SSL Security in Browser plug-in: Managing the list of CAs

Nikhil Khatu, Yuri Kolesnikov
{ngkhatu,ykolesn}@ncsu.edu

3/5/2013

Abstract

Write a brief overview of your project idea here.

1 Related Work

Certified lies: Detecting and defeating government interception attacks against ssl (short paper) - [24] Improved Approach on Modeling and Reasoning about PKI/WPKI - [30] Ten risks of PKI: What you're not being told about public key infrastructure - [5] The Web Accessibility Crisis of the Korea's Electronic Government: Fatal Consequences of the Digital Signature Law and Public Key Certificate - [17] Evaluating certification authority security - [12] Public Key Superstructure - [26] Introduction to public key technology and the federal PKI infrastructure - [13] Finding the PKI needles in the Internet haystack - [16] PKI scalability issues - [23] Trusted paths for browsers - [29] PKI seeks a trusting relationship - [8] Why phishing works - [4] Do security toolbars actually prevent phishing attacks? - [28] Client-side defense against web-based identity theft - [3] Browser interfaces and extended validation SSL certificates: an empirical study - [2] Phishing forbidden - [1] Building anti-phishing browser plugins: An experience report - [18] A Scheme to improve security of SSL - [7] Network security: private communication in a public world - [11] Access control meets public key infrastructure, or: Assigning roles to strangers - [6] Mitigating Man in the Middle Attack over Secure Sockets Layer - [9] Trust Darknet:Control and Compromise in the Internet's Certificate Authority Model - [19] Stronger Password Authentication Using Browser Extensions - [20] Do Security Toolbars Actually Prevent Phishing Attacks - [27] PhishGuard: A Browser Plugin-in for protection from Phishing - [10] Learning of Personalized Security Settings - [22] VeriKey: A Dynamic Certificate Verification System for Public Key Exchanges - [21] Design of a plug in for browser against phishing and spoofing attacks - [25] A Solution to Phishing and Pharming Attacks - [14] Shining Chrome: Using Web Browser Personas to Enhance SSL Certificate Visualization [15]

References

[1] N. Agarwal, S. Renfro, and A. Bejar. Phishing forbidden. *Queue*, 5(5):28–32, 2007.

[2] R. Biddle, P. Van Oorschot, A. S. Patrick, J. Sobey, and T. Whalen. Browser interfaces and extended validation ssl certificates: an empirical study. In *Proceedings of the 2009 ACM workshop on Cloud computing security*, pages 19–30. ACM, 2009.

[3] N. Chou, R. Ledesma, Y. Teraguchi, D. Boneh, and J. C. Mitchell. Client-side defense against web-based identity theft. In *11th Annual Network and Distributed System Security Symposium (NDSS04)*. San Diego, USA, 2004.

[4] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 581–590. ACM, 2006.

[5] C. Ellison and B. Schneier. Ten risks of pki: What you're not being told about public key infrastructure. *Comput Secur J*, 16(1):1–7, 2000.

[6] A. Herzberg, Y. Mass, J. Mihaeli, D. Naor, and Y. Ravid. Access control meets public key infrastructure, or: Assigning roles to strangers. In *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*, pages 2–14. IEEE, 2000.

[7] Z. Huawei and L. Ruixia. A scheme to improve security of ssl. In *Circuits, Communications and Systems, 2009. PACCS'09. Pacific-Asia Conference on*, pages 401–404. IEEE, 2009.

[8] A. Jøsang, I. Pedersen, and D. Povey. Pki seeks a trusting relationship. In *Information Security and Privacy*, pages 191–205. Springer, 2000.

[9] Y. Joshi, D. Das, and S. Saha. Mitigating man in the middle attack over secure sockets layer. In *Internet Multimedia Services Architecture and Applications (IMSAA), 2009 IEEE International Conference on*, pages 1–5, Dec.

[10] Y. Joshi, S. Saklikar, D. Das, and S. Saha. Phishguard: A browser plug-in for protection from phishing. In *Internet Multimedia Services Architecture and Applications, 2008. IMSAA 2008. 2nd International Conference on*, pages 1–6, Dec.

[11] C. Kaufman, R. Perlman, and M. Speciner. *Network security: private communication in a public world*. Prentice Hall Press, 2002.

[12] S. Kent. Evaluating certification authority security. In *Aerospace Conference, 1998 IEEE*, volume 4, pages 319–327. IEEE, 1998.

[13] D. R. Kuhn, V. C. Hu, W. T. Polk, and S.-J. Chang. Introduction to public key technology and the federal pki infrastructure. Technical report, DTIC Document, 2001.

[14] O. MahMood. Custom plugin - a solution to phishing and pharming attacks. In *Proceedings of the 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing*, pages 32–38. World Congress In Computer Science, 2006.

[15] M. Maurer, A. Luca, and T. Stockinger. Shiningchrome: Using web browser personas to enhance ssl certificate visualization. In *Human-Computer Interaction*, pages 44–51, 2011.

[16] M. Pala and S. W. Smith. Finding the pki needles in the internet haystack. *Journal of Computer Security*, 18(3):397–420, 2010.

[17] H. M. Park. The web accessibility crisis of the korea's electronic government: Fatal consequences of the digital signature law and public key certificate. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 2319–2328. IEEE, 2012.

[18] T. Raffetseder, E. Kirda, and C. Kruegel. Building anti-phishing browser plug-ins: An experience report. In *Proceedings of the Third International Workshop on Software Engineering for Secure Systems*, page 6. IEEE Computer Society, 2007.

[19] S. Roosa and S. Schultze. Trust darknet: Control and compromise in the internet and certificate authority model. volume PP, pages 1–1.

[20] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. Mitchell. Stronger password authentication using browser extensions. page 15. Stanford Crypto, 2005.

[21] M. Sharifi, E. Fink, and J. Carbonell. Verikey: A dynamic certificate verification system for public key exchanges. In *Detections of Intrusions and Malware, and Vulnerability Assessment*, pages 44–63, Jul 2008.

[22] M. Sharifi, E. Fink, and J. Carbonell. Learning of personalized security settings. In *Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on*, pages 3428–3432, Oct.

[23] A. J. Slagell and R. Bonilla. Pki scalability issues. *arXiv preprint cs/0409018*, 2004.

[24] C. Soghoian and S. Stamm. Certified lies: Detecting and defeating government interception attacks against ssl (short paper). *Financial Cryptography and Data Security*, pages 250–259, 2012.

[25] A. Upadhyaya. Design of a plugin for a browser against phishing and spoofing attacks. *World Journal of Science*, 2:30–33, 2012.

[26] S. Wilson. Public key superstructure. 2008.

[27] M. Wu, R. Miller, and S. Garfinkel. Do security toolbars actually prevent phishing. 2006.

[28] M. Wu, R. C. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 601–610. ACM, 2006.

[29] Z. E. Ye, S. Smith, and D. Anthony. Trusted paths for browsers. *ACM Transactions on Information and System Security (TISSEC)*, 8(2):153–186, 2005.

[30] M. Zhang, X. Zheng, S. Lv, and Y. Yu. Improved approach on modeling and reasoning about pki/wpki. In *Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on*, pages 1–4. IEEE, 2010.