introducing additional risk? What percentage of my proprietary code contains 'stolen' or 'copied' code from other third-party open source libraries without proper attribution?

It's not over

While Equifax holds the spotlight right now, there's a bigger issue that needs attention. The company has fixed the problem and has programmes in place to deal with the ramifications.

"In the cybercrime community, a successful breach gets the attention of other hackers. It starts a long tail of incidents and breaches for months and even years"

The big danger now is an open door for hackers. Heartbleed, which occurred more than three years ago, still leaves a trail of problems for IT security. In the cybercrime community, a successful breach gets the attention of other hackers. It starts a long tail of incidents and breaches for months and even years.

Development teams have the opportunity to play the hero role by initiating processes that produce secure software. Teams can conduct code-level security reviews, in addition to penetration tests, for their internally developed code before deployment. Outsourced development and business partners can conduct code-level audits. Monitoring can be put in place for all other third-party code included in software applications, for security flaws, intellectual property concerns and updated version information. Finally, the institution of internally developed applications with adequate checkpoints enables thorough audit trails.

The technical story behind the Apache Struts 2 vulnerability offers serious lessons and learning opportunities. It's time for development teams to act on them.

About the author

Jeff Luszcz is a VP of product management at Flexera (www.flexerasoftware.com). Previously, he was founder and CTO of Palamida. He has helped software companies learn how to use open source while complying with licence obligations and keeping on top of security issues. Throughout his career, he has been active in the Java, Macintosh and open source software communities. Luszcz is also the author of several well-known Macintosh software utilities and has served as a technical editor for Wrox Press.

References

1. 'Apache Struts Jakarta Multipart Parser Code Execution Vulnerability'. Flexera Secunia Advisory SA75730, 8 Mar 2017. Accessed Jan 2018. https://secuniare-search.flexerasoftware.com/community/advisories/75730.
2. Shah, Hardik. 'Analysing CVE-2017-9791: Apache Struts Vulnerability Can Lead to Remote Code Execution'. McAfee, 19 Jul 2017. Accessed Jan 2018. https://securing-tomorrow.mcafee.com/mcafee-labs/analyzing-cve-2017-9791-apache-struts-vulnerability-can-lead-remote-code-execution/.
3. Sahu, Suraj. 'CVE-2017-5638: Apache Struts 2 Vulnerability Leads to Remote Code Execution'. TrendLabs Security Intelligence Blog, 9 Mar 2017. Accessed Jan 2018. http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-5638-apache-struts-vulnerability-remote-code-execution/.

Securing the blockchain against hackers

Olivier Boireau

Olivier Boireau, Design SHIFT

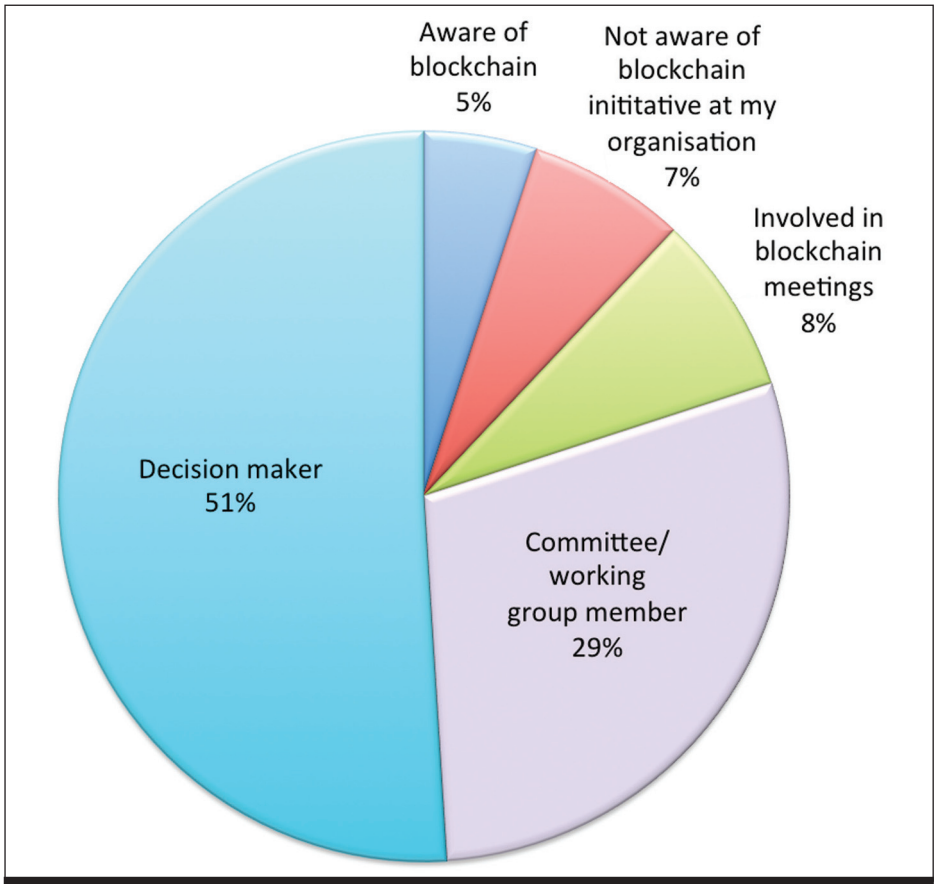
Blockchain technology is transforming the way data is shared and value is transferred. However, there remain significant obstacles that must be overcome before blockchain is ready for mainstream adoption – most notably, security. How to protect both the cryptographic keys that allow access to the ledger and blockchain applications remains a top concern for any organisation or individual interested in using blockchain to transact anything of significant value.

Many hail blockchain technology as a security innovation because it provides a trusted ledger that shifts data storage and protection from a centralised to a decentralised model. Trust comes from the process itself rather than from the status of any one participant. This allows two untrusted parties to efficiently record transactions in a verifiable, permanent way without using an intermediary.

However, while blockchain shows promises in its ability to support an endless number of innovative financial trading, payments, healthcare, government and other critical applications, recent high-profile breaches of exchanges show that blockchain participants and their access to the blockchain represent a security weakness that must be addressed before the technology can reach its full potential.

What is blockchain?

Blockchain is a distributed ledger technology that provides a historical record of all transactions that have taken place



Level of involvement with blockchain initiatives within organisations. Source: Greenwich Associates.

across a peer-to-peer network. Best known as the technology behind the Bitcoin crypto-currency, blockchain takes records – such as proof of ownership, confirmed transactions and contracts – and stores them as 'blocks'. New blocks are linked to previous blocks to form a linear and chronological 'chain' of events.

"Recent high-profile breaches of exchanges show that blockchain participants and their access to the blockchain represent a security weakness that must be addressed"

Any new record is verified by consensus – meaning that various network participants, called 'miners', work together to verify the integrity of the data. Once verified by a majority of the miners, the block is stored in an encrypted and decentralised fashion across the network. This results in a system of record-keeping that is maintained solely by network participants.

Blockchain is revolutionary because it enables the creation and operation of a 'trustless network'. Using blockchain, unrelated parties can transact with one another without pre-existing trust, middlemen or supervisory authorities. In the case of Bitcoin, for instance, blockchain helps create new depository and transaction mechanisms that no longer rely on banks or other third-party intermediaries. This gives blockchain the power to disrupt existing financial systems and create a new financial architecture based on computer algorithms rather than on interpersonal trust.

The power of blockchain to decentralise markets and undermine the control of existing middlemen has captured the imagination of Silicon Valley and Wall Street alike. Moving forward, blockchain isn't just about disintermediating the middleman, but rather about solving problems or seizing opportunities that have eluded current systems.

Despite all the allure of blockchain, significant security challenges still remain. A recent Greenwich Associates survey underscores the importance of overcoming these security roadblocks – 85% of survey respondents are concerned or very concerned that permissioned networks and centralised identity management systems are creating a big target for hackers.

Keys to the kingdom

In blockchain applications, the digital asset and the means to protect it are combined in one token. Nobody can steal or copy the digital asset unless they have the secret code or 'private key' that unlocks the cryptographic protection of the asset. However, storing private keys in software or on a piece of paper is the equivalent of leaving your house keys under the welcome mat.

"Most people currently use software called wallets or multi-signature wallets, but these solutions are driven more by convenience than security. Hardware wallets were designed to offer a higher level of private key security, but even these solutions are vulnerable to hacks"

While blockchain technology secures data in transit from place to place using cryptography, the private key becomes vulnerable to theft when it is stored or displayed at one end or the other – whether that is on a piece of paper, screen, disk, in memory or in the cloud.

To keep digital assets and private keys safe, most people currently use software called wallets or multi-signature wallets, but these solutions are driven more by convenience than security. Hardware wallets, such as Trezor or Keepkey, were designed to offer a higher level of private key security, but even these solutions are vulnerable to various hacks, including fault injections.[1,2]

A fault injection attack is a procedure used to maliciously introduce an error in a computing device in order to alter the software execution. The goal of the fault injection can be to either:

1. Avoid the execution of an instruction.
2. Corrupt the data the processor is working with.

These techniques can be used to compromise the security of hardware wallets

by bypassing security checks or leaking the private keys.

Once private keys are stolen, it does not matter how secure the blockchain itself is – anyone can monetise and exploit the asset and any malicious transfer of value is typically instantaneous and irreversible. Today, hackers commonly target online services that store the private keys for a large number of users or infect network participants with a malware that searches for private keys.

In August 2016, hackers stole $72m worth of bitcoin from accounts at the Hong Kong crypto-currency exchange Bitfinex.[3] In the Bitfinex hack, at least two private keys stored in a multi-signature wallet hosted by BitGo were compromised. Public blockchain participants have lost millions of dollars as a result of compromised security systems.

Lies become truth

Whether executing smart contracts or trading crypto-currencies, the digital assets that blockchains protect exist only in computer code. When stolen, it is possible for hackers to evade detection by rolling back the blockchain to a previous version of the code that existed before the hack. Basically, if more than half of the computers working as nodes to service the network tell a lie, the lie will become the truth.

This is exactly what happened with the Ethereum blockchain when an attacker tried to steal about $50m of the digital currency, Ether.[4] Two other blockchains based on Ethereum, Krypton and Shift, suffered what are commonly referred to as 51% attacks in August 2016.[5,6]

The attack works when hackers are able to compromise over half the nodes participating in the distributed ledger, in which case, they can prevent new transactions from gaining confirmations and halt transactions between some or all users. They also can reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins if attacking a crypto-currency blockchain.

Blockchains (like all distributed systems) are not so much resistant to bad actors as they are 'anti-fragile' – meaning, they respond to attacks and grow stronger. However, this requires a large network of users. If a blockchain is not a robust network with a widely distributed grid of nodes, it becomes more difficult to ensure the immutability of the ledger.

Protecting blockchains

Today, many security-conscious organisations rely on hardware security modules (HSMs) to safeguard and manage their digital keys. An HSM is a crypto-processor that securely generates, protects and stores keys. HSMs typically guarantee a level of regulatory assurance, in compliance with either the Federal Information Processing Standard (FIPS) certification or Common Criteria, an international standard – meaning that each device meets strict industrial-grade security control requirements.

"To execute a successful attack, attackers would either need to have administrative privileges, access to data before it is encrypted, or physical access to the HSM, which makes the attack vector extremely difficult and unprofitable for a hacker"

HSMs are designed to protect potential access points in virtually any application that requires secure, verified digital signatures. People rely on the security provided by HSMs in their everyday life without even knowing it. HSMs housed in bank datacentres verify PIN numbers every time a customer withdraws cash from an ATM and validate transactions at merchant POS terminals when consumers purchase goods.

Using HSMs to protect blockchain ledgers, digital wallets and applications against hacks can provide the trusted computing environment necessary to take full advantage of the blockchain protocol. To execute a successful attack, attackers would either need to have administrative privileges, access to data before it is encrypted, or physical access to the HSM, which makes the attack vector extremely difficult and unprofitable for a hacker. Some 58% of participants in the Greenwich Associates study agreed that HSMs are an essential part of addressing blockchain security concerns.

What makes HSMs so strong?

It seems to be obvious that cryptographic operations must be performed in a trusted environment – meaning no possibility of exposure due to viruses, malware, exploits or unauthorised access. But an ordinary wallet mixes the access code, business-logic and cryptographic calls in one big application. This is a dangerous approach because an attacker can then use crafted data and vulnerabilities to access cryptographic material or steal keys.

HSMs are dedicated hardware systems specifically designed to store and manage private and public keys. The entire cryptographic key lifecycle – from provisioning, managing and storing to disposing of or archiving the keys – occurs in the HSM. Digital signatures also may be captured via an HSM, and all access transactions are logged to create an audit trail.

An HSM is hardened against tampering or damage and may be located in a physically secure area of a datacentre to prevent unauthorised contact. The module may be embedded in other hardware, connected to a server as part of a network, or used as a standalone device offline.

An HSM is a trusted computing environment because it:

- Is built on top of specialised hardware, which is well-tested and certified in special laboratories.
- Has a security-focused OS.
- Limits access via a network interface that is strictly controlled by internal rules.
- Actively hides and protects cryptographic material.

Delivering industrial-grade security to the masses

Previously, HSMs were mainly used to protect digital assets and keys in institutional settings due to the high cost and

complexity of solutions developed to meet the needs of large datacentres. But recently a new category of personal computers has emerged that makes industrial-grade security available to the masses in a form factor that is affordable and easy to use.[7]

"Using trusted computers will give security-conscious users and organisations assurance that no matter what blockchain application they choose, they have the means to protect digital assets"

This next generation of ultra-secure PCs comes with an embedded HSM and requires two factors of authentication (a key and a password) to make sure that unauthorised users cannot access the device. Additionally, the PC is protected against physical attacks with a tamper-proof casing and the private key is erased if any of the PC's physical or logical security controls are breached.

Using trusted computers in place of digital wallets and as blockchain nodes provides the missing link that will give security-conscious users and organisations assurance that no matter what blockchain application they choose, they have the means to protect digital assets using a turnkey solution that is virtually impenetrable.

Innovations in blockchain security will make the technology increasingly attractive – and usable – for a wider number of organisations and consumers. It is difficult to predict where blockchain technology is headed next, but it has all the makings of a truly disruptive technology.

About the author

Olivier Boireau is the CEO and founder of Design SHIFT. He also develops hardware and software for POS, cameras, smartphones, netbooks and consumer electronics devices. He specialises in defining wireless hardware architecture, developing strategies for hardware device design (original design manufacturer, silicon partners, software platforms) and has received numerous industry awards for his innovations.

References

1. 'Tomshwom'. 'Lessons from the Trezor Hack'. Steemit, Aug 2017. Accessed Jan 2018. https://steemit.com/bitcoin/@tomshwom/lessons-from-the-trezor-hack.
2. Redman, Jamie. 'A Def Con 25 Demonstration Claims to Break Bitcoin Hardware Wallets'. Bitcoin.com, 27 Jun 2017. Accessed Jan 2018. https://news.bitcoin.com/def-con-25-demonstration-break-bitcoin-hardware-wallets/.
3. Baldwin, Clare. 'Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong'. Reuters, 3 Aug 2016. Accessed Jan 2018. www.reuters.com/article/us-bitfinex-hacked-hongkong/bitcoin-worth-72-million-stolen-from-bitfinex-exchange-in-hong-kong-idUSKCN10E0KP.
4. Popper, Nathaniel. 'A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency'. New York Times, 17 Jun 2016. Accessed Jan 2018. www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html.
5. 'Krypton recovers from a new type of 51% network attack'. Crypto Hustle, 26 Aug 2016. Accessed Jan 2018. https://cryptohustle.com/krypton-recovers-from-a-new-type-of-51-network-attack.
6. Redman, Jamie. 'Small Ethereum Clones Getting Attacked by Mysterious '51 Crew'. Bitcoin.com, 4 Sep 2016. Accessed Jan 2018. https://news.bitcoin.com/ethereum-clones-susceptible-51-attacks/.
7. Calore, Michael. 'This ultra-secure PC self destructs if someone messes with it'. Wired, 23 Jun 2017. Accessed Jan 2018. www.wired.com/2017/06/orwl-secure-desktop-computer/.

Blurring the boundaries between networking and IT security


Dave Nicholson

Dave Nicholson, Axial Systems

Networking and security used to be largely separate IT methodologies. They were even built separately. Traditionally, networks were constructed on standard building blocks (switches, routers etc) and security solutions such as perimeter firewalls, intrusion prevention systems and the like were applied afterwards.

As such these two key areas of operational technology could effectively be treated as separate domains by businesses, each with their own set of tools, strategic approaches and dedicated operational teams. IT security departments typically focused on the delivery of time-honoured threat detection methods and perimeter-based security defence mechanisms as well as incident response and remediation. Networking teams were more concerned with issues around latency, reliability and bandwidth.