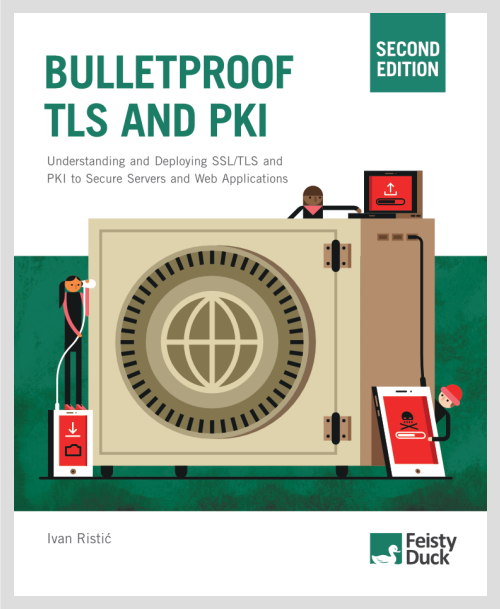
Feisty Duck



SSL/TLS and PKI History

A comprehensive history of the most important events that shaped the SSL/TLS and PKI ecosystem. Based on Bulletproof TLS and PKI, by Ivan Ristić. Tweet

Last updated in February 2022.

1994

SSL v2

Netscape develops SSL v2, an encryption protocol designed to support the Web as a hot new commerce platform. This first secure protocol version shipped in Netscape Navigator 1.1 in March 1995.

Keysight, EX-1032
Page 1

Feisty Duck

1995

PCT v1.0

Microsoft releases the first version of its PCT (Private Communication Technology) protocol, designed to complete SSL. PCT was backward compatible with SSLv2, but fixed its biggest security issues. Ultimately, however, PCT never gained traction outside Microsoft products.

October 1995

SSL v3

SSL v2 is shot down because of serious security issues. Consequently, Netscape scrambles to release SSLv3. This protocol seems good enough for now and the golden era of the Web begins. The specification was eventually published as RFC 6101.

November 1995

1999

TLS v1.0

In 1996, an IETF working group is formed to standardize SSL. Even though the resulting protocol is almost identical to SSL v3, the process takes 3 years. TLS v1.0 is published as RFC 2246. Microsoft forces the change of protocol name to Transport Layer Security (TLS), creating a confusion that continues to this day.

January 1999

Feisty Duck

Fraudulent Microsoft certificates

Someone calls VeriSign claiming to be from Microsoft, pays $400, and gets away with two code-signing certificates. The certificates have no special powers, but the owner name is misleading and potentially dangerous.

January 2001

2006

TLS v1.1

A new version of the TLS protocol is released as RFC 4346. This version addresses the BEAST attack, but it will be 5 years before the world realizes.

April 2006

2007

Extended Validation Certificates

In the early days, CAs are strict about identify verification before certificate issuance. Eventually, some CAs realise that they can get away with less work and domain-validated (DV) certificates are born. To restore the balance, Extended Validation (EV) certificates are designed as a way of guaranteeing a connection between a domain name and a real-life business entity.

June 2007

Feisty Duck

Debian RNG Flaw

It is discovered that a catastrophic programming error had been introduced to Debian in September 2006, becoming part of the official release in April 2007. All private keys generated on vulnerable systems were insecure.

May 2008

Misissued certificate for login.live.com

Mike Zusman realises he can obtain a certificate for live.com because he has access to the "sslcertificates" mailbox on the same domain name. Thawte is happy to provide one. Baseline Requirements will later standardise which email aliases can be used for certificate issuance.

July 2008

TLS v1.2

A new version of TLS is released as RFC 5246, although hardly anyone notices. A major new feature in this version is authenticated (AEAD) encryption, which removes the need for streaming and block ciphers (and thus the inherently vulnerable CBC mode).

August 2008

StartCom misissued certificates

Continuing with his probing of CA security, Mike Zusman finds a flaw on StartCom's web site that allows him to bypass owner validation before certificate issuance. He is caught only after requesting a certificates for high-profile paypal.com and verisign.com domain names.

December 2008

Keysight, EX-1032
Page 4

Feisty Duck

certificates without verifying domain ownership. He gets a certificate for mozilla.org.

December 2008

Rogue CA: MD5 Considered Harmful Today

A group of researchers led by Alex Sotirov and Marc Stevens exploit MD5 weaknesses to trick RapidSSL into effectively giving them their own CA certificate, which they could use to issue certificates for any web site in the world. They backdate the root certificate to prevent abuse. MD5 is promptly retired. Full collisions in MD5 were discovered several years earlier, in 2004, but most the world ignored the finding, eventually prompting the researchers to take action.

December 2008

2009

SSL Labs

SSL Labs launches to build better tools for secure server assessment and research how SSL/TLS and PKI are used in practice.

July 2009

Insecure renegotiation

Marsh Ray discovers that, via renegotiation, one TCP connection can be used for two separate TLS channels. Critically, from the server perspective, there's only one data stream. Abuses are possible when one stream belongs to the user and another stream belongs to the victim.

August 2009

Keysight, EX-1032
Page 5

communication and tricking end users into believing they are safe.

August 2009

NUL byte attacks

At the Black Hat conference in the US, Dan Kaminsky and Moxie Marlinspike independently demonstrate silent MITM attacks made possible by incorrect handling of the NUL byte in the major SSL/TLS stacks.

August 2009

2010

HSTS preloading

Chrome begins to preload HSTS information for some important web sites. For the sites on the list, even the first connection is secure. Preloading is eventually open to everyone and semi-automated.

May 2010

SSL Labs: State of SSL

For the first time, a large-scale analysis of SSL/TLS configuration (and some PKI) is published at the Black Hat conference in the US.

August 2010

Feisty Duck

focus on PKI. These two efforts lead to an era of continuous scanning and analysis of public systems.

August 2010

SPDY

Google starts to use SPDY, a new multiplexing protocol designed to be more efficient than HTTP. Crucially, SPDY always encrypts traffic.

September 2010

False Start

Google starts to use False Start, a new technique that speeds up TLS handshake by allowing clients to send application data before the handshake is fully authenticated.

September 2010

Firesheep

Although it's always been known that plaintext communication is inherently insecure; a Firefox add-on called Firesheep captures the public's imagination after making sidejacking trivially easy. The tool is used for high-profile demonstrations, leading to many companies adopting encryption by default.

October 2010

2011

HTTPS servers supported this obsolete protocol version in 2011.

March 2011

Comodo reseller breaches

Nine fraudulent certificates for seven high-profile domain names are obtained by someone calling themselves ComodoHacker. The attack was detected quickly and the certificates revoked within hours.

March 2011

BEAST

The BEAST attack is released to exploit predictable IVs in TLS 1.0. Even though this problem had been fixed in TLS 1.1 released in 2006 and TLS 1.2 in 2008, no one actually uses these newer protocol versions. Browsers will take about 2 more years to deploy TLS 1.2 and servers many years longer. We have no choice but to rely on browser counter-measures in the meantime. BEAST is the first attack to show how rich browser functionality can be abused to attack cryptography from multiple vantage points. Many similar attacks will follow.

June 2011

DigiNotar

A little-known Dutch CA spectacularly implodes after ComodoHacker gains access to all their systems and issues hundreds of fraudulent certificates. DigiNotar tries to cover up, but the incident is discovered when Chrome's public key pinning runs into a fraudulent Gmail certificate. This event leads to widespread unhappiness and attempts to design better approaches to public trust.

August 2011

Keysight, EX-1032
Page 8

based on the concept of notaries. Although the project is promising, it's abandoned after browsers show little interest in it.

August 2011

Public key pinning

Google begins to use public key pinning in Chrome to verify identity of their own properties. In the following years, this mechanism successfully discovers a number of misissued certificates.

August 2011

Google deploys forward secrecy

In a major improvement, Google deploys forward secrecy, making sure private key compromises can't be used to retroactively uncover captured encrypted traffic.

November 2011

2012

Insufficient Entropy on Embedded Devices

Researchers study the quality of private keys on the public Internet and discover that about 0.5% RSA keys and 1% DSA keys can be compromised due to insufficient entropy at the time of creation. Mostly embedded devices affected.

February 2012

Feisty Duck

decides to get rid of the checks altogether. Other browser vendors eventually follow. The net effect is that it's now virtually impossible to revoke certificates. Although vendors develop their own proprietary revocation mechanisms, they can use them only for a small number of high-profile certificates.

February 2012

HTTP/2 call for proposals

After the success with SPDY there is a critical mass of developers interested in working on the next revision of the HTTP protocol. A period of intense debate and discussion begins.

March 2012

SSL Pulse

SSL Labs launches SSL Pulse in order to perform automated monthly scans and reporting on about 150,000 most visited web sites.

April 2012

Flame

The Iranian CERT discloses the existence of Flame, a malware used in targeted cyber attacks against Iran. Flame is possibly the first cyberweapon that could have operated as early as 2007. In a stunning turn of events, it transpired that Flame exploited an MD5 collision of its own to obtain a fraudulent CA certificate.

May 2012

Baseline requirements

July 2012

Microsoft blocks RSA keys below 1024 bits

As CPU power continues to increase, low-strength private keys are coming under threat. Microsoft updated Windows to start blocking RSA keys weaker than 1024 bits.

August 2012

DANE TLSA

DNS-Based Authentication of Named Entities (DANE)—published as RFC 6698—offers the option to use the DNSSEC infrastructure to store and sign keys and certificates that are used by TLS.

August 2012

CRIME

Duong and Rizzo strike again with a working exploit against TLS compression, just when some browsers begin to support it. The offending functionality is quickly rolled back.

September 2012

HTTP Strict Transport Security

Four years after Jackson and Barth proposed the idea in the form of ForceHTTPS, HSTS is released as a standard in RFC 6797. With HSTS web sites can indicate that they require encryption even if plaintext access is requested for whatever version. Another important feature of HSTS is that it doesn't allow clicking through certificate warning errors. It's finally possible to deploy web site encryption in the way we were supposed to from the beginning.

November 2012

Feisty Duck

Content Security Policy

A new browser technology is released, predominantly to address Cross-Site Scripting (XSS) vulnerabilities which are out of control. However, a very useful feature of Content Security Policy (CSP) is the ability for web sites to control where page elements are loaded from. As a result, it's now possible to prevent third-party mixed content (plaintext and encrypted resources within the same page).

November 2012

ICSI Certificate Notary

International Computer Science Institute (ICSI) launches a certificate notary and starts to monitor and report on encrypted traffic on several large networks.

December 2012

TurkTrust misissued certificate

Chrome's public key pinning defences catch a misissued certificate for one of their properties. It later transpired that TurkTrust had mistakenly given two CA certificates to end users, a problem that remained undetected for 15 months.

December 2012

2013

Lucky 13

AlFardan and Paterson publish Lucky 13, their attack on CBC suites. In TLS, block encryption is designed to authenticate plaintext (rather than ciphertext), which creates an opportunity for the attacker to execute padding oracle attacks.

Keysight, EX-1032
Page 12

Feisty Duck

RC4 biases

New attacks against RC4 are discovered. Previously, it was thought that RC4 weaknesses don't affect TLS much, but that was shown to be wrong. This research marks the death of RC4, although it will take a couple of years before it actually happens.

March 2013

Certificate Transparency

Google launches Certificate Transparency (CT), which is a long-term effort to have a public record of all public certificates.

March 2013

TIME

Tal Be'ery presents TIME, a way of abusing information leakage stemming from HTTP compression (and then encryption).

March 2013

Edward Snowden

Edward Snowden releases thousands of classified NSA documents to selected journalists, changing the public's perspective of the Internet forever. We eventually realise the extent of passive monitoring of plaintext communication.

May 2013

released with a PoC tool that retrieves CSRF tokens from real sites in less than a minute. Although not easy to exploit, compression before encryption remains a real problem for all web applications.

August 2013

Work on TLS 1.3 begins

Although TLS 1.2 seems good enough for now, it's clear that it can't support the next few decades of Internet evolution. Thus, work on the next-generation encryption protocol begins.

August 2013

Chrome 29 supports TLS 1.2

In version 29, Chrome adds support for TLS 1.2.

August 2013

ZMap

ZMap, a fast open source network and SSL scanner, is released. With this tool, fast and efficient scanning is available to everyone.

August 2013

Bullrun and Edgehill

The world learns about Bullrun (NSA) and Edgehill (GCHQ), two projects whose goal is to subvert encryption standards worldwide.

September 2013

Feisty Duck

Dual EC DRBG, a pseudorandom number generated standardised and promoted by NIST is implicated as a potential backdoor. A TLS extension called 'Extended Random', submitted for standardisation by the NSA, exposes a larger amount of random numbers on the wire.

September 2013

scans.io

The University of Michigan launches Internet-Wide Scan Data Repository, and seeds it with the results of their own SSL scanning efforts.

September 2013

Analysis of the HTTPS Certificate Ecosystem

Research published by Durumeric et al., is the first comprehensive study of the SSL ecosystem, based on 110 Internet-wide scans carried out over 14 months.

October 2013

ChaCha20-Poly1305

After a long time, another AEAD encryption is introduced to the ecosystem when Google starts to use ChaCha20-Poly1305 TLS suites. These suites will later be standardised for everyone to deploy.

October 2013

Safari on OS X supports for TLS 1.2

Safari on iOS devices added support for TLS 1.2 in an earlier release, but OS X users can now also benefit from improved security.

Keysight, EX-1032
Page 15

Feisty Duck

IE11 supports TLS 1.2

Microsoft adds support for TLS 1.2 to IE11, but doesn't backport it to IE10 and earlier.

November 2013

ANSSI fraudulent certificates

Chrome's public key pinning detected a number of certificates used during transparent interception of encrypted traffic within ANSSI, French network and information security agency. Shortly thereafter, ANSSI's CA was limited to issuing certificates only for French territories.

December 2013

2014

RSA 2048 becomes minimum for leafs

At the beginning of 2014, 1024-bit RSA keys for subscriber certificates are retired; 2048-bit RSA certificates become the new minimum. Weak intermediate and root keys remain in use.

January 2014

Firefox 27 support TLS 1.2

Firefox is the last major browser to add support for TLS 1.2.

February 2014

again. The attack is quite exciting, but doesn't have much practical impact.

March 2014

Heartbleed

A critical vulnerability in OpenSSL, a very widely used TLS library, is discovered. If exploited, Heartbleed enables attackers to retrieve process memory from vulnerable servers, often resulting in private key compromise. Because of tremendous hype associated with the attack, most public servers fix the vulnerability practically overnight. A long tail of vulnerable devices remains, though. Heartbleed's biggest contribution is showing the world how severely underfunded the OpenSSL project was in its 20 years of existence. In the following months, large organisations start contributing to the project and a big cleanup begins.

April 2014

Google unveils BoringSSL

After several years of using a patched version of OpenSSL, Google creates an OpenSSL fork called BoringSSL and start to migrate Chromium to it.

June 2014

NIC India fraudulent certificates

Google again detected several fraudulent certificates issued for their properties. This time, they were a result of a compromise of NICCA, a subordinate of India's National Informatics Centre. As a result, Chrome limited CCA's roots to issue certificates only for certain Indian domain names.

July 2014

improve and modernise the codebase. The first release follows quickly, in July 2014.

April 2014

Bulletproof SSL and TLS

After five years of research and two years of writing, Ivan Ristić publishes his book Bulletproof SSL and TLS. For the first time, complexities of the SSL/TLS and Internet PKI ecosystem are described in one volume.

August 2014

New Bleichenbacher Side Channels and Attacks

Christopher Meyer et al. present their new research, applying the Bleichenbacher attach from 1998 to the modern TLS stacks.

August 2014

CloudFlare gives away free certificates

CloudFlare popularises encryption by giving free certificates to their 2+ million users.

September 2014

BERserk vulnerability

BERserk is an RSA signature forgery attack due to incorrect parsing of ASN.1 in Mozilla NSS. It's a modern example of the Bleichenbacher attack.

September 2014

Keysight, EX-1032
Page 18

Feisty Duck

POODLE

It is discovered that SSL v3 doesn't actually have a defence against padding oracle attacks. Fortunately, attacks are generally not that easy to carry out and most of the world can use better protocols. Most sites realise they can turn off this older protocol version without anyone noticing. In response to POODLE, browsers stop falling back to SSL v3 on TLS connection failure.

October 2014

POODLE TLS

Shortly thereafter, it is discovered that, even though TLS 1.0 does have built-in defences against padding oracle attacks, some implementations don't implement them correctly. This new problem is named POODLE TLS. This discovery shines light on the fact that most protocol implementations aren't tested in adversarial conditions.

December 2014

2015

Superfish

It came to light that Lenovo shipped some of their laptops with ad-injector software capable of intercepting encrypted traffic via a hardcoded CA certificate. To make things worse, Lenovo used the same root CA for all their laptops, meaning any one owner could extract the corresponding private key and use it against all other similar systems. Superfish was the first widely publicised incident of this type; a number of similar problems were detected, for example in products such as Komodia and PrivDog.

February 2015

Prohibiting RC4 Cipher Suites

Keysight, EX-1032
Page 19

Feisty Duck

CNNIC fraudulent certificate

China's Internet Network Information Center (CNNIC) issued a short-lived subordinate CA for testing purposes to a company called MCS (Mideast Communication Systems), which promptly loaded it into a device for transparent network interception, creating at least one misissued certificate. As a result, Google and Mozilla revoked trust in CNNIC roots.

March 2015

live.fi misissued certificate

Seven years after the original live.com certificate incident, it transpired that Microsoft forgot to lock down all the administrative mailboxes on the live.fi domain name. As a result, the mailbox owner was able to obtain a valid certificate for this domain name.

March 2015

Firefox introduces OneCRL

In version 37, Firefox introduces OneCRL, Mozilla's proprietary method of revoking certificates. Before this improvement, the only way for Mozilla to blacklist certificates was via Firefox software updates.

March 2015

Microsoft introduces Certificate Reputation

Windows 10 is extended to continuously sample certificates users encounter in every-day browsing. The recorded certificates are sent back to Microsoft, from where they can be forwarded to site owners via the Bing Webmaster programme.

March 2015

Keysight, EX-1032
Page 20

Feisty Duck

SMACK

SMACK is an acronym for State Machine AttaCKs. It targets weaknesses in the implementations of the TLS state machine in various libraries.

March 2015

FREAK

The researchers behind the FREAK attack disclose that any server using export cryptography can be exploited via a flaw in many client TLS implementations. Initially it was thought that the problem exists only with OpenSSL, but Schannel and Secure Transport were later found to be vulnerable too.

March 2015

Firefox disables TLS fallbacks

In Firefox 37, released on 31 March 2015, insecure TLS fallbacks are disabled.

March 2015

HTTP Public Key Pinning

After many years of discussions, RFC 7469 is released to enable any to use public key pinning to protect themselves from fraudulently-issued certificates.

April 2015

TLS Fallback SCSV

A defence against protocol downgrade attacks is published as RFC 7507. The reactions are mixed; Chrome and Firefox decide to support it, but Microsoft doesn't like the idea.

Feisty Duck

Logjam

Logjam is an attack against weak Diffie-Hellman key exchange which is used by some servers. In essence, an active network attacker forces use of a weak cipher suite (e.g., a suite that uses 512-bit DH parameters) then breaks the connection in real-time.

May 2015

Chrome requires CT for EV certificates

Google decides to start requiring Certificate Transparency (CT) in order to recognise EV certificates. If that goes well, the plan is to eventually require CT for all certificates if they're to be trusted.

May 2015

HTTP/2

The long-awaited upgrade of the HTTP protocol is released as RFC 7540. Google pledges to switch to HTTP/2 over time and fully retire SPDY. Unlike SPDY, HTTP/2 doesn't require encryption, but all browser vendors decide to implement the new protocol that way.

May 2015

Deprecating Secure Sockets Layer Version 3.0

After POODLE, the IETF deprecates SSL v3 in RFC 7568.

June 2015

Feisty Duck

Transparency logs.

June 2015

There are more POODLEs in the forest

In two blog posts, titled There are more POODLEs in the forest and The POODLE has friends, researcher and TLS developer Yngve Nysæter Pettersen published results of his research into TLS implementation problems similar to the POODLE attack.

July 2015

Safari 9 disallows mixed active content

Safari is the last browser to disallow mixed active content. All browsers continue to allow mixed passive content (e.g., images).

October 2015

TLS Feature Extension

After years of discussion, a new X.509 extension is published in RFC 7633 to couple certificates with certain TLS features. The first user of the extension is must-staple, a desperately needed feature that requires a valid stapled OCSP response before a certificate is trusted.

October 2015

Let's Encrypt

Let's Encrypt is launched to provide free certificates with automated issuance. It is widely expected that this new non-profit CA will further drive down the price of DV certificates and encourage similar

November 2015

Censys

The University of Michigan team behind scans.io makes another steps forward and puts all their data into a new online database called Censys. The bar has never been lower, as researchers now have quick and easy access to large amounts of network security data.

December 2015

2016

Major browsers stop supporting RC4

Browser vendors decide to stop supporting RC4 suites, after the number of sites supporting nothing else drops down to an acceptable level.

January 2016

SHA1 certificates no longer allowed

CAs are no longer allowed to issue public SHA1 certificates. The key word here is "public". Some CAs continue to issue SHA1 certificates from roots that are not trusted by modern browsers, but continue to be trusted by older devices.

January 2016

Elliptic Curves for Security

January 2016

SLOTH

Researchers from INRIA demonstrate SLOTH (Security Losses from Obsolete and Truncated Transcript Hashes, CVE-2015-7575), which exploits the fact that many clients and servers continue to support RSA-MD5 signatures, even though they are now considered insecure.

January 2016

TLS 1.3 Ready or Not? Workshop

Previous versions of SSL and TLS were either rushed (SSL v2 and SSL v3) or maintenance efforts (TLS v1.0-v1.2). With TLS v1.3, the working group is taking a different approach; after more than two years in development, a workshop is held to carefully analyse the new designs.

February 2016

Must-staple and short-lived certs in Firefox

In Firefox 45, Mozilla improves how they handle revocation. One new feature is recognition of short-lived certificates (whose lifetime is measured in days), which are not checked for revocation. The more important improvement is support for must-staple, certificates that are considered valid only with a fresh stapled OCSP response.

March 2016

DROWN

Researchers publish DROWN, a new way to exploit SSL v2. Depressingly, it is estimated that about 33% of all HTTPS servers were affected at the time of disclosure. An interesting aspect of this attack is that

Keysight, EX-1032
Page 25

March 2016

Chrome drops all TLS fallbacks

In version 50, Chrome no longer attempts to use older TLS protocol versions after the initial handshake is unsuccessful due to a networking error. This change is critical to prevent active network attackers from downgrading communication to protocols that can potentially be exploited.

April 2016

Google stops using RC4 and SSLv3

In an important step to show the world that RC4 and SSLv3 are no longer needed, Google switches off these obsolete encryption features.

June 2016

Google enables HSTS

Blaming the complexities of their infrastructure for the delay, Google finally announce enabling HSTS on www.google.com.

July 2016

SWEET32 shows dangers of 64-bit block size

A new attack called Sweet32 emphasizes the weaknesses of ciphers that use 64-bit blocks, exploited via the Birthday paradox. Ciphers such as 3DES and Blowfish (the default in OpenVPN) are affected.

August 2016

October 2016

WoSign and StartCom are distrusted

Apple, Chrome, and Mozilla decided that WoSign and StartCom (now owned by WoSign) can't be trusted any more. This action is a culmination of a long investigation and multiple rule violations by these CAs. The root stores all made attempts to ensure a smooth transition by trusting already existing certificates.

October 2016

Chrome will require CT for all certificates in 2017

The Chrome team announced that publicly trusted website certificates issued in October 2017 or later will be expected to comply with Chrome's Certificate Transparency policy in order to be trusted.

October 2016

2017

SHA1 certificates deprecated

Modern browsers stop accepting SHA1 certificates, seemingly before SHA1 weaknesses are exploited.

January 2017

Let's Encrypt has 20m active certificates

January 2017

Chrome and Firefox warn about unencrypted passwords

Chrome and Firefox browsers keep pushing the Web toward better security by starting to warn about the presence of password and credit card fields on plaintext pages.

January 2017

SHAttered: SHA1 finally falls

Reserchers from CWI and Google released SHAttered, an identical-prefix collision attack target at SHA1. The attack used about 6,500 CPU years and 110 GPU years.

February 2017

Google announces plans to distrust and constraint Symantec certificates

Google announced that they had lost confidence in Symantec's certificate issuance policies and practices and proposed a series of steps that would mean severely constraining Symantec's operations. The plan is later updated to be less restrictive.

March 2017

DigiCert announces plans to acquire Symantec's website security and PKI business

DigiCert announces plans to acquire Symantec's website security and PKI business. The transaction completes in October. By December 1st, DigiCert begins issues all Symantec certificates from a brand new PKI hierarchy.

Feisty Duck

CAA becomes mandatory

Four years after published as RFC 6844, Certification Authority Authorisation (CAA) becomes mandatory via CA/Browser Forum's Baseline Requirements.

September 2017

Google and Mozilla decide to stop trusting existing Symantec certificates

In March 2017 Google disclosed their plans to distrust existing Symantec certificates. Many months of discussion followed. By August, Google and Mozilla agreed to lesser penalties in return for Symantec outsourcing certificate issuance to a third party. Symantec not only chose DigiCert for the issuance, but also decided to move their entire certificate business to them.

September 2017

The ROBOT attack

ROBOT is the return of a 19-year-old vulnerability that allows performing RSA decryption and signing operations with the private key of a TLS server.

December 2017

2018

Let's Encrypt supports wildcard certificates

On March 13th, Let's Encrypt added support for ACMEv2 and wildcard certificates.

March 2018

Keysight, EX-1032
Page 29

Feisty Duck

TLS 1.3 approved

On March 21, the IESG approved the 28th revision of TLS 1.3 as Proposed Standard.

March 2018

Chrome requires CT for all new certificates

From today, Chrome requires that all publicly issued certificates support Certificate Transparency. Enforcement began with Chrome 68, released in late July.

May 2018

PCI Council deprecates TLS 1.0

From July 2018, PCI-compliant merchants must not support TLS 1.0. Originally, this date was intended to be in July 2016, but that was not realistic because of too many users relying on obsolete technology that doesn't support modern protocols.

July 2018

Chrome marks HTTP pages as 'not secure'

After several years of nudging the ecosystem toward full encryption, released on July 24, finally started marking all HTTP pages as not secure.

July 2018

TLS 1.3 published as RFC 8446

After 5 years in development, TLS 1.3 has finally been published as RFC 8446. This TLS protocol update comes 10 years after the previous version, TLS 1.2.

Keysight, EX-1032
Page 30

Feisty Duck

2019

ACME standardized as RFC 8555

Automatic Certificate Management Environment (ACME) is now a recognized standard, published as RFC 8555. ACME was one of the key factors for the success of Let's Encrypt.

March 2019

Gmail deploys MTA-STS

Google announced that Gmail had deployed MTA-STS, the email equivalent of HTTP Strict Transport Security. To work around the fact that DNS entries can be altered by a active network attacker, MTA-STS bootstraps via a HTTPS web site.

April 2019

Chrome and Firefox remove EV certificate indicators

Chrome 77, released in September 2019, and Firefox 70, released in October 2019, no longer prominently indicate when a web site uses an Extended Validation certificate.

September 2019

2020

Shambles: Chosen-prefix attack against SHA1

January 2020

Let's Encrypt has issued a billion certificates

Let's Encrypt announced that they have issued more than a billion certificates for 192 million web sites.

February 2020

Chrome activates DNS-over-HTTPS

Starting with Chrome 83, DNS-over-HTTPS (DoH) is detected and automatically used when available. Users are also able to manually configure to use DoH from one of the supported providers.

May 2020

Browsers disable TLS 1.0 and 1.1

TLS 1.0 and 1.1 have been removed from Chrome and Firefox. Internet Explorer removed support in September 2020.

July 2020

Apple reduces certificate lifetimes to one year

Certificates issued from today and valid for more than 398 days are no longer accepted by Apple. Chrome, Mozilla, and Microsoft follow.

September 2020

Feisty Duck

Manual configuration is also possible.

September 2020

Chrome no longer allows mixed content

Starting with version 86, Chrome auto-upgrades or blocks plaintext resources referenced from encrypted pages. Mixed content, passive or active, is thus no longer allowed. This change was initially announced in October 2019, but ended up being postponed for about a year.

October 2020

Raccoon attacks DH in TLS 1.2 and earlier

Researchers publish details on the Raccoon attack, a hard-to-exploit timing side channel in TLS 1.2 and earlier.

September 2020

Firefox introduces HTTPS-only browsing

Firefox 83 introduces a new mode of operation that allows only encrypted communication by default. Plaintext connections are allowed only with explicit user permission.

November 2020

2021

encrypted pages are no longer allowed. The changes were announced in February 2020 and implemented as a series of incremental improvements, with the first step starting with Chrome 83.

March 2021

IETF deprecates TLS 1.0 and 1.1

The Internet Engineering Task Force has published RFC 8996, which officially deprecates the old TLS versions 1.0 and 1.1. These old versions have inherent security weaknesses that can only be fixed by moving to a newer protocol version.

March 2021

Chrome rolls out SCT auditing

After a long time in development, SCT Auditing is being deployed to Chrome. This new type of auditing will provide better visibility into the correct operation of the CT ecosystem.

March 2021

Chrome defaults to HTTPS

Starting with version 90, Chrome will default to HTTPS for most typed navigations that don't specify a protocol.

April 2021

Apple's updated CT policy requires CT log operator diversity

With the most recent policy update, Apple now requires three SCTs for certificates valid for more than 180 days, as well as requires CT log operator diversity.

Keysight, EX-1032
Page 34

Feisty Duck

QUIC graduates to RFC 9000

QUIC, a new reliable and secure protocol, has been released as RFC 9000. This protocol marks a new direction in how networking standards are designed. QUIC ignores TCP in favour of UDP, as well as combines reliable transport with multiplexing and encryption.

May 2021

Apple deprecates TLS 1.0 and TLS 1.1

Apple announced TLS 1.0 and TLS 1.1 have been deprecated on iOS 15, iPadOS 15, macOS 12, watchOS 8, and tvOS 15. These older protocol version will be removed from future releases.

September 2021

Expiration of DST Root CA causes problems with Let's Encrypt certificates

In September, two events combined—expiration of DST Root CA and one of Let's Encrypt's intermediate certificates—caused widespread problems, highlighting poorly implemented path building in commonly used PKI libraries.

October 2021

2022

Chrome to remove the 'One Google Log' CT policy requirement

Chrome developers announced that, from 15 April 2022, Chrome will no longer require that certificates must be recorded in at least one CT log operated by Google. The new policy will instead focus on operator diversity instead, similar to Apple's approach.

Keysight, EX-1032
Page 35

The timeline design and code adapted from CodyHouse's Vertical Timeline project. Thanks!

Feisty Duck

THE FINEST IN TLS AND PKI EDUCATION

hello@feistyduck.com

@feistyduck

BOOKS

Bulletproof TLS and PKI

ModSecurity Handbook

OpenSSL Cookbook

TRAINING

Practical TLS and PKI

RESOURCES

Bulletproof TLS Newsletter

SSL/TLS and PKI History

Archived Books

COMPANY

Support

Website Terms of Use

Terms and Conditions

Privacy Policy

About Us