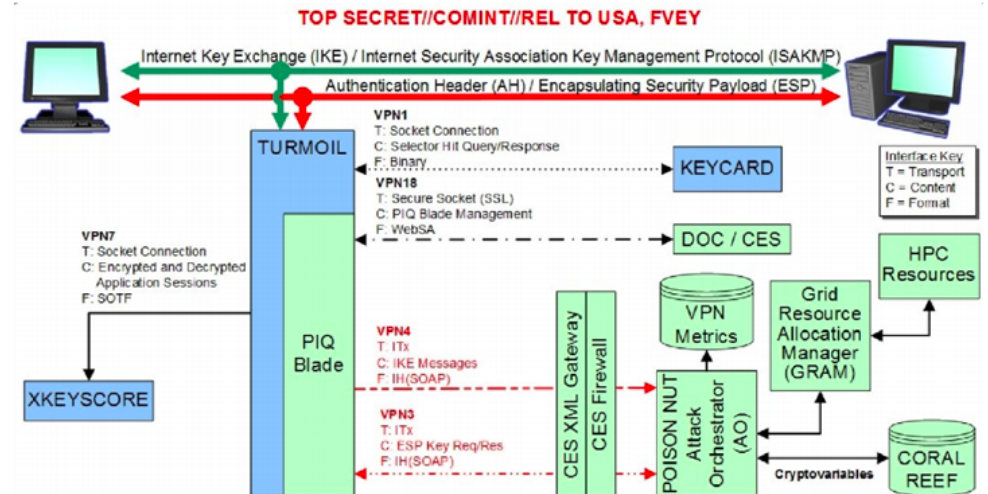




How NSA successfully Broke Trillions of Encrypted Connections

Friday, October 16, 2015 Swati Khandelwal

[G+](#) 437 [Like](#) 7.9k [Share](#) 7787 [Tweet](#) 939 [Share](#) 158 [Share](#) 35.6K



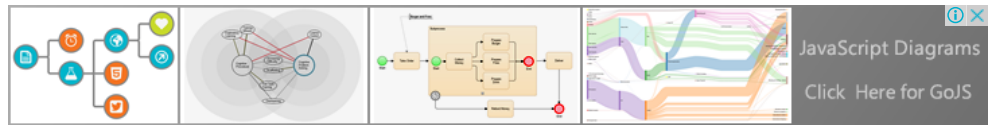
Yes, it seems like the mystery has been solved.

We are aware of the United States *National Security Agency (NSA)* powers to break almost unbreakable encryption used on the Internet and intercept nearly Trillions of Internet connections – thanks to the revelations made by whistleblower Edward Snowden in 2013.

However, what we are not aware of is exactly how did the NSA apparently intercept VPN connections, and decrypt SSH and HTTPS, allowing the agency to read hundreds of Millions of personal, private emails from persons around the globe.

Also Read: [Every Call You Make or Text You Send, They'll Be Tracking From Today](#)

Now, computer scientists Alex Halderman and Nadia Heninger have presented a paper at the ACM Conference on Computer and Communications Security that advances the most plausible theory as to how the NSA broke some of the most widespread encryption used on the Internet.



Ads by Google

- [▶ Hacking Password](#)
- [▶ Hacking Software](#)
- [▶ Password Hacker](#)

According to the paper, the NSA has exploited common implementations of the Diffie-Hellman key exchange algorithm – a common means of exchanging cryptographic keys over untrusted channels – to decrypt a large number of HTTPS, SSH, and VPN connections.

Diffie-Hellman – the encryption used for HTTPS, SSH, and VPNs – helps users communicate by swapping cryptographic keys and running them through an algorithm that nobody else knows except the sender and receiver.

Also Read: [NSA will not stop spying on us, next move Quantum computer to break strongest Encryption](#)

It is described as secure against surveillance from the NSA and other state-sponsored spies, as it would take hundreds or thousands of years and by them and a nearly unimaginable amount of money to decrypt directly.

However, a serious vulnerability in the way the Diffie-Hellman key exchange is implemented is allowing the intelligence agencies and spies to break and eavesdrop on trillions of encrypted connections.

To crack just one of the extremely large prime numbers of a Diffie-Hellman in the most commonly used 1024-bit Diffie-Hellman keys would take about a year and cost a few hundred Million dollars.

Also Read: [How to Crack RC4 Encryption in WPA-TKIP and TLS](#)

However, according to researchers, only a few prime numbers are commonly used that might have fit well within the agency's \$11 Billion-per-year budget dedicated to "*groundbreaking cryptanalytic capabilities*."

"Since a handful of primes are so widely reused, the payoff, in terms of connections they could decrypt, would be enormous," said Alex Halderman and Nadia Heninger in a [blog post](#) published Wednesday.

"Breaking a single, 1024-bit prime would allow the NSA to passively decrypt connections to two-thirds of VPNs and a quarter of all SSH servers globally. Breaking a second 1024-bit prime would allow passive eavesdropping on connections to nearly 20% of the top million HTTPS websites. In other words, a one-time investment in massive computation would make it possible to eavesdrop on trillions of encrypted connections."

Around 92% of the top 1 Million Alexa HTTPS domains make use of the same two primes for Diffie-Hellman, possibly enabling the agency to pre-compute a crack on those two prime numbers and read nearly all Internet traffic through those servers.

The Hacker News
 Media/News/Publishing · 802,199 Likes · October 17 at 11:34pm

f Liked

How U.S. Intelligence Agency Cracked and Intercepted Trillions of Encrypted VPN, SSH and HTTPS Connections. Read to Know...

How NSA successfully Broke Trillions of Encrypted Connections

How National Security Agency (NSA) successfully Broke Trillions of Encrypted Connections

THEHACKERNEWS.COM | BY SWATI KHANDLWAL

688 Likes · 31 Comments · 281 Shares

Like
 Comment
 Share

According to the duo, this NSA technological project to crack crypto on a scale has "*not seen since the Enigma cryptanalysis during World War II*."

For in-depth detail, you can read the full paper entitled Imperfect Forward Secrecy: How Diffie-Hellman Fails In Practice [[PDF](#)].

Also Read: [USB Killer v2.0 — Latest USB Device that Can Easily Burn Your Computer](#)

Ads by Google



[▶ Computer Hacking](#)

[▶ Crack](#)

[▶ NSA Surveillance](#)

Crack Encryption, Diffie-Hellman, Encrypted Connection, Encryption, Hacking News, NSA, VPN Software

Join us on Facebook:



You and 802,198 others like this.

ABOUT THE AUTHOR



Swati Khandelwal

Swati Khandelwal is Senior Technical Writer and Cyber Security Analyst at The Hacker News. She is a Technology enthusiast with a keen eye on the Cyberspace and other tech related developments. She is lover of digital culture, gadgets, creative media, technology, and general interest reporting.

ALIEN VAULT

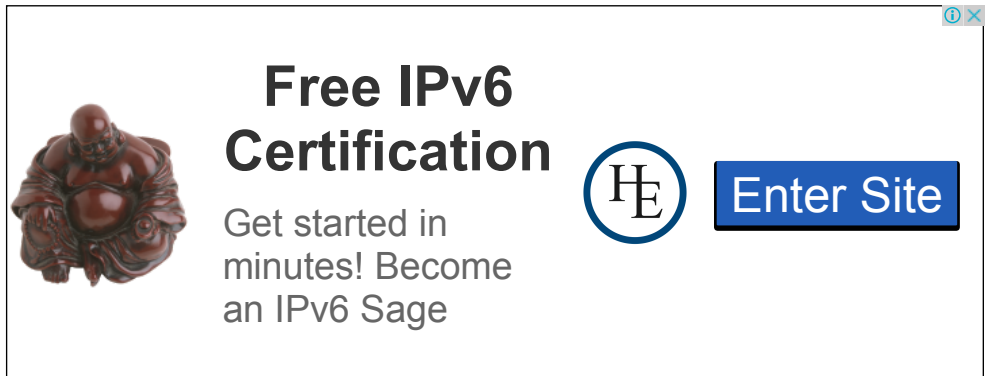
2015 GARTNER MAGIC QUADRANT FOR SIEM

IT'S HERE...
2015 GARTNER MAGIC QUADRANT FOR SIEM

COMPARE THE TOP SIEM VENDORS NOW ▶


SUBSCRIBE TO UPDATE

Want more Interesting Articles to your Inbox every Morning?.

 What's your email?
Sign Me Up


Free IPv6 Certification

Get started in minutes! Become an IPv6 Sage



Enter Site

LATEST STORIES
[ISIS Supporter Hacks 54,000 Twitter Accounts and Posts Details of Heads of the CIA and FBI](#)

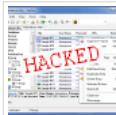
[Hackers have Hacked into US Arrest Records Database](#)

[What is Threat Intelligence and How It Helps to Identify Security Threats](#)

[FBI Deputy Director's Email Hacked by Teenager Who Hacked CIA Chief](#)

[ProtonMail Paid Hackers \\$6000 Ransom in Bitcoin to Stop DDoS Attacks](#)

[Anonymous Group Leaks Identities of 1000 KKK Members](#)
 Fourth, a 16-year-old Hacker,

[Arrested over TalkTalk Hack](#)

[Researcher releases Free Hacking Tool that Can Steal all Your Secrets from Password Manager](#)
COMMENTS**8 Comments****The Hackers News**
 **Исследовательс...**
 Recommend

 Share

Sort by Newest ▾



Join the discussion...

**Buge** · 21 days ago

A>round 92% of the top 1 Million Alexa

HTTPS domains make use of the same two primes for Diffie-Hellman, possibly enabling the agency to pre-compute a crack on those two prime numbers and read nearly all Internet traffic through those servers.

That is a completely false statement.

From the paper:

8.4% of Alexa Top 1M HTTPS domains allow DHE_EXPORT, of which 92.3% use one of the two most popular primes, shown here.

So only 7.7% of top 1M Alexa sites are vulnerable, not 92%. Please learn some reading comprehension.

6 ^ | ▾ · Reply · Share ·

**Samir Itelesfesses** · 22 days ago

Swati Khandelwal,
your articles are really interesting!!
Keep the very good work!

^ | v · Reply · Share ·

**LibertyIsBetter** · 22 days ago

It is a good thing that Congress and the government are looking out from us and protecting us from abuses of power. It is a good thing that the Left and moderate Republicans really believe in the inherent goodness of government and they will monitor themselves. The fact that the IRS was accused of seriously abusing it's powers at the exact same time Lois Lerner's hard drive crashed is pure coincidence. Hillary was looking out for security and the safety of the nation first and her own personal advancement second with the personal unsecured server. Yes, government will look out for us, the people first and themselves...second. Obama, Holder and now Lynch found "Not a smidgeon of corruption." Well, I feel better that the government investigated government corruption and found no corruption of government. It's probably impossible to have abuse of power in the U.S., right? Let's give them more power for our own good.

1 ^ | v · Reply · Share ·

**P4** · 23 days ago

Interesting and terrifying theory very much.

1 ^ | v · Reply · Share ·

**Andrey Arapov** · 23 days ago

Thank you for the article.

Just to clarify this point:

>"Diffie-Hellman – the encryption used for HTTPS, SSH, and VPNs – helps users communicate by swapping cryptographic keys and running them through an algorithm that nobody else knows except the sender and receiver."

Everyone, including sender and receiver know the Diffie-Hellman algorithm and the group. (Otherwise they would not be able to communicate and exchange a shared secret [see below]).

What they do not know is the shared secret key which used to encipher/decipher the data. (The data is then encrypted with some cipher, e.g. AES using that secret key)

DH (Diffie-Hellman) is the key exchange algorithm so that two parties (sender and receiver) can exchange a secret between themselves so that the secret key would never pass over the communication channel (be it secure or insecure communication channel, it does not matter). That's the key point of DH. (You can see how it works in this easy-to-understand DH example <https://github.com/arno01/dhte...>, code is available too)

Since 2010 it was pretty clear that it is time to move from DH primes of 1024 to at least 2048 bits (accepted minimum now).

DH (Diffie-Hellman) primes of 2048 or larger are considered safe. See "5. RECOMMENDATION" on page 11 of the <https://weakdh.org/imperfect-f...>

Here is a good page made by Cisco - "Recommendations for Cryptographic Algorithms"
<http://www.cisco.com/web/about...>

They have also mentioned algorithms that are QCR = quantum computer resistant.

Cheers

5 ^ | v · Reply · Share ·

**Skuly Kido** · 23 days ago

So, basically you have a super secure algorithm, which could have a thousand different keys, which would take years to decrypt every key, but you use 2 of them? Seriously? I'm amazed D:

1 ^ | v · Reply · Share ·

**sehrgut** → Skuly Kido · 21 days ago

Not exactly: the primes are used to parameterize the function. The keys are still random, but the "variant" of the Diffie-Hellman function used is publicly-agreed. The problem is that the particular, extremely-common "variants" were possible to pre-compute, allowing easy discovery of the random keys passed through it.

3 ^ | v · Reply · Share ·

**Grackos** · 23 days ago

wut

^ | v · Reply · Share ·

ALSO ON THE HACKERS NEWS

Researcher releases Free Hacking Tool that Can Steal all Your Secrets from Password ...

7 comments · 4 days ago

WHAT'S THIS?

FBI Deputy Director's Email Hacked by Teenager Who Hacked CIA Chief

6 comments · 2 days ago

Avatar James A Garfield — yes its safe. this do not compromise keepass encryption at all. this thing can be done on linux with little effort too. this ...

ProtonMail Paid Hackers \$6000 Ransom in Bitcoin to Stop DDoS Attacks

4 comments • 2 days ago

Avatar Ted Wood — Never pay random. Foolish move.

Avatar sammy — These guys actually make Hillary look smart! At least her e-mail server had a small measure of security, unlike AOL. How do such ...

Anonymous Group Leaks Identities of 1000 KKK Members

2 comments • 2 days ago

Avatar uldics — I red some disputes about which revealing was the right one and a lot of accused persons making statements of blah blah blah. ...

 [Subscribe](#)  [Add Disqus to your site](#)  [Privacy](#)

DISQUS

IT'S HERE...
2015 GARTNER
MQ FOR SIEM


ALIEN VAULT





COMPARE THE TOP SIEM
VENDORS NOW ▶

BARRON'S


WHENEVER,
WHEREVER YOU NEED.



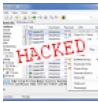
Only \$1 a week
for 26 weeks!

Subscribe Now


Popular Stories




Anonymous Group Leaks Identities of 1000 KKK Members



Researcher releases Free Hacking Tool that Can Steal all Your Secrets from Password Manager



Hackers WIN \$1 Million Bounty for Remotely Hacking latest iOS 9 iPhone



Kim Dotcom's Decentralized Internet

http://thehackernews.com/2015/10/nsa-crack-encryption.html

5/6




LegalN
Your own Private Decentralized



Anonymous Plans to Lead of Politicians with Racist Ku Klux Klan

Ready for Million March?

[illegible]

HACKED HIS BODY TO IMITATE BITCOIN PAYMENT CHARGE



a 16-year-old, Hacker



• Android Apps Spill Your Text Messages



Experience friendly!
Give time a break!

[Hover to Expand](#)

