Gaining Confidence in the Cloud

By Phillip Griffin – ISSA Fellow, Raleigh Chapter and Jeff Stapleton – ISSA member, Fort Worth Chapter

In cloud deployments organizations remain responsible for ensuring the security of their data. Can cloud-based technologies, such as the blockchain, play a role in providing cloud subscribers assurance their data is being properly managed and that their cloud service provider is in compliance with established security policies and practices?

Abstract

The Cloud offers organizations faster, cheaper, richer, and sometimes more secure application deployments than they themselves can orchestrate. However, organizations remain responsible for ensuring the security of their data, even when they transfer its physical control to a cloud service provider (CSP). What information does an organization require from a CSP to gain confidence they are meeting their data governance obligations? Can cloud-based technologies, such as the blockchain, play a role in providing cloud subscribers assurance their data is being properly managed and that their CSP is in compliance with established security policies and practices? For the financial service industry the X9.125 standard is under development to define requirements and provide a compliance model using blockchain technology.

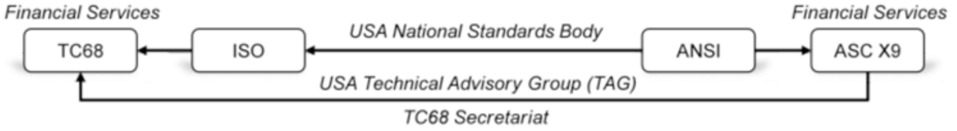

Figure 1 – Standards overview

Introduction

As organizations embrace the Cloud and migration or deploy applications and invariably data, they transfer control from internal processes to a cloud service provider (CSP). However, organizations (subscribers) remain responsible for industry information-security compliance despite the delegation to the CSP. Health care[1] data and payment[2] data notwithstanding, organizations must ensure they exert adequate governance over how their data is protected. Regardless of where their data is located and who actually has physical control over the data—whether within a virtual environment or the cloud—the organization remains responsible for ensuring it can meet legal and regulatory control requirements. For the financial services industry, the X9.125 standard for cloud compliance is being developed to address requirements and compliance between a cloud subscriber and its CSP.

Some background might help clarify how X9.125 fits into financial and cloud services. As shown in figure 1, the American National Standards Institute[3] (ANSI) is the United States' representative to the International Standards Organization[4] (ISO) among others. However, ANSI does not develop standards; rather, they accredit other organizations as industry-specific standards developers and technical advisory groups (TAG) to ISO technical committees. The Accredited Standards Committee X9[5] (ASC X9 or just X9) is one such organization designated by ANSI to perform the following roles:

- Develop ANSI standards for the financial services industry

[1] http://www.hhs.gov/ocr/privacy/index.html.

[2] https://www.pcisecuritystandards.org/.

[3] www.ansi.org.

[4] www.iso.org.

[5] www.x9.org.

- Represent the United States as the TAG to ISO technical committee 68 Financial Services (TC68)
- Manage TC68 and as the official secretariat

Consequently, many X9 standards are submitted to ISO for international standardization. Further, X9 often initiates ISO work items, adopts ISO financial standards, and retires ANSI standards in favor of its ISO version. Sometimes the US markets are uniquely distinct that a domestic X9 standard is needed in absence or parallel with an ISO standard. The cloud security work item is assigned to the X9F4 cryptographic protocols and application security work group; Jeff Stapleton is the X9F4 chair, and Phil Griffin is the X9.125 editor.

One of the first X9F4 actions was to review the existing body of work including special publications from the National Institute of Standards and Technology (NIST),[6] Federal Financial Institutions Examination Council (FFIEC)[7] cloud computing recommendations, Central Intelligence Agency (CIA) views on cloud computing, and the Cloud Security Alliance (CSA) research on comparable audit programs. These materials were digested to formulate a core set of security requirements for managing and securing information in the cloud, whether this information is located in a private cloud completely under control of the organization, or managed in a hybrid or public cloud environment. Regardless of the cloud service type or environment, these basic questions were identified:

1. What security controls does the cloud subscriber (the consumer of the cloud services) need to protect the confidentiality and integrity of its data?
2. What security controls does the cloud service provider offer to protect the confidentiality and integrity of its subscriber's data?
3. What security controls provided by the cloud service provider can be monitored by the cloud subscriber to verify compliance?

While the development of X9.125 is still work in progress and has undergone several redesigns, cloud services and its adoption in the financial industry have continued to evolve. Thus the X9.125 standard is attempting to hit a moving target. X9 standards provide requirements ("shall") and recommendations ("should") that are practical and verifiable. Thus, as shown in figure 2, the standard needs to address security controls and interoperability between the cloud service provider and the cloud subscriber, in addition transparency of any service sub-providers.

Cloud service providers, like any organization relying on information technology (IT), need to have their security controls documented in policy (why), practices (what), and procedures (who). They also need to securely manage resources, including people, places, and processes. IT controls include network, systems, and applications addressing authentication, authorization, and accountability (AAA). Data must also be managed across its life cycle including creation, distribution, storage, and termination. When cryptography is used, the keys must be managed in a secure manner. How the controls are deployed and managed depends on the relationship between the CSP and the subscriber is depicted in figure 2:

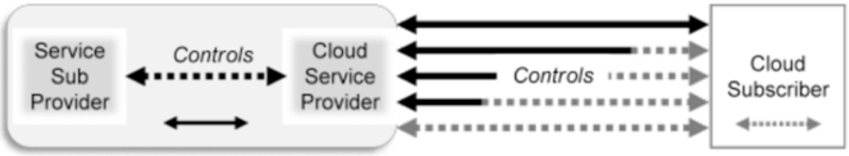

Figure 2 – Controls overview

- The topmost solid arrow shows the case when controls are provided solely by the CSP to the subscriber. For example, the CSP might encrypt the subscriber's data in storage using cryptographic keys managed solely by the CSP.
- The middle arrows show cases when controls are mutually managed by both the CSP and the subscriber. For example, data in transit is encrypted using a session key that is dynamically established, based on an exchange of public key certificates between the CSP and the subscriber.
- The bottommost dotted arrow shows the case when controls are provided solely by the subscriber. For example, the subscriber might encrypt or tokenize data before it is sent to the CSP for storage or processing.
- The dotted arrow between the CSP and its service sub-provider shows the case when controls are provided indirectly to the subscriber by the sub-provider. For example, the sub-provider might be a tokenization service used by the CSP to protect the subscriber's data in storage.

While the X9.125 is still work in progress, another major aspect is to develop a reporting model such that a cloud subscriber can verify a CSP's compliance. Compliance might be to the CSP policy and practices aligned with the subscriber, or preferably the security requirements being defined in the X9.125 standard adopted by both parties. Regardless, this implies that the CSP provides compliance information that is reliable and verifiable. One method for a digital ledger might be blockchain technology, more contemporarily known because of Bitcoin.

Blockchains

Blockchains have been around for decades. Notably Merkle trees were addressed in a US Patent [2] issued in 1982; so the technology is well vetted. While the Bitcoin blockchain is used as a general ledger for Bitcoin transactions, any information can be encapsulated within a blockchain that can provide data integrity. Incorporating timestamps within the blockchain (as does Bitcoin) also provides a historical record

[6] http://csrc.nist.gov/publications/PubsSPs.html.

[7] http://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf

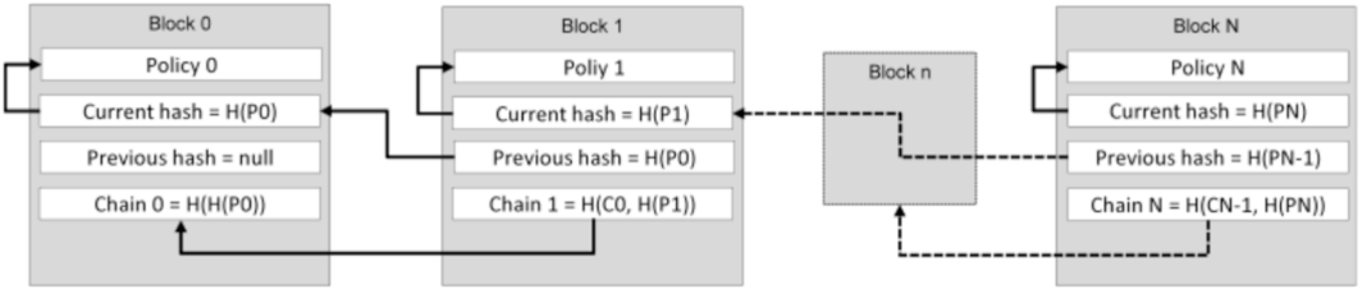

Figure 3 – Simple blockchain

of what happened when and by whom. Consider figure 3 as an example.

The blocks are number sequentially: Block 0, 1…to N. There is always an initial block conventionally numbered "0" to indicate its special nature. There is always a last block (N) which is the most current addition to the blockchain. Each block contains data, in this example a cloud service provider's policy numbered accordingly to its block number: P0, P1…PN and so on. In this example, each block contains a hash (H) of its own policy data, essentially a link to itself, so Block 0 contains H(P0), Block 1 contains H(P1), and Block N contains H(PN). Additionally, each block contains a hash of its processor, so Block 1 contains H(P0) as a link to Block 0, and Block N contains H(PN-1) as a link to Block N-1. Note that Block 0 does not contain a previous link since Block 0 is the blockchain origin. At this point one might think that the blockchain is completely reliable, but it turns out that simple links based on a hash of just the data in the previous block is unreliable.

Consider an attacker that takes some intermediary Block K which links to Block K-1 and has Block K+1 linked to it. The attacker makes a replica of Block K, which we will call Block J, modifies the data so it contains PJ and no longer PK, and publishes it as the real Block K. The attacker then updates Block K+1 to link to Block J instead of Block K. Thus, the blockchain has been compromised but yet still appears to be valid since all of the links are valid. Without some method of either verifying the publisher or the whole blockchain, a simple substitution attack is possible. Replacing the previous link as a simple hash of the previous data with a digital signature would prevent the substitution attack; however, this would require the support of a public key infrastructure (PKI) with certificates, private key storage, certificate authorities, revocation lists, and the like. Alternatively, replacing the previous link with a hash chain achieves the same anti-substitution control without the PKI overhead.

Referring back to figure 3, we have provided another a chain field where each block contains a chain numbered by its block number: C0, C1…CN. Each chain is a link to all of the previous blocks, which is a hash of two elements: the previous chain and a hash of its own data. Thus, Block N contains a hash of CN-1 and a hash of its own data H(PN), that is H(CN-1, H(PN)). Likewise, Block 1 contains a hash of C0 and a hash of its own data H(P1), namely H(C0, H(P1)). Block 0 only contains a hash of a hash of its own data H(H(P0)) because there is no previous chain. In this manner an attacker cannot replace any of the published blocks without updating the whole chain, which is the basis of the Bitcoin blockchain security. The presumption is that it is cheaper to be honest than dishonest.

> If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added. [3]

Much of the media discussion around Bitcoin has focused on its role as a crypto currency. Bitcoin provides a means for achieving efficient, anonymous financial transactions. In this context, Bitcoin is sometimes described as a disruptive technology, one that facilitates the activities of drug dealers and terrorists, one that threatens to disintermediate and undermine the existing financial services industry, or one that presents banks who serve Bitcoin industry players with heightened "Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Act compliance risks" [1].

On the other hand, Bitcoin has seen adoption by e-commerce stalwarts such as PayPal, Overstock, Dish Network, and Dell Computers, as wells as "many community-driven organizations" that "allow anonymous donations using Bitcoin" [6]. Despite any negative aspects associated with Bitcoin, "there remain many legitimate uses for Bitcoin and businesses that facilitate these legitimate transactions" [7]. There is also growing interest in leveraging the blockchain technology that underpins Bitcoin to both reduce transaction costs and strengthen financial services security. To this end, more general purpose applications of the blockchain that are far removed from the use of Bitcoin to facilitate financial services transactions are being considered. For example, blockchains might be used to evaluate, monitor, assess, or even audit a cloud services provider:

- The CSP might publish its information security policy and practices in a blockchain providing a historical record of versions and changes. In this manner, new subscribers can evaluate the CSP, existing subscribers can monitor changes, internal audit can assess the CSP, and professionals can perform independent audits of the CSP.
- The CSP might distribute information security news in a blockchain providing notifications or alerts to its subscribers about incidents or events about new vulnerabilities in a reliable manner. Today, this information is typically provided via emails or blogs.
- The CSP might issue information security details in a blockchain providing real-time data about its controls. In this manner, existing subscribers can monitor the CSP for its dependability, consistency, and overall trustworthiness. Another name for this would be *compliance*.

Hence, the concept of using blockchains to record and verify CSP compliance data is not as farfetched as might have been initially considered. For cloud subscribers to gain such assurance, and to exercise due diligence in the conduct of their governance and risk management responsibilities, they need some insight into what goes on under the covers at their CSP. Cloud subscribers need the same types of operational evidence of compliance from their CSP that they would expect their internal IT departments to provide. Whether an organization's data is inside its firewall or floating around in the cloud, informed information security management practices still depend on access to the basics: vulnerability scan results, penetration test results, system logs, application logs, analytical results, security alerts, and summarized information. Compliance evidence must have origin authenticity, data integrity, and often confidentiality safeguards that prohibit access by attackers and other unauthorized individuals.

The attractiveness of the Bitcoin blockchain includes its decentralization. Bitcoin spenders submit their transactions (signature, inputs, outputs) to multiple Bitcoin nodes such that the transaction get published in the next block which is originated by the next miner to solve the hash solution. The idea is that the amount of work to perpetrate fraud far exceeds the work factor for mining. Sometimes a race condition creates a bifurcated blockchain generated by two different Bitcoin nodes; however, consensus processing will eventually prune the blockchain to only one authentic version. There is no central authority that provides a processing choke point, a single point of failure, or a single point of attack.

However, blockchain management is not without its problems. There are orphaned blocks, which are valid but did not make it into the main Bitcoin chain. There are always unconfirmed transactions waiting for the next block, which might get lost during the bifurcation and pruning process. There are double spends, transactions where the same Bitcoin fractions get spent by the same entity to two different receivers. There are strange transactions, where the syntax or semantics are invalid. And there are outright rejected transactions dropped by Bitcoin nodes that never get included in the chain. Some of these might be processing errors due to software bugs, Bitcoin versions, or rules issues. Alternatively, some transactions might be fraudulent in nature. Bitcoin fraud management is relatively nascent, and without a central authority there are no arbitration or adjudication programs available.

Bitcoin information is publicly accessible by definition. Hash algorithms provide the links between blocks and transactions, and digital signatures provide transaction integrity and authentication. Non-repudiation is not feasible as Bitcoin identifiers support anonymity, and the lack of arbitration does not meet legal needs discussed in the *Digital Signature Guidelines* [4] and the *PKI Assessment Guideline* [5]. Further, the Bitcoin blockchain does not offer data confidentiality. Some of the cloud server provider's information security management data is sensitive such that it might need to be encrypted, but only accessible by authorized clients or regulatory bodies. Thus, key management schemes need to be considered.

There is also growing interest in cloud data confidentiality and user anonymity. In a paper presented at the Security Standardization Research (SSR) 2015[8] conference held recently in Tokyo, Japan, researchers McCorry, Shahandashti, Clarke, and Hao proposed a new category of Authenticated Key Exchange (AKE) protocols. These new protocols, which "bootstrap trust entirely from the blockchain," are identified by the authors as "Bitcoin-based AKE" [6]. The SSR 2015 paper describes two new protocols, one with a guarantee of forward secrecy, and offers proof-of-concept prototypes with experimental results to demonstrate their practical feasibility. Both protocols provide greater anonymity than can be achieved using digital certificate or password-based AKE.

Following the guidance of international security standards can help ensure that the same information security policies used to manage risk when information systems resides in traditional non-cloud environments are also applied in the cloud. Recently, the big three international security standard-

[8] http://www.ssr2015.com/.

ization bodies published Recommendation ITU-T X.1631 | ISO/IEC 27017 *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.[9] This standard builds on selected parts of the familiar ISO/IEC 27002 *Code of practice for information security management*[10] but adds additional cloud-specific recommendations and guidance.

Although ITU-T X.1631 | ISO/IEC 27017 provides important recommendations and guidance, it contains no actual requirements. Conversely, the draft X9.125 standard hardens the ISO, IEC, and ITU-T recommendations and guidance into a set of specific information security management requirements. Where ITU-T X.1631 | ISO/IEC 27017 relies on clauses 5 through 18 of the ISO/IEC 27002 Code of Practice, X9.125 defines requirements based on comparable clauses in the ISO/IEC 27001 *Information security management systems – Requirements*.[11]

Conclusions

Blockchains, a decades old cryptographic technology, has become a creature of the Cloud. Its adoption and use carry many of the same security concerns as other cloud-based applications and services. But for blockchains to be trusted in the current financial services regulatory environment, and for it to be widely adopted, blockchain-based systems must comply with an organization's existing security policy and practices. Many of the policies needed to manage blockchains and other cloud-based deployments are the same as those used to manage security risk within an organization. Organizations must continue to manage risk and fully exercise their information security governance responsibilities regardless of where their data and applications roam. Cloud subscribers need the ability to verify that their cloud service providers are securing information in a compliant manner with established requirements.

ASC X9 is currently developing the X9.125 standard with the option of the United States submitting the work to ISO for international standardization. Once the cloud security requirements have been completed, the corresponding compliance data might be encapsulated in a publicly available or privately provided blockchain. Cloud subscribers, internal or external auditors, regulators, or any independent third-party assessor should be able to validate the CSP by verifying its information security blockchain.

This article is also a call for participation. Cloud service providers, cloud subscribers, or organizations that are interested in the development of the X9.125 standard are encouraged to contact the ASC X9 or the X9F4 work group chair. Participation by any X9 member is welcomed. Once the X9.125 standard is approved as a new ANSI standard, the possibility of it being submitted to ISO as a USA offering is something that will be seriously considered with the appropriate organizations' support.

References

1. King, Douglas. (2015). *Banking Bitcoin-Related Businesses: A Primer for Managing BSA/AML Risks*. Federal Reserve Bank of Atlanta. Retrieved November 19, 2015, from https://www.frbatlanta.org/-/media/Documents/rprf/rprf_pubs/2015/banking-Bitcoin-related-businesses.pdf.
2. Merkle, R. C. (1988). "A Digital Signature Based on a Conventional Encryption Function." *Advances in Cryptology — CRYPTO '87*. Lecture Notes in Computer Science 293. p. 369. doi:10.1007/3-540-48184-2_32 ISBN 978-3-540-18796-7. US Patent 4309569, *Method of Providing Digital Signatures*, Ralph C. Merkle, January 5, 1982.
3. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin.org, retrieved 31 October 2008, https://bitcoin.org/bitcoin.pdf.
4. ISC, *Digital Signature Guidelines, Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*, Information Security Committee (ISC), Electronic Commerce and Information Technology Division, Section of Science and Technology, American Bar Association (ABA), ISBN 1-57073-250-7, August 1996.
5. ISC, *PKI Assessment Guideline (PAG)*, Information Security Committee (ISC), Electronic Commerce Division, Section of Science & Technology Law, American Bar Association (ABA), ISBN 1-57073-943-9, June 2001.
6. Patrick McCorry, Siamak F. Shahandashti, Dylan Clarke, Affiliated with School of Computing Science, Newcastle UniversityFeng Hao, *Authenticated Key Exchange over Bitcoin*, Security Standardisation Research, Volume 9497, Lecture Notes in Computer Science, pp 3-20, December 9, 2015 – retrieved November 8, 2015, from http://eprint.iacr.org/2015/308.pdf.
7. Douglas King, *Retail Payments Risk Forum Working Paper*, Federal Reserve Bank of Atlanta, October 2015.

About the Authors

Phillip H. Griffin, CISM, has over 20 years experience in the development of commercial, national, and international security standards and cryptographic messaging protocols. Phil has a Master's of Information Technology, Information Assurance and Security degree, and he has been awarded nine US patents at the intersection of biometrics, radio frequency identification (RFID), and information security management. He may be reached at phil@phillipgriffin.com.

Jeff Stapleton has been an ISSA member and participated in X9 for over twenty years; he has contributed to the development of over three dozen X9 and ISO security standards, and has been the chair of the X9F4 work group for over 15 years. The X9F4 work group's program of work includes the five-year review of two published standards (X9.73, X9.84) and development of three new standards (X9.112, X9.122, X9.125) in addition to supporting ISO standard efforts. He may be reached at jjs78023@yahoo.com.

[9] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757.

[10] http://www.iso.org/iso/catalogue_detail?csnumber=54533.

[11] https://en.wikipedia.org/wiki/ISO/IEC_27001:2013.