Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

PKI and Information Security Awareness: Opportunity and Obligation

The core technology of PKI, public key cryptography, was invented some 25 years ago. So why has this technology been so slow to gain acceptance? Frequently discussed challenges to successful PKI deployments include integration with internal business processes and legacy systems, automation of processes that extend beyond the firewall to business partners, and user acceptance. In this paper we explore the latter: "In the final analysis, the single most difficult criterion for a successful PKI rollout is user acceptance....

Copyright SANS Institute
Author Retains Full Rights

AD

PKI and Information Security Awareness: Opportunity and Obligation

Jerry K Brown

October, 2001

The Promise not Met

Could 2002 be the "Year of PKI"? This question has been posed annually since at least 1997. The promise offered by Public Key Infrastructure (PKI) in electronic commerce is compelling: instantaneous transactions at a potential cost reductions of up to 99% over traditional paper-based commerce. "And although the research firm International Data Corp. (IDC) predicts that the total market for PKI products and services will grow to $3 billion in 2004, PKI technology has not yet broadly penetrated the B2B market…" (Stross). Further, an oft-cited Gartner study reported last year that "80 percent of PKI deployments are only pilot projects and of the 20 percent of production deployments, a full 40 percent will fail within two years of implementation" (Johnson & Manusco, Feb 16, 2001). The core technology of PKI, public key cryptography, was invented some 25 years ago. So why has this technology been so slow to gain acceptance?

Frequently discussed challenges to successful PKI deployments include integration with internal business processes and legacy systems, automation of processes that extend beyond the firewall to business partners, and user acceptance. In this paper we explore the latter: "In the final analysis, the single most difficult criterion for a successful PKI rollout is user acceptance." (Johnson & Manusco, March 27, 2001)

In this context, user involvement and acceptance has two main aspects:

- Will personnel understand and accept the risks of conducting business in the electronic world without the familiar financial and legal instruments that are the underpinning of traditional commerce?

  > Today [May 2001] in the United States, less than 1 percent of the gross domestic product is handled through the digital channel. In addition, many commercial and government enterprises have yet to realize the potential lift in their operations by transforming points of customer interaction through the Internet. However, without fundamental trust among parties in the process, the use of the Internet for complex transactions will continue to be impeded. (Howard)

- Do employees understand the policies and will they follow the procedures that are required in the world of digital certificates?

  > A limitation to nearly all security systems is its users. Policies can provide clear and concise direction, but are useless if misinterpreted or misused. Well-defined policies can decrease user errors and increase user awareness. (Bobbitt)

A Question of Trust

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Besides being a technology based on public/private keys and digital certificates, PKI is also a trust network which operates at several levels: Trust between organizations and their PKI service providers (certificate authorities for example), between companies and their trading partners, and among individual employees who, at the end of the day, are the ultimate buyers and sellers. At the organizational level this trust is embodied in contracts and service level agreements. But at the user level trust must be promoted through training and developing awareness.

A grounding in security fundamentals is essential, but with an emphasis on the practical aspects, particularly as they relate to commerce. At a minimum, the core concepts of PKI - authentication, confidentiality, integrity and non-repudiation – should be covered, as they also form the legal basis of traditional commerce. Personnel with an understanding of these concepts will be more comfortable with engaging in electronic business transactions. The following table summarizes the essential aspects of the information employees will need in this regard.

Fundamental Security Concepts Embodied by PKI			
Concept	**Meaning**	**Traditional Method**	**PKI Mechanism**
Privacy, Confidentiality	Information is available only to those authorized for it.	Sealed envelope Invisible ink	Encryption with a public key ensures that only the owner of the paired private key can decrypt the message.
Authentication, Identification	You are who you say you are and you have rights to entry or information	Employee ID, driver's license, passport Mother's maiden name	A digital certificate issued by a trusted certificate authority binds a public key to an individual
Integrity	Information is genuine and un-altered.	Permanent ink Letterhead stationary, water-marked paper	A digital signature comprising a message digest and the sender's private key can be validated using the sender's public key.
Non-repudiatio	Evidence that an activity or transaction cannot later be denied.	Notarized signature, Paper trail Registered mail	The digital signature validating a transaction can only be created by the private key holder.

These concepts, along with a basic presentation of encryption, should form the basis of an employee education program in support of a successful PKI program. Managers and key project personnel in particular will need a thorough understanding of this information and the related PKI mechanisms so that they can communicate to staff and help with questions and problems.

Of course user awareness must extend beyond just PKI basics to include all aspects of

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

information security principles, but a PKI project presents a major opportunity for leveraging communication efforts to maximum effect. For example, the potential threat of social engineering now represents additional risk as the payoff for malfeasance as a result of compromised or stolen digital certificates may be significantly increased in a PKI-enabled environment. It becomes more important than ever that employees recognize that they are in fact the organization's first line of defense against electronic crime. Additionally, PKI means that business is increasingly dependent upon functioning computing resources, so that downtime resulting from careless email habits or lax virus protection may have a direct impact on operating efficiencies. In summary, there will now be an expanded set of business risks associated with PKI that can be used to reinforce awareness of the real world consequences of poor security habits. The following table, while not an exhaustive list, provides a summary of common security threats, their PKI consequences, potential business impacts, and suggested countermeasures.

Common Security Threats & PKI Risks			
Threat	**PKI Risk**	**Business Impact**	**Countermeasures**
Social engineering	Compromised certificate	Fraud, espionage	Verify identity, report suspicious behavior
Computer theft	Stolen certificate	Fraud	Secure laptop computers & follow safety precautions in airports and public places
Hacking	Stolen or compromised certificate	Fraud, espionage	Strong passwords, firewalls, intrusion detection
Virus	Corrupt certificate	Loss of function	Avoid attachments from unknown parties, use anti-virus software & keep it current
Data loss	Lost certificate	Loss of function	Back up regularly, secure backup media
Open file sharing	Stolen or compromised certificate	Fraud, espionage	Avoid sharing computer drives, use passwords on shares

User awareness of general information security principles and best practices is a necessary, but not sufficient requirement for successful PKI deployments.

> if the technology is to catch on as many predict it will, some sticky management problems will have to be solved, and companies will have to find a way to convince users that the added security is worth the hassle. … If your employees, partners, and customers aren't properly following security policy, they could be leaving you at risk (Desmond).

Policy and Practice

As stated above, PKI is among other things a trust network between business partners and service providers. The anchor of the trust relationship is the certificate authority (CA), the entity that is responsible for issuing digital certificates as well as maintaining and publishing

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

certificate status information (revocations, expirations). The details on how this is managed vary broadly depending on the PKI model (enterprise, trading partner, or community of interest) and the specific implementation and are beyond the scope of this paper. The important point here is that what the CA provides, i.e., practices and procedures, is documented in a certification practice statement (CPS) published by the CA. And as defined in X.509, within the certificate itself a set of rules called the certificate policy (CP) "indicates the applicability of the certificate to a particular community and/or class of application" (ISO/IEC 9594-8).

So we see that the PKI infrastructure itself embodies a set of policies and practices, which are designed to support the needs of particular applications or trust models. Hence the selection of specific PKI services and resources must be based on the security requirements of the organization and the goals of the project. Furthermore, the deployment must incorporate organizational policies that are consistent with the CP and CPS as well as internal security and business requirements. The execution of some of these policies can be built into applications, for example, transaction dollar limits based on specific personnel or business partner criteria. However, there will be many others that fall upon the shoulders of individuals and which ultimately must be distilled into accessible and easily understood form as a set of operational policies and procedures.

> … clear and concise policies are the backbone of any PKI that's used outside its own closed community. … With this new way of looking at policies, the end user and relying party are considered above all else. Trusted relationships are meaningless if these two parties cannot reasonably understand the policies. (Bobbitt)

Whereas a PKI initiative presents an opportunity for communicating information security principles and best practices broadly across an organization, it also represents an obligation to ensure that the requisite security policies and business procedures are communicated clearly to those on the front lines and their management. Within the context of a PKI deployment, this would normally be included in the training curriculum associated with the project. Details would necessarily vary for different application areas. For example in a supply chain scenario, personnel on the procurement side, those placing materials orders and receiving goods, would typically have a very different set of policies and procedures from those at the sales and fulfillment end. And of course the associated financial functions, payables and receivables, would likewise require specific training in their application areas. The important point here is that personnel in various functional areas will need a solid understanding of specific policies and procedures in addition to a general comprehension of PKI and security principles.

The obligation is not limited only to the PKI deployment phase; in fact it presents a challenge to organizations to maintain ongoing security awareness programs as well as periodic training refreshers. These efforts have two objectives: The first, of course, is to preserve as much as possible the level of comprehension and compliance achieved during the initial phase. Secondly, to counter the inevitable dilution of awareness and knowledge of specific functional policies and procedures which results from normal personnel turnover and organizational movement as well as the passage of time.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Meeting the Challenge

In general, a PKI project would not necessarily affect all personnel directly, that is, as immediate participants. However, it is likely that such an initiative could engender widespread notice in the employee population at large. Herein lies the first element of the awareness opportunity: interest. Besides the captive audience of participants and others in supporting roles, the attention of a larger audience of the curious and those who may simply be looking for opportunities to contribute is up for grabs. Attracting people's attention is at least half the battle in the field of communications.

Additionally, by collaborating on the design and content of printed matter and online presentations, training course curricula, and other communication media, PKI project managers and those responsible for information security awareness programs have the opportunity to realize synergies in pursuit of related goals. Through coordination and shared effort, they may be able maximize their return on investment of time and resources and avoid redundant and/or conflicting efforts.

Finally, senior management support for PKI can be tapped to communicate their commitment to information security objectives and its alignment with business goals. Ultimately, security awareness must become part of the organizational culture and both top down and bottom up communication strategies will be required in order to achieve this aim.

It is beyond the scope of this paper to delve into specifics regarding the use of various media and communication channels to achieve communication objectives. The effectiveness of different approaches will vary from one organization to the next and there is much prior work regarding specific options. However, the most effective campaigns will utilize a range of channels, including but not limited to printed matter to enhance training sessions, intranet web pages for broader availability, and coverage in online and printed publications to inform and stimulate general interest.

Summary

PKI, one of the most promising developments of the digital age, has been slow to gain broad acceptance and major market penetration. It is widely acknowledged that user awareness of security fundamentals, as well as the understanding of specific PKI policies and procedures are critical factors in the ultimate success of PKI projects. PKI is a trust network both at the organizational and at the user level. Trust must be cultivated and promoted through general security awareness initiatives and focused training efforts, both initially as a component of PKI rollouts and as ongoing programs and/or periodic refreshers. A PKI project presents an opportunity for leveraging information security awareness resources and efforts to reach beyond those directly involved into the organization at large.

References

Bobbitt, Mike. "PKI Policy Pitfalls." Information Security, July 2001. URL: http://www.infosecuritymag.com/articles/july01/features_pki.shtml

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Desmond, Paul. "E-Security: Trends and Futures". Softwaremag.com, October/November 2000. URL: http://www.softwaremag.com/archive/2000oct/E-Security.html

Ford, Warwick and Baum, Michael S. Secure Electronic Commerce. Upper Saddle River: Prentice Hall, 2001.

Housley, Russ and Polk, Tim. Planning for PKI. New York: John Wiley & Sons, 2001.

Howard, Pat. "Time to get serious about e-trust". News.com Perspectives, May 8, 2001. URL: http://news.cnet.com/news/0-1276-210-5851487-1.html

ISO/IEC 9594-8, Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks

Johnson, Cam and Manusco, Matthew. "The Burden of Proof". Intelligent Enterprise, Feb 16, 2001. URL: http://www.intelligententerprise.com/010216/trust1_2.shtml

Johnson, Cam and Manusco, Matthew. "The Weakest Links". Intelligent Enterprise, March 27, 2001. URL: http://www.intelligententerprise.com/010327/trust1_1.shtml?edev

Stross, Kenner. "Managed PKI for B2B Computing". EBiz Q, March 26, 2001. URL: http://www.messageq.com/security/stross_1.html

© SANS Institute 2001, Author retains full rights

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**