guardtime

Cloud Insecurity and True Accountability

Primer for CIOs on Guardtime and Keyless Signature Infrastructure (KSI) for Attributed Networking

Matthew C. Johnson, CTO of Guardtime

At the end of 2013, the Cloud Security Alliance (CSA) published its annual report on “The Notorious Nine: Cloud Computing’s Top Threats in 2013” and the shift from ‘server to service-based thinking’.

The concerns of CIOs recalcitrant to embrace cloud migration and services are well-founded. Among the top threats outlined in the report include data breaches, data loss, account or service hijacking, insecure interfaces and APIs, denial of service, malicious insiders, abuse of cloud services, insufficient due diligence, and shared technology vulnerabilities. Quite a list.

> *“…the most significant security risks associated with cloud computing is the tendency to bypass information technology (IT) departments and information officers. Although shifting to cloud technologies exclusively is affordable and fast, doing so undermines important business-level security policies, processes, and best practices. In the absence of these standards, businesses are vulnerable to security breaches that can quickly erase any gains made by the switch to cloud’.*
>
> The Notorious Nine: Cloud Computing Top Threats in 2013
> - Cloud Security Alliance

Handing over competition sensitive, Personally Identifiable Information (PII), or related Intellectual Property information to a Cloud Provider is indeed an exercise in extreme trust without the ability to independently verify Cloud Provider coherence to purported security guarantees, controls, and associated contracts.

In 2014, in light of the CSA assessment and analysis of threats to Cloud Providers, as well as governments' perceived nefarious interactions with the telecommunications and data storage, social media, and search industries; it has become evident that blind trust in the service provider is a doomed strategy.

For the CIO, outsourcing business trust to the largely unregulated Cloud Provider industry today (regardless of your service provider contract) ultimately belies your belief in the constraints of administrator (and indeed government) interactions with your data, as well as the integrity of purported technical security controls, abeyance of best practices and associated policies and processes. The siren song has become 'we implemented NIST best practices!!' to assuage concerns. Our response has always been, 'so prove it in a way I can independently verify any time I want'.

Even recent US FedRAMP cloud accreditation criteria only serve as a 'point-in-time' assessment of the service provider, whose infrastructure and service exposure is constantly in flux.

Having witnessed these accreditation events for major federal acquisition efforts and the dynamic architecture of many Cloud Providers, these point-in-time assessments, while a good start, do not reflect the dynamically changing reality of a Cloud Provider's architecture – constantly changing software & configuration(s), API exposure(s) and input/output paths, as well as security baselines. Continuous monitoring of the Cloud Provider to accreditation baselines would help, but would likely impede the ability of the Cloud Provider to quickly offer new services at the desired demand of low-cost.

While CSA has pioneered a number of policy and best practice tenants to manage cloud computing risks and security threats. Their best practices framework, also known as "Security as a Service Implementation Guidance" for business, organizations, and governments is merely a risk management framework for cloud and does not address very fundamental integrity problems associated with cloud models.

CIO's should make the assumption that any outsourced infrastructure will at some point be compromised (if not

already). You can't outsource trust with the complexities offered today or with the people operating those resources on your behalf.

Also assume your own infrastructure is already compromised or soon will be in the (near) future. The more important and valuable your intangible assets are (your intellectual property, customer and supplier base, etc.), the more likely you are to be compromised.

We will next discuss how you mitigate threats even with this foundational assumption.

To get started, let's address some of the Top Threats, outlined by the CSA's Top Threat's Working Group (as surveyed by largely unnamed industry experts from the cloud industry) with a focus on truth, not trust and transparent accountability of the service provider industry.

Top Threat: Data Breach & Data Loss

While there are many attack vectors in a cloud (IaaS, PaaS, SaaS) model affecting potential data breaches, CSA outlines some of these attack classes including Virtual Machine (VM) side-channel attacks to exploit cryptographic keys belonging to multiple customers as well as implementation specific vulnerabilities affecting multi-tenant cloud service databases, where application flaws result in cascading compromises of multiple client's data. (For further info, please see: http://www.cs.unc.edu/~yingian/papers/crossvm.pdf and http://msdn.microsoft.com/en-us/library/Aa479086)

Risk management criteria to mitigate these threats include a number of CSA recommendations across data governance, information security, and security architecture best practices to minimize the threat of a data breach.

In addition to SLAs, a CIO should expect these risk management principles to be addressed in contracted activities with the outsourced Cloud Provider, who should provide guarantees for verification in the event of a compromise or mishap.

However, these best practices and layered security defense mechanisms are not enough. There will always be implementation specific attacks, holes identified in code that can be exploited, and vulnerable M2M interfaces (an attack surface increasingly being exploited and largely undetected due to abstracted automation and Software Defined Networking - SDN).

Top Threat: API Service Exposure & Insecure Interfaces

Cloud Service Providers expose APIs and software interfaces so customers can interact with those services. Amazon Web Services (AWS) is essentially a set of cloud APIs that let users host resources on remote servers and storage. AWS APIs include support for things like block storage, relational databases, email, and tools for solutions such as web hosting to content delivery. Even their IaaS platform is a set of AWS APIs that allow consumers to control the hosting of machine images on Amazon servers.

In contrast, Microsoft instead puts specific Operating Systems and middeware on the cloud to create their PaaS platform, while AWS offers basic IT services thru APIs without requiring those APIs to link to a particular Operating System. AWS's approach permits users to blend their own Apps with AWS features like storage, which benefit software developers who want to build their our SaaS Apps on the infrastructure at a greatly reduced cost.

AWS has received a lot of criticism for failing to endorse industry standards, having proprietary APIs, and being opaque in their management and reporting of their own cloud management activities, associated interfaces, and compromises.

So, 'trust us, everyone else does with their data and applications' has become the mantra.

Warranted criticism or not, this is contrasted by AWS's position that by adopting standards constrains AWS, making it harder for the company to evolve its service to meet the demands of innovation. Recently, AWS has opened a portion of their operations to meet FedRAMP accreditation compliance in order to win government contracts. Indeed the US Federal Accreditation community is

chagrin to tell you how they intend to provide persistent oversight of Cloud Providers to keep pace with updated and added service layers.

However, with the recent shift to an API economy for these platforms, the integrity of the APIs that are produced and consumed is now more important than ever. Security and availability of cloud resources is dependent upon the security of these basic APIs and their related 'access, authentication, encryption, and activities'. In short, these APIs must be designed to protect against, "accidental and malicious attempts to circumvent policy".

The Notorious Nine: Cloud Computing Top Threats in 2013
Cloud Security Alliance

Layered APIs offered by these service providers makes the problem that much worse to support the value added services that customers want. Risk is increased as credential management system complexities, cryptographic key management, and automation require handoff of credentials to third parties in order to enable their agency… again, 'trust us.. it works!'.

The truth is that with the velocity of these value-added service delivery components, their associated interfaces, credential management, and increased automation and M2M abstraction, security vulnerabilities are inevitable and credentials can (and have been compromised). The early days of SAML implementation for online shopping and CRM systems highlighted the threat to these services.

In 2013 alone, account details, files, credentials, and/or billing information belonging to over 100 million sharing, social networking and online shopping cloud service users were illegally accessed via data breaches and service layer exploitation.

Report: Cloud Security Analysis and Recommendations 2013.
FCC TAC Communications Infrastructure Security Working Group

Trust vs. Truth

Trust is defined as, “firm belief in the reliability or ability of someone or something”. Trust of a Cloud Service Provider is nonsense without the instrumentation and metrics to develop a formal sight picture into how reliable they really are and what they are doing with your data, services, and applications.

A Guardtime KSI-enabled infrastructure means undeniable independent proof = truth, not trust - of any Cloud Provider operation and interactions with your data. Guardtime offers undeniable truth (not trust), which can be verified independent of the Cloud Provider. With this truth, definitive accountability can be realized and recovered from the Cloud Provider, and identifies indemnification responsibility in the event of compromise.

With Guardtime KSI, a new cost-efficient integrity era is possible and can bring independently verifiable truth to network operations and the provenance of integrity events. For cloud and enterprise environments, Guardtime’s technology offers a new form of massive-scale Authentication, Advanced Persistent Threat (APT) detection, Data Loss Prevention (DLP), transparency, and independently verifiable proof of service provider activities and their provenance.

Service Owner	SaaS	PaaS	IaaS
Data	Joint	Tenant	Tenant
Application	Joint	Joint	Tenant
Compute	Provider	Joint	Tenant
Storage	Provider	Provider	Joint
Network	Provider	Provider	Joint
Physical	Provider	Provider	Provider

In general, the cloud provider can have sole or joint responsibility up and down the implementation stack – the above graphic highlights the common joint interface points. From a threat perspective, this means direct injection and attacks are possible into your enterprise IT environment at the nexus of these interfaces (if vulnerable), applications, credentialing systems or services.

So how as the CIO can you get to the truth as to the integrity of the responsible interfaces, applications, and service layers? Evidence of integrity and undisputable portability of integrity evidence is a must – and should be independently verifiable by anyone.

There must be transparency and accountability if indemnification is to be identified when a mishap or compromise occurs – who was responsible? The service provider, the enterprise, the application, the credential management systems, or external supplier? How can you possibly trust the service provider to say, 'it's not our fault, we are not liable', when there is no evidence to confirm or contradict the statement and what little evidence that might be presented is entirely shaped from the perspective of that service provider.

Using Guardtime in this way can bring accountability to the service provider by highlighting the complete chain-of-custody and digital provenance of service provider interactions, which in turn then identifies the responsibility and indemnification for compromises, tamper, malicious insider activities, or misconfiguration.

With KSI truth becomes widely witnessed evidence without disclosing the content of the underlying data (ensuring privacy), the evidence is portable and independently verifiable across infrastructures, and travels with the data.

A Guardtime-enabled organization means that customers, auditors, data-brokers, and investigators can independently answer the critical question: "What changed, what was eliminated, when did it occur, and what was responsible"

Guardtime provides this immutable proof and is the instrumentation necessary to verify Cloud Service Provider activities on your data as well as the integrity of the services the support (like PaaS-layer API integrity, etc).

Guardtime's Keyless Signature Infrastructure (KSI) and our solutions such as Guardtime's Security Operations Center suite of integrated products (see: GuardView SOC) change this perspective.

To quote Jason Hoffman, Ph.D. VP of Corporate Strategy and Portfolio Management at Ericsson, he said about Attributable Networks: “You can’t be perfect at preventing crime, but you can be perfect at detecting crime”. Guardtime is the foundational instrumentation required to provide this detection mechanism and provides the cloud client and operators visibility (and accountability) into their operations; bringing truth to network and data interactions. This is a paradigm shift in security – instrumentation afforded from the inside out at the data-level, with real-time integrity reporting for critical organizational applications and assets. This baseline instrumentation allows your organization to visualize threats and manipulation of those assets in real-time.

Guardtime digital signatures bring truth to what are loosely described as ‘trusted’ Cloud Provider operations, and their M2M, SDN, CDN, and the API service layer and related-audit environment(s).

Attributed Networking with Guardtime Keyless Signatures

Now imagine the possibility of an ‘Attributable Network’. Attribution means that the properties of important digital assets (trade secret, proprietary information, etc.) and network component software and/or firmware for assets like routers, switches, applications, virtual machines, configuration information, audit and event log systems, and associated network services can be tagged, tracked, located, and subsequently authenticated – that this unique authentication evidence is portable and can be independently verified by anyone.

With Guardtime’s infrastructure technology, the realization of this implementation is possible at the scale required, where digital assets and their provenance can be authenticated in real-time, anywhere in the world, independent of the service provider. For API and application integrity real-time monitoring from any baseline instantiation is possible. KSI signatures are portable, literally becoming part of the application, configuration files, credentials, and responsible access, authentication, and authorization assets.

The instant these components are tampered with is the instant you know there has been an integrity breach and that your customers and enterprise environment – your intellectual property – is at risk.

This proof affords the consumer, service provider, or data broker to finally trust the provenance and integrity of any network interactions, as well as the digital assets they are managing and/or consuming.

Fundamentally, the signatures generated by Guardtime KSI baseline the state of important digital assets – Guardtime calls this concept '**Clean State Proof'**, highlighting their authenticity, time, and identity. This proof information can then be sent and escrowed (aggregated) across the network enterprise or across service providers without disclosing the underlying contents of the data the signatures protect.

By collecting, analyzing, correlating and reporting this evidence one can build a real-time integrity picture of the network and/or important digital repositories and archives.

With this real-time awareness regarding the integrity state of important digital asset components, organizations seeking to protect the integrity of their network can make real-time decisions in the event that the network and/or asset is compromised and quickly identify the cause and specific component(s) responsible for the loss of integrity.

Subsequently, with this real-time awareness, real-time incident response, real-time data-loss prevention, investigation, and/or network resilience is now possible to detect and react to any misconfiguration, network and/or component/application failure.

Moreover, KSI directly supports enhanced continuity of operations, data loss prevention (due to theft or maliciousness), and is a new form of Advanced Persistent Threat (APT) detection for cloud when malware infects a crucial network or system component. The changed state of the asset provides a real-time alert, which can then be investigated, audited, and/or behavior stopped. If an asset is affected by malware, the signature information changes, the

asset can be ‘sandboxed’ or firewalled before further infection or transfer.

Guardtime’s believes that the CSA’s emphasis on data integrity represents the industry’s greatest security-related gap and chance to bring truth to cloud operations and client data and service interactions. While the CSA does outline best practice areas such as retention policies, risk assessments, use of encryption and user ID credentialing, differentiation amongst production/non-production environments and remote user multi-factor authentication.

Addressing integrity challenges at the scale required for cloud computing holds the greatest promise to actually address industry hesitance to move to cloud; providing a better solution to identify malicious insider behaviors and/or asymmetric threats that takes advantage of ever new implementation specific vulnerabilities not imagined by the software vendor or the Cloud Provider (such as zero-day exploits, insider threat challenges, subversion by governments, etc).

Moreover, your important organization’s digital assets: your competitive advantage (now being stored in the cloud) can be lost to a number of reasons other than malicious attacks. Your Cloud Service Provider’s interaction with your data and its migration to/from their cloud is largely opaque.

Cloud Service Providers have been hesitant and stonewalling integrity verification and transparency technologies. The reason? Compromise of your data or exploitation may or may not indemnify them for losses and has direct effects on insurance and reinsurance of both your and their assets.

If they (or you) can’t prove what was lost or compromised on their watch and how it occurred – if the evidence doesn’t exist, they can claim they are not liable. “Prove it”.

Target claims they are not responsible for the loss of over 100 million credit cards under their care. That’s quite an irresponsible statement and belies an industry willing to ignore consequences in the race to provide and implement low-cost competitive services.

Guardtime KSI brings truth, not trust to important digital assets and associated network interactions.

KSI Technology Primer

The information derived from a KSI signature means the asset's chain-of-custody information, creation time, and authenticity information remains undisputable and can be subsequently trusted and verified without trusting or solely relying upon an administrator or a secret (such as a key or PKI credential). Instead, KSI uses a 'proof-based' method to accomplish authentication and our forensic evidence is portable across any Cloud Service Provider or Enterprise network.

Forensically, KSI signatures are based on mathematical proofs and keyless cryptographic functions approved by the EU and the US National Institute of Standards (NIST). These proofs and functions will withstand exploitation even with advances in quantum computing meaning that assets signed by KSI will have proof information retained over the lifetime of the asset. The forensic evidence of the signatures makes legal indemnification issues easy to resolve; highlighting who, what, where, and when a digital asset was touched, modified, created, or transmitted. This evidence holds up in a court of law.

Literally any digital asset can be signed with Guardtime KSI and access (to the underlying data the signatures are protecting) is not necessary to determine if there is an integrity loss or compromise. An organization's Network Operations Center (NOC) or Security Operations Center (SOC) can simply adjudicate and trace any changes to signatures to determine the integrity state of their network or important archives via automated (or manual) reporting, analysis, and visualization (dashboards).

This concept and infrastructure does not rely on cryptographic secrets or credentials that can be compromised, nor does KSI rely on trusting administrators. The signature information afforded by Guardtime KSI can be used in fact to preserve and verify administration/user activities, behaviors, and interactions across the network.

Guardtime and KSI to Verify Cloud Service Provider Controls and Data Integrity

In addition to the best practices outlined by the CSA, a CIO should also expect integrity-based approaches to move the trust anchor reporting any potential compromise from the Cloud Provider or trusted insiders to a truth-based system like Guardtime KSI.

Today, the Cloud Provider cannot provide proof you can trust that your company's hosted data, applications, and services have integrity – that your critical data has not been manipulated without your knowledge or that it has been migrated to unauthorized locations (stolen) or altered. The cloud service industry attempts to address their integrity problems either thru 'hardened security appliances and modules' and associated cryptographic services.

However, this paradigm breaks down quickly when cryptographic keys and credentials are compromised and/or physical processes that rely trusting an administrator that your organization does not know, nor has a relationship with. Also, your own organization keys and credentials can be compromised agnostic of the Cloud Provider. Both of these methods can be exploited or subverted – 'secret' keys can be compromised and administrators can be incredibly subversive due to their 'trusted' access. Your insurers know this, which is why cyber liability policies are an expensive proposition.

With the resultant insider access these credentials afford, how would you ever know if your data was altered or stolen?

The question plaguing companies doing business with their cloud service providers is, "can I trust my data from being altered in your infrastructure?" Keyless Signature Infrastructure (KSI™) was designed as a proof-based system for authenticating data using only hash function cryptography, obviating the need for key management, security of key stores, and trusted system administrators.

Related material:

http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12913/FCC-TAC-Cloud-Sec-Group-Gaps-V14.pdf

http://www.darkreading.com/cloud-security/167901092/security/application-security/232900809/insecure-api-implementations-threaten-cloud.html

http://www.darkreading.com/authentication/167901072/security/news/232602844/web-services-single-sign-on-contain-big-flaws.html

About Guardtime

There are no competitive technologies like Guardtime KSI. Until Guardtime, there was no way to instrument the network at the scale required to track the state and authenticity of organizational assets at exabyte-scale and constrain their activities. Even at exabyte-scale Guardtime KSI signatures have minimal impact on network overhead for signing, escrow, and verifying operations.

Organizational ICT environments today may span multiple service or cloud providers. With the advent of cloud computing a new technology needed to be developed that worked at scale, with portable evidence, and needed to move the trust anchor from the administrator or cryptographic secret to an immutable proof (proof that does not change or can be tampered with). Guardtime KSI provides this proof with the context of time, integrity, and identity information for the assets being signed and monitored.

In contrast to Guardtime KSI, traditional digital signature technologies and credential-based signature technologies (such as PKI) DO NOT work well at scale, and ultimately rely on an underlying cryptographic secret, which when compromised results in a loss of trust in the security and event reporting systems. The complexities of key management and revocation make PKI systems inefficient with high overhead and enterprise administration costs.

Also, unlike KSI, if a PKI credential is compromised, you cannot trust any of the security evidence being reported by the system because the applications or logs may be subverted. If you can't trust the reporting mechanisms, then you cannot trust the state of the assets the security layer is protecting. Therefore, if these systems become compromised a network may be exploited for days, weeks, months, or years before the attack is understood or the data loss caught. In fact, an organization may never discover the compromise.

Guardtime brings transparency and accountability to digital society. Founded in 2007, Guardtime invented and is commercializing a Keyless Signature Infrastructure (KSI) technology that allows any type of electronic activity to be independently verified using only formal mathematical methods, without the need for trusted parties. Deployed by the enterprise and governments, KSI provides an independent audit trail for everything that happens in digital society, limiting liability and making it impossible for insiders or sophisticated cyber attackers to manipulate data and cover their tracks.

Read more at www.guardtime.com