CS 458/658 - Computer Security and Privacy **Fall 2018**

Lecture 13 - 18: October 23 - November 8, 2018

Lecturer: Ian Goldberg *Notes By: Harsh Mistry*

13.1 Cryptography

- Cryptography is the science that studies producing secret messages and breaking secret messages. The intention being, to develop methods to communicate securely via a insecure medium
- Cryptography contains three major types of components
  - Confidentiality. Preventing authorized reading
  - Integrity. Preventing modification
  - Authenticity. Preventing impersonation
- Kerckhoffs' Principle
  - The security of a cry[tosystem should not rely on a secret that's hard (or expensive) to change.
  - Implication → The system is at most secure as the number of keys
  - A strong cryptosystem is where the best an attack can do, is try every combination

13.1.1 Strong Cryptosystems

- A attacker may
  - know the algorithm
  - know part of the plain text
  - know corresponding plaintext/cipher pairs
  - have access to an encryption and/or decryption oracle
- Strong systems intend to defend against that may know all of these

13.1.2 Secret Key Encryption

- Simplest form of cryptography
- Also called symmetric encryption
- Keys are the same on both sides
- Its possible to have a unbreakable system if you use the One-Time pad which involves a system where the key is truly random bit string of the same length. Encrypt and Decrypt are just XOR functions

13.1.2.1 Computational Security

- In contrast to "Perfect Security", most cryptosystems have computational security. Which means they can be broken with enough work
- 128-bit is the modern standard

13.1.2.2 Types of secret-key crypto

- Stream ciphers
  - A stream cipher is what you get if you take the one-time pad, but use a pseudorandom keystream instead of a truly random one
  - RC4 is the most commonly used stream cipher
  - Are really fast and good for sending large amounts of data
  - Are tricky to use because what happens if use the same key twice
  - WEP, and PPTP are great examples of ppor Stream implementation
- Block ciphers
  - Block ciphers operate on blocks of a message rather than each bit
  - Blocks are usually 64 to 128 bits
  - AES is an example of a block cipher
  - Modes of operation
    - ECB (Electronic Code Book), encrypt each successive block separately
    - CBC (Cipher Block Chaining) - Needs IV
    - CTR (Counter) - Needs IV
    - GCM (Galois Counter) - Needs IV

13.1.3 Key Exchange

13.1.3.1 Public Key Cryptography

- Called asymmetric cryptography
- Common example are RSA, ElGamal, ECC, and NTRU
- Public key sizes are important, as many public-key methods have short cuts

13.1.3.2 Hybrid Cryptography

- Public key encryption is slow, so we can take a hybrid approach
  1. Pick a random 128-bit key for a secret-key
  2. Encrypt a large message with the key K
  3. Encrypt K with the public-key
  4. Send the encrypted message with encrypted K to receiver
- This is used for almost every cryptography application on the internet today

13.1.4 Integrity

- Checksum is not a valid way of determining validity, as a new message with the same checksum can be computed
- A cryptographic check-sum is needed

13.1.4.1 Cryptographic Hash Functions

- A hash function h takes an arbitrary length string x and computes a fixed length string y = h(x) called a message digest
- Hash functions should have 3 properties
  - Preimage-resistance, its hard to find the input from the output
  - Second preimage-resistance, given a input its hard to find a second input that yields the same result
  - Collision-resistance, Its hard to find two values that yield the same result
- Crytographic hash functions aren't a guarantee, as a MIM can just recompute a new message digest,
- Hash functions provide integrity guarantees only when there is secure way of sending and/or storing the message digest.

13.1.5 Authentication

13.1.5.1 Message Authentication Codes

- We can do the same thing as encryption for hash functions. Used a shared secret key to pick the correct hash function
- Only those with the secret key can generate or even check the computed hash (tag)
- These keyed hash functions are usually caled Message Authentication Codes or MACs

13.1.5.2 Repudiation

- Repudiation is where the sender can claim the receiver falsely produced the message.
- Its basically a situation, where there is no guarantee a user sent a message

13.1.5.3 Digital Signatures

- For non-repudiation, we can use a digital signature to ensure the sender actually sent the message
- To make a digital signature, the sender signs the message with their private key, then the receiver verifies the message with their copy of the public key

13.1.5.4 Hybrid Signatures

- Just like encryption in public key crypto, signing messages is slow
- We can hybridize things to make them faster
- Message is sent unsigned, but the hash is signed
- Authenticity and confidentiality are separate

13.1.6 Certificate Authorities

- One of the hardest problems of public key crypto is key management
- CA's solve this problem
- CA's are trusted third parties, who keep a directory of people's verification keys
- CA generates a certificate consisting of alice's personal information, as well as her verification key. The entire certificate is signed with the CA's signature key
- Everyone is assumed to have a copy of the CA's verification key
- There can be multiple levels of certificate authorities

13.2 Internet Security and Privacy

- The primary use for cryptography is "Separating the security of the medium from the security of the message"
- Entities you can only communicate with over a network are inherently less trustworthy.
- Network cryptography is used at every layer of the network stack for both security and privacy applications

13.2.1 Link Layer Security Controls

- Intended to protect local area networks
- WEP (Wired Equivalent Privacy) is a widespread example of a solution where none of the CIA properties were properly enforced

13.2.1.1 WEP

- The sender and receiver share a secret k where K is either 40 or 104 bits long
- In order to transmit a message M
  1. Compute checksum of M : c(M)
  2. Pick an IV (random number) v and generate a keystream RC4(v,k)
  3. XOR `<M, c(M)>` with the keystream to get the cipher text

4. Transmist v and the ciphertext over the wireless link

- Upon receipt of v and the ciphertext:
  1. Use the received c and shared k to generate keystream RC4(v,k)
  2. XOR the cipher text with RC4(v, k) to get `<M',c'>`
  3. check to see if check sum matches
  4. if it matches, accept the decrypted message
- Authentication Protocol
  1. Access point sends a challenge string
  2. Client sends back the challenge, WEP encrypted with the shared secret k
  3. The wireless access point checks if the challenge is correctly encrypted and if so accept the client

13.2.1.2 WEP Problems

- v is only 24 bits long, which can lead to reused random numbers
- Checksum used in WEP is CRC-32, which can easily exploited since it is linear and independent of k and v. This allows an attacker to inject a new message into the network simply by replacing the message and recalculating the check-sum
- Authentication protocol gives away plain-text/cipher pair for free
- The authentication protocol leaves room for an attacker to execute the protocol himself by observing the authentication process
- When RC4 is used on similar keys, the output stream has a subtle weakness. Observing the output stream can lead to a 104-bit ot 40-bit key in under 60 seconds

13.2.1.3 WPA

- Wifi Protected Access is a short term patch to WEP
- Replaces CRC-32 with a real MAC (Called a MIC to avoid confusion with Media access control)
- IV is 48 bits long
- Key is changed frequently
- Has ability to use 802.1x auth server
- Can run on most older WEP hardware

13.2.1.4 WPA2

- Replaces RC4 and MIC algorithms in WPA with the CCM auth encryption mode (AES)
- Considered strong, but dictionary attacks are still possible

13.2.2 Network Layer Security

- Security within our network is not enough, we need security across networks.

13.2.2.1 VPN

- VPNs connect two or more networks that are physically separated, and make them appear to be a single network
- The goal is to prevent an attacker from being able to read of modify traffic flowing between two locations

13.2.2.2 Tunnelling

- Tunnelling is the sending of message of one protocol inside message of another protocol, out of their usual protocol nesting sequence
- TCP-over-IP is not tunnelling, but IP-over-TCP is tunnelling

13.2.2.3 IPSec

- IPSec is one standard way of setting up a VPN
- There is two modes
  - Transport mode which is useful for connecting a single machine to a home network. Only the contents of the ip are encrypted
  - Tunnel mode which is useful for connecting two networks. The contents and the header of the original packet are encrypted and authenticated
- Some other VPN styles are Microsoft PPTP and VPNs over SSH

13.2.3 Transport Layer Security and Privacy

- Network layer security mechanisms arrange to send individual IP packets securely from one network to another
- They transform arbitrary TCP connections to add security
- TLS is the main security mechanism and Tor is the main privacy mechanism

13.2.3.1 TLS/SSL

- High Level
  1. Client connections to server indicated it wants to use TLS
  2. Server sends its certificate to client which contains admin info
  3. Server chooses which ciphersuite to use
  4. Client validates server's certificate

5. Client and Server run a key agreement protocol to establish keys for symmetric encryption an MAC algorithms from the chosen ciphersuite
6. Communication then proceeds using the chosen symmetric encryption

- Security properties provided by TLS
  - Server authentication
  - Message integrity
  - Message confidentiality
  - Client authentication
- Most successful Privacy Enhancing Technology (PET)

13.2.3.2 Tor

- Tor is another successful privacy enhancing technology that works at the transport layer
- Tor allows you to make TCP connections without revealing your IP
- Tor tunnels your connection across through multiple nodes. Each link is encrypted except the last link
- No node knows both the user and website
- The connection between each node results in a new encrypted link with a new encryption secret
- Tor provides **anonymity** for both unlinkably (Long-term) and linkably (short term)

13.2.3.3 The Nymity Slider

- We can place transactions (both online and offline) on continuum according to the level of nymity they represent
  - Verinymity (e.g Government ID)
  - Persistent Pseudonymity (e.g Many Blogs)
  - Linkable anonymity (e.g loyalty cards)
  - Unlinkable anonymity (e.g Cash Payments)
- If you build a system at a certain level of nymity, its easy to modify it to have a higher level of nymity, but hard to modify it to have a lower level.
- So, design systems with a low level of nymity

13.2.4 Application Layer Security And Privacy

- Many applications want true end to end encryption, so we add an additional layer of security on the application it self

13.2.4.1 SSH

- Secure Remote Login
- Usual Usage
  - Client connects to server
  - Server sends its verification key
  - Client and Server run key agreement protocol
  - Client authenticates to server
  - Server accepts authentication and login proceeds
- There is two methods of authentication, sending a password over a encrypted channel or sending a random challenge with a private signature.

13.2.4.2 Remailer

- Provide Anonymity for email by providing you the ability to send an email without revealing your own email
- Type 0 Remailers work by having a third party server simply forwarding a sent email under a random address. The new address is stored in a table, so the central server can relay responses back to you
- Type 1 Remailers remove the central server by relaying the message through multiple remailers and each step is encrypted to avoid observation. Additionally, remailers delay and reorder messages. This type does not support responses
- Type 2 Remailers enforced constant length messages to avoid observers from watching a big file travel through the network, but requires a special mail client to construct message fragments
- Type 3 remailers have native support for pseudonymity, but aren't well deployed or mature

13.2.4.3 Pretty Good Privacy

- First popular implementation of public key cryptography
- Primarily used to protect emails
- Main functions
  - Four kinds of keys (Encryption, decryption, signature, and verification)
  - Encrypt messages using someone else's encryption
  - Decrypt messages using your own decryption key
  - Verify signatures using someone elses verification key
  - Sign other people's key using your own signature key

13.2.4.4 OTR

- Off-the-Record Messaging (OTR) is software that allows you to have private conversations over instant messaging providing Confidentiality and Authentication.
- Perfect Forward Secrecy : After forwarding the message is unreadable to anyone else
- Deniablity : You can't convince others a message was truly sent by someone else even though you know who the sender was
- Signal Protocol is a perfect example of this and is used by many popular messaging services
  - Uses "ratchet" technique to constantly rotate session keys to ensure Perfect Forward Secrecy
  - Deniability is provided by Triple Diffie-Hellman deniable authenticated key exchange (DAKE)