SWITCH-CERT report on the latest IT security and privacy trends

July/August 2019

SWITCH

I. Attacks on PGP key server: is pretty good still good enough?

If you don't want everyone between you and your recipient to read your email like a postcard, you'll usually rely on S/MIME or PGP, plus a few isolated solutions. But even PGP has recently been the target of nasty attacks. PGP is based on a public key process in which every participant has a key pair consisting of a public and a private key (asymmetrical encryption). The public key is usually on a key server – something like a phone book. To give the user of the public key certainty (more or less) that the key belongs to their correspondent, there is a 'web of trust'. This means that both parties sign each other's public keys to confirm their ownership.

In the generous view of one of its creators, Robert J. Hansen, the PGP encryption system and its SKS key server network is 'an extremely large, extremely reliable, extremely censorship-resistant distributed file system which anyone can write to.' But it also has serious drawbacks that some, including Hansen himself, have been quick to point out.

- The system is inherently paradoxical because it creates a secure, private communication channel using data that is accessible, at least in part, to the public.
- Out of fear of censorship, it was set up in such a way that, once created, certificates could never be deleted.
- This applies to certificate signatures too – attachments whose purposes include confirming the authenticity of those certificates. Once they are attached to a certificate, they remain there and may result in huge appendices with enormous quantities of data that can end up blocking servers.
- There is no standardised, reliable method for verifying who composed the certificate signature or whether it is correct.

Hackers exploited this vulnerability to compromise the PGP key server network in the last week of June. They launched a ‘certificate spamming attack’ on the security certificates of Hansen and Daniel Kahn Gillmor, another member of the OpenPGP community’s inner circle. The attack also attached huge amounts of new signatures with spam information to the keys. Hanson reported on GitHub that more than 150,000 such signatures were attached to his public key alone. These signatures were included with every email that used the key, ultimately overloading the software and bringing down the system. His piece is a sober account of how such a hack was possible, and warns readers against continued use of the network.

One possible workaround is the OpenPGP key server project launched a few weeks ago with a new server and an updated release of the GnuPG software. Once a new key is uploaded, the server sends an email to all of the addresses in the user’s address book. The email contains a link that each recipient uses to enable the new key. Users can also opt to delete keys that are registered to their email address (further details in the last of the links listed below). But this process ignores signatures, and key servers now lack the foundation of trust on which PGP was based.

With this in mind, we are following technology journalist Jürgen Schmidt’s recommendation to hold ‘key signing parties’ to increase security by signing each other’s keys face to face after mutually verifying identities. This has been the norm with CERTs for many years already.

Read more:

https://www.it-daily.net/it-sicherheit/datenschutz/21858-e-mail-verschluesselung-mit-pgp-ist-nicht-sicher
https://gist.github.com/rjhansen/67ab921ffb4084c865b3618d6955275f
https://dkg.fifthhorseman.net/blog/openpgp-certificate-flooding.html
https://www.zdnet.de/88364171/spam-attacken-gefaehrden-pgp-infrastruktur
https://www.heise.de/security/artikel/PGP-Der-langsame-Tod-des-Web-of-Trust-4467052.html
https://latacora.singles/2019/07/16/the-pgp-problem.html
https://www.heise.de/security/meldung/PGP-E-Mail-Verschluesselung-akut-angreifbar-4048489.html
https://www.heise.de/security/meldung/Angriff-auf-PGP-Keyserver-demonstriert-hoffnugslose-Situation-4458354.html

II. We need to talk! About how virtual assistants are listening in.

Allan and Barbara Pease published their bestseller *Why Men Don't Listen and Women Can't Read Maps* in 2000. Now, nearly 20 years later, the more gender-conscious among us are starting to wonder whether it’s just a coincidence that Alexa, Cortana and Siri are all female names – or whether manufacturers are actually pulling one over on us. After all, ever since Pease and Pease, we know that men don’t listen. And the fact is, nearly all virtual assistants do listen. Even when their users don’t want them to, and to such a degree that it’s making headlines and prompting action from data protection officers. The charge: voice-controlled digital assistants from providers like Google, Apple and Amazon are proving to be a major risk for user privacy. This was the conclusion reached by the city of Hamburg’s officer for data protection and information security upon learning that the three providers had millions of recordings from their ‘digital outposts’ converted to text files, stored and analysed – without informing the users who had been recorded. In early July 2019, Amazon admitted the charge, adding that it was storing the data indefinitely to train the AI that runs Alexa. A short while later, a whistle-blower working for a Google contractor gave Belgian broadcaster VRT around one thousand recordings that prove Google Home and the Google Assistant smartphone app record everything that users say after ‘OK Google’. In late July, *The Guardian* reported that employees at Apple subcontractors were collecting and analysing Siri recordings – regardless of the sensitivity of the content. In 10 to 15% of all cases, virtual assistants (or should we call them spies?) switch on when their users have no intention of activating them. This is because their microphones and/or voice recognition systems are not as reliable as manufacturers lead us to believe.

Google has suspended its recording activities for three months in response to pressure from the media and legal bodies. Apple says it will get users’ express consent from now on, and Amazon’s latest software update offers an opt-out option.

But we still don’t know how other providers and their virtual assistants or other smart devices equipped with microphones (smart home control systems, smart TVs, smart toys, etc.) are treating our privacy. Around four weeks after Alexa was exposed, *Motherboard* reported that employees at Microsoft contractors monitor and record voice communications by Skype and Cortana users – only in the interests of improving their services, of course. We have been reporting on these issues for years; in May 2015 we reported that Hello Barbie, a wifi-connected doll, sends voice recordings to the marketing department of its manufacturer, Mattel.

It’s not yet known whether makers of cars that are equipped with their own virtual assistants record conversations that take place in vehicles. When the Basel police department questioned Tesla in the context of fleet procurement in 2018, the carmaker denied that it engages in such practices. On the other hand, there is no question that carmakers are already collecting and analysing vehicle data without buyers’ consent. So we may be in for a rude awakening.

Read more:

https://steigerlegal.ch/2019/08/05/google-assistant-datenschutz
https://www.handelsblatt.com/technik/it-internet/apple-google-amazon-sprachassistenten-und-datenschutz-wer-zuhoeren-will-muss-fragen/24865836.html?ticket=ST-7871286-JAKLMphM455YvRS5bcBC-ap1
https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings
https://www.vrt.be/vrtnws/en/2019/07/10/google-employees-are-eavesdropping-even-in-flemish-living-rooms
https://www.sueddeutsche.de/digital/alexa-siri-google-datenschutz-1.4552480
https://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/microsoft-hoert-bei-skype-mit/story/16596840
https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-05.pdf
https://www.srf.ch/news/regional/basel-baselland/datenschutzprobleme-basler-polizei-auto-weiss-zuviel
https://www.zeit.de/wirtschaft/2017-09/datenschutz-autohersteller-apps-datenverschluesselung-stiftung-warentest

III. Breaking Binance: the world’s largest Bitcoin trading platform is hacked and blackmailed

More than 700 customers of the Bitcoin trading platform Binance found their KYC (know your customer) data – portrait photo of each customer as well as a copy of their Binance sign up information and their passport, ID or driving licence – posted in a public group that had been specially created for the purpose in messenger service Telegram on 7 August. A few hours after the first posts appeared, blockchain-hero.com reported that this data, most of which came from Binance customers in Asia, had apparently been stolen from the database of a partner that Binance had contracted to verify sign-ups. To the best of their knowledge, only customers who signed up between February and March 2018 were affected. Binance experienced another information leakage incident during this period as well. When Binance CEO Changpeng Zhao went on Twitter right after the incident to warn customers, he did not confirm whether the posted data had been stolen during that leak or another attack.

A short time later, Binance published a piece on its blog from which it emerged that an unknown hacker had demanded 300 bitcoins or else he would post an additional 10,000 sign-up photos and KYC data. Binance notified prosecution authorities and announced a reward of up to 25 bitcoins for information that would help identify the culprit and enable Binance to initiate criminal proceedings. As blockchain-hero.com reported, the hacker had allegedly tried to sell the data on the dark net. As this was evidently unsuccessful, he seems to have chosen another approach to making money.

This cybercriminal appears to be following the example of Kim Jong-un, whose state-sponsored hackers used more than 35 cyberattacks on financial institutions and crypto platforms to steal up to USD 2 billion for North Korea’s nuclear programme and weapons programme. These figures come from an official report by independent experts for the United Nations’ committee on North Korean sanctions.

Investigators have had less luck in identifying hackers who cracked Japan’s BITPoint platform on 11 July 2019 and stole more than USD 28 million in various cryptocurrencies from the hot wallets of its operator and around 50,000 customers. Two thirds of that money belonged to customers, while one third belonged to the platform itself. A BITPoint press release following the incident announced that over USD 2.3 million of the stolen funds had already been found on an offshore platform. The next day the company announced that everyone affected by the hack would be compensated for their losses in cryptocurrency.

This was the second major attack on an Asian crypto platform in a matter of weeks. The first occurred on 26 June, when cybercriminals made off with USD 9.3 million in XRP (Ripple) and ADA (Cardano) from Bitrue, a bitcoin trading platform from Singapore.

But both incidents were small change compared to the largest virtual bank robbery in the history of cryptocurrency. In January 2018, a party that remains unidentified to this day used an inadequately secured hot wallet to steal USD 440 million in NEW (New Economy Movement) tokens from around 260,000 customers of Japan’s Coincheck trading platform. Coincheck has since been acquired by online broker Monex and has largely compensated those affected. As of 11 January 2019, it resumed operations with an official licence from the Japanese financial supervisory authority.

Read more:

https://blockchain-hero.com/eilmeldung-binance-kyc-datenleak
https://www.btc-echo.de/breaking-massiver-datenleak-bei-bitcoin-boerse-binance
https://www.binance.com/en/blog/365766157488967680/Statement-on-False-KYC-Leak
https://www.btc-echo.de/gehackte-bitcoin-boerse-bitpoints-verspricht-entschaedigungen-fuer-kunden
https://www.heise.de/newsticker/meldung/Malware-Attacken-ueber-Avalanche-Botnet-Drahtzieher-vor-Gericht-4423942.html
https://de.cointelegraph.com/news/japanese-regulators-grant-cryptocurrency-exchange-license-to-coincheck

From the editors: new on the SWITCHcert security blog

Attacks on DNS continue, with some targets in Switzerland

https://securityblog.switch.ch/2019/07/10/attacks-on-dns-infrastructure-continue/

SWITCH Public DNS Resolver with DoT/DoH support

https://securityblog.switch.ch/2019/08/07/switch-public-dns-resolver/

This SWITCH-CERT security report was written by Dieter Brecheis and Frank Herberg.

The security report does not represent the views of SWITCH; it is a summary of various reports published in the media. SWITCH does not assume any liability for the content or opinions presented in the security report nor for the correctness thereof.