Bettercrypto - Applied Crypto Hardening for Sysadmins

Attacks

Aaron Zauner
azet@azet.org

BetterCrypto.org

Hack.lu - 21/10/2014

Internet Dark Ages

- SSLv1 engineered at Netscape, never released to the public
- Kipp Hickman of Netscape introduces SSLv2 as an IETF draft back in 1995:

  ```
  The SSL Protocol is designed to provide privacy
  between two communicating applications (a client
  and a server).  Second, the protocol is designed
  to authenticate the server, and optionally the
  client.  [...]
  ```

`http://tools.ietf.org/html/draft-hickman-netscape-ssl-00`

Internet Dark Ages

- SSLv2 was fundamentally broken and badly designed. Basically full loss of Confidentiallity and integrity of on-wire data thus susceptible to MITM attacks, see: `http://osvdb.org/56387`
- CipherSpec is sent in the clear
- Size of Block-cipher padding is sent in the clear

Internet Dark Ages

- SSLv3 was introduced in 1996 by Paul Kocher, Phil Karlton and Alan Freier, utilizing an algoritm by Taher ElGamal, a known cryptographer and Chief Scientist at Netscape at the time: `https://tools.ietf.org/html/rfc6101`

Internet Dark Ages

On a side note; back then the choice algorithms was limited and export ciphers (low security) common as recommended by NSA and mandated by US law. Google: “Bernstein vs. United States”

- encryption algorithms (Confidentiality): NULL, FORTEZZA-CBC (NSA), IDEA-CBC, RC2-CBC-40 (40bit security), RC4-128, DES40-CBC (40bit security), DES-CBC (56bit security), Triple-DES-EDE-CBC
- hash functions (integrity): NULL, MD5 and SHA

Internet Dark Ages

David Wagner and Bruce Schneier publish a paper entitled "Analysis of the SSL 3.0 protocol":

- Keyexchange algorithm rollback
- Protocol fallback to SSLv2
- Protocol leaks known plaintexts – may be used in cryptanalysis
- Replay attacks on Anonymous DH (don't use it anyway!)

`https://www.schneier.com/paper-ssl.pdf`

TLS appears

1999. The SSL protocol is renamed to TLS (version 1) with little improvements over SSLv3. The spec. is almost identical.

- Diffie-Hellman, DSS and Triple-DES are now required by implementors
- most SSLv3 security issues are still present in TLS 1.0

(RFC2246)

TLS gets padding attacks

2002. Vaudenay publishes a paper entitled “Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS...”

- Side-channel attack on CBC mode padding
- valid/invalid padding causes different reactions
- can be used to influence decryption operations
- introduces “padding oracle attacks” in SSL

`http://www.iacr.org/cryptodb/archive/2002/EUROCRYPT/2850/2850.pdf`

TLS gets extended

2003. TLS extensions get specified in RFC3546.

- General: Extended Handshake, ClientHello and ServerHello
- Server Name Indication (SNI) for virtual hosting
  (SNI leaks metadata!)
- Certificate Status Request (CSR) support via OCSP
- (...)

TLS gets timing attacks

2003. Brumley and Boneh publish a paper entitled “Remote timing attacks are practical”.

Timing attack on RSA in SSL/TLS implementations (OpenSSL):

- Send specially crafted ClientKeyExchange message
- Mesure time between ClienyKeyExchange and Alert response
- do a bit of statistics
- retrieve Private Key

`http://dl.acm.org/citation.cfm?id=1251354`

TLS gets padding oracle password retrieval

2003. Canvel, Hiltgen, Vaudenay, Vuagnoux publish “Password Interception in a SSL/TLS Channel”.

Extend earlier work of Vaudenay and successfully intercept IMAP passwords in TLS channels.

`http://www.iacr.org/cryptodb/archive/2003/CRYPTO/1069/1069.pdf`

TLS gets chosen plaintext attacks

2004 & 2006. Bard demonstrates Chosen-Plaintext Attacks against SSL and TLS1.0

Attack on CBC:

- CBC exchanges an Initialization Vector (IV) during Handshake
- these IVs turn out to be predictable
- PINs and Passwords can be decrypted
- VPNs/Proxies can also be used to accomplish this task

`https://eprint.iacr.org/2004/111`
`https://eprint.iacr.org/2006/136`

TLS gets updated

2006. A new TLS protocol version is standardized: TLS 1.1

- EXPORT ciphers removed
- Session resumption
- Protection against the CBC attacks by Bard
- IANA TLS parameters standardized
- (...)

(RFC4346)

TLS gets modern crypto

2008. A new TLS protocol version is standardized: TLS 1.2

- MD5/SHA1 removed as pseudorandom function (PRF)
- configurable PRFs in ciphersuites (e.g. SHA256)
- Authenticated encryption: CCM, GCM
- AES ciphersuites
- (...)

(RFC5246)

Rouge CA Certificates

2008. Sotirov, Stevens, Appelbaum, Lenstra, Molnar, Osvik and de Weger present a paper based on earlier work by Lenstra et al. at 25c3 entitled “MD5 considered harmful today”

- MD5 Hash-collision of a CA Certificate
- Create colliding (rouge) CA Certificates
- Generate any Certificate for MITM you want

`http://www.win.tue.nl/hashclash/rogue-ca/`
`https://www.youtube.com/watch?v=PQcWyDgGUVg`

sslstrip

2009. Moxie Marlinspike releases *sslstrip* at BlackHat DC 2009.

- Client connects to server
- Attacker intercepts session via MITM
- Attacker sends HTTP 301 (moved permanently)
- Attacker forwards requests to/from server via SSL/TLS
- Client receives data via unencrypted channel
- Attacker reads plaintext

`http://www.thoughtcrime.org/software/sslstrip`
`http://vimeo.com/50018478`

Null-prefix attacks against Certificates

2009. Moxie Marlinspike publishes “Null prefix Attacks against SSL/TLS Certificates”.

- Specially crafted domain strings trick CA checking
- null-terminate stuff in a domain name
- ex.: `www.paypal.com\0.thoughtcrime.org` is valid
- ex.: `*\0.thoughtcrime.org` is valid
- CA ignores prefix
- Client does not -> Certificate valid for prefix

Moxie updated his *sslsniff* project to carry out this attack.

`http://www.thoughtcrime.org/papers/null-prefix-attacks.pdf`
`http://thoughtcrime.org/software/sslsniff`

SSLv2 Forbidden

2011. IETF publishes and standardized a RFC to prohibit negotiation and thus compatibility of SSLv2 in TLS1.0–1.2 entirely.

`https://tools.ietf.org/html/rfc6176`

Comodo

2011. Comodo CA: Attacker issues 9 certificates via reseller account for popular domains (google.com, yahoo.com, live.com, skype.com [...])

`https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html`

BEAST

2011. Doung and Rizzo publish the BEAST attack at ekoparty and demo a live attack on PayPal. Based on Bards earlier work on predictable IVs in CBC:

- Phishing gets victim to visit a certain website
- Script on said website makes request to genuine site
- Attacker records encrypted cookie information
- Tries to guess session-cookie with known CBC attack

Same Origin Policy (SOP) forbids this attack in client software. If SOP can be bypassed (as shown by the authors with Java's SOP) this attack is still practical.

`http://vnhacker.blogspot.co.at/2011/09/beast.html`

Trustwave

2012. Trustwave CA: Trustwave sells subordinate CAs to big corporations to be used for Deep Packet Inspection.

A sub-CA can issue and fake any certificate for MITM attacks.

http://blog.spiderlabs.com/2012/02/clarifying-the-trustwave-ca-policy-update.html
http://arstechnica.com/business/2012/02/critics-slam-ssl-authority-for-minting-cert-used-to-impersonate-sites/

DigiNotar

2012. DigiNotar CA: Attackers compromise DigiNotar in it's entirety.

- attackers generate tons of certificates
- Google Chromes certificate store detects mismatches
- DigiNotar acknowledges breach
- DigiNotar files for bankrupcy
- FOX-IT never gets paid for the investigation

https://en.wikipedia.org/wiki/DigiNotar
http://cryptome.org/0005/diginotar-insec.pdf
http://nakedsecurity.sophos.com/2011/09/05/
operation-black-tulip-fox-its-report-on-the-diginotar-breach

Certificate validation in non-browser software

2012. Georgiev, Iyengar, Jana, Anubhai, Boneh and Shmatikov publish a paper entitled “The most dangerous code in the world: validating SSL certificates in non-browser software”

Certificate validation vulnerabilities in:

- OpenSSL
- GnuTLS
- JSSE
- EC2 Java libraries & Amazon SDKs
- PayPal SDKs
- eCommerce/WebShop software
- ..cURL, PHP, Python, tons of Java middleware

`https://crypto.stanford.edu/~dabo/pubs/abstracts/ssl-client-bugs.html`

CRIME

2012. Doung and Rizzo publish an attack against TLS Compression and SPDY titled CRIME.

- MITM attacker sees length of compressed ciphertext
- compression has direct affect on the length
- attacker makes client compress/encrypt data (or uses known data) with secret data
- attacker compares
- correct guesses yield shorter messages due to compression
- repeat until done

This is only feasible for small amounts of data, e.g. session strings, cookies and so forth.

`https://isecpartners.com/blog/2012/september/details-on-the-crime-attack.aspx`

TIME

2013. Be'ery and Shulman present TIME at BlackHat Europe. Extend on the CRIME Attack:

- Attacker generates HTTP requests (XSS, injection,..)
- Attacker exploits SOP design flaw and measures RTT differences
- determines correct or failed guesses by SOP timing leak

https://media.blackhat.com/eu-13/briefings/Beery/bh-eu-13-a-perfect-crime-beery-wp.pdf
https://www.youtube.com/watch?v=rTIpFfTp3-w

Lucky13

2013. AlFardan and Paterson present a novel attack against CBC for TLS and DTLS based on timing analysis.

- Attacker intercepts and modifies a message including padding
- Attacker tempers with the padding of the message
- MAC computation takes longer during decryption process
- Attacker repeats and measures
- Attacker performs padding oracle attack described earlier
- (Extremely latency sensitive attack)

`http://www.isg.rhul.ac.uk/tls/Lucky13.html`
`http://www.isg.rhul.ac.uk/tls/TLStiming.pdf`

RC4 Biases

2013. AlFardan, Bernstein, Paterson, Poettering and Schuldt publish a generic attack on the RC4 cipher for TLS and WPA.

- Statistical biases in the first 257 bytes of ciphertext
- Recovery of the first 200 bytes after 2^{28} to 2^{32} encryption operations of the same plaintext
- A broadcast attack: mounted on unique keys
- May also be mounted with a single key with repeating target plaintexts
- Only feasible for large amounts of data and very time consuming

`http://www.isg.rhul.ac.uk/tls`
`http://www.isg.rhul.ac.uk/tls/RC4biases.pdf`

NIST curves

2013 & 2014. Daniel J. Bernstein and Tanja Lange voice concern about the NIST Elliptic Cuves that are widely implemented and used in TLS for ECDH and ECDSA

- NIST curves defined on recommendations by NSA's Jerry Solinas
- Unclear why these curves and their parameters were chosen
- NIST cites efficiency: more efficient and secure curves available
- Possible mathematical backdoor through previous analysis and carefully chosen and unexplained parameters
- Start SafeCurves project (ongoing)

http://www.hyperelliptic.org/tanja/vortraege/20130531.pdf
http://cr.yp.to/talks/2013.09.16/slides-djb-20130916-a4.pdf
http://safecurves.cr.yp.to
https://archive.org/details/ShmooCon2014_SafeCurves

BREACH

2013. Gluck, Harris and Prado demonstrate yet another attack based on CRIME at BlackHat USA.

Very similar to CRIME but the attack works based on information leaks from HTTP compression instead of TLS compression.

`http://breachattack.com`
`https://www.youtube.com/watch?v=CoNKarq1IYA`

Unused Certificates in Truststores

2014. Perl, Fahl, Smith publish a paper entitled “You Won’t Be Needing These Any More: On Removing Unused Certificates From Trust Stores”

- Compared 48 mio. HTTP certificates
- 140 CA Certificates are unused in all major trust stores
- Of 426 trusted root certificates only 66% are even used

`http://fc14.ifca.ai/papers/fc14_submission_100.pdf`

Triple Handshakes Considered Harmful

2014. Bhargavan, Delignat-Lavaud, Pironti, Langley and Ray present an attack one day before the IETF'89 meeting in London.

- Limited to client-certificate authentication with renegotiation
- MITM attack on renegotiation with a three-way handshake
- Variations of the attack also discussed on their website
- Can't possibly fit this into one slide, homework: understand the attack by reading their excellent description on the website

`https://secure-resumption.com`
`https://secure-resumption.com/IETF-triple-handshakes.pdf`

Frankencerts

2014. Brubaker, Jana, Ray, Khurshid and Shmatikovy publish a paper entitled “Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations”

- Fuzzing of X.509 related code in all major implementations shows serious weaknesses in certificate validation and handling
- OpenSSL, NSS, GnuTLS, MatrixSSL, PolarSSL, CyaSSL, cyptlib [...]

`https://www.cs.utexas.edu/~shmat/shmat_oak14.pdf`
`https://github.com/sumanj/frankencert`

Heartbleed

2014. Heartbleed is independently discovered by Codenomicon and a Google Security engineer.

Faulty implementation in OpenSSL of the TLS Heartbleed extension leaks memory content over the wire. This has been all over the media and discussed in detail all over the internet. People have successfully extracted sensitive information (password files et cetera) from victim memory.

I wrote an nmap plugin to scan for Heartbleed:
`https://github.com/azet/nmap-heartbleed`

`http://heartbleed.com`

Virtual Host Confusion

2014. At BlackHat Delignat-Lavaud presents an attack based on SSLv3 downgrade and sharing of session caches

- Attacker forces downgrade to SSLv3
- For SSLv3: larger deployments share session caches
- attacker exploits a server vulnerability where session caches are reused
- attacker requests different subdomain with SSLv3 using the same session
- vulnerable server will allow connection w/o authentication
- www.company.com vs git.company.com

`https://bh.ht.vc`

POODLE

2014. POODLE: Padding Oracle On Downgraded Legacy Encryption – OpenSSL/Google

- MITM attacker downgrades to SSLv3 (once again)
- attacker does block duplication
- takes on average 256 requests to decrypt 1 byte (!)
- disabling SSLv3 or using the FALLBACK_SCSV TLS extension (draft) mitigates this issue entirely

`https://www.openssl.org/~bodo/ssl-poodle.pdf`

Implementation Issues

There are tons of other issues with TLS stacks and software implementations that have not been discussed.

OpenSSL alone published 24 security advisories in 2014 until today.

- Apple's GOTO fail
- GnuTLS GOTO fail
- various GnuTLS vulnerabilities
- wrong use of OpenSSL API in server and client software

...
Clearly; a lot of people current have their eyes on this very topic.

Implementation Issues

For this crowd: It's up to you to find them and improve existing implementations, protocols and standards.