SSLv3: Dead or Alive?

Yuji Suga

The Nightmare Before Christmas in 2014

The Nightmare Before Christmas in 2014

- **A lot of problem in cryptographic modules:**

The Nightmare Before Christmas in 2014

- **A lot of problem in cryptographic modules:**

[April] **Heartbleed Bug in OpenSSL**
[June] **CCS Injection attack in OpenSSL**
[Sept.] **Verf. miss RSAsign in Mozilla NSS**
[Oct.] **POODLE attack in spec. of SSLv3**

The Nightmare Before Christmas in 2014

- A lot of problem in cryptographic modules:

[02/14] goto fail; goto fail;

[04/14] Heartbleed Bug in OpenSSL

[06/14] CCS Injection attack in OpenSSL

[08/14] Some fixes in OpenSSL

[10/14] POODLE attack in spec. of SSLv3

[12/14] ???

The Nightmare Before Christmas in 2014

- A lot of problem in cryptographic modules:

[02/14] goto fail; goto fail;

[04/14] Heartbleed Bug in OpenSSL

[06/14] CCS Injection attack in OpenSSL

[08/14] Some fixes in OpenSSL

[10/14] POODLE attack in spec. of SSLv3

[12/14] ??? (after POODLE?)

Earthly Branches

地支: 子、丑、寅、卯、辰、巳、午、未、申、酉、戌、亥

POODLE attack

- CVE-2014-3566
- published on Oct. 14
  - https://www.openssl.org/~bodo/ssl-poodle.pdf
- is caused by issues of protocol specification.
  - Only applied in using CBC mode over SSLv3

https://www.cellos-consortium.org/index.php?PoodleAttack_20141015

POODLE attack

- CVE-2014-3566
- published on Oct. 14
  - https://www.openssl.org/~bodo/ssl-poodle.pdf
- is caused by issues of protocol specification.
  - Only applied in using CBC mode over SSLv3
- BEAST-like attack
  - The “1/n-1 division” method against BEAST
  - So we can use TLS1.0, but SSLv3 would be vuln.

https://www.cellos-consortium.org/index.php?PoodleAttack_20141015

Fundamental countermeasures

- (1) Disable SSL3.0 (in client or server)
  - Major browser vendors have announced that they will disable SSLv3 in the future.

- (2) Introducing TLS_FALLBACK_SCSV (in both client and server)
  - protecting against potential downgrade attacks
  - draft-ietf-tls-downgrade-scsv

Available Ciphersuites of SSLv3

SSL_NULL_WITH_NULL_NULL
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
SSL_RSA_WITH_IDEA_CBC_SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_DSS_WITH_DES_CBC_SHA
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_RSA_WITH_DES_CBC_SHA
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
SSL_DH_anon_WITH_RC4_128_MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_anon_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_FORTEZZA_KEA_WITH_NULL_SHA
SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA
SSL_FORTEZZA_KEA_WITH_RC4_128_SHA

https://www.tools.ietf.org/html/rfc6101

Available Ciphersuites of SSLv3

- **Disable null-cipher and anon-server**

SSL_NULL_WITH_NULL_NULL
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
SSL_RSA_WITH_IDEA_CBC_SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_DSS_WITH_DES_CBC_SHA
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_RSA_WITH_DES_CBC_SHA
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
SSL_DH_anon_WITH_RC4_128_MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_anon_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_FORTEZZA_KEA_WITH_NULL_SHA
SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA
SSL_FORTEZZA_KEA_WITH_RC4_128_SHA

https://www.tools.ietf.org/html/rfc6101

Available Ciphersuites of SSLv3

- **Disable EXPORT**

SSL_NULL_WITH_NULL_NULL
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
SSL_RSA_WITH_IDEA_CBC_SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_DSS_WITH_DES_CBC_SHA
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_RSA_WITH_DES_CBC_SHA
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA

SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
SSL_DH_anon_WITH_RC4_128_MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_anon_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_FORTEZZA_KEA_WITH_NULL_SHA
SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA
SSL_FORTEZZA_KEA_WITH_RC4_128_SHA

https://www.tools.ietf.org/html/rfc6101

Available Ciphersuites of SSLv3

- **Disable DES, ...**

SSL_NULL_WITH_NULL_NULL
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
SSL_RSA_WITH_IDEA_CBC_SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_DSS_WITH_DES_CBC_SHA
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_RSA_WITH_DES_CBC_SHA
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA

SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
SSL_DH_anon_WITH_RC4_128_MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_anon_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_FORTEZZA_KEA_WITH_NULL_SHA
SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA
SSL_FORTEZZA_KEA_WITH_RC4_128_SHA

https://www.tools.ietf.org/html/rfc6101

Available Ciphersuites of SSLv3

- **Now we can use only…**

SSL_NULL_WITH_NULL_NULL
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
SSL_RSA_WITH_IDEA_CBC_SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_DSS_WITH_DES_CBC_SHA
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_RSA_WITH_DES_CBC_SHA
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA

SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
SSL_DH_anon_WITH_RC4_128_MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_anon_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_FORTEZZA_KEA_WITH_NULL_SHA
SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA
SSL_FORTEZZA_KEA_WITH_RC4_128_SHA

https://www.tools.ietf.org/html/rfc6101

Available Ciphersuites of SSLv3

- **Now we can use only…**

SSL_NULL_WITH_NULL_NULL
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
SSL_RSA_WITH_IDEA_CBC_SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_DSS_WITH_DES_CBC_SHA
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_RSA_WITH_DES_CBC_SHA
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA

RC4

3DES-CBC

SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
SSL_DH_anon_WITH_RC4_128_MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_anon_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_FORTEZZA_KEA_WITH_NULL_SHA
SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA
SSL_FORTEZZA_KEA_WITH_RC4_128_SHA

https://www.tools.ietf.org/html/rfc6101

Available Ciphersuites of SSLv3

- **Due to the POODLE attack, …**

SSL_NULL_WITH_NULL_NULL
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
SSL_RSA_WITH_IDEA_CBC_SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_DSS_WITH_DES_CBC_SHA
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_RSA_WITH_DES_CBC_SHA
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
SSL_DH_anon_WITH_RC4_128_MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA

RC4

3DES-CBC

https://www.tools.ietf.org/html/rfc6101

Available Ciphersuites of SSLv3

- **Due to the invited talk today, ...**

SSL_NULL_WITH_NULL_NULL
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
SSL_RSA_WITH_IDEA_CBC_SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_DSS_WITH_DES_CBC_SHA
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_RSA_WITH_DES_CBC_SHA
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
SSL_DH_anon_WITH_RC4_128_MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_anon_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_FORTEZZA_DMS_WITH_NULL_SHA
SSL_FORTEZZA_DMS_WITH_FORTEZZA_CBC_SHA
SSL_FORTEZZA_DMS_WITH_RC4_128_SHA

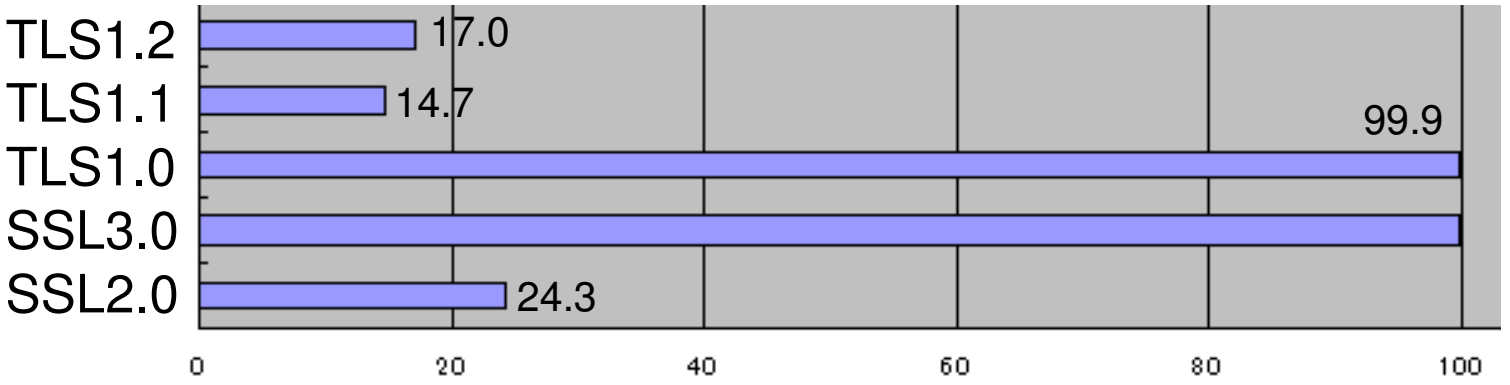
~~RC4~~

~~3DES~~-CBC

https://www.tools.ietf.org/html/rfc6101

Before the POODLE attack

- **April 15 (Heartbleed)** **SSL-enable sites=5677**



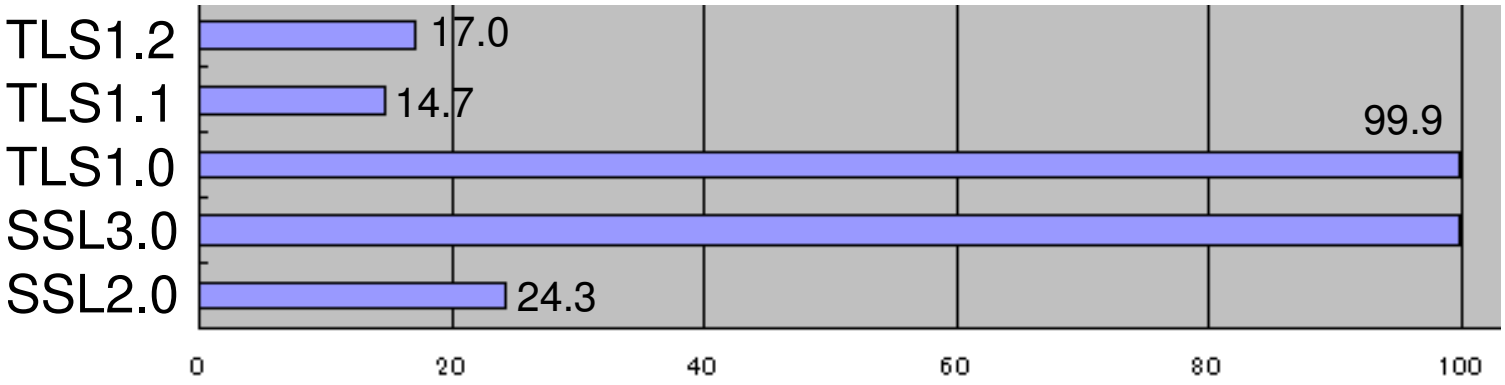
99.9%

Surveyed: .jp domain 17988 sites listed in the AlexaTop100M

http://www.iij.ad.jp/company/development/tech/techweek/pdf/141127_1_2.pdf

After the POODLE attack

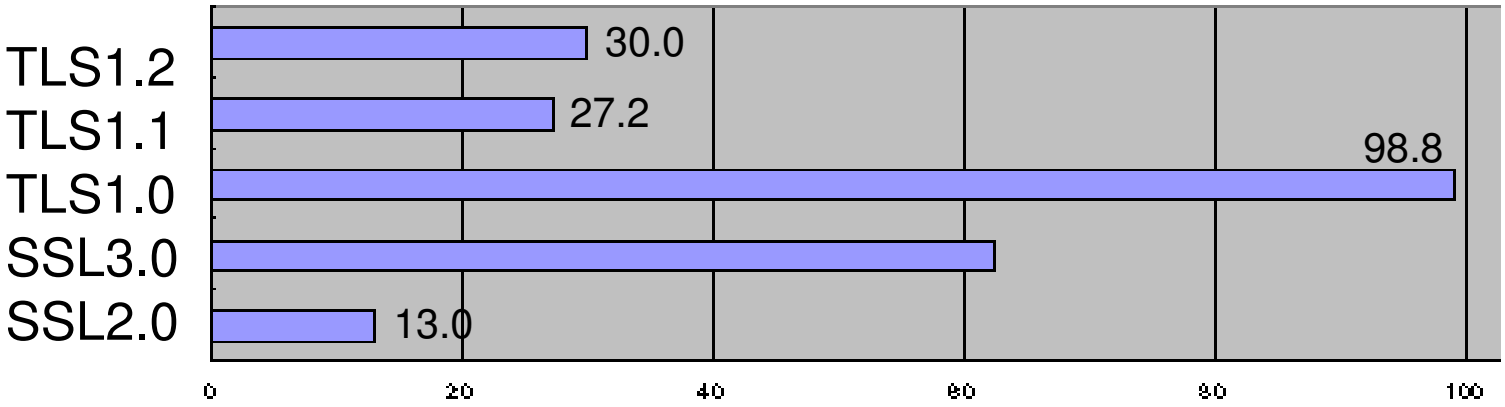
- **April 15 (Heartbleed)** SSL-enable sites=5677



99.9%

1 out of 3 servers disabled SSLv3

- **November 26** SSL-enable sites=5620



62.3%

http://www.iij.ad.jp/company/development/tech/techweek/pdf/141127_1_2.pdf

5 major internet shopping sites in Taiwan

	Site-A	Site-B	Site-C	Site-D	Site-E
TLS1.2	✓	✓			
TLS1.1	✓	✓			
TLS1.0	✓	✓	✓	✓	✓
SSL3.0				✓	✓
SSL2.0					

5 major internet shopping sites in Taiwan

	Site-A	Site-B	Site-C	Site-D	Site-E
TLS1.2	✓	✓			
TLS1.1	✓	✓			
TLS1.0	✓	✓	✓	✓	✓
SSL3.0				✓	✓
SSL2.0					

Using RC4 is prior to AES

5 major internet shopping sites in Taiwan

	Site-A	Site-B	Site-C	Site-D	Site-E
TLS1.2	✓	✓			
TLS1.1	✓	✓			
TLS1.0	✓	✓	✓	✓	✓
SSL3.0				✓	✓
SSL2.0					

Only using RC4 and TripleDES

Using RC4 is prior to AES

Why do servers still enable SSLv3?

- Due to server misconfiguration?
- Afraid of lost opportunity?

Why do servers still enable SSLv3?

- Due to server misconfiguration?

- Afraid of lost opportunity?
  - For that reason, once SSL/TLS servers remove support for SSLv3, in some cases it will no longer be possible to view websites from legacy devices.
  - It will be difficult to implement measures for legacy products such as feature phones and game devices.

Motivation

- **Are there "life extension technologies" of SSLv3?**
  - **remain SSLv3-enable legacy devices (no updates)**
  - **can fix problems in only server-side**
  - **can apply both**
    the POODLE attack and
    RC4 bias attacks

Sketch of ideas

Against POODLE attack :

- **Server should NOT return "padding error".**
  - **Attackers can not know whether altered message is accepted or not.**

Sketch of ideas

Against RC4 bias attacks :

- **Servers can detect a plenty of encrypted SSLv3 messages for same plaintxt.**

- **HTTP message Malleability**
  - **Encode other way for same plaintxt.**
  - **Encoded data are different, but semantically same.**

Practical fixes for servers?

- **Evaluate CPU cost?**
- **Easy to implement?**

- **Please continue discussions at**

CELLOS

Cryptographic protocol Evaluation toward
Long-Lived Outstanding Security

https://www.cellos-consortium.org/index.php?Symposium%2F2014

CELLOS

Cryptographic protocol Evaluation toward
Long-Lived Outstanding Security

- **We established the Cryptographic protocol Evaluation toward Long-Lived Outstanding Security (CELLOS) last year,**

with the aim of promoting secure cryptographic protocols, by bringing together and sharing information on security of cryptographic protocols, based on the results of previous research and development, discussing security issues based on modern ICT systems, and publishing the resulting security information.

https://www.cellos-consortium.org/

Announcement

- **CELLOS symposium 2014**

  https://www.cellos-consortium.org/index.php?Symposium/2014

- **IWSEC2015**

  http://www.iwsec.org/2015/

- **ProvSec2015**

  Deadline : **June 17th**, 2015
  Notification: August 17th, 2015

https://security-lab.jaist.ac.jp/provsec2015/