CE0973a - Issues in Network Security
3: Final SSL, Firewalling

James A Sutherland

Abertay University

Monday, 25th January 2016

Security Standards

ISO 27001, 27017, 27018 – security, cloud security, PII
`http://www.iso27001security.com/html/27017.html`
Amazon and co – aimed at organisations of any size, though.

- Management
- Support
- Operation
- Evaluation
- Improvement

TCP recap

Standard Ethernet: frames of up to 1,500 bytes
Jumbo Frames, can be c 9k
IP packet: 16 bit size, so up to 65,535 bytes, but best to use 1 frame.
TCP: Unlimited streams in IP packets.
4 (or 10) initially, so roughly 6k (or 15).
Initial Congestion Window: initcwnd

TCP performance issues

Problem for small assets, e.g. web icons
Mitigations: keepalive, pipelining, HTTP2, CSS icons
Also ACK bottleneck
Early cable modems & satellite links - fast half duplex link, dialup for return path.
ACKs could be bottleneck – one (small) packet per (large) incoming, pre-SACK
Also DOCSIS issue, each packet required obtaining the send token, regardless of size – fixed by packet aggregation in later DOCSIS

SSL recap

- Client asks for SSL vN with www.example.com
- Server replies with version, algorithm, certificate for www.example.com, possibly also chain and OCSP status
- Certificate = name(s), public key, signature of issuer plus some metadata (address, valid dates, purpose etc)
- Both do fancy maths, producing a set of symmetric keys for both signing and encrypting the data in each direction
- SSL also uses records (like big packets) over TCP - signs and encrypts each one

SSL parameters

Total of FOUR keys and THREE algorithms agreed during handshake:

- public key crypto: RSA, ECDSA etc
- secret key crypto: AES256, AES128, 3DES etc
- hashing: SHA256, SHA1, MD5

Session keys then thrown away afterwards - usually can't be deduced even with the private key: Forward Secrecy

Other SSL safeguards

Also packs various randomness in to guard against replays etc
"Nonces" (Numbers used ONCE) – v important in crypto
Sequence numbers to guard against resequencing, deletion etc
Also hashing of handshake stages, to guard against downgrade attack (intercept, "I only support DES with MD5", export grade) – POODLE attack

SSL messages

Message structure:

type	8 bits	handshake=22 change cipher=20 alert=21 (close or error) data=23
version	16 bit	SSLv2=0x0002 SSLv3=0x0300 TLSv1=0x0301
length	16 bit	TLSv1 RFC2246: max 16383 ($2^{14} - 1$)
data	variable	
MAC	variable	Signature on the preceding data

SSL notes and wrapup

IE and IIS ignore the maximum record length.
SSL supposed to shut down cleanly before TCP close. One browser screws that up, guess which ...
Further reading:
`http://www.cisco.com/c/en/us/support/docs/security-vpn/secure-socket-layer-ssl/116181-technote-product-00.html`
Other precautions: certificate transparency, cert pinning, public key pinning, HSTS, CA pinning

Firewalls

- Stateful v stateless
- Block/allow based on rules: must have bit N set, must not be port X, no more than Y packets per sec
- Packet filter vs application gateway
- "No incoming connections" (typical home setup)
- "No incoming, except to the server" (typical SME with DMZ)
- SYN flood

Week 3 labs

Week 3 labs:

- Create own CA, install cert on client.
- Build a phishing site in Apache SSL.
- Check which sites it works and doesn't work on.
- Also establish IPtables rules to block non-SSL web access and inbound SSH. Block DNS, see what happens. Restore it.