Network Security

Encrypting Network Communication

Radboud University Nijmegen, The Netherlands

Autumn 2014

Acknowledgement

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

A short recap

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

A short recap

- 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

A short recap

- 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

A short recap

- 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

A short recap

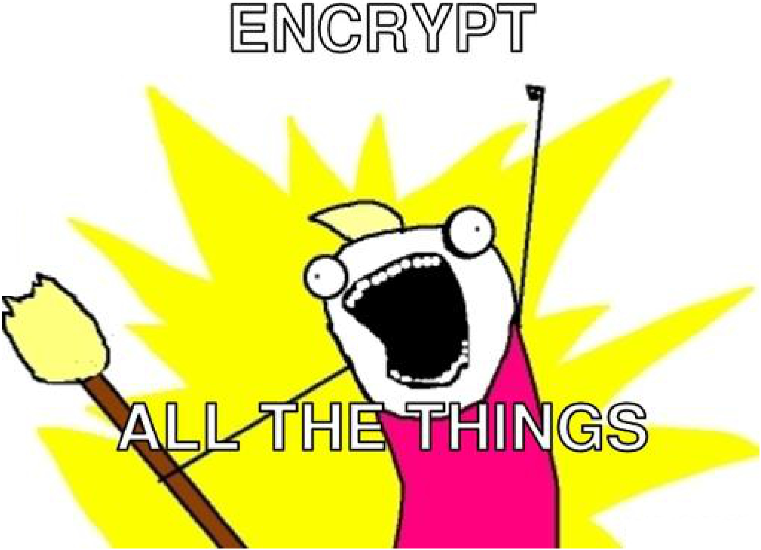
- Hostname resolution in the Internet uses DNS
- Two kinds of servers: authoritative and caching
- Two kinds of requests: iterative and recursive
- DNS tunneling:
  - Encode (SSH) traffic in DNS requests to authoritative server
  - Special authoritative server extracts and handles SSH data
- DNS DDOS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

A longer recap

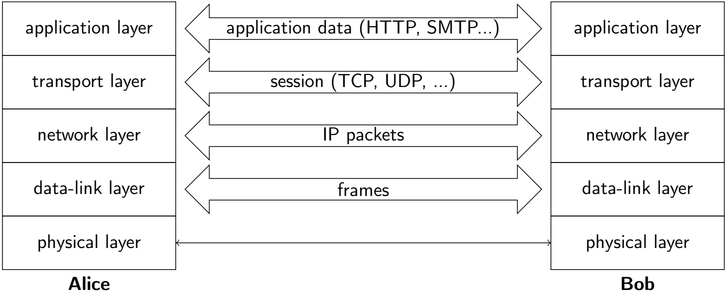
- So far in this lecture: various attacks (often MitM):
  - ARP spoofing
  - Routing attacks
  - DNS Attacks
- Conclusion: sniffing (and modifying) network traffic is not dark arts
- It's doable for 2nd-year Bachelor students
- It's even easier for administrators of routers

A longer recap

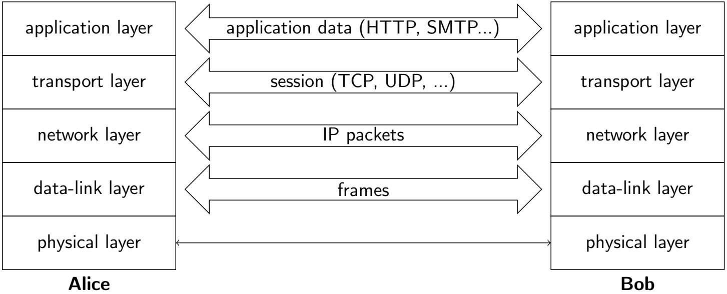
- So far in this lecture: various attacks (often MitM):
  - ARP spoofing
  - Routing attacks
  - DNS Attacks
- Conclusion: sniffing (and modifying) network traffic is not dark arts
- It's doable for 2nd-year Bachelor students
- It's even easier for administrators of routers
- So far, relatively little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


ENCRYPT
ALL THE THINGS

Cryptography in the TCP/IP stack

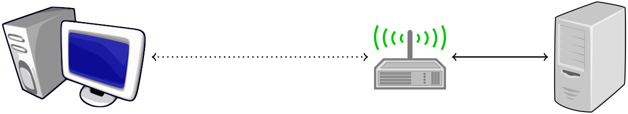


Cryptography in the TCP/IP stack



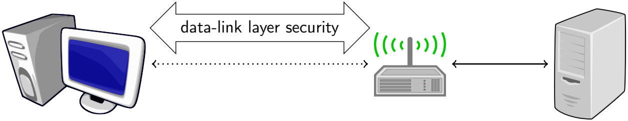
- Application-layer security (e.g., PGP, S/MIME, OTR)
- Transport-layer security (e.g., TLS/SSL)
- Network-layer security (e.g., IPsec)
- Link-layer security (e.g., WEP, WPA, WPA2)

Link-layer security



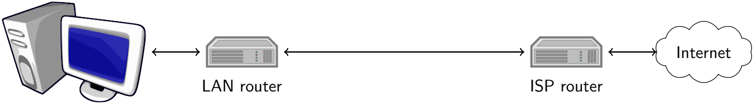
- Encrypt all network packets between network links, e.g., WPA2
- Point-to-point security between network interfaces
- “Encrypt to a MAC address”

Link-layer security



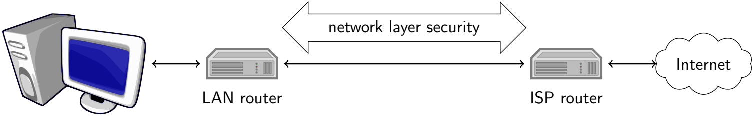
- Encrypt all network packets between network links, e.g., WPA2
- Point-to-point security between network interfaces
- “Encrypt to a MAC address”

Network-layer security



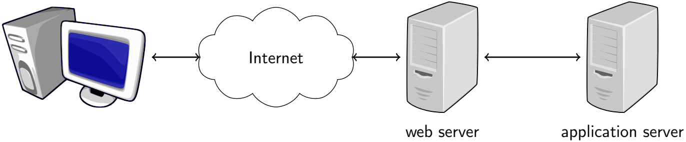
- Encrypt IP packets, main protocol: IPsec
- Point-to-point security between entities identified by IP addresses, typically routers or firewalls
- Routers encrypt and decrypt unnoticed by higher layers
- “Encrypt to an IP address”

Network-layer security



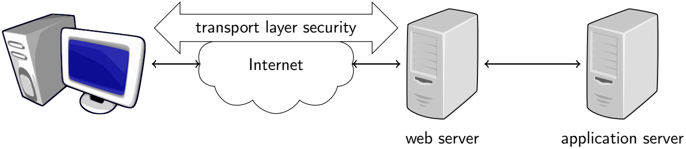
- Encrypt IP packets, main protocol: IPsec
- Point-to-point security between entities identified by IP addresses, typically routers or firewalls
- Routers encrypt and decrypt unnoticed by higher layers
- “Encrypt to an IP address”

Transport-layer security



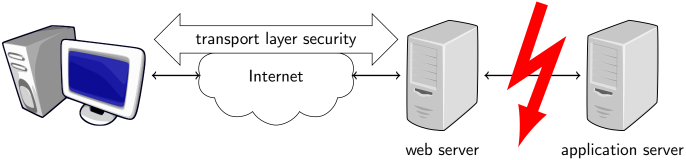
- Encrypt sessions and messages, e.g. TLS/SSL
- communication between web browser and server, or email clients and servers
- entities identified by connections, port numbers
- "Encrypt to a server process"
- part of the communication might still be unprotected (to application server or between mail servers)

Transport-layer security



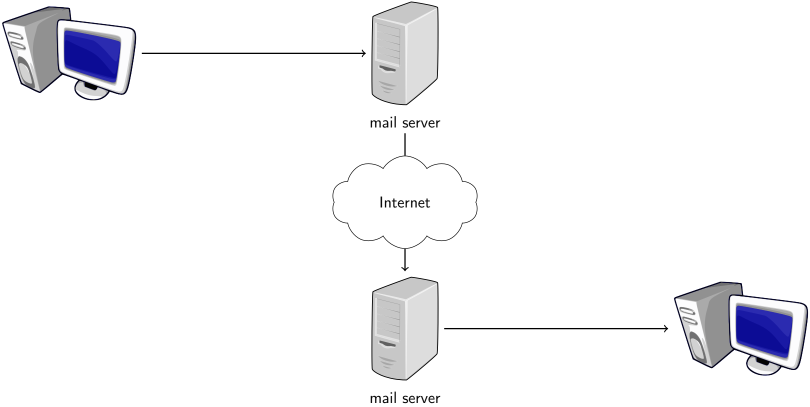
- Encrypt sessions and messages, e.g. TLS/SSL
- communication between web browser and server, or email clients and servers
- entities identified by connections, port numbers
- “Encrypt to a server process”
- part of the communication might still be unprotected (to application server or between mail servers)

Transport-layer security

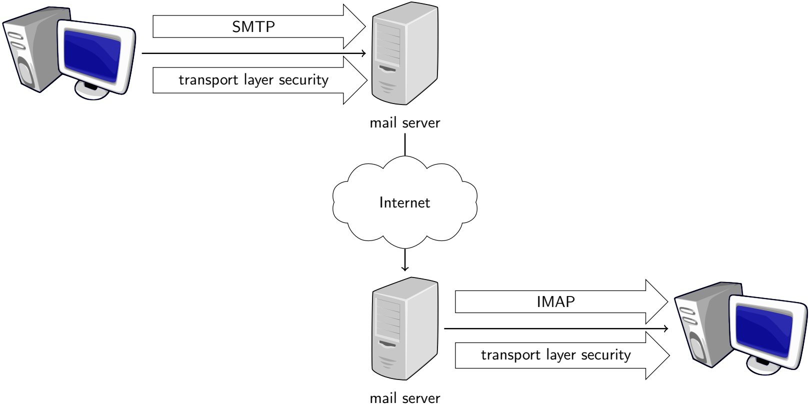


- Encrypt sessions and messages, e.g. TLS/SSL
- communication between web browser and server, or email clients and servers
- entities identified by connections, port numbers
- “Encrypt to a server process”
- part of the communication might still be unprotected (to application server or between mail servers)

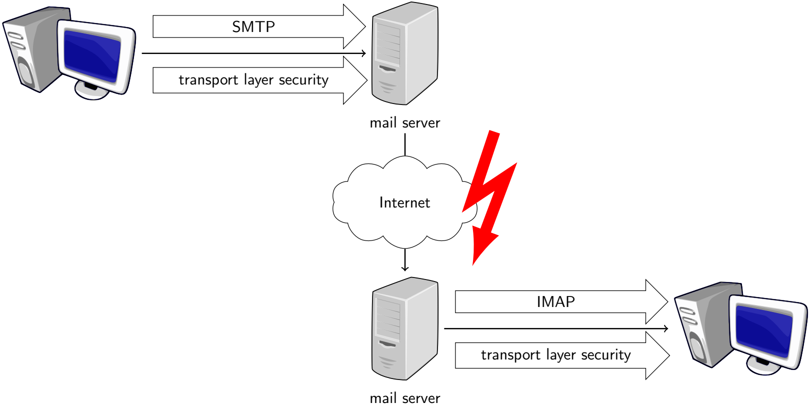
Transport-layer security



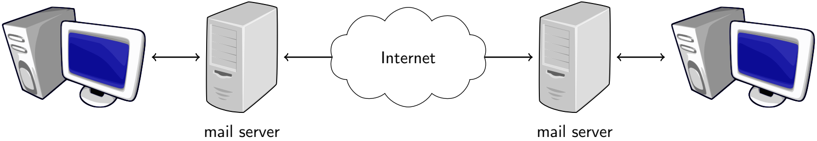
Transport-layer security



Transport-layer security

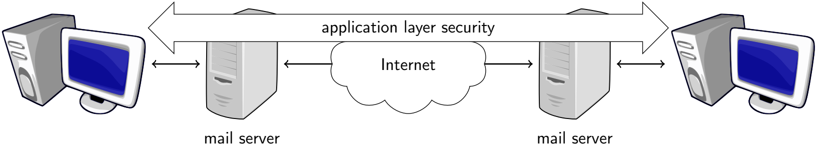


Application-layer security



- 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")

IPsec

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

IPsec

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

IPsec

- 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?

IPsec

- 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

IPsec

- 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
- Transport-layer security needs applications to be modified to use secure transport layer

IPsec

- 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
- 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 – Modes of Operation

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

IPsec – Modes of Operation

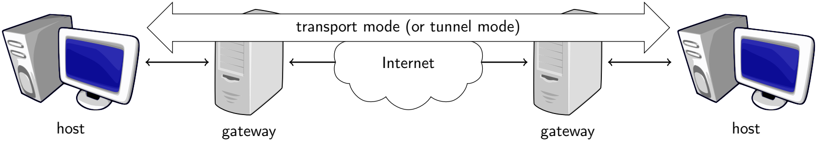
Transport mode:

- 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

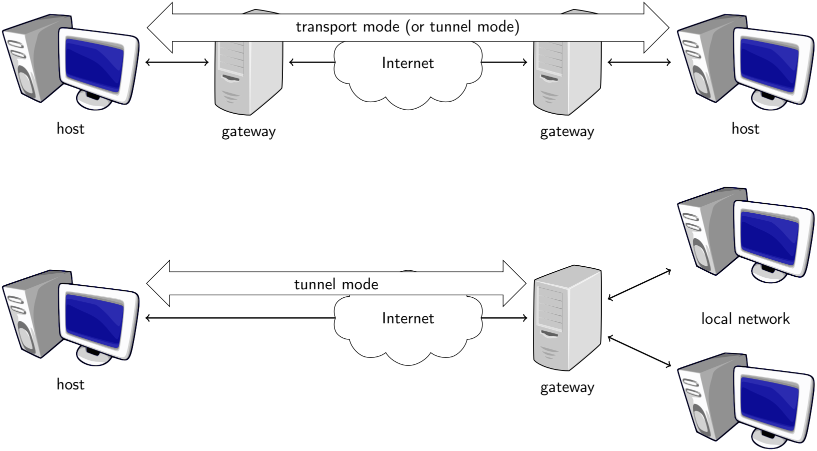
Tunnel mode:

- 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

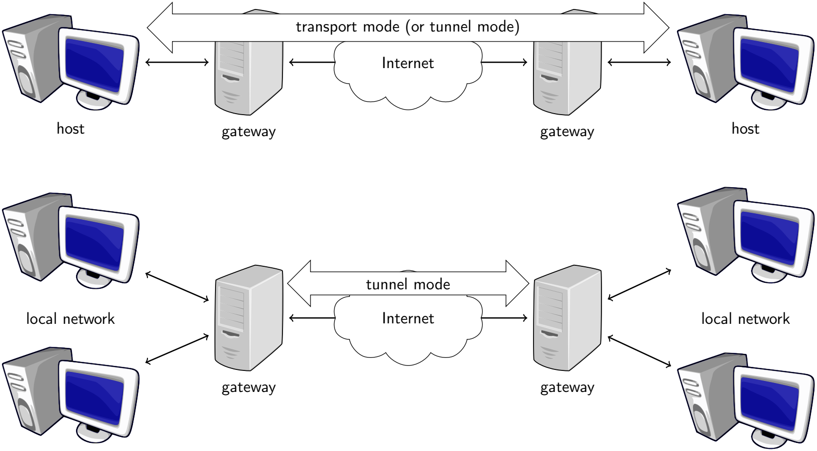
IPsec – Modes of Operation



IPsec – Modes of Operation



IPsec – Modes of Operation



IPsec Protocols

- Authentication Header (AH)
- Encapsulating Security Payloads (ESP)
- Security Associations (SA)

IPsec – Authentication Header

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.

IPsec – Authentication Header

The Authentication Header provides

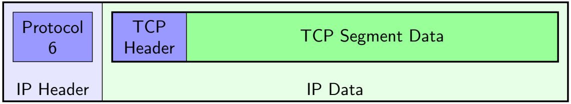
- data integrity,
- authentication of IP packets,
- protection against replay attacks.

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).

IPsec – Authentication Header

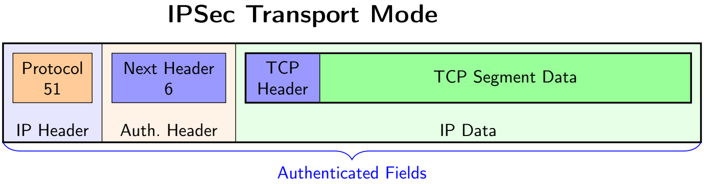


ICV (truncated HMAC) is computed over:

- 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 – Authentication Header

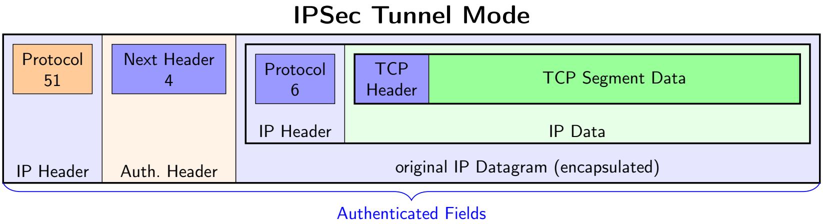


ICV (truncated HMAC) is computed over:

- 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 – Authentication Header



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 – Authentication Header

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)

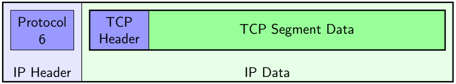
The Encapsulating Security Payload provides:

- 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:

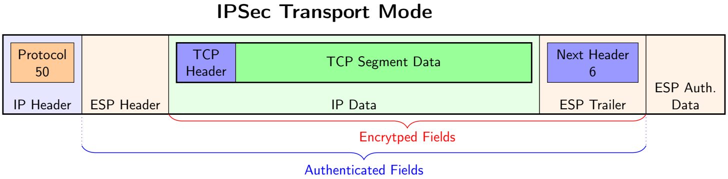
- security parameter index (SPI),
- sequence number,
- payload data (encrypted),
- padding – to achieve data length a multiple of 32 bits (encrypted),
- padding length (encrypted),
- next header (encrypted),
- (optional) authentication data.

IPsec – Encapsulating Security Payload



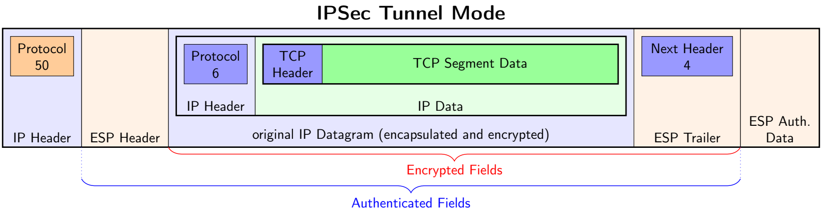
- In transport mode, only data is encrypted, i.e. source and destination are in the clear
- In tunnel mode, the whole package is encrypted, i.e. real source and destination addresses are hidden
- Authentication not over IP header fields, only ESP header and data

IPsec – Encapsulating Security Payload



- 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



- 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 – 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

IPsec - crypto algorithms

See RFC 4835

- 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

See RFC 4835

- 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

See RFC 4835

- 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 problems

- Crypto of IPsec is not really state of the art

IPsec problems

- 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 problems

- 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 requires extra effort

IPsec problems

- 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 requires extra effort
- Most important problem: **It's complicated!**

IPsec problems

"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

Userspace VPN

- Sort-of alternative to IPsec tunnel: `sshuttle` (“poor-man’s VPN”)
- Disadvantages:
  - You 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 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
- Question: How does the software get the traffic to tunnel (preferably without `iptables`)

TUN interfaces

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

TUN interfaces

- 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`

TUN interfaces

- 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 l 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 l set dev tun5 up

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

TUN interfaces

- 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 l 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 l 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 l 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 l 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 l 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 l 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 l 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 l 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 in the same broadcast domain

SSL/TLS

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

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

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 → HTTPS, SMTP → SMTPS, ...

SSL/TLS

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 → HTTPS, SMTP → 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.
SHA256	SHA with 256-bit output for HMAC.

SSL/TLS Handshake (cont.)

- 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 → 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.

SSL/TLS Handshake (cont.)

- Client → 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.

SSL/TLS Handshake (cont.)

- Client → 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.

SSL/TLS Handshake (cont.)

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

SSL/TLS Handshake (cont.)

- Server → Client: ChangeCipherSpec
  - Notify that client 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 sequential 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.

Which SSL/TLS Cipher Suites to use?

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_3DES_EDE_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_ECDHE_RSA_WITH_NULL_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_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_PSK_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_DSS_WITH_AES_128_GCM_SHA256
TLS_DH_anon_WITH_AES_256_CBC_SHA256
TLS_ECDH_RSA_WITH_NULL_SHA
TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384
TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA
TLS_RSA_WITH_SEED_CBC_SHA
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_NSS_WITH_AES_256_CBC_SHA
TLS_PSK_WITH_RC4_128_SHA
TLS_DHE_DSS_WITH_SEED_CBC_SHA
TLS_RSA_WITH_HC_128_CBC_SHA
TLS_RSA_PSK_WITH_NULL_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_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_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_DSS_WITH_AES_128_CBC_SHA25
TLS_PSK_WITH_NULL_SHA384
TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA
TLS_KRB5_EXPORT_WITH_RC4_40_MD5
TLS_RSA_EXPORT1024_WITH_RC2_56_MD5
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_PSK_WITH_RC4_128_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5
TLS_PSK_WITH_AES_256_CBC_SHA
TLS_DHE_PSK_WITH_NULL_SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_PSK_WITH_RC4_128_SHA
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_NULL_SHA256
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
SSL_FORTEZZA_KEA_WITH_RC4_128_SHA
SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_DSS_WITH_AES_128_CBC_SHA
TLS_PSK_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_NULL_SHA
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_RC4_128_MD5
TLS_PSK_WITH_NULL_SHA
TLS_DH_RSA_WITH_AES_256_CBC_SHA256
TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_RSA_WITH_AES_256_GCM_SHA384
TLS_DH_DSS_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_RABBIT_CBC_SHA
TLS_KRB5_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_RSA_WITH_RC4_128_MD5
TLS_NTRU_RSA_WITH_RC4_128_SHA
TLS_DHE_PSK_WITH_NULL_SHA
TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
SSL_CK_DES_64_CBC_WITH_MD5
TLS_RSA_WITH_DES_CBC_SHA
TLS_DHE_DSS_WITH_DES_CBC_SHA
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_ECDHE_ECDSA_WITH_RC4_128_SHA
SSL_CK_DES_192_EDE3_CBC_WITH_MD5
TLS_DH_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
SSL_CK_RC2_128_CBC_WITH_MD5
TLS_PSK_WITH_AES_256_CBC_SHA384
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_FORTEZZA_KEA_WITH_NULL_SHA
TLS_DHE_PSK_WITH_NULL_SHA256
SSL_CK_IDEA_128_CBC_WITH_MD5
SSL_CK_RC4_64_WITH_MD5
TLS_KRB5_WITH_3DES_EDE_CBC_MD5
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_KRB5_WITH_RC4_128_MD5
TLS_NULL_WITH_NULL_NULL
TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_DSS_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_PSK_WITH_AES_256_CBC_SHA
TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
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_RSA_WITH_NULL_SHA
SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA
TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA
TLS_RSA_WITH_NULL_MD5
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_KRB5_WITH_DES_CBC_MD5
SSL_RSA_FIPS_WITH_DES_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_KRB5_WITH_RC4_128_SHA
TLS_DH_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_PSK_WITH_AES_128_CBC_SHA
TLS_KRB5_EXPORT_WITH_RC4_40_SHA
TLS_KRB5_WITH_IDEA_CBC_SHA
TLS_DHE_RSA_WITH_DES_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_RSA_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_KRB5_WITH_DES_CBC_SHA
TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA
SSL_CK_RC4_128_WITH_MD5
TLS_RSA_PSK_WITH_AES_128_GCM_SHA256
TLS_PSK_WITH_3DES_EDE_CBC_SHA
TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_RC4_128_SHA
SSL_RSA_FIPS_WITH_3DES_EDE_CBC_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_RSA_WITH_HC_128_CBC_MD5
TLS_DH_DSS_WITH_AES_256_CBC_SHA256
TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA
TLS_NTRU_NSS_WITH_AES_128_CBC_SHA
TLS_NTRU_NSS_WITH_RC4_128_SHA
TLS_PSK_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_NTRU_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_NTRU_NSS_WITH_3DES_EDE_CBC_SHA
TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
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_RSA_PSK_WITH_NULL_SHA256
TLS_RSA_PSK_WITH_AES_128_CBC_SHA
TLS_DH_DSS_WITH_SEED_CBC_SHA
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256
TLS_RSA_PSK_WITH_AES_256_CBC_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_anon_WITH_RC4_128_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_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_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_NTRU_RSA_WITH_AES_256_CBC_SHA
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256
TLS_DH_anon_WITH_AES_256_GCM_SHA384
TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_DH_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_PSK_WITH_NULL_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_DH_ANON_WITH_SEED_CBC_SHA
TLS_ECDHE_PSK_WITH_NULL_SHA
TLS_ECDH_RSA_WITH_AES_256_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_SRP_SHA_DSS_WITH_AES_128_CBC_SHA
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_DHE_PSK_WITH_AES_256_CBC_SHA384
TLS_ECDHE_PSK_WITH_NULL_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Which SSL/TLS Cipher Suites to use?

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

Which SSL/TLS Cipher Suites to use?

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_3DES_EDE_CBC_SHA

TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA

TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_NULL_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_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_PSK_WITH_AES_128_CBC_SHA256

TLS_DH_anon_WITH_AES_128_CBC_SHA256

TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA

TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256

TLS_DH_DSS_WITH_AES_128_GCM_SHA256

TLS_DH_anon_WITH_AES_256_CBC_SHA256

TLS_ECDH_RSA_WITH_NULL_SHA

TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA

TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384

TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA

TLS_RSA_WITH_SEED_CBC_SHA

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_NSS_WITH_AES_256_CBC_SHA

TLS_PSK_WITH_RC4_128_SHA

TLS_DHE_DSS_WITH_SEED_CBC_SHA

TLS_RSA_WITH_HC_128_CBC_SHA

TLS_RSA_PSK_WITH_NULL_SHA

TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA

TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_DSS_WITH_AES_256_CBC_SHA256

TLS_DHE_DSS_WITH_AES_128_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_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA

TLS_DH_DSS_WITH_AES_128_CBC_SHA25

TLS_PSK_WITH_NULL_SHA384

TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA

TLS_RSA_EXPORT1024_WITH_RC2_56_MD5

TLS_KRB5_EXPORT_WITH_RC4_40_MD5

TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256

TLS_DHE_PSK_WITH_RC4_128_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5

TLS_PSK_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS_DHE_PSK_WITH_NULL_SHA384

TLS_RSA_PSK_WITH_RC4_128_SHA

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256

TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA

TLS_RSA_WITH_NULL_SHA256

TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384

SSL_FORTEZZA_KEA_WITH_RC4_128_SHA

SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_DH_anon_WITH_DES_CBC_SHA

TLS_DH_DSS_WITH_AES_128_CBC_SHA

TLS_PSK_WITH_AES_128_CBC_SHA

TLS_ECDH_anon_WITH_NULL_SHA

TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA

TLS_DH_anon_WITH_RC4_128_MD5

TLS_PSK_WITH_NULL_SHA

TLS_DH_RSA_WITH_AES_256_CBC_SHA256

TLS_DH_RSA_WITH_AES_256_GCM_SHA384

TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA

TLS_DH_DSS_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_RABBIT_CBC_SHA

TLS_KRB5_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256

TLS_RSA_WITH_RC4_128_MD5

TLS_NTRU_RSA_WITH_RC4_128_SHA

TLS_DHE_PSK_WITH_NULL_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_DES40_CBC_SHA

TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA

SSL_CK_DES_64_CBC_WITH_MD5

TLS_RSA_WITH_DES_CBC_SHA

TLS_DHE_DSS_WITH_DES_CBC_SHA

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_ECDHE_ECDSA_WITH_RC4_128_SHA

SSL_CK_DES_192_EDE3_CBC_WITH_MD5

TLS_DH_RSA_WITH_DES_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

SSL_CK_RC2_128_CBC_WITH_MD5

TLS_PSK_WITH_AES_256_CBC_SHA384

TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

TLS_RSA_EXPORT_WITH_DES40_CBC_SHA

SSL_FORTEZZA_KEA_WITH_NULL_SHA

TLS_DHE_PSK_WITH_NULL_SHA256

SSL_CK_IDEA_128_CBC_WITH_MD5

SSL_CK_RC4_64_WITH_MD5

TLS_KRB5_WITH_3DES_EDE_CBC_MD5

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

TLS_KRB5_WITH_RC4_128_MD5

TLS_NULL_WITH_NULL_NULL

TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA

TLS_DH_DSS_WITH_DES_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_PSK_WITH_AES_256_CBC_SHA

TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA

TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5

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_RSA_WITH_NULL_SHA

SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA

TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA

TLS_RSA_WITH_NULL_MD5

TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA

TLS_DH_RSA_WITH_AES_128_GCM_SHA256

TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA

SSL_RSA_FIPS_WITH_DES_CBC_SHA

TLS_KRB5_WITH_DES_CBC_MD5

TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

TLS_KRB5_WITH_RC4_128_SHA

TLS_DH_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_PSK_WITH_AES_128_CBC_SHA

TLS_KRB5_EXPORT_WITH_RC4_40_SHA

TLS_KRB5_WITH_IDEA_CBC_SHA

TLS_DHE_DSS_WITH_AES_128_GCM_SHA256

TLS_DHE_RSA_WITH_DES_CBC_SHA

TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA256

TLS_DH_RSA_WITH_AES_128_CBC_SHA

TLS_DH_anon_WITH_AES_128_CBC_SHA

TLS_KRB5_WITH_DES_CBC_SHA

TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA

SSL_CK_RC4_128_WITH_MD5

TLS_RSA_PSK_WITH_AES_128_GCM_SHA256

TLS_PSK_WITH_3DES_EDE_CBC_SHA

TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5

TLS_DH_anon_WITH_AES_256_CBC_SHA

TLS_DHE_DSS_WITH_RC4_128_SHA

SSL_RSA_FIPS_WITH_3DES_EDE_CBC_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_RSA_PSK_WITH_AES_128_CBC_SHA256

TLS_DHE_DSS_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_HC_128_CBC_MD5

TLS_DH_DSS_WITH_AES_256_CBC_SHA256

TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA

TLS_NTRU_NSS_WITH_AES_128_CBC_SHA

TLS_NTRU_NSS_WITH_RC4_128_SHA

TLS_PSK_WITH_AES_128_GCM_SHA256

TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA

TLS_DHE_DSS_WITH_AES_256_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_NTRU_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_SEED_CBC_SHA

TLS_NTRU_NSS_WITH_3DES_EDE_CBC_SHA

TLS_DHE_PSK_WITH_AES_128_GCM_SHA256

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_RSA_PSK_WITH_NULL_SHA256

TLS_RSA_PSK_WITH_AES_128_CBC_SHA

TLS_DH_DSS_WITH_SEED_CBC_SHA

TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256

TLS_RSA_PSK_WITH_AES_256_CBC_SHA384

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDH_anon_WITH_RC4_128_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_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_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_NTRU_RSA_WITH_AES_256_CBC_SHA

TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256

TLS_DH_anon_WITH_AES_256_GCM_SHA384

TLS_DHE_PSK_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_DH_RSA_WITH_SEED_CBC_SHA

TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256

TLS_ECDH_RSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_PSK_WITH_NULL_SHA384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

TLS_DH_ANON_WITH_SEED_CBC_SHA

TLS_ECDHE_PSK_WITH_NULL_SHA

TLS_ECDH_RSA_WITH_AES_256_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_SRP_SHA_DSS_WITH_AES_128_CBC_SHA

TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA

TLS_ECDH_anon_WITH_AES_128_CBC_SHA

TLS_ECDH_anon_WITH_AES_256_CBC_SHA

TLS_DHE_PSK_WITH_AES_256_CBC_SHA384

TLS_ECDHE_PSK_WITH_NULL_SHA256

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Which SSL/TLS Cipher Suites to use?

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_3DES_EDE_CBC_SHA
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA
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_SRP_SHA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA
TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA
TLS_PSK_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
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_3DES_EDE_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_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_NSS_WITH_AES_256_CBC_SHA
TLS_PSK_WITH_RC4_128_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_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_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_DSS_WITH_AES_128_CBC_SHA25
TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_PSK_WITH_RC4_128_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_PSK_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_PSK_WITH_RC4_128_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
SSL_FORTEZZA_KEA_WITH_RC4_128_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DH_anon_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_RSA_WITH_AES_256_CBC_SHA256
TLS_DH_RSA_WITH_AES_256_GCM_SHA384
TLS_DH_DSS_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_RABBIT_CBC_SHA
TLS_KRB5_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
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
SSL_CK_DES_64_CBC_WITH_MD5
TLS_RSA_WITH_DES_CBC_SHA
TLS_DHE_DSS_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
SSL_CK_DES_192_EDE3_CBC_WITH_MD5
TLS_DH_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
SSL_CK_RC2_128_CBC_WITH_MD5
TLS_PSK_WITH_AES_256_CBC_SHA384
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
SSL_CK_IDEA_128_CBC_WITH_MD5
SSL_CK_RC4_64_WITH_MD5
TLS_KRB5_WITH_3DES_EDE_CBC_MD5
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_KRB5_WITH_RC4_128_MD5
TLS_DH_DSS_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_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
SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DH_RSA_WITH_AES_128_GCM_SHA256
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_FIPS_WITH_DES_CBC_SHA
TLS_KRB5_WITH_DES_CBC_MD5
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_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DH_RSA_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_KRB5_WITH_DES_CBC_SHA
TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA
SSL_CK_RC4_128_WITH_MD5
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_SHA
SSL_RSA_FIPS_WITH_3DES_EDE_CBC_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_RSA_PSK_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_HC_128_CBC_MD5
TLS_DH_DSS_WITH_AES_256_CBC_SHA256
TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA
TLS_NTRU_NSS_WITH_AES_128_CBC_SHA
TLS_NTRU_NSS_WITH_RC4_128_SHA
TLS_PSK_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_NTRU_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_NTRU_NSS_WITH_3DES_EDE_CBC_SHA
TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
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_RSA_PSK_WITH_AES_128_CBC_SHA
TLS_DH_DSS_WITH_SEED_CBC_SHA
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256
TLS_RSA_PSK_WITH_AES_256_CBC_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_anon_WITH_RC4_128_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_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_PSK_WITH_RC4_128_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_NTRU_RSA_WITH_AES_256_CBC_SHA
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256
TLS_DH_anon_WITH_AES_256_GCM_SHA384
TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DH_RSA_WITH_SEED_CBC_SHA
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_DH_ANON_WITH_SEED_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_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_SRP_SHA_DSS_WITH_AES_128_CBC_SHA
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_DHE_PSK_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Which SSL/TLS Cipher Suites to use?

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

Which SSL/TLS Cipher Suites to use?

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

Which SSL/TLS Cipher Suites to use?

TLS_ECDHE_ECDSA_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_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_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_SRP_SHA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA
TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA
TLS_PSK_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDH_anon_WITH_3DES_EDE_CBC_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_3DES_EDE_CBC_SHA
TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_SEED_CBC_SHA
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_NSS_WITH_AES_256_CBC_SHA
TLS_PSK_WITH_RC4_128_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_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_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_DSS_WITH_AES_128_CBC_SHA25
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_DSS_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_PSK_WITH_RC4_128_SHA
TLS_PSK_WITH_AES_256_CBC_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
SSL_FORTEZZA_KEA_WITH_RC4_128_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DH_anon_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_RSA_WITH_AES_256_CBC_SHA256
TLS_DH_RSA_WITH_AES_256_GCM_SHA384
TLS_DH_DSS_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_RABBIT_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_KRB5_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
SSL_CK_DES_64_CBC_WITH_MD5
TLS_RSA_WITH_DES_CBC_SHA
TLS_DHE_DSS_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
SSL_CK_DES_192_EDE3_CBC_WITH_MD5
TLS_DH_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
SSL_CK_RC2_128_CBC_WITH_MD5
TLS_PSK_WITH_AES_256_CBC_SHA384
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
SSL_CK_IDEA_128_CBC_WITH_MD5
SSL_CK_RC4_64_WITH_MD5
TLS_KRB5_WITH_3DES_EDE_CBC_MD5
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_KRB5_WITH_RC4_128_MD5
TLS_DH_DSS_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_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
SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DH_RSA_WITH_AES_128_GCM_SHA256
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_FIPS_WITH_DES_CBC_SHA
TLS_KRB5_WITH_DES_CBC_MD5
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_DHE_DSS_WITH_AES_128_GCM_SHA256
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DH_RSA_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_KRB5_WITH_DES_CBC_SHA
TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA
SSL_CK_RC4_128_WITH_MD5
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_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_PSK_WITH_AES_256_GCM_SHA384
TLS_RSA_PSK_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DH_DSS_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_HC_128_CBC_MD5
TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA
TLS_NTRU_NSS_WITH_AES_128_CBC_SHA
TLS_NTRU_NSS_WITH_RC4_128_SHA
TLS_PSK_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_NTRU_RSA_WITH_3DES_EDE_CBC_SHA
TLS_NTRU_NSS_WITH_3DES_EDE_CBC_SHA
TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
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_RSA_PSK_WITH_AES_128_CBC_SHA
TLS_DH_DSS_WITH_SEED_CBC_SHA
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256
TLS_RSA_PSK_WITH_AES_256_CBC_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_anon_WITH_RC4_128_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_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_PSK_WITH_RC4_128_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_NTRU_RSA_WITH_AES_256_CBC_SHA
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256
TLS_DH_anon_WITH_AES_256_GCM_SHA384
TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_DH_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_DH_ANON_WITH_SEED_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_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_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_DHE_PSK_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Which SSL/TLS Cipher Suites to use?

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_PSK_WITH_AES_128_CBC_SHA
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_SRP_SHA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA
TLS_PSK_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_AES_128_CBC_SHA256
TLS_DH_anon_WITH_CAMELLIA_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_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_NSS_WITH_AES_256_CBC_SHA
TLS_PSK_WITH_RC4_128_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_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_DSS_WITH_AES_128_CBC_SHA25
TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_PSK_WITH_RC4_128_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_PSK_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_PSK_WITH_RC4_128_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
SSL_FORTEZZA_KEA_WITH_RC4_128_SHA
TLS_RSA_WITH_AES_128_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_RSA_WITH_AES_256_CBC_SHA256
TLS_DH_RSA_WITH_AES_256_GCM_SHA384
TLS_DH_DSS_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_RABBIT_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_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_SHA
TLS_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_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DH_RSA_WITH_AES_128_CBC_SHA
TLS_DH_anon_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_RSA_PSK_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DH_DSS_WITH_AES_256_CBC_SHA256
TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA
TLS_NTRU_NSS_WITH_AES_128_CBC_SHA
TLS_NTRU_NSS_WITH_RC4_128_SHA
TLS_PSK_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_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_DHE_PSK_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_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_RSA_PSK_WITH_AES_128_CBC_SHA
TLS_DH_DSS_WITH_SEED_CBC_SHA
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256
TLS_RSA_PSK_WITH_AES_256_CBC_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_anon_WITH_RC4_128_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_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_NTRU_RSA_WITH_AES_256_CBC_SHA
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256
TLS_DH_anon_WITH_AES_256_GCM_SHA384
TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_DH_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_DH_ANON_WITH_SEED_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_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_SRP_SHA_DSS_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA
TLS_DHE_PSK_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Which SSL/TLS Cipher Suites to use?

RC4

- Stream cipher by Rivest from 1987
- Multiple attacks, also against its use in TLS (AlFardan, Bernstein, Paterson, Poettering, Schuldt, 2013).
- Appelbaum, 2013: "RC4 is broken in real time by the #NSA"

Which SSL/TLS Cipher Suites to use?

RC4

- Stream cipher by Rivest from 1987
- Multiple attacks, also against its use in TLS (AlFardan, Bernstein, Paterson, Poettering, Schuldt, 2013).
- Appelbaum, 2013: “RC4 is broken in real time by the #NSA”

CBC Mode

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

Which SSL/TLS Cipher Suites to use?

RC4

- Stream cipher by Rivest from 1987
- Multiple attacks, also against its use in TLS (AlFardan, Bernstein, Paterson, Poettering, Schuldt, 2013).
- Appelbaum, 2013: “RC4 is broken in real time by the #NSA”

CBC Mode

- 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

Which SSL/TLS Cipher Suites to use?

RC4

- Stream cipher by Rivest from 1987
- Multiple attacks, also against its use in TLS (AlFardan, Bernstein, Paterson, Poettering, Schuldt, 2013).
- Appelbaum, 2013: "RC4 is broken in real time by the #NSA"

CBC Mode

- 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)

Which SSL/TLS Cipher Suites to use?

RC4

- Stream cipher by Rivest from 1987
- Multiple attacks, also against its use in TLS (AlFardan, Bernstein, Paterson, Poettering, Schuldt, 2013).
- Appelbaum, 2013: "RC4 is broken in real time by the #NSA"

CBC Mode

- 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)

Which SSL/TLS Cipher Suites to use?

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_PSK_WITH_AES_128_CBC_SHA

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_SRP_SHA_WITH_AES_256_CBC_SHA

TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256

TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA

TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA

TLS_PSK_WITH_AES_128_CBC_SHA256

TLS_DH_anon_WITH_AES_128_CBC_SHA256

TLS_DH_anon_WITH_CAMELLIA_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_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_NSS_WITH_AES_256_CBC_SHA

TLS_PSK_WITH_RC4_128_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_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA

TLS_DH_DSS_WITH_AES_128_CBC_SHA25

TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA

TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256

TLS_DHE_PSK_WITH_RC4_128_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_PSK_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS_RSA_PSK_WITH_RC4_128_SHA

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256

TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384

SSL_FORTEZZA_KEA_WITH_RC4_128_SHA

TLS_RSA_WITH_AES_128_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_RSA_WITH_AES_256_CBC_SHA256

TLS_DH_RSA_WITH_AES_256_GCM_SHA384

TLS_DH_DSS_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_RABBIT_CBC_SHA

TLS_DHE_RSA_WITH_CAMELLIA_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_SHA

TLS_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_DH_anon_WITH_CAMELLIA_256_CBC_SHA256

TLS_DHE_DSS_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA256

TLS_DH_RSA_WITH_AES_128_CBC_SHA

TLS_DH_anon_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_RSA_PSK_WITH_AES_128_CBC_SHA256

TLS_DHE_DSS_WITH_AES_128_CBC_SHA

TLS_DH_DSS_WITH_AES_256_CBC_SHA256

TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA

TLS_NTRU_NSS_WITH_AES_128_CBC_SHA

TLS_NTRU_NSS_WITH_RC4_128_SHA

TLS_PSK_WITH_AES_128_GCM_SHA256

TLS_DHE_RSA_WITH_CAMELLIA_256_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_DHE_PSK_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_128_CBC_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_RSA_PSK_WITH_AES_128_CBC_SHA

TLS_DH_DSS_WITH_SEED_CBC_SHA

TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256

TLS_RSA_PSK_WITH_AES_256_CBC_SHA384

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDH_anon_WITH_RC4_128_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_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_NTRU_RSA_WITH_AES_256_CBC_SHA

TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256

TLS_DH_anon_WITH_AES_256_GCM_SHA384

TLS_DHE_PSK_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_DH_RSA_WITH_SEED_CBC_SHA

TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256

TLS_ECDH_RSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

TLS_DH_ANON_WITH_SEED_CBC_SHA

TLS_ECDH_RSA_WITH_AES_256_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_SRP_SHA_DSS_WITH_AES_128_CBC_SHA

TLS_ECDH_anon_WITH_AES_128_CBC_SHA

TLS_ECDH_anon_WITH_AES_256_CBC_SHA

TLS_DHE_PSK_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Which SSL/TLS Cipher Suites to use?

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_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_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

Which SSL/TLS Cipher Suites to use?

anonymous

- “anonymous” ciphers don’t use certificates
- Susceptible to a MitM attack

Which SSL/TLS Cipher Suites to use?

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

Which SSL/TLS Cipher Suites to use?

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_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_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

Which SSL/TLS Cipher Suites to use?

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_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_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

Which SSL/TLS Cipher Suites to use?

Use ephemeral key exchange!

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

Which SSL/TLS Cipher Suites to use?

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`

Which SSL/TLS Cipher Suites to use?

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_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_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

Which SSL/TLS Cipher Suites to use?

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

Which SSL/TLS Cipher Suites to use?

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

Which SSL/TLS Cipher Suites to use?

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

Which SSL/TLS Cipher Suites to use?

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

Which SSL/TLS Cipher Suites to use?

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?

Better algorithms in the future?

- Biggest problem: no fully satisfactory symmetric authenticated encryption
- Current IETF draft by Langley: ChaCha20 and Poly1305 for TLS: https://tools.ietf.org/html/draft-agl-tls-chacha20poly1305-01
- ChaCha20 is a state-of-the art stream cipher
- Poly1305 is a state-of-the art authenticator
- Both designed by Bernstein
- Both very efficient in software

Who do you trust?

- 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

Who do you trust?

- 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

Who do you trust?

- 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/

Who do you trust?

- 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/

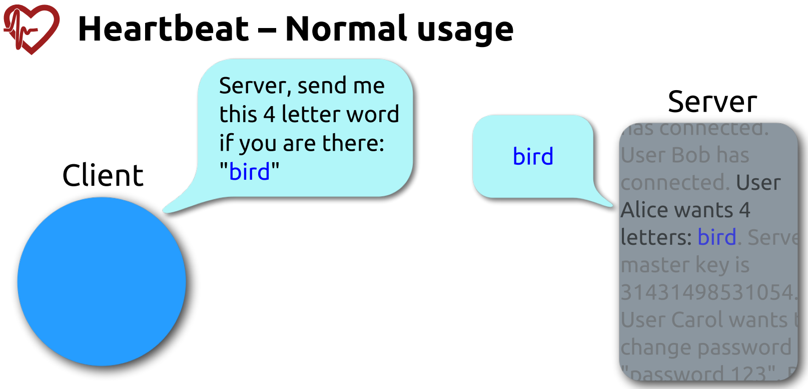
OpenSSL Heartbleed Bug

Bug in the implementation of the Heartbeat Extension (RFC 6520):

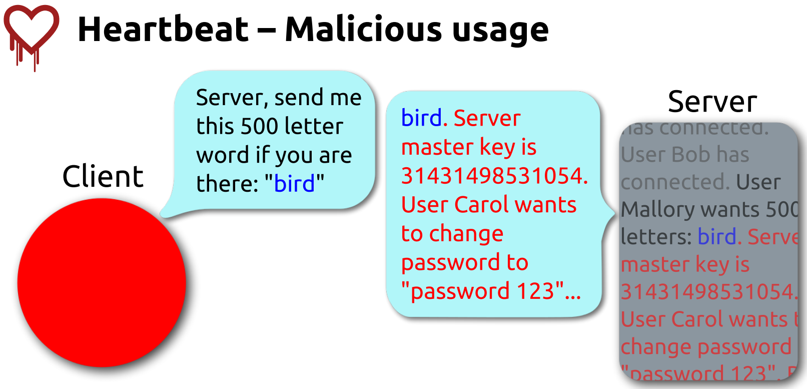
```
   struct {
  HeartbeatMessageType type;
  uint16 payload_length;
  opaque payload[HeartbeatMessage.payload_length];
  opaque padding[padding_length];
} HeartbeatMessage;

[...]
When a HeartbeatRequest message is received [...],
the receiver MUST send a corresponding HeartbeatResponse
message carrying an exact copy of the payload of the received
HeartbeatRequest.
```

OpenSSL failed to check actual length of payload data.

OpenSSL Heartbleed Bug


Heartbeat – Normal usage
Client
Server, send me this 4 letter word if you are there: "bird"
bird
Server
has connected. User Bob has connected. User Alice wants 4 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P

OpenSSL Heartbleed Bug



Heartbeat – Malicious usage

Client

Server, send me this 500 letter word if you are there: "bird"

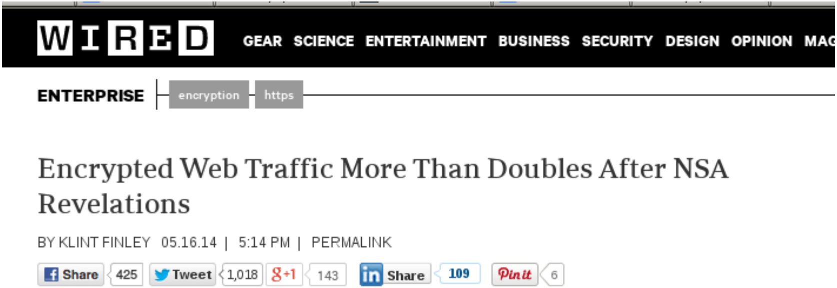
bird. Server master key is 31431498531054. User Carol wants to change password to "password 123"...

Server

has connected. User Bob has connected. User Mallory wants 500 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P

How much web traffic is encrypted?

How much web traffic is encrypted?



WIRED
GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION MAG
ENTERPRISE
encryption
https

Encrypted Web Traffic More Than Doubles After NSA Revelations

BY KLINT FINLEY 05.16.14 | 5:14 PM | PERMALINK

How much web traffic is encrypted?

From the article:

“Early last year–before the Snowden revelations–encrypted traffic accounted for 2.29 percent of all peak hour traffic in North America, according to Sandvine’s report. Now, it spans 3.8 percent. But that’s a small jump compared to other parts of the world. In Europe, encrypted traffic went from 1.47 percent to 6.10 percent, and in Latin America, it increased from 1.8 percent to 10.37 percent.”

—Klint Finley on wired.com, May 16, 2014.