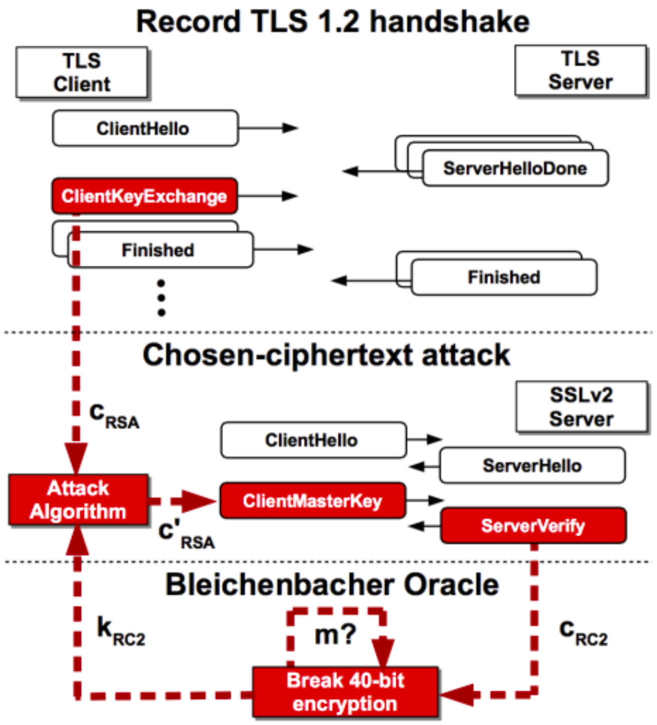
RISK ASSESSMENT / SECURITY & HACKTIVISM

More than 11 million HTTPS websites imperiled by new decryption attack

Low-cost DROWN attack decrypts data in hours, works against TLS e-mail servers, too.

by **Dan Goodin** - Mar 1, 2016 9:02pm CST

Share Tweet Email 24



Enlarge

Aviram et al.

More than 11 million websites and e-mail services protected by the transport layer security protocol are vulnerable to a newly discovered, low-cost attack that decrypts sensitive communications in a matter of hours and in some cases almost immediately, an international team of researchers warned Tuesday. More than 81,000 of the top 1 million most popular Web properties are among the vulnerable HTTPS-protected sites.

The attack works against TLS-protected communications that rely on the RSA cryptosystem when the key is exposed even indirectly through SSLv2, a TLS precursor that was retired almost two decades ago because of crippling weaknesses. The vulnerability allows an attacker to decrypt an intercepted TLS connection by repeatedly using SSLv2 to make connections to a server. In the process, the attacker learns a few bits of information about the encryption key each time. While many security experts believed the removal of SSLv2 support from browser and e-mail clients prevented abuse of the legacy protocol, some misconfigured TLS implementations still tacitly support the legacy protocol when an end-user computer specifically requests its use. The most notable implementation subject to such fatal misconfigurations is the OpenSSL cryptographic library, which on Tuesday is expected to release an update that makes such settings much less likely to occur.

Recent scans of the Internet at large show that more than 5.9 million Web servers, comprising 17 percent of all HTTPS-protected machines, directly support SSLv2. The same scans reveal that at least 936,000 TLS-protected e-mail servers also support the insecure protocol. That's a troubling finding, given widely repeated advice that SSLv2—short for secure sockets layer version 2—be disabled. More troubling still, even when a server doesn't allow SSLv2 connections, it may still be susceptible to attack if the underlying RSA key pair is reused on a separate server that does support the old protocol. A website, for instance, that forbids SSLv2 may still be vulnerable if its key is used on an e-mail server that allows SSLv2. By the researchers' estimate, that leaves 11.5 million HTTPS-protected websites and a significant number of TLS-protected e-mail servers open to attack.

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Life in Technicolor—One month wearing EnChroma's color blindness-fixing glasses

By blocking wavelengths, glasses create a new world complete with grass, traffic lights.

WATCH ARS VIDEO

MWC 2016: Hands-on Samsung Galaxy S7 & S7 Edge

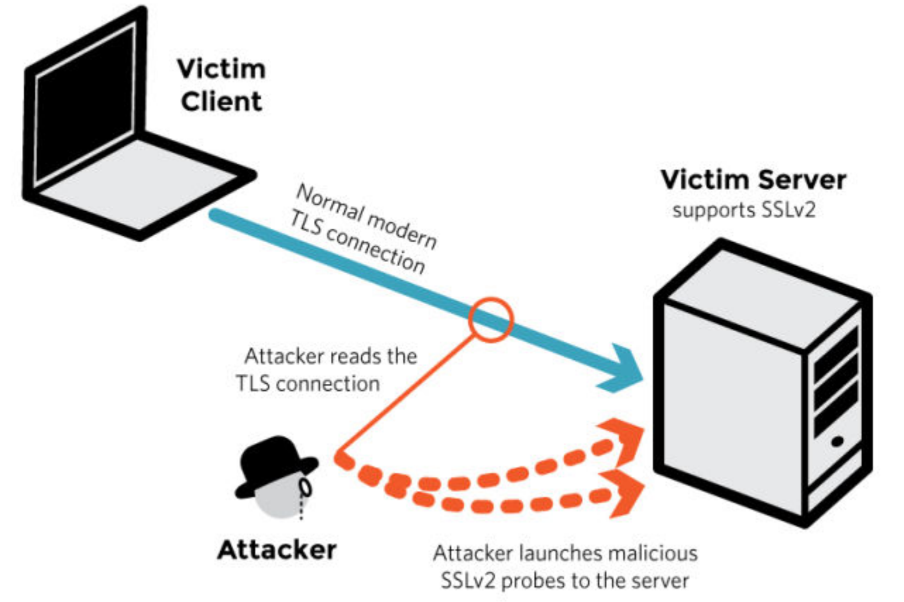
Ars Technica UK gets their hands on the shiny new Samsung Galaxy S7 and S7 Edge devices at MWC 2016.

STAY IN THE KNOW WITH

LATEST NEWS

BLOCK PARTY

Minecraft finally gets a combat overhaul with v1.9 update


Victim Client
Normal modern TLS connection
Victim Server
supports SSLv2
Attacker reads the TLS connection
Attacker
Attacker launches malicious SSLv2 probes to the server

Enlarge
Aviram et al.

The vulnerability joins a swarm of other critical bugs that over the past five years have given attackers the ability to break TLS. With names including BEAST, CRIME, BREACH, and FREAK, the proof-of-concept exploits have demonstrated dangerous holes in a protocol that's the sole means for most websites and e-mail servers to encrypt and authenticate communications over an Internet that was never designed to be secure or private. TLS security hit a new low last May with the discovery of Logjam, a vulnerability caused by deliberately weakened cryptography that allowed eavesdroppers to read and modify data passing through tens of thousands of Web and e-mail servers. The researchers have dubbed the latest vulnerability DROWN, short for Decrypting RSA with Obsolete and Weakened eNcryption.

"This shouldn't keep happening"

"It's pretty practical because if you know you want to target certain websites and they're vulnerable, you can pretty much set up shop and the next thing you know you have all of these secure connections, the passwords, and everything else," Matt Green, a cryptography expert at Johns Hopkins University who has read the research paper, told Ars. "It's amazing to me that we keep finding one or two of these [vulnerabilities] per year for protocols that are this old. This shouldn't keep happening. It kind of makes me feel like we're not doing our jobs."

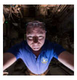
The most widely used TLS implementation known so far to be vulnerable to DROWN is OpenSSL. While current versions by default don't allow SSLv2 connections, administrators sometime inadvertently override those settings, often in an attempt to optimize applications such as the Apache and Nginx Web servers or the Sendmail or Postfix e-mail servers. Tuesday's OpenSSL updates make it impossible for ordinary end users to enable SSLv2 without declaring explicit intent to do so. The patch also removes support for extremely weak 1990s-era ciphers that are key to making DROWN attacks work. The weak ciphers were added to all SSL and TLS versions prior to 2000 as part of US government's export regulations (more about that later).

Servers that rely on the open source code library should upgrade to version 1.0.2g or 1.0.1s as soon as possible. The patches were released Tuesday in coordination with the researchers' disclosure of the DROWN vulnerability. Maintainers of OpenSSL are expected to publish much more about the update here. The researchers' technical paper is titled DROWN: Breaking TLS using SSLv2. They have also published this blog post with additional information.

Microsoft's IIS versions 7.0 and on and versions 3.13 and above of the NSS crypto library all have SSLv2 disabled by default. Anyone using older versions of either of these programs should upgrade right away. The researchers recommend that even those running versions presumed to be safe use this form incorporated into their blog post to test if specific TLS-protected services are vulnerable, since it's possible to inadvertently override the defaults disallowing SSLv2 connections. A longer list of software that's affected by DROWN is expected to be compiled in the coming days.

For servers that can't be updated right away, using a firewall to filter SSLv2 traffic is a reasonable work-around, although it will prevent the researchers' testing script and other benign services from detecting vulnerable servers. Administrators who want to know if their networks have been targeted by DROWN may be able to detect attacks by examining logs for large numbers of SSLv2 connections to any servers. (A small number of SSLv2 connections made over the past two months are likely part of the Internet-wide scans conducted by the researchers.) At the moment, the researchers have no evidence indicating DROWN is being actively exploited. Like most attacks against TLS, DROWN works only when an attacker has the ability to monitor traffic passing between an end user and the server. Since DROWN is a server-side exploit, there's nothing end users can do to prevent being attacked, short of

Dark Souls 3: Cowards and newcomers need not apply


Liveblog: Scott Kelly comes home from space tonight after nearly a year

Quantum Break's time-bending gameplay gets caught in the uncanny valley

Microsoft makes big Xbox-on-PC push with 4K, 60 fps *Forza 6 Apex*

WHEELS OF STEEL
Technics SL-1200G costs $4,000 because original manufacturing tools "were gone"

not using vulnerable TLS services.

Fatally weak export-grade crypto strikes again

The most general DROWN attack exploits 1990s-era cryptography that uses extremely weak 40-bit symmetrical encryption so software would comply with export restrictions mandated by the Clinton administration. The attacker captures roughly 1,000 RSA key exchanges made between an end user and a vulnerable TLS server, and the connections can use any version of the SSL or TLS protocols, including the current TLS 1.2. The attacker then uses the intercepted RSA ciphertexts to initiate several thousand SSLv2 connection attempts that include an instruction for the server to use the 40-bit cipher. The attacker then compares the ciphertext to all the 2^{40} possibilities.

Decrypting the TLS connection requires just 2^{50} computations, a task that in a worst-case scenario Amazon's EC2 service can perform in eight hours for just $440. The researchers devised an alternate decryption method that uses a cluster of graphics cards and takes 18 hours. With additional work, the exploits could almost certainly be optimized so they're faster and less costly. The attack works by decrypting the "premaster secret" that's supposed to be known only to the server and end user. Because the premaster secret serves as the key that encrypts data once the initial TLS handshake is completed, DROWN exploits allow attackers to decrypt any intercepted TLS connections that use it.

The researchers also devised a significantly more severe version of DROWN that works against servers running versions of OpenSSL that haven't been patched since March 2015. It allows attackers to decrypt the "premaster secret" almost instantly. An attacker can use the technique to perform man-in-the-middle attacks that cryptographically impersonate a vulnerable server. Scans performed by the researchers show that a significant percentage of servers vulnerable to DROWN are also susceptible to this more severe version of the exploit. The finding suggests that a surprisingly large number of OpenSSL users have yet to install the March 2015 update, which unknowingly fixed the vulnerabilities that make the more severe attack possible.

DROWN is an extension of what cryptographers call the 1998 Bleichenbacher attack, named after Daniel Bleichenbacher, the Swiss cryptographer who discovered the underlying weakness in the PKCS#1 v1 encoding function. While considered a seminal exploit for the mathematical insight it provided, it wasn't considered especially practical, because it required attackers to make hundreds of thousands or millions of connections to the victim server to compromise a single session key.

Ironically, some of the Bleichenbacher countermeasures built into the SSLv2 provided precisely the type of data required to carry out the type of so-called "padding oracle" attack that Bleichenbacher discovered. The Bleichenbacher defenses, it turned out, provided its own oracle that exposed TLS version 1.0 and later exposed it to plaintext recovery attacks. The DROWN research is notable not only because it requires many fewer queries to the server, but also because its cross-protocol nature allows attackers to exploit the SSLv2 weakness to defeat the separate TLS specification. The DROWN findings are also significant because they were the first to identify the ineffectiveness of the Bleichenbacher countermeasures, some two decades after they were added to SSLv2.

Logjam redux

The other crucial ingredient in DROWN is the addition of extremely weak 40-bit symmetric encryption to SSLv2 as mandated by Clinton administration restrictions on the export of encryption software. Along with the Bleichenbacher weakness, the export-grade ciphersuites make it possible to brute-force decrypt the intercepted TLS communications. Together with last year's Logjam vulnerability, DROWN underscores the danger of adding deliberately weakened ciphers to production software specifications, even when people presume those specifications are no longer in use.

"Our results illustrate, like FREAK and Logjam, the continued harm that a legacy of deliberately weakened export-grade cryptography inflicts on the security of modern systems, even decades after the regulations influencing the original design were lifted," the researchers wrote in their paper. "The

MAIN MENU MY STORIES: 24 FORUMS SUBSCRIBE JOBS

they would be at the limits of the computational power available to an attacker. The technical debt induced by cryptographic 'front doors' has left implementations vulnerable for decades."

DROWN is only the latest attack to demonstrate troubling weaknesses in what's arguably the Internet's most important security measure. Other attacks include: BEAST in 2011, CRIME in 2012, TIME, Lucky 13, BREACH in 2013, POODLE in 2014, last year's FREAK, and Logjam. TLS serves as a sole means for most websites and e-mail servers to encrypt and authenticate traffic as it passes over the Internet.

DROWN was developed by researchers at Tel Aviv University, Munster University of Applied Sciences, Ruhr University Bochum, the University of Pennsylvania, the Hachcat project, the University of Michigan, Two Sigma, Google, and the OpenSSL Project. Besides underscoring the dangers of deliberately weakened crypto, DROWN demonstrates the problems that result when obsolete protocols and specifications aren't explicitly forbidden and instead are allowed to be called on in what developers assume are special cases. Cryptographers have long been reluctant to disable old SSL and TLS specifications, particularly as applied to e-mail servers, out of concern the move will kill backward compatibility with servers that haven't been updated. The thinking was that even less optimal encryption was better than none at all. DROWN shows that outdated crypto specifications have the ability to completely torpedo TLS sessions that otherwise are believed to be robust.

"DROWN shows that sometimes, bad crypto is even worse than no crypto," Graham Steel, cofounder and CEO of crypto software provider Cryptosense, told Ars. "Hopefully, DROWN will strengthen the general movement to eliminate weak crypto all over the Internet."

Post updated to change the number of servers estimated to be vulnerable, as reflected in the most recent Internet scans.

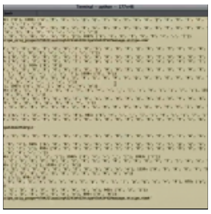
READER COMMENTS 24

Share 80 Tweet Email Google 7 Reddit 0

Dan Goodin / Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.
@dangoodin001 on Twitter

← OLDER STORY NEWER STORY →

YOU MAY ALSO LIKE



Crack in Internet's foundation of trust allows HTTPS session hijacking

HTTPS-crippling attack threatens tens of thousands of Web and mail servers

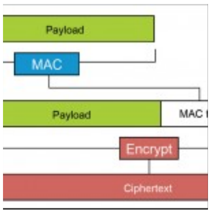
Still reeling from Heartbleed, OpenSSL suffers from crypto bypass flaw

Why you probably shouldn't be doing work on that in-flight Wi-Fi

"FREAK" flaw in Android and Apple devices cripples HTTPS crypto protection

Apple prevails in forced iPhone unlock case in New York court

HTTPS-crippling FREAK attacks become cheaper and easier to carry out



"Lucky Thirteen" attack snarfs cookies protected by SSL encryption

SITE LINKS
About Us
Advertise with us
Contact Us
Reprints

MORE READING
RSS Feeds
Newsletters
Visit Ars Technica UK

CONDE NAST SITES
Reddit
Wired
Vanity Fair
Style

SUBSCRIPTIONS

Subscribe to Ars

Details

Visit our sister sites

Subscribe to a magazine

VIEW MOBILE SITE

CONDÉ NAST

Ad Choices