Security Now! #555 - 04-12-16

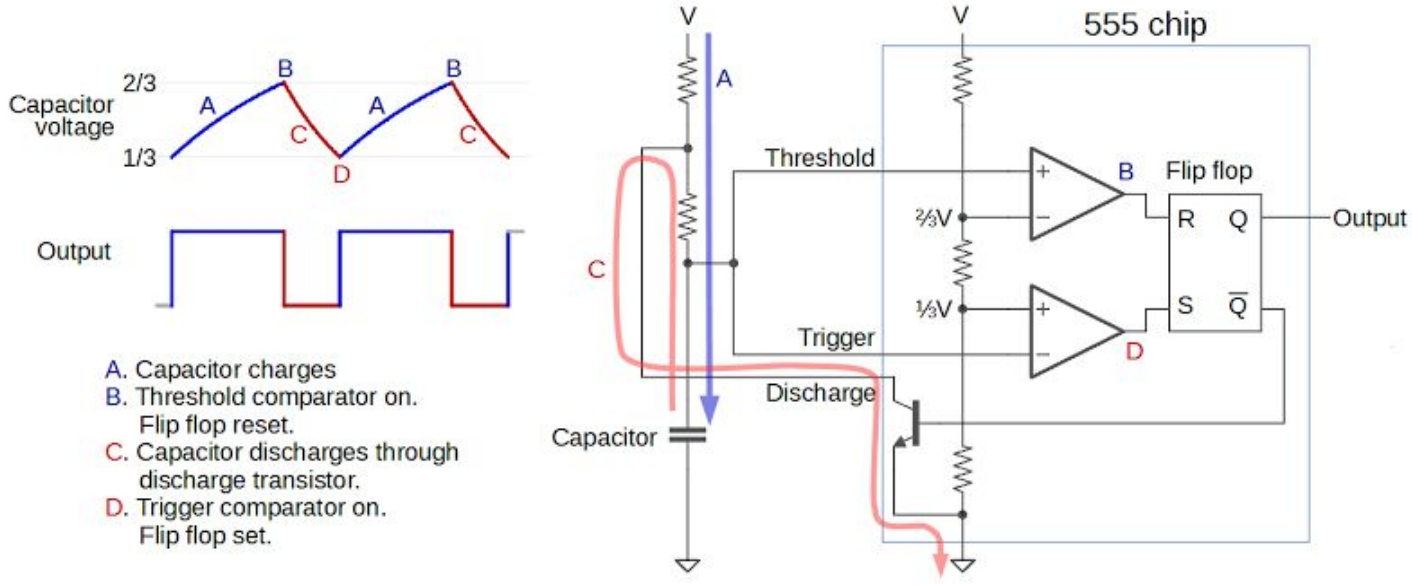
WhatsApp

(Pre show: Leo's PERFECT 3rd-party cookie explanation at the end of Sunday's Tech Guy show.)

This week on Security Now!

- BadLock!!
- Burr Feinstein and a new SN abbreviation: DOD - Decryption on Demand
- But Hungary goes WAY further
- iPhone FBI hack update
- A worrisome architectural problem in Mozilla's Firefox extension handling
- HTTPS gets a BIG new supporter
- At least tens of thousands of commercial CCTV DVR's can be remotely hacked
- And Amazon is (was) selling a malware-infected Webcam system
- A bunch of ransomware news
- A major "You're doing it wrong" in the UK.
- And… ***The result of my analysis of WhatsApp***
    - The ONE non-default security setting you MUST CHANGE in WhatsApp,
    - And the ONE thing you MUST DO JUST ONCE for every contact you communicate with in WhatApp... to have more than an illusion of connection security.

The Incredible 555 Timer



(http://www.righto.com/2016/02/555-timer-teardown-inside-worlds-most.html)

Ken Shirriff reverse-engineers classic Integrated Circuits

Security News

BadLock -- Mega-Patch Tuesday??

- MITM vulnerability and a possible remote DoS on the server.
- Mostly due to configuration errors that have been known for many years
- SMB is not fully encrypted.
- Corporate VPN users will be protected by their VPN tunnel encryption.
- Microsoft: "Security Update for SAM and LSAD Remote Protocols (3148527)"
    - https://technet.microsoft.com/library/security/MS16-047
    - This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker launches a man-in-the-middle (MiTM) attack. An attacker could then force a downgrade of the authentication level of the SAM and LSAD channels and impersonate an authenticated user.
    - This security update is rated Important for all supported editions of Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, and Windows 10. For more information, see the **Affected Software** section.
    - The security update addresses the vulnerability by modifying how the SAM and LSAD remote protocols handle authentication levels. For more information about the vulnerability, see the **Vulnerability Information** section.

Burr Feinstein

http://www.macrumors.com/2016/04/08/senate-draft-encryption-bill-dangerous/
http://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare/
https://assets.documentcloud.org/documents/2796927/Burr-Encryption-Bill-Discussion-Draft.pdf

- Does **not** outlaw encryption
- Does **not** weaken encryption… but by **compelling decryption** -- **DOES** weaken **privacy**

- The point of my last blog posting, exactly one month ago on March 12th, was that this debate keeps getting sidetracked by non-experts and also ivory tower idealist cryptographers, talking about encryption technology. This issue is not about technology -- it's about legal policy.

- The technology will do anything the technologists ask of it.
- The question is… as a society, what do we want it to do?
- New SN abbreviation: "DOD" - Decryption on Demand

Meanwhile... Hungary's government is planning to go further!

https://mappingmediafreedom.org/#/2058

Hungary: Government plans to criminalise the use of encrypted services

Mapping Media Freedom writes:

> The Hungarian government plans to criminalize the use of applications for encrypted communication. The measure is part of a new anti-terrorism legislation package put forward by the Interior Ministry, and was first presented on 31 March by János Lázár, the Minister heading the Prime Minister's Office. If the package is implemented in its present form, anyone caught using encrypted software can be punished by 2 years of prison. The providers would be obliged to ensure access to the content of the encrypted messages, and they would have to provide the identification data of the users as well as the IP address used for registration. Failure to comply qualifies as misdemeanor, and is also punishable with a 2 years prison sentence. The anti-terrorism package also contains provisions regarding an increase of surveillance in public spaces and enables the Interior Ministry to prohibit mass events.

FBI hack reportedly won't work on newer iPhones

- FBI Director James Comey said last Wednesday that the government had purchased "a tool" from a private party in order to unlock the iPhone used by one of the San Bernardino shooters.
- Quoting Comey: "The people we bought this from, I know a fair amount about them, and I have a high degree of confidence that they are very good at protecting it, and their motivations align with ours."
- Comey also said the purchased tool could only be used on a "narrow slice of phones" that does not include the newest Apple models, or the 5S.
- Comey said the government was currently considering whether to tell Apple how it pulled off the hack.
- Quote: "We tell Apple, then they're going to fix it, then we're back where we started from. We may end up there, we just haven't decided yet."
- While that doesn't confirm exactly how the hack worked, the distinction being drawn here may suggest that it's specifically the lack of the Secure Enclave on the iPhone 5c's A6 SoC that renders the phone vulnerable: that extra hardware security debuted with the A7 SoC we find on the iPhone 5s.

CrossFire: NoScript and other popular Firefox add-ons open millions to new attack

http://www.buyukkayhan.com/publications/ndss2016crossfire.pdf

http://arstechnica.com/security/2016/04/noscript-and-other-popular-firefox-add-ons-open-millions-to-new-attack/

http://www.ghacks.net/2016/04/06/firefox-cross-extension-vulnerability-discovered/
A malicious FF extension can sneak past Mozilla's human and automated extension review because it doesn't directly use any sensitive API calls.
<quote> Despite the abundance of research focusing on the security of browser extensions in isolation, to the best of our knowledge, the possible interactions between multiple browser extensions have not been well-studied from a security perspective. In particular, the Firefox extension architecture allows all JavaScript extensions installed on a system to share the same JavaScript namespace, hence making it possible for an extension to invoke the functionality (or modify the state) of others. This problem has long been recognized as a namespace pollution problem that can introduce errors if multiple extensions define identical global names [27]. However, its impact on security has not been studied so far.
https://blog.mozilla.org/addons/2009/01/16/firefox-extensions-global-namespace-pollution/

Of the Top 10 Firefox Extensions:

- Adblock Plus // NO PROBLEM //
- Video DownloadHelper 15
- Firebug 1
- NoScript 7
- DownThemAll! 19
- Greasemonkey 20
- Web of Trust 34
- Flash Video Down 5
- FlashGot Mass Down 8
- Down. YouTube Videos 2

(New release of FireFox 45.0.2 / Monday)

HTTPS Everywhere: Encryption for All WordPress.com Sites
https://en.blog.wordpress.com/2016/04/08/https-everywhere-encryption-for-all-wordpress-com-sites/
https://en.support.wordpress.com/https/

70 different brands of commercial DVR systems vulnerable to remote hijack
A WONDERFUL walk through showing how >30,000 "on the net" commercial CCTV / DVR security systems can be compromised.
http://www.kerneronsec.com/2016/02/remote-code-execution-in-cctv-dvrs-of.html

Rotem Kerner:

Since there are many vendors who redistribute this hardware-software it is hard to rely on vendors patch to arrive at your doorstep. I believe there are few more vulnerabilities being exploited in the wild against these machines and therefore your best shot would probably be to deny any connection from an unknown IP address to the DVR services. And so I will leave you here with a list of vendors who are selling some of TVT's re-branded gear.

Last note about the responsible disclosure process. I've been trying to contact TVT for quite some time with no luck. They have been ignoring me for too long, so they left me with no choice but to disclose.

Mike Olson: "Beware, even things on Amazon come with embedded malware..."

http://artfulhacker.com/post/142519805054/beware-even-things-on-amazon-come

I needed a simple set of good outdoor surveillance cameras for a friends home. Like everything else I buy, I turned to Amazon. I found (what seemed like) a great deal for a set of 6 poe cameras and the necessary recording equipment. Here is the link:

http://www.amazon.com/Sony-Chip-Camera-1080P-CCTV/dp/B00YMEVSGA

When trying to get the cameras to work on my friends machine I simply logged into the admin webpage and went to configure it. First of all something seemed a bit off, the interface showed the camera feed but none of the normal controls or settings were available. Being one of those guys who assumes bad CSS, I went ahead and opened up developer tools. Maybe a bad style was hiding the options I needed. Instead what I found tucked at the bottom of the body tag was an iframe linking to a very strange looking host name.

http://www.Brenz.pl/rc/

A well known malware distribution domain.

New "Petya" ransomware modus: encrypting "entire" disk.

http://www.darkreading.com/endpoint/ransomware-authors-break-new-ground-with-petya/d/d-id/1324955

https://labsblog.f-secure.com/2016/04/01/petya-disk-encrypting-ransomware/

- Encrypts the MBR to show a scary red screen ransom demand.
- But ALSO encrypted the system's MFT$ (Master File Table).
- MFT: Describes all files on the volume, including file names, timestamps, stream names, and lists of cluster numbers where data streams reside, indexes, security identifiers, and file attributes like "read only", "compressed", "encrypted", etc.

BUT!!!! Unlike the well-designed cryptolocker which left no clues about the key behind, Petya's author made a mistake allowing decryption without payment!

http://thehackernews.com/2016/04/ransomware-decrypt-tool.html

https://petya-pay-no-ransom.herokuapp.com/

http://www.bleepingcomputer.com/news/security/petya-ransomwares-encryption-defeated-and-password-generator-released/

Victims paid more than $24 million to ransomware criminals in 2015

http://www.businessinsider.com/doj-and-dhs-ransomware-attacks-government-2016-4

REUTERS: The US Departments of Justice (DOJ) and Homeland Security (DHS) last week provided new insights into the impact of ransomware and cyberattacks on public institutions and the public.

The DOJ revealed that the Internet Crime Complaint Center (IC3) had received nearly 7,700 public complaints regarding ransomware since 2005, totaling $57.6 million in damages. Those damages include ransoms paid — generally $200 to $10,000, according to the FBI — as well as costs incurred in dealing with the attack and estimated value of data lost.

In 2015 alone, victims paid over $24 million across nearly 2,500 cases reported to the IC3.

Speaking of Ransomware... Abode just rushed out an emergency FLASH update

http://arstechnica.co.uk/security/2016/04/adobe-flash-update-ransomware-windows-10/

Sophos explained: "The bug allows an attacker to send booby-trapped content to Windows 10's browser's Flash plugin in such a way that the browser will not only crash, but also hand over control to the attacker in the process."

Adobe claimes that the latest in-the-wild exploits were only targeting Windows 10 users, it would be wise for Flash fans to update the software immediately.

SERIOUSLY!?!?!?! -- BOY are you doing it wrong!!

GCHQ intervenes to prevent catastrophically insecure UK smart meter plan

http://www.theinquirer.net/inquirer/news/2451793/gchq-intervenes-to-prevent-catastrophically-insecure-uk-smart-meter-plan

INTELLIGENCE AGENCY GCHQ has intervened in the rollout of smart meters to demand better encryption to protect UK electricity and gas supplies.

GCHQ barged in after they saw the plans and realized that power companies were proposing to use a single decryption key for communications to the 53 million smart meters that will eventually be installed in the UK.

The agency was concerned that the glaring security weakness could enable hackers, once they'd cracked the key, to gain access to the network and potentially wreak havoc by shutting down meters en masse, causing power surges across the network.

The security flaws would have been particularly catastrophic as the UK's 'Rolls Royce' (i.e. unnecessarily expensive) smart metering system doesn't just automate meter reading. It enables power companies to engage in power management and even to cut people off remotely

if they haven't paid their bills.

Telecoms industry veteran Nick Hunn, director of WiFore Consulting, told INQ's sister publication Computing 15 months ago that the system designed by the utilities and metering industries was "fiendishly complicated". Quoting Nick: "Too many cooks have ratcheted up the technical complexity to the point where it is no longer fit for purpose. As a result, it's lining up to be the next major government IT disaster."

Miscellany

Hover -- the overwhelming favorite.

- (I suspect that Google is losing its soul.)

Never10 v1.3

- Finds (and can delete with one click) ~6.5 GB of files on Win8.1/64
- Full silent command-line switches for all actions.

Seriphos - sold out at Amazon & iHerb

grc.health: Looks like Steve's HSF popularity has depleted the stock of Seriphos. I can't seem to find it anywhere. I am going to run out in a couple days and I don't want to miss a night of good sleep. I had forgotten what it was like to sleep through the night and I'm not willing to go back. Anyone know of an alternate source online?

The Sugar Conspiracy

http://www.theguardian.com/society/2016/apr/07/the-sugar-conspiracy-robert-lustig-john-yudkin
http://bit.ly/sn-sugar

Peter F. Hamilton: The Abyss Beyond Dreams

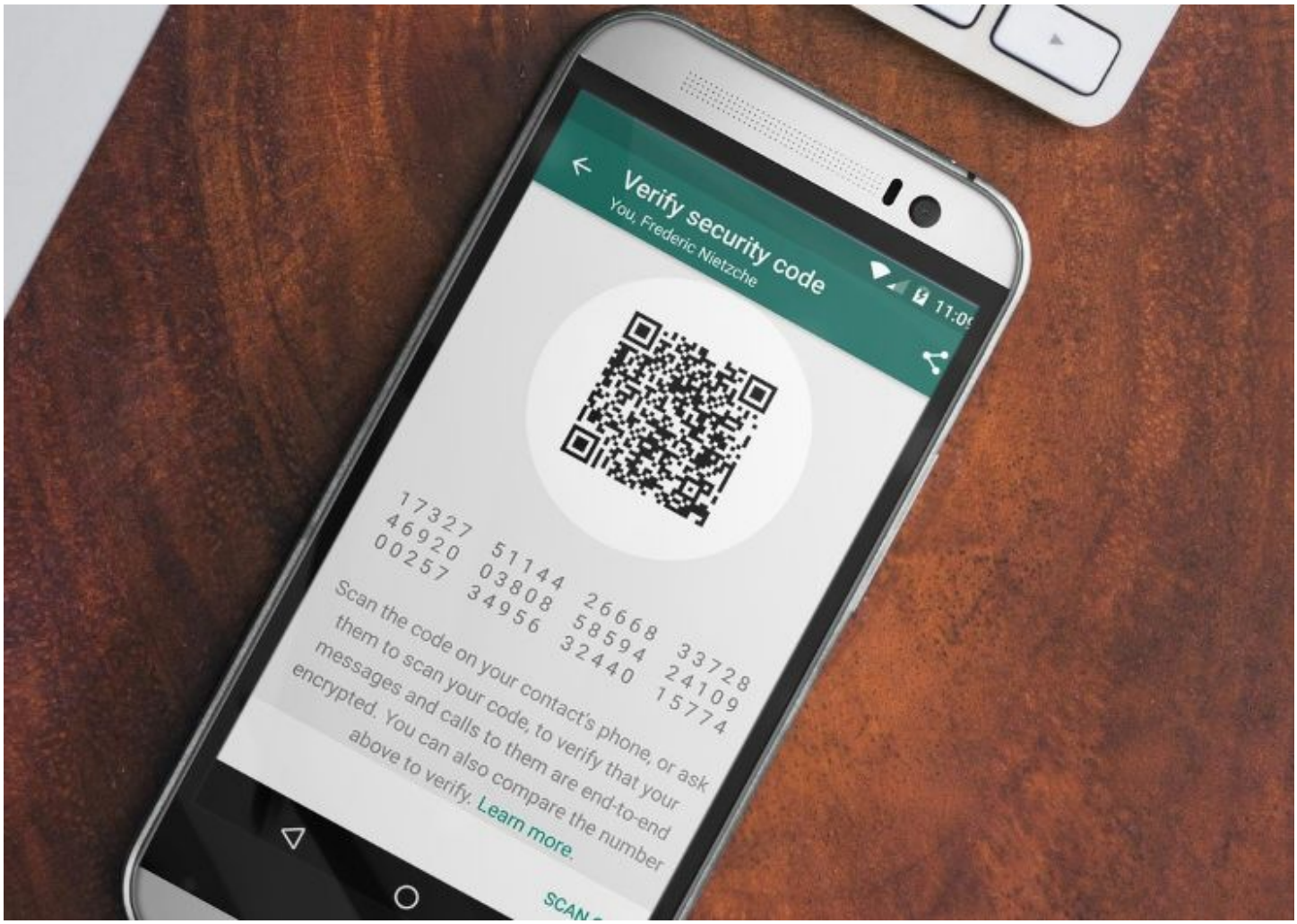
> Okay, I admit it, I'm a complete sucker for Hamilton's work. I've read everything he's written... and not just once. Before you read this you must read The Void Trilogy. And before you read those you must read the Pandora's Star and Judas Unchained pair. And, really... the absolute best place to start would be with Fallen Dragon. I envy anyone who has these amazing pieces of truly wonderful space opera ahead of them.
>
> As for this work... I never believe that anything I read of Hamilton's will be able to live up to everything he has already done. How could it possibly?? ... And then it does.
>
> This does. You will love it. I guarantee it.

SpinRite

Stuart Carroll (@stuart_carroll) / 3/24/16, 4:54 AM
After hearing about @spinrite on @SecurityNow for so long I tried it yesterday & it brought my media drive back from the dead! Thanks @SGgrc

---

WhatsApp



https://whispersystems.org/blog/whatsapp-complete/

"TextSecure" becomes "Signal"
The unpronounceable "Axolotl" becomes the "Signal protocol". (AXE-oh-LOT-el)

(It was named after the critically endangered (and adorable) aquatic salamander Axolotl, which has extraordinary self-healing capabilities.)

<quote from the blog posting>
To continue eliminating confusion and simplifying everything within the Signal ecosystem, we're renaming Axolotl to Signal Protocol. The implementations have been renamed, so there are open source Signal Protocol libraries available for C, Objective C, Java, and JavaScript in our GitHub repository, as before. These have been making their way into an increasing number of communication apps, and we're excited for the future of the Signal Protocol as it continues to spread.

<quote from the blog posting> As of today, the integration is fully complete. Users running the most recent versions of WhatsApp on any platform now get full end to end encryption for every message they send and every WhatsApp call they make when communicating with each other. This includes all the benefits of the Signal Protocol -- a modern, open source, forward secure, strong encryption protocol for asynchronous messaging systems, designed to make end-to-end encrypted messaging as seamless as possible.

The final Signal protocol provides:

- Confidentiality - encrypted communications
- Integrity - any message alteration will be detected and will fail the transaction
- Authentication - it's ***possible*** to confirm the identity of the correspondent
- Participant consistency - unfortunately it defaults to 'off'
- Destination validation - related to the two above
- Forward secrecy - future compromise of private key won't allow decryption of past msgs.
- Backward secrecy (aka future secrecy) - past compromise of key… same protections.
- Message unlinkability - messages are asynchronous, independent, can be missing.
- Message repudiation - recipient can also recreate a valid message from sender.
- Asynchronicity - messages can be queued by server until recipient is ready to receive.

It does not provide for anonymity preservation - No provision for sending anonymous messages.

It does require servers for the relaying of messages and storing of public key material.

Single Ratchet:

- One end sends 1st half of DH key agreement.
- Other end returns acknowledgement of receipt and their other half of the agreement.
- When first end receives agreement it updates key.

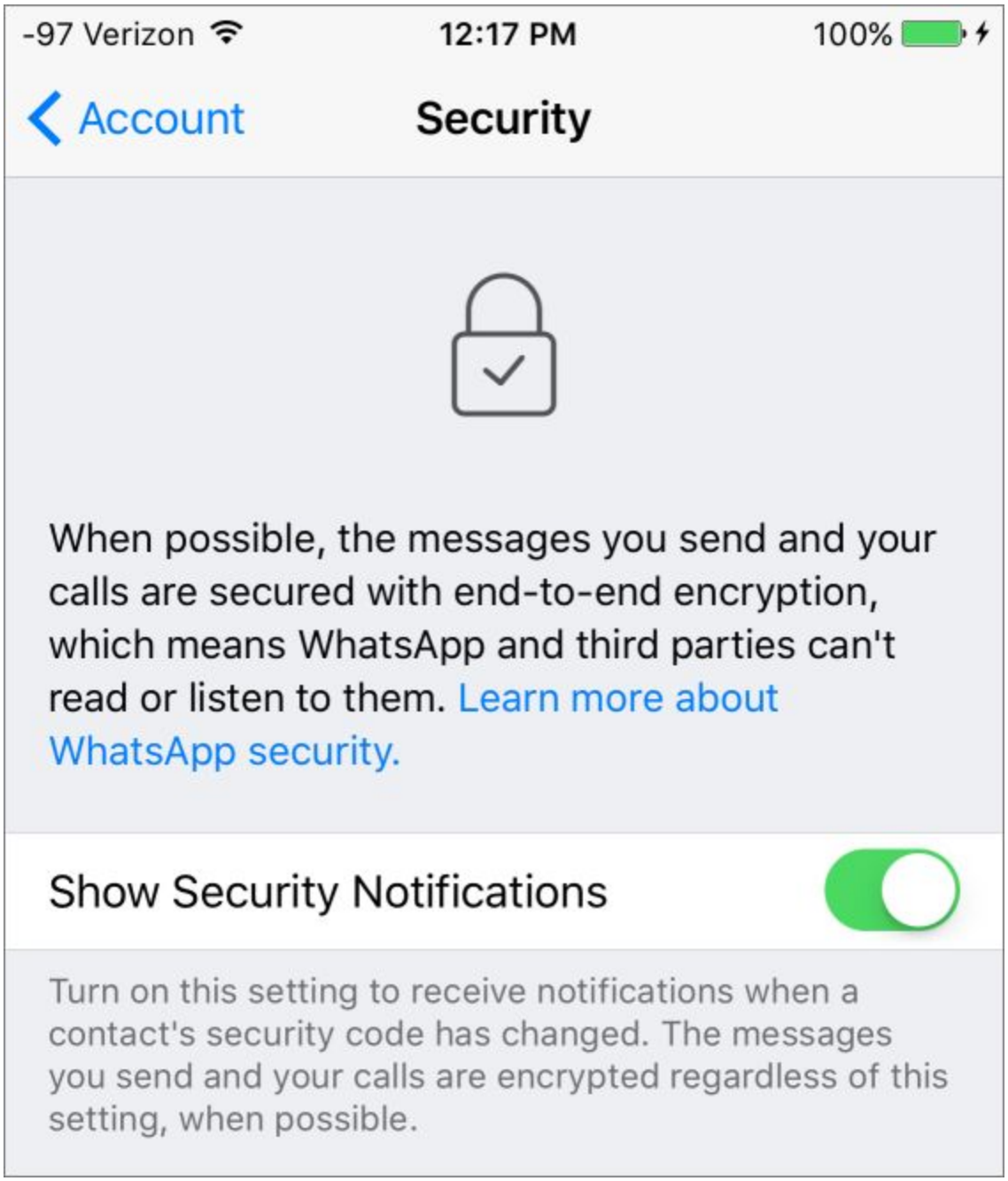
But this only works with real time communications.

Double Ratchet:

- Employs two ratchets:
    - An online DH key agreement
    - An offline one-sided hash ratchet.
    - Any online response re-synchronizes the offline ratchet.

For multiple messages sent without replies, a hash ratchet is used to evolve the key until a reply is received from the other end.

100 "Pre-keys" are seeded with the server to allow single-ended asynchronous encryption.
But!... AUTHENTICATION of the other end remains the big missing piece.



For those interested in delving further into HOW this is all achieved, here are some recommended, nicely written and quite understandably explainers:

https://whispersystems.org/blog/advanced-ratcheting/
https://whispersystems.org/blog/asynchronous-security/
https://whispersystems.org/blog/simplifying-otr-deniability/