Adaptive Security Architecture and the Evolution to Continuous Adaptive Risk and Trust Assessment

Issue

In a world of continuously changing systems and a constantly changing threat landscape the protection needs to move from blocking known malicious behavior to detection of suspicious behavior and reacting appropriately, without waiting for a "blacklist" to be updated. The protection strategy needs to be changed from controlling checkpoints for known malicious behavior to monitoring the behavior of the system and constantly checking for deviations from "good" behavior ("whitelisting"). Also, the target moves from total prevention of attacks to a reduction of the potential impact of an attack. There are multiple ways to limit the impact of an attack. The first way is to limit the spread of an infection and thus shrinking the "attack surface". This can be achieved by a segmentation of the system (e.g. at network level). Other methods include slowing down the rate of attack and reducing remediation time by quickly responding to all attacks. This is achieved with an adaptive security architecture (ASA)[1].

Adaptive security architecture describes a new information security approach. The core property of ASA is its ability to adapt to changes. ASA is listed in Gartner's Top 10 Strategic Technology trends of 2016 and 2017. Figure 1 shows a graphical representation of the four main elements of an adaptive security approach.

The traditional security approach focuses on the upper half of Figure 1, (prediction and prevention of threats). This is mainly done by intrusion detection and prevention systems (IDS/IPS). These systems monitor the traffic in and out of a system and compare it to a list of known malicious patterns ("blacklisting"). The blacklists need to be updated as new threats evolve. Due to the continuous evolution of threats this approach is chronically one step behind. Another disadvantage of the traditional security approach mainly relying on IDS/IPS is the focus on the traffic across the borders of the system instead of focusing on the system itself. Attacks which unfold within a system cannot be detected.

Both problems mentioned can be solved with ASA. The adaptive security approach extends the traditional security approach by adding two new elements: detection of and response to attacks. The four main elements prediction, prevention, detection and response work together in ASA to achieve a secure system.

[1] Also known as secure adaptive architecture (SAA).

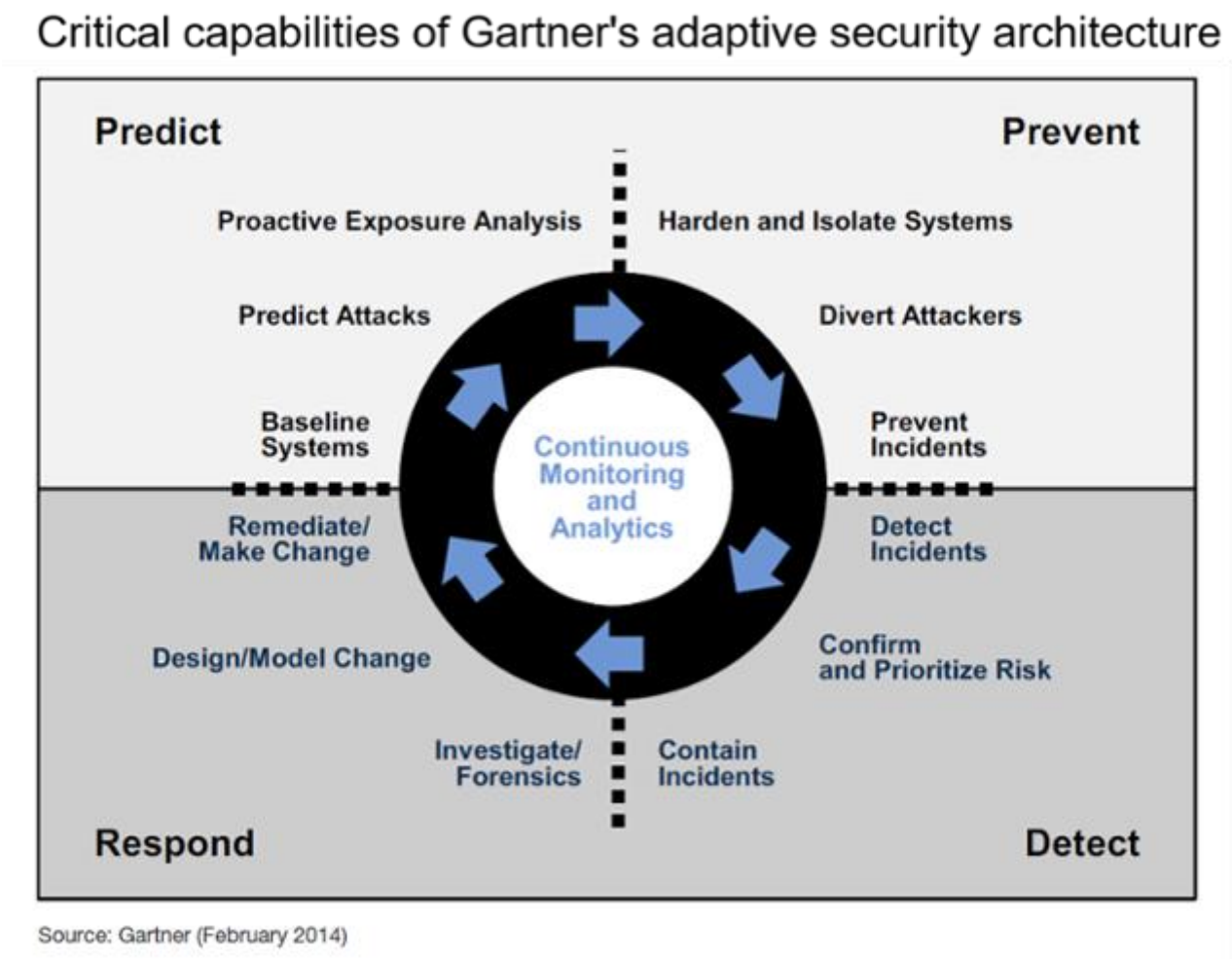

Figure 1: The four main elements of an ASA.

The four main elements of an Adaptive Security Architecture

The first two are prediction and prevention, which provide the functionality of the traditional security approach. To form an adaptive system these are complemented by the two elements of detection and response.

The role of **prediction** is to analyze the existing exposure to threats, to predict potential threats and to anticipate new attack types against the current system. Intelligence from past attacks and other sources is used to predict future attack scenarios. From the element of prediction there is a seamless transition to **prevention**. The system is hardened and isolate to protected against the identified threats by reducing the surface area for potential attacks. Known malicious activities are countered by using the blacklisting approach based on past incidents.

The next element is where the adaptive components start to play a role. Continuous monitoring of the system enables **detection** of a successful attack as early as possible. After the detection of an incident, the risk associated with it is assessed and prioritized. Subsequently the incident can be contained by isolating the affected part of the system and thereby preventing potential damages from turning into actual damages. This step initiates the transition to the fourth

element of **responding** to an attack. The attack that has taken place needs to be investigated to gain intelligence about the full scope of the breach and the impact it could have on the system. This information is then used to design or adjust the model that is used to prevent further attacks on the system. Remediation of damage that has been done is also part of the retrospective response. This step can be simplified by automating some of the responses to the attack. The insight gained from investigating the attack or potential attack is then fed into the predictive parts of the system to help prevent further attacks on the system thereby closing the cycle.

Since it is not possible to entirely prevent the success of an attack it is important to recognize an attack as early as possible. Furthermore, it is important to limit the spread of the attack and to repair any damage done to the system.

How is it done?

No security mechanism can guarantee that a system will never be vulnerable to an attack. Instead of wasting resources trying to prevent an attack from happening, ASA helps to reduce the impact of the attack when it actually happens. In contrast to the traditional security approach ASA protects the system by monitoring the behavior of the system instead of applying traditional perimeter protection or monitoring the behavior of a single user. In contrast to the blacklisting approach in traditional security ASA relies on whitelisting the desired behavior. In an environment of continuous delivery[2] and dynamic systems it is easier to keep the whitelist of desired good behavior up to date than to keep track of all possible malicious behaviors.

If a new system or update is deployed it is already known what the expected behavior of the system (whitelist) will be. Anything diverging from the expected behavior will be flagged and assessed. If the new behavior is found to be harmless or desired it will be added to the whitelist, thereby adapting the whitelist to the changing environment. This classification can be done by security personnel. Alternatively, machine learning or artificial intelligence (AI) can be used to create a system than can categorize new behavior on its own. Tools like user and entity behavior analytics (UEBA) help to analyze the data generated by user activities. Thereby, inside attacks or an attacker using a compromised account can be detected. This use of automation is useful to increase the security of the system. One example is the Splunk User Behavior Analytics tool that uses machine learning to identify previously unknown malicious behavior. The use of automation can speed up the categorization of minor divergences from the expected system behavior since they are less likely to be malicious and therefore give security personnel the ability to quickly respond to major events. Nevertheless, using machine learning can give the opportunity to detect an attack by identifying the small changes in behavior that are unsuspicious on their own. For an adaptive security system to work effectively the necessary

[2] Continuous delivery describes the ability of a system to incorporate changes into the productive system at any time in a reliable manner. This goes along with short software production cycles and thus a continuously changing system with continuously changing potential threats.

flexibility needs to be integrated into the protected system by design. The system must allow to contain incidents without shutting down the whole system.

In practice, the use of a modular system will help to achieve the goal of a system that can easily be adapted to the changing environment. The individual modules can be exchanged like LEGO bricks to provide the adjustability of the system without compromising the functionality. The modules also help to contain an attack. Like with the LEGO bricks the different modules need defined and controllable interfaces to allow for real-time flexibility of the system. A flexible system is what is needed to allow the security system to coevolve with the threat landscape.

Modularization is also helpful when it comes to containing an attack because it is easier to isolate the affected parts of the system.

The next evolutionary step after going from the traditional security architecture to an adaptive security architecture would be a self-adaptive security system. A self-adaptive security system is capable of monitoring its internal security state and the external threat landscape in order to reveal security violations. Furthermore, it is capable to react to possible security violations and ongoing attacks by selecting alternative security mechanisms and parameters to keep the system in a secure state or to move it back to a secure state.

Examples of ASA:

Adaptive security architecture is mainly a concept but a few examples already exists.

One implementation of ASA is the Behavior Blocker component of the Emsisoft Anti-Malware. The Behavior Blocker component continuously monitors the behavior of all active programs and alerts if suspicious behavior is detected. For example, the Emsisoft Anti-Malware successfully prevented WannaCry from encrypting the files. Similarly, the Microsoft advanced threat analytics tool, which is part of the Microsoft 365 Enterprise plan for companies, uses behavioral analytics and machine learning to identify and block unusual patterns.

Beyond ASA – CARTA

The adaptive security architecture is the basic concept necessary to implement a Continuous Adaptive Risk and Trust Assessment (CARTA). CARTA is one of the Gartner Top 10 for 2018 and beyond.

While ASA only provides adaptability of the architecture CARTA also incorporates the decision-making process into the concept.

The security of the system should be **continuous**ly monitored and **adapted** to the changing circumstances. **Risks** should be assessed based on the sequence of events instead of a single event. A combination of harmless, unsuspicious events ca be a security issue. **Trust** also needs to be continuously assessed and adjusted to the changes in environment. Both, the definitions of risk and trust, can change based on the context. The **automated assessment** of data generated

by the system provides the bases for the real time adaption of risk and trust. This enables the security of a system to keep pace with the changing threat-landscape.

The flexible nature of an Adaptive Security Architecture and Continuous Adaptive Risk and Trust Assessment (CARTA) can help to achieve the goal of a secure system. Implementing an adaptive security system is especially interesting for long-term and complex projects.

cnlab contribution

cnlab can help you while migrating from the traditional security approach to an adaptive security architecture. In a first conceptional consulting step we familiarize you with the concepts of ASA and CARTA. Together with you we evaluate the feasibility of an adaptive security architecture in the context of your daily business. The existing solution is compared against an adaptive security solution to illustrate where your organization could benefit from an ASA.

cnlab can also help you testing the capabilities of an existing adaptive security system. This is done by challenging the system with unknown behavior and by observing its reactions.

Success Stories

cnlab has analyzed large computer networks and network components since 1997, for Internet Service Providers, for hosting providers in the banking area, for major international banks and for public administrations. Reviews have shown a wide area of common weaknesses in state-of-the-art systems. We have also analyzed the behavior of these systems, both in normal and in abnormal use cases.

Based on the engineering background of our consultants, we have always been able to work out improvements which could be implemented within reasonable time and budget, and which could effectively fight the weaknesses, or which would counter unexpected behavior.