Security Now! #641 - 12-12-17

The iOS 11 Security Tradeoff

This week on Security Now!

This week we discuss the details behind the "USB / JTAG takeover" of Intel's Management Engine, a rare Project Zero discovery, Microsoft's well-meaning but ill-tested IoT security project, troubles with EV certs, various Cryptocurrency woes, a clever DNS spoofing detection system, a terrific guide to setting up the EdgeRouterX for network segmentation, last week's emergency out-of-cycle patch from Microsoft, a mitigated vulnerability in Apple's Homekit, Valve's ending of Bitcoin for Steam purchases, finally some REALLY GOOD news in the elusive quest for encrypted eMail, a bit of miscellany, some closing the loop feedback with our listeners, and a look at the security sacrifice Apple made in the name of convenience... and what it means.

Our Picture of the Week

CUSTOMERS WHO BOUGHT THIS ITEM:
ALSO BOUGHT:
piccolo

Security News

Hackers Turn On “GOD MODE” To Hack Intel ME Chip Like A Boss #BlackHatEurope
https://fossbytes.com/intel-me-chip-god-mode-hack-black-hat-europe/

Positive Technologies

The unpublished Huffman decoding tables were reverse engineered.

Intel changed the Management Engine controller from an ARC family RISC engine to their own x86 processor core.

This allowed the use of full mature code analysis tools making the binary far more reverse-engineerable.

They found a stack overflow vulnerability.

Then a way around the built-in stack overflow protection system.

But the stack is non-executable.

But ASLR is absent. This gave them fixed known code to use for ROP exploitation.
This was used to create a new process with enhanced system rights.

File system components used during the BUP (Boot Up Process) can be replaced to allow unsigned code to be run.

By exploiting this flaw, they were able to turn on a mechanism known as "PCH Red Unlock" that opens full access to all PCH (Platform Controller Hub) devices using JTAG. Since once such PCH device is the x86 ME processor itself, they obtained access to its internal JTAG interface.

So... it's not as if JTAG was left negligently exposed over USB. It's necessary to first have intimate physical contact with the machine. But after carefully subverting Intel's many layers of carefully designed security, it IS possible to obtain full debugging access to the system's central governing ME processor.

The Jailbreaking Community is loving Google’s Publicly Drop an iPhone Exploit
A Google researcher announced that he is planning to release a powerful tool for iOS 11 that the security community thinks it can use to jailbreak the iPhone.
https://motherboard.vice.com/en_us/article/d3xpyz/google-iphone-ios-jailbreak

Ian Beer is a Google Project Zero security researcher, and one of the most prolific iOS bug hunters.

He is Project Zero’s iOS specialist.

Last Wednesday Ian told his twitter followers to keep their “research-only” devices on iOS 11.1.2 because he was about to release “tfp0” soon.

December 5th: Ian Beer / @i41nbeer
"If you're interested in bootstrapping iOS 11 kernel security research keep a research-only device on iOS 11.1.2 or below. Part I (tfp0) release soon."

("tfp0" stands for “task for pid 0,” or the kernel task port, which gives control of the core of the operating system.)

December 11th: Ian Beer / @i41nbeer
"iOS 11.1.2, now with more kernel debugging:
https://bugs.chromium.org/p/project-zero/issues/detail?id=1417#c3
"tfp0 should work for all devices, the PoC local kernel debugger only for those I have to test on (iPhone 7, 6s and iPod Touch 6G) but adding more support should be easy"

"async_wake" exploit attached.
Gets tfp0 on all 64-bit devices plus an initial PoC local kernel debugger.
See the README and kdbg.c for details.

Leverages two different bugs together to get access to the kernel and the ability to set a breakpoint to inspect and alter the kernel's state.

In the latest security bulletin for iOS 11.2, five of the 15 iOS 11.1.2 vulnerabilities that were patched were discovered and reported to Apple by Beer.

So the accumulated evidence suggests that what Beer plans to release is something that he discovered and that was recently patched by Apple.

With iOS's rounds of ever-increasing security, the platform has become ever more dark and inaccessible to legitimate researchers who are interested in poking around for the true purpose of improving iOS security. After all... iOS security is largely as strong as it is BECAUSE past researchers have been able to pry inside, poke around, and help Apple to find things they missed.

Microsoft's Project Sopris
https://www.wired.com/story/project-sopris-iot-security/

The good news is that Microsoft is exploring the idea of making IoT security better by designing it in, integrating it, and thus effectively eliminating its cost.

The bad news is... they're going about it all wrong.

HackerOne:
Project Sopris Challenge

The Microsoft Research Project Sopris team invites the security research community to test our most recent experiment, the Sopris security kit, by applying to the Project Sopris Challenge (The Challenge).

To learn more about Microsoft Research Project Sopris visit the website:
https://www.microsoft.com/en-us/research/project/sopris/

A primary goal of The Challenge is to broadly engage with the security community towards sharing and learning - 150 security experts have been selected to receive and test a Sopris security kit through The Challenge. The application period closed at mid-night on April 14th Pacific Daylight Time. Applicants have been notified if they are accepted to participate in The Challenge by email by April 21st. Devices have been distributed by early May with the challenge ending on July 12th. It is free to participate and there are no fees for the hardware.

Microsoft Boasts:
"Project Sopris Security Challenge"

Thanks to all the skilled hackers who participated!

Over 150 hackers pounding on their Project Sopris boards for 60 days. Microsoft Research Sopris Challenge completes as a great learning experience with no verified exploits.

Stay tuned for updates from the Project Sopris team as we continue to work with the security community to explore devices secured from the silicon up.

One of the research hackers who participated in the research and who goes by the handle "HexDecimal" was quoted for the story in Wired's coverage saying: “It’s stupidly easy to hack most IoT devices, but this was very different. The chip was definitely built for security from the ground up. One of the noteworthy things would be the lack of information. The board and its web server were very closed off, nothing that would hint at an exploit. I only started to get a foothold after decompiling one of the setup tools that came with it. But I never managed to find anything and neither did anyone else in the challenge.”

Okay... That's the dumbest thing I've ever heard. Microsoft gave these guys an undocumented black box and said "try to hack it"??

Galen Hunt, the managing director for Project Sopris, says the team was actually disappointed that the penetration testers didn’t find more flaws; better to find out under controlled conditions than in the wild. Project Sopris has another security challenge planned, in which the attack surface for the chip will be a bit larger, giving hackers more avenues in, like connection to cloud services.

Screw that!... give them total documentation, source, and schematics. Everything. Only THEN will you know whether you have been wasting your time and money... or not.

Extended Validation Is Broken
https://stripe.ian.sh/

Leo: Go there in Safari... what do you see as the URL?

In Firefox I see -- in happy glowing green "Stripe, Inc (US)"

Unlike in Safari, under both Firefox and Chrome it IS possible to examine the URL. But this would still make spoofing much easier and likely more successful... just as we are finally getting people to care.

Another researcher obtained an EV for "Identity Verified" which creates a sort of universally applicable EV spoofing cert since Firefox and Chrome will display "Identity Verified" in front of the URL and Safari will proudly center "Identity Verified" in the URL field.

MyEtherWallett: https://myetherwallet.com/

MEW is one of the internet's most popular services for storing ETH and other crypto coins

Annoying Click-Through: FABULOUS ANNOYING NECESSARY

Welcome to MyEtherWallet.com
We know this click-through stuff is annoying. We are sorry.

Please take some time to understand this for your own safety. ?? Your funds will be stolen if you do not heed these warnings.

We cannot recover your funds or freeze your account if you visit a phishing site or lose your private key.

What is MEW?

- MyEtherWallet is a free, open-source, client-side interface.
- We allow you to interact directly with the blockchain while remaining in full control of your keys & your funds.
- You and only you are responsible for your security.

MyEtherWallet is not a Bank

- When you open an account with a bank or exchange, they create an account for you in their system.
- The bank keeps track of your personal information, account passwords, balances, transactions and ultimately your money.
- The bank charge fees to manage your account and provide services, like refunding transactions when your card gets stolen.
- The bank allows you to write a check or charge your debit card to send money, go online to check your balance, reset your password, and get a new debit card if you lose it.

- You have an account with the bank or exchange and they decide how much money you can send, where you can send it, and how long to hold on a suspicious deposit. All for a fee.

MyEtherWallet is an Interface

- When you create an account on MyEtherWallet you are generating a cryptographic set of numbers: your private key and your public key (address).
- The handling of your keys happens entirely on your computer, inside your browser.
- We never transmit, receive or store your private key, password, or other account information.
- We do not charge a transaction fee.
- You are simply using our interface to interact directly with the blockchain.
- If you send your public key (address) to someone, they can send you ETH or tokens. (Okay!)
- If you send your private key to someone, they now have full control of your account. (NOT okay!)

Wait, WTF is a Blockchain?

- The blockchain is like a huge, global, decentralized spreadsheet.
- It keeps track of who sent how many coins to whom, and what the balance of every account is.
- It is stored and maintained by thousands of people (miners) across the globe who have special computers.
- The blocks in the blockchain are made up of all the individual transactions sent from MyEtherWallet, MetaMask, Exodus, Mist, Geth, Parity, and everywhere else.
- When you see your balance on MyEtherWallet.com or view your transactions on etherscan.io, you are seeing data on the blockchain, not in our personal systems.
- Again: we are not a bank.

Why are you making me read all this?

Because we need you to understand that we cannot...

- Access your account or send your funds for you X.
- Recover or change your private key.
- Recover or reset your password.
- Reverse, cancel, or refund transactions.
- Freeze accounts.

You and only you are responsible for your security.

- Be diligent to keep your private key and password safe. Your private key is sometimes called your mnemonic phrase, keystore file, UTC file, JSON file, wallet file.
- If you lose your private key or password, no one can recover it.
- If you enter your private key on a phishing website, you will have all your funds taken.

If MyEtherWallet can't do those things, what's the point?

- Because that is the point of decentralization and the blockchain.
- You don't have to rely on your bank, government, or anyone else when you want to move your funds.
- You don't have to rely on the security of an exchange or bank to keep your funds safe.
- If you don't find these things valuable, ask yourself why you think the blockchain and cryptocurrencies are valuable. ??
- If you don't like the sound of this, consider using Coinbase or Blockchain.info. They have more familiar accounts with usernames & passwords.
- If you are scared but want to use MEW, get a hardware wallet! These keep your keys secure.

How To Protect Yourself from Phishers

- (Blah blah blah)

How To Protect Yourself from Scams

- (Blah blah blah)

How To Protect Yourself from Loss

- (Blah blah blah)

Alright, I'm done lecturing you!

Sorry for being like this. Onwards!

Apple let a knockoff version of one of the world’s biggest crypto wallets into the App Store
https://techcrunch.com/2017/12/11/apple-knockoff-myetherwallet-ios

Yesterday, TechCrunch reported that an imposter of "MyEtherWallet.com"

And then, despite all of that web-facing care and concern, an app MASQUERADING as MyEtherWallet -- which is in no way affiliated with MyEtherWallet -- made its way into the Apple App Store... and up to the top of the iOS popularity charts.

TechCrunch wrote that: The app rose to the number three spot in Finance category of the App Store last weekend as part of a bitcoin frenzy that saw exchange Coinbase top Apple’s free download list in the U.S. In this case, however, it is important to note this app is not official so users should avoid downloading it.

The app developer — who is listed as Nam Le — has three other apps with Apple, including two panda fighting games, but no history of crypto or bitcoin services.

The creators of MyEtherWallet said in a tweet that they have contacted Apple in a bid to have the app removed.

And today it is gone.

DNS Twist
https://github.com/elceef/dnstwist

See what sort of trouble users can get in trying to type your domain name. Find similar-looking domains that adversaries can use to attack you. Can detect typosquatters, phishing attacks, fraud and corporate espionage. Useful as an additional source of targeted threat intelligence.

The idea is quite straightforward: dnstwist takes in your domain name as a seed, generates a list of potential phishing domains and then checks to see if they are registered. Additionally it can test if the mail server from MX record can be used to intercept misdirected corporate e-mails and it can generate fuzzy hashes of the web pages to see if they are live phishing sites.

Linux: Ubuntu Linux is the primary development platform.
macOS: Homebrew as be used
Docker can be used.

A TERRIFIC guide to setting up a Ubiquity EdgeRouter X for network segmentation:
https://github.com/mjp66/Ubiquiti
https://github.com/mjp66/Ubiquiti/blob/master/Ubiquiti%20Home%20Network.pdf

(GRC's Linkfarm page updated with these permanent links.)

CVE-2017-11937 | Microsoft Malware Protection Engine Remote Code Execution Vulnerability Emergency Out-Of-Cycle across-the-board Update
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11937

<quote> A remote code execution vulnerability exists when the Microsoft Malware Protection Engine does not properly scan a specially crafted file, leading to memory corruption. An attacker who successfully exploited this vulnerability could execute arbitrary code in the security context of the LocalSystem account and take control of the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, a specially crafted file must be scanned by an affected version of the Microsoft Malware Protection Engine. There are many ways that an attacker could place a specially crafted file in a location that is scanned by the Microsoft Malware Protection Engine. For example, an attacker could use a website to deliver a specially crafted file to the victim's system that is scanned when the website is viewed by the user. An attacker could also deliver a specially crafted file via an email message or in an Instant Messenger message that is scanned when the file is opened. In addition, an attacker could take advantage of websites that accept or host user-provided content, to upload a specially crafted file to a shared location that is scanned by the Malware Protection Engine running on the hosting server.

If the affected antimalware software has real-time protection turned on, the Microsoft Malware Protection Engine will scan files automatically, leading to exploitation of the vulnerability when the specially crafted file is scanned. If real-time scanning is not enabled, the attacker would need to wait until a scheduled scan occurs in order for the vulnerability to be exploited. All systems running an affected version of antimalware software are primarily at risk. </quote>

We've spoken about how anti-malware systems can, themselves, create an expanded attack surface. This recent emergency out-of-cycle patch shows that Microsoft's own system is not immune... but their immediate response and ability to push out an update is what we want, and it's the best we can expect.

Zero-day iOS HomeKit vulnerability allowed remote access to smart accessories including locks, fix rolling out
https://9to5mac.com/2017/12/07/homekit-vulnerability/

A HomeKit vulnerability in the current version of iOS 11.2 has been demonstrated to 9to5Mac that allows unauthorized control of accessories including smart locks and garage door openers. Our understanding is Apple has rolled out a server-side fix that now prevent unauthorized access from occurring while limiting some functionality, and an update to iOS 11.2 coming next week will restore that full functionality.

The vulnerability, which we won't describe in detail and was difficult to reproduce, allowed unauthorized control of HomeKit-connected accessories including smart lights, thermostats, and plugs.

The most serious ramification of this vulnerability prior to the fix is unauthorized remote control of smart locks and connected garage door openers, the former of which was demonstrated to 9to5Mac.

The issue was not with smart home products individually but instead with the HomeKit framework itself that connects products from various companies.

Bugs are not good. But the centralized nature of HomeKit's architecture in this instance allowed Apple to immediately neuter the undisclosed vulnerability at their end... while preparing a proper fix, pushing it out, then re-enabling the reduced functionality.

Valve ends support for Steam purchases made with Bitcoin
“It has become untenable to support Bitcoin as a payment option”
https://www.polygon.com/2017/12/6/16742622/steam-ends-support-bitcoin-volatility

In a post on Steam, Valve wrote: “In the past few months we've seen an increase in the volatility in the value of Bitcoin and a significant increase in the fees to process transactions on the Bitcoin network. For example, transaction fees that are charged to the customer by the Bitcoin network have skyrocketed this year, topping out at close to $20 per transaction last week (compared to roughly $0.20 when we initially enabled Bitcoin). Unfortunately, Valve has no control over the amount of the fee. These fees result in unreasonably high costs for purchasing games when paying with Bitcoin. The high transaction fees cause even greater problems when the value of Bitcoin itself drops dramatically.”

Valve also explained why surges like that can have an impact on purchases through Steam:

“When checking out on Steam, a customer will transfer x amount of Bitcoin for the cost of the game, plus y amount of Bitcoin to cover the transaction fee charged by the Bitcoin network. The value of Bitcoin is only guaranteed for a certain period of time, so if the transaction doesn’t complete within that time window, and with Bitcoin value fluctuating wildly, the amount of Bitcoin needed to cover the transaction can change. The amount it can change has been increasing recently to a point where it can be significantly different.”

Valve said that those price discrepancies will normally result in a refund or an additional payment from the customer when more traditional, more stable currencies are involved. But in the case of bitcoin, high transaction fees can make even those resolutions costly.

They concluded: “At this point, it has become untenable to support Bitcoin as a payment option. We may re-evaluate whether Bitcoin makes sense for us and for the Steam community at a later date.”

What's this about transaction fees?

Only 1MB of data is allowed per Bitcoin block, and one block is completed every ten minutes, so only 1 MB of data allowed every 10 minutes. This creates a transaction rate scarcity... and thus those wishing to push higher-value transactions through the system create a bidding war to get their transactions into the next block being computed.

Introducing ProtonMail Bridge, email encryption for Outlook, Thunderbird & Apple Mail
https://protonmail.com/blog/thunderbird-outlook-encrypted-email/

I FINALLY have truly good news about eMail encryption.

Today we are officially launching ProtonMail Bridge, which brings easy-to-use email encryption to desktop email clients.

Ever since the day that we first got the idea to create ProtonMail, one of the most enduring challenges has been how to do email security right while simultaneously making encrypted email easy enough to use for normal people. Since our early days working from the CERN cafeteria, we have been working tirelessly to address this specific problem.

In the years since, we have made many great strides towards creating usable encrypted email, first with ProtonMail’s webmail interface and then with our award-winning iOS and Android secure email apps. However, one of our goals has always been to bring easy-to-use encrypted email to desktop. The problem is formidable. Desktop systems encompass multiple operating systems with dozens of popular email clients with their own adherents, and virtually none of them natively speak PGP, the email encryption standard upon which ProtonMail is built.

Around two years ago, we created a small task force to tackle this challenge. Today, we are finally ready to present ProtonMail Bridge.

Later...

Furthermore, after the technical documentation of the ProtonMail Bridge code is done, we will be releasing the source code of the Bridge, so that you can even compile it yourself instead of getting the binaries from us, so there is even less need to trust us. This is an important step in our work to eliminate ProtonMail itself as a threat vector.

Currently, the officially supported email clients are Thunderbird, Apple Mail, and Outlook, on both Windows and MacOS (Linux is coming in Spring of 2018). However, in theory, any IMAP email client can work with the Bridge, and in our beta testing, many were shown to work. If you are a paid ProtonMail user, you can immediately get started here:

Miscellany

Just moved grc.com & grctech.com over to Hover.

On a distressing note... If early ransomeware miscreants left their ill gotten proceeds in bitcoins -- back when one coin was about $400 dollars... they will have made out VERY well. :(

SpinRite

Al in Portugal / Subject: SpinRite Sound Recovery
Date: 10 Dec 2017 08:40:01
Hi Steve,

Am still running Win8 here. Today the sound stopped playing back. I checked the sound troubleshooting area in the control panel but it said it found nothing wrong with the sound. Brilliant!

So I dug around the Sound dialog from control panel to see if I could refresh the playback by disabling and re-enabling things, but nothing worked. In fact when I clicked the playback tab sometimes it would bring up the small spinning blue circle that never stopped spinning. I had to terminate the rundll32.exe to close the Sound dialog.

This made me think that perhaps there was something wrong with Windows being unable to read some files somewhere. So I thought why don't I give SpinRite a go to see if it fixed things. I first tried rebooting twice to see if it might help, but it did not.

So I then started SpinRite on level 2 and let it run for just the first 1.5 percent of the 500MB disk drive. I only did such a small amount because I heard that sometimes people had only run SpinRite for a little while, and it had fixed various problems. I think it fixes some stuff in the filesystem. Anyway, I fired up windows after that and the sound was working again, so I think it must have been SpinRite finding and fixing the problem.

Thanks very much Steve for SpinRite, and for the Security Now podcast too.
Al in Portugal.

Closing The Loop

jim clary / @jimclary
@SGgrc Any security reason for a "I'm not a robot" check on a logon page? I understand usefulness for account generation, but not login. @Humana uses it, making it more difficult to use a password manager.

Peter Griffiths / @pxg638
@SGgrc branded router always best? Visiting folks, and given recent router security awareness wanted to update their firmware. Linksys router, no firmware update available newer than 2013! Time to buy new one?

Patrick Hogan @paddyhogan
@SGgrc Steve, do you think it's annoying that some ISPs don't enable custom DNS servers to be configured in their customers' home routers? @SkyUK are dragging their feet with this.

Michael Munger / @ArrayElement
@SGgrc about 30 minutes ago, yet another one of my clients gave you a yabba-dabba-do. :-) Now, we can get to work fixing this drive to get a good image of it before we do a warranty return!

Jonathan Harris / @AbdulaOblongata
@SGgrc I believe I have found a bug in a brand of networking equipment my company uses. I have tried contacting them regarding the issue but receive no response. How can I verify this problem and how should I proceed.
https://securitytxt.org/

belwig / @belwig
@SGgrc long time security now listener. I don't recall you ever going over the right (and wrong) way to handle password resets. Are the token-based links in emails secure for resets? Waiting patiently for SQRL

Yosef N Berger / @yosef_berger
@SGgrc When storing passwords by hashing and salting, why is it considered bad practice to use the user's name as the salt? If we want to make it so different users with the same password don't end up with the same hashed password, why is a unique username not as good as a RSG?

Javier Matusevich @_matusevich
@SGgrc You've said: "It's incredible WINE works at all." Running your DNS Benchmark on my Mac. Flawlessly works.

iOS Security vs Convenience

iOS 11 Horror Story: the Rise and Fall of iOS Security
https://blog.elcomsoft.com/2017/11/ios-11-horror-story-the-rise-and-fall-of-ios-security/

Publishers of:

- iOS Forensic Toolkit
- Elcomsoft Phone Breaker (with Keychain Explorer)
- Elcomsoft Phone Viewer

With the release of iOS 11, Apple developers made too many assumptions, breaking the fragile security/convenience balance and shifting it heavily onto convenience side.

Once an intruder gains access to the user’s iPhone and knows (or recovers) the passcode, there is no single extra layer of protection left. Everything (and I mean, everything) is now completely exposed. Local backups, the keychain, iCloud lock, Apple account password, cloud backups and photos, passwords from the iCloud Keychain, call logs, location data, browsing history, browser tabs and even the user’s original Apple ID password are quickly exposed. The intruder gains control over the user’s other Apple devices registered on the same Apple account, having the ability to remotely erase or lock those devices. Finally, regaining control over hijacked account is made difficult as even the trusted phone number can be replaced.

This is just scary. Why Apple decided to get rid of the system that used to deliver a seemingly perfect balance between security and convenience is beyond us. Once someone has your iPhone and your passcode, you are no longer in control of your device or your Apple account.

What can you do to protect yourself? Since the passcode is now the one and only safeguard left, make sure you use at least 6 digits. Four-digit PINs are no longer secure. Other than that, we’ll just wait and see if Apple can fix it.

Backup Passwords in iOS 8, 9 and 10

In these versions of iOS, one could protect their backups by specifying a backup password in iTunes. One would only need to do it once. Once a password was set, all future backups made on that computer and any other computer, with no exceptions, would be protected with that password:

The password would become the property of the i-device and not the PC (or the copy of iTunes) that was used to set the password. You could connect your phone to a different computer and make a local backup with a freshly installed copy of iTunes, and that backup would still be protected with the password you set a long time ago.
Any attempt to change or remove that password must pass through iOS, which would require to provide the old password first. Forgot the original password? There’s no going back, you’re stuck with what you have unless you are willing to factory reset the device and lose all data in the process.

If you ask me, this was a perfect and carefully thought through solution. Want to protect your data against an attacker? Set a long and complex backup password and don't store it anywhere. Forgot that password? You can still make a cloud backup and restore your phone from that backup; even your passwords (keychain) would be restored if you rolled out the cloud backup onto the same device you made the backup from (or used iCloud Keychain if that was to be a different device).

A perfect system? Apparently, it was not to everyone's liking. The users whined. The police complained. The FBI complained. And Apple gave up.

iOS 11: Stripping Backup Passwords

In iOS 11 you can still specify a backup password in iTunes, and you still cannot change or reset it through iTunes if you don't know the original password. However, this means very little as you can now easily remove that password from iOS settings.

This is what Apple has to say in its Knowledge Base:

You can't restore an encrypted backup without its password. With iOS 11 or later, you can make a new encrypted backup of your device by resetting the password. Here's what to do:

1. *On your iOS device, go to Settings > General > Reset.*
2. *Tap Reset All Settings and enter your iOS passcode.*
3. *Follow the steps to reset your settings. This won't affect your user data or passwords, but it will reset settings like display brightness, Home screen layout, and wallpaper. It also removes your encrypted backup password.*
4. *Connect your device to iTunes again and create a new encrypted backup.*

You won't be able to use previous encrypted backups, but you can back up your current data using iTunes and setting a new backup password.

If you have a device with iOS 10 or earlier, you can't reset the password.

That's it? That's it. You have just removed the backup password. You can now make a new backup or, rather, extract information from the device. Don't rush and make sure to specify a temporary password ("123" always works) before you make that backup.

A password-protected backup will allow you decrypting the user's passwords, credit card data, health data and other things that would be otherwise inaccessible.

So, set a temporary password, make that backup, decrypt it with Elcomsoft Phone Breaker or just use *Keychain Explorer* (a tool in Elcomsoft Phone Breaker) to access that user's passwords, authentication tokens, credit card numbers and other interesting things. Oh, and their pictures, too.