Computer Security: PROG1340

01/03/2015

24 Deadly Sins of Computer Security

Assignment #1 Book Report

Book by Michael Howard

Report by Brandon Davies (6271977)

Contents

Brandon Davies

What is the full name of the book and the author

The book title is “24 Deadly Sins of Computer Security” and was written by Michael Howard, David LeBlanc and John Viega.

Background about the author

Michael Howard is currently a principal security program manager on the Trustworthy Computing Group’s Security engineering team at Microsoft. He is responsible for managing secure design, programming, and testing techniques for the entire company. Michael Howard started at the New Zealand branch of Microsoft in 1992 working with compilers with the Product Support Services team. In 1997, he move to America to work on the Windows division on Internet Information and then moved to his current job in the year 2000.

How many pages are in it

There are 370 pages of information in this book, not including the index.

What are the author's objectives and audience

The author’s objectives are to make programmers aware of the most common and most hazardous security flaws that can be programed. They tell you what they are, how to spot them, and how to fix them. The key audience is anyone in the field of programming. This book covers all types of applications from web to mobile and databases, and on platforms from Windows to Linux and Mac OS X.

Summary of the book

The book is designed to inform the reader about the major security flaws that can be make when making any program. The 24 flaws that he covers are:

1. SQL Injection
2. Web Server-Related Vulnerabilities
3. Web Client-Related Vulnerabilities
4. Use of Magic URLs, Predictable cookies, and hided form fields
5. Buffer Overruns
6. Format String Problems
7. Integer Overflow
8. C++ Catastrophes
9. Catching Exceptions
10. Command Injection
11. Failure to Handle Errors Correctly
12. Information Leakage
13. Race Conditions
14. Poor Usability
15. Not Updating Easily
16. Executing Code with Too Much Privilege
17. Failure to Protect Stored Data
18. The Sins of Mobile Code

19. Use of Weak Password Paced Code
20. Weak Random Numbers
21. Using Cryptography Incorrectly
22. Failing to protect Network Traffic
23. Improper Use of PKI, Especially SSL
24. Trusting Network Name Resolution.

Each chapter is laid out to show the reader: An overview of the flaw, what the effected languages are, examples in the main affected languages, how to spot them in code, and how to program around them.

Did the author support/demonstrate their arguments/statements adequately

Yes the author supported their arguments and their statements adequately. Every "Sin" is backed up with code demonstrating the flaw and a full explanation of the code and what the user can do to exploit it.

"

```
char buf[1024];
snprintf(buf, "system lpr –P %s", user_input, sizeof(buf)-1);
system("buf);
```

In this case, the user was unprivileged, since it could be absolutely anyone wondering by a workstation. Yet, simply typing the text **FRED; xterm&** would cause a terminal to pop up because the ; would end the original command in the system shell; then the *xterm* command would create a whole new window ready for commands…"[1]

This quote clearly shows the example of command line injection and how it can be exploited by a user. After which he then goes on to show code that gets around the flaw and explains why it is more secure.

My thoughts and analysis of the book

Was it easy to understand

24 Deadly Sins of Computer Security is a very well laid out book that allows for understanding each flaw, how to spot them and how to not have the flaw in your code. It is difficult to follow for the languages that you do not know, but that is expected for such a technical book; I simply skimmed over the languages I do not know. If you are using this book to learn about flaws in a certain language or to learn about a specific flaw this book is very understandable. If you are reading it for general knowledge, there are parts that will be hard to follow.

Was it outdated

This book looks to be very up-to-date showing what is common now, and has been common for many years, but I cannot fully judge this criteria because I am not fully up to speed on what the current trends are in security flaws. This book has praise for being up to date on its' publish date in 2009, and I am sure that the flaws this book covers have not been corrected on a language level.

Would you recommend it to a classmate

I would recommend *24 Deadly Sins of Computer Security* to a classmate. This book is full of flaws and security holes common in programing today no matter what programming field you are entering. It is also laid out very well to allow you to find only the information you are interested in for fast look up. Therefore it is useful for programmers as well as my classmates.

Would you recommend it to a friend who is not in the computer industry

I wound not recommend this book to a friend outside the industry. *24 Deadly Sins of Computer Security* is very technical in nature because a lot of the content is very specific about programming languages and full of code examples. A person that is not familiar with programming will not get any usable information from, or understand this book.

Did the author have any obvious biases

I did not see any bias in the reading of this book. It is a very technical book, almost like a manual, which leaves little room for bias.

Was the book relevant to my career development

This book is related to my career development because it covered crucial flaws from all types of programming. No matter what field of programming I go into, there are lessons from this book that I can apply to make my code more secure.

Overall opinion of the book

I think this book is a very good tool for learning how to write more secure code. The book is laid out in such a way that it can be used for general knowledge or for learning about specific issues. *24 Deadly Sins of Computer Security* covers a large array of security issues that makes this book useful to any programmer from developing databases to mobile applications. For new programmers, this book is a little hard to follow because of the level of technicality, but is still usable because of the in depth explanations and examples. Michael Howard does a great job explaining what the issues are so that you know what you are learning about, then about how the flaw can be used against your program to show you why it matters. He then tells you how to find the flaw and fix it in your own code so that your code is more secure. I learned a lot about comment security flaws, giving me more confidence in writing secure code.

References

Howard, H. (2009). *24 Deadly Sins of Computer Security*. New York: McGraw-Hill Osborne Media

[1] Howard, H. (2009). *24 Deadly Sins of Computer Security*, page 173.