GBBC Open-Source Ideas Series: Cybersecurity

Part I: Delivering 21st Century Information Security

14 January 2021

Edinburgh, Scotland

"Every barbarian is at every gate"

Andy Greenberg, Senior Writer for WIRED, in his monograph *Sandworm*, reflecting on a new era of cyber warfare following the 2017 NotPetya malware attack on the Ukrainian power grid.[1]

An Inconvenient Truth

Delivering continuous data assurance

The compromise of Texas-based SolarWinds, a company which provides computer networking monitoring services to corporations and government agencies worldwide, reveals a new generation of cyberattack characterised by access, sophistication, and patience. In this case, the source code of SolarWind's Orion platform was compromised and directly modified to include malicious backdoor code which was compiled, signed, and delivered through an existing software patch release management system. While the scope of the compromise is still being assessed, the injected malware has potentially allowed a cyber attacker, thought to be a state-sponsored agency, access to the networks of over 18,000 customers. A security vendor who decoded SolarWind's Domain Generation Algorithm (DGA) revealed that government agencies, multinational corporations, and universities were potentially compromised.[2]

While it is too early to assess the impact of the SolarWinds hack conclusively, it is clearly a very sophisticated clandestine cyberattack. Moreover, one that went undetected for over a year, during which the attackers were able to prove that the Orion supply chain could be compromised multiple times and used as a trojan horse.[3]

As defined by emerging technology journalist Maria Korolov, a supply chain attack, also called a value-chain or third-party attack, occurs when someone infiltrates a system through an outside partner or provider with access to the target's systems and data. This has dramatically changed the attack surface of the typical enterprise in the past few years, with more suppliers and service providers touching sensitive data than ever before.[4]

As a case study, SolarWinds reveals the pressing need for enterprises to protect their critical data, detect any attempts to tamper with it, respond in real time, and recover the original data. To achieve this, cybersecurity initiatives need to move beyond simply tracking data changes to delivering continuous data assurance.

[1] Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers by Andy Greenberg (Random House: 2019)

[2] See SolarWinds victims revealed after cracking the Sunburst malware DGA *Bleeping Computer* (Sergio Gatlan, December 22 2020)

[3] See Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor *FireEye Threat Research Blog* (December 13 2020)

[4] Supply chain attacks show why you should be wary of third-party providers *CSO from IDG* (Maria Korolov, October 22 2020)

Data, distrust, and an impending crisis in the 21st century

The advent of the internet and the web has enabled an interconnected, hyper-accessible, and globalised economy which has created practically immeasurable value. Like the spoils of empire, the relentless innovation of the digital age has had an endemic influence on the character of modern states, economies, and their respective citizens. Economic historians confidently attribute the collapse of the British Empire to the concentrated allocation of resources during the war efforts of the twentieth century in Europe, which weakened and eroded its authority overseas, enabling the loss of Britain's key imperial assets, diplomatically and violently. It is a neat historical explanation, expressed via the relationship between the centre and its peripheries. However, such an analogy cannot be applied to the multi-party, globalised nature of the digital economy. For this, the key asset is trust – entities must trust the veracity of the data, the veracity of the networks, and the veracity of the software that enables transactions. Without trust, the systems upon which our modern economies rely can fail, presenting an impending and avoidable crisis of modernity.

The inconvenient truth is that trust in data is under sustained attack and our defences are deeply vulnerable

Data has undergone rapid organisational transformation in the last decade, reflecting the aggressive digital transformations that companies have undergone to remain competitive. Companies have become decentralised and so has their data. The data has never been more exposed by moving to locations in the cloud and hybrid cloud/data centre locations. The result is that data which companies were able to keep confidential and proprietary is now exposed to competitors and nation states seeking competitive advantage. Maintaining control of this data that is now outside the walls of companies and governmental organizations is the cause of a major inconvenient truth: data is no longer fully confidential with today's tools and methods and, worse still, data is no longer immutable and is vulnerable to malicious change.

The economies of scale afforded by the emergence of major cloud service providers have enabled the development of myriad software tools and services, which in turn has enabled more efficient, decentralised business models. However, the deepening complexity of the supply chain underpinning critical business services has led to less centralised control over data and a weaker trust architecture. We are at an inflection point where half of all data is now stored in the cloud, half of which is classified as sensitive. IBM has determined that 78% and 36% of enterprises are storing sensitive data in software as a service (SaaS) and platform as a service (PaaS) offerings, respectively.[5]

The proliferation of data and its access points has led to systemic data breaches and leaks, affecting almost half of all businesses in the last year at an average cost of $4.27 million per breach globally; in the United States the average cost is a staggering $8.64 million.[6]

[5] The Changing Face of Data Security - 2020 Thales Data Threat Report p. 9

[6] IBM Security - 2020 Cost of a Data Breach Report p. 12

Governments are reporting sustained cyber-offensive campaigns that threaten national security. For example, the United Kingdom's National Cyber Security Centre reported 60 'high-level' cyberattacks on the UK per month.[7] Critical National Infrastructure (CNI) across the world has proven vulnerable to cyberattacks, as older computer systems were often designed before cybersecurity was a major concern. As illustrated with Sandworm, critical attacks have involved power grids, nuclear power plants, hospitals, telecommunications, and more. Public policy now must create standard responses to possible cyber-physical disasters and, in cases where government communications may have been potentially breached, all data must be considered compromised. This is an immediate concern in the aftermath of the SolarWinds hack given the recent revelation that a foreign state almost certainly has ongoing access to U.S. government networks.

With the interconnectedness of the physical and digital world accelerated by the Internet of Things (IoT), the placement of data in the cloud, as well as on storage devices both within a corporate network and at the edge, the problem of data vulnerability will become worse unless a new approach is adopted. To make matters worse, advances in quantum computing mean that data storage must be able to adapt as encryption methods become obsolete.

At present, cybersecurity focuses on on-premises, perimeter-centric approaches, which does not reflect the reality of global, competitive business models which interact with an array of interconnected services provided by a growing ecosystem of software vendors. The Thales Group, a leading security company, advocates for an alternative approach: the zero-trust model.

In its 2020 Data Threat Report, Thales describes a zero-trust model as requiring "a least privileged, continuous validation and verification approach, providing both network and application centric access protections" to eliminate the binary trust versus do not trust approach prevalent today.[8] This is a hat-tip to the consensus, consortium-driven model provided by blockchain technology.

A zero-trust, consensus-driven approach: the application of blockchain to data assurance and security

Now that the redoubt approach, comprising firewall-defended moats protecting company networks, has been shown to be severely lacking by hackers, a zero-trust security model has become the way of protecting every creator and consumer of data.

Blockchain technology has the capability to satisfy a zero-trust approach to data assurance and security. The consensus-driven, consortium-based architecture of a blockchain accurately reflects the needs of multi-party, distributed business models. It does this by providing a method to continuously verify transactions while ensuring that each party makes decisions based on a single source of truth. A computational answer to the age-old Byzantine Generals Problem, blockchain,

[7] UK Parliament Research Briefing - Cyber Security of UK Infrastructure *UK Parliament POSTnote 554* (Harry Beeson, May 2 2017)
[8] The Changing Face of Data Security - 2020 Thales Data Threat Report p. 9

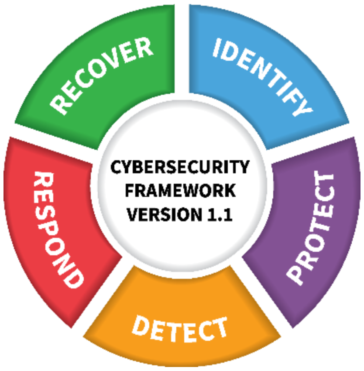
deployed correctly, can protect that commodity which is essential to the functioning of globalised systems: trust.

The acceptance of blockchain as a means beyond cryptocurrency to develop trust is well acknowledged and its adoption across a variety of enterprise use cases has increased thanks to the development of open source software foundations providing open standards and governance for the development of relevant protocols, consensus mechanisms, libraries, tools, and languages. Prominent foundations include the Hyperledger initiative[9], which is part of the wider Linux Foundation umbrella, and the Enterprise Ethereum Alliance.[10] The increasing receptiveness of government regulation worldwide on the adoption of blockchain, particularly in financial services, is also an encouraging sign.

Data Integrity, Blockchain and the NIST Cybersecurity Framework

In its Cost of a Data Breach 2020 report, IBM determined that the average time it takes for a company to identify and contain a breach is 280 days. The healthcare sector has suffered the longest breach 'lifecycle' at 329 days.[11]

The National Institute of Standards and Technology (NIST) Cybersecurity Framework[12] was created as part of President Obama's Executive Order on Cyber Security[13] and is composed of three distinct phases:



1. Identify & Protect
2. Detect & Respond
3. Recover

In response to the increasing number of ransomware attacks NIST recently published a draft whitepaper focusing on its use by organizations.[14]

Applying this framework to data integrity, once you have **identified** critical data in your organization, at a bare minimum you need to **protect** it but preferably also **detect** any attempts to compromise it in order to **respond** effectively and **recover** it.

[9] See Hyperledger - Open Source Blockchain Technologies
[10] See Enterprise Ethereum Alliance
[11] IBM Security - 2020 Cost of a Data Breach Report p.11
[12] NIST Cybersecurity Framework
[13] Foreign Policy Cyber Security Executive Order 13636 | The White House
[14] Securing Data Integrity Against Ransomware Attacks: Using the NIST Cybersecurity Framework and NIST Cybersecurity Practice Guides

If there is a breach, it is critical that it is detected as quickly as possible so the organization can respond to the threat, ideally remedying it and ultimately recovering their data. Blockchain has a significant role to play addressing three key areas: protect, detect, and recover.

A simplistic approach: cryptographic hashing

Cryptographic hashing[15] has been widely adopted by cybersecurity companies to ensure that critical data files have not been tampered with, as any change to a file results in a corresponding change to the hash. Once stored on a blockchain these hashes become immutable references which, underpinned by an efficient consensus mechanism, provide users with the assurance that a bad actor cannot hide the fact that a file or record has been changed.

Used correctly, cryptographic hashing is certainly a step in the right direction as a value-add to existing cybersecurity best practices because it allows organizations to determine if a file is the original file as created. However, it is practically impossible to determine when a file was changed, how it was changed, or who changed it.

In short, storing cryptographic hashes protects critical data to the extent that it enables an organization to detect that it has been tampered with, though this could be weeks or months after the breach occurred. In addition, recovering the original data from its hash is impossible.

A holistic approach: a blockchain-based file system

A more robust approach involves using a blockchain to implement a blockchain-based file system where the entire file is stored on blockchain from its inception onwards, instead of just a cryptographic hash after the fact.

An immediate advantage is that the user no longer has to store their file on one system with the verifying hash stored on an entirely different system. Instead, users can eliminate the associated risk of dealing with two locations by storing the entire file on a blockchain. Furthermore, this file can be stored with an encrypted immutable record of all changes, who made those changes, and when they made them. Instead of comparing the hash to the original file, one has an immutable record of all file alterations and creation dates. Additionally, unlike the hash, it is possible to restore the file change by change to get to the original file. As changes are made to the file, an alert may be sent to a Security Orchestration, Automation and Response (SOAR) dashboard.

In short, this approach is well aligned with the NIST cybersecurity framework as it ensures that the file is **protected**, that any changes to it can be **detected** as soon as they occur, and, most important of all, that the original file is **recoverable**.

[15] See for example Cryptographic Hashing *Hackernoon* (Shaan Ray, November 3 2017)

Ubiquity is the key to enterprise adoption

Another advantage of implementing a blockchain-based file system is that file systems are ubiquitous, the cornerstone of storage for organizations worldwide. Implementing data assurance in this way makes it easy to integrate it within existing IT operational workflows. In contrast, introducing changes to these well-established workflows in order to accommodate new software products invariably leaves holes at the edges that can be exploited.

The truth is that the assembly of all the software applications of an organization has lent itself to being protected by machine learning (ML) and artificial intelligence (AI). But then the organization is dependent on their AI and ML being better than the attackers' AI and ML. The AI and ML tools of the organization and those of the attacker are seeking the same vulnerabilities and opportunities. No organization wants to be at war with hackers. When it comes to data, an organization cannot depend solely on hunting down the weaknesses in its network, as by then it is often too late.

For a zero-trust IT organization, data is the first and most important layer that must be protected. Most systems store data in a file system or a database which itself may be based on a file system. However, instead of protecting critical data by hashing it and piping that hash to a blockchain, each system stores its entire data on a node of a blockchain. There is no need for the added complexity of constantly comparing the hash against the file to ensure it has not been compromised. Instead, the data is readily available using a standard idiom, the file system, backed by a blockchain.

Storage of critical data on a blockchain using a common interface, a file system, can be thought of as the baseline for zero-trust IT systems

Three key benefits of this approach

First, the data needs to be approved via a programmatic "consensus" mechanism prior to storage on the blockchain-based file system. Rejected files are brought to the immediate attention of the IT administrator.

Second, once on the blockchain, the entire file is then "chained" cryptographically to the prior file written to the file system. This immutability is part of the appeal of the blockchain, as it increases the sophistication required to get to the data.

Third, any file is automatically distributed to the other nodes on the chain, which can be in physically distributed locations. Although perceived by some IT organizations as a weakness, this is actually an advantage: an organization of any size has an online real time multi-site backup of its critical data, especially for its operational systems. This eliminates the need for complex and time-consuming backup software or "cold storage" of data in case of a catastrophic loss of operational data.

Thus, there is no need for IT organizations to periodically backup this data offsite. Because the entire file is represented within a file system, the blockchain replaces the need for these backup systems, as the blockchain maintains a perfect replica at all of its nodes. Any attempt to change the files on any given node will immediately alert the IT administrator. Furthermore, the validation and cryptographic enclosures ensure that any intrusion into the data files is automatically detected. A blockchain-based file system enables greater protection against a compromise in which a malicious actor has secured root permissions.

Protecting against supply chain attacks

Returning to the SolarWinds Orion supply chain attack, the hackers identified an inherent weakness in the software distribution mechanism itself. According to analysts, they were able to compromise the server responsible for managing this, which allowed them to create a malware version of the Orion software that included a backdoor, which was then rolled out to 18,000 SolarWinds customers.[16]

Fortunately, one of the SolarWinds customers affected was cybersecurity specialist FireEye, whose team discovered and named the original Sandworm attack in 2014.[17] FireEye also discovered this supply chain attack and raised the alarm. It is also becoming clear that there are links between the two attacks.[18]

This begs the question: could this latest attack have been prevented by protecting the data - in this case the Orion source code itself - using a blockchain-based file system?

Had this been done, any update to the source code would have been automatically flagged and could have been verified or, if unauthorised, investigated immediately. As it was, the hackers were able to release multiple versions of these trojanised updates over many months.

This is a canonical use case that BTP and its partner Taekion have set out to address with the release of Sextant for TFS, a specialised version of BTP Sextant that deploys and manages the Taekion File System, a blockchain-based file system implemented on Hyperledger Sawtooth.

Introducing the Taekion File System

The Taekion File System (TFS) has been developed with the help of seed funding from the U.S. National Science Foundation and the U.S. Department of Energy in the form of a Small Business Innovation Research (SBIR) award to Taekion, a U.S.-based cybersecurity startup, to build secure enclaves for critical national infrastructure.[19] They were tasked with developing a solution that

[16] Microsoft unleashes 'Death Star' on SolarWinds hackers in extraordinary response to breach *Geekwire* (Christopher Budd, December 16 2020)
[17] Here's the Evidence That Links Russia's Most Brazen Cyberattacks WIRED (Andy Greenberg, November 15 2019)
[18] The SolarWinds Hackers Shared Tricks With a Notorious Russian Spy Group WIRED (Andy Greenberg, January 11 2021)
[19] US Energy Department Eyes Blockchain to Prevent Power Plant Cyberattacks *Coindesk* (Togita Khatri: April 11 2019)

would store attributes for a variety of different systems with various storage methods designed to last for decades.

Taekion recognized early on that a permissioned blockchain had the capability to ensure that that decentralized systems could share critical data while assured that each participant had access to a single source of truth. They chose Hyperledger Sawtooth[20], an open source blockchain framework whose source code was initially contributed by Intel Labs to the Hyperledger initiative.

A key requirement of Taekion's work with the U.S. Department of Energy was that critical operational data needed to be shared efficiently and securely across a multitude of various devices, potentially over a wide area network. However, unlike typical hashing models, Taekion took the approach of enabling entire files to be stored on the blockchain, an approach which has been productised as TFS.

By having the entire file on the blockchain, TFS can track all changes in a single, metadata file which is stored immutably. This ensures that a user can track any changes based on who made the change (based on ID), when it was made, and potentially where it was made.

Crucially, TFS retains all the features of a journaling file system – storing the entire file on the blockchain but ensuring that standard operations are available to the end user, such as taking snapshots, creating files, or deleting volumes.

Delivering TFS

To deliver TFS, Taekion has teamed up with Blockchain Technology Partners (BTP) and selected their blockchain and smart contract management platform, BTP Sextant, to automate the deployment and management of the underlying permissioned blockchain network required by TFS.

Sextant is a product that radically simplifies the deployment and ongoing management of blockchain and smart contract infrastructure, whether for an enterprise, a network operator, or a full-blown consortium. A key consideration for Taekion was that BTP also provides long term support for Hyperledger Sawtooth through its freely available software distribution, Paralos[21], which is in turn used extensively by Sextant.

Since their initial meeting at Hyperledger Global Forum 2020 in Phoenix the two companies have forged a strong partnership which has led to the development of Sextant for TFS, a specialised version of BTP Sextant designed to deliver TFS. Sextant for TFS ensures that TFS is easy to administer and can be used as a potential drop-in replacement for conventional systems

[20] See Hyperledger Sawtooth *Investopedia*

[21] BTP delivers Paralos—the first long term support (LTS) release of its Hyperledger Sawtooth distribution *Medium* (BTP Press Release, April 29 2020)

that provide advanced information assurance (e.g. supporting mission or life critical file syste ms distributed to various managed locations across a corporate network).

Until now, blockchain has been a square peg to security's round hole within most corporate infrastructure. However, integrating Sextant for TFS into a company's Security Orchestration, Automation, and Response (SOAR) cybersecurity orchestration dashboard brings the blockchain closer to the cyber security infrastructure that today's security conscious companies use.

The result is a highly secure file system that retains the operational patterns of a file system with the advantages of a blockchain, all integrated into modern cybersecurity operations without having to adopt a new mode of operation and overcome a steep learning curve.

Sextant for TFS brings a blockchain into the modern corporation's security infrastructure, offering a clear path to attaining three key NIST cybersecurity framework requirements — protect, detect and recover — to keep files from being swept away by another "SolarWinds" style supply chain attack.

About Blockchain Technology Partners

Founded in 2018, BTP is a leading enterprise blockchain company. BTP brings the benefits of blockchain, smart contracts and military grade data protection to business by providing Sextant — a management platform that radically simplifies the deployment and ongoing management of distributed ledgers, smart contract and secure data infrastructure.

BTP has strategic partnerships with Digital Asset and Taekion. Its customers include The Demex Group, Tel Aviv Stock Exchange and Quantum Materials Corp. BTP has offices in Edinburgh and New York and is a member of the Global Blockchain Business Council, the InterWork Alliance, Hyperledger, the Cloud Native Computing Foundation, ScotlandIS and techUK. Learn more at https://blockchaintp.com

About Taekion

Taekion is a data security company created by two Colorado software startup veterans in 2017. Focused on its core mission of keeping mission critical data safe, Taekion has been awarded development grants from the US National Science Foundation and the Department of Energy. The result is the Taekion File System (TFS), a highly secure distributed file system built with a blockchain at its core. TFS is built to ensure seamless integration into today's networks and cyber security platforms while appearing as a simple file system.

Taekion brings the immutability of a blockchain along with ease of use and management for full file integrity. For more information visit https://taekion.com

Sextant for TFS™ Overview

The Sextant for TFS product brought to you by Taekion and Blockchain Technology Partners is an easy-to-use blockchain-based trusted data solution that keeps data safe, tamper-resistant, verifiable, and trusted over your system's life cycle. The solution can prevent unauthorized activity such as file modifications, deletions, or false data injection attacks. The product is simple to integrate and maintain using one-click deployment using best-in-class open source components. Sextant for TFS protects data from source to destination and is designed to be the data protocol that underlies all decision making and analytical systems providing decision makers with an initial "Ground State" for truth. It protects data before it can be compromised.

References

The SolarWinds Hackers Shared Tricks With a Notorious Russian Spy Group WIRED (Andy Greenberg, January 11 2021)

SolarWinds victims revealed after cracking the Sunburst malware DGA *Bleeping Computer* (Sergio Gatlan, December 22 2020)

Microsoft unleashes 'Death Star' on SolarWinds hackers in extraordinary response to breach *Geekwire* (Christopher Budd, December 16 2020)

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor *FireEye Threat Research Blog* (December 13 2020)

Here's the Evidence That Links Russia's Most Brazen Cyberattacks WIRED (Andy Greenberg, November 15 2019)

Supply chain attacks show why you should be wary of third-party providers *CSO from IDG* (Maria Korolov, October 22 2020)

The Changing Face of Data Security - 2020 Thales Data Threat Report (April 2020)

BTP delivers Paralos—the first long term support (LTS) release of its Hyperledger Sawtooth distribution *Medium* (BTP Press Release, April 29 2020)

US Energy Department Eyes Blockchain to Prevent Power Plant Cyberattacks *Coindesk* (Togita Khatri: April 11 2019)

Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers by Andy Greenberg (Random House: 2019)

Cryptographic Hashing *Hackernoon* (Shaan Ray, November 3 2017)

UK Parliament Research Briefing - Cyber Security of UK Infrastructure *UK Parliament POSTnote 554* (Harry Beeson, May 2 2017)

IBM Security - 2020 Cost of a Data Breach Report

Foreign Policy Cyber Security Executive Order 13636 | The White House

NIST Cybersecurity Framework

Securing Data Integrity Against Ransomware Attacks: Using the NIST Cybersecurity Framework and NIST Cybersecurity Practice Guides