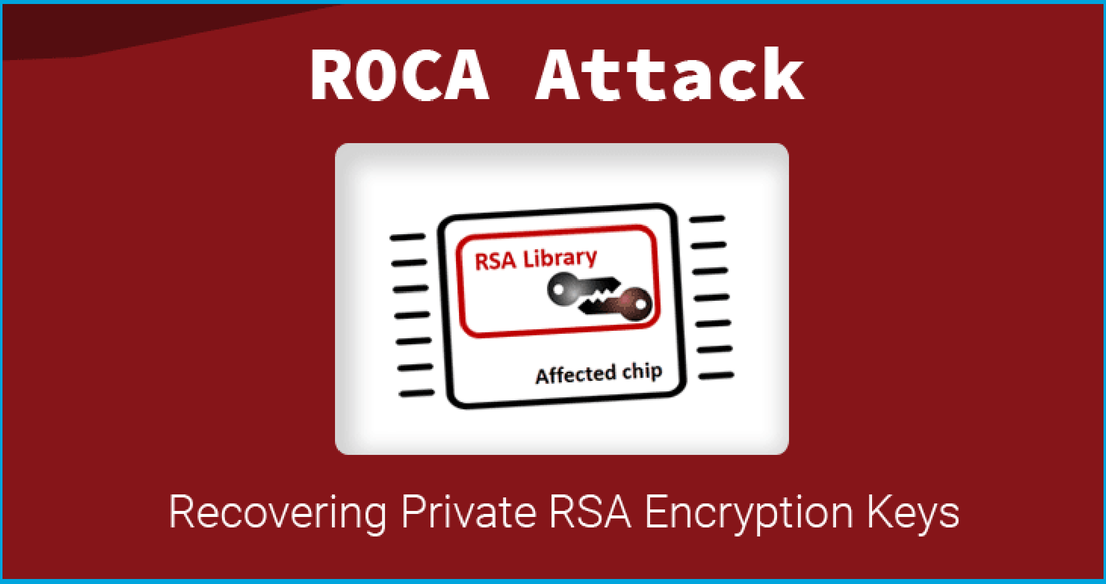
kindred

Security Newsletter

23 October 2017

Subscribe to this newsletter

Serious Crypto-Flaw Lets Hackers Recover Private RSA Keys generated by faulty TPM



Microsoft, Google, Lenovo, HP and Fujitsu are warning their customers of a potentially serious vulnerability in widely used RSA cryptographic library produced by German semiconductor manufacturer Infineon Technologies. Infineon's Trusted Platform Module (TPM) is a widely-used, dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices and is used for secured crypto processes.

This 5-year-old algorithmic vulnerability, dubbed ROCA (Return of Coppersmith's Attack), is a factorization attack that could potentially allow a remote attacker to reverse-calculate a private encryption key just by having a target's public key. This can allow to impersonate key owner, decrypt victim's sensitive data, inject malicious code into digitally signed software, and bypass protections that prevent accessing or tampering with the targeted computer.

The team has provided rough estimates on how long and how much it would cost attackers to be able to crack a private key based on their knowledge of a public key using cloud services such as AWS. 512 bit RSA keys - 2 CPU hours (the cost of $0.06). 1024 bit RSA keys - 97 CPU days (the cost of $40-$80). 2048 bit RSA keys - 140.8 CPU years, (the cost of $20,000 - $40,000)

The researchers have provided offline and online detection tools for users to check to see whether or not they are affected. If a vulnerable key is found, then you should contact your device vendor for further advice. The following general advices may apply: Apply the software update if available. Replace the device with one without the vulnerable library. Generate a secure RSA keypair outside the device (e.g., via the OpenSSL library) and import it to the device. Use other cryptographic algorithm (e.g., ECC) instead of RSA on affected devices.

Read More

Original advisory on CVE-2017-15361

ROCA Vulnerability Test Suite

Vulnerability in WPA2 Protocol Allows Attackers to Intercept and Decrypt Encrypted Data Traffic

there is a dangerous flaw in the WPA2 protocol which can be exploited by cybercriminals to intercept emails, passwords and other kinds of encrypted data. An attacker can also inject malicious content such as ransomware into a website when a client is visiting. The proof-of-concept of this exploit has been dubbed as KRACK, which is an abbreviation of Key Reinstallation Attacks.

The vulnerability affects the core WPA2 protocol and devices running Linux, Android and OpenBSD are mainly vulnerable to be exploited while to some extent macOS, MediaTek Linksys and Windows devices are also vulnerable.

KRACK performs the attack by targeting the four-way handshake. KRACK tricks the client, which is vulnerable, into reinstalling a key that is already in-use, which forces the nonce reuse in such a way that breaks encryption.

Devices running on Android 6.0 and later versions are far more vulnerable to be exploited with this vulnerability than other devices. Using KRACK, the attacker can force the device to reinstall a null, all-zero encryption key instead of the original key.

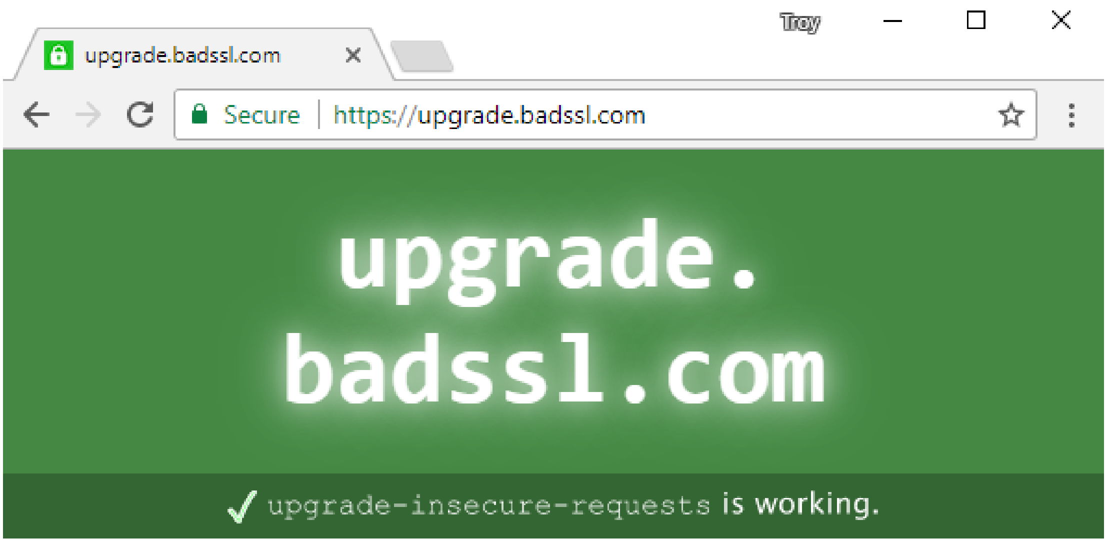
To protect your device, it is highly important to update all the wireless devices such as routers, laptops, phones, and tablets or whatever device you own with the latest security patches because updating them would prevent KRACK vulnerability. If your router hasn't been fixed or a patch is not released then switch to Ethernet and turn off all the functions of wireless until a patch is released.

Read More

Key Reinstallation Attacks: Breaking WPA2 by forcing nonce reuse

Test if your Access Point is vulnerable

The 6-Step "Happy Path" to HTTPS



upgrade.
badssl.com

✓ upgrade-insecure-requests is working.

It's finally time: it's time the pendulum swings further towards the "secure by default" end of the scale than what it ever has before. At least insofar as securing web traffic goes because as of this week's Chrome 62's launch, any website with an input box is now showing "Not Secure" when served over an insecure connection.

It's not doing it immediately for everyone, but don't worry, it's coming very soon even if it hasn't yet arrived for you personally and it's going to take many people by surprise.

Get a free cert, implement the 301 redirect, add HSTS, change your insecure references, use the CSP to fix any of the ones you've missed in non-MS browsers then finally, sit back and watch for any violations by reporting to the free Report URI service. HTTPS doesn't have to be hard, you just have to follow the happy path

Read More

What’s New In Android 8.0 Oreo Security

In addition to the many tweaks and new features in Google’s Android 8.0 Oreo operating system introduced last month, the biggest changes are its security enhancements. Oreo security additions are meaningful and go far beyond what recent OS updates have brought to the table.

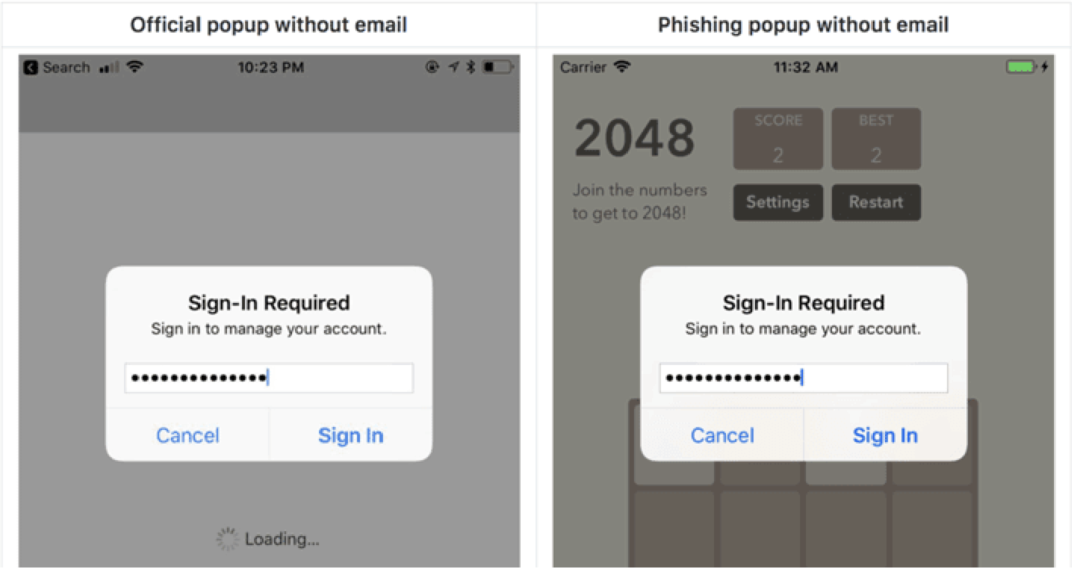
Project Treble separates the hardware-specific drivers and firmware used by companies such as Samsung or Qualcomm from the Android operating system. The implications will be significant when it comes Google’s ability roll out OS patches without having to wait for things such as chipset compatibility.

Android O limits access to the kernel via the introduction of a seccomp filter. Seccomp (short for secure computing mode) is a security feature that filters system calls to the kernel using a configurable policy. Because these syscalls cannot be accessed by apps, they can’t be exploited by potentially harmful apps.

Verified Boot goes a step further and prevents users or hackers from booting to older more vulnerable versions of the OS an adversary may have rolled the system back to. Google has also hardened certain network connection APIs from not falling back to older TLS versions that can leak sensitive data.

Read More

Malicious iOS app popup windows could be stealing your Apple ID


Official popup without email
Search
10:23 PM
Sign-In Required
Sign in to manage your account.
Cancel
Sign In
Loading...
Phishing popup without email
Carrier
11:32 AM
2048
SCORE
2
BEST
2
Join the numbers to get to 2048!
Settings
Restart
Sign-In Required
Sign in to manage your account.
Cancel
Sign In

It's simple to spoof a password request window, and nearly impossible to detect a fake. Here's what iOS users and devs should watch out for. The average user won't question the legitimacy of an Apple ID password request, which makes the spoof a very dangerous form of phishing. All an app needs to do is show a UIAlertController popup—an incredibly common part of an app.

As impossible as it may be for a user to tell the difference between a fake and legitimate dialog window there are still things that iOS users can do to protect themselves. If you get a popup asking for a password inside an app, hit the home button. If you can quit back to the home screen it's not a legitimate request. Real system dialogs that ask for passwords are run as a separate process and can't be quit in that fashion.

Treat password requests inside apps like you would a link in an email—don't use it. Instead, open the Settings app and put the password in there, similar to going directly to a website that wants you to verify your information. Finally, don't type anything into a password-requesting popup. Even if you press the cancel button the information has already been captured.

Read More

Even More

Microsoft Kept Secret That Its Bug-Tracking Database Was Hacked In 2013

Microsoft had also suffered a data breach four and a half years ago (in 2013), when a "highly sophisticated hacking group" breached its bug-reporting and patch-tracking database, but the hack was never made public until today.

As its name suggests, the bug-reporting and patch-tracking database for Windows contained information on critical and unpatched vulnerabilities in some of the most widely used software in the world, including Microsoft's own Windows operating system.

Group known by various names, including Morpho, Butterfly and Wild Neutron, who exploited a JAVA zero-day vulnerability to hack into Apple Mac computers of the Microsoft employees, "and then move to company networks." With such a database in hands, the so-called highly sophisticated hacking group could have developed zero-day exploits and other hacking tools to target systems worldwide.

Although the study found that the flaws in the stolen database were used in cyber attacks, Microsoft argued the hackers could have obtained the information elsewhere, and that there's "no evidence that the stolen information had been used in those breaches."

Read More

Leaked: Facebook security boss says its corporate network is run "like a college campus"

The source of the recording said Facebook's senior management and executives were apathetic to matters of cybersecurity. Facebook's security chief said he used one of the remarks "as a figure of speech". Alex Stamos made the comments to employees at a late-July internal meeting where he argued that the company had not done enough to respond to the growing threats that the company faces, citing both technical challenges and cultural issues at the company.

"Tech companies are famous for providing freedom for engineers to customize their computing environments and to experiment with new tools, frameworks and development processes," he said. "Allowing for this freedom helps creativity and productivity, but we have to weigh that against the fact that we have become a potential target of advanced threat actors. As a result, we can't architect our security in the same way a defense contractor can, with extremely limited computing options and no freedom."

In fairness, Stamos isn't wrong. Facebook likely has more citizen data now than most governments, making the social network as much of a target today as defense contractors were ten years ago. But while Facebook may not be storing plans for spy planes and autonomous drones, private citizen data is a commodity -- the social network has billions of people's data -- and nation states are hungry for it.

Read More

Cutting room floor

- Flash 0-day in the wild – patch now!
- DDoS attacks on Sweden' Transport Agencies Delay Train Service
- Yet Another Linux Kernel Privilege-Escalation Bug Discovered
- Call for WPA3 - what's wrong with WPA2 security and how to fix it
- Microsoft tsk-tsk-tsks at Google: Chrome security fixes made public too early
- Google Announces Three New Chrome Security Features
- VulnScan – Automated Triage and Root Cause Analysis of Memory Corruption Issues
- Scam Alert: Your Trusted Friends Can Hack Your Facebook Account
- 'BoundHook' Technique Enables Attacker Persistence on Windows Systems
- EternalBlue – Everything there is to know
- Looks like NSA knew about the Krack attacks
- WaterMiner – a New Evasive Crypto-Miner
- Wiping Out CSRF
- Google's strongest security for those who need it most
- Peoplesoft password decryption

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us