BLOCKCHAIN EXPERTS ARE PUTTING A STOP TO GOVERNMENTS PUTTING BACKDOORS IN SOFTWARE

FREE! 2024 TRENDS AND EMERGING TECHNOLOGY CODEXES

By Matthew Griffin

Security and Privacy

27th August 2017

WHY THIS MATTERS IN BRIEF

- Governments want backdoors in software and criminals want to exploit them to spread malware, now a blockchain based system from Switzerland could put a stop to both

A new blockchain based software update framework from the team at the Decentralized-Distributed Systems (DEDIS) lab at the Swiss Federal Institute of Technology in Lausanne (EPFL), Switzerland could help prevent the spread of malware like Petya, but, as an added bonus it would also make it difficult, if not impossible, for governments to force software companies to deliver software updates with backdoors in them in secret.

From flying aircraft carriers to submarine

FREE! 2024 TRENDS AND EMERGING TECHNOLOGY CODEXES

The Petya ransomware, and its “wiperware” variant NotPetya, were both spread after an attacker managed to take over the network of Ukrainian accounting firm, M.E. Doc, and inject malicious code into one of their legitimate software updates.

The new proof-of-concept technology, which has been dubbed “Chainiac” by its team is a first of a kind decentralised framework that eliminates these single points of failure and enforces a new level of transparency on software updates which, in turn, makes it possible for security analysts and other interested individuals to continuously review and monitor the authenticity of updates and identify vulnerabilities.

“What Chainiac is trying to do,” said Bryan Ford who led the group that conducted the research, “is create an end-to-end architecture for software life cycle management, all the way from the developers to deployment and updates on end-user devices.”

See also Unhackable quantum technologies debut in France

As criminals and nation states continue to increase their attacks on the software supply ch it’s going to become increasingly important that we can ensure the integrity of the software we all use, and rely on. After all, I doubt you’ll want to download a version of Apple’s next iOS update only to then find the NSA, or someone else is watching you via your webcam.

Wave and say hi, now go and get the sticky tape and shove it over the lens – who says beating the government isn’t easy? For example, documents released by NSA whistleblower Edward Snowden revealed that in 2011, the NSA was looking at how to compromise the Google Play Store in order to replace legitimate smartphone apps with backdoor versions they could use to spy on users or even manipulate them with targeted propaganda. And over in the UK, under the Investigatory Powers Act, which came into force in January this year, the government’s currently considering passing a law that will legally compel software makers to build backdoors into their software using secret court orders – and other nations are following suit.

See also Autonomous AI could create an autonomous

FREE! 2024 TRENDS AND EMERGING TECHNOLOGY CODEXES

“How do we know what software we are really running?” said Emin Gün Sirer, associate professor at Cornell University and co-director of the Initiative for Cryptocurrencies and Smart Contracts, “a lot of attacks go after that exact foundation. Someone switches the binaries you’re using but everything appears to be the same.”

Chainiac builds on Cothority, a blockchain based transparency tool Ford’s team released in 2015 that allows independent individuals and experts to collectively sign off on the authenticity of software updates.

Collective signing means that every time Apple, for example, releases a new iOS update the iOS device won’t accept the update until it’s been collectively signed and verified by a threshold number of thousands of trusted witnesses attesting publicly that a valid, non-backdoored update had been issued.

See also The internet pioneer behind Apache pushes blockchain to fuel the next big internet revolution

However, while a collectively signed software updates could still contain backdoored code, example, developers could be bribed, blackmailed, or threatened to insert a backdoor, Cothority, now a component of Chainiac, would make it impossible to ship the update in secret. Chai also integrates reproducible builds, a system which lets technical end users, or automated witness servers, to recompile the source code and get a byte-for-byte identical binary, ensuring the distributed binaries haven’t been tampered with.

“The essence of the idea is that [Chainiac] allows users, who just want the latest binary, to check this one collective signature,” Ford said, “and see that this signature shows that this group of Cothority servers has independently reproduced this binary, and tested that this is the one and only correct output corresponding to the source code that the developer has produced.”

See also Apple iMessage has been upgraded with post quantum encryption

FREE! 2024 TRENDS AND EMERGING TECHNOLOGY CODEXES

cloud servers and embedded devices, plus its downstream variant Ubuntu. Ford’s team tested Chainiac on Debian packages with good results, and Debian seems like they could be an early adopter.

Meanwhile, proprietary software, such as Apple’s iOS or Microsoft’s Windows, could also use Chainiac to achieve similar levels of transparency, Ford emphasized.

“In that case the Cothority nodes responsible for checking the reproducible builds need to be run by organisations that have NDAs with the software provider giving them access to the source code for this purpose. That makes it at least in principle feasible for proprietary software,” he added.

See also First fake regulatory filing sent Blackrock's XRP crypto to the moon

The project also incorporates a novel form of blockchain technology, called a “Skipchain,” t allows software updates to be announced on a distributed ledger.

“Blockchains are used to transfer things, but that’s not their only use,” Sirer said, “they’re grea for transferring things like Bitcoin, but they’re also great for announcing facts. … [Chainiac] i also a broadcast medium for vetting software updates.”

Ford’s research seems unlikely to please government leaders who are increasingly frustrated at the growing use of encryption, as well as the upcoming 5G standard, and how it cuts off their ability in some ways, but not completely, to surveil people.

See also A dead gradma story fooled Bing chat into helping solve a CAPTCHA

If you’re a government type though put down those tissues, and stop wiping your eyes, because, thanks to Quantum Computers, you’ll soon be able to crack over 70 percent of all the encryption

FREE! 2024 TRENDS AND EMERGING TECHNOLOGY CODEXES

Chainiac is the latest salvo in an increasingly bitter war between software makers and governments for control of the integrity of the code on which our lives depend, and it's also likely that nation states who want to subvert the software development process for law enforcement or espionage purposes are already looking for new ways to undermine these new "transparency mechanisms."

See also Self-destructing algorithms could usher in a new era of cyber security

"We've seen sovereign states put enormous resources into hacking," Sirer said, "will [Chain be open to gaming? Will it be more secure or open to attack? There is every reason for hope and every reason for experimentation."

Cryptographers have been vocal against government use of backdoored software updates, arguing that destroying trust in software updates makes everyone less safe, and security e Bruce Schneier, a fellow at the Berkman Klein Center at Harvard University, said it is never acceptable for governments to use backdoored software updates.

"It is akin to a public health issue," he said, "we need everyone to be able to trust the update process implicitly, and that it will always work in the best interests of the user. Hijacking th process for surveillance or espionage purposes threatens to undermine trust in one of the m critical security technologies we need and all rely on."

Backdoors Blockchain Cyber Security Debian Project Linux Foundation
M.E. Doc Malware NSA Public Sector Ransomware Security
Software Updates Swiss Federal Institute of Technology Switzerland
Technology Sector

FREE! 2024 TRENDS AND EMERGING TECHNOLOGY CODEXES