Network Security Encrypting Network Communication

Radboud University, The Netherlands



Spring 2018

Acknowledgement

Slides (in particular pictures) are based on lecture slides by Ruben Niederhagen (http://polycephaly.org)

- ▶ Hostname resolution in the Internet uses DNS
- ► Two kinds of servers: authoritative and caching
- ► Two kinds of requests: iterative and recursive

- Hostname resolution in the Internet uses DNS
- ► Two kinds of servers: authoritative and caching
- ► Two kinds of requests: iterative and recursive
- ► DNS tunneling:
 - ► Encode (SSH) traffic in DNS requests to authoritative server
 - Special authoritative server extracts and handles SSH data

- Hostname resolution in the Internet uses DNS
- ► Two kinds of servers: authoritative and caching
- Two kinds of requests: iterative and recursive
- DNS tunneling:
 - ► Encode (SSH) traffic in DNS requests to authoritative server
 - Special authoritative server extracts and handles SSH data
- ► DNS DDOS amplification:
 - Send DNS request with spoofed target IP address
 - Much larger reply launched onto target

- Hostname resolution in the Internet uses DNS
- ► Two kinds of servers: authoritative and caching
- Two kinds of requests: iterative and recursive
- DNS tunneling:
 - Encode (SSH) traffic in DNS requests to authoritative server
 - Special authoritative server extracts and handles SSH data
- ► DNS DDOS amplification:
 - Send DNS request with spoofed target IP address
 - Much larger reply launched onto target
- ▶ DNS spoofing/cache poisoning: provide wrong DNS data
- ▶ Blind spoofing: cannot see (but trigger) request
- ► Countermeasure against blind spoofing: randomization

- Hostname resolution in the Internet uses DNS
- ► Two kinds of servers: authoritative and caching
- Two kinds of requests: iterative and recursive
- DNS tunneling:
 - Encode (SSH) traffic in DNS requests to authoritative server
 - Special authoritative server extracts and handles SSH data
- ► DNS DDOS amplification:
 - Send DNS request with spoofed target IP address
 - Much larger reply launched onto target
- ▶ DNS spoofing/cache poisoning: provide wrong DNS data
- ▶ Blind spoofing: cannot see (but trigger) request
- ► Countermeasure against blind spoofing: randomization
- Most powerful attack: sniffing DNS spoofing
- ► Countermeasures: Use crypto to protect DNS
 - ► DNSSEC (with various problems)
 - Alternative: DNSCurve

- Hostname resolution in the Internet uses DNS
- ► Two kinds of servers: authoritative and caching
- Two kinds of requests: iterative and recursive
- DNS tunneling:
 - Encode (SSH) traffic in DNS requests to authoritative server
 - Special authoritative server extracts and handles SSH data
- ► DNS DDOS amplification:
 - Send DNS request with spoofed target IP address
 - Much larger reply launched onto target
- ▶ DNS spoofing/cache poisoning: provide wrong DNS data
- ▶ Blind spoofing: cannot see (but trigger) request
- ► Countermeasure against blind spoofing: randomization
- Most powerful attack: sniffing DNS spoofing
- ► Countermeasures: Use crypto to protect DNS
 - DNSSEC (with various problems)
 - Alternative: DNSCurve
 - Some developments: TRR and DoH (https://hacks.mozilla. org/2018/05/a-cartoon-intro-to-dns-over-https/)

A longer recap

- ▶ So far in this lecture: various attacks (often MitM):
 - ARP spoofing
 - Routing attacks
 - DNS Attacks
- ► Conclusion: sniffing (and modifying) network traffic is not dark arts
- ▶ It's doable for 2nd-year Bachelor students
- ▶ It's even easier for administrators of routers

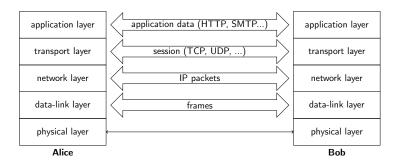
A longer recap

- ▶ So far in this lecture: various attacks (often MitM):
 - ARP spoofing
 - Routing attacks
 - DNS Attacks
- ► Conclusion: sniffing (and modifying) network traffic is not dark arts
- ▶ It's doable for 2nd-year Bachelor students
- ▶ It's even easier for administrators of routers
- ▶ So far, relatively little on countermeasures... so, what now?

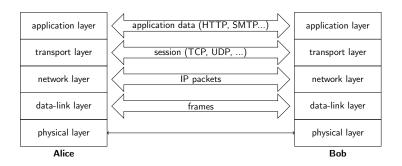
ENCRYPT



Cryptography in the TCP/IP stack



Cryptography in the TCP/IP stack



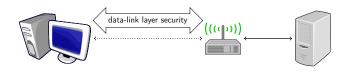
- ► Application-layer security (e.g., PGP, S/MIME, OTR)
- ► Transport-layer security (e.g., TLS/SSL)
- Network-layer security (e.g., IPsec)
- ▶ Link-layer security (e.g., WEP, WPA, WPA2)

Link-layer security



- ► Encrypt all network packets between network links, e.g., WPA2
- ▶ Point-to-point security between network interfaces
- "Encrypt to a MAC address"

Link-layer security



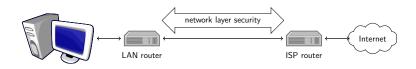
- ► Encrypt all network packets between network links, e.g., WPA2
- ▶ Point-to-point security between network interfaces
- "Encrypt to a MAC address"

Network-layer security

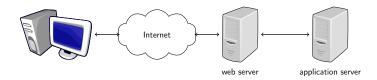


- ► Encrypt IP packets, main protocol: IPsec
- Point-to-point security between entities identified by IP addresses, typically routers or firewalls
- Routers encrypt and decrypt unnoticed by higher layers
- "Encrypt to an IP address"

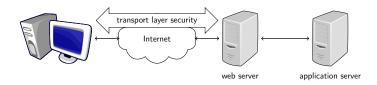
Network-layer security



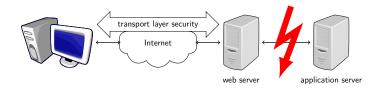
- ► Encrypt IP packets, main protocol: IPsec
- Point-to-point security between entities identified by IP addresses, typically routers or firewalls
- ▶ Routers encrypt and decrypt unnoticed by higher layers
- ▶ "Encrypt to an IP address"



- ► Encrypt sessions and messages, e.g. TLS/SSL
- communication between web browser and server, or email clients and servers
- entities identified by connections, port numbers
- "Encrypt to a server process"
- part of the communication might still be unprotected (to application server or between mail servers)



- ► Encrypt sessions and messages, e.g. TLS/SSL
- communication between web browser and server, or email clients and servers
- entities identified by connections, port numbers
- "Encrypt to a server process"
- part of the communication might still be unprotected (to application server or between mail servers)

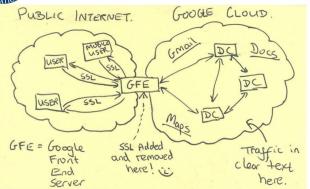


- ► Encrypt sessions and messages, e.g. TLS/SSL
- communication between web browser and server, or email clients and servers
- entities identified by connections, port numbers
- "Encrypt to a server process"
- part of the communication might still be unprotected (to application server or between mail servers)

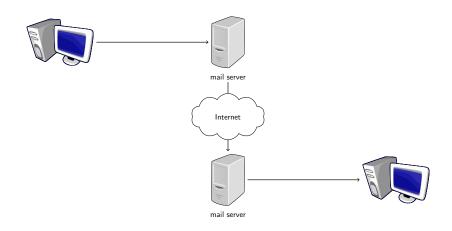
TOP SECRET//SI//NOFORN

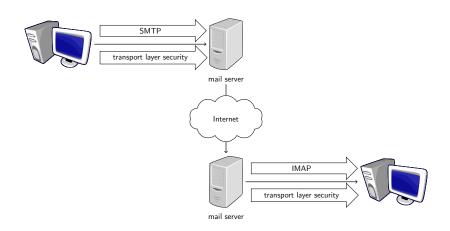


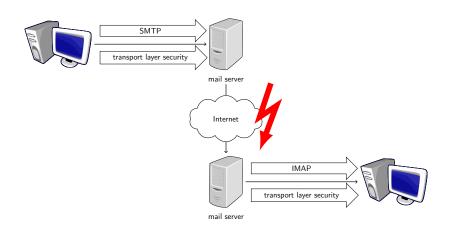
Current Efforts - Google



TOP SECRET//SI//NOFORN





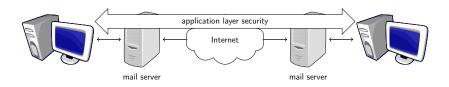


Application-layer security



- ► Add security to standard message formats
- ▶ For email: entire link between two user mail clients is protected
- authentication of sender and data
- end users have control over their keys (but need to know what they are doing, how to use PKI)
- end-to-end security ("encrypt to an e-mail address")

Application-layer security



- ► Add security to standard message formats
- ▶ For email: entire link between two user mail clients is protected
- authentication of sender and data
- end users have control over their keys
 (but need to know what they are doing, how to use PKI)
- end-to-end security ("encrypt to an e-mail address")

▶ Obvious first reflex: we want end-to-end security

- ▶ Obvious first reflex: we want end-to-end security
- ▶ How many people here regularly encrypt e-mail?

- ▶ Obvious first reflex: we want end-to-end security
- How many people here regularly encrypt e-mail?
- How many people here already did before first-semester "Security" lecture?

- Obvious first reflex: we want end-to-end security
- How many people here regularly encrypt e-mail?
- How many people here already did before first-semester "Security" lecture?
- Problem with application-level security: users
 - Need to rewrite every single application
 - Need users to switch to secured applications
 - Need users to take care of keys

- ▶ Obvious first reflex: we want end-to-end security
- How many people here regularly encrypt e-mail?
- How many people here already did before first-semester "Security" lecture?
- Problem with application-level security: users
 - Need to rewrite every single application
 - Need users to switch to secured applications
 - Need users to take care of keys
- Not impossible... who is using WhatsApp or Signal?

- ▶ Obvious first reflex: we want end-to-end security
- How many people here regularly encrypt e-mail?
- How many people here already did before first-semester "Security" lecture?
- Problem with application-level security: users
 - ▶ Need to rewrite every single application
 - ▶ Need users to switch to secured applications
 - Need users to take care of keys
- ▶ Not impossible... who is using WhatsApp or Signal?
- But tricky. Who checked the fingerprints of their contacts?

- ▶ Obvious first reflex: we want end-to-end security
- How many people here regularly encrypt e-mail?
- How many people here already did before first-semester "Security" lecture?
- Problem with application-level security: users
 - Need to rewrite every single application
 - ▶ Need users to switch to secured applications
 - Need users to take care of keys
- Not impossible... who is using WhatsApp or Signal?
- But tricky. Who checked the fingerprints of their contacts?
- Transport-layer security needs applications to be modified to use secure transport layer

- ▶ Obvious first reflex: we want end-to-end security
- How many people here regularly encrypt e-mail?
- How many people here already did before first-semester "Security" lecture?
- Problem with application-level security: users
 - Need to rewrite every single application
 - Need users to switch to secured applications
 - Need users to take care of keys
- Not impossible... who is using WhatsApp or Signal?
- But tricky. Who checked the fingerprints of their contacts?
- Transport-layer security needs applications to be modified to use secure transport layer
- Idea of network-layer security: No need to change applications (or user behavior)

- ▶ Obvious first reflex: we want end-to-end security
- How many people here regularly encrypt e-mail?
- How many people here already did before first-semester "Security" lecture?
- Problem with application-level security: users
 - Need to rewrite every single application
 - Need users to switch to secured applications
 - Need users to take care of keys
- Not impossible... who is using WhatsApp or Signal?
- ▶ But tricky. Who checked the fingerprints of their contacts?
- Transport-layer security needs applications to be modified to use secure transport layer
- Idea of network-layer security: No need to change applications (or user behavior)
- ► IPsec's promise: network security happening without you even noticing

IPsec overview (simplified)

IPSec is a protocol suite

- Authentication header (AH) protocol
 - ► Transport mode
 - ► Tunnel mode
- Encapsulating Security Payloads (ESP) protocol
 - ► Transport mode
 - Tunnel mode
- Security Association (SA) protocol

IPsec – Security Associations

- Concept to formalize unidirectional security relationships between two parties
- Security Association Database (SADB) contains list of active security associations (SA)

IPsec – Security Associations

- Concept to formalize unidirectional security relationships between two parties
- Security Association Database (SADB) contains list of active security associations (SA)

SA parameters:

- sequence number, sequence number overflow
- anti-replay window
- ▶ AH information: authentication algorithm, key, key lifetime, etc.
- ▶ ESP information: encryption algorithm, key, key lifetime, etc.
- lifetime of the SA
- IPsec protocol mode (tunnel or transport)
- maximal packet size

Transport mode:

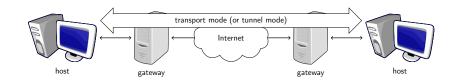
- Only the payload of the IP packet is protected
- ▶ Data is protected from source to destination
- ▶ Header information is completely in the clear
- Used only between hosts

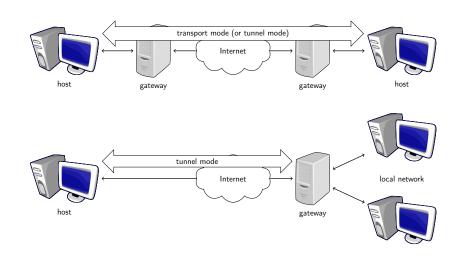
Transport mode:

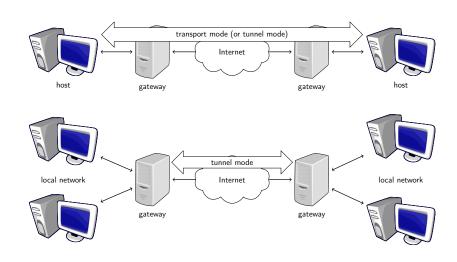
- Only the payload of the IP packet is protected
- ▶ Data is protected from source to destination
- ▶ Header information is completely in the clear
- Used only between hosts

Tunnel mode:

- ► Entire IP packet is protected (i.e. IP header and data)
- Becomes the payload of a new IP packet
- May contain different source and destination addresses
- Can be used between hosts, gateways, or host-gateway







The Authentication Header provides

- data integrity,
- authentication of IP packets,
- protection against replay attacks.

First two by use of a Message Authentication Code (MAC), e.g. HMAC-SHA1-96.

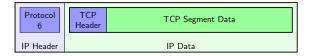
The Authentication Header provides

- data integrity,
- authentication of IP packets,
- protection against replay attacks.

First two by use of a Message Authentication Code (MAC), e.g. HMAC-SHA1-96.

IP packet is expanded with an AH that contains items such as:

- next header type of the header following this header,
- payload length length of AH,
- Security Parameter Index (SPI) identifies an SA,
- sequence number,
- authentication data contains the MAC of the packet, also called Integrity Check Value (ICV).

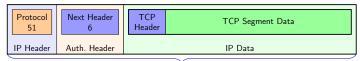


ICV (truncated HMAC) is computed over:

- immutable IP header fields (fields that do not change in transit), e.g., source address, IP header length,
- Auth. Header (except authentication data field),
- ▶ IP data.

Excluded fields are set to zero for HMAC computation.

IPSec Transport Mode



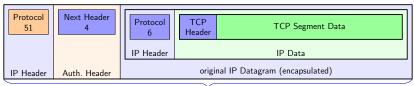
Authenticated Fields

ICV (truncated HMAC) is computed over:

- immutable IP header fields (fields that do not change in transit), e.g., source address, IP header length,
- Auth. Header (except authentication data field),
- ▶ IP data.

Excluded fields are set to zero for HMAC computation.

IPSec Tunnel Mode



Authenticated Fields

ICV (truncated HMAC) is computed over:

- immutable IP header fields (fields that do not change in transit), e.g., source address, IP header length,
- Auth. Header (except authentication data field),
- ▶ IP data.

Excluded fields are set to zero for HMAC computation.

Anti-replay protection prevents resending copies of authenticated packets.

- ▶ Uses sequence number field.
- ▶ For each new SA, sequence counter set to 0.
- ▶ Keep track of overflow (sequence number is 32 bits), negotiate new SA when counter reaches $2^{32} 1$.
- Check whether counter is in window of fixed size.
- Right edge = highest sequence number so far received (with valid authentication).
- ▶ Mark numbers of received packets with valid authentication.
- Advance window if new sequence number falls to the right of window and packet authenticates.
- Discard packet if number falls to the left of window or packet does not authenticate.

IPsec - Encapsulating Security Payload (ESP)

The Encapsulating Security Payload provides:

- confidentiality, i.e. encryption with block cipher in CBC mode, e.g. AES-CBC,
- functionality as in AH-like authentication, anti-replay (optional).

IPsec – Encapsulating Security Payload (ESP)

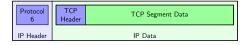
The Encapsulating Security Payload provides:

- confidentiality, i.e. encryption with block cipher in CBC mode, e.g. AES-CBC,
- functionality as in AH-like authentication, anti-replay (optional).

ESP adds an ESP header, encrypts the payload and adds an ESP trailer. An ESP packet contains:

- security parameter index (SPI),
- sequence number,
- payload data (encrypted),
- padding to achieve data length a multiple of 32 bits (encrypted),
- padding length (encrypted),
- next header (encrypted),
- (optional) authentication data.

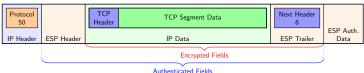
IPsec - Encapsulating Security Payload



- In transport mode, only data is encrypted, i.e. source and destination are in the clear
- ► In tunnel mode, the whole package is encrypted, i.e. real source and destination addresses are hidden
- Authentication not over IP header fields, only ESP header and data

IPsec - Encapsulating Security Payload

IPSec Transport Mode



- In transport mode, only data is encrypted,
 i.e. source and destination are in the clear
- ► In tunnel mode, the whole package is encrypted, i.e. real source and destination addresses are hidden
- ▶ Authentication not over IP header fields, only ESP header and data

IPsec - Encapsulating Security Payload

IPSec Tunnel Mode



Authenticated Fields

- ► In transport mode, only data is encrypted, i.e. source and destination are in the clear
- In tunnel mode, the whole package is encrypted, i.e. real source and destination addresses are hidden
- ▶ Authentication not over IP header fields, only ESP header and data

IPsec - crypto algorithms (until 2014)

See RFC 4835 (now obsolete)

- Encryption: block ciphers in Cipher Block Chaining (CBC) mode Must have:
 - ► NULL encryption (RFC 2410)
 - ► AES-CBC with 128-bit keys
 - TripleDES-CBC (168-bit keys)

IPsec - crypto algorithms (until 2014)

See RFC 4835 (now obsolete)

- Encryption: block ciphers in Cipher Block Chaining (CBC) mode Must have:
 - ▶ NULL encryption (RFC 2410)
 - AES-CBC with 128-bit keys
 - ► TripleDES-CBC (168-bit keys)
- Message authentication/integrity: Hash-based Message Authentication Code (HMAC), Must have:
 - ► HMAC-SHA1-96

May have:

► HMAC-MD5-96

IPsec - crypto algorithms (until 2014)

See RFC 4835 (now obsolete)

- Encryption: block ciphers in Cipher Block Chaining (CBC) mode Must have:
 - ▶ NULL encryption (RFC 2410)
 - ► AES-CBC with 128-bit keys
 - ► TripleDES-CBC (168-bit keys)
- Message authentication/integrity: Hash-based Message Authentication Code (HMAC), Must have:
 - HMAC-SHA1-96

May have:

- ► HMAC-MD5-96
- ▶ These are symmetric algorithms, need a pre-shared secret key
- ▶ Different options for key-agreement protocols: PSK, Internet Key Exchange (IKE, IKE2), Kerberos (KINK), IPSECKEY DNS records

IPsec - crypto algorithms (since 2014)

See RFC 7321

Old Requirement	New Requirement	Algorithm
MAY	SHOULD+	AES-GCM with a 16 octet ICV
MAY	SHOULD+	AES-GMAC with AES-128
MUST-	MAY	TripleDES-CBC
SHOULD NOT	MUST NOT	DES-CBC
SHOULD+	SHOULD	AES-XCBC-MAC-96
SHOULD	MAY	AES-CTR

► Crypto of IPsec is not really state of the art

- Crypto of IPsec is not really state of the art
- ▶ IPsec ESP allows (in principle) encryption without authentication
- ► Attack by Degabriele and Paterson, 2007
- ► Consequence: don't use encrypt-only!

- Crypto of IPsec is not really state of the art
- ▶ IPsec ESP allows (in principle) encryption without authentication
- Attack by Degabriele and Paterson, 2007
- ► Consequence: don't use encrypt-only!
- ▶ IPsec AH authenticates IP header (incl. source and dest.)
- ▶ NAT changes IP header (source or dest.)
- Possible to get IPsec through NAT, but needs effort (RFC 3715)

- Crypto of IPsec is not really state of the art
- ▶ IPsec ESP allows (in principle) encryption without authentication
- Attack by Degabriele and Paterson, 2007
- ► Consequence: don't use encrypt-only!
- ▶ IPsec AH authenticates IP header (incl. source and dest.)
- ▶ NAT changes IP header (source or dest.)
- Possible to get IPsec through NAT, but needs effort (RFC 3715)
- Most important problem: It's complicated!

"The first two generations of these documents (principally RFCs 1825–1829, published in 1995, and 2401–2412, published in 1998) are really only intended to provide a guide for implementors and are notoriously complex, difficult to interpret and lacking in overall structure.

. . .

The third and latest incarnation of the core IPsec standards were published as RFCs 4301–4309 in December 2005, and are somewhat more accessible.

. . .

However, the new RFCs are still a long and complex set of documents, totalling over 300 pages."

—Paterson, 2006

Another quote...

"We are of two minds about IPsec. On the one hand, IPsec is far better than any IP security protocol that has come before: Microsoft PPTP, L2TP, etc. On the other hand, we do not believe that it will ever result in a secure operational system. It is far too complex, and the complexity has lead to a large number of ambiguities, contradictions, inefficiencies, and weaknesses. It has been very hard work to perform any kind of security analysis; we do not feel that we fully understand the system, let alone have fully analyzed it."

—Ferguson, Schneier, 2003

ENGRYPT



Userspace VPN

- ► Sort-of alternative to IPsec tunnel: sshuttle ("poor-man's VPN")
- Disadvantages:
 - You need SSH access to the target
 - Need iptables rules to redirect traffic

Userspace VPN

- ► Sort-of alternative to IPsec tunnel: sshuttle ("poor-man's VPN")
- Disadvantages:
 - You need SSH access to the target
 - Need iptables rules to redirect traffic
- ► Generalize this idea: user-space VPN
- Software that authenticates users and tunnels traffic
- Examples: SSH, OpenVPN, WireGuard
- Question: How does the software get the traffic to tunnel (preferably without iptables)

- ► Linux provides TUN (tunneling) "software network interface"
- ► For routing, this acts like any other interface

- ► Linux provides TUN (tunneling) "software network interface"
- ► For routing, this acts like any other interface
- Output IP packets are fed into software that reads from file /dev/net/tun

- Linux provides TUN (tunneling) "software network interface"
- ▶ For routing, this acts like any other interface
- Output IP packets are fed into software that reads from file /dev/net/tun
- Use this mechanism to set up VPN between tyrion and arya with SSH:

```
tyrion # echo 1 > /proc/sys/net/ipv4/ip_forward
tyrion # ip tuntap add dev tun3 mode tun
tyrion # ip addr add dev tun3 10.0.5.1/24
tyrion # ip 1 set dev tun3 up

arya # echo 1 > /proc/sys/net/ipv4/ip_forward
arya # ip tuntap add dev tun5 mode tun
arya # ip addr add dev tun5 10.0.5.2/24
arya # ip 1 set dev tun5 up

tyrion # ssh -o Tunnel=point-to-point -w 3:5 arya
```

- Linux provides TUN (tunneling) "software network interface"
- ► For routing, this acts like any other interface
- Output IP packets are fed into software that reads from file /dev/net/tun
- Use this mechanism to set up VPN between tyrion and arya with SSH:

```
tyrion # echo 1 > /proc/sys/net/ipv4/ip_forward
tyrion # ip tuntap add dev tun3 mode tun
tyrion # ip addr add dev tun3 10.0.5.1/24
tyrion # ip 1 set dev tun3 up

arya # echo 1 > /proc/sys/net/ipv4/ip_forward
arya # ip tuntap add dev tun5 mode tun
arya # ip addr add dev tun5 10.0.5.2/24
arya # ip 1 set dev tun5 up

tyrion # ssh -o Tunnel=point-to-point -w 3:5 arya
```

Now try:

tyrion # ping 10.0.5.2

TAP interfaces

- ► TUN interfaces input/output IP packets
- ▶ Alternative: TAP interfaces that input/output ethernet frames
- Example (again with SSH)

```
tyrion # echo 1 > /proc/sys/net/ipv4/ip_forward
tyrion # ip tuntap add dev tap3 mode tap
tyrion # ip addr add dev tap3 10.0.5.1/24
tyrion # ip 1 set dev tap3 up
```

```
arya # echo 1 > /proc/sys/net/ipv4/ip_forward
arya # ip tuntap add dev tap5 mode tap
arya # ip addr add dev tap5 10.0.5.2/24
arya # ip 1 set dev tap5 up
```

```
tyrion # ssh -o Tunnel=ethernet -w 3:5 arya
```

TAP interfaces

- ► TUN interfaces input/output IP packets
- ▶ Alternative: TAP interfaces that input/output ethernet frames
- Example (again with SSH)

```
tyrion # echo 1 > /proc/sys/net/ipv4/ip_forward
tyrion # ip tuntap add dev tap3 mode tap
tyrion # ip addr add dev tap3 10.0.5.1/24
tyrion # ip 1 set dev tap3 up

arya # echo 1 > /proc/sys/net/ipv4/ip_forward
arya # ip tuntap add dev tap5 mode tap
arya # ip addr add dev tap5 10.0.5.2/24
arya # ip 1 set dev tap5 up

tyrion # ssh -o Tunnel=ethernet -w 3:5 arya
```

► Now try:

```
tyrion # ping 10.0.5.2
```

TAP interfaces

- ► TUN interfaces input/output IP packets
- ▶ Alternative: TAP interfaces that input/output ethernet frames
- Example (again with SSH)

```
tyrion # echo 1 > /proc/sys/net/ipv4/ip_forward
tyrion # ip tuntap add dev tap3 mode tap
tyrion # ip addr add dev tap3 10.0.5.1/24
tyrion # ip 1 set dev tap3 up

arya # echo 1 > /proc/sys/net/ipv4/ip_forward
arya # ip tuntap add dev tap5 mode tap
arya # ip addr add dev tap5 10.0.5.2/24
arya # ip 1 set dev tap5 up
```

```
tyrion # ssh -o Tunnel=ethernet -w 3:5 arya
```

- ► Now try: tyrion # ping 10.0.5.2
- ▶ You receive ARP packets through TAP
- ▶ The hosts are logically connected on the link layer
- ▶ They are in the same broadcast domain

Secure Sockets Layer (SSL) and Transport Layer Security (TLS):

- ► TLS is a variant of SSLv3
- SSL originally designed for web environment by Netscape
- Design goals: security of web traffic, email, etc.
- Had to work well with HTTP
- Provides transparency for higher layers

Secure Sockets Layer (SSL) and Transport Layer Security (TLS):

- ► TLS is a variant of SSLv3
- SSL originally designed for web environment by Netscape
- Design goals: security of web traffic, email, etc.
- Had to work well with HTTP
- Provides transparency for higher layers

SSL/TLS provides a secure channel between server and client:

- Confidentiality
- Server (and client) authentication
- Message integrity

SSL/TLS runs on top of TCP:

- ► Transparent for application-layer protocols
- SSL/TLS connection acts like a secured TCP connection
- ▶ Most protocols running over TCP can be run over SSL/TLS instead e.g., HTTP \rightarrow HTTPS, SMTP \rightarrow SMTPS, . . .

SSL/TLS runs on top of TCP:

- ► Transparent for application-layer protocols
- SSL/TLS connection acts like a secured TCP connection
- Most protocols running over TCP can be run over SSL/TLS instead e.g., HTTP \rightarrow HTTPS, SMTP \rightarrow SMTPS, ...

Protocols in SSL/TLS:

- Handshake Protocol: initiate session, Authenticate server/client, establish keys
- Record Protocol: data transfer,
 Compute MAC for integrity, encrypt MAC and data
- ► Alert Protocol: alert the other side of exceptional conditions, e.g., errors and warnings.

SSL/TLS Handshake

- ► Client → Server: ClientHello
 - ClientRandom: random number,
 - Session ID (when resuming a session),
 - List of available CipherSuites:
 pk key exchange, pk auth, sym encryption, hash alg.

Example: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256

ECDH Elliptic curve Diffie Hellman key exchange.
ECDSA Elliptic curve digital signature algorithm.
AES_128_CBC AES with 128-bit key in CBC mode.
SHA with 256-bit output for HMAC.

- ▶ Server → Client: ServerHello
 - ServerRandom: random number,
 - Session ID: implementation specific, random number
 - Chosen CipherSuite.
- ► Server → Client: Certificate
 - Server sends server certificate to client,
 client obtains server's public key and verifies certificate.
- Server \rightarrow Client: ServerKeyExchange for DHE: P^a , random a, for ECDHE: [a]P, random a, for RSA: -
- ▶ Server → Client: ServerHelloDone
 - Message marks end of server messages.

- ▶ Client \rightarrow Server: ClientKeyExchange for DHE: P^b for a random b, for ECDHE: [b]P for a random b, for RSA: random value encrypted with server's public key.
- ▶ Client → Server: ChangeCipherSpec
 - Notify that client switched to new CipherSuite.
- ▶ Client → Server: Finished
 - Encrypted Finished message containing hash over the previous handshake messages.

- ▶ Client \rightarrow Server: ClientKeyExchange for DHE: P^b for a random b, for ECDHE: [b]P for a random b, for RSA: random value encrypted with server's public key.
- ▶ Client → Server: ChangeCipherSpec
 - Notify that client switched to new CipherSuite.
- ▶ Client → Server: Finished
 - Encrypted Finished message containing hash over the previous handshake messages.
- ▶ For DHE and ECDHE, client and server compute joint session key.

- ▶ Server → Client: ChangeCipherSpec
 - ▶ Notify that server switched to new CipherSuite.
- ▶ Server → Client: Finished
 - Encrypted Finished message containing hash over the previous handshake messages.

- ▶ Server → Client: ChangeCipherSpec
 - Notify that server switched to new CipherSuite.
- ▶ Server → Client: Finished
 - Encrypted Finished message containing hash over the previous handshake messages.

Interrupted session can be resumed:

- ► Server and client are supposed to store session ID and MasterSecret,
- client sends session ID in ClientHello,
- reduced protocol: Hello, ChangeCipherSpec and Finished messages,
- new keying data is exchanged,
- new session keys are derived.

SSL/TLS Record Protocol

Record protocol to exchange encrypted and authenticated data:

- Payload data is split into fragments which are protected and transmitted independently; when received, fragments are decrypted and verified independently.
- ► Each fragment is authenticated with a MAC which is appended; MAC is over a sequence number (anti-replay) and the content.
- ▶ Data fragment and MAC are encrypted.
- ▶ A record header is attached to the encrypted data, containing information necessary for interpreting the record such as type of data (e.g. Handshake or ApplicationData), length, and SSL version.
- ▶ (header || encrypted fragment and MAC) is sent.

```
TLS ECDH ECDSA WITH NULL SHA
                                                                                                                                                                                                                                                                                                                    TLS ECDH RSA WITH AES 256 CBC SHA384
                                                                                                                                                                                       TLS SRP SHA WITH AES 128 CBC SHA
                                              TLS ECDHE ECDSA WITH AES 128 GCM SHA256
                                                                                                                                                                          TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_TLS_ECDHE_RSA_WITH_3DE
TLS_DHE_RSA_WITH_AES_128_CCM
                                                                   TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_NULL_SHA
                                                                                                                                                                                                                                                                                                                                                             TLS ECDHE PSK WITH AES 128 CBC SHA
                                                                                                                                                                                                      TLS DHE DSS WITH AES 256 GCM SHA384
                                                                                                                                                                                                                                                                                                     TLS SRP SHA WITH AES 256 CBC SHA
                 TLS ECDH RSA WITH AES 128 CBC SHA256 TLS_ECDHE_ECDSA WITH NULL SHA
                                                                                                                                                               TLS DHE DSS WITH CAMELLIA 256 CBC SHA
                                                                                                                                                                                                                                                                                                    TLS ECDH ECDSA WITH AES 128 CBC SHA
                 TLS SRP SHA RSA WITH 3DES EDE CBC SHA
                                                                                                                                                                                                TLS DH anon_WITH_AES_128_CBC_SHA256 TLS DH anon_WITH_CAMELLIA_128_CBC_SHA256
                                                                                                             TLS PSK WITH AES 128 CBC SHA256
                  TLS_ECOH_anon_WITH_3DES_EDE_CRC_SHA TLS_TON_WITH_AND_LEQ_AND_MANUAL SHATES_THOSE DESCRIPTION OF TISS_EDH SAW WITH AND STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STATES_TON_BASE_WITH_AND_STA
                                                                                                                                                                                                                                                                                                                                         TLS ECDH ECDSA_WITH_AES_256_CBC_SHA384
                                                                                                                                                                 TLS DH anon_WITH_CAMELLIA_128_CBC_SHA
                                     TLS ECDHE ECDSA WITH AES 128 CBC SHA256
                                                                                                                                                                                                                                                                          TLS DH anon WITH AES 128 GCM SHA256
                                                                                                                                                                             TLS_NTRU_MSS_WITH_AES_256_CBC_SHA TLS_DHE_DSS_WITH_SEED_CBC_SHA TLS_RSA_WITH_HC_128_CBC_SHA
                                                             TLS PSK WITH RC4 128 SHA
TLS DH anon WITH CAMELLIA 256 CBC SHA
                                                                                                                                                                              TLS RSA PSK WITH NULL SHA TLS DHE_DSS_WITH_SEED_LBC_SHA
TLS ECDH_ECOSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
                                                           TLS DHE DSS WITH AES 256 CBC SHA256
                                                                                                                                            TLS PSK WITH NULL SHA256 TLS NTRU RSA WITH AES 128 CBC SHA TLS DHE PSK WITH AES 128 CBC SHA256
   TLS DHE DSS WITH CAMELLIA 256 CBC SHA256
                                                                                                                                                    TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_EXPORT1024_WITH_RC4_56_MD5 TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256
                      TLS DH DSS WITH CAMELLIA 256 CBC SHA
                                                                                                            TLS_DH_DSS_WITH_AES_128_CBC_SHA25TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
                                                                                                                                                                                                                                                                                                       TLS PSK WITH NULL SHA384
               TLS ECDHE PSK WITH AES 256 CBC SHA
                   TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA_TLS_KRB5_EXPORT_WITH_RC4_40_MD5
                                                                                                                                                                                                                                                                                         TLS RSA EXPORT1024 WITH RC2 56 MD5
                                 SH RSA WITH AS 128 CCM SHAZED TO, DOA WITH LAWRELD, LOU, DOA, DOA
TIS, DIE COS WITH CAMELLU 128 CCC, SHAZED ST, SISA WITH AS 525 CCC, SHA
ST, SPEX WITH AS 256 CCC, SHA TIS, MISS, DOVON, WITH DOS, CSC, CAN, MOD TIS, DIE RSA WITH AS 128 CCC, SHA TIS, DIE PERK WITH MALE SHAZEN
TIS, SHA WITH AS 128 CCC, SHAZED STORM, WITH CAMELLUA 128 CCC, SHAZED
TIS, SHA WITH AS 128 CCC, SHAZED STORM, WITH CAMELLUA 128 CCC, SHAZED
                                                              TLS PSK WITH RES 250 USE 3FTO THE TILS DHE DSS EXPON: TLS RSA PSK WITH RC4_128_SHATLS_RSA_WITH_NULL_SHA256 SSL_FORTEZZA_KEA_WITH_RC4_128_SHA
         TLS RSA, WITH RC4 128 SHA SSL CK RC4 128 EXPORT4D WITH MD5 TL5 DHE RSA, WITH 3DES EDE CBC, SHA
SSL CK RC2 128 CBC, WITH MD5 SSC CK DES 192 EDE3 CBC, WITH MD5 TLS DH, RSA, WITH DE
                                                                             TIS SEA, WITH TACK JOB SHAS SL. CK, RS. LEE SECVICES, 192 (DEC, CRC, WITH, MDS.

SS. CK, CK JOZ GEC WITH, MDS. SSC(CC, CDS. 192 (DEC, CDC, SHA

TIS, DHE, RSA, EXPORT WITH DESAO CRC, SHA

SSL, FORTEZA, MDS, SSL, CK, CSL, WITH, MDS.

TIS, DHE, RSA, EXPORT WITH DESAO CRC, SHA

TIS, DHE, TIS, DHE, TIS, DHE, TIS, DHE, TIS, DHE

TIS, DHE, TIS, DHE, TIS, DHE

TIS, DHE, TIS,
                                                                                                                                                                                                                                                                                                             TLS RSA EXPORT1024 WITH DES CBC SHA
 TLS ECDHE ECDSA WITH RC4 128 SHA
         TLS PSK WITH AES 256 CBC SHA384
                                                                     SSLCK IDEA 128 CBC WITH MOS
SSLCK IDEA 128 CBC WITH MOS
S NULL WITH NULL NULL
S NULL WITH NULL NULL STAR FOR FOR SWA TLS DH_DSS_WITH_DES_CBC_SHA
                                                                TLS NULL WITH NULL NULL TLS KRB5
TLS RSA WITH 3DES EDE CBC SHA
                                                                                                                                        TLS RSA EXPORT WITH RC2 CBC 40 MD5
TLS DH anon WITH 3D
TLS ECDH ECDSA WITH AES 256 CBC SHATLS RSA WITH IDEA CBC SHA
                                                                                                                                                                                                                 3DES EDE CBC SHA TLS KRB5 W
SSL FORTEZZA KEA WITH FORTEZZA CBC SHA
                                                                                                                                                                                                                                                                                   TLS KRB5 WITH IDEA CBC MD5
                                                                                                                                                 TLS RSA WITH NULL SHA
                                                                                                                                                                                                                                                                                                                 TLS DH DSS WITH AES 256 GCM SHA384
                                  TLS KRB5 EXPORT WITH RC2 CBC 40 SHA
                                    TLS RSA WITH NULL MDS
                                                                                                              TLS DHE DSS WITH 3DES EDE CBC SHA
                                                                                                                                                                                                                                                                                                                        TLS DH RSA WITH AES 128 GCM SHA256
                                                                                                                                                                                                                             TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA TLS_I
TLS_KRBS_WITH_DES_CBC_MDS
                                                                                                                                                                                                                                                                                                                                                            SSL RSA FIPS WITH DES CBC SHA
                                              TLS_DH anon_EXPORT_WITH_RC4_40_MDS_TLS_KRB5_WITH_RC4_128_SHATLS_DH_RSA_WITH_AES_256_CBC_SHA_TLS_KRB5_EXPORT_WITH_RC4_40_SHA_TLS_DHE_PSK_WITH_AES_228_CBC_SHA
                                                                 TLS KRB5 WITH IDEA CBC SHA
TLS DHE DSS WITH AES 128 GCM SHA256
                                                                                                                                                                                                                                                     TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
                                                                             HE, USS, WITH, AES, 128, GCM, SHA256

TIS, DH, and, WITH, AES, 128, GCC, SHATLS, DH, RSA, WITH, AES, 128, GCC, SHATLS, DH, RSA, WITH, AES, 128, GCM, SHA256

TLS, DHE, DSS, WITH, ACR, 128, SFA, SFA, WITH, AES, 12

TLS, RSA, PSK, WITH, AES, 226, GCM, SHA384

TLS, RSA, PSK, WITH, AES, 226, GCM, SHA384
                                                                                                                                                                    TLS DHE RSA WITH DES CBC SHA
                                                                                                                                                                                                                                         TLS KRBS WITH DES CBC SHA
                                                                                                                                                                                                                                                                                                                  TLS RSA PSK WITH 3DES EDE CBC SHA
               TLS RSA PSK WITH AES 128 GCM SHA256
                                                                                                                                                                                                                        TLS DH anon WITH AES 256 CBC SHA
                                                                                                                                                                                                                                                                                                                         TLS_PSK_WITH_3DES_EDE_CBC_SHA
                                                                                                                                                                                                                                                                        TIS, RSA, WITH CAMELLIA 256 CBC SHA SSL RSA, FIPS WITH 3DES, EDE_CBC_SHA
TIS, RSA, PSK, WITH AES, 128, CBC_SHA256
TIS, RSA, PSK, WITH AES, 128, CBC_SHA256
TIS, SPS, SHA, RSA, WITH AES, 128, CBC_SHA
                                                                                                                                                                                 TLS RSA WITH AES 128 CBC SHA256
      TLS ECDHE RSA WITH RC4 128 SHA
                                             TLS DH DSS WITH AES 256 CBC SHA256 TUS REA WITH PE 128 CBC MDS TLS DHE DSS WITH AES 128 CBC SHA TLS NRU NSS WITH AES 128 CBC SHA TLS NRU NSS WITH AES 128 CBC SHA TLS NR LS NRU NSS WITH AES 128 CBC SHA TLS NR LS NRU NSS WITH AES 128 CBC SHA TLS NR LS NRU NSS WITH AES 128 CBC SHA TLS NR LS NRU NSS WITH AES 128 CBC SHA TLS NR LS NRU NSS WITH AES 128 CBC SHA TLS NR LS NRU NSS WITH AES 128 CBC SHA TLS NRU NSS WITH AES 128 CBC SHA 
                                                                                                                                                                                                                                                        TLS_NTRU_NSS_WITH_RC4_128_SHA_TLS_PSK_WITH_AES_128_GCM_SHA256
                                                                                                                                                                                                                                  TLS DHE DSS_WITH AES 256_CBC SHA
TLS DHE RSA_WITH SEED_CBC SHA
TLS DHE RSA_WITH SEED_CBC SHA
                                                                                                   TLS NTRU RSA WITH ABES EDE CBC SHA
TLS DHE PSK WITH ABES 128 GCM SHA256
TLS DHE PSK WITH ABES 128 GCM SHA256
TLS DHE RSA WITH ABES 128 GBC SHA256
TLS DH RSA WITH ABES TAB GBC SHA256
TLS ECDHE ECDSA WITH AES 256 GCM SHA384
                                                                                                                                                                                                                                                                                                                                     TLS ECDHE RSA WITH AES 128 CBC SHA256
TLS ECDH ECDSA WITH RC4 128 SHA
    TLS SRP SHA DSS WITH 3DES EDE CBC SHA
                                                                                                                                                                                                                                         TLS DH RSA WITH CAMELLIA 256 CBC SHA
                                                         TLS_RSA_PSK_WITH_NULL_SHA256 TLS_DH_DSS_WITH_SEED_CBC_SHA
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256
                                                                                                                                                                                                                                                                      TLS RSA PSK WITH AES 128 CBC SHA
                                                                                                                                                                                                                                                                                                                                 TLS RSA PSK WITH AES 256 CBC SHA384
TLS ECDH anon WITH RC4 128 SHA
                                                                                                                                                                           TLS RSA WITH AES 256 GCM SHA384 TLS_DHE_RSA_WITH AES 256 CBC SHA
                                                                TLS DHE PSK WITH 3DES EDE CBC SHA
                                                                                                                                                                                                                                                                                                                               TLS DHE RSA WITH CAMELLIA 128 CBC SHA256
                                                                                                                                                                                                                                    TIS ECOH BSA WITH BC4 128 SHA
                       TLS SRP SHA DSS WITH AES 256 CBC SHA
                                                                                                                                      TLS DHE PSK WITH AES 256 CBC SHA
                                                                                                                                                                                                                           TLS RSA WITH AES 128 GCM SHA256
                                                                                                                                                                                                                                                                                                                                                   TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
                              TLS RSA PSK WITH NULL SHA384
                                                                                                               TLS DH DSS WITH CAMELLIA 256 CBC SHA256
                                                                                                                                                                                                                                         TLS ECDHE ECDSA WITH 3DES EDE CBC SHA
                                                                             TLS ECDHE PSK WITH RC4 128 SHA TLS RSA EXPORT1024 WITH RC4 56 SHA
                                                                                                                                                                                                                                   TLS NTRU RSA WITH AES 256 CBC SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
                             TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256
                                                                                                                          TLS DH anon WITH AES 256 GCM SHA384
                                        TIS ECDHE RIA WITH ARS 256 ECN SHABAY TIS DIR PISA WITH SEED CELC SHA
TIS ECDHE STAN WITH CAMELIA 256 ECN SHABAY
TIS ECDHE SECON WITH ARS 256 ECN SHA TIS ECDHE PISA WITH ARS 256 ECN SHA TIS ECDHE RIA WITH ARS 256 ECN SHA
                                                                                                                                                                                                                         TLS DHE PSK WITH AES 256 GCM SHA384
                                                                                                                                                                                                                                                                                                                                                 TLS ECDHE ECDSA WITH AES 256 CBC SHA384
       TLS ECDHE PSK WITH NULL SHA
                                                                                                              TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 TLS_PSK_WITH_AES_256_GCM_SHA384
                 TLS ECDH ECDSA WITH AES 256 GCM SHA384
                                                                                                                                                                                                                                                                         TLS ECDHE RSA WITH AES 256 CBC SHA
                   TLS SRP_SHA_DSS_WITH AES_128_CBC_SHA TLS_ECDH_RSA_WITH_3DES_
TLS_ECDH_anon_WITH_AES_256_CBC_SHA TLS_DHE_PSK_WITH_AES_256_CBC_SHA384
                                                                                                                                TLS ECDH RSA WITH 3DES EDE CBC SHA
                                                                                                                                                                                                                                              TLS ECDH anon WITH AES 128 CBC SHA
TLS ECDHE PSK WITH NULL SHA256 TL
                                                                                                                                                                                                                                                                                                                                         TLS ECDHE RSA WITH AES 128 GCM SHA256
```

NULL and EXPORT

- ▶ NULL obviously provides no protection
- ▶ EXPORT ciphers are very low-security
- US export laws used to forbid strong crypto
- Strong crypto was considered a weapon
- EXPORT ciphers are a leftover from that time

```
TIS ECOH ECOSA WITH_NULL_SHA
                                                                                                                                                                                              TLS SRP SHA WITH AES 128 CBC SHA
                                                                                                                                                                                                                                                                                                                                  TLS ECDH RSA WITH AES 256 CBC SHA384
                                                TLS ECDHE ECDSA WITH AES 128 GCM SHA256
                                                                                                                                                                                 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
                                                                     TLS ECDH ECDSA WITH AES 128 GCM SHA256
                                                                                                                                                                                                                                                                                                                                                                            TLS ECDHE PSK WITH AES 128 CBC SHA
                                                                                                                                                              A WITH NULL SHA
                                                                                                                                                                                                              TLS DHE DSS WITH AES 256 GCM SHA384
                 TLS ECDH RSA WITH AES 128 CBC SHA256 TLS ECDHE ECDSA WITH NULL SHA
                                                                                                                                                                                                                                                                                                                 TLS SRP SHA WITH AFS 256 CRC SHA
                                                                                                                                                                                                                                                                                                                TLS ECDH ECDSA WITH AES 128 CBC SHA
                 TLS SRP SHA RSA WITH 3DES EDE CBC SHA
                                                                                                                                                                      TLS DHE DSS WITH CAMELLIA 256 CBC SHA
                                                                                                                                                                                                         TLS_DH_anon_WITH_AES_128_CBC_SHA256 TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
                                                                                                                   TLS PSK WITH AES 128 CBC SHA256
                   TLS ECDH anon WITH 3DES EDE CBC SHA
                   TLS SRP SHA RSA WITH JOES EDE CRE SHA TLS ECDH RSA WITH NULL SHATLS DH DSS WITH AES 128 GCM SHA256 TLS DH JOON WITH AES 256 CBC SHA256 TLS SRP SHA RSA WITH AES 256 CBC SHA364 TLS ECDHE PSK WITH AES 256 CBC SHA384 TLS DH JOES EVEN SHA256 TLS DH JO
                                                                                                                                                                                                                                                                                                                                              TLS ECDHE PSK WITH 3DES EDE CBC SHA
                                                                                                  HE_DSS_EXPORT1024_WITH_RC4_56_SHA
                                                                                                                                                                                                                                                                          TLS RSA WITH SEED CBC SHA
                                                                                                                                                                                                                                                                                                                                                       TLS ECDH ECDSA WITH AES 256 CBC SHA384
                                       TLS ECDHE ECDSA WITH AES 128 CBC SHA256
                                                                                                                                                                        TLS DH anon WITH CAMELLIA 128 CBC SHA
                                                                                                                                                                                                                                                                                     TLS DH anon WITH AES 128 GCM SHA256
                                                                                             TLS PSK WITH RC4 128 SHA
                                                                                                                                                                                    TLS NTRU_NSS_WITH_AES_256_CBC_SHA
                                                                                                                                                                                                                                                                    TLS DHE DSS WITH SEED CBC SHA TLS RSA WITH HC 128 CBC SHA
                                                               TLS DH anon WITH CAMELLIA 256 CBC SHA
                                                                                                                                                                                     TLS_ECDH_ECOSA_WITH_SDES_EDE_CBC_SHA TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
                                                            TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
                                                                                                                                                   TLS_PSK_WITH_NULL_SHA256 TLS_NTRU_RSA_WITH_AES_128_CBC_SHA TLS_DHE_PSK_WITH_AES_128_CBC_SHA256
   TLS DHE DSS WITH CAMELLIA 256 CBC SHA256
                                                                                                                                                          TLS DH DSS WITH CAMELLIA 128 CBC SHA TLS RSA EXPORT1024 WITH RC4 56 MD5 TLS DH RSA WITH CAMELLIA 128 CBC SHA256
                      TLS DH DSS WITH CAMELLIA 256 CBC SHA
                                                                                                                TLS_DH_DSS_WITH_AES_128_CBC_SHA25TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
                                                                                                                                                                                                                                                                                                                   TES PSK WITH NULL SHARRA
               TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA
                        S ECDH RSA WITH AES 128 GCM SHA256 TLS RSA WITH CAMELLIA 128 CBC SHA TLS_KRB5_EXPORT_WITH_RC4_40_MD5
                                                                                                                                                                                                                                                                                                     TLS RSA EXPORT1024 WITH RC2 56 MD5
                                   TILS DHE DSS_WITH CAMELIA 128 CBC SHA256 TES SSA WITH AES 256 CBC SHA
TLS DHE DSS_WITH AES 128 CBC SHA71S DHE PSK WITH AES 128
                                                               TLS RSA PSK WITH RC4 128 SHATLS RSA WITH NULL SHA256 SSL FORTEZZA KEA WITH RC4 128 SHA
                                                                                                                                                                                                                                                                                                                                                                 TLS RSA WITH CAMELLIA 128 CBC SHA256
             TLS_ECOH_RSA_WITH_AES_256_GCM_SRA384_TLS_RSA_WITH_AES_128_CBC_SHA_SSL_M
TLS_DH_anon_WITH_DES_CBC_SHA
                                                                                                                                                                                                                                                                                                                SSL CK RC2 128 CBC EXPORT40 WITH MD5
                                                                                                                                                                                                               TLS DH DSS WITH AES 128 CBC SHA
                                                                                                                                                                                                                                                                                                       TLS PSK WITH AES 128 CBC SHA TLS ECDH anon WITH NULL SHA
                                                                                                                                              TIS DH JOHO WITH RC4 128 MD5
TIS DH JOHO WITH RC4 128 MD5
TIS DH JOSS EXPORT WITH DES40 CBC SHA TIS DH DSS WITH AES 256 CBC SHA TIS DH RSA WITH AES 256 CBC SHA256
TIS DH JOSS EXPORT WITH DE540 CBC SHA TIS DH DSS WITH AES 256 CBC SHA TIS RSA WITH RABBIT CBC SHA
           TLS DH RSA WITH ASS 256 GCM SHA384 TLS DH CSS E
TLS DH RSA WITH ASS 256 GCM SHA384 TLS DH CSS E
TLS DHE RSA WITH CAMELLIA 256 CBC SHA256 TLS KRB5 WITH 3DES EDE CBC SHA
                                                                                                                                                                                                           TLS RSA WITH RC4 128 MD5
                                                                                                                                                                                                                    RSA WITH RC4 128 MD5
TLS NTRU RSA WITH RC4 128 MD5
TLS NTRU RSA WITH RC4 128 SHA
TLS SRP SHA WITH 3DES EDE CBC SHA
TLS RSA EXPORT WITH RC4 40 MD5
                      TLS DH RSA WITH CAMELLIA 128 CBC SHA TLS DH anon EXPORT WITH DESGO CBC SHA
                                                                                                                                                                                                                                                                                          TLS DHE DSS EXPORT1024 WITH DES CBC SHA
                                            TLS RSA WITH DES CBC SHA TLS DHE DSS WITH DES CBC SHA
                                                                                                                                                                                                                 SSL CK DES 64 CBC WITH MDS
                                                                                                                                                                                                                          TLS DHE RSA WITH 3DES EDE CBC SHA
                                                                                                                                                                                                                                                                                                                          TLS RSA EXPORT1024 WITH DES CBC SHA
                                                                                    TLS RSA WITH RC4 128 SHA SSL CK RC4 128 EXPORT40 WITH MD5 TLS DHE
SSL CK RC2 128 CBC WITH MD5 SSL CK DES 192 EDE3 CBC WITH MD5
 TLS ECDHE ECDSA WITH RC4 128 SHA
                                                                                                                                                                                                                                                              TLS DH RSA WITH DES CBC SHA TLS DHE RSA WITH AES 256 CBC SHA256
                                                                                                                                                                                                                                                                                      TLS DHE RSA EXPORT WITH DES40 CBC SHA
         TLS PSK WITH AES 256 CBC SHA384
                                                                                TLS DH DSS WITH 3DES EDE CBC SHA
TLS RSA EXPORT WITH DES40 CBC SHA
SSI FORTEZZA YEA WITH NULL SHA
                                                                         SSL CK IDEA 128 CBC, WITH MDS TLS, KRBS, WITH ACL 128 MDS SSL CK RC4 64 WITH MDS TLS, KRBS, WITH 3DES EDE, CBC, MDS TLS, DHE FAS, WITH ACL 128 MDS SMLL WITH MDS TLS, KRBS, WITH ACL 128 MDS SMLL WITH MDS TLS, KRBS, WITH ACL 128 MDS TLS, DHE FAS, WIT
                                                                  TLS NULL WITH NULL NULL TLS KKB
TLS RSA WITH 3DES EDE CBC SHA
                                                                                                                                                                                                                                                          TLS KRB5 EXPORT WITH DES CBC 40 SHA TLS RSA PSK_WITH_AES_256_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_IDEA_CBC_SHA
                                                                                                                                                                                                                                                                                            TLS KRB5 WITH IDEA CBC MD5
                                                                                                                                                                                   TLS DH anon WITH 3DES EDE CBC SHA
                                                                                                                                                                                                                                                                                                                                TLS DH DSS WITH AES 256 GCM SHA384
                                    TLS KRB5_EXPORT_WITH_RC2_CBC_40_SHA
TLS RSA_WITH_NULL_MD5
                                                                                                                                                        TIS RSA WITH NUIT SHA
                                                                                                                                                                                                                          SSL FORTEZZA KEA WITH FORTEZZA CBC SHA
                                                                                                                 TLS DHE DSS WITH 3DES EDE CBC SHA
                                                                                                                                                                                                                                       TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA TLS_ITLS_KRB5_WITH_DES_CBC_MD5
                                                                                                                                                                                                                                                                                                                                     TLS DH RSA WITH AES 128 GCM SHA256
                                                TLS DH anon EXPORT WITH RC4 40 MDS TLS KRB5 WITH RC4 128 SHA TLS DH RSA WITH AES 256 CBC SHA TLS KRB5 EXPORT WITH RC4 40 SHA TLS DHE PSK WITH AES 128 CBC SHA TLS KRB5 EXPORT WITH RC4 40 SHA TLS DHE PSK WITH AES 128 CBC SHA
                                                                    TLS DHE DSS WITH AES 128 GCM SHA256
                                                                                                                                                                          TLS DHE RSA WITH DES CBC SHA
                                                                                                                                                                                                                                                               TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
                                                                               HE DSS WITH AES 128 GCM SHAZED TIES DH RSA WITH AES 128 CBC SHA TLS DH RSA WITH AES 128 CBC SHA TLS DH RSA WITH AES 128 CBC SHA M SHA256 TLS KRBS EXPORT WITH RCZ CBC 40 MD5 TI
                                                                                                                                                                                                                                                    TLS KRRS WITH DES CRC SHA
                                                                                                                                                                                                                                                                                                                                TLS RSA PSK WITH 3DES EDE CBC SHA
               TLS RSA PSK WITH AES 128 GCM SHA256
                                                                                                                                                                                                                                                                                                                                      TLS PSK WITH 3DES EDE CBC SHA
                                                                                                                                                                                                                                 TLS DH anon WITH AES 256 CBC SHA
                                                                                    TLS DHE DSS WITH RC4 128 SRA
                                                                                                                                                                                                                                                                                   TLS_RSA_WITH_CAMELLIA 256 CBC_SHA_SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
                                                                                                                                                                                         TLS RSA WITH AES 128 CBC SHA256
      TLS ECDHE RSA WITH RC4 128 SHA
                                                TLS_DH_DSS_WITH_AES_256_GBC_SHA256 TLS_RSA_WITH_HC_128_CBC_MDS TLS_DHE_DSS_WITH_AES_128_CBC_SHA
                                                                                             TLS RSA PSK WITH AES 256 GCM SHA384
                                                                                                                                                                                                                                                                                                                TLS_RSA_PSK_WITH_AES_128_CBC_SHA256
                                                                                                                                                                                                                                                                 TLS_NTRU_NSS_WITH_RC4_128_SHA_TLS_PSK_WITH_AES_128_GCM_SHA256
                                                                                                                                                                                                                                                                                                                                                                TLS SRP SHA RSA WITH AES 128 CBC SHA
                                                                                    TIS PIRE AS WITH CAMELLE AS CEC SHA

ASS WITH AS LESS WIT
                                                                                                                                                                                                                                            TLS DHE DSS WITH AES 256 CBC SHA
 TLS ECDHE ECDSA WITH AES 256 GCM SHA384
                                                                                                                                                                                                                                                                                                             TLS DHE RSA WITH SEED CBC SHA
TLS ECDHE RSA WITH AES 128 CBC SHA256
    TLS SRP SHA DSS WITH 3DES EDE CBC SHA
                                                                                                        TLS DH RSA WITH AES 128 CBC SHA256
                                                                                                                                                                                                                                                    TLS DH RSA WITH CAMELLIA 256 CBC SHA
                                                                                                                                                                                                                                                                                                                                                            TLS ECDH ECDSA WITH RC4 128 SHA
                                                                 TIS ECOHE SHAZ36
TIS ECOHE PSK WITH AES 128 CBC SHA256
TIS DHE PSK WITH 3ES EDE CBC SHA256
                                                           TLS RSA PSK WITH NULL
                                                                                                                                                                                                                                                                                 TLS RSA PSK WITH AES 128 CBC SHA
                                                                                                                                                                                                                                                                                                                                              TLS RSA PSK WITH AES 256 CBC SHA384
TLS ECDH anon WITH RC4 128 SHA
                                                                                                                                                                                  TLS RSA WITH AES 256 GCM SHA384 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
                                                                                                                                                                                                                                            TLS ECDH RSA WITH RC4 128 SHA
                                                                                                                                                                                                                                                                                                                                            TLS DHE RSA WITH CAMELLIA 128 CBC SHA256
                        TLS SRP SHA DSS WITH AES 256 CBC SHA
                                                                                                                                           TLS DHE PSK WITH AES 256 CBC SHA
                                                                                                                                                                                                                                    TLS RSA WITH AES 128 GCM SHA256
TLS ECDHE ECDSA WITH 3DES EDE CBC SHA
                                                                                                                                                                                                                                                                                                                                                                 TLS ECDH ECDSA WITH AES 128 CBC SHA256
                                                                                                                    TLS DH DSS WITH CAMELLIA 256 CBC SHA256
                                                                               TLS ECDHE PSK WITH RC4 128 SHA TLS RSA EXPORT1024 WITH RC4 56 SHA
                                                                                                                                                                                                                                             TLS_NTRU_RSA_WITH_AES_256_CBC_SHA_TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
                              TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256 TLS_DH_anon_WITH_AES_256_GCM_SHA384
                                                                                                                                                                           48, 236, GOM SHA384 TLS, DIÊT, PEK JOHN JAES, 235, LOM, JOHANNA
HI SEED, GEG, MITH, MULL, SHASSA TLS, DH RSA, WITH, AMELIA, 236, GEG, SHAZSE
TLS, ECDHE, PSK, WITH, MULL, SHASSA TLS, DH RSA, WITH, AMELIA, 236, GEG, SHA
TLS, ECDHE, PSK, WITH, MULL, SHASSA TLS, DH RSA, WITH, AMELIA, SHA
                                         TLS ECDHE RSA WITH AES 256 GCM SHA384 TLS DH RSA WI
TLS ECDH RSA WITH AES 128 CBC SHA
TLS DH ANON WITH SEED CBC SHA
                                                                                                                                         TLS DH RSA WITH SEED CBC SHA
                                                                                                                                                                                                                                                                                                                                                               TLS ECDHE ECDSA WITH AES 256 CBC SHA384
                                                                                                                                                                                                                                                                                                                                                                TLS ECDHE RSA WITH AES 128 CBC SHA
       TLS ECDHE PSK WITH NULL SHA
                                                                                                                  TLS RSA WITH CAMELLIA 256 CBC SHA256 TLS_PSK_WITH_AES_256_GCM_SHA384
                 TLS ECDH ECDSA WITH AES 256 GCM SHA384
                                                                                                                                                                                                                                                                                    TLS ECDHE RSA WITH AES 256 CBC SHA
                                                                                                                                     TLS ECDH_RSA_WITH_3DES_EDE_CBC_SHA
                    TLS SRP SHA DSS WITH AES 128 CBC SHA TLS ECDH RSA WITH 3DES TLS ECDH anon WITH AES 256 CBC SHA TLS DHE PSK WITH AES 256 CBC SHA384
                                                                                                                                                                                                                                                         TLS ECDH anon WITH AES 128 CBC SHA
TLS ECDHE PSK WITH NULL SHA256 TLS ECDHE RSA WITH AES 128 GCM SHA256
```

```
TLS SRP SHA WITH AES 128 CBC SHA
                                                                                                                                                       TLS ECDH RSA WITH AES 256 CBC SHA384
                      TLS ECDHE ECDSA WITH AES 128 GCM SHA256
                                                                                   TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
                                TLS ECDH ECDSA WITH AES 128 GCM SHA256
                                                                                                                                                                           TLS ECDHE PSK WITH AES 128 CBC SHA
                                                                                                 TLS DHE DSS WITH AES 256 GCM SHA384
        TLS ECDH RSA WITH AES 128 CBC SHA256
                                                                                                                                               TLS SRP SHA WITH AFS 256 CRC SHA
                                                                             TLS DHE DSS WITH CAMELLIA 256 CBC SHA
                                                                                                                                               TLS ECDH ECDSA WITH AES 128 CBC SHA
        TLS SRP SHA RSA WITH 3DES EDE CBC SHA
                                                                                              TLS_DH_anon_WITH_AES_128_CBC_SHA256 TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
                                                      TLS PSK WITH AES 128 CBC SHA256
         TLS ECDH agon WITH 3DES EDE CRC SHA
                                                                              TLS DH DSS WITH AES 128 GCM SHA256 TLS DH anon WITH AES 256 CBC SHA256

TLS ECDHE PSK WITH AES 256 CBC SHA384

TLS ECDHE PSK WITH AES 256 CBC SHA384

TLS ECDHE PSK WITH AES 256 CBC SHA384
         TLS SRP SHA RSA WITH AES 256 CBC SHA
                                                                                                                            TIS RSA WITH SEED CRC SHA
                                                                                                                                                                 TLS ECDH ECDSA WITH AES 256 CRC SHA384
                  TLS ECDHE ECDSA WITH AES 128 CBC SHA256
                                                                                                                                  TLS DH anon WITH AES 128 GCM SHA256
                                            TLS PSK WITH RC4 128 SHA
                                                                                    TLS NTRU NSS WITH AES 256 CBC SHA
                                                                                                                           TLS DHE DSS WITH SEED CBC SHA TLS RSA WITH HC 128 CBC SHA
                             TLS DH anon WITH CAMELLIA 256 CBC SHA
                                                                                     TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
                            TLS DHE DSS WITH AES 256 CBC SHA256
                                                                                                  TLS_NTRU_RSA_WITH_AES_128_CBC_SHA TLS_DHE_PSK_WITH_AES_128_CBC_SHA256
 TLS DHE DSS WITH CAMELLIA 256 CBC SHA256
                                                                        TLS DH DSS WITH CAMELLIA 128 CBC SHA
                                                                                                                                                         TLS DH RSA WITH CAMELLIA 128 CBC SHA256
          TLS DH DSS WITH CAMELLIA 256 CBC SHA
                                                    TLS_DH_DSS_WITH_AES_128_CBC_SHA25TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
       TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA
           S ECDH RSA WITH AES 128 GCM SHA256 TLS RSA WITH CAMELLIA 128 CBC SHA
                                                                                                           TLS_DHE_RSA_WITH_AES_128_CBC_SHA<sup>TLS_</sup>DHE_PSK_WITH_RC4_128_SHA
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
                TLS DHE DSS WITH CAMELLIA 128 CBC SHA256 TLS RSA WITH AES 256 CBC SHA
TLS PSK WITH AES 256 CBC SHA
                             TLS RSA PSK WITH RC4 128 SHA
      SSL FORTEZZA KEA WITH RC4 128 SHA
                                                                                                  TLS DH DSS WITH AES 128 CBC SHA
                                                                                                                                          TLS PSK WITH AES 128 CBC SHA
                     TLS DHE DSS WITH CAMELLIA 128 CBC SHA
                                                                   TLS DH anon WITH RC4 128 MD5
                                                                                                                 TLS_DH_DSS_WITH_AES_256_CBC_SHATLS_DH_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_RABBIT_CBC_SHA
     TLS DH RSA WITH AES 256 CCM SHA384

TLS DH RSA WITH AES 256 CCM SHA384

TLS DHE RSA WITH CAMELLIA 256 CBC SHA256 TLS KRBS WITH 3DES EDE CBC SHA
                                                                                                TLS_RSA_WITH_RC4_128_MD5
                                                                                                                                    TLS_NTRU_RSA_WITH_RC4_128_SHA_TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA
          TLS DH RSA WITH CAMELLIA 128 CBC SHA
                     TLS RSA WITH DES CBC SHA TLS DHE DSS WITH DES CBC SHA
                                                                                                  SSL CK DES 64 CBC WITH MDS
                                                                                                      TLS DHE RSA WITH 3DES EDE CBC SHA
                                       TLS RSA WITH RC4 128 SHA
                                          SSL_CK_RC2_128_CBC_WITH_MD5 SSL_CK_DES_192_EDE3_CBC_WITH MD5
TLS_ECDHE_ECDSA_WITH_RC4 128 SHA
                                                                                                                       TLS_DH_RSA_WITH_DES_CBC_SHA_TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
    TLS PSK WITH AES 256 CBC SHA384
                                                                                         TLS DH DSS WITH 3DES EDE CBC SHA
                                  SSL_CK_IDEA_128_CBC_WITH_MD5
TI.S_KRB5_WITH_RC4_128_MD5
                                                                                               SSL_CK_RC4_64_WITH_MD5 TLS_KRB5_WITH_3DES_EDE_CBC_MD5 TLS_DHE RSA WITH AES 128 CBC SHA256
                                        TLS RSA WITH 3DES EDE CRC SHA
                                                                                     TLS DH DSS WITH DES CBC SHA
                                                                                                                                                            TLS RSA PSK WITH AES 256 CBC SHA
TLS ECDH ECDSA WITH AES 256 CBC SHATLS RSA WITH IDEA CBC SHA
                                                                                                                                      TLS KRB5 WITH IDEA CBC MD5
                                                                                    TLS DH anon WITH 3DES EDE CBC SHA
                                                                                                                                                      TLS DH DSS WITH AES 256 GCM SHA384
                                                                                                      SSI FORTEZZA KEA WITH FORTEZZA CRC SHA
                                                     TLS DHE DSS WITH 3DES EDE CBC SHA
                                                                                                            TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA TLS_
TLS_KRB5_WITH_DES_CBC_MD5
                                                                                                                                                         TLS DH RSA WITH AES 128 GCM SHA256
                                                                                                                                                                          SSL RSA FIPS WITH DES CBC SHA
                                                             TLS_KRB5_WITH_RC4_128_SHA TLS_DH_RSA_WITH_AES_256_CBC_SHA
                                                                                                                                                               TLS DHE PSK WITH AES 128 CBC SHA
                                       TLS KRB5 WITH IDEA CBC SHA
                                                                               TLS DHE RSA WITH DES CBC SHA
                                                                                                                       TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
                               TLS DHE DSS WITH AES 128 GCM SHA256
                                     TLS_DH_anon_WITH_AES_128_CBC_SHATLS_DH_RSA_WITH_AES_128_CBC_SHA
                                                                                                                  TIS KRBS WITH DES CRC SHA
                                                                                                                                                      TLS RSA PSK WITH 3DES EDE CBC SHA
TLS PSK WITH 3DES EDE CBC SHA
                                                                         SSL CR RC4 128 WITH MD5
       TLS RSA PSK WITH AES 128 GCM SHA256
                                                                                                         TLS DH anon WITH AES 256 CBC SHA
                                       TLS DHE DSS WITH RC4 128 SHA
                                                                                                                                 TLS_RSA_WITH_CAMELLIA 256 CBC_SHA_SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
                                                                                       TLS RSA WITH AES 128 CBC SHA256
  TLS ECDHE RSA WITH RC4 128 SHA
                      TLS_DH_DSS_WITH_AES_256_GBC_SHA256 TLS_RSA_WITH_HC_128_CBC_MDS TLS_DHE_DSS_WITH_AES_128_CBC_SHA
                                            TLS RSA PSK WITH AES 256 GCM SHA384
                                                                                                                                               TLS_RSA_PSK_WITH_AES_128_CBC_SHA256
                                                                                                                         TLS_NTRU_NSS_WITH_RC4_128_SHA_TLS_PSK_WITH_AES_128_GCM_SHA256
                                                                                                                                                                     TLS SRP SHA RSA WITH AES 128 CBC SHA
                                       TLS DHE DSS WITH AES 256 CBC SHA
TLS ECDHE ECDSA WITH AES 256 GCM SHA384
                                                                                                                                             TLS DHE RSA WITH SEED CBC SHA
TLS ECDHE RSA WITH AES 128 CBC SHA256
 TLS SRP SHA DSS WITH 3DES EDE CBC SHA
                                                 TLS DH RSA WITH AES 128 CBC SHA256
                                                                                                                  TLS DH RSA WITH CAMELLIA 256 CBC SHA
                                                                                                                                                                   TLS ECDH ECDSA WITH RC4 128 SHA
                              TLS_ECDHE_PSK_WITH_ABS_128_CBC_SHA256<sup>TLS_DH_DSS_WITH_SEED_CBC_SHA</sup>TLS_DHE_PSK_WITH_3DES_EOE_CBC_SHA
                                                                                                                                TLS RSA PSK WITH AES 128 CBC SHA
                                                                                                                                                             TLS RSA PSK WITH AES 256 CBC SHA384
TLS ECDH anon WITH RC4 128 SHA
                                                                                   TLS RSA WITH AES 256 GCM SHA384 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
                                                                                                               TLS ECDH RSA WITH RC4 128 SHA
                                                                                                                                                            TLS DHE RSA WITH CAMELLIA 128 CBC SHA256
           TLS SRP SHA DSS WITH AES 256 CBC SHA
                                                                 TLS DHE PSK WITH AES 256 CBC SHA
                                                                                                           TLS RSA WITH AES 128 GCM SHA256
TLS ECDHE ECDSA WITH 3DES EDE CBC SHA
                                                                                                                                                                      TLS ECDH ECDSA WITH AES 128 CBC SHA256
                                                      TLS DH DSS WITH CAMELLIA 256 CBC SHA256
                                     TLS ECDHE PSK WITH RC4 128 SHA
                                                                                                          TLS NTRU RSA WITH AES 256 CBC SHA TLS ECDHE RSA WITH AES 256 CBC SHA384
TLS_DHE_PSK_WITH AES 256 GCM_SHA384
TLS_DHE_PSK_WITH AES 256 GCM_SHA384
              TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256 TLS_DH_anon_WITH_AES_256_GCM_SHA384
                                                                                                                 JOSE WITH JEES 256 GCM_SHA384
TIS_DH RSA WITH CAMELLIA 256 CBC SHA256
TIS_ECDHE ECDSA WITH JES 256 CBC SHA
TIS_ECDHE ECDSA WITH JES 256 CBC SHA
WITH JES 256 CBC SHA
                   TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DH_RSA_W
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_DH_ANON_WITH_SEED_CBC_SHA
                                                                TLS DH RSA WITH SEED CBC SHA
                                                                                                                                                                     TLS ECDHE ECDSA WITH AES 256 CBC SHA384
                                                                                                                                                                     TLS ECDHE RSA WITH AES 128 CBC SHA
                                                     TLS RSA WITH CAMELLIA 256 CBC SHA256 TLS_PSK_WITH_AES_256_GCM_SHA384
       TLS ECDH ECDSA WITH AES 256 GCM SHA384
                                                                                                                                 TLS ECDHE RSA WITH AES 256 CBC SHA
                                                                                                                             TLS_ECUPIE_ROB_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
                                                              TLS ECDH_RSA_WITH_3DES_EDE_CBC_SHA
             TLS SRP SHA DSS WITH AES 128 CBC SHA
         TLS ECDH anon WITH AES 256 CBC SHA TLS DHE PSK WITH AES 256 CBC SHA384
```

DES

- ▶ Data Encryption Standard from 1976
- ► Extremely low-security 56-bit key
- ▶ Some sort of fix: 3DES (112-bit or 168-bit key)
- ▶ Main problem with 3DES: it's slow

DES

- ▶ Data Encryption Standard from 1976
- ► Extremely low-security 56-bit key
- ▶ Some sort of fix: 3DES (112-bit or 168-bit key)
- ▶ Main problem with 3DES: it's slow

MD5

- ▶ Hash algorithm by Rivest from 1992
- ► Collision-resistance totally broken
- Also more advanced attacks (chosen-prefix collision attack)
- ▶ Weaknesses used to create a rogue CA certificate in 2008
- Weaknesses used against Windows update in Flame malware

```
TLS SRP SHA WITH AES 128 CBC SHA
                                                                                                                                                             TLS ECDH RSA WITH AES 256 CBC SHA384
                       TLS ECDHE ECDSA WITH AES 128 GCM SHA256
                                                                                      TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA_
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
                                  TLS ECDH ECDSA WITH AES 128 GCM SHA256
                                                                                                                                                                                 TLS ECDHE PSK WITH AES 128 CBC SHA
                                                                                                    TLS DHE DSS WITH AES 256 GCM SHA384
        TLS ECDH RSA WITH AES 128 CBC SHA256
                                                                                                                                                     TLS SRP SHA WITH AFS 256 CRC SHA
                                                                                 TLS DHE DSS WITH CAMELLIA 256 CBC SHA
                                                                                                                                                    TLS ECDH ECDSA WITH AES 128 CBC SHA
        TLS SRP SHA RSA WITH 3DES EDE CBC SHA
                                                                                                  TLS_DH_anon_WITH_AES_128_CBC_SHA256 TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
                                                        TLS PSK WITH AES 128 CBC SHA256
         TLS ECDH agon WITH 3DES EDE CRC SHA
                                                                                  TLS DH DSS WITH AES 128 GCM SHA256 TLS DH anon WITH AES 256 CBC SHA256

TLS ECDHE PSK WITH AES 256 CBC SHA384

TLS ECDHE PSK WITH AES 256 CBC SHA384

TLS ECDHE PSK WITH AES 256 CBC SHA384
         TLS SRP SHA RSA WITH AES 256 CBC SHA
                                                                                                                                  TLS RSA WITH SEED CBC SHA
                                                                                                                                                                       TLS ECDH ECDSA WITH AES 256 CBC SHA384
                   TLS ECDHE ECDSA WITH AES 128 CBC SHA256
                                                                                                                                       TLS DH anon WITH AES 128 GCM SHA256
                                             TLS PSK WITH RC4 128 SHA
                                                                                        TLS NTRU_NSS_WITH_AES_256_CBC_SHA
                                                                                                                                TLS DHE DSS WITH SEED CBC SHA TLS RSA WITH HC 128 CBC SHA
                               TLS DH anon WITH CAMELLIA 256 CBC SHA
                                                                                        TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
                             TLS DHE DSS WITH AES 256 CBC SHA256
                                                                                                      TLS_NTRU_RSA_WITH_AES_128_CBC_SHA TLS_DHE_PSK_WITH_AES_128_CBC_SHA256
 TLS DHE DSS WITH CAMELLIA 256 CBC SHA256
                                                                           TLS DH DSS WITH CAMELLIA 128 CBC SHA
                                                                                                                                                                TLS DH RSA WITH CAMELLIA 128 CBC SHA256
           TLS DH DSS WITH CAMELLIA 256 CBC SHA
                                                      TLS_DH_DSS_WITH_AES_128_CBC_SHA25TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
       TLS_ECDHE_PSK_WITH_AES_256 CBC SHA
          ILS ECDH RSA WITH AES 128 GCM SHA256 TLS RSA WITH CAMELLIA 128 CBC SHA
                 TLS DHE DSS WITH CAMELLIA 128 CBC SHA256 TLS RSA WITH AES 256 CBC SHA
TLS PSK WITH AES 256 CBC SHA
                                                                                                                TLS_DHE_RSA_WITH_AES_128_CBC_SHATLS_DHE_PSK_WITH_RC4_128_SHA
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
                               TLS RSA PSK WITH RC4 128 SHA
      TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA
                                                                                           SSL FORTEZZA KEA WITH RC4 128 SHA
                                                                             WITH DES CBC SHA
                                                                                                      TLS DH DSS WITH AES 128 CBC SHA
                                                                                                                                                TLS PSK WITH AES 128 CBC SHA
                     TLS DHE DSS WITH CAMELLIA 128 CBC SHA
                                                                      TLS DH anon WITH RC4 128 MD5
                                                                                                                      TLS_DH_DSS_WITH_AES_256_CBC_SHATLS_DH_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_RABBIT_CBC_SHA
     TLS DH RSA WITH AES 256 CCM SHA384

TLS DH RSA WITH AES 256 CCM SHA384

TLS DHE RSA WITH CAMELLIA 256 CBC SHA256 TLS KRBS WITH 3DES EDE CBC SHA
                                                                                                                                         TLS NTRU RSA WITH RC4 128 SHA TLS SRP SHA WITH 3DES EDE CBC SHA
                                                                                                   TLS RSA WITH RC4 128 MD5
           TLS DH RSA WITH CAMELLIA 128 CBC SHA
                     TLS RSA WITH DES CBC SHA. TLS DHE DSS WITH DES CBC SHA
                                                                                                      SSL CK DES 64 CBC WITH MD5
                                                                                                          TLS DHE RSA WITH 3DES EDE CBC SHA
                                         TLS RSA WITH RC4 128 SHA
                                           SSL_CK_RC2_128_CBC_WITH_MD5 SSL_CK_DES_192_EDE3_CBC_WITH_MD5
TLS ECDHE ECDSA WITH RC4 128 SHA
                                                                                                                           TLS_DH_RSA_WITH_DES_CBC_SHA_TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
    TLS PSK WITH AES 256 CBC SHA384
                                                                                            TLS DH DSS WITH 3DES EDE CBC SHA
                                   SSL_CK_IDEA_128_CBC_WITH_MD5
TLS_KRB5_WITH_RC4_128_MD5
                                                                                                  SSL_CK_RC4_64_WITH_MD5 TLS_KRB5_WITH_3DES_EDE_CBC_MD5 TLS_DHE RSA WITH AES 128 CBC SHA256
                                          TLS RSA WITH 3DES EDE CRC SHA
                                                                                         TLS DH DSS WITH DES CBC SHA
                                                                                                                                                                  TLS RSA PSK WITH AES 256 CBC SHA
TLS ECDH ECDSA WITH AES 256 CBC SHATLS RSA WITH IDEA CBC SHA
                                                                                                                                           TLS KRB5 WITH IDEA CBC
                                                                                       TLS DH anon WITH 3DES EDE CBC SHA
                                                                                                                                                            TLS DH DSS WITH AES 256 GCM SHA384
                                                                                                           SSL FORTEZZA KEA WITH FORTEZZA CBC SHA
                                                        TLS DHE DSS WITH 3DES EDE CBC SHA
                                                                                                                TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA TLS_
TLS_KRBS_WITH_DES_CBC_MDS
                                                                                                                                                               TLS DH RSA WITH AES 128 GCM SHA256
                                                               TLS_KRB5_WITH_RC4_128_SHA TLS_DH_RSA_WITH_AES_256_CBC_SHA
                                                                                                                                                                     TLS DHE PSK WITH AES 128 CBC SHA
                                         TLS KRB5 WITH IDEA CBC SHA
                                                                                                                            TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
                                 TLS DHE DSS WITH AES 128 GCM SHA256
                                       TLS_DH_anon_WITH_AES_128_CBC_SHATLS_DH_RSA_WITH_AES_128_CBC_SHA
                                                                                                                      TLS KRB5 WITH DES CBC SHA
                                                                                                                                                            TLS RSA PSK WITH 3DES EDE CBC SHA
                                                                             SSL CR RC4 128 WITH MD5
       TLS RSA PSK WITH AES 128 GCM SHA256
                                                                                                              TLS DH anon WITH AES 256 CBC SHA
                                                                                                                                                               TLS PSK WITH 3DES EDE CBC SHA
                                         TLS DHE DSS WITH RC4 128 SHA
                                                                                                                                      TLS_RSA_WITH_CAMELLIA 256 CBC_SHA_SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
                                                                                          TLS RSA WITH AES 128 CBC SHA256
   TLS ECDHE RSA WITH RC4 128 SHA
                       TLS_DH_DSS_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_HC_128_CBC_MD5 TLS_DHE_DSS_WITH_AES_128_CBC_SHA
                                                                                                                                                    TLS_RSA_PSK_WITH_AES_128_CBC_SHA256
TLS_RSA_PSK_WITH_AES_128_CBC_SHA256
TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA
                                                                                                                             TLS_NTRU_NSS_WITH_RC4_128_SHA_TLS_PSK_WITH_AES_128_GCM_SHA256
                                         TES ATRU NSS WITH AES 128 CBC SHA
TLS DHE RSA WITH CAMELLIA 256 CBC SHA
                                                                                                                   TLS DHE DSS WITH AES 256 CBC SHA
TLS ECDHE ECDSA WITH AES 256 GCM SHA384
                                                                                         SHA TLS NTRU NSS WITH 3DES EDE CBC SHA
                                                                                                                                                   TLS DHE RSA WITH SEED CBC SHA
TLS ECDHE RSA WITH AES 128 CBC SHA256
                                                    TLS DHE PSK WITH AES 128 GCM SHA256
  TLS SRP SHA DSS WITH 3DES EDE CBC SHA
                                                   TLS DH RSA WITH AES 128 CBC SHA256
                                                                                                                      TLS DH RSA WITH CAMELLIA 256 CBC SHA
                                                                                                                                                                          TLS ECDH ECDSA WITH RC4 128 SHA
                                     TLS ECDHE PSK WITH AES 128 CBC SHA256 TLS_DH_DSS_WITH_SEED_CBC SHA
                                                                                                                                     TLS RSA PSK WITH AES 128 CBC SHA
                                                                                                                                                                   TLS RSA PSK WITH AES 256 CBC SHA384
TLS ECDH anon WITH RC4 128 SHA
                                                                                       TLS RSA WITH AES 256 GCM SHA384 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
                                                                                                                   TLS ECDH RSA WITH RC4 128 SHA
                                                                                                                                                                  TLS DHE RSA WITH CAMELLIA 128 CBC SHA256
           TLS SRP SHA DSS WITH AES 256 CBC SHA
                                                                    TLS DHE PSK WITH AES 256 CBC SHA
                                                                                                               TLS RSA WITH AES 128 GCM SHA256
TLS ECDHE ECDSA WITH 3DES EDE CBC SHA
                                                                                                                                                                            TLS ECDH ECDSA WITH AES 128 CBC SHA256
                                                         TLS DH DSS WITH CAMELLIA 256 CBC SHA256
                                      TLS ECDHE PSK WITH RC4 128 SHA
                                                                                                              TLS NTRU RSA WITH AES 256 CBC SHA TLS ECDHE RSA WITH AES 256 CBC SHA384
TLS DHE PSK WITH AES 256 CCM SHA384
TLS DHE PSK WITH AES 256 CCM SHA384
              TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256 TLS_DH_anon_WITH_AES_256_GCM_SHA384
                                                                                                                      TIS_DOTHERS 256_GCM_SHA389

TIS_DH RSA_WITH_CAMELLIA 256_CBC_SHA256

TIS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA___TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA___TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA___TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA___
                    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DH_RSA_WITH_SEED_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_DH_ANON_WITH_SEED_CBC_SHA
                                                                                                                                                                           TLS ECDHE ECDSA WITH AES 256 CBC SHA384
                                                                                                                                                                            TLS ECDHE RSA WITH AES 128 CBC SHA
                                                       TLS RSA WITH CAMELLIA 256 CBC SHA256 TLS_PSK_WITH_AES_256_GCM_SHA384
        TLS ECDH ECDSA WITH AES 256 GCM SHA384
                                                                                                                                       TLS ECDHE RSA WITH AES 256 CBC SHA
                                                                                                                                  TLS_ECUPIE_ROB_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
                                                                 TLS ECDH RSA WITH 3DES EDE CRC SHA
          TLS SRP SHA DSS WITH AES 128 CBC SHA TLS ECOH RSA WITH 3DES
TLS ECOH anon WITH AES 256 CBC SHA TLS DHE PSK WITH AES 256 CBC SHA384
```

```
TLS SRP SHA WITH AES 128 CBC SHA
                                                                                                                                                           TLS ECDH RSA WITH AES 256 CBC SHA384
                       TLS ECDHE ECDSA WITH AES 128 GCM SHA256
                                                                                     TLS ECDHE ECDSA WITH AES 128 CBC SHA
                                 TLS ECDH ECDSA WITH AES 128 GCM SHA256
                                                                                                                                                                                TLS ECDHE PSK WITH AES 128 CBC SHA
                                                                                                                         TLS DHE RSA WITH AES 128 GCM SHA256
                                                                                                   TLS DHE DSS WITH AES 256 GCM SHA384
        TLS ECDH RSA WITH AES 128 CBC SHA256
                                                                                                                                                   TLS SRP SHA WITH AFS 256 CRC SHA
                                                                                TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA

TLS_ECDH_ECUSA_WITH_AES_120_CBC_SHA256

TLS_DH_anon_WITH_AES_128_CBC_SHA256

TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
                                                                                                                                                   TLS ECDH ECDSA WITH AES 128 CBC SHA
                                                       TLS PSK WITH AES 128 CBC SHA256
                                                                                 TLS DH DSS WITH AES 128 GCM SHA256 TLS DH anon WITH AES 256 CBC SHA256
TLS ECDHE PSK WITH AES 256 CBC SHA384
         TLS SRP SHA RSA WITH AES 256 CBC SHA
                                                                                                                                TLS RSA WITH SEED CBC SHA
                                                                                                                                                                      TLS ECDH ECDSA WITH AES 256 CBC SHA384
                   TLS ECDHE ECDSA WITH AES 128 CBC SHA256
                                                                                 TLS DH anon WITH CAMELLIA 128 CBC SHA
                                                                                                                                      TLS DH anon WITH AES 128 GCM SHA256
                                             TLS PSK WITH RC4 128 SHA
                                                                                       TLS NTRU NSS WITH AES 256 CBC SHA
                                                                                                                              TLS DHE DSS WITH SEED CBC SHA TLS RSA WITH HC 128 CBC SHA
                              TLS DH anon WITH CAMELLIA 256 CBC SHA
                             TLS DHE DSS WITH AES 256 CBC SHA256
                                                                                                                                  TLS DHE DSS WITH AES 128 CBC SHA256
                                                                                                    TLS NTRU RSA_WITH_AES_128_CBC_SHA TLS_DHE_PSK_WITH_AES_128_CBC_SHA256
 TLS DHE DSS WITH CAMELLIA 256 CBC SHA256
                                                                          TLS DH DSS WITH CAMELLIA 128 CBC SHA
                                                                                                                                                              TLS DH RSA WITH CAMELLIA 128 CBC SHA256
           TLS DH DSS WITH CAMELLIA 256 CBC SHA
                                                      TLS_DH_DSS_WITH_AES_128_CBC_SHA25TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
       TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA
                                                                                                               TLS_DHE_RSA_WITH_AES_128_CBC_SHA_TLS_DHE_PSK_WITH_RC4_128_SHA
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
           S ECDH RSA WITH AES 128 GCM SHA256 TLS RSA WITH CAMELLIA 128 CBC SHA
                 TLS DHE DSS WITH CAMELLIA 128 CBC SHA256 TLS RSA WITH AES 256 CBC SHA
TLS PSK WITH AES 256 CBC SHA
                              TLS RSA PSK WITH RC4 128 SHA
      TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA
                                                                                          SSL FORTEZZA KEA WITH RC4 128 SHA
                                                                                                     TLS_DH_DSS_WITH_AES_128_CBC_SHA
                                                                                                                                              TLS PSK WITH AES 128 CBC SHA
                     TLS DHE DSS WITH CAMELLIA 128 CBC SHA
                                                                                                                     TLS_DH_DSS_WITH_AES_256_CBC_SHATLS_DH_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_RABBIT_CBC_SHA
                         TLS DH RSA WITH AES 256 GCM SHA384
     TLS DHE RSA WITH CAMELUA 256 CBC SHA256
                                                                                                                                        TLS NTRU RSA WITH RC4 128 SHA
           TLS DH RSA WITH CAMELLIA 128 CBC SHA
                                        TLS RSA WITH RC4 128 SHA
TLS ECDHE ECDSA WITH RC4 128 SHA
                                                                                                                                                            TLS DHE RSA WITH AES 256 CBC SHA256
    TLS PSK WITH AES 256 CBC SHA384
                                                                                                                                                                 TLS DHE RSA WITH AES 128 CBC SHA256
                                                                                                                                                                 TLS RSA PSK WITH AES 256 CBC SHA
TLS ECDH ECDSA WITH AES 256 CBC SHATLS RSA WITH IDEA CBC SHA
                                                                                                                                                           TLS DH DSS WITH AES 256 GCM SHA384
                                                                                                          SSL FORTEZZA KEA WITH FORTEZZA CBC SHA
                                                                                                                                                              TLS DH RSA WITH AES 128 GCM SHA256
                                                               TLS KRB5 WITH RC4 128 SHA TLS DH RSA_WITH_AES_256_CBC_SHA
                                                                                                                                                                   TLS DHE PSK WITH AES 128 CBC SHA
                                TLS KRB5 WITH IDEA CBC SHA TLS DHE DSS WITH AES 128 GCM SHA256
                                                                                                                                                                TLS DH anon WITH CAMELLIA 256 CBC SHA256
                                                                                                                           TLS RSA WITH AES 256 CBC SHA256
                                      TLS_DH_anon_WITH_AES_128_CBC_SHATLS_DH_RSA_WITH_AES_128_CBC_SHA
       TLS RSA PSK WITH AES 128 GCM SHA256
                                                                                                             TLS DH anon WITH AES 256 CBC SHA
                                        TLS DHE DSS WITH RC4 128 SHA
                                                                                          TLS RSA WITH AES 128 CBC SHA256
                                                                                                                                     TLS_RSA_WITH_CAMELLIA_256 CBC_SHA
   TLS ECDHE RSA WITH RC4 128 SHA
                                             TLS RSA PSK WITH AES 256 GCM SHA384
                                                                                              TLS DHE DSS WITH AES 128 CBC SHA
                                                                                                                                                   TLS_RSA_PSK_WITH_AES_128_CBC_SHA256
                       TLS DH DSS WITH AES 256 CBC SHA256
                                         TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
                                                                                                                             TLS_NTRU_NSS_WITH_RC4_128_SHA_TLS_PSK_WITH_AES_128_GCM_SHA256
                                                                                                                                                                           TLS SRP SHA RSA WITH AES 128 CBC SHA
                                                                                                                  TLS DHE DSS WITH AES 256 CBC SHA
TLS ECDHE ECDSA WITH AES 256 GCM SHA384
                                                                                                                                                 TLS DHE RSA WITH SEED CBC SHA
TLS ECDHE RSA WITH AES 128 CBC SHA256
                                                   TLS DHE PSK WITH AES 128 GCM SHA256
                                                  TLS DH RSA WITH AES 128 CBC SHA256
                                                                                                                     TLS DH RSA WITH CAMELLIA 256 CBC SHA
                                                                                                                                                                        TLS ECDH ECDSA WITH RC4 128 SHA
                                    TLS_ECDHE_PSK_WITH_AES 128 CBC_SHA256 TLS_DH_DSS_WITH_SEED_CBC_SHA
                                                                                                                                    TLS RSA PSK WITH AES 128 CBC SHA
                                                                                                                                                                  TLS RSA PSK WITH AES 256 CBC SHA384
TLS ECDH anon WITH RC4 128 SHA
                                                                                      TLS RSA WITH AES 256 GCM SHA384 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
                                                                                                                  TLS ECDH RSA WITH RC4 128 SHA
                                                                                                                                                                 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
           TLS SRP SHA DSS WITH AES 256 CBC SHA
                                                                   TLS DHE PSK WITH AES 256 CBC SHA
                                                                                                              TLS_RSA_WITH_AES_128_GCM_SHA256
                                                                                                                                                                           TLS ECDH ECDSA WITH AES 128 CBC SHA256
                                                        TLS DH DSS WITH CAMELLIA 256 CBC SHA256
                                      TLS ECDHE PSK WITH RC4 128 SHA
                                                                                                             TLS_NTRU RSA WITH AES 256 CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
TLS_ECDUE_ECOSA_WITH_AES_256_GCM_SHA384
              TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256 TLS_DH_anon_WITH_AES_256_GCM_SHA384
                                                                                                                     JOSE WITH JEES 256 GCM_SHA384
TIS_DH RSA WITH CAMELLIA 256 CBC SHA256
TIS_ECDHE ECDSA WITH JES 256 CBC SHA
TIS_ECDHE ECDSA WITH JES 256 CBC SHA
WITH JES 256 CBC SHA
                    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DH_RSA_W
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_DH_ANON_WITH_SEED_CBC_SHA
                                                                  TLS DH RSA WITH SEED CBC SHA
                                                                                                                                                                          TLS ECDHE ECDSA WITH AES 256 CBC SHA384
                                                                                                                                                                          TLS ECDHE RSA WITH AES 128 CBC SHA
                                                                                                  TLS_PSK_WITH_AES_256_GCM_SHA384
                                                       TLS RSA WITH CAMELLIA 256 CBC SHA256
        TLS ECDH ECDSA WITH AES 256 GCM SHA384
                                                                                                                                      TLS ECDHE RSA WITH AES 256 CBC SHA
                                                                                                                                 TLS_ECUPIE_ROB_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
          TLS SRP SHA DSS WITH AES 128 CBC SHA
TLS ECOH anon WITH AES 256 CBC SHA TLS DHE PSK WITH AES 256 CBC SHA384
```

RC4

- Stream cipher by Rivest from 1987
- ► Multiple attacks, also against its use in TLS (AlFardan, Bernstein, Paterson, Poettering, Schuldt, 2013).
- ... see earlier slides on WEP insecurity

RC4

- Stream cipher by Rivest from 1987
- Multiple attacks, also against its use in TLS (AlFardan, Bernstein, Paterson, Poettering, Schuldt, 2013).
- ... see earlier slides on WEP insecurity

- ► CBC needs full blocks of plaintext
- ▶ Use padding to fill up to full block
- ▶ Padding oracle: Decryption leaks whether padding is correct

RC4

- Stream cipher by Rivest from 1987
- Multiple attacks, also against its use in TLS (AlFardan, Bernstein, Paterson, Poettering, Schuldt, 2013).
- ... see earlier slides on WEP insecurity

- ► CBC needs full blocks of plaintext
- ▶ Use padding to fill up to full block
- ▶ Padding oracle: Decryption leaks whether padding is correct
- ▶ TLS before 1.1: check MAC only if padding is correct
- Different error message for incorrect padding or incorrect MAC

RC4

- Stream cipher by Rivest from 1987
- Multiple attacks, also against its use in TLS (AlFardan, Bernstein, Paterson, Poettering, Schuldt, 2013).
- ... see earlier slides on WEP insecurity

- ► CBC needs full blocks of plaintext
- Use padding to fill up to full block
- ▶ Padding oracle: Decryption leaks whether padding is correct
- ▶ TLS before 1.1: check MAC only if padding is correct
- Different error message for incorrect padding or incorrect MAC
- ► Fix: always check MAC, but "small timing channel" (RFC 4346)

RC4

- Stream cipher by Rivest from 1987
- Multiple attacks, also against its use in TLS (AlFardan, Bernstein, Paterson, Poettering, Schuldt, 2013).
- ...see earlier slides on WEP insecurity

- CBC needs full blocks of plaintext
- Use padding to fill up to full block
- ▶ Padding oracle: Decryption leaks whether padding is correct
- ▶ TLS before 1.1: check MAC only if padding is correct
- Different error message for incorrect padding or incorrect MAC
- ► Fix: always check MAC, but "small timing channel" (RFC 4346)
- ► Timing channel exploited by "Lucky 13" attack (AlFardan and Paterson, 2013)

```
TLS SRP SHA WITH AES 128 CBC SHA
                                                                                                                                                   TLS ECDH RSA WITH AES 256 CBC SHA384
                     TLS ECDHE ECDSA WITH AES 128 GCM SHA256
                                                                                 TLS ECDHE ECDSA WITH AES 128 CBC SHA
                                TLS ECDH ECDSA WITH AES 128 GCM SHA256
                                                                                                                  TLS DHE RSA WITH AES 128 GCM SHA256
                                                                                                                                                                      TLS ECDHE PSK WITH AES 128 CBC SHA
                                                                                              TLS DHE DSS WITH AES 256 GCM SHA384
        TLS ECDH RSA WITH AES 128 CBC SHA256
                                                                                                                                            TLS SRP SHA WITH AFS 256 CRC SHA
                                                                           TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA TLS_ECDH_ECU5A_WITH_AES_126_CBC_SHA256 TLS_DH_anon_WITH_AES_128_CBC_SHA256 TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
                                                                                                                                           TLS ECDH ECDSA WITH AES 128 CBC SHA
                                                     TLS PSK WITH AES 128 CBC SHA256
                                                                            TLS DH DSS WITH AES 128 GCM SHA256 TLS DH anon WITH AES 256 CBC SHA256
         TLS SRP SHA RSA WITH AES 256 CBC SHA
                                                                                 TLS ECDHE PSK WITH AES 256 CBC SHA384
                                                                                                                         TLS RSA WITH SEED CBC SHA
                                                                                                                                                            TLS ECDH ECDSA WITH AES 256 CBC SHA384
                 TLS ECDHE ECDSA WITH AES 128 CBC SHA256
                                                                            TLS DH anon WITH CAMELLIA 128 CBC SHA
                                                                                                                               TLS DH anon WITH AES 128 GCM SHA256
                            TLS_PSK_WITH_RC4_128_SHA
TLS_DH anon_WITH_CAMELLIA_256_CBC_SHA
                                                                                  TLS NTRU NSS WITH AES 256 CBC SHA
                                                                                                                       TLS DHE DSS WITH SEED CBC SHA TLS RSA WITH HC 128 CBC SHA
                           TLS DHE DSS WITH AES 256 CBC SHA256
                                                                                                                           TLS DHE DSS WITH AES 128 CBC SHA256
                                                                                               TLS NTRU RSA_WITH_AES_128_CBC_SHA TLS_DHE_PSK_WITH_AES_128_CBC_SHA256
 TLS DHE DSS_WITH_CAMELLIA_256_CBC_SHA256
                                                                      TLS DH DSS WITH CAMELLIA 128 CBC SHA
                                                                                                                                                      TLS DH RSA WITH CAMELLIA 128 CBC SHA256
          TLS DH DSS WITH CAMELLIA 256 CBC SHA
                                                  TLS_DH_DSS_WITH_AES_128_CBC_SHA25TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
       TLS ECDHE PSK WITH AES 256 CBC SHA
         TLS ECDH RSA WITH AES 128 GCM SHA256 TLS RSA WITH CAMELLIA 128 CBC SHA
                                                                                                         TLS_DHE_RSA_WITH_AES_128_CBC_SHA_TLS_DHE_PSK_WITH_RC4_128_SHA
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
                TLS DHE DSS WITH CAMELLIA 128 CBC SHA256 TLS RSA WITH AES 256 CBC SHA
TLS PSK WITH AES 256 CBC SHA
                            TLS RSA PSK WITH RC4 128 SHA
      TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384_TLS_RSA_WITH_AES_128_CBC_SHA
                                                                                     SSL FORTEZZA KEA WITH RC4 128 SHA
                                                                                                TLS_DH_DSS_WITH_AES_128_CBC_SHA
                                                                                                                                      TLS PSK WITH AES 128 CBC SHA
                    TLS DHE DSS WITH CAMELLIA 128 CBC SHA
                                                                                                              TLS_DH_DSS_WITH_AES_256_CBC_SHA_TLS_DH_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_RABBIT_CBC_SHA
                        TLS DH RSA WITH AES 256 GCM SHA384
     TLS DHE RSA WITH CAMELUA 256 CBC SHA256
                                                                                                                                 TLS NTRU RSA WITH RC4 128 SHA
          TLS DH RSA WITH CAMELLIA 128 CBC SHA
                                      TLS RSA WITH RC4 128 SHA
TLS ECDHE ECDSA WITH RC4 128 SHA
                                                                                                                                                    TLS DHE RSA WITH AES 256 CBC SHA256
    TLS PSK WITH AES 256 CBC SHA384
                                                                                                                                                       TLS DHE RSA WITH AES 128 CBC SHA256
                                                                                                                                                        TLS RSA PSK WITH AES 256 CBC SHA
TLS ECDH ECDSA WITH AES 256 CBC SHATLS RSA WITH IDEA CBC SHA
                                                                                                                                                  TLS DH DSS WITH AES 256 GCM SHA384
                                                                                                   SSL FORTEZZA KEA WITH FORTEZZA CBC SHA
                                                                                                                                                     TLS DH RSA WITH AES 128 GCM SHA256
                                      TLS_KRBS_WITH_IDEA_CBC_SHA
                                                                                                                                                          TLS DHE PSK WITH AES 128 CBC SHA
                                                                                                                                                       TLS DH anon WITH CAMELLIA 256 CBC SHA256
                               TLS DHE DSS WITH AES 128 GCM SHA256
                                                                                                                     TLS RSA WITH AES 256 CBC SHA256
                                    TLS_DH_anon_WITH_AES_128_CBC_SHATLS_DH_RSA_WITH_AES_128_CBC_SHA
       TLS RSA PSK WITH AES 128 GCM SHA256
                                                                                                       TLS DH anon WITH AES 256 CBC SHA
                                      TLS DHE DSS WITH RC4 128 SHA
                                                                                     TLS RSA WITH AES 128 CBC SHA256
  TLS ECDHE RSA WITH RC4 128 SHA
                                                                                                                              TLS RSA WITH CAMELLIA 256 CBC SHA
                                           TLS RSA PSK WITH AES 256 GCM SHA384
                                                                                         TLS DHE DSS WITH AES 128 CBC SHA
                                                                                                                                           TLS_RSA_PSK_WITH_AES_128_CBC_SHA256
                     TLS DH DSS WITH AES 256 CBC SHA256
                                       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
                                                                                                                      TLS_NTRU_NSS_WITH_RC4_128_SHA_TLS_PSK_WITH_AES_128_GCM_SHA256
                                                                                                                                                                  TLS SRP SHA RSA WITH AES 128 CBC SHA
                                                                                                            TLS DHE DSS WITH AES 256 CBC SHA
                                                                                                                                          . SHA
TLS DHE RSA WITH SEED CBC SHA
TLS ECDHE RSA WITH AES 128 CBC SHA256
TLS ECDHE ECDSA WITH AES 256 GCM SHA384
                                                TLS DHE PSK WITH AES 128 GCM SHA256
                                                TLS DH RSA WITH AES 128 CBC SHA256
                                                                                                               TLS DH RSA WITH CAMELLIA 256 CBC SHA
                                                                                                                                                               TLS ECDH ECDSA WITH RC4 128 SHA
                                  TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256 TLS_DH_DSS_WITH_SEED_CBC_SHA
                                                                                                                             TLS RSA PSK WITH AES 128 CBC SHA
                                                                                                                                                         TLS RSA PSK WITH AES 256 CBC SHA384
TLS ECDH appn WITH RC4 128 SHA
                                                                                 TLS RSA WITH AES 256 GCM SHA384 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
                                                                                                            TLS ECDH RSA WITH RC4 128 SHA
                                                                                                                                                        TLS DHE RSA WITH CAMELLIA 128 CBC SHA256
          TLS SRP SHA DSS WITH AES 256 CBC SHA
                                                                TLS DHE PSK WITH AES 256 CBC SHA
                                                                                                        TLS_RSA_WITH_AES_128_GCM_SHA256
                                                                                                                                                                  TLS ECDH ECDSA WITH AES 128 CBC SHA256
                                                     TLS DH DSS WITH CAMELLIA 256 CBC SHA256
                                    TLS ECDHE PSK WITH RC4 128 SHA
                                                                                                            TLS_NTRU_RSA_WITH_AES_256_CBC_SHA_TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
             TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256 TLS_DH_anon_WITH_AES_256_GCM_SHA384
                                                                                                       TLS DHE PSK WITH AES 256 GCM SHA384
                                                                                                              EPSK WITH AES 256 UCM STRAUGH
TIS DH RSA WITH CAMELLIA 256 CBC SHA256
TIS ECDHE ECDSA WITH AES 256 CBC SHA
TIS ECDH RSA WITH AES 256 CBC SHA
                                                                                                                                                                 TLS ECDHE ECDSA WITH AES 256 CBC SHA384
                    TLS ECDHE RSA WITH AES 256 GCM SHA384
                                                               TLS DH RSA WITH SEED CBC SHA
                                     TLS ECDH RSA WITH AES 128 CBC SHA
TLS DH ANON WITH SEED CBC SHA
                                                                                                                                                                 TLS ECDHE RSA WITH AES 128 CBC SHA
       TLS_ECDH_ECDSA_WITH AES 256 GCM SHA384 TLS_RSA_WITH_CAMELLIA 256 CBC_SHA256
                                                                                             TLS PSK WITH AES 256 GCM SHA384
                                                                                                                              TLS ECDHE RSA WITH AES 256 CBC SHA
                                                                                                                          TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_E RSA_WITH_AES_128_GCM_SHA256
         TLS SRP SHA DSS WITH AES 128 CBC SHA
TLS ECOH anon WITH AES 256 CBC SHA TLS DHE PSK WITH AES 256 CBC SHA384
```

TLS ECDHE ECDSA WITH AES 128 GCM SHA256 TLS ECDH ECDSA WITH AES 128 GCM SHA256

TLS DHE RSA WITH AES 128 GCM SHA256 TLS DHE DSS WITH AES 256 GCM SHA384

TLS DH DSS WITH AES 128 GCM SHA256

TLS_DH_anon_WITH_AES_128_GCM_SHA256

TLS ECDH RSA WITH AES 128 GCM SHA256

TLS RSA PSK WITH AES 128 GCM SHA256

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS ECDH RSA WITH AES 256 GCM SHA384

TLS DH RSA WITH AES 256 GCM SHA384

TLS DH DSS WITH AES 256 GCM SHA384 TLS DH RSA WITH AES 128 GCM SHA256

TLS DHE DSS WITH AES 128 GCM SHA256

TLS RSA PSK WITH AES 256 GCM SHA384

TLS PSK WITH AES 128 GCM SHA256

TLS ECDHE ECDSA WITH AES 256 GCM SHA384 TLS DHE PSK WITH AES 128 GCM SHA256

TLS RSA WITH AES 256 GCM SHA384

TLS RSA WITH AES 128 GCM SHA256

TLS_DH_anon_WITH_AES_256_GCM_SHA384 TLS DHE PSK WITH AES 256 GCM SHA384 TLS ECDHE RSA WITH AES 256 GCM SHA384

TLS PSK WITH AES 256 GCM SHA384 TLS ECDH ECDSA WITH AES 256 GCM SHA384

TLS ECDHE RSA WITH AES 128 GCM SHA256

anonymous

- "anonymous" ciphers don't use certificates
- Susceptible to a MitM attack

anonymous

- "anonymous" ciphers don't use certificates
- Susceptible to a MitM attack

PSK

- ▶ Pre-shared keys (PSK) only practical in special environments
- ► Advantage: faster crypto
- ► Can be easier in small closed environments
- Doesn't scale for the Internet

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256

TLS DHE RSA WITH AES 128 GCM SHA256 TLS DHE DSS WITH AES 256 GCM SHA384

TLS_DH_DSS_WITH_AES_128_GCM_SHA256

TLS_DH_anon_WITH_AES_128_GCM_SHA256

TLS ECDH RSA WITH AES 128 GCM SHA256

TLS ECDH RSA WITH AES 256 GCM SHA384

TLS DH RSA WITH AES 256 GCM SHA384

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS DH DSS WITH AES 256 GCM SHA384

TLS_DH_RSA_WITH_AES_128_GCM_SHA256

TLS RSA PSK WITH AES 128 GCM SHA256

TLS RSA PSK WITH AES 256 GCM SHA384

TLS DHE DSS WITH AES 128 GCM SHA256

TLS PSK WITH AES 128 GCM SHA256

TLS ECDHE ECDSA WITH AES 256 GCM SHA384

TLS DHE PSK WITH AES 128 GCM SHA256

TLS RSA WITH AES 256 GCM SHA384

TLS RSA WITH AES 128 GCM SHA256

TLS DH anon WITH AES 256 GCM SHA384

TLS DHE PSK WITH AES 256 GCM SHA384

TLS ECDH ECDSA WITH AES 256 GCM SHA384

TLS ECDHE RSA WITH AES 256 GCM SHA384

TLS PSK WITH AES 256 GCM SHA384

TLS ECDHE RSA WITH AES 128 GCM SHA256

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_DSS_WITH_AES_256_GCM_SHA384

TLS_DH_DSS_WITH_AES_128_GCM_SHA256

TLS ECDH RSA WITH AES 128 GCM SHA256

TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384

TLS DH RSA WITH AES 256 GCM SHA384

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS_DH_DSS_WITH_AES_256_GCM_SHA384 TLS_DH_RSA_WITH_AES_128_GCM_SHA256

TLS DHE DSS WITH AES 128 GCM SHA256

TLS ECDHE ECDSA WITH AES 256 GCM SHA384

TLS_RSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS ECDHE RSA WITH AES 256 GCM SHA384

TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384

TLS ECDHE RSA WITH AES 128 GCM SHA256

Use ephemeral key exchange!

- ► Can encrypt with long-term public key
- Problem: key gets compromised, read all old messages

Use ephemeral key exchange!

- ► Can encrypt with long-term public key
- ▶ Problem: key gets compromised, read all old messages
- ▶ Better: use long-term public key for authentication
- ▶ Agree on new (ephemeral) encryption key for each session
- ► This is known as *perfect forward secrecy*
- ▶ Use ciphers containing DHE or ECDHE

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_DSS_WITH_AES_256_GCM_SHA384

TLS_DH_DSS_WITH_AES_128_GCM_SHA256

TLS ECDH RSA WITH AES 128 GCM SHA256

TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384

TLS DH RSA WITH AES 256 GCM SHA384

TLS DHE DSS WITH AES 128 GCM SHA256

TLS ECDHE ECDSA WITH AES 256 GCM SHA384

TLS_RSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS ECDHE RSA WITH AES 256 GCM SHA384

TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384

TLS ECDHE RSA WITH AES 128 GCM SHA256

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS DH DSS_WITH_AES_256_GCM_SHA384 TLS DH RSA WITH AES_128_GCM_SHA256

TLS ECDHE ECDSA WITH AES 128 GCM SHA256

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_DSS_WITH_AES_256_GCM_SHA384

TLS DHE RSA WITH AES 256 GCM SHA384

TLS_DHE_DSS_WITH_AES_128_GCM_SHA256

TLS ECDHE ECDSA WITH AES 256 GCM SHA384

TLS ECDHE RSA WITH AES 256 GCM SHA384

TLS ECDHE RSA WITH AES 128 GCM SHA256

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

TLS_DHE_DSS_WITH_AES_256_GCM_SHA384

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS_DHE_DSS_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS ECDHE RSA WITH AES 256 GCM SHA384

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

DSS and ECDSA

- ▶ DSS and ECDSA need random value for each signature
- Small biases in randomness are disastrous
- Attacker can compute signing key from various messages with few known "random" bits
- ▶ Bad ECDSA randomness allowed Sony PS3 crack



Image from http://search.dilbert.com/comic/Random%20Number%20Generator

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

TLS_DHE_DSS_WITH_AES_256_GCM_SHA384

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS_DHE_DSS_WITH_AES_128_GCM_SHA256

TLS ECDHE ECDSA WITH AES 256 GCM SHA384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

AES-GCM

- ► AES-GCM only available since TLS 1.2
- Consists of AES in counter mode and GHASH
- ► GHASH is designed for hardware implementation
- ▶ Intel built AES and GHASH hardware support into their recent CPUs
- ► Terribly hard to implement fast and securely in software
- Matter of time until we see timing attacks?

What now?

A reasonable selection of algorithms

- AES-GCM is quite good for many CPUs
- ► AES-CBC is not so terrible (after implementation fixes)
- ▶ DSS and ECDSA is maybe (hopefully!) not that much of a problem
- ▶ Client-side selection of algorithms is a tradeoff:
 - ▶ I really only want ECDHE, RSA, AES-GCM, SHA2
 - ▶ I also want to connect to at least a few web sites
- ► Good test: https://howsmyssl.com

What now?

A better selection of algorithms

- ▶ Better symmetric algorithms: ChaCha20-Poly1305
- ► ChaCha20 is a state-of-the art stream cipher
- ▶ Poly1305 is a state-of-the art authenticator
- Both designed by Bernstein
- ► RFC 7905
- ▶ Standardized for TLS since June 2016

- HTTPS (HTTP over SSL/TLS) uses pre-installed root certificates in the browser
- ▶ Operating systems come with various pre-installed certificates
- Authenticating a communication partner means: follow chain of trust to root CA

- HTTPS (HTTP over SSL/TLS) uses pre-installed root certificates in the browser
- Operating systems come with various pre-installed certificates
- Authenticating a communication partner means: follow chain of trust to root CA
- Compromise one root CA and all browsers are compromised
- ► Forge a root CA's certificate and all browsers are compromised

- HTTPS (HTTP over SSL/TLS) uses pre-installed root certificates in the browser
- ▶ Operating systems come with various pre-installed certificates
- Authenticating a communication partner means: follow chain of trust to root CA
- Compromise one root CA and all browsers are compromised
- ▶ Forge a root CA's certificate and all browsers are compromised
- Rogue CA certificate from MD5 vulnerabilities, 2008: http://www.win.tue.nl/hashclash/rogue-ca/

- HTTPS (HTTP over SSL/TLS) uses pre-installed root certificates in the browser
- Operating systems come with various pre-installed certificates
- Authenticating a communication partner means: follow chain of trust to root CA
- Compromise one root CA and all browsers are compromised
- ▶ Forge a root CA's certificate and all browsers are compromised
- ► Rogue CA certificate from MD5 vulnerabilities, 2008: http://www.win.tue.nl/hashclash/rogue-ca/
- ▶ DigiNotar compromised in 2011: >300,000 Iranian Gmail users compromised

SSLstrip

- ► Marlinspike, 2009: sslstrip
- ▶ Possible for an active attacker to "avoid" HTTPS
- ▶ Idea: rewrite links from HTTPS to HTTP

SSLstrip

- ► Marlinspike, 2009: sslstrip
- ▶ Possible for an active attacker to "avoid" HTTPS
- ▶ Idea: rewrite links from HTTPS to HTTP
- Requires that client does not enforce HTTPS
- ► More details:
 - Erik's lecture on Web Security
 - http://www.thoughtcrime.org/software/sslstrip/

SSLstrip

- ► Marlinspike, 2009: sslstrip
- ▶ Possible for an active attacker to "avoid" HTTPS
- ▶ Idea: rewrite links from HTTPS to HTTP
- Requires that client does not enforce HTTPS
- ► More details:
 - ► Erik's lecture on Web Security
 - http://www.thoughtcrime.org/software/sslstrip/
- ▶ Next homework assigment...

Common problem with cryptographic systems

▶ Users?

Common problem with cryptographic systems

- ▶ Users?
 - System is too hard to use
 - System puts important choices in the hands of the user

BLAME



▶ Interesting implementation of a modification detection code

- ▶ Interesting implementation of a modification detection code
- Provide plaintext that doesn't pass verification

- Interesting implementation of a modification detection code
- Provide plaintext that doesn't pass verification
- ▶ Blame users of the system for consuming that plaintext

- Interesting implementation of a modification detection code
- Provide plaintext that doesn't pass verification
- ▶ Blame users of the system for consuming that plaintext

"If your system interacts with dozens of third party clients, and all (or many) are using your stuff in the same, insecure way, then maybe the problem isn't with your clients."

—Green, 2018

▶ How to solve the user-problem?

- ▶ How to solve the user-problem?
- OpenVPN built on TLS, with lots of ciphersuite options
- ▶ WireGuard is *opinionated*: Users do not get to choose

- How to solve the user-problem?
- OpenVPN built on TLS, with lots of ciphersuite options
- ▶ WireGuard is *opinionated*: Users do not get to choose
- ▶ OpenVPN supports (until recently, defaulted to) 64-bit ciphers
- WireGuard only uses state-of-the-art crypto (Noise protocol framework, chacha20-poly1305, ...)

- How to solve the user-problem?
- OpenVPN built on TLS, with lots of ciphersuite options
- WireGuard is opinionated: Users do not get to choose
- ▶ OpenVPN supports (until recently, defaulted to) 64-bit ciphers
- WireGuard only uses state-of-the-art crypto (Noise protocol framework, chacha20-poly1305, ...)
- OpenVPN needs a certificate hierarchy (or pre-shared, static, symmetric keys)
- WireGuard's asymmetric trust relations are easy (like SSH keys)

- ▶ How to solve the user-problem?
- OpenVPN built on TLS, with lots of ciphersuite options
- WireGuard is opinionated: Users do not get to choose
- ▶ OpenVPN supports (until recently, defaulted to) 64-bit ciphers
- WireGuard only uses state-of-the-art crypto (Noise protocol framework, chacha20-poly1305, ...)
- OpenVPN needs a certificate hierarchy (or pre-shared, static, symmetric keys)
- WireGuard's asymmetric trust relations are easy (like SSH keys)
- OpenVPN supports layer 3 and layer 2
- WireGuard only supports layer 3

- ▶ How to solve the user-problem?
- OpenVPN built on TLS, with lots of ciphersuite options
- WireGuard is opinionated: Users do not get to choose
- ▶ OpenVPN supports (until recently, defaulted to) 64-bit ciphers
- WireGuard only uses state-of-the-art crypto (Noise protocol framework, chacha20-poly1305, ...)
- OpenVPN needs a certificate hierarchy (or pre-shared, static, symmetric keys)
- WireGuard's asymmetric trust relations are easy (like SSH keys)
- OpenVPN supports layer 3 and layer 2 (though they will tell you to use layer 3)
- WireGuard only supports layer 3

- ▶ How to solve the user-problem?
- OpenVPN built on TLS, with lots of ciphersuite options
- WireGuard is opinionated: Users do not get to choose
- OpenVPN supports (until recently, defaulted to) 64-bit ciphers
- WireGuard only uses state-of-the-art crypto (Noise protocol framework, chacha20-poly1305, ...)
- OpenVPN needs a certificate hierarchy (or pre-shared, static, symmetric keys)
- WireGuard's asymmetric trust relations are easy (like SSH keys)
- OpenVPN supports layer 3 and layer 2 (though they will tell you to use layer 3)
- WireGuard only supports layer 3
- WireGuard's use of network namespacing provides zero-effort leakfree VPN (https://www.wireguard.com/netns/)
 - ► No routing table changes required!