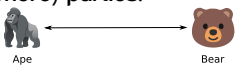
CSci 4271W
Development of Secure Software Systems
Day 18: Cryptography part 2: attacks

Stephen McCamant (he/him)
University of Minnesota, Computer Science & Engineering

Cryptography

The goal of cryptography is to provide a "secure channel" between two (or more) parties:



1. Revealing no information about the messages
2. Delivering only messages from Ape and Bear
3. Delivering messages in order or not at all.

Cryptography

The goal of cryptography is to provide a "secure channel" between two (or more) parties:

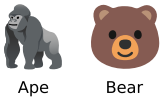
Even though Eve can inspect, modify, or drop any message and even if she knows there are only two possible conversations.

Keys

If Ape and Bear and Eve all know the same things, what keeps Eve from reading messages like Bear does?

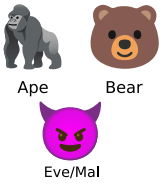
Bear knows a secret "key" that changes the decryption. Knowing it lets Ape and Bear keep secrets from Eve.

Potential attackers



Compromised code or a side channel may allow some information about keys or messages to leak

Potential attackers



Compromised code or a side channel may allow some information about keys or messages to leak

Intercepts, modifies, injects, replays, redirects traffic to "Eve"sdrop or "Mal"iciously interfere

Potential attackers

Compromised code or a side channel may allow some information about keys or messages to leak

Intercepts, modifies, injects, replays, redirects traffic to "Eve"sdrop or "Mal"iciously interfere

Turtles are trusted not to break security (but are they trustworthy?)

Attacks on encryption

- In a known ciphertext (or ciphertext-only) attack, the attacker recovers key or message from just ciphertext. (This is almost never a correct model of the attacker)

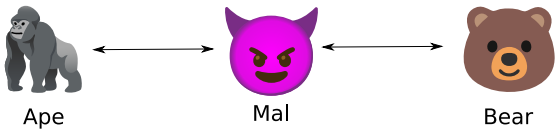
Attacks on encryption

- In a known ciphertext (or ciphertext-only) attack, the attacker recovers key or message from just ciphertext. (This is almost never a correct model of the attacker)
- Usually, attackers also know something about the plaintext. We can imagine Eve creating a small list, and Ape encrypts a chosen plaintext from this list.

Attacks on encryption

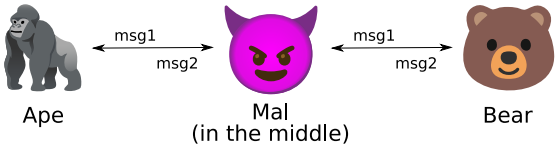
- In a known ciphertext (or ciphertext-only) attack, the attacker recovers key or message from just ciphertext. (This is almost never a correct model of the attacker)
- Usually, attackers also know something about the plaintext. We can imagine Eve creating a small list, and Ape encrypts a chosen plaintext from this list.
- A chosen ciphertext attack happens when Mal modifies a ciphertext to see what happens when Bear decrypts.

Attacks on crypto protocols



Mal may have a legitimate role in the protocol, or act as an on- or off-path attacker. Mal usually attacks how the crypto is used, rather than the cryptographic primitives.

Mal in the middle (MITM) attacks (1)

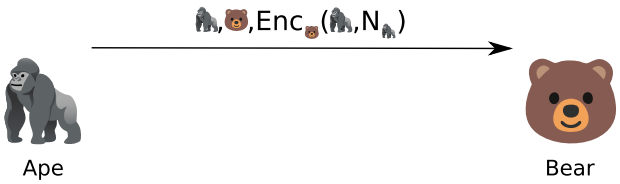


In a relay attack, Ape and Bear appear to communicate directly, but Mal is reading all of their messages.

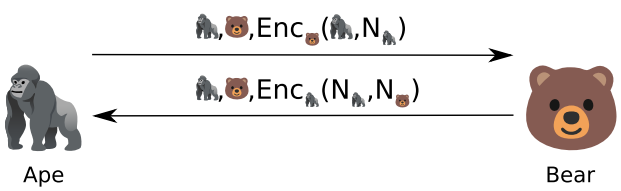
Example: Needham-Schroeder (background)

- Crypto protocols can have subtle vulnerabilities, even when boiled down to their core aspects.
- Suppose that Ape and Bear have a trustworthy source of public keys, but need to check whether they're really talking to each other.
- Based on choosing unique numbers N, called nonces (numbers used only once).

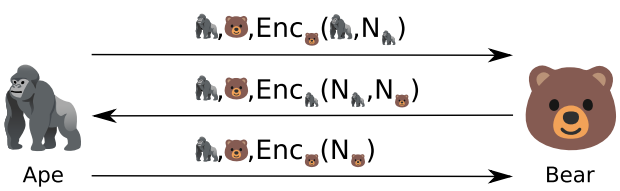
Example: Needham-Schroeder (honest)



Example: Needham-Schroeder (honest)

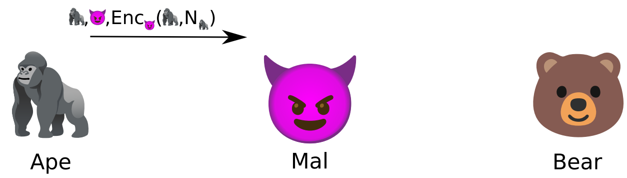


Example: Needham-Schroeder (honest)

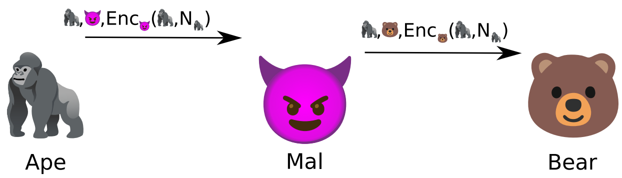


Example: Needham-Schroeder MITM

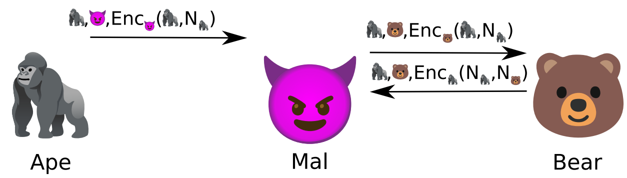
Example: Needham-Schroeder MITM



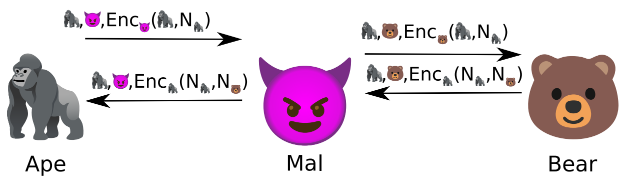
Example: Needham-Schroeder MITM



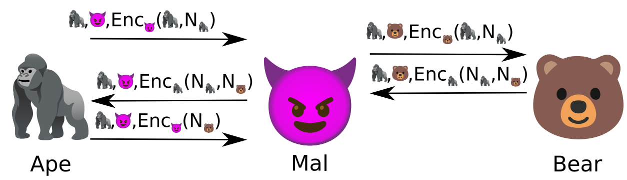
Example: Needham-Schroeder MITM



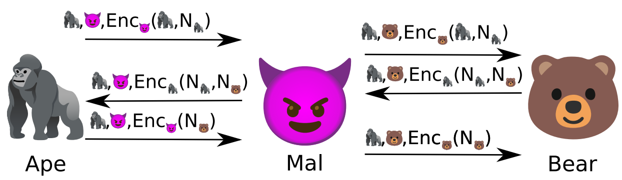
Example: Needham-Schroeder MITM



Example: Needham-Schroeder MITM



Example: Needham-Schroeder MITM



Outline

Attacks on cryptography and protocols

Announcements intermission

More cryptographic protocol attacks

Midterm 2 score distribution

```
5 | *
6 | ***
7 | *
8 | **
9 | ***
Mean: 76
Median: 77.5
```

Assignments, other logistics

- Homework 5 on cryptography due next Tuesday night
  - After today's lecture we've covered all the material
- Recommended crypto reading: Shostack chapter 16
- Ask project questions on Piazza or at office hours

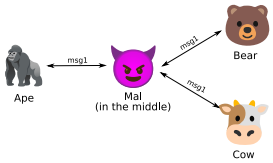
Outline

Attacks on cryptography and protocols

Announcements intermission

More cryptographic protocol attacks

Mal in the middle (MITM) attacks (2)



In a replay attack, Mal records a message from one execution of a protocol and replays it later.

Example: Denning-Sacco (honest)

Ape

Can sign, chooses $K_{🦍🐻}$

Bear

Can decrypt, wants $K_{🦍🐻}$

Example: Denning-Sacco (honest)

$🦍,🐻,Enc_{🐻}(date,K_{🦍🐻},Sig_{🦍}(date,K_{🦍🐻}))$

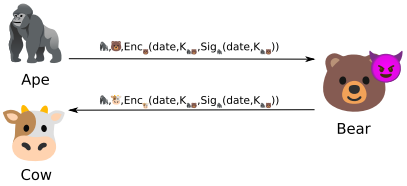
Ape

Can sign, chooses $K_{🦍🐻}$

Bear

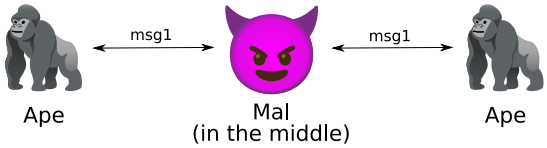
Can decrypt, wants $K_{🦍🐻}$

Example: Denning-Sacco replay



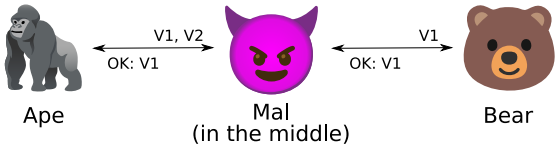
A malicious Bear could replay the signed key, re-encrypted to Cow, to impersonate Ape to Cow.

Mal in the middle (MITM) attacks (3)



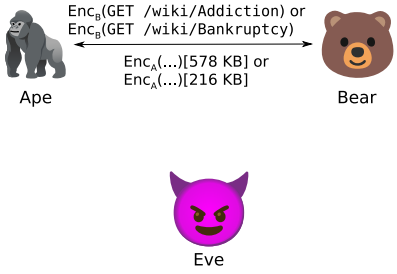
In a reflection attack, Mal plays Ape's message back to Ape later. Ape might decrypt or sign the message for Mal.

Mal in the middle (MITM) attacks (4)



In a downgrade attack, Mal convinces Ape and Bear to speak an old/insecure version of a protocol.

Traffic analysis (1)



Traffic analysis (2)