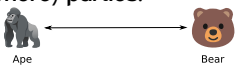
CSci 4271W
Development of Secure Software Systems
Day 19: Cryptography part 3: crypto in network protocols

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.

Key management

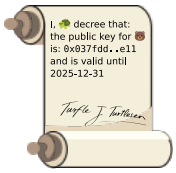
How does Ape get Bear's public encryption / verification key? (Without Mal injecting their own key?)

Key management

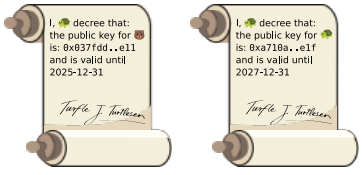
How does Ape get Bear's public encryption / verification key? (Without Mal injecting their own key?)

Key Pinning, Trust on First Use (TOFU), Web of Trust, DANE, ...

Certificates and PKI

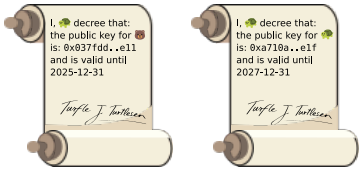


Certificates and PKI



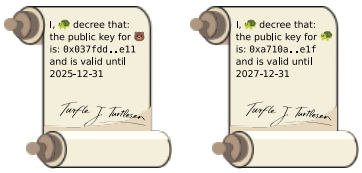
← Certificate Authority (CA)

Certificates and PKI



← Certificate Authority (CA)
~200 "root" CAs in modern OSes

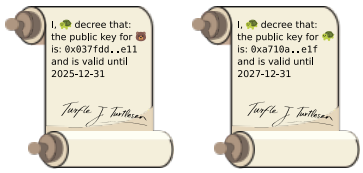
Certificates and PKI



← Certificate Authority (CA)
~200 "root" CAs in modern OSes

Who is the "right" CA for a website? (CA Pinning, CT)

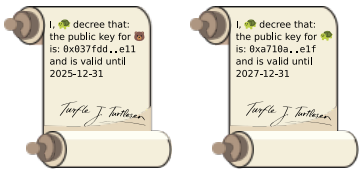
Certificates and PKI



← Certificate Authority (CA)
~200 "root" CAs in modern OSes

Who is the "right" CA for a website? (CA Pinning, CT)
How is a certificate verified? (DV, EV,...)

Certificates and PKI



← Certificate Authority (CA)
~200 "root" CAs in modern OSes

Who is the "right" CA for a website? (CA Pinning, CT)
How is a certificate verified? (DV, EV,...)
Is a certificate still valid? (CRLs, OCSP)

Cryptography in action

Previously, we saw several STRIDE threats to networks for which cryptography is the only solution"
Today: crypto protocols that can mitigate spoofing, tampering, repudiation (maybe?) and information disclosure.

Cryptography in action

Previously, we saw several STRIDE threats to networks for which cryptography is the only solution"
Today: crypto protocols that can mitigate spoofing, tampering, repudiation (maybe?) and information disclosure.

Protect flows
TLS
SSH
Signal
DoH

Cryptography in action

Previously, we saw several STRIDE threats to networks for which cryptography is the only solution"
Today: crypto protocols that can mitigate spoofing, tampering, repudiation (maybe?) and information disclosure.

Protect flows	Protect the network
TLS	IPsec
SSH	DNSSEC
Signal	BGPsec
DoH	

Outline

Key management and protocols

Announcements intermission

Specific protocols

Assignments, other logistics

- Homework 5 on cryptography is due tonight
- Entering the last week for Project 2

Outline

Key management and protocols

Announcements intermission

Specific protocols

TLS

...or Transport Layer Security Protocol, runs over TCP and provides confidentiality, integrity and authentication

HTTP/SMTP/FTP...
TLS (application/ transport)
TCP (transport)
IP (network)
Link

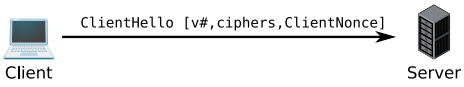
Formerly SSL (TLS 1.0 > SSL 3.1)

Long history of interesting protocol and implementation bugs...

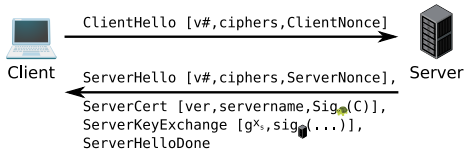
Versions 1.2 and 1.3 mostly OK!

TLS handshake

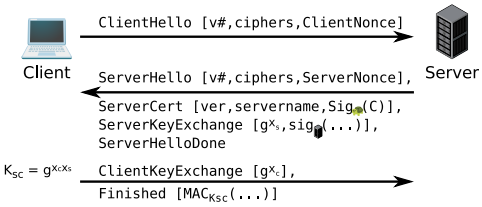
TLS handshake



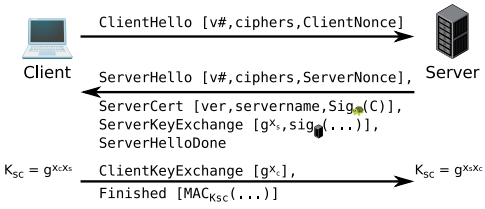
TLS handshake



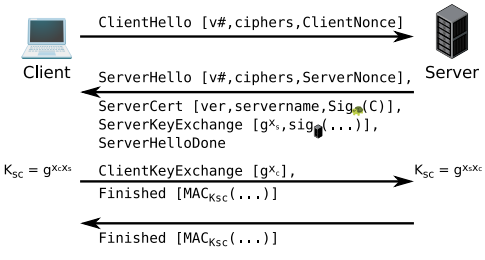
TLS handshake



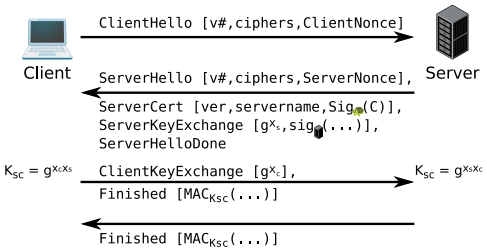
TLS handshake



TLS handshake

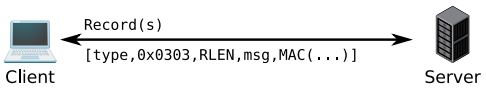


TLS handshake



TLS 1.3 always provides forward secrecy

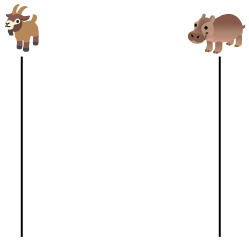
TLS records



TLS (1.2+) records are always authenticated and encrypted; handshakes include a hash of the entire conversation so far.
A decryption/MAC failure terminates the connection.
Several good (standard) libraries implement TLS

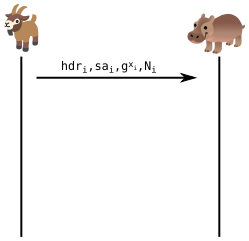
IPsec

IPsec is a network-level encryption and authentication protocol.
It creates a "virtual" network link between two hosts.



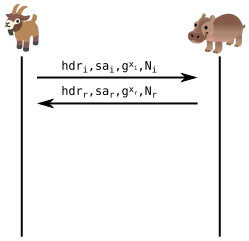
IPsec

IPsec is a network-level encryption and authentication protocol.
It creates a "virtual" network link between two hosts.



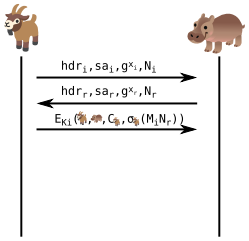
IPsec

IPsec is a network-level encryption and authentication protocol.
It creates a "virtual" network link between two hosts.



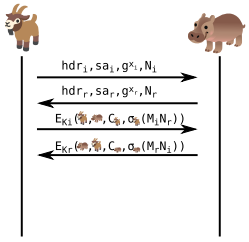
IPsec

IPsec is a network-level encryption and authentication protocol.
It creates a "virtual" network link between two hosts.



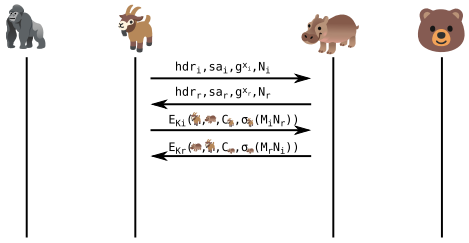
IPsec

IPsec is a network-level encryption and authentication protocol.
It creates a "virtual" network link between two hosts.



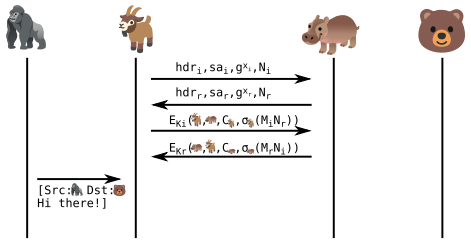
IPsec

IPsec is a network-level encryption and authentication protocol.
It creates a "virtual" network link between two hosts.



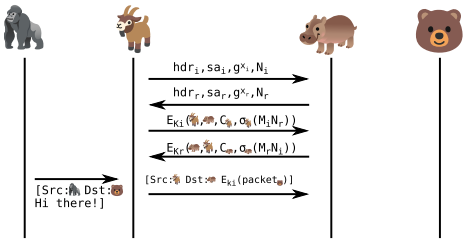
IPsec

IPsec is a network-level encryption and authentication protocol.
It creates a "virtual" network link between two hosts.



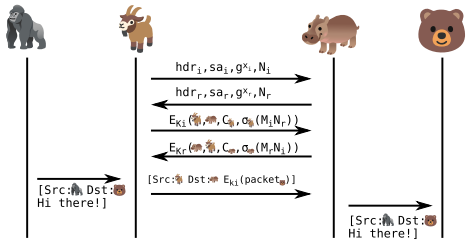
IPsec

IPsec is a network-level encryption and authentication protocol.
It creates a "virtual" network link between two hosts.



IPsec

IPsec is a network-level encryption and authentication protocol.
It creates a "virtual" network link between two hosts.



SSH

- Is another transport layer, with (authenticated) key exchange followed by encrypted records.

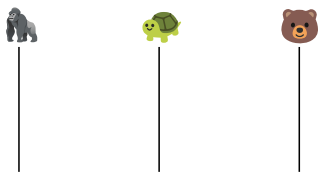
SSH

- Is another transport layer, with (authenticated) key exchange followed by encrypted records.
- It can be used transparently between hosts without network gateways (via "port forwarding")
- Not typically implemented in (standard) libraries
- Provides a wide array of authentication options, more than are commonly used

OpenSSH t-shirt

Signal

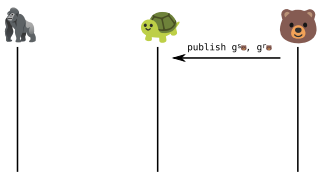
. . . is an asynchronous message-oriented encrypted channel protocol.
(Used by Signal, WhatsApp, FB Messenger, RCS)



It uses ratcheting to provide post-compromise security. Developers can integrate it into their apps with libsignal.

Signal

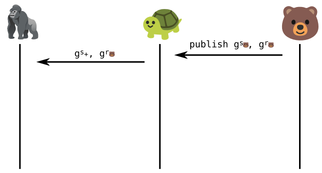
. . . is an asynchronous message-oriented encrypted channel protocol.
(Used by Signal, WhatsApp, FB Messenger, RCS)



It uses ratcheting to provide post-compromise security. Developers can integrate it into their apps with libsignal.

Signal

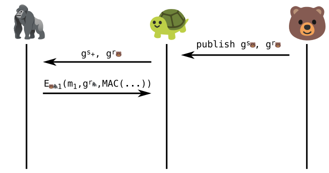
...is an asynchronous message-oriented encrypted channel protocol. (Used by Signal, WhatsApp, FB Messenger, RCS)



It uses ratcheting to provide post-compromise security. Developers can integrate it into their apps with libsignal.

Signal

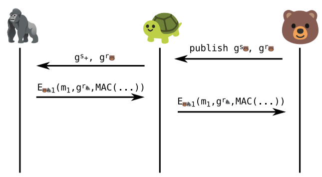
...is an asynchronous message-oriented encrypted channel protocol. (Used by Signal, WhatsApp, FB Messenger, RCS)



It uses ratcheting to provide post-compromise security. Developers can integrate it into their apps with libsignal.

Signal

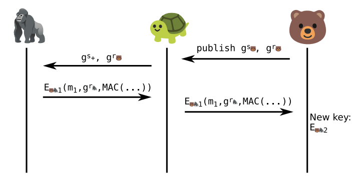
...is an asynchronous message-oriented encrypted channel protocol. (Used by Signal, WhatsApp, FB Messenger, RCS)



It uses ratcheting to provide post-compromise security. Developers can integrate it into their apps with libsignal.

Signal

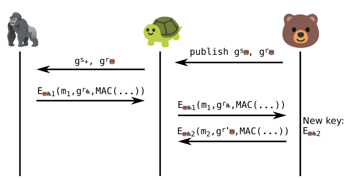
...is an asynchronous message-oriented encrypted channel protocol. (Used by Signal, WhatsApp, FB Messenger, RCS)



It uses ratcheting to provide post-compromise security. Developers can integrate it into their apps with libsignal.

Signal

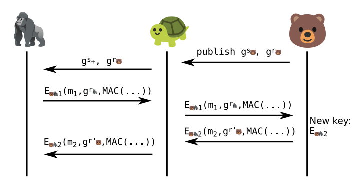
...is an asynchronous message-oriented encrypted channel protocol. (Used by Signal, WhatsApp, FB Messenger, RCS)



It uses ratcheting to provide post-compromise security. Developers can integrate it into their apps with libsignal.

Signal

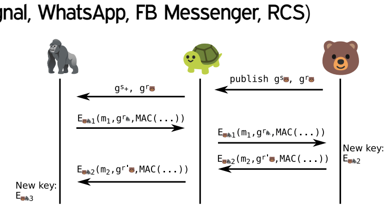
...is an asynchronous message-oriented encrypted channel protocol. (Used by Signal, WhatsApp, FB Messenger, RCS)



It uses ratcheting to provide post-compromise security. Developers can integrate it into their apps with libsignal.

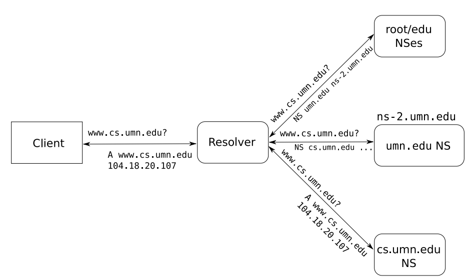
Signal

...is an asynchronous message-oriented encrypted channel protocol. (Used by Signal, WhatsApp, FB Messenger, RCS)

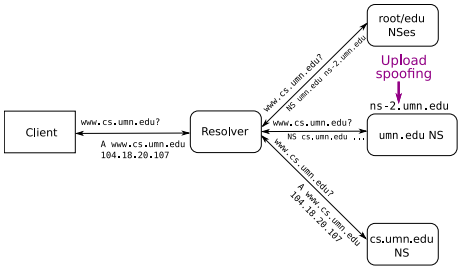


It uses ratcheting to provide post-compromise security. Developers can integrate it into their apps with libsignal.

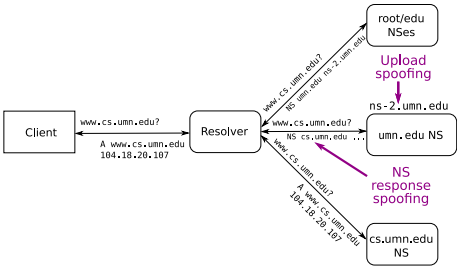
😈 Mal and DNS



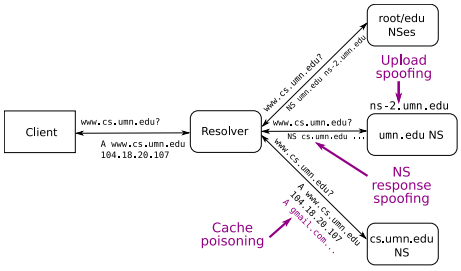
Mal and DNS



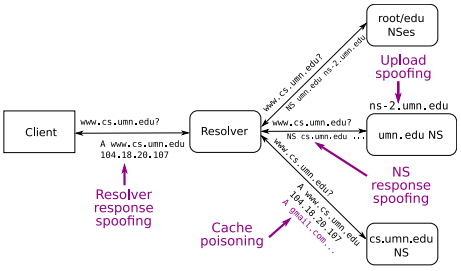
Mal and DNS



Mal and DNS

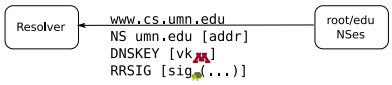


Mal and DNS



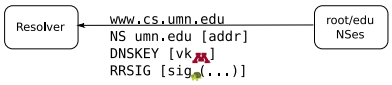
DNSSEC

The "root" DNSSEC key signs keys for subdomains:

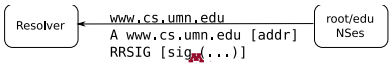


DNSSEC

The "root" DNSSEC key signs keys for subdomains:

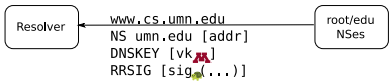


Subdomain keys can sign further sub-keys or other records:

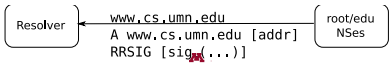


DNSSEC

The "root" DNSSEC key signs keys for subdomains:



Subdomain keys can sign further sub-keys or other records:

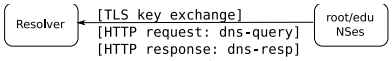


(Note this does not prevent subdomain owners from signing incorrect or misleading results…)

DoH

For domains without keys, DNSSEC can't prevent spoofing.

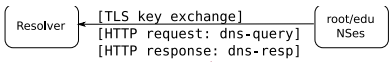
DoH is DNS-over-HTTPS (also: DoT (TLS), DoQ (QUIC))



DoH

For domains without keys, DNSSEC can't prevent spoofing.

DoH is DNS-over-HTTPS (also: DoT (TLS), DoQ (QUIC))



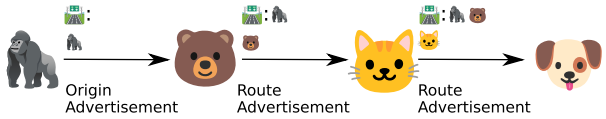
Does not prevent some "resolver-in-the-middle" attacks

Prevents information disclosure, response spoofing.

Available as 3rd party libraries

BGP

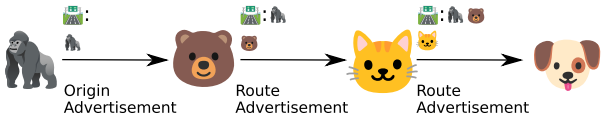
Recall that the Internet is a network of ASes (ISPs). ASes find routes to IP addresses via the BGP routing protocol.



Both origin and route advertisements can be forged in BGP.

RPKI and BGPsec

RPKI: IANA/ARIN sign origin attestations, preventing ASes from spoofing origin advertisements



BGPsec: IANA/ARIN sign AS certificates, ASes sign route advertisements. Prevents both route forgery and repudiation.