1.264 Lecture 26

Security protocols

Next class: Anderson chapter 4. Exercise due before class

Encryption

- Encryption is the process of:
  - Transforming information (referred to as plaintext)
  - Using an algorithm (often called a cipher)
  - To make it unreadable to anyone
  - Except those possessing special knowledge, usually referred to as a key.
- The result of the process is encrypted information, or ciphertext.
- The reverse process, i.e. to make the encrypted information readable again, is referred to as decryption, (i.e. to make it unencrypted).

Protocols

- Security processes are called protocols. They address:
  - Identity and authentication of identity
  - Roles and authorization of roles
  - Accounting for resources used by principals
    - Including non-repudiation
  - Valid and invalid actions taken by principals, including attackers, e.g.,
    - Man in the middle attacks
    - Replay attacks, and other issues with freshness/staleness
    - Tampering with network connections
    - Impersonation, extortion, physical theft, …
- If your organization has significant assets, you must protect against sophisticated/tailored attacks

Protocol notation example

- **Notation**
  - $T \text{ -> } G : T, \{T, N\}_{KT}$
  - Token T used to enter garage G (T and G are principals)
    - Token (e.g. like EZ Pass) transmits its serial number T
    - Then transmits its serial number T and a number used only once (nonce) N, encrypted with its key K_T
    - Nonce assures that message is fresh, not a replay
      - Nonce can be sequential, random, or third party challenge
      - Assume nonce is sequential in this protocol
    - K_T known by both T and G
  - Parking garage server:
    - Reads T
    - Looks up the corresponding key K_T from its database
    - Deciphers $\{T, N\}_{KT}$
    - Checks that the message includes T, and
    - Checks that N has not been seen before or has expected value

Exercise: flaws in garage protocol?

- Describe whether it is possible to have:
  - Man in the middle attack?
  - Denial of service attack?
  - Replay attack?
  - Crack (obtain) the key?
  - Other attacks that you can imagine?
- Think like a criminal…

Solution: flaws in garage protocol?

- Describe whether it is possible to have:
  - Man in the middle attack?
    - Yes. Have a rogue reader before garage entrance that reads all EZ Pass units seen. Copy the tag's message to the reader onto another unit. Use that one to enter garage.
  - Denial of service attack?
    - Yes. Break the reader, cut its power, etc. Gate will be left up
  - Replay attack?
    - No. Since each message has nonce.
  - Crack the key?
    - Yes. Attacker Z can go into garage with rogue reader and interrogate an EZ Pass unit repeatedly. Z knows part of the message is the sequential number and part is the fixed key. Z can infer K_T from enough (N, N_{KT}) pairs
  - Other attacks that you can imagine? (Easiest one!)
    - Yes. Attacker can break into car and steal EZ Pass unit

Exercise: challenge and response

- Vehicle anti-theft system as example
  - Vehicle key inserted into steering lock
  - Car key has serial number, which is its identifier
  - Engine management unit sends random number challenge to car key using short range radio
  - Car key computes response by encrypting the random number challenge and also sends car key identifier
  - Engine management unit decrypts, reads response and verifies it matches the challenge, and car key serial nbr correct
- Exercise: write out the protocol using the notation conventions from the last slide:
- E (engine)->_______________________________
- C (car key) ->______________________________

Solution

- E (engine)-> C (car key): N
- C -> E : $\{C, N\}_{KC}$
- Note the car key must send its identifier
  - E must verify that C is valid.
  - N can often be predicted somewhat because the engine controller is simple (e.g., black hat intercepts N and knows next N is based on it)
  - Forcing black hat to find C makes break-in significantly harder
  - Key and engine management unit must be matched at time of manufacture; engine management unit must know K_C
- Notes:
  - The protocol is between a key and the engine. Since the user has the key, the key and engine are only in proximity when the user is too.
  - The key must be in the ignition for the protocol to start. This also makes the protocol better: contact rather than contactless.
  - These factors make man in the middle attacks harder, but not impossible.

Challenge response

- This is very common approach but has been broken repeatedly
  - Random numbers often not very random and can be grabbed or guessed by thief
- It is also vulnerable to man-in-the-middle attacks
  - A <-> B <-> C
  - B can masquerade as C, passing A's requests to C and sending C's responses to A. After (fraudulent) authentication, B gains access
  - Parking garage example:
    - Black hat has reader, masquerades as garage reader, interrogates card, gets its serial number T, $(N,T)_{KT}$, plays it to real reader, gets response back, enters garage
- Denial of service attack: jam radio frequency so car owner can't lock car when leaving

Exercise: physical security

- Pharmaceutical anti-counterfeiting
  - Manufacturer places bar code or RFID tag on each drug item
  - Store scans bar code or RFID tag to verify authenticity with manufacturer server
  - Customer has 800 number to call to verify serial number
- List possible attacks
  - Again, think like a criminal

Solution: physical security

- Pharmaceutical anti-counterfeiting
  - Place bar code or RFID tag on drug item
  - Store scans to verify
  - Customer has 800 number to call to verify serial number
- Possible attacks
  - Copy bar code or RFID tag and place on counterfeit item, sell it before the real item
  - Set up fake Web site and 800 number that will verify anything. Alter instructions to stores or consumers
  - If store can be compromised, even more attacks are possible. Store can fail to check, falsify records, etc.
  - *Supply chain and transportation increasingly involved in anti-counterfeiting and other security requirements*
- These are versions of replay, man in the middle…