guardtime

Internet of Things (IoT) Security

Turning Defense into Offence

guardtime.com

Internet of Things (IoT) economic impact is estimated at $6.2 trillion annually by 2025.

Mckinsey Global Institute study, May 2013

Welcome to the Future

Imagine the future, you are in 2020, the alarm clock coordinates with your wearable sleep sensor to gently wake you up.

Simultaneously, your car reviews the calendar, determining you need to be at the airport in three hours, and starts monitoring traffic patterns. The coffee maker starts to grind and brew the perfect cup of coffee. The car sends you a text: 'best routes to San Francisco airport and what time to leave'. Coffee is ready, cooled to temperature and ready for drinking as the car takes you to the airport. You have time to catch up on emails and voicemails as the car navigates to the departure gate. Home security, lighting, plant watering and HVAC systems adjust to the calendar, knowing you will be out for three days. You get out of the car at the departure gate; the car drives off to self-park in the long-term parking lot.

But wait! You land, an urgent text arrives, and your car is not in the parking lot, your home has been broken into, your personal electronic records compromised. Your worst nightmare, thousands of miles away and you are a victim of a new wave of crime sweeping the country: "Sensor Network Attacks". Monitoring and security agencies are fighting to contain the outbreak, déjà vu the early days of the Internet!

At Guardtime, we understand IoT security requires a different mindset, one where security is tied to your data, protecting data through keyless signatures wherever the data moves, changes or is accessed, creating digital footprints to monitor and report any malicious or suspicious activities. Irrespective of where the data resides, in the cloud, your car, home or on your smart phone.

IoT primer

1

Defined by Gartner as:

"Network of physical objects that contain embedded technology to communicate and sense or interact with their internal state or the external environment."

2

Proliferation of low cost wearable devices, in home sensors, driver less cars, smart phones, and cloud-based applications are all enabling IoT to become a reality.

3

IoT security architecture and products are evolving. IoT solutions cut across raditional technology boundaries of Information Technology (IT), Operational Technology (OT) and Telecom cellular networks (TN). Focus on data protection and privacy becomes paramount.

The Industrial Internet will have a $270 billion impact to GE businesses.

Jeff Immelt,
GE CEO

The Challenges of IoT Security

The social, economic and political impacts of IoT are just starting to be understood and debated. The effects on quality of life, health, environment, productivity, agriculture will unleash the next wave of innovation as we transition from the consumer internet to the industrial internet. Projections by McKinsey model 10-20% cost reductions in chronic disease management, up to 5% improve-ments in manufacturing operating costs, 10%- 20% improvements in travel time and congestion control and 20% increase in yields from precision application of fertilizer and irrigation by famers.

Ecosystem of supporting innovation facilitates the adoption of IoT technologies, with low cost low power embedded sensors, LTE / 4G IP cellular networks, smart phones, cloud infra and IPV 6.0.

In contrast, security technologies, procedures and policies leverage the investments made in Information Technology, Operational Technology and Telecommunication – Cellular networks creating a fortress mentality to protect and defend assets via:

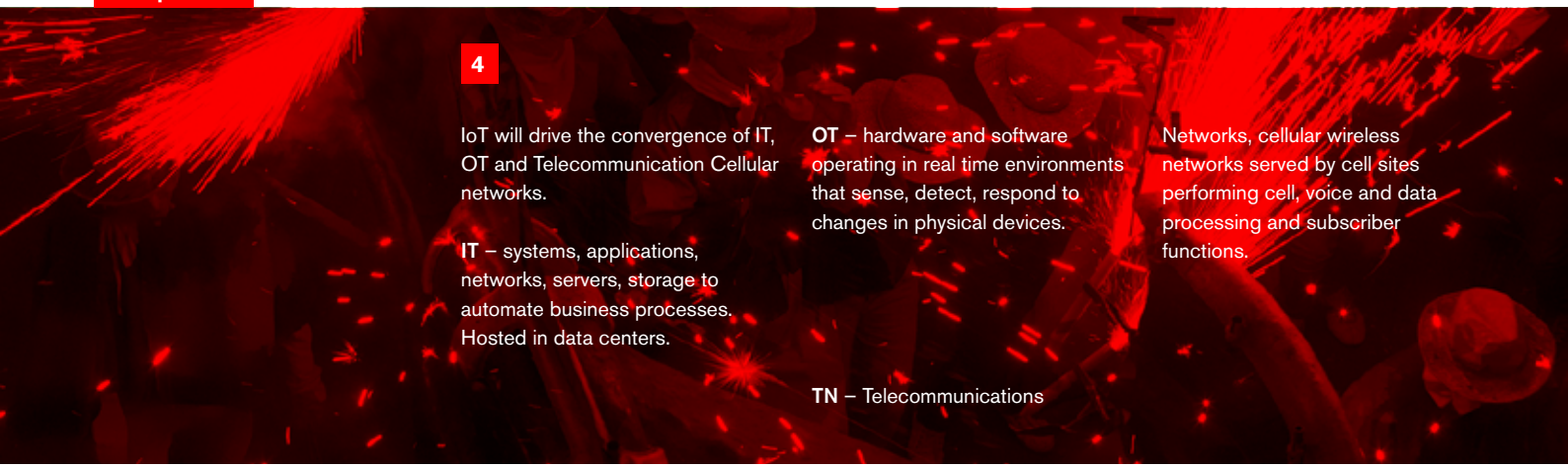
- Physical appliances:
  firewalls and network access control
- Virtual and private networks with monitoring
- Digital certificates, anti virus and malware scanning
- Patch management of critical security defects
- Intrusion detection and prevention systems
- Vulnerability and penetration testing tools
- Data encryption and data segregation

Although these are all valid and good practices to adopt, many of these practices are IT focused and are limited in how they can be deployed into real time plant networks or directly managing physical objects.

These environments have four major constraints:

- Real time, 24x7x365 infrastructures cannot be brought down for security updates and patching.
- Low latency, proprietary protocols limit the ability to deploy anti virus and malware software.
- Embedded processors, running RTOS (real time operating systems) have limited processor and memory capacity to execute security software.
- Traditional anti-virus and malware detection does not work for the proprietary protocols, applications and real-time embedded operating systems traditionally used in IOT.

IoT primer



The Internet of Everything will have a $14.7 trillion economic impact.

John T Chambers, Cisco CEO

Securing IoT the Right Way

Architecting an IoT security strategy requires an understanding of the core principles by which of IoT applications and solutions will be built and deployed.

Guardtime experience in securing massive scale and reliable digital assets for security and government agencies, provides the experience and foundation to define the following key IoT security principles:

Event Driven – sense, detect and react to events intelligently. An event is a change in state of the physical object.

Traceable – record and play back events over time horizons to aid in discovery and root cause analysis.

Assurance – verify the reliability and integrity of the data, preserving time and authenticity.

Identity – authentication and authorization of physical devices with IoT applications.

To address the number and complexity of potential vulnerabilities within an IoT solution requires an alternative approach to how security has historically been designed and managed. Security within IT, OT and Telecommunications Cellular networks is secondary to the functionality and services being delivered to the customer.

Security is a back office, technically focused organization that is called upon usually after product design or as a result of a major attack. Guardtime is leading the thinking, envisioning a future of IoT solutions, where Security is at the forefront and an integral component of business strategy.

At Guardtime, we believe security should and must be seen as a competitive advantage to organizations looking to capitalize on IoT opportunities.

IoT primer

5

Technology trends in Cloud, Big Data and Mobility will fuel the innovation and growth of IoT applications and solutions.

Cloud technology enables a more cost effective and scalable means to deliver compute infrastructure and software applications on a pay as you go basis.

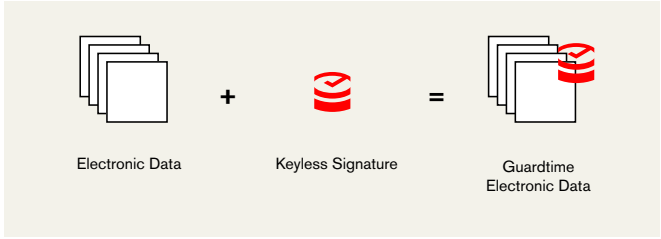
Big Data technologies allow for massive amounts of structured (relational) and unstructured data (media) to be analyzed on low cost commodity hardware (Cloud based) to model and predict future scenarios and trade-offs.

Mobile technologies such as smart phones and tablets provide substantial processing capabilities and high bandwidth connectivity to LTE / 4G networks to empower remote workers and control physical devices remotely.

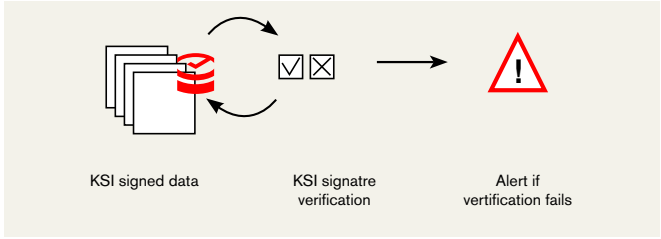
Google's $3.2 billion acquisition of Nest allows Google to tie home devices with Google software.

Guardtime's KSI for IoT

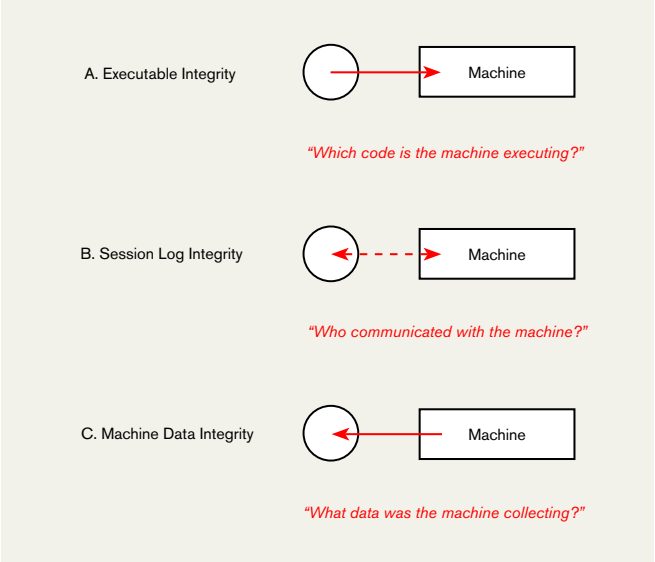
Guardtime's technology assigns a unique "keyless" signature to any type of data. The signature, is stored with the data, as an attribute which can be used to verify the time of creation, identity of creator and integrity of the data, independently from keys, secrets and certificates.



Real time verification of the data signature occurs and notifications sent should data integrity be compromised and / or unauthorized access occur.



The outcome of deploying a Keyless Signature Infrastructure (KSI) within IoT solutions is the ability to seamlessly integrate into IT, OT and Telecommunication Networks, securing IoT data, ensuring integrity and accountability. KSI's technology addresses the three constraints identified with real time plant networks, by providing firmware code, session and data integrity between the physical device and external IoT systems.



IoT primer

6

IoT infrastructures will depend on the design, configuration and security of Wireless Sensor Networks (WSN).

- A Wireless Sensor Network can consist of the following components:
- RFID tags and readers
- Sensors configured to detect temperature, humidity, moisture, weight, traffic flow etc.
- WIFI 802.15.4 / ZigBee / Bluetooth / 802.11ah
- Access points
- Encryption
- Gateways
- Data Collection Engines

The Internet of Things will take more than 10 years to become mainstream, mainly due to security challenges, privacy and standards.

Gartner 2012
IoT paper

Conclusion

To mitigate Sensor Network Attacks now and in the future, Guardtime's technologies protect IoT infrastructures by providing a 360-degree view of the data at anytime, anywhere and on any device, static or in motion. Legacy operating systems and applications mean persistent vulnerabilities in control system architectures that cannot be mitigated until a technology refresh.

Due to the long cycle times to tech refresh these systems (think windows XP used extensively), the only way to do advanced persistent threat detection post support expiring is KSI and continuous monitoring. Indeed, KSI extends the life and deployment of these legacy systems with real-time monitoring and resilience attributes in the event of an implementation specific vulnerabilities.

Selecting Guardtime's KSI technology will allow organizations and governments planning IoT projects to gain the following advantages:

- **Trusted partner** to security and government agencies worldwide.
- **Attribution**: prevent data loss of important digital assets, assure the integrity of the networks and verify behaviors across service providers.
- **Exabyte-scale Integrity**: independent verification for the absence of compromise in systems, networks, devices and data.
- **Auditability**: Indemnification for organizations as there is independent mathematical audit trail for what happened when across all networks and devices.
- **Monitoring**: Real time monitoring to prevent data loss, monitoring changes to state, access, custody and identity.
- **Integration and interoperability**: leverage existing investments in Security and Network infrastructure.
- **Service lifetime extension**: extends the life and deployment of these legacy systems with real-time monitoring and resilience attributes.

guardtime