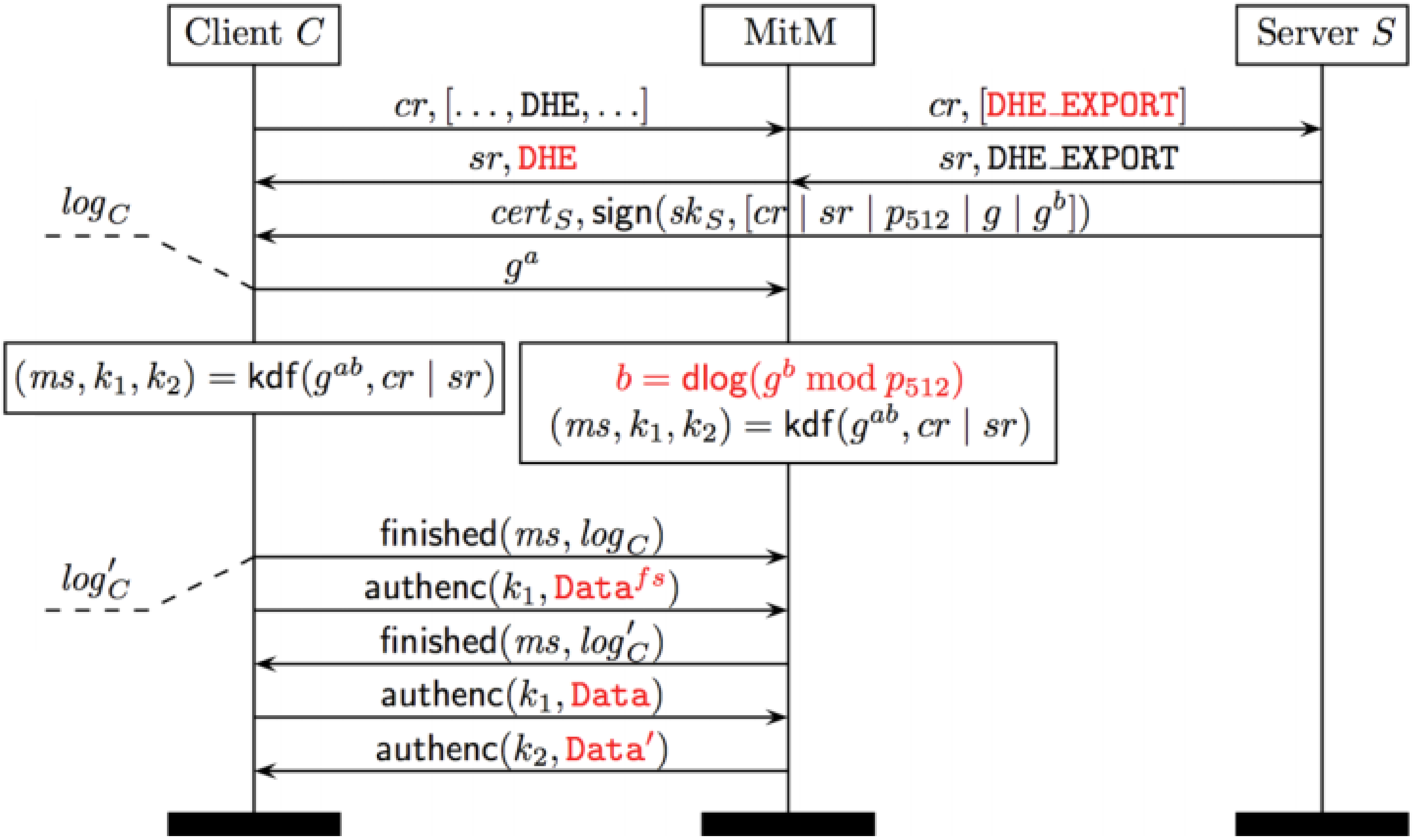
Security Now! #509 - 05-26-15

LOGJAM: Imperfect Forward Secrecy

This week on Security Now!

- Let's Encrypt's Terms of Service.
- Another worrisome consumer router flaw.
- The Government Backdoor debate continues.
- More on Chris Roberts, the whacky airliner hacker.
- Blocking scripts on Chrome.
- A few passive keyless entry & start follow-ups.
- Some fun miscellany... **and LOGJAM!**

"LOGJAM" leverages a weakness in the TLS protocol, allowing a man in the middle to make an undetected change in the strength of the negotiated ciphersuite:



Client C
MitM
Server S
$cr, [\ldots, \mathsf{DHE}, \ldots]$
$cr, [\mathsf{DHE\_EXPORT}]$
sr, DHE
$sr, \mathsf{DHE\_EXPORT}$
log_C
$cert_S, \mathsf{sign}(sk_S, [cr \mid sr \mid p_{512} \mid g \mid g^b])$
g^a
$(ms, k_1, k_2) = \mathsf{kdf}(g^{ab}, cr \mid sr)$
$b = \mathsf{dlog}(g^b \bmod p_{512})$
$(ms, k_1, k_2) = \mathsf{kdf}(g^{ab}, cr \mid sr)$
$\mathsf{finished}(ms, log_C)$
log'_C
$\mathsf{authenc}(k_1, \mathsf{Data}^{fs})$
$\mathsf{finished}(ms, log'_C)$
$\mathsf{authenc}(k_1, \mathsf{Data})$
$\mathsf{authenc}(k_2, \mathsf{Data}')$

Security News

Draft Let's Encrypt Subscriber Agreement

- https://letsencrypt.org/2015/05/21/draft-le-sa.html
- https://letsencrypt.org/LE-Draft-SA-May-21-2015.pdf
- Short 6-page, actually readable, legal agreement.
- Agreement in effect only so long as your certificates are.
- User's Warranties under this agreement:
  - You Warrant to ISRG (Internet Security Research Group) and the public-at-large that You are the legitimate registrant of the Internet domain name that is, or is going to be, the subject of Your Certificate, or that You are the duly authorized agent of such registrant.
  - You Warrant to ISRG and the public-at-large that You have not participated in the seizure of a domain name that had ongoing lawful uses.
  - You Warrant that all information in Your Certificate regarding You or Your domain name is accurate, current, reliable, complete, and not misleading.
  - You Warrant that all information You have provided to ISRG is accurate, current, complete, reliable, complete, and not misleading.
  - You Warrant that You rightfully hold the Private Key corresponding to the Public Key listed in Your Certificate.
  - You Warrant that You have taken all appropriate, reasonable, and necessary steps to secure and keep your Private Key secret.
  - You Warrant that You will not use Your Certificates to attack, defraud or intercept the traffic of others.

- **Use of Your Certificate:** The purpose of Your Certificate is to encrypt Internet communications. You are responsible for all legal and other consequences associated with the use of Your Certificate. You agree that You will not use Your Certificate for fail-safe performance, such as the operation of utilities or power facilities, air traffic control or navigation, weapons systems, or any other system, the failure of which would reasonably be expected to lead to injury or property damage.

- **When to Revoke Your Certificate:** You must immediately request that Your Certificate be revoked if: (i) You suspect or discover that Your Private Key has been, or is in danger of being, lost, stolen, otherwise compromised, or subjected to unauthorized use or (ii) any information in Your Certificate is no longer accurate, current, complete, or becomes misleading. You may make a revocation request to ISRG using ACME Client Software. You should also notify anyone who may have relied upon Your use of Your Certificate that Your encrypted communications may have been subject to compromise.

- **When to Cease Using Your Certificate:** You must immediately cease using Your Certificate if: (i) You suspect or discover that the Private Key corresponding to Your Certificate has been or may be stolen, lost, otherwise compromised, or subjected to unauthorized use, (ii) any information in Your Certificate is no longer accurate, current, complete, or becomes misleading, or (iii) upon the revocation or expiration of Your Certificate.

NetUSB bug

- Millions of Routers Vulnerable to Attacks Due to NetUSB Bug
- http://www.securityweek.com/millions-routers-vulnerable-attacks-due-netusb-bug
- NetUSB is USB over IP allows users to connect over their network to USB devices plugged into a router, access point, or other Linux-based embedded system. Users can access speakers, printers, hard drives, webcams and other USB devices by connecting to a NetUSB server via the Windows or OS X client.
- Company: KCodes is the provider of the technology.
- NetUSB driver has a buffer overflow vulnerability in the kernel that can be exploited by an unauthenticated attacker to execute arbitrary code or cause a denial-of-service (DoS) condition. The flaw, caused by insufficient input validation, can be triggered by specifying a computer name that is longer than 64 characters when the client connects to the server.
- Router OEMs: D-Link, Netgear, TP-Link, ZyXEL, and TRENDnet
    - Print Sharing, USB share port or ReadySHARE.
- If your router has a USB connection for network sharing of USB-attached peripherals, there's almost certainly a problem.
- LOCAL network exploit... but some routers are known to expose this to the WAN side as well!
- Michael Horowitz @defensivecomputing (ComputerWorld)
    - @SGgrc Test your #router for public (WAN side) exposure to #NetUSB flaw with https://www.grc.com/x/portprobe=20005

The Government Encryption Backdoor debate continues.

Techdirt reports (with attitude):

- https://www.techdirt.com/articles/20150518/21180031044/pretty-much-anyone-with-any-understanding-crypto-tells-president-obama-that-backdooring-crypto-is-monumentally-stupid.shtml
- Headline: “Pretty Much Anyone With Any Understanding Of Crypto Tells President Obama That Backdooring Crypto Is Monumentally Stupid”
- Nearly 150 tech companies and cryptography experts signed the letter:
    - Google, Apple, Cisco, Microsoft, Twitter and Facebook
    - Phil Zimmermann (who lived through this sort of thing before), Whitfield Diffie (who invented public key cryptography), Ron Rivest, Bruce Schneier, Matt Blaze, Richard Clarke (long-time counterterrorism guy in the White House)
- https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf

And then...

- “FBI Director Claims That The World's Most Knowledgeable Cybersecurity Experts Are Not 'Fair Minded' About Encryption Backdoors”
- https://www.techdirt.com/articles/20150521/18021531082/fbi-director-claims-that-worlds-most-knowledgeable-cybersecurity-experts-are-not-fair-minded-about-encryption-backdoors.shtml
- FBI Director, James Comey, responds…
    - A group of tech companies and some prominent folks wrote a letter to the

> President yesterday that I frankly found depressing. Because their letter contains no acknowledgment that there are societal costs to universal encryption. Look, I recognize the challenges facing our tech companies. Competitive challenges, regulatory challenges overseas, all kinds of challenges. I recognize the benefits of encryption, but I think fair-minded people also have to recognize the costs associated with that. And I read this letter and I think, "Either these folks don't see what I see or they're not fair-minded." And either one of those things is depressing to me. So I've just got to continue to have the conversation.
>
> We've got to have a conversation long before the logic of strong encryption takes us to that place. And smart people, reasonable people will disagree mightily. Technical people will say it's too hard. My reaction to that is: Really? Too hard? Too hard for the people we have in this country to figure something out? I'm not that pessimistic. I think we ought to have a conversation.

- Techdirt editorializes:
  - Hey, Comey! No one is saying it's "too hard." They're saying it's IMPOSSIBLE to do this without weakening everyone's security. Impossible. It's not a "hard" problem, it's an impossible problem. Because if you weaken security to let the FBI in, by definition you are weakening the security to let others in as well. That's the point that was being made.

More on Chris Roberts:

- 'Plane hacker' Chris Roberts claims he hacked into the International Space Station
  - http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11620237/Plane-hacker-Chris-Roberts-claims-he-hacked-into-the-International-Space-Station.html
- Anatomy of a Story: Why the 'Airliner Hacking' Claim is Bull
  - http://www.nycaviation.com/2015/05/anatomy-story-airliner-hacking-claim-bull/#.VV35Ms4-DVo

"ScriptBlock" for Chrome

https://chrome.google.com/webstore/detail/scriptblock/hcdjknjpbnhdoabbngpmfekaecnpajba

PKES Follow-ups (Passive Keyless Entry & Start)

Pu Leather Cell Phone Anti-tracking Anti-spying GPS Rfid Signal Blocker Pouch Case Bag Handset Function Bag Black

- http://www.amazon.com/gp/product/B00ITRBV54/

FOBGuard

- http://www.fobguard.com/

AndyFerguson (@AndyFerguson) · 3:54pm · 21 May 2015 · Twitter for iPad

- @SGgrc An empty Altoids tin also works nicely!!

Kyle Boroff (@jimmyjazz2005)

- My ford gets broken into once a week in front of my own house. I always locked didn't know how they got in, now I know. faraday bag on order

Miscellany:

Why 3D hasn't obtained much traction...

- Is it a bit like "Quadrophonic" was in the 80's ??

Blockwick for iOS *(Blockwick 101 is free)*

- Blockwick 2 (also for Android) looks gimmicky and much less wonderful.

antd (@antdq)

- Hi, please consider sharing more health information. I haven't been sick in 2 years since Vit D3 (due to you); used to have very bad health :)

SpinRite:

av440studios (@ArtVandelay440)

- @SGgrc We just recovered over 1TB of potentially lost family pictures and home movies thanks to SpinRite. Best $89 spent of my life!
  5:36pm · 16 May 2015 · Twitter Web Client

Simmo3D (@Simmo3D)

- @SGgrc I recommended a friend purchase SpinRite to recover their drive and it fixed their issues with bad sectors. #youralegend
  7:06pm · 17 May 2015 · Twitter for Windows Phone

Logjam: Imperfect Forward Secrecy

Links:

Official Site: https://weakdh.org/

- Matthew Green: http://blog.cryptographyengineering.com/2015/05/attack-of-week-logjam.html
- https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained/
- https://blog.digicert.com/logjam-attack/
- http://www.computerworld.com/article/2924185/malware-vulnerabilities/logjam-encryption-flaw-puts-web-surfers-at-risk.html

The nature of the exposure:

- 8.4% of the Top 1 Million domains were initially vulnerable.
- The researchers created a precomputation against the most common 512-bit prime used for TLS and demonstrate that the Logjam attack can be used to downgrade connections to 80% of TLS servers supporting DHE_EXPORT.
- They further estimate that an academic team can break a 768-bit prime and that a nation-state can break a 1024-bit prime.
- Breaking the single, most common 1024-bit prime used by web servers would allow passive eavesdropping on connections to 18% of the Top 1 Million HTTPS domains.
- A second prime would allow passive decryption of connections to 66% of VPN servers and 26% of SSH servers.
- A close reading of published NSA leaks shows that the agency's attacks on VPNs are consistent with having achieved such a break.

What:

- Key exchanges:
    - Static RSA
    - Ephemeral Diffie-Hellman (DHE)
    - Elliptic-Curve Epheeral Diffie-Hellman (ECDHE)
- Non-EC Diffie-Hellman key exchange (DHE).
    - Discrete Logarithm Problem.
    - Exponentiation: G^a^b == G^b^a
        - modulus a mutually agreed upon prime 'p'
    - G and p can (and are) publicly known.

g^a mod p

Setup:

- Server is "default configured" and still supports DHE_EXPORT key agreement cipher suites.
- But we assume that's okay, because no browser clients offer any of those to any server.

Downgrade attack:

- In the ClientHello: Client offers a list of cipher suites, NOT INCLUDING any DHE_EXPORT.
- MITM intercepts the ClientHello list, removes all others and offers only DHE_EXPORT.
- Server shrugs and agrees. In it's (unsigned) ServerHello, it agrees to use DHE_EXPORT.
- The MITM now modifies the server's ServerHello back to one of the DHE's the client offered.
- The server then picks DHE parameters and DOES sign them... but the defect in TLS <= v1.2 is that the server's signed parameters do NOT include any indication of the cipher suite that those parameters are for.
- Only each side's FINISHED handshake message contains the MAC for the entire transcript to prove to each other that they saw all of the same data -- specifically to thwart any man-in-the-middle. But if the attacker can crack the key quickly enough... they can spoof the proper MAC to the client.

NFS: Number Field Sieve

- Uses a technique known as "index calculus" involving 4 stages, each with differing computational requirements... but where the first 3 stages are ONLY dependent upon the value of the prime 'p'.
- It turns out that almost ALL of the time consuming work occurs during those first 3 stages.

Top 512-bit DH Primes for TLS

- 8% of Alexa's top 1 million sites allow DHE_EXPORT.
- Of those 8%, 92% use one of two never-changing primes:
    - Apache -- 82%
      9fdb8b8a004544f0045f1737d0ba2e0b274cdf1a9f588218fb435316a16e3741
      71fd19d8d8f37c39bf863fd60e3e300680a3030c6e4c3757d08f70e6aa871033
    - mod_ssl -- 10%
      d4bcd52406f69b35994b88de5db89682c8157f62d8f33633ee5772f11f05ab22
      d6b5145b9f241e5acc31ff090a4bc71148976f76795094e71e7903529f5a824b

WHY are so many servers (and VPNs and SSH and IPSec) using a single fixed prime modulus?

- It's easier than coming up with a new prime.
- It wasn't believed to be a problem.
- <quote from the paper>
  The NFS algorithm for discrete logarithms allows an attacker to perform a single precomputation, after which computing individual logs in that group has a much lower marginal cost. Although the cheaper cost of individual discrete logs was known to cryptographers, it appears to not have been as widely understood by implementers.

  Indeed, many implementations believed RSA key exchange to be inferior to Diffie-Hellman, which offered forward secrecy. Ironically, the opposite appears to be true: for a medium-value target, a fresh, well-generated 1024-bit RSA key would be significantly more expensive to factor than a 1024-bit discrete log in a group for which precomputation has already been done.

  A key lesson from this state of affairs is that cryptographers and creators of practical systems need to communicate better. Systems builders should be aware of the difficulty of cryptographic attacks and tradeoffs, and cryptographers should be aware of how systems are actually being implemented and used in practice.

Mitigation:

- Simply modify clients not to EVER accept 512-bit primes ('p') from the server. Period.
- Quoting from the paper:
  We notified both client and server software developers of the vulnerabilities discussed in this work. As a result of our disclosure, Microsoft Internet Explorer [36], Mozilla Firefox, and Google Chrome have increased the minimum size of the groups they accept for DHE to 1024 bits, and OpenSSL and Apple Safari are expected to follow suit.

On the server side, we notified Apache, Oracle, IBM, Cisco, and various hosting providers. Akamai has removed all support for export ciphersuites. In the medium-term, many TLS developers plan to support a new extension that allows clients and servers to negotiate a few well-known groups of size 2048-bits and higher, and to gracefully reject weak ones

Is the NSA breaking 1024-bit DH?

- Knowing what we know now... many of the puzzling and questionable assertions leaked in the Edward Snowden documents suddenly seem much less puzzling and questionable.

On the NSA / FBI / US law enforcement as our adversary…

Alex Neihaus (@yobyot) 6:26am · 21 May 2015

- Running IIS on @windowsserver? #Logjam is yet another reason to use the @SGgrc cipher suite order: http://bit.ly/grcciphers Thanks, Steve.