CLOUD SECURITY ARCHITECTURE

FROM PROCESS TO DEPLOYMENT
The Trust Engine concept and logical cloud security architecture presented in this paper provide cloud vendors, service providers and tenants with a framework to clearly and efficiently discuss security threats, risks, controls, compliance and other security requirements within the cloud context.
INTRODUCTION

The Networked Society will be built on unprecedented connectivity and the ability to access cloud services from anywhere in the world. At the same time, security for cloud computing has become one of the top concerns for cloud actors such as cloud service providers, tenants and tenants’ customers, as well as for governments and regulators. Many of society’s critical functions are already being moved into clouds, and this trend is likely to accelerate. For attackers such as spies, hacktivists and organized criminals, this provides attractive opportunities to compromise society’s critical processes.

The ability to withstand, detect, respond to and recover from attacks by malicious parties, or from unintentional security breaches, is seen as a cornerstone for trustworthiness by cloud actors. Trustworthiness is built on transparently ensuring security and privacy for tenants in an evolving environment. Security and privacy will therefore gradually become a business driver, more than a business enabler, on a global scale.

For a cloud service provider, security cannot be a permanent state reached through a one-time effort. Instead, it is a continuous process supported by cloud architecture. Technical mechanisms and operational policy management (and enforcement) should all be treated in a unified manner. Each provider needs security governance to constantly follow risk landscape changes, make adjustments for security controls and enforce efficient security processes. The Trust Engine concept presented in this paper addresses these aspects.

Executing security as a process using the Trust Engine concept enables transparency and proof of compliance with best practices, specifications, standards and regulations. In this way, cloud service providers can offer better security for many customers than the customers are able to provide in their own IT networks. To move the security discussion between the different cloud actors forward, we will illustrate a combination of the Trust Engine and logical cloud security architecture.
SECURITY CHALLENGES

Mass adoption of cloud, increased network programmability and an estimated 50 billion connected devices will generate new threats and attack scenarios such as advanced persistent threats, distributed denial-of-service attacks and data breaches. These emerging threats are causing a shift in the security community mindset from prevention to resilience, as well as a gradual movement from perimeter protection to data protection. Several organizations, for example, the European Network and Information Security Agency [1] and the Cloud Security Alliance [2], have studied the security challenges of cloud computing and have found them to culminate in the following three basic challenges:

- **Multi-tenancy** – resources are shared between tenants according to Service Level Agreements (SLAs). Each provider is responsible for a proper isolation of its tenants’ computing, networking and storage resources.
- **Divided responsibility** – besides the provider, tenants also have the responsibility to protect their assets. Dividing responsibility between the provider and the tenant depends on the SLA, and needs to be agreed between the actors before the service is taken in use.
- **Dynamic environment** – the cloud environment is constantly evolving, and resources may dynamically scale up and down or even change their locations. Security policies have to capture and govern these dynamic changes.

To counteract these challenges, it is important for the tenant to be able to verify that services are available and that they are protected according to a desired or agreed-upon policy and SLAs. The challenges also imply the importance of data protection. Data needs to be available, its integrity protected and the confidentiality of sensitive data assured. For example, multi-tenancy must not disclose data to unauthorized tenants, nor cause deviation from the desired level of data availability. Confidentiality and integrity of data cannot be lost due to divided responsibility between actors. The integrity of security policies should not be broken because of dynamic changes in the service deployment.
The previously mentioned security challenges generate an obvious need for advanced risk and threat management. In the current business environment, each cloud service provider needs relevant and efficient measures for turning cybersecurity from an uncontrollable extra cost into an efficiently managed competitive advantage. To run a trusted cloud business, an organization utilizing cloud-based services requires trusted operations, trusted networks and trusted products enabling trusted services.

The Trust Engine discussed in this chapter, together with logical cloud security architecture, provides a structured approach for this purpose. In the following sections, we dissect the Trust Engine (as illustrated in Figure 1) with respect to both the technical and operational aspects of running business in a safe telecommunications and IT cloud.

Risk insight
Setting up security governance and a security policy framework for an organization is the responsibility of top management. In particular, it is a business decision to assess risks, accept residual risks, manage unacceptable risks and set the ambition level for security. This requires the establishment of a risk management process. Risk insight and security risk evaluation from a business perspective are the fundamental cornerstones in order to efficiently define, implement, and manage security in both cloud and telecommunication networks independent of deployment models.

Cloud providers and tenants need to acquire risk insight for their cloud business in order to take the necessary actions to mitigate threats and risks. This means that risks on all levels have to be considered – for example, at operational, deployment-wide and individual node and server levels. Assessments must be executed using the same methods and procedures in order to produce comparable and reproducible results. The identification of new risks as well as changes in earlier findings should be fed back into the overall risk management process for further risk mitigation decisions.

Build and deploy
The applicable set of controls on the operational, network and node levels are selected through the risk management process. These controls need to be designed and implemented to ensure the specific security objectives of the organization are met. Risk insight and respective risk mitigation decisions guide the provider and tenants to select, build and deploy optimal security controls. The security management and orchestration layer in the cloud security architecture is responsible for deploying the required technical security controls. Optimal build and deployment of security controls can be reached by balancing costs, usability and effectiveness.

Operate and control
During operations, the effectiveness of implemented controls needs to be continuously monitored, maintained and improved. Constant monitoring of the risk landscape is required to ensure controls continuously evolve with business needs. Efficient management makes the system more resilient against the threat landscape. Regular recurrent security assessments and audits need to be executed to ensure security is implemented and operated in accordance with the security policy.
Predict and learn
Predict and learn is based on security analytics that provide real-time preemptive information about new potential cloud security risks. It enables corrective actions in case of deviations from the desired security ambition level. In a cloud environment, a high degree of automation is necessary to ensure quick response to any identified threats and anomalies. Security analytics help efficiently update risk insight in the cloud context. It is foreseeable that current Security Information and Event Management and big data-based security analytics will converge into unified security analytics solutions.

Comply
Cloud service providers and tenants have their respective areas of control, ownership and responsibility for assets in the cloud. Tenant assets are usually virtualized, whereas providers often have responsibility for physical assets as well. The division of responsibility for security controls and assets depends on the SLA. Each party must be able to verify that the cloud deployment complies with their requirements. Proof of compliance regarding best practices, specifications, standards and regulations helps cloud providers to demonstrate regulatory and SLA fulfillment. An up-to-date, transparent compliance view is made available by an active process involving the Trust Engine components. Cloud service providers and tenants implement and enforce their respective security controls for protecting assets.

Trust
The Trust Engine provides a solid foundation and the steps for running efficient risk and security management for cloud. The Trust Engine can be seen as a process that is executed on the logical cloud security architecture that manages the dynamic nature of the cloud (see Figure 2). In practice, cloud security architecture addresses the build and deploy, operate and control, and predict and learn parts of the Trust Engine, while the other parts of the Trust Engine are more governance-oriented.
SECURITY MANAGEMENT AND ORCHESTRATION

The security management and orchestration layer dynamically deploys and adjusts security functions, policies and related configurations of tenants and providers, for example, in IT cloud and telecommunications cloud deployments. The layer is seamlessly integrated into common network management and analytics infrastructure with a security operations center (SOC) view providing situational awareness. Based on constantly updated risk insight, the SOC can ensure optimal security controls are implemented in the dynamic cloud environment at all times. The SOC is the execution point for security management and orchestration, and supports automated and manual management of security incidents and events. This, for example, shortens propagation delays in correcting zero-day vulnerabilities in the live environment.

The security controls and services are divided into 6+1 groups in the logical cloud security architecture (see Figure 3). They should be seamlessly coupled with security management and orchestration to achieve end-to-end security responses. Security management ensures consistent security across the system. It translates business and operational security policies of providers and customers into actionable security policies. Logically centralized security policies are enforced by highly distributed and programmable security functions through application programming interface exposure. Security orchestration executes the actions based on security policies. It provides deployment and configuration of all network and product security controls, including virtualized and physical network functions.

An identity and access management (IdAM) security control group contains adaptation of multifactor authentication, identity federation, granular authorization frameworks and reputation management. IdAM ensures only authorized actors are allowed to access data in a usable manner (single sign-on). The group needs to be seamlessly coupled with certificate and key management that handles the life cycle management of cryptographic keys and digital certificates. Cloud providers and customers need cryptographic keys for multiple different purposes, including secure communication, to provide identity assurance of the originating entity and for encryption of data.

Data protection requires support from the other security function groups in the different phases of data life cycle management. Data protection takes care of secure data life cycle management in the multi-tenant environment. It covers confidentiality, integrity and the availability of data at rest, data in transfer and data in use.

Security monitoring and analytics functions play an important role in data protection. Security-related events are collected from networks and nodes and correlated against indicators of compromise together with the system data. These functions provide both live security status (reactive response) and information on past security events, making it possible to respond to threats even before a new incident occurs (predictive response). On the other hand, when incidents occur, data provided by the security analytics shortens the time consumed in investigations and forensics.

Data in transit requires traffic separation, protection, filtering and integrity protection that belong to the network and infrastructure protection controls. Infrastructure integrity protection and secure isolation are built on hardware-rooted trust and secure bootstrapping procedures.

While falling outside the scope of this paper, it is also important to be aware that there are other security functions needed. These fall into the “+1” control group.
THE IMPORTANCE OF DATA INTEGRITY – A USE CASE

Given the three main security challenges for cloud – multi-tenancy, divided responsibility and dynamic environment – one specific customer concern is data protection (access control, encryption, integrity and origin verification). In cloud environments, the amount of data at rest, in transfer and in use is considerably larger than in traditional networks. Let us consider the need of a user to ensure the integrity of this data at all times.

Data integrity in a cloud context is extremely important in building enough trust for a user to put data in the hands of a cloud provider. Unfortunately, data integrity often does not receive as much attention as data encryption. Integrity can assure the consistency of important data, whether it is system data or application data.

Most security-conscious users want assurance of any – or all – of the following:

- Time – when the data was generated or protected.
- Integrity – assurance that data has not been changed from its original form.
- Origin verification – for example, the identity of the data producer, which can be especially relevant during forensics investigations, in facilitating forensics auditability, or for legal and contractual purposes.

These properties can be achieved using, for example, symmetric cryptography, public key infrastructure (PKI) or Keyless Signing Infrastructure (KSI) [3]. These techniques can be used separately or can complement each other, and the selection of technology should be based on the use case and user requirements. PKI-based signing technology utilizes public-private key pairs, while KSI technology utilizes data hashes and hash trees for generating and publishing a root hash for the data to be integrity protected. Integrity verification is done using signature tokens that enable verification of data relative to the previously published root. Which technology to select for data integrity protection can be based, for instance, on the following aspects:

- The timescale of the need for integrity protection (short term versus long term).
- The type of time information needed.
- The number of data items that need to be protected.
- The level to which the origin needs to be verifiable.
- Other organizational policies that, for example, mandate the use of specific cryptography.

Symmetric cryptography and KSI have benefits in cloud (big data) contexts in terms of efficiency. In KSI, integrity does not rely on a single key that could be breached: no key is needed to verify if data matches the root hash. Security management is also facilitated in KSI since there is no need for revocation.

By combining data integrity and data encryption technologies with other security orchestration and management tools, unique use cases could be demonstrated including near real-time data integrity monitoring. Telecommunications cloud providers would be able to transparently demonstrate that cloud tenants own and control their data at all times.
CONCLUSION

The Networked Society is built on interconnections between devices, people, information and services. Cloud environments are used both for casual resource optimization – for example, to try out a new service concept at low cost – and for critical services and information, such as banking or individual health records. Different use cases and service models will result in differences in security requirements: there is no one size that would fit all.

Cloud vendors, service providers and tenants must establish a shared view on cloud security in order to establish and drive trusted business. This shared view will enable cloud service providers to understand and fulfill the security needs of their customers. In various sectors, such as health care, automotive, manufacturing, public utilities or banking, these needs are also subject to applicable regulations.

Through the Trust Engine, this paper provides a conceptual basis to support different actors in their discussions about cloud security risks, threats, controls, management and compliance, as well as other security requirements in a cloud system. In addition, different design factors, best security design practices and the application of the right security technologies will need to be taken into account.

A good cloud service provider is able to combine a solid conceptual foundation and a common understanding of customer needs with technical know-how in design and implementation. This will allow it to provide, in a cost-efficient way, more trustworthy operations, networks and components than many customers could achieve independently, and to fully realize the benefits of sharing resources through a cloud model.
GLOSSARY

IdAM  identity and access management
KSI  Keyless Signing Infrastructure
SOC  security operations center
PKI  public key infrastructure
SLA  Service Level Agreement
REFERENCES

