Phishing Prevention Using Digital Signatures and PKI

Christopher Furton

Syracuse University

For many organizations, email is heavily relied on and has the potential to significantly enhance communications or, without it, to detrimentally impact performance. However, because email is often an essential service, with it comes substantial risk. Part of that risk is the use of email to execute phishing attacks. Phishing is “a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users’ confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion” (Jakobsson & Myers, 2007, p. 1).

Email Phishing occurs when a threat agent sends a malicious email to a computer user containing a link that, when clicked, redirects the user to a fraudulent website. That website can collect confidential information from the user such as login credentials, credit cards, or other personal information (Jakobsson & Myers, 2007, p. 1). These phishing attacks take advantage of people who are not that technically savvy and trick them into revealing important information. In a recent phishing attack, threat agents attempted to gain access to U.S. government official’s personal email accounts and monitor email traffic by forwarding copies to the attacker’s email address (Zorz, 2011). Fortunately, the email service provider was able to disrupt this attack; however, many attacks go undetected. Organizations need to take precautions to protect their users from malicious phishing attacks.

One method to reduce the success of email phishing attacks is to implement a Public Key Infrastructure (PKI) and mandate the use of digital signatures. “PKI is a system for encrypting, authentication, and validating network transactions through certificate authorities and digital certificates” (Hazari, 2002, p. 386). Using PKI, a digital signature can be added to every email that, once validated, proves to the recipient that the email came from the sender. Since phishing attacks often spoof the sender's identity so that the receiver thinks the included link is safe (Jakobsson & Myers, 2007, p. 1), the likelihood of success is reduced because the email will not be digitally signed. Lack of digital signature or failure to validate a signature will alert the receiver to a potential attack. All email users will need to be trained on how to recognize digital signatures and what to do if one doesn't exist.

Because of the importance of user understand with regard to PKI, training is essential. All email users need to be trained on how to digitally sign an email and policy should be developed to mandate the use of digital signatures on all emails. Additionally, training will need to be conducted to show email users how to recognize a digital certificate and what to do if a validation error is presented by the email program while attempting to verify the authenticity of an email message. Even with successful implementation of PKI and appropriate policy directing the use of digital signatures, there is still risk associated due to the human factor. However, training can reduce that risk.

With a properly trained workforce, Public Key Infrastructure can also provide additional value by increasing control over confidentiality and integrity of emailed information while in transit. For example, the phishing attack mentioned in the Zorz article, the malicious agents forwarded emails from compromised accounts to an unauthorized individual. With the use of PKI, encryption could be utilized that would have ensured that only the intended recipient of that email could have opened it (Robiette, 2001).

In conclusion, phishing attacks pose a significant risk to an organization's information and information systems. The risk can be reduced by implementing technical controls such as Public Key Infrastructure and policy controls mandating use of digital signatures. With added encryption capability and non-repudiation, the investment in a complete PKI system is worth the cost. Although the risk associated with phishing cannot be eliminated due to the ever changing technology and the human factor, the addition of this layer of defense will prove beneficial.

References

Hazari, S. (2002). Challenges of implementing public key infrastructure in netcentric enterprises. *Logistics Information Management , 15*, 385-392.

Jakobsson, M., & Myers, S. (2007). *Phishing and counter measures: understanding the increasing problem of electronic identity theft.* Hoboken, NJ: John Wiley & Sons.

Robiette, A. (2001). Digital certificates and public key infrastructure. *VINE , 31* (2), 42-49.

Zorz, Z. (2011, June 02). Retrieved June 06, 2011, from Help Net Security: http://www.net-security.org/secworld.php?id=11106

About the author

Author: Christopher Furton

Website: Http://christopher.furton.net

Certified professional with over 12 years of Information Technology experience and 8 years of hands-on leadership. An expert in cyber security with both managerial and technical skills proven throughout a career with increasing responsibility and performance expectations. Known ability to translate complex information for universal understanding. Detail-driven, results-focused leader with superior analytical, multitasking, and communication skills. Well-versed in industry best practices including Project Management and IT Service Management. Currently holding active CISSP, CEH, ITIL Foundations, Security+, and Network+ certifications.

Visit the auhor's blog:
IT Management Perspectives - https://christopherfurton.wordpress.com/

Social Sphere:

LinkedIn	Twitter	Google+	Quora	Wordpress	Flavors.me
Slide Share	Tumblr	YouTube	Pinterest	About.me	Vimeo