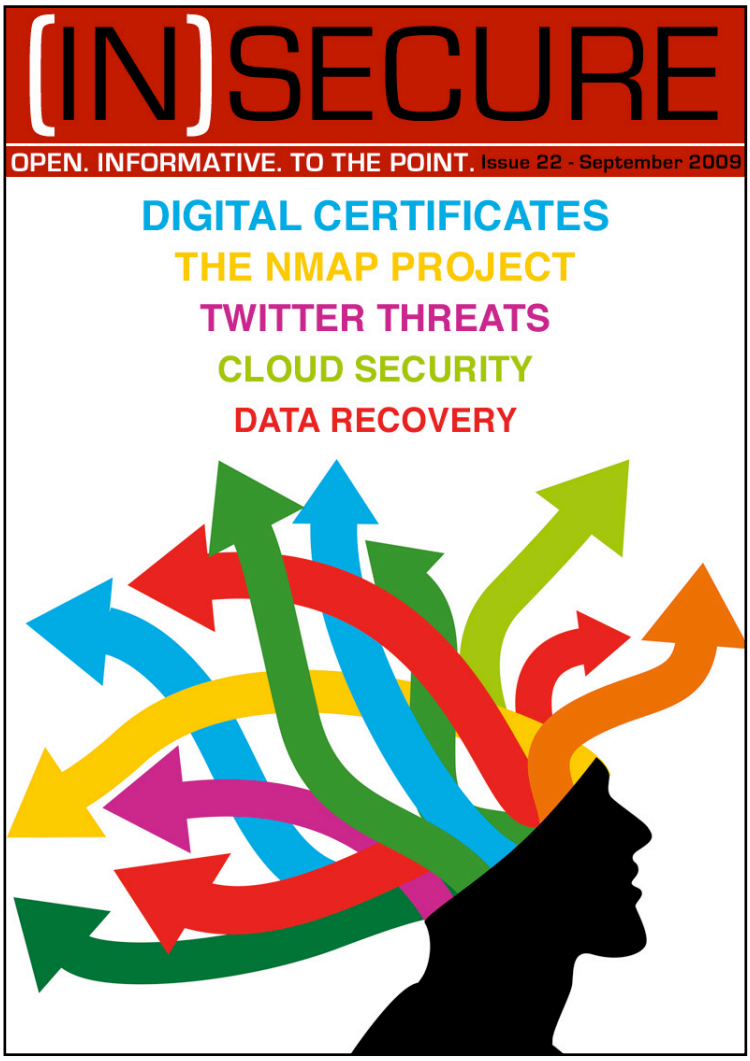
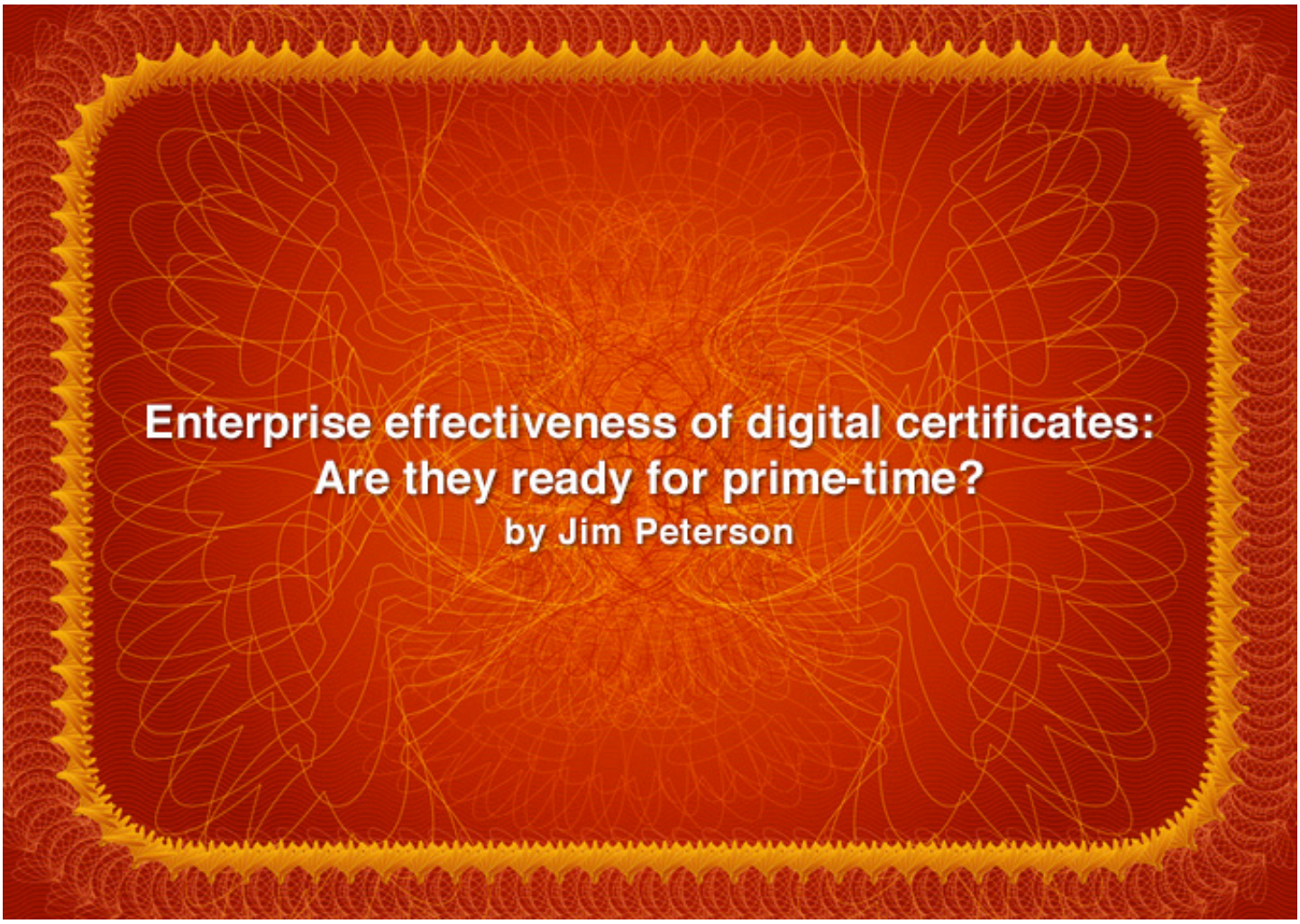


Enterprise effectiveness of digital certificates: Are they ready for prime-time?

by Jim Peterson

As published in (IN)SECURE Magazine issue 22 (September 2009).
www.insecuremag.com



Ever-expanding audit and regulatory requirements leave enterprise IT departments with increasing security compliance concerns. At the same time, budgets are decreasing as a result of current economic conditions. Security standards such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 focus on ensuring sensitive information is protected at all times, regardless of physical location. Increasing demands coupled with reduced resources strain IT departments, constantly requiring them to do more with less.

The combination of increased compliance requirements, reduced resources, and little tolerance for gaps in data security forces enterprises to adapt by rethinking their security strategies. As technology has evolved, needs have changed and risks have multiplied; approaches rejected in the past based on complexity or cost concerns must be reconsidered. While many rejected Public Key Infrastructure (PKI) in the past, the need for persistent, easy-to-use credentials for encryption and identification prompts a second look.

Mature security technologies (e.g., firewall, anti-virus, anti-spam) assure enterprises that their systems are safe from compromise. These systems reliably protect the standard data infrastructures of most organizations. With these trusted protections already in place, IT managers might consider themselves safe from most attacks aimed at any of the standard ports and protocols carrying and storing today's critical business information. In the face of new security challenges, such as the dramatic rise of insider threats and increased regulatory requirements, these protections alone are no longer enough. While many of these technologies provide continuous protection within the band they are designed to work, they cannot safeguard

information wherever it is or wherever it goes.

Protecting sensitive data from threats both inside and outside the organization, throughout its lifecycle, is a difficult and daunting task. This task cannot be met fully by solutions routinely deployed. Reliable IT solutions of the past can be applied on an as-needed basis in an attempt to address new security requirements; however, this approach is costly and is not flexible enough to meet ever-expanding data protection needs.

SECURITY IS NOW MORE THAN JUST THE RESPONSIBILITY OF ENTERPRISE IT DEPARTMENTS

Consider, for example, just a few of the different ways in which a sensitive data file can be exchanged during a typical course of business. It can be delivered through email, using an email security solution that will protect it while in transit to its intended recipients.

Once opened at its destination it can no longer be protected by the email security solution. Alternately, that same file can be delivered using a portable storage device (e.g., CD, tape) that cannot be protected by the email security application. This potentially leaves the data at risk, unless additional solutions are in place for protecting portable media. How would that same data be protected if it must move to the cloud or if it is sent via Instant Message (IM)? Implementing numerous point solutions for each case may address individual problems today, but cannot address the problem as it evolves. They also cannot protect information pervasively as it moves beyond the reach of a given end-point solution. A security framework built on a series of point solutions leaves many opportunities for gaps that leave data vulnerable as it moves from point to point.

Further, security is now more than just the responsibility of enterprise IT departments; it has rightfully become the responsibility of everyone within an organization to ensure the sensitive data they work with is used appropriately.

Often times, IT does not know the nature of sensitive information used by trusted end-users. In fact, in most organizations, the majority of this sensitive information being exchanged both internally and externally should not be accessible by IT workers. IT must be reliable and diligent in providing appropriate tools and technologies, but they are not the appropriate resource for making critical decisions about protecting sensitive data. Consequently, IT must select and deploy flexible, comprehensive security solutions for their enterprises, and then appropriately train users on how and when to use them. Individual users must recognize the responsibility they hold for the data they work with. This approach to security will only be effective when the ability to apply protections is part of the users' standard workflows. User responsibility can be augmented by point solutions such as Data Loss Prevention (DLP), but cannot fully or effectively be replaced by them.

As this approach to data security expands to include all users within an organization as well as external parties with whom sensitive data is shared, the need for appropriate credentials for individual users becomes increasingly important. This need drives forward-thinking data security professionals to reconsider how digital certificates can meet this need. In an effort to combine a scalable data security solution with user accountability, organizations are adopting digital certificates and finding them effective. Certificates provide their users with the security credentials useful for both identification and data encryption.

Digital certificates are based on the concept of public/private key cryptography. This concept utilizes a mathematically related pair of keys. One key, the public key, is used when encrypting data which only the other key, the private key, can open. A digital certificate is issued by a trusted third party, a Certificate Authority (CA), that validates the identity of the holder of the private key. This provides a verifiable chain of trust behind each certificate.

A digital certificate provides a much more durable level of security than traditional methods such as password authentication or encryption systems. Passwords remain a familiar, but vulnerable means of protecting data due to the inherent difficulties of managing and using passwords. Password-based systems also pose a security risk due to on-going susceptibility to common password cracking methods such as brute-force or dictionary attacks that will reveal a password if the attacker is persistent.

Digital certificate technology has evolved over the past 20 years. It is now a stable and mature technology that has become an important security component embedded within many popular IT functions such as web browsers with SSL, Virtual Private Networks (VPNs), secure FTP, email, and many other systems widely used today. Given the increasing use of digital certificates for enterprise security, how do they measure up in their effectiveness for deployment within large scale individual security?

A forum at RSA Conference 2009 brought together technology experts and IT administrators for an informal peer discussion on how digital certificates are meeting industry security needs. This open discussion offered useful insight into the current state of the enterprise readiness of digital certificates from the perspective of those that are actually implementing them to solve real business issues.

PASSWORDS REMAIN A FAMILIAR, BUT VULNERABLE MEANS OF PROTECTING DATA

The specific needs of attendees for credentials ranged from security for corporate websites and portals to individual end-user credentials for securing email and unstructured data files. A critical goal shared by attendees was a need to effectively provision end-users with end-to-end data protection. Forum participants agreed that digital certificates offer the most viable option available for providing both identity verification and data privacy.

Few issues were raised with using digital certificates for web security or other embedded systems. Most attendees reported they can easily and routinely obtain and deploy SSL certificates sufficient for their organizations' needs. Forum participants voiced concerns of how effective the same technologies are when used for individual user credentials. These concerns aligned with three key topics of discussion:

- Misconceptions about PKI
- Usability of digital certificates
- Management & control of digital certificates.

Identifiable gaps in digital certificate technology leave barriers in the path of wider adoption. These gaps block the ability of IT to support and maintain secure systems and inhibit the ability of organizations to effectively elevate the responsibility for security beyond just the domain of IT.

Misconceptions about PKI

PKI is an acronym for Public Key Infrastructure, a method for issuing and managing verifiable digital certificates issued by a trusted Certificate Authority (CA). Despite both the maturity and stability of PKI, it is still routinely spoken of negatively and, as a result, enterprises often resist implementing a security strategy utilizing digital certificates. Stories of failed PKI projects, cost overruns, and lack of benefits have created a perception that key management is too difficult and too costly to implement. These perceptions are mostly based on experiences of early adopters of the technology that had only a few choices for obtaining certificates.

Implementation options for PKI today have expanded and largely mitigate the issues encountered by those early adopters. Organizations can now choose a certificate management solution that fits both their budget and their administrative needs. Available options range from internal PKI solutions purchased from any of the leading industry vendors

to externally hosted services that can provide any quantity of certificates from just a few up to large numbers. Today, internal options for hosting PKI are now bundled with major enterprise operating platforms such as Windows and IBM System z. This option is suitable for larger organizations that need to issue many certificates and that prefer to manage their certificates within their internal IT group.

Choosing an external certificate source can reduce the administrative costs by removing the need to purchase and internally manage a PKI solution. This approach provides a good solution for organizations that plan to adopt certificates gradually through a pay-as-you go model and ensures certificates are associated with an established global trust source.

USERS HAVING CERTIFICATES MAY STILL OFTEN USE THEM INAPPROPRIATELY

Usability

To some, digital certificates are still considered too difficult to use and maintain within most organizations where technical complexity of any kind introduces costly end-user training concerns. Despite the advances in available options and improvements in setting up and maintaining a PKI as a certificate source, the end-user component - digital certificates – may still be viewed as an obstacle. Too many steps and administrative touchpoints with users still exist in the delivery, use, and exchange of certificates.

Opportunities for user error abound in both the enrollment and use of certificates in environments where there is user resistance to adopting a new technology - most users are comfortable with using a password for data privacy and protection, while a digital certificate is unfamiliar and is perceived as complicated. Forum panelists pointed out that one benefit offered by digital certificates is that they can be integrated more transparently into user workflows, removing the need to remember or retrieve a password. This transparency requires readily available access to both the public and private key pair of the certificate, as well as the public keys of other certificate users. Private keys may often be available only from a single system which restricts where a user may effectively use it for protecting information. Increasing availability of portable, hardened certificate storage options in the form of a smart card or smart token offer the promise to remove this restriction; however, interoperability with these devices remains limited to only a few applications today.

Public key access can be impeded by limited availability of hosted public key directories. This leaves users few options other than resorting to complex, technical key exchange steps. Alternate solutions offering the promise of simplifying the use of public/private keys through easily available identifiers (e.g., email address), unfortunately, fall short as a result of their inability to scale to meet the needs of a large and often widely dispersed population of internal and external users.

Management and control

Managing data security across disparate applications that integrate inconsistently, if at all, with centrally issued certificates, increases the cost and complexity of administration and can leave gaps in protection. Few applications make use of certificates today for end-user encryption or authentication (digital signing), yet data often moves between different applications and passes through many hands during normal use. This presents areas of risk as data moves between users and between cross-platform and cross-vendor applications possessing varying levels of certificate support. Applications that attempt to reduce perceived end-user complexity by “hiding” their use of digital certificates inside the application provide only limited data protection - protection that is lost as the data moves beyond the boundaries of that application.

Users having certificates may still often use them inappropriately. Lack of policy support to ensure appropriate use and contingency access to encrypted data complicate audit and regulatory compliance efforts.

Finding an effective solution

Questions remain about how to effectively use digital certificates to ensure data is both secure and remains available to efficiently respond to business needs. More specifically, how can digital certificates be used without resorting to multiple vendor solutions with varying levels of certificate support? The answer is data-centric security.

Data-centric security always stays with the data, protecting it wherever it is, wherever it goes, and however it gets there. Applying security directly to the data reduces the need to rely on certificate solutions for each application, reducing the complexity and cost of using and managing digital certificates. Use of digital certificates with data-centric encryption applications does, indeed, confirm that digital certificates are an answer for enterprise security. Data-centric solutions that fit seamlessly into existing user workflows avoid certificate enrollment and management complexity; they ensure appropriate use through policy and provide the level of usability, management, and control necessary for making digital certificates an effective enterprise data security solution. A few solutions are now available that offer usable certificate solutions and control, making digital certificates ready for primetime.

Jim Peterson is the Chief Scientist at PKWARE (www.pkware.com). He has been developing commercial software products for over 20 years and has spoken on data security issues at a number of industry forums.