



Imperfect Forward Secrecy:

How Diffie-Hellman Fails in Practice

David Adrian Karthikeyan Bhargavan Zakir Durumeric Pierrick Gaudry Matthew Green
J. Alex Halderman Nadia Heninger Drew Springall Emmanuel Thomé Luke Valenta
Benjamin VanderSloot Eric Wustrow Santiago Zanella-Béguelink Paul Zimmermann

Pete Guan

PRESENTATION CONTENT



01. Background

- 01-1. What is Diffie-Hellman
- 01-2. What makes Diffie-Hellman less security

02. Logjam Attack

- 02-1. The Number Field Sieve Algorithm
- 02-2. TLS Cipher Version Down-grade

03. Who is Affected?

- 03-1. Who is still supporting DHE_EXPORT
- 03-2. Websites use common group primes

04. What Should I Do?

- 04-1. If you run a server...
- 04-2. If you use a browser...
- 04-3. If you're a sysadmin or developer ...



01

BACKGROUND

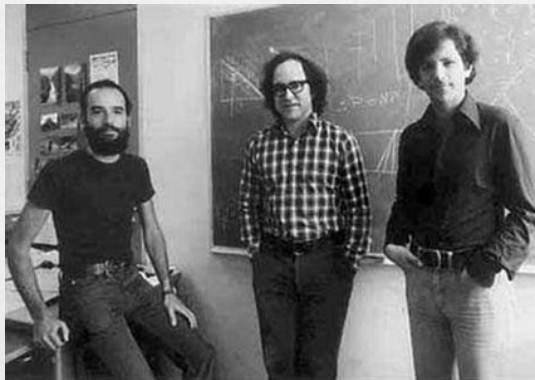
Let's talk about Diffie-Hellman

Diffie-Hellman key exchange is widely used to establish session keys in Internet protocols. It is the main key exchange mechanism in SSH and IPsec and a popular option in TLS. We examine how Diffie-Hellman is commonly implemented and deployed with these protocols and find that, in practice, it frequently offers less security than widely believed.

1.1 What is Diffie-Hellman?

BACKGROUND

- Diffie–Hellman is a specific method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle and named after Whitfield **Diffie** and Martin **Hellman**.



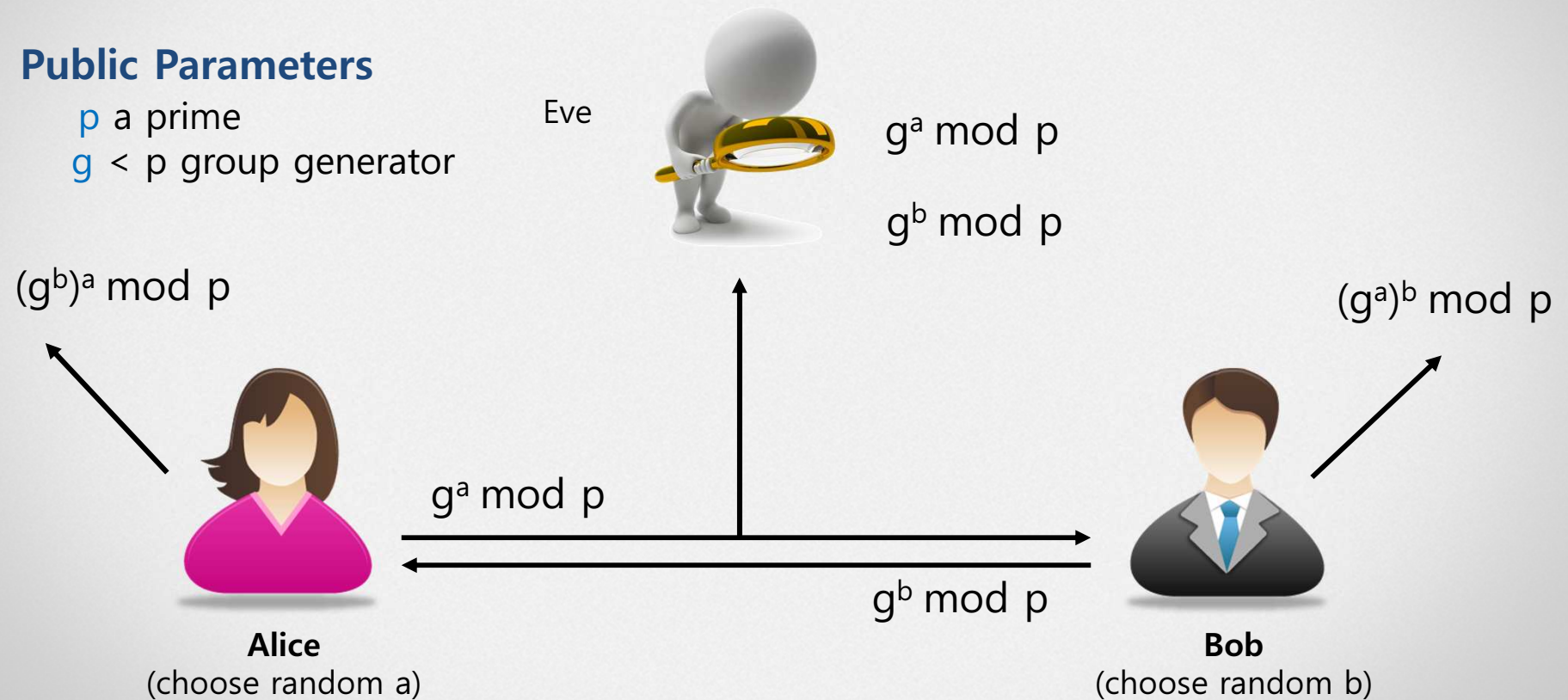
1.1 What is Diffie-Hellman?

BACKGROUND

Public Parameters

p a prime

$g < p$ group generator



1.1 What is Diffie-Hellman?

BACKGROUND

1. Alice and Bob agree to use a modulus $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).
2. Alice chooses a secret integer $a = 6$, then sends Bob $A = g^a \bmod p$
 $A = 5^6 \bmod 23 = 8$
3. Bob chooses a secret integer $b = 15$, then sends Alice $B = g^b \bmod p$
 $B = 5^{15} \bmod 23 = 19$
4. Alice computes $s = B^a \bmod p$
 $s = 19^6 \bmod 23 = 2$
5. Bob computes $s = A^b \bmod p$
 $s = 8^{15} \bmod 23 = 2$
6. Alice and Bob now share a secret

Both Alice and Bob have arrived at the same value s , because, under mod p ,

$$A^b \bmod p = g^{ab} \bmod p = g^{ba} \bmod p = B^a \bmod p^{[9]}$$

More specifically,

$$(g^a \bmod p)^b \bmod p = (g^b \bmod p)^a \bmod p$$

CG1

Note that only a , b , and $(gab \bmod p = gba \bmod p)$ are kept secret. All the other values – p , g , $ga \bmod p$, and $gb \bmod p$ – are sent in the clear. Once Alice and Bob compute the shared secret they can use it as an encryption key, known only to them, for sending messages across the same open communications channel.

Chenghuachen Guan, 2017/2/21

1.1 What is Diffie-Hellman?

BACKGROUND

How much time does it take to break?

- 512-bit = 10 core years
- 768-bit = 35,000 core years
- 1024-bit = 45,000,000 core years
- 2048-bit = recommended currently

1.2 What makes Diffie-Hellman less security?

BACKGROUND

DHE_EXPORT

- It so happens that in previous century, there were some rather strict US export regulations on crypto, and this prompted "export cipher suites."
- In particular, some cipher suites that use DHE and mandate a DH modulus of no more than 512 bits.
- Reusing the same modulus as everybody else is not a big issue.



02

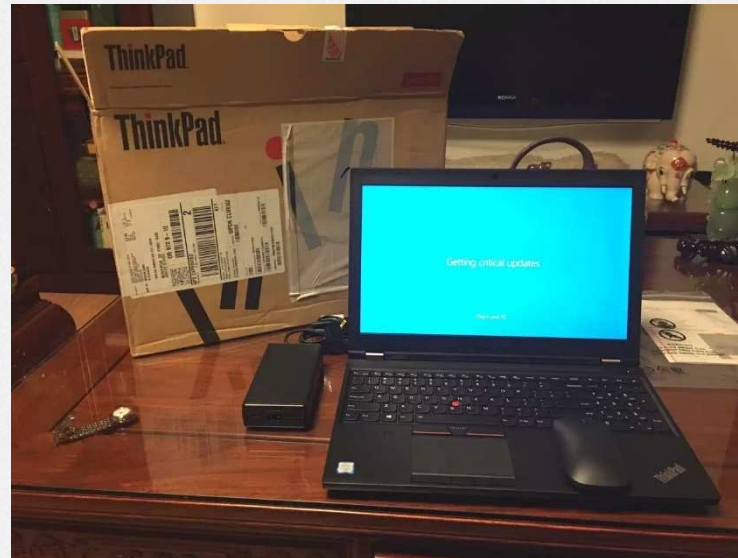
LOGJAM ATTACK

The new attack that makes DHE imperfect

Diffie-Hellman key exchange is widely used to establish session keys in Internet protocols. It is the main key exchange mechanism in SSH and IPsec and a popular option in TLS. We examine how Diffie-Hellman is commonly implemented and deployed with these protocols and find that, in practice, it frequently offers less security than widely believed.

2.1 The Number Field Sieve Algorithm

LOGJAM ATTACK



$$(10 * 365 * 24) / 16 = 7300 \text{ hours}$$

2.1 The Number Field Sieve Algorithm

LOGJAM ATTACK



Specifications	
Essentials	
Status	Launched
Launch Date	June 6, 2016
Processor Number	E7-8890V4
Cache	60 MB
Bus Speed	9.6 GT/s QPI
# of QPI Links	3
Instruction Set	64-bit
Instruction Set Extensions	AVX2.0
Embedded Options Available	No
Lithography	14 nm
Scalability	S85
Recommended Customer Price	\$7174.00

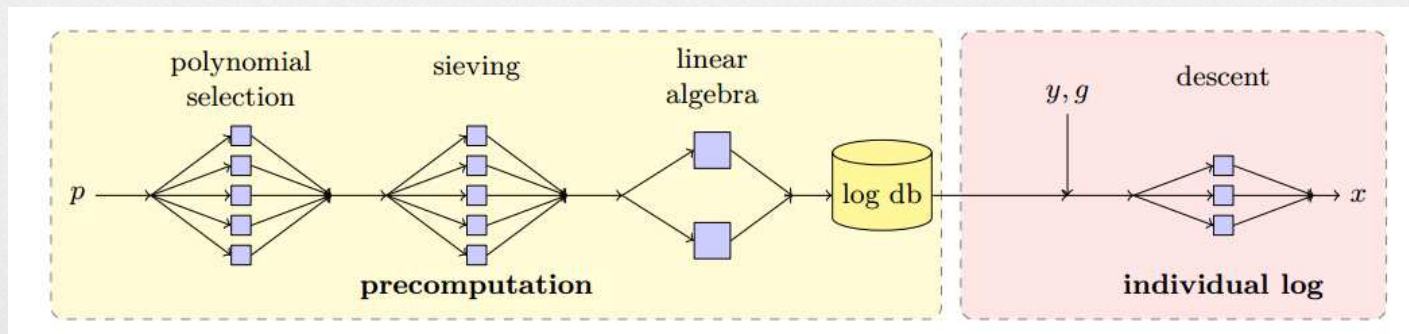
Performance	
# of Cores	24
# of Threads	48
Processor Base Frequency	2.2 GHz
Max Turbo Frequency	3.4 GHz
TDP	165 W

$$(10 * 365 * 24) / 48 = 1825 \text{ hours}$$

2.1 The Number Field Sieve Algorithm

LOGJAM ATTACK

The number field sieve algorithm for discrete log consists of a precomputation stage that depends only on the prime p and a descent stage that computes individual logs. With sufficient precomputation, an attacker can quickly break any Diffie-Hellman instances that use a particular p . ($y = g^a \bmod p$)



<https://math.dartmouth.edu/~carlp/PDF/paper99.pdf>

2.1 The Number Field Sieve Algorithm

LOGJAM ATTACK

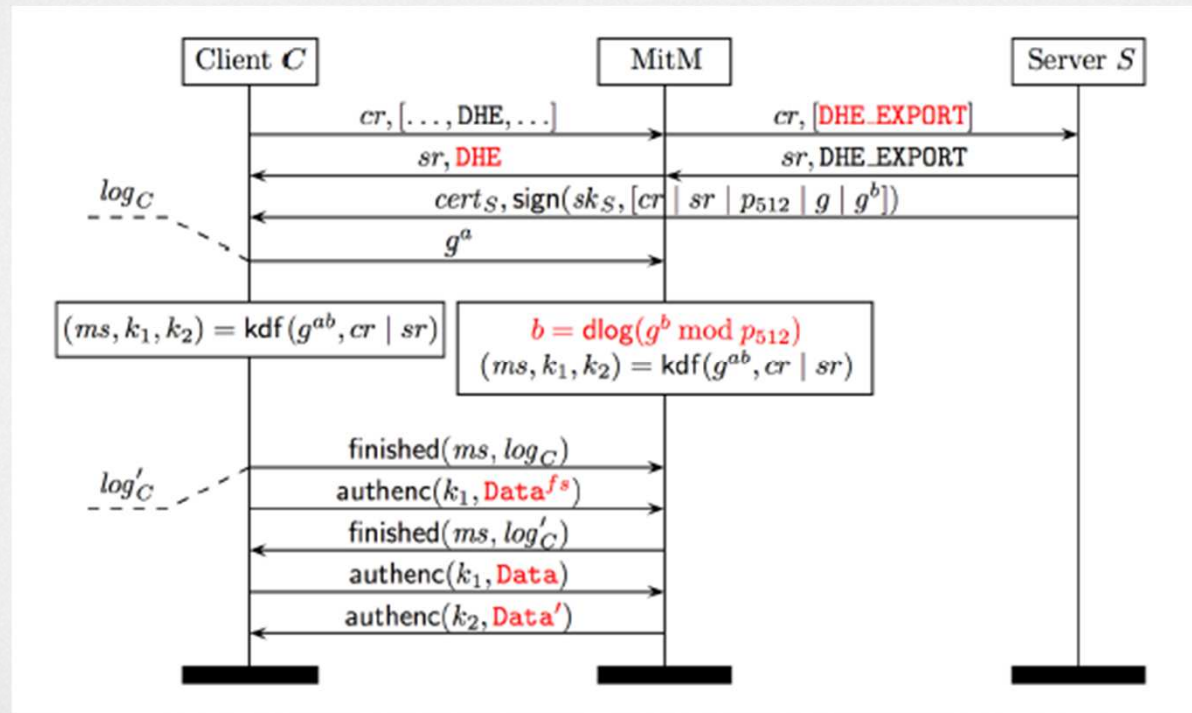
- Carried out precomputation for Apache, mod_ssl, OpenSSL primes

	polysel	sieving	linalg	Descent
	2000-3000 cores		288 cores	36 cores
DH-512	3 hours	15 hours	120 hours	70 seconds

- The authors needed several thousand CPU cores for a week to precompute data for a single 512-bit prime.
- After 1 week precomputation, median individual log time 70s

2.2 TLS Cipher Vision Down-grade

LOGJAM ATTACK



2.2 TLS Cipher Vision Down-grade

LOGJAM ATTACK

Source	Popularity	Prime
Apache	82%	9fdb8b8a004544f0045f1737d0ba2e0b 274cdf1a9f588218fb435316a16e3741 71fd19d8d8f37c39bf863fd60e3e3006 80a3030c6e4c3757d08f70e6aa871033
mod_ssl	10%	d4bcd52406f69b35994b88de5db89682 c8157f62d8f33633ee5772f11f05ab22 d6b5145b9f241e5acc31ff090a4bc711 48976f76795094e71e7903529f5a824b
(others)	8%	(463 distinct primes)

Top 512-bit DH primes for TLS. 8.4% of Alexa Top 1M HTTPS domains allow DH E_EXPORT, of which 92.3% use one of the two most popular primes, shown here.

2.2 TLS Cipher Vision Down-grade

LOGJAM ATTACK



From published Snowden documents that suggests NSA may already be exploiting 1024-bit Diffie-Hellman to decrypt VPN traffic.



03

Who is Affected?

The new attack that makes DHE imperfect

Diffie-Hellman key exchange is widely used to establish session keys in Internet protocols. It is the main key exchange mechanism in SSH and IPsec and a popular option in TLS. We examine how Diffie-Hellman is commonly implemented and deployed with these protocols and find that, in practice, it frequently offers less security than widely believed.

03-1. Who is still supporting DHE_EXPORT

Who is Affected?

Websites, mail servers, and other TLS-dependent services that support **DHE_EXPORT** ciphers are at risk for the Logjam attack. We use Internet-wide scanning to measure who is vulnerable.

Protocol	Vulnerable to Logjam
HTTPS — Top 1 Million Domains	8.4%
HTTPS — Browser Trusted Sites	3.4%
SMTP+StartTLS — IPv4 Address Space	14.8%
POP3S — IPv4 Address Space	8.9%
IMAPS — IPv4 Address Space	8.4%

03-2. Websites use common group primes

Who is Affected?

Websites that use one of a few commonly shared 1024-bit Diffie-Hellman groups may be susceptible to passive eavesdropping from an attacker with nation-state resources. Here, we show how various protocols would be affected if a single 1024-bit group were broken in each protocol, assuming a typical up-to-date client

	Vulnerable if most common 1024-bit group is broken
HTTPS — Top 1 Million Domains	17.9%
HTTPS — Browser Trusted Sites	6.6%
SSH — IPv4 Address Space	25.7%
IKEv1 (IPsec VPNs) — IPv4 Address Space	66.1%

04

What Should I Do?

How to avoid Logjam attack

The findings indicate that one of the key recommendations from security experts in response to the threat of mass surveillance— promotion of DHE-based TLS ciphersuites offering “perfect forward secrecy” over RSA-based ciphersuites—may have actually reduced security for many hosts. In this section, we present concrete recommendations to recover the expected security of Diffie-Hellman as it is used in mainstream Internet protocols.



04-1. If you run a server...

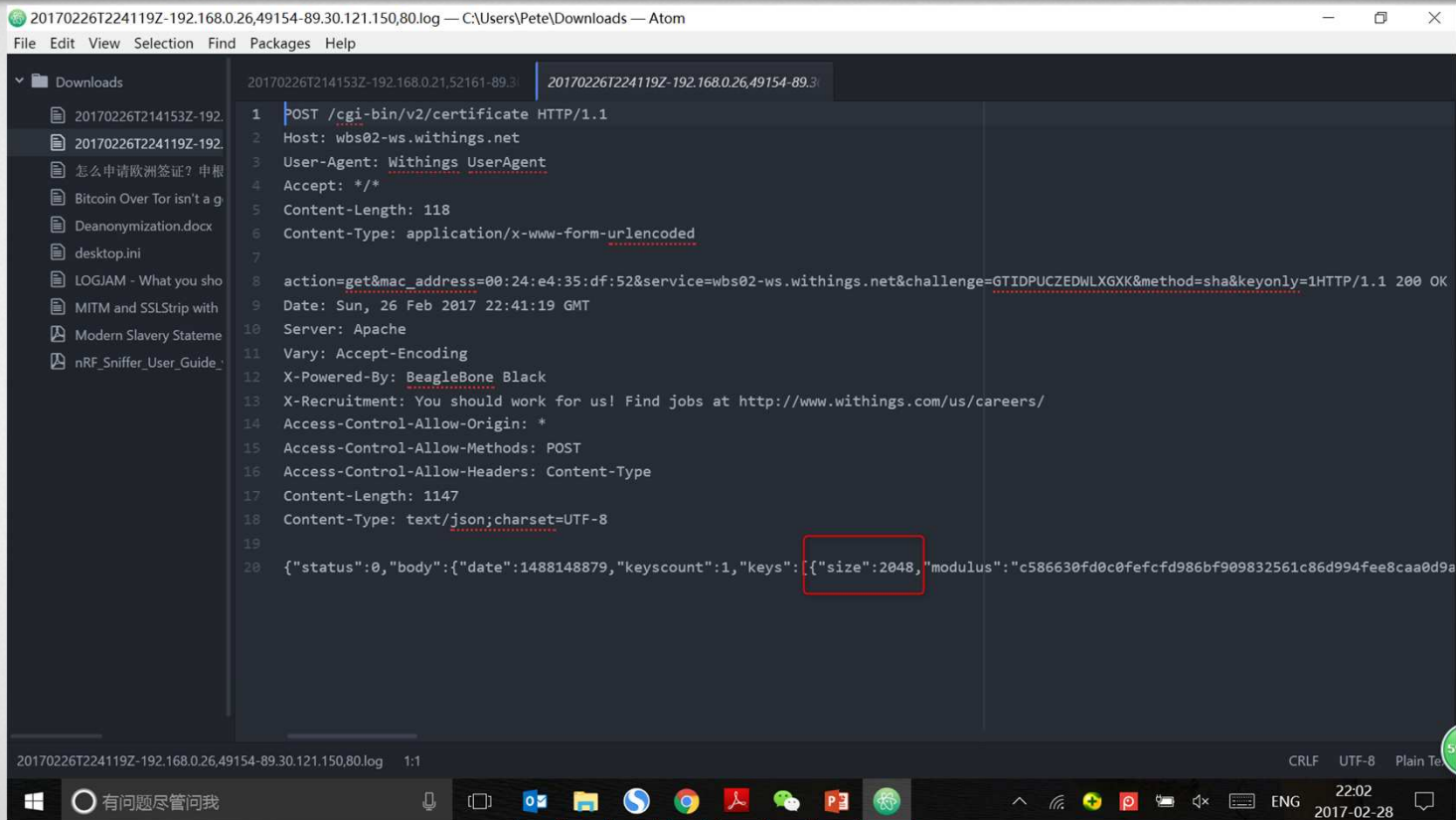
What Should I Do?

If you run a server...

- If you have a web or mail server, you should disable support for export cipher suites and use a 2048-bit Diffie-Hellman group.

04-1. If you run a server...

What Should I Do?



```
20170226T224119Z-192.168.0.26,49154-89.30.121.150,80.log — C:\Users\Pete\Downloads — Atom
File Edit View Selection Find Packages Help

20170226T214153Z-192.168.0.21,52161-89.30.121.150,80.log 20170226T224119Z-192.168.0.26,49154-89.30.121.150,80.log
1 POST /cgi-bin/v2/certificate HTTP/1.1
2 Host: wbs02-ws.withings.net
3 User-Agent: Withings UserAgent
4 Accept: */*
5 Content-Length: 118
6 Content-Type: application/x-www-form-urlencoded
7
8 action=get&mac_address=00:24:e4:35:df:52&service=wbs02-ws.withings.net&challenge=GTIDPUCZEDWLXGK&method=sha&keyonly=1HTTP/1.1 200 OK
9 Date: Sun, 26 Feb 2017 22:41:19 GMT
10 Server: Apache
11 Vary: Accept-Encoding
12 X-Powered-By: BeagleBone Black
13 X-Recruitment: You should work for us! Find jobs at http://www.withings.com/us/careers/
14 Access-Control-Allow-Origin: *
15 Access-Control-Allow-Methods: POST
16 Access-Control-Allow-Headers: Content-Type
17 Content-Length: 1147
18 Content-Type: text/json; charset=UTF-8
19
20 {"status":0,"body":{"date":1488148879,"keyscount":1,"keys":[{"size":2048,"modulus":"c586630fd0c0fefcfd986bf909832561c86d994fee8caa0d9a
```


04-2. If you use a browser...

What Should I Do?

If you run a browser...

- Make sure you have the most recent version of your browser installed, and check for updates frequently.
- Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, and Apple Safari are all deploying fixes for the Logjam attack.

04-3. If you're a sysadmin or developer ...

What Should I Do?

If you're a sysadmin or developer ...

- Make sure any TLS libraries you use are up-to-date, that servers you maintain use 2048-bit or larger primes, and that clients you maintain reject Diffie-Hellman primes smaller than 1024-bit.



THANK YOU