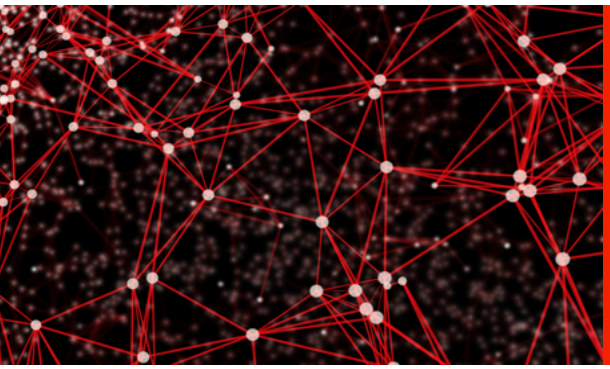
guardtime



Attributable Networks

Matthew Johnson, CTO of Guardtime

January 2014

Guardtime is an Information and Software Assurance company to offer the world's first massively scalable real-time authentication and integrity solution for any type of digital asset. With Guardtime's **Keyless Signature Infrastructure (KSI)** technology, the realization of 'truly attributable' networks is possible, where digital assets and their provenance can be authenticated in real-time, anywhere in the world, independent of the service provider. KSI signatures are portable, literally becoming part of the digital asset, and are used to provide proof of time, identity, and authenticity.

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.

Guardtime's KSI technology is used across a variety of United States and European Union e-government and federal agency platforms to authenticate and validate important digital and M2M assets **in real-time and regardless of scale**; verifying their authenticity, time, chain-of-custody and associated interactions. Guardtime KSI serves as a proactive Information and Software Assurance, Insider Threat, and Advanced Persistent Threat detection capability.

Guardtime's definition 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.

1 Definition: 'attribution' means that the digital assets and network components can be tagged, tracked, located, and subsequently authenticated, in real-time, at scale.

2 Guardtime's KSI technology serves as a proactive Information- and Software Assurance, Insider Threat, and Advanced Persistent Threat detection capability.

3 KSI technology is in use today across a variety of United States and European Union eGovernment and federal agency platforms.

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.

4 KSI signatures are based on mathematical proofs and keyless cryptographic functions approved by the EU and the US National Institute of Standards (NIST).

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).

5 KSI does not rely on cryptographic secrets or credentials that can be compromised, nor does KSI rely on trusting administrators.

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.

6 The forensic evidence of the KSI signatures makes legal indemnification issues easy to resolve, highlighting who, what, where, and when a digital asset was touched, modified, created, or transmitted.

7 The information afforded by KSI holds up in a court of law.

Why is Attribution important?

Fundamentally, the signatures generated by Guardtime KSI baseline the state of your 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 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.

8 Organizations can build a real-time integrity picture of the network and/or important digital repositories and archives.

9 KSI instrumented attributable networks enables discovery and real-time decisions in the event that the network and/or asset is compromised.

Contrasting Guardtime KSI

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 status of the hundreds of thousands, millions, or even billions of organizational assets contained across a large enterprise environment and constrain their activities. Guardtime KSI signatures can work at Exabyte scale and have minimal impact to network overhead for signing, escrow, and verifying operations.

Organizational ICT environments today may span multiple service or cloud providers. For example: 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.

10 Guardtime KSI technology can work at exabyte scale while having minimal impact to network overhead for signing, escrow, and verifying operations – there are no competitive technologies with similar capabilities.

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.

11 Traditional PKI relies on an underlying cryptographic secret, which when compromised results in a complete collapse of trust in the entire security and event reporting system.

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.

12 Additionally, PKI does NOT work well at scale; the complexities of key management and revocation make PKI systems inefficient with high overhead and administration costs.

The Target case

Recently a major corporation's customer credit card and billing information was stolen resulting in the loss of over 100MM credit card numbers via the exploitation of multiple network components across Target's enterprise. More info: http://bit.ly/1eLWpKa

Implications of the Target case

With Guardtime KSI, the Target compromise would have never occurred; as the compromised integrity of the credit card database configuration(s), machine reader software, and security layer components would have been detected in real-time and subsequently responded to. As of writing (February 2014) Target still cannot answer the United States Congress if they have eliminated the malware inside the enterprise and if backdoors still remain into their customer records system(s). They are not instrumented from the inside out to begin to understand their networks integrity, what has changed, and what was responsible.

The implications for any organization creating an attributable network means that they can prevent data loss of important digital assets, assure the integrity of their network, and verify enterprise behaviors even across service providers without having to put their trust in cryptographic secrets or administrators that may also be compromised (also known as the 'insider threat').

Strategically, a new era in trusted networking and digital asset and content protection is possible with Guardtime KSI. Every component, configuration, and digital asset can be tagged, tracked, and located with real-time integrity information no matter where that asset is transmitted, stored, or received.

13 With Guardtime KSI, Target compromise would have never happened.

14 For any organization creating an attributable network, it means that they can prevent data loss of important digital assets, assure the integrity of their network, and verify enterprise behaviors even across the service providers without having to put their trust in cryptographic secrets or systems administrators

15 Strategically, a new era in trusted networking and digital asset and content protection is possible with Guardtime KSI.

Contact: matthew.johnson@guardtime.com