PRIVACY AND SECURITY OF MODERN TECHNOLOGY

THE ARTICLES IN THIS E-BOOK WERE ORIGINALLY PUBLISHED BY INFOSEC INSTITUTE

DANIEL DIMOV & RASA JUZENAITE

Privacy and Security of Modern Technology

By Daniel Dimov and Rasa Juzenaite

2015

The content of this book was originally published by: InfoSec Institute, Inc.

7310 W. North Ave

Suite 4D

Elmwood Park, IL, 60707

http://www.infosecinstitute.com

DISCLAIMER OF WARRANTY

The authors make no representations or warranties with the respect to the accuracy or completeness of the contents herein and specifically disclaim all warranties, including, but not limited to, fitness for a particular purpose. The advice provided in this e-book may not be suitable for every situation.

First Edition, 2015

ABOUT AUTHORS

Daniel Dimov is an Internet law expert based in Belgium. Daniel is a fellow of the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Society (ISOC). He did traineeships with the European Commission (Brussels), European Digital Rights (Brussels), and the Institute for EU and International law "T.M.C. Asser Institute" (The Hague). He has a Master's Degree in European law (The Netherlands), a Master's Degree in Law (Bulgaria), and a certificate in Public International Law from The Hague Academy of International law. Daniel is a PhD candidate at the Center for Law in the Information Society at Leiden University, the Netherlands. Daniel Dimov has authored several peer-reviewed publications in the area of alternative dispute resolution. He presented his articles at conferences in Cyprus, Belgium, and the Netherlands.

Rasa Juzenaite works as a project manager in the IT legal consultancy firm in Belgium. She has a Master degree in cultural studies with a focus on digital humanities, social media, and digitization. She is interested in the cultural aspects of the current digital environment. Rasa also regularly contributes to InfoSec Institute by writing about information security and digital culture.

For more information about authors, please visit

http://www.dimov.pro.

TABLE OF CONTENTS

PREFACE

This e-book is a compilation of 44 articles published by InfoSec Institute within the period 2012 - 2015. The articles, published in the chronological order of their first publication, are focused on the privacy and security implications of modern technologies, such as the Internet of Things, human-implanted RFID chips, crowdsensing technologies, beacons, smartwatches, sleep-tracking devices, Google Glass, and nanorobots.

While there are hundreds of quality publications in the field of information security, there are few books that analyse the privacy and security of the cutting-edge technologies. Thus, the present book can be an important supplement to any textbooks and other materials dealing with information security in general.

Since one of the authors of the present work is a lawyer and the other has a background in digital culture, the book “Privacy and Security of Modern Technology” pays specific attention on the legal and cultural aspects of the modern technologies. Furthermore, the information in the book is easy to understand even for people who do not have extensive knowledge in the field of information security.

LEGAL AND TECHNOLOGICAL CONCERNS REGARDING THE USE OF BIOS ANTI-THEFT TECHNOLOGIES

1. Introduction

In 2006, a laptop containing personal and health data of 26,500,000 veterans was stolen from a data analyst working for the US Department of Veterans Affairs. The data contained the names, dates of birth, and some disability ratings of the veterans. It was estimated that the process of preventing and covering possible losses from the theft would cost between USD 100 million and USD 500 million.

One year later, a laptop used by an employee of the UK's largest building society was stolen during a domestic burglary. The laptop contained details of 11 million customers' names and account numbers. The information was unencrypted. Subsequently, the UK's largest building society was fined with GBP 980,000 by the Financial Services Authority (FSA). The reason for the fine was failing to have effective systems and controls to manage its information security risks.

From these two examples, it can be inferred that laptop theft is a serious problem that concerns both businesses and individuals. Victims of laptop theft can lose not only their software and hardware, but also sensitive data and personal information that have not been backed up. The current methods to protect the data and to prevent theft include alarms, anti-theft technologies utilized in the PC BIOS, laptop locks, and visual deterrents.

This article is focused on the BIOS anti-theft technologies. It starts with an overview of these technologies (Section 2). Next, the work discusses the legal (Section 3) and technological problems (Section 4) arising from the use of BIOS anti-theft technologies. Then, it recommends solutions to those problems (Section 5). Finally, a conclusion is drawn (Section 6).

2. Overview of BIOS anti-theft technologies

BIOS anti-theft technologies are embedded in the majority of laptops sold on the market. They consist of two components, namely, an application agent and a persistence module. The application agent is installed by the user. It periodically provides device and location data to the anti-theft technology vendor. In case a laptop containing an installed application agent is stolen, the anti-theft technology vendor connects to the application agent with the aims of determining the location of the computer and deleting the data installed on the laptop.

Upon a request of the owner of the laptop, the anti-theft technology may permanently erase all data contained on the magnetic media. In order to make sure that the data have been deleted property, some anti-theft technology vendors overwrite the data sectors of the deleted files.

The persistence module is embedded in the BIOS of most laptops during the manufacturing process. The BIOS is the code running when the computer is powered on. It initialises chipset, memory subsystem, devices and diagnostics. The BIOS is also

referred to as firmware.

The persistence module is activated during the first call of the application agent to the anti-theft technology vendor. The persistence module restores the application agent if it has been removed. For instance, in case a thief steals a computer and reinstalls the operating system, the persistence module will restore the agent. It should be noted that, until the application agent is installed by the user, the persistence module remains dormant.

Even if the BIOS is flashed, a persistence module that has been enabled will continue restoring the application agent. This is because the persistence module is stored in a part of the BIOS that cannot be flashed or removed.

3. Legal issues

Principally, if the buyer of a laptop agrees with the installation of an application agent on her computer, there is nothing illegal in the use of anti-theft technologies. However, in some cases, a seller of a laptop may either accidentally activate the application agent before sending it out or sell to the buyer a machine that was originally meant for a customer who ordered a computer with an installed application agent.

When an application agent is installed without the consent of the user, it falls into the scope of the definition of backdoor. Backdoor is a program that gives a remote, unauthorized party complete control over a system by bypassing the normal authentication mechanism of that system.

The application agent is not the first case of a backdoor not specifically designed to damage and/or disrupt a system. In April of 2000, several e-commerce websites discovered that their Cart32 shopping card software contained a backdoor password enabling any user to obtain a listing of the passwords of every authorized user on the system. The purpose of the backdoor was to enable technical support personnel to recover the users' passwords. Because the backdoor password was embedded in the program code itself, anyone with access to the software could exploit it undetectably.

The activation of an application agent without the consent of the user infringes most privacy laws around the world. In order to stop the violation of their privacy rights, the affected users may submit a request to the anti-theft vendor for the purpose of removing the application agent from their computers and have recourse to a court.

Actually, an affected user often does not know that the application agent is installed on its computer. This is because the agent is very difficult to detect. It runs as a non-descript service and is not listed as an application. The agent does not appear on the programs menu listing or as a system tray icon.

In relation to the submission of a request for removal of the content to the anti-theft technology vendor, it should be noted that a number of unsatisfied users complained in online forums because of anti-theft technology vendors' failure to respond in time to their questions and requests to have the application agent removed. For example, a user complains that, despite sending more than five emails to the company producer of his

laptop and the anti-theft technology vendor, he did not receive a reply on his request to remove the application agent from his computer. He was not able to reach them even after several phone calls.

4. Technology issues

In 2009, security researchers Anibal Sacco and Alfredo Ortega published an article stating that the implementation of an application agent of a particular vendor embedded in the BIOS has security vulnerabilities. These vulnerabilities can be used for insertion ofa dangerous form of BIOS-enhanced rootkit that can bypass all chipset or installation restrictions and reutilize the existing features offered by an anti-theft technology.

Rootkit is a software or code that allows a persistent undetectable presence on a computer. The BIOS is the best place that a rootkit can attack because it survives reboots and power cycles, leaves no trace on disk, survives and re-infects re-installations of same operation system (OS), survives and re-infects re-installations of a new OS, and is difficult to detect and remove.

The capabilities of a BIOS rootkit can be seen from an experimental rootkit for desktop computers developed by researchers from Microsoft and University of Michigan. The rootkit, called SubVirt, can survive hard disk replacement and OS reinstallation. Because it can modify the boot sequence and loads itself before the OS, it can operate outside the OS and remain hidden from many anti-virus programs. Moreover, by using hardware virtualization technology from CPU manufacturers, SubVirt is able to load the original OS as a virtual machine and intercept the OS's calls to hardware.

It should be reminded that use of BIOS embedded rootkits in mobile devices is not a new phenomenon. In October 2008, criminals in Europe inserted rootkits in a credit card-reading machines while they were still in the supply-chain. The compromised card-reading devices continued to function like normal credit card readers with the exception that they copied customer's credit card information and transmitted it to criminals via a cell phone network. The only way to remove the toolkit was to flash (rewrite) the BIOS with a known clean copy, delete the hard drive, and reload the OS from clean installation media.

In relation to the use of anti-theft technologies, a question arises as to whether the protection against thieves deserves paying the high price of having a low-level information security. In this regard, it should be pointed out that an unauthorized access to a computer system can be as disturbing as a theft of a laptop.

5. Solutions

5.1 Solutions to legal problems caused by anti-theft technologies

Pertaining to the legal issues arising from the use of anti-theft technologies, this article recommends four solutions.

Firstly, anti-theft technology vendors should guarantee that the application agent is not

accidentally activated. This can be done, for instance, by adopting a policy of activating the application agent only after receiving a written consent from the user.

Secondly, measures should be taken to ensure that machines meant for a customer who ordered a computer with an installed application agent are not resold to a customer who has not agreed with the installation of the agent. Such measures may include additional checks before selling laptops to customers.

Thirdly, a user who activated the application agent should be regularly informed about the presence of the agent. This will give the users an opportunity to unsubscribe if the agent is installed incidentally. The dissatisfaction of the users with regard to incidentally installed application agents can be seen from the following excerpts of a comment posted in an internet forum:

“I have a new laptop, and never paid for a subscription. I didn’t even know I had their damned spyware installed in my BIOS (or in whatever other piece of hardware it is). I’ve never even been invited to subscribe. Yet my firewall one fine day warned me that rpcnet.exe was trying to access the net. I googled it, and that’s how I know what it is.

Don’t believe them if they say it “lies dormant” until activated with a subscription. I personally caught it talking to them. Do not believe them when they say they have deactivated it.”

Fourthly, anti-theft technology vendors should provide the users with a way to check whether the application agents are installed on their computers. At present, it is difficult for a layman to establish whether the application agent has been activated.

5.2 Solutions to technological problems caused by the use of anti-theft technologies

Concerning the technological problems related to the use of anti-theft technologies, this article recommends to the producers of BIOS anti-theft technologies that they put more effort in order to eliminate the vulnerabilities found by Anibal Sacco and Alfredo Ortega. Instead of responding by press releases containing statements that avoid discussion of the actual findings of the researchers, it would be better if the anti-theft technology vendors present technical facts indicating that the findings of the researchers are wrong, patching the problem, or offering any updates to fix the issue.

6. Conclusion

According to the statistics, 1 of every 10 laptops is stolen or lost. A Gartner Group report notes that one laptop is stolen every 53 seconds in the United States. BIOS anti-theft technologies make the retrieving of a lost or stolen laptop possible. All that’s needed is a little luck and the foresight to enable or install the application agent.

However, this article has shown that, apart from benefits, anti-theft technologies have two major drawbacks. The first drawback is that the privacy rights of the users are infringed when the application agent is activated without the consent of the user. The information security vulnerabilities of these technologies constitute the second drawback.

These drawbacks were noticed by both security researchers and the users of laptops. In the modern era of privacy conscious societies, it should not come as a surprise that laptop users want to ensure that their personal information will not be shared without their consent and that their machines are as secure as possible.