IMMUNIO

Application Defense in Depth

Making your Applications First Class Citizens

authored by Oliver Lavery
for **IMMUNIO**

IMMUNIO /eBooks

Application Defense in Depth:

Making Your Applications First Class Citizens

authored by Oliver Lavery
for **IMMUNIO**

VP of Research

It is easier and easier these days to make applications for the web, and businesses are using them at ever increasing rates. But not everyone—including developers and those who must defend their systems—knows how to secure them properly. Because of the interconnection of most web applications and IT systems, this lack of knowledge exposes enterprises to security risks from hackers who know how to exploit vulnerabilities to gain access to systems, software, and sensitive data.

CONFIRMED BREACHES BY INCIDENT PATTERN

40%	Web Application attacks
23%	POS intrusions
8.7% ●	Miscellaneous errors
7.6% ●	Privilege misuse
6.8% ●	Cyber-espionage
5.5% ●	Everything else
3.8% ●	Payment card skimmers
2.4% •	Physical theft/loss
2.1% •	Crimeware
>1% •	Denial-of-service

Source: *Verizon 2016 Data Breach Investigations Report*

It is easier and easier these days to make applications for the web, and businesses are using them at ever increasing rates. But not everyone—including developers and those who must defend their systems—knows how to secure them properly. Because of the interconnection of most web applications and IT systems, this lack of knowledge exposes enterprises to security risks from hackers who know how to exploit vulnerabilities to gain access to systems, software, and sensitive data.

As the threat landscape continues to evolve and the definition of a network expands to fit all the devices and applications that touch it, enterprises must expand their idea of what constitutes effective security. There is no single point of entry. Therefore there is no single solution to address all the vulnerabilities and threats to enterprise information assets.

A comprehensive enterprise IT security program must include robust defense of web applications. Protecting the perimeter is vital, but hackers are getting more sophisticated and their attacks more advanced—targeting web applications and data. Securing the application itself is necessary for protection against attacks that breach the perimeter.

This is a real world problem. In 2015, the median number of days an organization was compromised before discovering a breach was 146. It was 205 in 2014, so security is improving. But do you really want your systems to be vulnerable for four months?

2015

2,260

Breaches with confirmed data loss

64,199

Confirmed security incidents*

**As analyzed in the Verizon 2016 Data Breach Investigations Report*

By 2019, enterprises will spend over $1.2 billion on application security, doubling the $600 million spent in 2014.

Source: *Gartner, Predicts 2016: Application and Data Security*

Spending on application security continues to grow as enterprises seek to find the best solutions:

According to Gartner, in 2014 organizations spent more than $600 million on application security and almost $8.9 billion on firewalls and intrusion prevention systems. Yet, "[these] technologies are failing to adequately protect resources. Network traffic and content inspectors treat applications like a black box, analyzing application traffic and/or user sessions. Solutions designed in such a manner cannot see how input is being processed within the application."[2]

The best security solutions for web applications build a layer of protection inside and around an application: They must controls access, monitor and log activity, and sanitize input to the application. When vulnerabilities and threats are discovered they must be reported to staff in an actionable manner. A best in class security solution correlates information from multiple applications to present an accurate picture of attacks on the perimeter and those within it.

Securing third-party and legacy applications is also vital for achieving a fully secure system, but enterprises aren't doing the best job of assessing risks for all the applications they bring into their systems. According to SANS only 26% of IT security professionals perform risk assessment on all of their applications all of the time and only 32% assess risks most of the time (based on the criticality of the application). About a quarter of those in the SANS survey rarely or never run a risk assessment even on new web applications.

[7] *Wagner, Ray, Ayal Tirosh, et al., "Predicts 2016: Application and Data Security," Gartner: 2 December 2015, https://www.gartner.com/doc/3174923/predicts--application-data-security*

EFFECTIVE DEFENSE

Security-aware enterprises know that the most effective defense is comprehensive and flexible. The traditional security posture of protecting the perimeter is just the first step. The networked world is complex and growing ever more so, and threats to the system evolve with the same complexity. Enterprises must be adaptive and ready to protect all of their systems, including applications, mobile devices, and connected devices that are part of the Internet of Things (IoT).

Enterprises are often driven to security by compliance regulations and industry standards, which move at the pace of government and are necessarily years behind the contemporary threat environment. Effective security goes beyond simple compliance and is based on an understanding of the risk profile of all parts of the system and the threats to which they will be exposed.

There is no single solution to securing a system. The truth is that enterprises cannot protect all of their assets all of the time—a dedicated hacker with vast resources and a sophisticated approach is a serious adversary. The goal is to minimize the threats to the system, easily deal with less sophisticated attacks, and recognize when the system is at risk.

The truth is that one vulnerable application can compromise an enterprise's entire network. Hackers look for the weakest point—web applications, mobile devices, email, etc. So a key challenge for information security professionals is understanding all possible entry points, including all the applications on their systems. Yet, according to SANS more than a quarter of their respondents (developers and information security professionals) "didn't know how many applications their organization used or managed."

Most security continues to be reactive—fix the bugs and close the gaps after a breach has occurred. Effective security is about preventing an attack from becoming a breach in the first place. To be effective, a security solution must:

- ***Prevent****—by eliminating vulnerabilities, including updates and patches*
- ***Identify****—the risk, and type and source of attack*
- ***Detect****—with continuous monitoring and logging*
- ***Respond****—address attacks and fix the vulnerability*

Defense in depth

Defense in depth is an approach to network security that has grown in popularity over the last decade. It is a layered approach that works well to prevent attacks from outside the perimeter of the network. Once a hacker gets through the first layer of protection, there are more layers to penetrate or bypass in order to access any particular asset. This is an excellent approach for deterring many types of automated attacks and less sophisticated hackers: Once they hit an impenetrable layer of defense, they will either be detected or be stopped.

Protecting the perimeter is vital, with tools such as firewalls, anti-malware software, demilitarized zones, and intrusion detection. However, once a hacker finds a vulnerability that allows access into the system, those perimeter defenses are useless. And more and more threats are exploiting holes in the perimeter, in the form of vulnerable web applications and access points outside the network perimeter—such as mobile or IoT devices.

DEFENSE IN DEPTH

- **Anti-malware software**
- **Content matching**
- **Data leakage protection**
- **Demilitarized zones**
- **Email gateways**
- **Firewalls**
- **Host security**
- **Session security**
- **User authentication and validation**
- **Virtual private network (VPN)**

BREACHES FROM APPLICATION LEVEL ATTACKS

Anthem Insurance
78 MILLION medical records of current and former customers and employees

Ashley Madison
32 MILLION customer email addresses and personal information

Blue Cross / Blue Shield
10 MILLION customer records

Premera Blue Cross
11 million customer medical and financial records

U.S. Office of Personnel Management
5.6 million fingerprints of current and former federal government employees

**As analyzed in the Verizon 2016 Data Breach Investigations Report*

ENTERPRISE INFORMATION NETWORKS

Seen holistically, global information networks are vast. Even within a single enterprise the level of complexity is barely comprehensible. Easily identifiable assets like the main brand website may be secure. Yet chances are that there are significant vulnerabilities elsewhere in the system, and those vulnerabilities can be used to compromise critical assets. Enterprises can have hundreds of web applications—third-party applications and those developed in-house, newly acquired and legacy. Any vulnerabilities in any of these applications threatens the entire system.

A significant challenge is posed by legacy applications that have typically been built using an architecture that is not designed to deal with contemporary classes of attacks. It is costly and time consuming to rewrite these applications. So, information security professionals often adapt these legacy systems to work with newer systems and interfaces—web-enabled green screen applications, client-server applications, or even older web applications that have been retrofitted to support mobile devices. Even if the application had been designed with protection in mind, that protection is often mismatched to today's advanced threat environment.

A network defense in depth strategy leaves these applications vulnerable. Controls and a defensive strategy that were designed to prevent networks from being vulnerable to the worms of a decade ago are not well matched to a threat environment that targets applications at layer 7. More modern controls like web application firewalls (WAF) are bridge technologies at best. They are a marginally effective attempt to adapt network security technologies like firewalls to address application security threats.

You would never dream of putting a Windows workstation on your perimeter with unprotected Internet access. Yet that is essentially what many security professionals are doing with their applications. What is the

[7] *2016 Data Breach Investigations Report, Verizon Enterprise*

strategy for defending web applications from application-layer attacks? Certainly investing in writing more secure software is money well spent, but what about applications written by third parties? What about the stack of legacy applications accessed from web-facing applications via services or legacy interfaces?

Today, application security is seen as part of a network defense in depth strategy. This is wrong. Applications are first class citizens, like network devices. A comprehensive defensive strategy must equally address the unique challenges of protecting both the network and the application layer—the layer 7 services that network provides.

When information assets resided in files on FTP servers and Windows shares, information security was network security. In today's network of web services and complex applications moving data around with unprecedented efficiency and reliability, information security is just as much about the application as it is the computer it runs on.

Application Defense in Depth

Defense in depth is about protecting the entire perimeter of the network and creating layered internal perimeters to contain breaches. Application defense in depth means using layered defenses within applications and application layer protocols to create multiple, robust layers of defense within the application stack. It uses redundancy as an implicit control. If an attack makes it through one layer, it will not compromise every information asset processed by the system of networked applications.

The foundation of this security approach is that an enterprise's information systems are not simply a mix of network components, some of which are applications. Rather, the view is more holistic—networks and physical systems are the substrate on which applications are built to provide the substance of information processing. Keeping information assets secure then requires parallel, complimentary defensive strategies to protect both the networks and the applications they support.

BENEFIT

In a world of a application-layer attacks and sophisticated threat agents, it is no longer effective to use network boundaries as near absolute trust boundaries: A threat agent who is able to compromise an application can breach even a perfectly secure network. We may, for instance deploy a host-based intrusion detection system (HIDS) to detect if an application is compromised. An attacker who is able to run arbitrary code within that application, however, can access deeper layers of the network without necessarily doing anything that would be detected as a host intrusion.

An application defense in depth strategy moves past the idea of protecting just the network perimeter and assets, and defines and protects the application perimeter and assets in parallel. This is different than viewing applications as things on the network. For example, a web service between an Internet facing application and a critical internal application presents very similar risks to a network cable bridging an Internet facing system to an internal network.

This strategy is critical because the application perimeter continues to expand. Application security used to be peripheral; it was sufficient to view a small number of web applications as simple components of a network. But today, enterprise systems are evolving into complex service oriented architectures. They have enormous numbers of applications interacting to provide the critical information access that allows an enterprise to function.

A typical global enterprise uses many bespoke and third-party applications, spread throughout networks across multiple time zones, supporting desktop users, mobile devices, B2B web services, IP telecommunications, and services in the cloud. When left unsecured, any of these applications has the potential to compromise information assets anywhere on the network. Ultimately, a breach would render the traditional network perimeters and defense-in-depth model irrelevant.

Service Oriented Architecture

The advent of internetworking and Internet connectivity changed the network threat environment. In the past, access control was a matter of keeping the bad guys out. Now, the environment is complex layered strategies comprising many controls and business processes to defend networks. In much the same way, the growth of web services and service oriented architecture (SOA) has fundamentally changed the application threat environment.

Critical information assets sit in trusted areas of the network, behind comprehensive network controls. But if those assets are served up to applications facing the Internet via web services and SOA, is it true to say that they are in a secure network? An asset may be secure from network attacks, and yet critically exposed to application level attack. Today application level controls lag behind network level controls—enterprises simply don’t see them as basic or as necessary to security.

TOP 10 IOT VULNERABILITIES[6]

1. *Insecure web interface*
2. *Insufficient authentiation / authorization*
3. *Insecure network services*
4. *Lack of transport encryption*
5. *Privacy concerns*
6. *Insecure cloud interface*
7. *Insecure mobile interface*
8. *Insufficient security configurability*
9. *Insecure software / firmware*
10. *Poor physical security*

Source: OWASP

Internet of Things

An additional threat to a comprehensive security policy is the Internet of things, those physical objects that can connect to the network and send and receive data via small, embedded web services. Cisco estimates that there will be 50 billion devices connected by 2020. That significantly increases application security risks.

When protecting an enterprise's footprint on the Internet of Things (IoT), it is not just the device that needs to be secured. The network connection and clients are important, but IoT applications that are both inside and outside the network must be protected as well. This leaves organizations open to new vulnerabilities, and the growth of IoT will cause enormous growth in the number of devices running web applications. This presents a huge challenge: While securing IoT devices within the network perimeter is a challenge, an even greater problem will be securing the new application perimeter they create. Increasingly it will be difficult to keep these small embedded devices away from the Internet, buried in the most secure zone of the network.

As Hewlett-Packard notes, "The current state of Internet of Things security seems to take all the vulnerabilities from existing spaces, e.g. network security, application security, mobile security, and Internet-connected devices, and combine them into a new (even more insecure) space, which is troubling."[7]

The problem:[8]

- Six out of 10 devices that provide user interfaces were vulnerable to a range of issues such as persistent XSS and weak credentials.
- 80% of devices along with their cloud and mobile application components failed to require passwords of sufficient complexity and length.
- 70% of devices along with their cloud and mobile application enable an attacker to identify valid user accounts through account enumeration.
- 70% of devices used unencrypted network service.

[7] *Miessler, Daniel, "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," 29 July 2014, http://community.hpe.com/t5/Protect-Your-Assets/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VzcvB2Z5Jrx*

[8] *"Internet of Things Research Study 2015 Report," Hewlett-Packard Enterprise, November 2015, http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf*

BENEFIT

Application defense in depth does present some challenges. Much as an asset inventory is critical to network security, to effectively secure the application layer, security teams need an accurate inventory of applications, and an understanding of the asset value and risk profiles for each.

Even once an inventory is established, enterprises are challenged with finding tools to secure applications that were not developed in-house. Tools, that is, that are not prohibitively expensive in terms of staff time spent fixing code-level defects. The focus of traditional application security is finding defects so that developers can fix them. But this is an expensive proposition, when it is even possible.

A true application defense in depth strategy is tasked to secure applications developed by third parties and those that are no longer actively maintained. Software development is expensive – finding and fixing every defect is ideal for the most critical applications, but what about the breadth of an enterprise application inventory where it is simply unrealistic to bear this cost?

By 2017 25% of application runtime environments will have self-protection capabilities, up from less than 1% in 2012.

Source: *Gartner, Runtime Application Self-Protection: Technical Capabilities*

Runtime Application Self-Protection

Gartner calls for adaptive security architecture to look beyond just defending the perimeter as a way to truly enhance an enterprise's security profile. This is the essence of defense in depth at the application layer. And one key element of this type of security architecture is application self-protection.

Runtime application self-protection is built into or added onto an application runtime environment, protecting the application from within. This technology is an enabler of application defense in depth because it can be applied to applications across the perimeter and within inner trust boundaries, cost-effectively and without access to application source code.

In addition, when built into a new application, runtime application self-protection (RASP) is able to identify vulnerabilities early in the development cycle, to deliver a final product with a stronger security posture.

RASP works inside the application it is protecting, in the application runtime environment. And it can adapt automatically when the application is updated without requiring code updates. In addition to automatically protecting the application at runtime, it is useful for dealing with vulnerabilities even when source code is not available, such as third-party or legacy applications.

By working inside the application, a RASP security solution has deep insight into the inner workings of the application, unlike network layer controls like WAFs. It looks for the logic and data flows inside the application and monitors application execution. It can take the proper steps to secure the application under certain defined conditions, such as a request to access a database, access to a file, or rendering a page for a user. RASPs protect applications by responding to threats with specified actions, such as terminating the session and sending an alert to the security team, preventing a malicious database transaction from executing, or presenting a CAPTCHA to thwart automated attacks by bots.

BENEFITS

- Runtime protection
- RASP continuously analyzes and protects an application.
- Monitor logic flows—including events and machine instructions, to accurately detect and prevent attacks.
- Monitor data flows—know where in the application the data goes and how it is processed.

Centralized information gathering and maintenance

- RASP always resides within the application server, so it works for web, cloud, mobile, and IoT deployments.
- Protects applications that are updated frequently.
- Protects distributed applications throughout the network environment.
- Protects applications programmed in dynamic languages such as Ruby or Python.

RASP is the promise of a web application firewalls (WAF) delivered on by moving the security controls inside the application. WAF technology help protect web applications by protecting the server externally. It analyzes incoming traffic, but it doesn't know what happens inside the application—user behavior or the logic or data flows. Because WAFs see applications as black boxes on a network they block legitimate traffic and are seldom configured to provide preventative controls as a result.

WAF and RASP work together in an application defense in depth strategy. One WAF can protect many servers and RASP protects the runtime environment for each application it secures. WAFs are useful for inspecting the network data entering an application. RASP technology couples this view with an understanding of how potentially malicious input translates into real risks when processed by an application.

CHALLENGES

Dependent on the runtime environment.

- RASP protects only those applications running on the runtime environment in which it is installed.
- Must be added or updated when adding new servers or otherwise changing a runtime environment.
- Requires individual sensor agents to protect all traffic or applications, in separate runtime environments.

Impacts performance

- Uses computing capacity to run, even when using intelligent techniques to analyze only selected data.

The threat landscape is rapidly changing, the network perimeter is expanding, and threats are getting more and more sophisticated. Web applications present a unique security challenge—as the Verizon data shows, the risk from attacks to web applications today dwarfs the risk from traditional network attacks. A single solution to securing your enterprise IT assets does not exist. Adding a comprehensive application defense in depth strategy to supplement your network security posture is the best way to predict when attacks may happen, prevent them when possible, detect breaches, and respond in a timely way to attacks.

ABOUT IMMUNIO

IMMUNIO is a pioneer in real-time application self-protection (RASP), providing automatic detection and protection against web application security vulnerabilities. IMMUNIO augments applications with the necessary protection services and hardens applications against common attacks targeting typical security weaknesses. The company's mission is to make truly effective real-time web protection technology easily available and widely deployed, and by doing so, stop the biggest source of breached data records.

For more information, visit or connect with us at:

www.immun.io
@immunio
info@immun.io