SECURITY 2025

BIG CLOUDS

OVER SNOWDONIA

OUR DATA IS IN THE CLOUD.
WE HAVE MOSTLY SIGNED AWAY THEIR OWNERSHIP.

IMPORTANT INTERESTS WANT TO KNOW ALL ABOUT US.


Google


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

ADVANCED PERSISTENT THREATS


SONY


13
14
15
16
17
18
9
0
1
2
3


PRESS ANY KEY!


MAERSK
MAERSK
MAERSK
MAERSK LINE
Matson

PRE-SNOWDEN:

Confidentiality requires Authentication:

» Attacker might mount Man-in-the-Middle Attack

» Use Certificates to prevent MITM

» But Certificates are complicated

FEW SITES ACTUALLY USED HTTPS

POST-SNOWDEN:

Confidentiality no matter what

MAKE HTTPS THE DEFAULT

... and where that doesn't work:

ADD OPPORTUNISTIC ENCRYPTION

PERVASIVE MONITORING

... is an Attack! (RFC 7258)

We now know pervasive monitoring actually happens

» not a surprise in principle

» but a big difference in extent

THAT CHANGES THE PRIORITIES!

OPPORTUNISTIC ENCRYPTION

Encrypt, even if we are not quite safe against MITM

» An attacker now has to become active

  » active attacks won't become pervasive in civilized countries

» Increase cost of pervasive monitoring

RFC 7435: "Opportunistic Security: Some Protection Most of the Time."

WHY DIDN'T WE DO THAT EARLIER?

There is a cost to "perceived security":

» People think that the system is giving them "security"

» People act in a more careless manner

COST IS NOW JUSTIFIED

» And make sure OE is not advertised when present

THE CORRUPTION OF SECURITY PROCESSES

It is now clear that NSA has subverted Dual_EC_DRBG.

So far, NIST, IETF, and others have relied on NSA's integrity.

They now consider themselves to have been betrayed.

How to win back their customers' trust in their Security Processes?

THE BIG FIGHT FOR NEW CURVES

Elliptic Curve Cryptography (ECC) is more efficient than, e.g.:

» RSA (Integer Factorization Cryptography, IFC), or

» El Gamal (Finite Field Cryptography, FFC)

ECC Math is way more complex than IFC or FFC math, and newer.

Does NSA have an Ace up their sleeves?

ECC STATUS QUO

Certicom [Blackberry] patented away most newer ECC.

Prime-field ECC is too old for patents (RFC 6090)

Two curves dominate prime-field ECC:

» P-256 (good for US SECRET, with AES-128)

» P-384 (good for US TOP SECRET, with AES-256)

We have switched much of HTTPS to P-256.

[Blackberry] Certicom became part of Blackberry in 2009.

HOW WERE P-256/-384 CREATED?

NSA suggested vital parameters in the 1990s*.

“I no longer trust the constants. I believe the NSA has manipulated them through their relationships with industry.”
Bruce Schneier

Does NSA know something about these constants we don't?

Can they use this to break P-256/P-384?

* Jerry Solinas (NSA) suggested e.g. P-256's seed, c49d360886e704936a6678e1139d26b7819f7e90.

1999 Michael Scott
“Re: NIST annouces set of Elliptic Curves”:

Consider now the possibility that one in a million of all curves have an exploitable structure that "they" know about, but we don’t.. Then "they" simply generate a million random seeds until they find one that generates one of "their" curves. Then they get us to use them. And remember the standard paranoia assumptions apply - "they" have computing power way beyond what we can muster. So maybe that could be 1 billion.

"SAFE" CURVES

» are mathematically minimal ("rigid" [Bernstein])

» do not rely on "random" numbers

  » that could be Aces up someone's sleeves

» are easily implementable

  » no (or easily testable) weak values

  » easy to avoid timing and cache leaks

[Bernstein] http://safecurves.cr.yp.to/rigid.html

SO: ARE P-256/-384 »BROKEN«?

Only NSA knows.

For the rest of us, that is a matter of opinion.

» Peddlers of new curves ask why we should accept a possibility of manipulation.

» Peddlers of existing crypto accelerators don't see a problem.

(Impartial experts tend to agree.)

INCREASING RESILIENCE

» NSA is listening, as well as actively attacking

» North Korea is actively attacking! (we think)

Can we make protocols less brittle?

What are the self-healing properties we can achieve?

How can we minimize the damage of each intrusion?

IMPROVING FORWARD SECRECY

(Perfect) Forward Secrecy protects past conversations against future attacks

Many existing schemes do not offer PFS, e.g.:

» RSA key agreement in TLS

→

» deprecate non-PFS cipher suites

» offer D-H-based alternatives

UNBEARABLE: GETTING RID OF BEARER TOKENS

Bearer Tokens are presented again and again

» e.g., in Cookies

Problem: compromise once → compromise Authorization forever (cf. passwords)

Solution: Proof-of-Possession protocols

(can use JOSE – JSON Object Signing and Encryption and COSE – CBOR Object Signing and Encryption)

Quelle:

https://haveibeenpwned.com

REDUCING USE OF PASSWORDS

DESIGN FOR PRIVACY (RFC 6973)

Data minimization:
Do not collect data if not actually needed

» vs. operational requirements

Do not provide linkability, e.g.

» do not use MAC addresses in IPv6 addresses

» even better: randomized MAC addresses

BUILD A POST-INTERNET INFRASTRUCTURE

Various "indie" attempts

Freifunk

Tor

» Darknets: e.g., Silk Road

ANONYMITY VIA MIXING

Encryption is not enough: Need to mix to be anonymous

Multiple mixing steps

» reduce impact of any single mixer compromise

Attack: Correlation (Traffic analysis)

» Mixmaster etc. include delays (e-mail)

» Real-time mixers such as Tor cannot really delay

ACKNOWLEDGMENTS

Wikimedia: Snowdonia NSA-Badge Petya

Web: Google Target Heartbleed NSA-Heartbleed Maersk Giessen

Snowdonia http://commons.wikimedia.org/wiki/File:Llyn_Llydaw_from_Crib_Goch_2.jpg

NSA-Badge http://upload.wikimedia.org/wikipedia/commons/thumb/0/04/National_Security_Agency.svg/1024px-National_Security_Agency.svg.png

Petya https://upload.wikimedia.org/wikipedia/commons/4/44/2017_Petya_cyberattack_screenshot.jpg

Google http://www.agom.biz/wp-content/uploads/2014/04/Google-SERPs.png

Target http://static.businessinsider.com/image/51114c736bb3f7af20000000/image.jpg

Heartbleed http://heartbleed.com/heartbleed.png

NSA-Heartbleed http://www.extremetech.com/wp-content/uploads/2014/04/nsa-fort-meade-heartbleed-640x436.jpg

Maersk https://www.ccn.com/shipping-giant-maersk-deploys-first-blockchain-based-marine-insurance

Giessen https://aware7.de/en/blog/hacker-attack-university-of-giessen

ISPS (SS 2025) → 03-IMAP-ISPS

Informationssicherheit: Prozesse und Systeme

» Sicherheitsprotokolle und -abläufe in der Praxis

Wir diskutieren relevante Standards aus W3C und IETF, z.B.:

» Authentisierung und Autorisierung:
Von OAuth bis zu FIDO; GNAP

» Beyond Dolev-Yao: Endorsement, Attestation, Appraisal
Secure Enclaves, Trusted Execution Environments,
Confidential Computing

» Supply-Chain Integrity, SBOM, Digital Ledgers