GlobalLogic®

An Introduction to Information Security

Juan Manuel Caracoche
CTO, Latin America

Tzvi Kasten
AVP, Business Development

As trends such as machine-to-machine connectivity, smart devices, social networks, and migrating to the cloud progress, there is a growing concern around the compromise of privacy and data security.

This white paper will provide a high-level description of the current security environment, including the various aspects of this domain and how they interact. Future white papers in this series will take a deeper look at the various challenges and solutions of Information Security.

www.globallogic.com

Table of Contents

Juan Manuel Caracoche, CTO, Latin America
Tzvi Kasten, AVP, Business Development

Executive Summary

As trends such as machine-to-machine connectivity, smart devices, social networks, and migrating to the cloud progress, there is a growing concern around the compromise of privacy and data security. Even government and commercial organizations are threatened by sophisticated intrusion tactics. There is now a growing need to gather and analyze data on potential security risks through advanced measures.

Not only will the demand for security-related products in the market rise, but commercial and enterprise products will themselves need to be designed with security as an important consideration. As a product R&D services provider, GlobalLogic is intimate with these requirements and has established the required leadership, processes, and technologies to help our customers address these issues.

We have written this white paper in order to provide a high-level description of the current security environment, including the various aspects of this domain and how they interact. This white paper is the first publication in a series that will take a deeper look at the various challenges and solutions of Information Security.

Why You Should Be Aware of Security

Our online connectivity has increased exponentially in the past five years, from social networking to cloud computing to e-banking. Many of us share our personal information online without taking into account how that information is managed or what policies govern the use of our information. Often, people only learn the significance of Information Security after they become the victims of identity theft or other crimes. Regardless of one's level of technical expertise, it is crucial that all online and device users at least be aware of the security levels of their applications or services.

On the other end of the spectrum, solution providers need to consider how their products and/or services will handle secure information. A product's development lifecycle should include basic security considerations, such as privacy, authenticity, integrity, and non-repudiation. In fact, many solution providers do already address these security issues due to certain industry standards and regulations that their services and applications are required to meet. However, there are still large gaps in "security consciousness" that need to be realized during product conception and development.

Demystifying Security

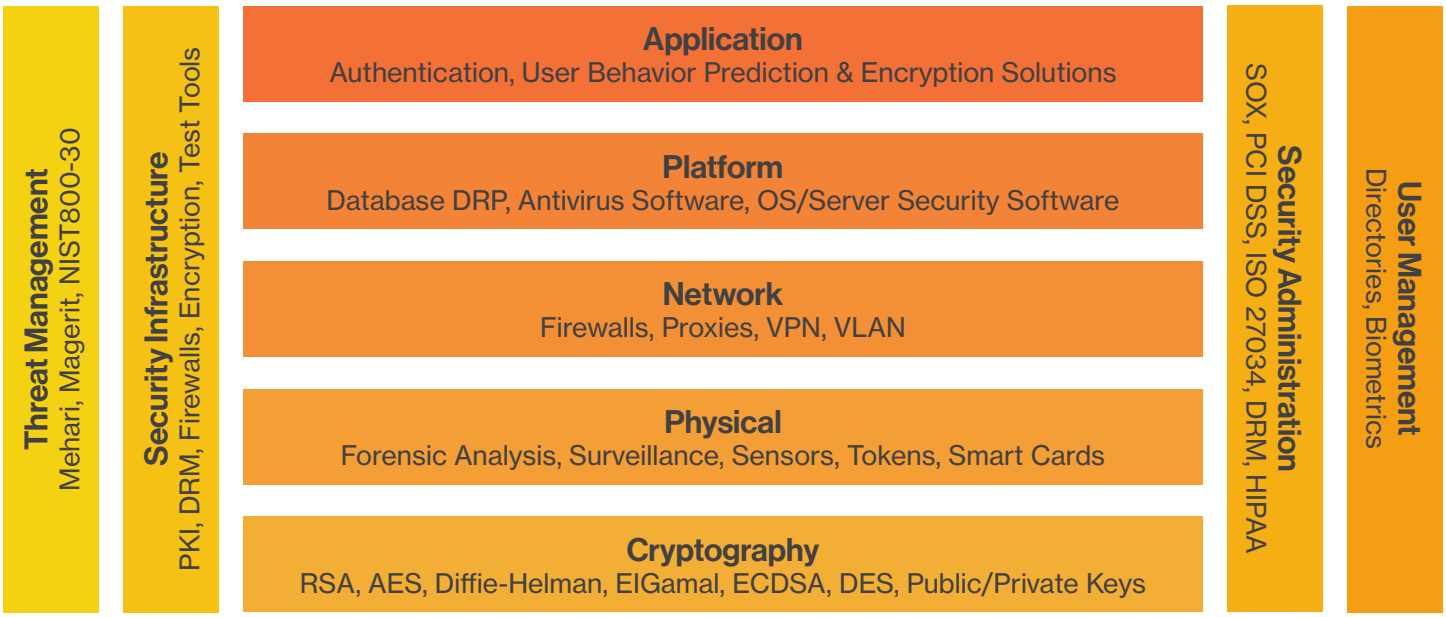
Information Security is often perceived as an obscure science filled with complex math and elaborate algorithms. In reality, anyone who uses the internet or performs a Google search is making use of Information Security. However, it is true that Information Security utilizes many technologies. It can cause quite a headache to understand each one and how they all fit together.

To help you navigate the security space, we have created a simple map with stacks of vertical (i.e., objective) and horizontal (i.e., technology) layers. In this section, we will provide you with an overview of the relationships between these two stacks. We will then go into further detail about each specific layer in the next section.

A Map to Security

In the IT world, a layered Open Systems Interconnection (OSI) conceptual model is a generally well-known and helpful way to understand networks. Leveraging this model, we have created a map that divides Information Security into two stacks: (1) vertical layers that focus on specific security objectives and (2) horizontal layers that focus on the technologies that help achieve these objectives.

Figure 1: Information Security Conceptual Model



Vertical Stack: Security Objectives

The main objective of security is to manage threats, which can be addressed through strong security infrastructures. You may notice that both the "threat management" and "security infrastructure" layers deal with protecting against security attacks. However, the threat management layer focuses more on the "what" (i.e., security objective) while the security infrastructure layer focuses more on the "how" (i.e., underlying layers and protocols). We wanted to make this distinction in order to prevent a very complex topic from being condensed into a single layer.

The other major security objective is user management, since it's useless to talk about protecting a user's information without first protecting his or her identity. Specifically, you must be able to accurately verify a user's identity while also authorizing his or her access to data. We will talk more on this topic in the next section.

To make all these different components work together, you need to implement a strong security administration that allows you to monitor and control the required security levels. The security administration layer also encomposses specific domain security standards and governance regulations.

Horizontal Stack: Security Technologies

The underlying technology of Information Security is the science of cryptography, which allows you to share information with some parties while hiding it from others. On top of this abstract methodology, security is managed on various levels: physical, network, platform, and application. The physical layer manages the tangible aspects of security, while the network layer protects data in transit and prevents attacks through the data network. The platform layer deals with special challenges related to specific product platforms, and the application layer manages risks associated with the application itself.

Now let's look at the relationship between all these different horizontal layers. Users engage with applications that interact with information. Applications run on a platform, and depending on the platform, they can be client or server applications. (Note: there are also standalone applications, but these are not considered to be much at risk.) Then each application interacts with various devices (e.g., servers, databases, external services, etc.) through a communication channel that is composed of a network layer and a physical layer.

All these layers are exposed to threats, from hacking into a network to cutting a physical cable. This is why it is critical to consider the security of every component, as we will discuss next.

The Components of Security

In the previous section, we broke down the large topic of Information Security into more digestible layers based on how organizations and users interact. In this section, we will describe each vertical and horizontal layer in greater detail.

Vertical Stack: Security Objectives

Threat Management
Security is by definition the management of threats. Below are the basic guarantees that a good Information Security plan should provide:

- Confidentiality (i.e., preventing the unwanted exposure of data)
- Integrity (i.e., preventing the loss or modification of data)
- Availability (i.e., preventing a user from not being able to access or share data; preventing the failure of vital systems)
- Authenticity (i.e., preventing people who claim false identities from completing a transaction)
- Non-repudiation (i.e., preventing parties in a transaction from denying that they sent or received that transaction)

When deciding how to address threats, there are several questions that must first be answered:

- What will the impact be if the threat materializes?
- What is the probability of an attack?
- What measures can be taken to avoid or identify the security event?
- What is the cost of eliminating the threat?

In some cases, it may be too costly (monetarily or otherwise) to eliminate the threat altogether, and it is sufficient to simply identify an attack in real-time or even afterwards. Before making this decision or moving forward with prevention measures, it is important to first understand the different types of Information Security attacks and the motivations behind them.

In the past, security attacks were somewhat random and had obscure motivations. Today, we face a much more sophisticated level of attack that can be powered by strategic business motivations. For example, government-funded “advanced persistent threats” (APT) are extremely difficult to eliminate because they target “zero day exploits” -- unknown vulnerabilities that are almost impossible to protect against. Governments, corporations, and other organizations are also vulnerable to attacks by underground “hactivists” who want to expose private messages and other information.

There is also a growing awareness of risks related to trusted personnel, sometimes referred to as “the internal threat.” It can be very challenging for organizations to protect confidential data from their employees, especially those who work in the IT department. Some of the highest profile Information Security breaches in recent history have been performed by internal personnel, such as leaking government and enterprise information to the Internet (e.g., WikiLeaks).

Other threats focus on denying access to information rather than stealing it. These “denial of service” (DOS) attacks, which prevent users from accessing their accounts or other information, are difficult to prevent and require companies to significantly increase their

Figure 2: Information Security Vertical Stack

computing power and also block incoming traffic in order to preserve the systems and server integrity until the issue is resolved. Unfortunately, these response measures further magnify the effect of the DOS attack and can negatively impact the user experience by creating a "no service" environment.

Because threat management is actually a type of risk management, we recommend the use of common risk management methods such as Mehari, Magerit, and NIST800-30.

Security Infrastructure
To secure systems and information, you must couple strategy and policy with special tools. These tools include software such as anti-viruses, network equipment such as firewalls and proxies, solutions such as public key infrastructure (PKI), algorithms such as encryption or key exchange, product testing tools such as penetration testing tools, and security processes such as Microsoft's Security Development Lifecycle (SDL).

Security Administration
One critical aspect of security is the ability to manage and administer it. After all, if the essence of security is allowing some people to access data but not others, then defining who can access which data is key. Some industries or domains even have special security requirements, either because of government regulations or because their products and/or services manage sensitive information. Examples include PCI DSS for credit card-based systems, DRM administration for digital media, and HIPAA for health insurance.

User Management
Many organizations have customers who interact with their systems, such as online banking or cloud-based software. To provide users with the required functionality while also ensuring the security of the system, organizations must verify the identity of their users. However, users often have multiple identities and passwords for different systems (e.g., Facebook account, online banking account, employer system, etc.). Remembering or securely storing different IDs and passwords -- or even using physical tokens to authenticate each system -- can be very frustrating and complicate application use.

This is why identity management (IDM) is a key component of Information Security. Two security measures associated with IDM -- authenticating a user's identity and authorizing his or her access to specific data -- are necessary for any interaction with a system or application. However, this can be challenging because users must often be authenticated and authorized across multiple levels (e.g., application, network, platform, etc.). We will take a deeper dive into this issue in future white papers in our Information Security series.

Horizontal Stack: Security Technologies

Cryptography
All security protocols, as well as many products and technologies, rely on the science of cryptography and the cryptographic algorithms and protocols that enable you to share information between parties while hiding it from others. This is the foundation layer upon which the Information Security world is built. We view this layer as beneath the physical layer, as it represents the theoretical basis of security.

In most cases, cryptographic algorithms use a "key" to encrypt or decrypt information. The benefit of using public and private keys is that you can assign encryption and decryption functions to different keys. For example, if you wanted a colleague to send you encrypted data, you would share a public key with them. Once you received the data, you would then use a private key to decrypt it. Since only you have access to the private key, the data remains secure, even if your colleague shares the public key. Similarly, public and private keys allow you to separate certificate creation and validation permissions.

Physical Security
As shown in Figure 3 (next page), the physical layer considers all the physical aspects of the data communication channels. It also includes the physical facilities and devices in which the data is stored. This layer includes security aspects such as how to physically secure a wire, how a data center should guarantee its power supply, how to minimize fire hazards, and how to mitigate physical access threats. It also considers how data is stored (e.g., on a hard drive or other device) and the techniques applied to physical parameters to trace data (e.g., forensic analysis).

Network Security
Unless a threat is physical, it will generally involve the network in one way or another. A threat may be to the data in transit over the network or through the network as the gate to the information. The network security layer therefore deals with network encryption solutions (e.g., VPNs and VLANs), network gateways in devices (e.g, firewalls), and the security of the content in specialized proxies that monitor information traveling in and out of the organization.

Trends like wireless communications introduce new security challenges to the WAN. Protocols and standards that are defined by ITU-T and IEEE in regards to the link layer (e.g., 802.1x for port authentication, 802.1q for VLAN, and 802.1p for QoS) are also within the scope of network security layer.

Platform Security
When talking about platforms, we are referring to the general implementation aspects of a solution. In regards to platform security, you must ask questions such as:

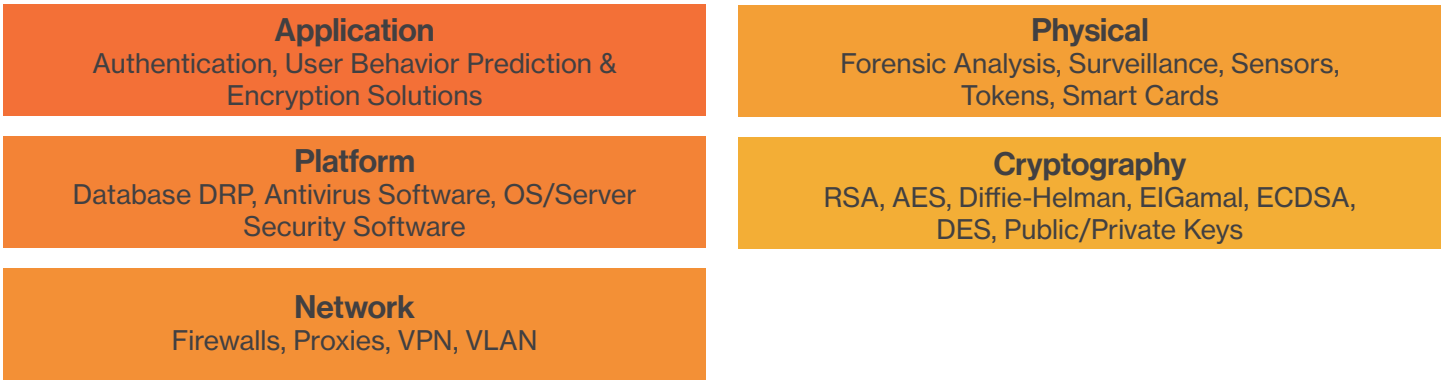
- Is it a web, mobile, or desktop solution?
- What operating system is being used: iOS, Android, Linux, or Windows?
- What database is being used?
- Is any specific application server infrastructure being used?
- Are any Cloud PaaS or IaaS solutions being used?

The platform is the "place" where the applications run, and each platform has its own nature that may cause it to be exposed to some risk. For example, the mobile platform is exposed to risks of being stolen, broken, dropped in water, etc. If you have critical information on your mobile device, it could be lost in seconds. Similarly, if you have information stored on a database, you could easily lose it if the server stops working and you don't have a disaster recovery plan (DRP) or a high-availability platform.

Cloud platforms are sometimes referred to as the solution for everything, but there are several implicit risks. What happens if the startup with whom you entrust your CRM goes bankrupt, and you don't have a way to migrate the information? What happens if you don't have a signed SLA? Because each OS, tool, or technology has both known and unknown weaknesses, it is necessary to analyze the platform and understand what security risks need to be addressed and how.

Application Security
Applications are challenging in terms of security due to several reasons. The first reason is that each application has its own unique functionality, data, and vulnerabilities. In many cases, entire systems are compromised through specific application vulnerabilities. Applications are generally less tested than platforms, and developers tend to focus more on functional logic than security aspects.

Figure 3: Information Security Horizontal Stack



Another challenge is that some applications have special security requirements, either because of government regulatory mandates or because of the nature of the application or domain. For example, banking and financial applications are sensitive to fraud and theft, and healthcare applications must protect sensitive patient medical information. Examples of such government and industry security requirements include Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes–Oxley Act (SOX), Gramm–Leach–Bliley Act (GLBA), and Check Clearing for the 21st Century Act (Check 21).

To meet these regulatory standards and mitigate special risks, you can leverage enhanced authentication solutions, solutions that identify exceptions in a user's predicted regular behavior, enhanced encryption solutions, and other similar solutions for at-risk applications. The application security layer is especially interesting because it applies to direct human interaction as the user of information. This layer not only deals with the applications themselves, but it may also deal with protocols like HTTP, FTP, RTMP, and others.

We typically classify applications as either standalone or connected applications. A standalone app generally does not operate with other components of a communications network, whereas a connected app does. We consider connected apps to be more vulnerable to attacks because they depend on other components. However, even standalone apps can be attacked, either physically or through their maintenance interfaces.

Since applications run on specific platforms, they inherit the platform's risk in addition to their own technical risks that result from the programming language and/or framework on which the application relies. Applications are also exposed to the "human risk factor." This refers to the developers' skills and/or the quality assurance process under which the applications are developed, the procedures that the deployment process involves, user risks (e.g., writing down passwords), etc.

The Creation of Secure Products

Now that we have a general understanding of the different aspects of security, it is important to address how to create secure products.

The Process of Security

Product security is an aspect of product quality. When ensuring product quality in general -- and security specifically -- the development process is a key factor. There are several known processes that can be used to help ensure that products meet security requirements. Examples include Microsoft's Security Development Lifecycle (SDL) and CERT. MS SDL focuses on C, C++, and .NET development for commercial software, whereas CERT focuses on incidents, theory and research in more mature environments (e.g., government and defense). We should note that several leading software developers have adopted MS SDL, and the process is considered compliant with ISO 27034-1.

Whichever process you select, it should address the product requirement definition cycle, the development and testing cycles, etc. It is also critical to ensure that the personnel involved in development have adequate professional knowledge regarding security aspects.

There are also some methodologies and organizations that are focused on specific applications or platform security, such as the Open Web Application Security Project (OWASP). This organization publishes research on web-based app security, and its "Top 10 List" identifies the most critical web application security risks.

Furthermore, there are special tools for performing code review, penetration testing, regression testing, and others. Examples of these tools include free open source tools such as Matriux, MetaSploit, and Kvasir, as well as production tools such as Seeker, Coverity, and Fortify.

The combination of these processes and tools, along with an organizational commitment to security quality, will help ensure that your products meet the required levels of security.

Juan Manuel Caracoche, CTO, Latin America
Tzvi Kasten, AVP, Business Development

About GlobalLogic

Who We Are

GlobalLogic combines cross-industry expertise and experience with market-defining customers to make connections between makers and markets worldwide. Leveraging our unique insight from working on innovative products and disruptive technologies, we help business leaders make amazing products, discover new revenue opportunities, and accelerate time-to-market. Whether working as project-based teams or as carefully assembled in-house labs, our employees take pride of ownership in the products they help design, develop, test, and support.

Our Security Practice Organization

Because Information Security is such an important aspect across multiple markets, we have leveraged our global team of security experts to take a leadership role in this area. We collaborate with our customers to develop security-oriented products and services that excel across all standards. For more information about our services and areas of expertise, please visit www.globallogic.com

The Authors

Juan Manuel Caracoche is GlobalLogic Argentina's CTO and serves as a Professor of Cryptography and Information Security at Universidad de Buenos Aires in Buenos Aires, Argentina.

Tzvi Kasten is GlobalLogic's Associate Vice President of Business Development and leads the company's Security Practice Organization.

About GlobalLogic Inc.
GlobalLogic is a full-lifecycle product development services leader that combines deep domain expertise and cross-industry experience to connect makers with markets worldwide.Using insight gained from working on innovative products and disruptive technologies, we collaborate with customers to show them how strategic research and development can become a tool for managing their future. We build partnerships with market-defining business and technology leaders who want to make amazing products, discover new revenue opportunities, and accelerate time to market.

For more information, visit www.globallogic.com

GlobalLogic®

Contact

Emily Gunn
+1.512.394.7745
emily.gunn@globallogic.com