20th Annual IEEE International Conference and Workshops on the Engineering of Computer Based Systems (ECBS)

Software Security

Johannes Sametinger
Dept. of Information Systems – Software Engineering
JKU – Johannes Kepler University
Linz, Austria
johannes.sametinger@jku.at

Abstract—**The importance of IT security is out of doubt. Data, computer and network security are essential for any business or organization. Software security often remains out of focus, from an organization's, a developer's and from an end-user's point of view. We will consider security terminology, security bugs, security flaws, and mitigation issues.**

Keywords-software security; IT security; security bugs; security flaws; secure software development

I. Introduction

Nowadays, security issues are permanently reported in the media. The topic is also on the radar of mass media where mostly stories are reported when many users are affected. Prominent examples are data breaches against Sony [1] or Yahoo [2]. Also, the term cyber war has often been used lately. Computers are becoming important in political conflicts and are increasingly used as weapons [3]. The Stuxnet virus is an example of highly sophisticated malware intended to cause physical damage to industrial facilities [4].

Software vulnerabilities are often the entrance door for attackers, which software vendors have to fix in their updates. Microsoft and Apple, for example, periodically offer updates to their operating systems, including many security fixes.

II. Terminology

IT security is about protecting information and information systems from unauthorized access and use. Confidentiality, integrity and availability of information are core goals. Besides IT security, other security terms that are often used include network security, computer security, web security, mobile security, and software security. Software security is "the idea of engineering software so that it continues to function correctly under malicious attack" [5].

III. Security Bugs and Flaws

Prominent software security bugs include buffer overflows, SQL injections and cross-site scripting. There are many recent examples, where these bugs have occurred and caused damage. While security bugs are problems at the implementation level, security flaws are located at the architecture or design level. Security flaws are much harder to detect and typically need more detailed expert knowledge. Log forging is a simple example for a security flaw. The secure logger pattern, for example, provides a potential solution to this problem [6].

IV. Mitigation

Mitigation issues can be seen from two different perspectives, from a developer's point of view and from an end-user's point of view. What does it need to develop secure software? Security touch points [5], the security development life-cycle [7], and issues of secure coding [8] are important for developers. Input validation can be an effective first step for improved software security. For end-users, the importance and urgency of software updates is an important question. A recent study of the German BSI has emphasized the necessity to keep software up-to-date [9].

V. Conclusion

Technical aspects are necessary but not sufficient to guarantee security. Humans remain the weakest link in the security chain. An amusing example of consequences of the simple fact that users share their passwords with colleagues has been shown in [10].

References

[1] D. Wakabayashi, "Sony Plan for Network Takes a Blow", The Wall Street Journal, April 28, 2011. http://online.wsj.com/article/SB10001424052748704187604576288703220414540.html

[2] D. Fitzgerald, "Yahoo Passwords Stolen in Latest Data Breach", The Wall Street Journal, July 12, 2012. http://online.wsj.com/article/SB10001424052702304373804577522613740363638.html

[3] NYT, "Cyberwar", The New York Times, Feb. 28, 2013. http://topics.nytimes.com/topics/features/timestopics/series/cyberwar/index.html

[4] CBS News, "Stuxnet: Computer worm opens new era of warfare", March 4, 2012. http://www.cbsnews.com/8301-18560_162-57390124/stuxnet-computer-worm-opens-new-era-of-warfare/

[5] G. McGraw, "Software Security," IEEE Security & Privacy, vol. 2, no. 2, pp. 80-83, March-April 2004. doi:10.1109/MSECP.2004.1281254

[6] C. Steel, R. Nagappan, R. Lai, "Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management", Prentice Hall, 2012.

[7] M. Howard, S. Lipner, "The Security Development Lifecycle", Microsoft Press, 2006.

[8] M. Howard, D. LeBlanc, "Writing Secure Code", 2nd Edition, Microsoft Press, 2003.

[9] BSI. „Überprüfung der Wirksamkeit der BSI-Konfigurationsempfehlungen für Windows 7", BSI-CS 048, v1.00, 12. Nov. 2012 (German)

[10] K. Poulsen, "Hacker Disables More Than 100 Cars Remotely", Wired, 03.2010. http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/

978-0-7695-4991-0/13 $26.00 © 2013 IEEE
DOI 10.1109/ECBS.2013.24