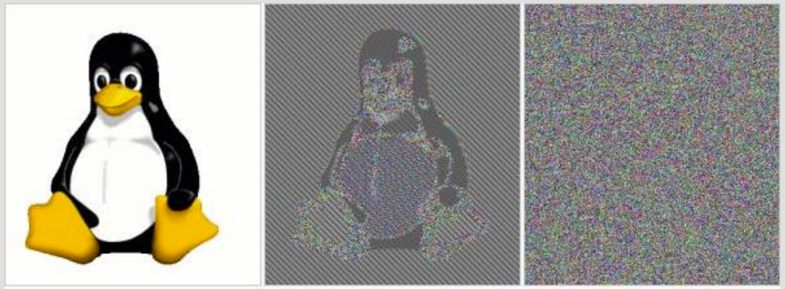
- Cryptography is all about the algorithm, therefore, as long as we use the right cryptographic tool, and random keys, the system is secure.
- What is the key space of substitution cipher for English alphabet, how would you crack this?
- What is the intuitive idea / formal definition of Shanon's idea of perfect secrecy?
- What is OTP, what's its limitation, and what mathematical property gives it perfect secrecy intuitive?
- What is the definition of semantic security? Why is it a weaker notion of perfect secrecy?
- Can stream cipher have perfect secrecy?
- Name two attacks against stream cipher? What can an adversary achieve with these two attacks?

Summary – Block Cipher

Encryption method that takes a block of unencrypted bytes (plaintext) and outputs a block of encrypted bytes (ciphertext)

- Design principles of block cipher
- AES and DES
- One time key vs Many time key (Penguin Picture)
- Ciphertext only attack vs Chosen-plaintext attack
- Randomized encryption vs counter-based encryption
- Modes of operations – ECB, CBC, CTR
  - Drawbacks on each mode
- Predictable IVs

ECB is not secure, but why?



Original image

Encrypted using ECB mode

Modes other than ECB result in pseudo-randomness

Review Questions

- How is block cipher different from stream cipher, how is it similar to stream cipher?
- What are PRP and PRF, what constructions will allow one to construction a PRP from PRF?
- What are the four key design principles of block cipher?
- What the root cause behind the vulnerability in ECB mode of AES?
- What are the two approaches we studied in class to address the problem of one-time-key?
- What are the requirements for IVs in block cipher modes of operation?
- T/F questions
  - DES is still secure
  - The key length of block cipher need to be the same as the length of the block
  - When the file is not a multiple of blocksize, we pad it with random bytes to secure it, since the goal is to have the output as random as possible
  - The entries in the S-box has to be non-linear, therefore we just randomly generate it

Summary – Message Integrity

Protects the integrity of the message

- Message Authentication Code (MAC) – Defend against existential forgery attack
  - ECBC-MAC
- MAC requires a key to create tag, but why?
- MAC should not be too short, why?
- Hash Function
  - Collision Resistant
  - Collision attack on MD5, SHA1

Review Questions

- What is MAC, name one property of MAC
- What is Hash function, name the most important function of hash
- Why should there be two keys in MAC design
- What was the construction that allows hash function to handle very long messages
- If I have a message that I want to send to the bank, but I don’t care who can read it, what can I do?

Summary – Authenticated Encryption

Authenticated encryption:

CPA security + ciphertext integrity

- Confidentiality in presence of **active** adversary
- Prevents chosen-ciphertext attacks

Limitation: cannot help bad implementations …

Authenticated encryption modes:

- Standards: GCM
- General construction: encrypt-then-MAC

Review

- What is authenticated encryption?
- In real systems, it is always possible to have confidentiality without integrity?
- What are the different ways to combine MAC and Symmetric Cipher? Which one is always correct?
- Given a network protocol, what is a common mistake that was shown in last class, how would you defend against them?

Summary – Key Exchanges

- Need for key exchange
- Key exchange using trusted third party (TTP)
- Key exchange without TTP
  - Diffie-Hellman protocol
    - MiTM attack
- Public key encryption made possible by one-way functions with special properties.
  - DLOG, RSA
  - Textbook RSA is not secure, do not directly encrypt raw message using RSA

Digital Signature

Digital version of physical world signature, signed using private key and verified using public key

- PKI - public key infrastructure

Review Questions

- How many symmetric keys does it take to support secure communications among 4 peers? What are the possible approaches to mitigate this issue?
- What is Diffie-Hellman key exchange, what attack is it vulnerable to, how do you launch that attack?
- What is public key crypto and how is different than symmetric key crypto? What key do Alice use if Alice wants to deliver a secret to Bob.
- In practice, can we use RSA to directly encrypt secret key for communication?
- What is digital signature? What key does Alice use to sign a file that she wants to authenticate and why?

Quick Review: primitives

To protect non-secret data: (data integrity)

- using small read-only storage: use collision resistant hash
- no read-only space: use MAC … requires secret key

To protect sensitive data: only use authenticated encryption

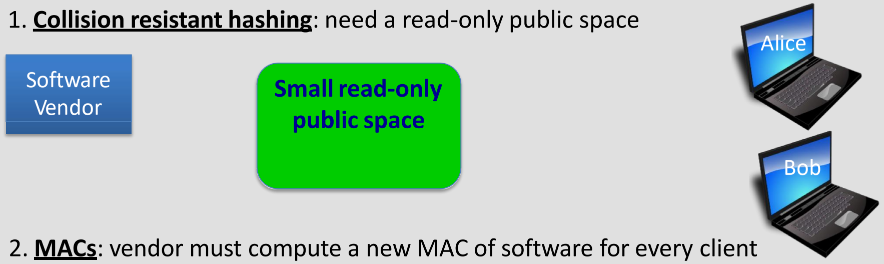
(eavesdropping security by itself is insufficient)

Session setup:

- use public-key encryption

Review: three approaches to data integrity

1. **Collision resistant hashing**: need a read-only public space

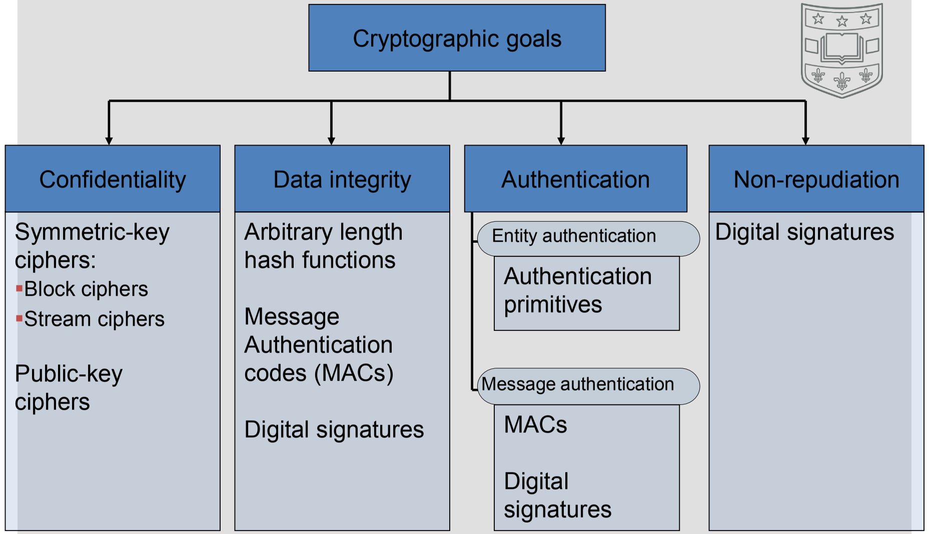


2. **MACs**: vendor must compute a new MAC of software for every client

- and must manage a long-term secret key (to generate a per-client MAC key)

3. **Digital signatures**: vendor must manage a long-term secret key

- Vendor's signature on software is shipped with software
- Software can be downloaded from an untrusted distribution site



Cryptographic goals

Confidentiality
Symmetric-key ciphers:
- Block ciphers
- Stream ciphers

Public-key ciphers

Data integrity
Arbitrary length hash functions

Message Authentication codes (MACs)

Digital signatures

Authentication
Entity authentication
Authentication primitives
Message authentication
MACs

Digital signatures

Non-repudiation
Digital signatures

Final Words

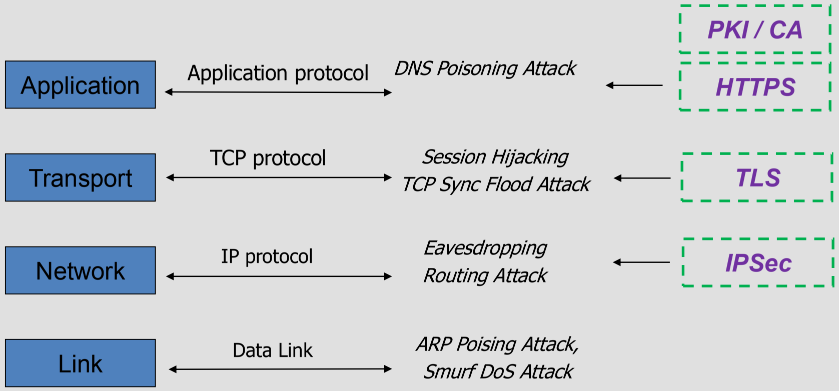
Be careful when using crypto:

- A tremendous tool, but if incorrectly implemented: system will work, but may be easily attacked

Make sure to have others review your designs and code

Don't invent your own ciphers or modes, implementation of Crypto is also very important

This module - Network defense

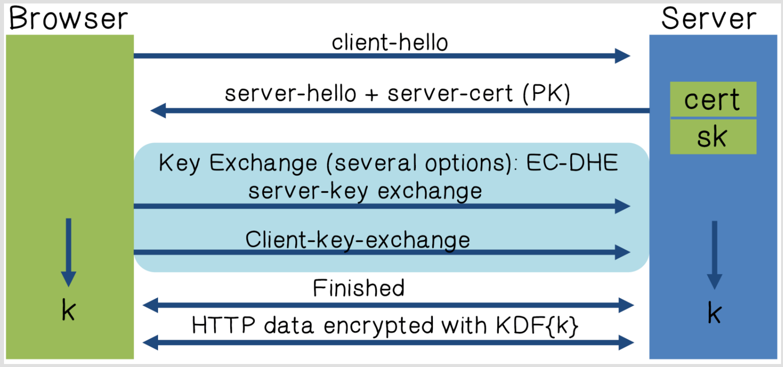


Assumption of PKI

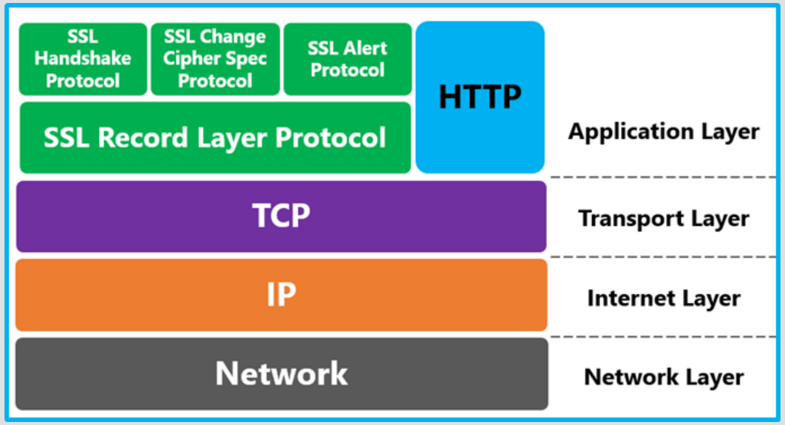
- As long as the CA is trustworthy…
  - Honest, and properly verifies Alice's identity
- *…and the CA's private key has not been compromised*

- *What else can you think of?*

TLS Summary


Browser
Server
cert
sk
client-hello
server-hello + server-cert (PK)
Key Exchange (several options): EC-DHE
server-key exchange
Client-key-exchange
Finished
HTTP data encrypted with KDF{k}
k
k

Where is HTTPS



Problems with HTTPS

☞ Upgrade from HTTP to HTTPS

Forged certs

Mixed content: HTTP and HTTPS on the same page

Review Questions

- What is a common design paradigm to defend against replay attack?
- What is TLS, how are we using TLS when we browse websites, and why is TLS capable to defending against man-in-the-middle attack and replay attack?
- What is HTTPS?
- Can you name three attacks on HTTPS?
- What is IPSec designed to do ?
- What are the two modes of operation in IPSec ?