HOW A LAYERED APPROACH IMPROVES SECURITY

INDUSTRY PERSPECTIVE

BROCADE

govloop

Executive Summary

As government relies more heavily on information technology to store, manage and access critical data, it also creates greater potential for that information to be misused or exposed. Data clearly shows that internal threats and external hackers are taking advantage of those vulnerabilities. According to one Government Accountability Office report, the number of cyber incidents in the federal space rose from just 5,503 in 2006 to 67,168 in 2014 – and the number will only continue to exponentially increase.

To help safeguard this ever-expanding attack surface, public key infrastructures, or PKI, have become a standard security measure for most federal government organizations. PKI is a system of digital keys that are assigned to individuals in order to give them access to protected content and IT systems. By creating and verifying digital keys, the federal PKI ensures that only privileged, internal users are able to access government data.

But even as more agencies adopt the infrastructure, some cybersecurity professionals question whether PKI is enough to protect sensitive and confidential information.

According to Niko Agnos, Federal Software Security Specialist, and Darren Rivey, Federal Software Security Technologist at Brocade, the binary functionality of PKI cannot solely eliminate internal vulnerabilities or prevent external hacks. While PKI adds a necessary first level of security, it nevertheless can still leave agencies vulnerable to credential misuse and application-layer attacks.

In this Industry Perspective, created in partnership with GovLoop and Brocade, Agnos and Rivey explain how a layered approach to security and authentication is necessary. They also outline how industry partners like Brocade, a leading provider of modern network solutions, can help agencies deploy this layered defense to their current infrastructures.

The Current Government Environment

Today, nearly every valid user of federal government IT systems is required to have a digital key to unlock the kingdom of sensitive information and public sector data. Those keys are all part of the federally mandated PKI, which provides baseline security to agencies' IT infrastructures by assigning roles, policies and procedures to digital certificates, providing blanket encryption to applications and preventing users without keys from accessing application data.

Agnos described PKI as "the ability to provide the checks and balances between the utilization of digital certificates to identify and authenticate users." However, he said, while PKI does provide some degree of authentication, most organizations will need to add more layers to their cybersecurity protocols in order to truly safeguard their information from malicious users.

"PKI is a binary solution, meaning it gives you a yes or no solution," Agnos explained. While PKI prevents users without digital keys from accessing protected information, those who do have a key gain nearly universal access to what lies within the infrastructure. More often than not, that results in users having unnecessary or even inappropriate access to information.

In addition to potentially providing excessive access to users, PKI also leaves agencies vulnerable to illegitimate users via falsified credentials. Agnos referenced a previous breach at an intelligence agency, where an insider fabricated digital keys to gain access to sensitive information. This tactic is not uncommon, given its relative ease: A malicious user only has to replicate the infrastructure key to gain nearly unlimited access to information and applications when PKI is the only layer of defense.

Moreover, while PKI authenticates digital certificates, it doesn't dive into the details or credentials of individual users.

"An insider threat isn't necessarily always an employee or a contractor who compromises your information," Rivey said. "It could be someone who has stolen your identity or who has executed a phishing attack on an employee or contractor and inserted malicious software into the infrastructure. You can address that sort of insider threat by adding more layers of defense."

Especially in government, further segmentation of access is necessary to reduce the risk of data overexposure and ensure that only the appropriate users can access sensitive or classified information. Adding additional attribute checks to sign-on protocols, as well as applying security directly to applications, can provide better information protection guarantees.

Attribute-Based Authentication

To increase agency security, both Agnos and Rivey impressed the need to supplement, rather than replace, PKI. Given the investment already made in PKI technologies and processes, as well as the general familiarity most federal employees have with the infrastructure, agencies should continue to use it for baseline security.

Agencies can, however, add onto that security by creating additional levels of authentication and protection, placing more checks and more key access points. That's where Brocade's layered approach to security comes in, Agnos said: "And layer one is what we call our Identity Authentication, Authorization, Access and Delivery Solution."

This first layer is created using a Virtual Traffic Manager, which is placed between the access point and application to provide a new point of identity verification. With the traffic manager, an agency can leverage PKI but also better validate the identity of users with additional information correlation. Under this multi-factor authentication process, a user would not only require a digital key but also the necessary personal credentials to access protected information.

"The Virtual Traffic Manager would check the user at the same time that they're checking the PKI certificate," explained Rivey. "And the manager would initiate another check to an attributes database." That attributes database could take an assortment of forms and query a variety of personal identifiers. For instance, human resources databases could be used to verify the employment status and managerial level of staff. Security clearance databases can be checked to certify permission levels. Finally, organizational databases could be used to match an employee's department to relevant content permissions.

Those additional credentials would not only verify an identity but also limit the information that an individual has within the system, rather than giving him or her blanket access with their encryption key.

The idea of using an additional certification isn't an entirely new concept for government. As Agnos noted, "Currently in the Intelligence community they verify an individual at three separate layers: username and password, PKI digital certificate, and security clearance level."

With the Virtual Traffic Manager, agencies across the federal government can easily link additional attributes to their identity authentication procedures. Ultimately, that gives IT leaders greater visibility into who is accessing sensitive information and why they should have that access.

> *With the Virtual Traffic Manager, agencies across the federal government can easily link additional attributes to their identity authentication procedures. Ultimately, that gives IT leaders greater visibility into who is accessing sensitive information and why they should have that access.*

LAYERED SECURITY:

Secure Applications, Not Just Infrastructure

To re-enforce these authentication procedures, Rivey and Agnos also advised creating an additional level of security at the application layer. That way, applications remain protected even if initial authentication procedures are faulty or circumvented by hackers.

Think of it like adding additional protection to your house to keep out intruders, rather than just relying on the fence surrounding your yard. With bars on your windows or an alarm at your front door, you are better prepared should someone get past your perimeter of defense.

This tactic is especially necessary given current IT deployment practices that focus on operational, rather than security, needs.

"Applications are built for business-specific requirements," Rivey explained. "As a result, there's not much attention paid to the security of the application because it's thought that others (outside of the IT operations team) will look after the security."

"When the application is being built, it's actually very common that security defects remain, and the existing security infrastructure doesn't protect against them," he said.

While some application vulnerabilities can be solved quickly with a patch in a third-party component or operating system (OS) module, it is not unusual for logic flaws or data leaks to take months to solve in production systems — leaving doors open for hackers. Some off-the-shelf applications can go unpatched for a year or more, depending on the priorities of the application vendors and the perception of risk.

When applications aren't secure, access policies aren't effectively enforced at the application layer. And, as Agnos explained, many of today's firewalls don't prevent malicious traffic from getting to that layer.

"What you see in the federal space is that the most common firewalls are all focused on things that are done in the infrastructure," he said. "But right now the information that's being compromised is further up the stack at the application level." As a result, many hackers are targeting application security because it is most often left vulnerable.

To remedy this vulnerability and ensure appropriate access, agencies can safeguard their applications with real-time policy enforcement, including transparent secure session management, URL encryption and form-field virtualization.

Brocade Virtual Web Application Firewall (vWAF) is a massively scalable solution for application-level security. It can apply business rules to HTTP(S) traffic, inspecting and blocking attacks such as SQL injection and cross-site scripting, while filtering outgoing traffic to mask personal identifiable information like Social Security numbers and help maintain compliance with federal risk management frameworks.

How to Enhance Your Data Protection Strategy

While the benefits of attribute-based authentication and application-layer security are clear, Rivey said many agencies may be hesitant to pursue additional credentialing processes, particularly if their budgets or IT staff time are constrained. Nevertheless, layered security is a necessity in the face of increasingly sophisticated, multi-tactic cyberattacks.

Rivey said agencies can start small if the idea of overhauling their authentication process seems overwhelming. When it comes to crosschecking additional attributes, for instance, many agencies will already have databases that can be referenced by the Virtual Traffic Manager.

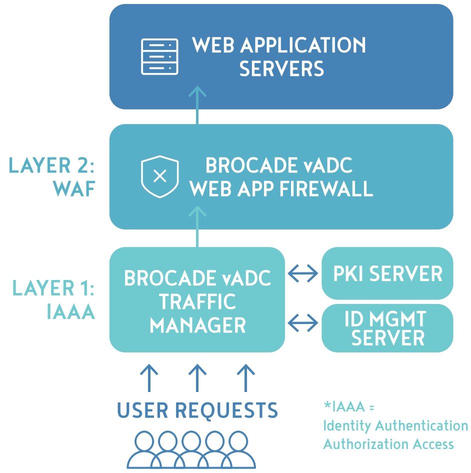
Rather than creating entirely new databases, Rivey suggested starting with commonplace information lists. For instance, most organizations already have robust information sets within their human resources databases. Once you've connected your authentication measures to basic attributes like employment level, you can expand your authentication protocols to investigate more granular details of an identity.

And while IT departments pursue this more nuanced identify verification system, they can continue to leverage their existing public key infrastructures. "What's important to understand is that IT leaders are not going to throw anything away. They are going to build upon and add to what they already have in a way that's unobtrusive and maintains the current level of service for the user," said Rivey.

Similarly, applying a firewall to the application layer of your enterprise doesn't have to significantly disrupt processes or current security investments. Brocade's vWAF solution is quickly installed and application traffic is investigated in real-time. It can also be applied to both off-the-shelf applications and custom-built solutions, ensuring that you can seamlessly incorporate application-level security across your entire infrastructure.

While security can no longer be maintained by PKI alone, Rivey and Agnos asserted that creating a multi-layer strategy doesn't have to be a heavy burden to your employees or your processes. Instead, Brocade's solutions can be seamlessly incorporated into your current infrastructure, building upon and enhancing existing cybersecurity solutions.

vADC Layered Security Solution



> *"What's important to understand is that IT leaders are not going to throw anything away. They are going to build upon and add to what they already have in a way that's unobtrusive and maintains the current level of service for the user."*
>
> – Darren Rivey, Federal Software Security Technologist at Brocade

CONCLUSION:

A Layered Approach is Critical

Following a number of high-profile federal data breaches over the last two years, scrutiny of government information security has never been higher.

"We don't want to see anybody be that next casualty, so we have to make sure that we protect the information," said Agnos.

While PKI provides baseline security via digital certificates and keys, the federal government can no longer rely on this tactic alone to safeguard sensitive information and critical applications. Instead, agencies will need to invest in multiple cybersecurity solutions to craft a nuanced, layered defense against internal and external threats.

"**Real security requires more than a single threaded approach. It's got to be a layered approach**," Rivey concluded. "We have to take the PKI even further and provide attribute-based authentication for those individuals trying to access our systems, as well as a scalable Web Application Firewall for securing data at the application level. If we take this layered approach to information security we will deny inappropriate access to sensitive data, limit breaches, and protect our country."

About Brocade

Brocade® networking solutions empower federal agencies to achieve their critical initiatives in a world where applications and information reside anywhere. By focusing on agility and innovation, Brocade helps agencies modernize their networks while accelerating their journey to the New IP.

Utilizing open, software-driven, and hardware-optimized solutions, agencies can deploy breakthrough technologies in the areas of:

- Storage networking
- Data center switching and routing
- Campus networking
- Software networking: SDN, NFV, and vADC
- Mobile networking
- Network visibility and analytics

To deliver a truly best-in-class solution, Brocade partners with world-class IT companies. Learn more at www.brocade.com.

BROCADE®

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

www.govloop.com | @GovLoop

govloop

1152 15th St. NW, Suite 800
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
@GovLoop