BACKDOORS IN SOFTWARE: A CYCLE OF FEAR AND UNCERTAINTY

Leah Holden, Tufts University, Medford, MA

Abstract:

With the advent of cryptography and an increasingly online world, an antagonist to the security provided by encryption has emerged: backdoors. Backdoors are slated as insidious but often they aren't intended to be. Backdoors can just be abused maintenance accounts, exploited vulnerabilities, or created by another agent via infecting host servers with malware. We cannot ignore that they may also be intentionally programmed into the source code of an application. Like with the cyber attrition problem, it may be difficult to determine the root cause of a backdoor and challenging to prove its very existence. These characteristics of backdoors ultimately lead to a state of being that I liken to a cycle of fear where governments or companies throw accusations around, the public roasts the accused, and other companies live in fear of being next. Notably missing from this cycle are any concrete solutions for preventing backdoors. A pervasive problem underlies this cycle: backdoors could be mitigated if software developers and their managers fully embraced the concept that no one should ever be able to bypass authentication. From the Clipper chip to the FBI and Apple's standoff, we will examine requested, suspected, and proven backdoors up through the end of 2017. We will also look at the aftermath of these incidents and their effect on the relationship between software and government.

Introduction:

A backdoor has been defined as both "an undocumented portal that allows an administrator to enter the system to troubleshoot or do upkeep" and " a secret portal that hackers and intelligence agencies used to gain illicit access" (Zetter). These two definitions may seem very different, but a simple administrative portal, if discovered by a malicious user, could very easily become a secret portal for attackers. Essentially, a backdoor is a method of bypassing the authentication and other security features

for convenience or malicious purposes. Backdoors are heavily involved in what has been described as a 'shadow war' between different nation-states; this list often includes the U.S., Russia, and China.

While the public hears of some cyber conflicts and is fearful of their consequences, a more subtle cycle of fear plays out between nation-states. Many countries suspect their competitors of studding imported software with backdoors to 'spy' on them. Due to this fear, governments will demand to view the source code of software to verify that it has no backdoors. This in turn presents another issue: who is to say that these countries didn't discover vulnerabilities or maintenance backdoors during their viewing of the source code? Any such vulnerability or backdoor could potentially be abused to create a malicious backdoor. Backdoors are the ultimate weapon in intelligence because they can enable an agency to listen in on conversations, peruse data, and generally monitor online activity. The more backdoors that an agency has access to, the more information they have at their disposal.

To the Community:

Privacy is a big issue in an increasingly online world. As citizens of a democratic nation, Americans need to be aware of what is going on to inform how they vote, and everyone should think critically about what they put on the Internet. Moreover, technology users need to be aware of recent developments, such as the Kaspersky Lab and NetSarang incidents, to inform their choice of software. With the suspicions during the last election that cybercrimes affected the outcome, as Americans it is also our responsibility to uphold the tenets our democracy, particularly our ability to elect officials. Whether the software is designed to speed up voting or count calories, we need to develop a no-tolerance policy for maintenance portals, egregious vulnerabilities, and overt backdoors alike in the software we use.

Background:

When encryption was starting to become more popular, the government was worried that they would lose the ability to gain intelligence through Internet traffic. The NSA, endorsed by the Clinton

administration, tried to mandate that a computer chip called the Clipper chip be installed in all American-made computer hardware. In a *New York Times* article published in 1994, Steven Levy described the resulting debate centered around the issue that "cryptography shields the law abiding and the lawless equally." The same debate over privacy for law-abiding citizens versus the ability to track criminals has continued into the twenty-first century. Opponents of the Clipper chip remarked that "truly sophisticated criminals would never use it" and instead default to other hardware without a backdoor. Levy quoted Senator Patrick J. Leahy as adding that "the Government should not be in the business of mandating particular technologies." Moreover, a Bell Laboratories researcher said that they had found a flaw in the chip itself that a user could take advantage of to "bypass the security function of the chip in some applications" (Levy). Overall, the consensus appeared to be that the chip would violate the privacy of the law-abiding without being effective at tracking criminal activity.

Even after being defeated in their attempts to install Clipper chips, the NSA continued to try to subvert encryption— this time without informing their citizens. Project BULLRUN was one such attempt to fight encryption through a multi-pronged attack. These methods included "covert measures to ensure NSA control over setting of international, encryption standards, the use of supercomputers to break encryption with 'brute force', and – the most closely guarded secret of all – ***collaboration with technology companies and internet service providers themselves***" (James Ball et al.). With Edward Snowden's release of thousands of secret documents over a year, Project BULLRUN first was introduced to the public eye and brought this discussion of privacy versus security into the spotlight again. Your closest friends, your favorite coffee shop, your strange Internet browsing habits— the NSA might have access to all that data, and most people had no idea. How can there be checks and balances to the power the NSA holds if the public doesn't even know about it? What basic rights to privacy are Americans allowed to keep?

After the release of the Snowden documents, tensions between government and the technology companies that develop software were high. These tensions erupted when the FBI demanded that Apple

give them access to an iPhone used by a man who shot 14 people in San Bernardino in December of 2015. The FBI wanted Apple to rewrite the operating system of the iPhone so that it would be easier for them to extract data. When Apple said no, the FBI sued them and paid a third party to crack the phone for them (Kharpal). While the FBI eventually dropped the suit because the third party retrieved the data, this is concerning as well because the third party very well have found a way to get into any iPhone more easily. For now, we don't know because the government won't tell the public or even Apple how the third party retrieved the data. Apple's website still hosts a page of answers to commonly asked questions about this incident where they state, "it would be wrong to intentionally weaken our products with a government-ordered backdoor." While we do not know how rigorously they stick to this principle throughout their products, this is the attitude that is needed to prevent all backdoors, malicious or not. Apple demonstrates an understanding of the ultimate threat of backdoors when they continued, **"**the only way to guarantee that such a powerful tool isn't abused and doesn't fall into the wrong hands is to ***never create it*****"** ("Answers to your questions about Apple and security").

Case Studies:

A backdoor was discovered in server management software produced by NetSarang. This backdoor was discovered because suspicious DNS requests were detected on systems used to process transactions that were running NetSarang software (Mimoso). Ultimately, the source of this malicious behavior was found in the nssockc2.dll code library, a dependency of the application. According to *The Register,* it is generally assumed that "someone managed to hack into NetSarang's operations and silently insert the backdoor," which the discoverers nicknamed Shadowpad, into that dependency (Thomson). This dependency was in use by NetSarang's Xmanager and Xshell software suites. Shadowpad "pings out every eight hours to a command-and-control server with the identity of the compromised computer, its network details, and user names"; it also provides a full backdoor for an attacker to run code and extract

data with (Thomson). While this backdoor has now been patched with an update, there are some lessons that we can extract from this incident.

This situation points to the fact that security can be comprised at any point within the lifecycle of an application. One update to NetSarang's software exposed all users to the malicious group responsible for Shadowpad. The only way to prevent this, since we can't permanently stop cybercrimes, is to foster security as a mentality within academia and company culture. The best prevention is the education of each software developer. We should also try to think like an attacker so that we can defend against them. Since antivirus and update systems require more privileges, cyber attackers would likely find infiltrating this type of software the most rewarding; with more privileges, it is easier for attackers to steal data, install applications, and carry out a variety of malicious actions. This is one chain of thinking that would lead us to conclude that companies that produce antivirus programs and update systems should be particularly vigilant about security.

While it seems like this specific incident does not involve government at all, Kaspersky Lab claims that "the malware bears certain resemblance [to] the PlugX and Winnti attack code used by Chinese hacking groups" (Thomson). While Shadowpad could have been manufactured by a different group and just modeled after other code, there is a chance that the same groups executed this attack. Since a large number of Chinese hackers are thought to be closely linked to the government and operating under their orders as well, we cannot ignore the possibility that this was an attempt at intelligence-gathering by the Chinese government. The scariest part is that we will likely never know who did this.

Doubt and suspicion permeates the topic of backdoors in the technology industry. Kaspersky Lab, the same company that discovered Shadowpad, itself has been accused of having a backdoor in its software, which is mostly comprised of antivirus for home and enterprise users. Believe it or not, Kaspersky has been accused of inserting this backdoor for the use of the Russian government, to which the Moscow-based company is suspected to have strong ties. Accusations mostly stem from the U.S. government's order to wipe any software made by Kaspersky Lab from its systems within 90 days

(Rosenberg). Since this investigation is classified, the government is not providing any evidence of the backdoor, but other companies are following suit and removing Kaspersky software. Moreover, the U.S. Senate voted in late September to ban the federal government from using Kaspersky Lab's products (Volz). Why wouldn't companies follow suit? Who would possibly want to keep Kaspersky Lab's software after the U.S. government's warning and take the chance of exposing their data? Try explaining that choice to your boss, customers, or investors.

While it is disturbing that this allegation, without any accompanying proof released to the public, may very well take down Kaspersky Lab, software sales ultimately depend on reputation. No one can *make* a company or individual buy software that they don't fully trust. A software company's reputation heavily depends on its ability to protect its customers from cyber attackers. A statement from Mr. Kaspersky himself adds a chilling layer of subtlety to this incident: "Even though we have an internal security team and do bug bounties, we can't give 100% guarantee that there are no security issues in our products, name another security software vendor who can!" (Hern). Ultimately, Kaspersky is arguing here that the alleged backdoor was an exploited vulnerability, not something that was intentionally coded into their product. We may never know if this backdoor was placed by Kaspersky Lab or not. We may never know if the Chinese government commissioned someone to insert Shadowpad into NetSarang's software or if it was some lone wolf attacker. The cyber attrition problem adds deep uncertainty to the issue of backdoors, entrenching the online world more deeply into the cycle of fear.

Action Items:

We don't need to give in to despair. While most of these incidents may be difficult to understand for the average U.S. citizen, all software consumers need to be informed. Firstly, we need to know what we're downloading. Whether we Google the file, vet the website it's from, or inspect the file thoroughly, we need to build awareness of what we're clicking so we don't accidentally download a backdoor. This is a risk both at home and at work, where one click's consequences in particular could break a company's

reputation and expose user data. Secondly, it is important to keep up to date on security issues. Someone else may have discovered a vulnerability in software you use, allowing you to ideally uninstall the software before you become the next target. Finally, as software consumers living in a democracy it is our responsibility to call out the government when they take actions that overstep their role in society or violate our privacy. What this means for different people will vary widely, but the most important thing is that we all are engaged in these issues so that we are not caught unaware.

As developers, our role in this fight against backdoors is crucial. Do not add any maintenance backdoors to software unless you absolutely must and can think of no alternative solution. If you do add one, make sure to monitor their use heavily and protect them as much as possible. There is a hard line to walk here because you don't want to be dishonest with consumers and hide this maintenance backdoor, but at the same time, telling the public about a maintenance portal would just increase the number of attackers who try to take advantage of it. The only concrete solution, as Apple described, is to never have created a backdoor at all.

There are plenty of other actions we can take to mitigate the risks of a backdoor being manufactured by an attacker via a vulnerability they discovered in your software. Thoroughly check out any outside sources of code that you use in your projects. When almost anyone can edit open source software, for example, you shouldn't give your trust easily. Do look for vulnerabilities in your own code before pushing it as well. Bug hunting shouldn't only be about looking for and fixing issues in functionality; security is just as important, if not more, long-term. Do expediently look for vulnerabilities in your code that are brought to your attention; don't just let them sit in the backlog. Finally, work to make sure that your encryption is truly end-to-end. Data should not be able to be accessed by a third-party before encryption or after decryption. These are just a handful of actions you can take as a developer to improve the security of your programs.

Conclusion:

With the current state of security, it's easy to become embroiled in the cycle of fear and become overly paranoid or ignore the situation entirely. The only way to break the cycle is to inform ourselves, demand that technology companies raise their security standards, and push the government to behave in a way that meets our expectations. Backdoors are only one part of the larger debate of how privacy and security should be balanced. Instead of electing officials that can't even form a good working relationship with the intelligence agencies, we need officials that will both communicate with them to inform policy decisions but also impose restrictions on them to protect citizens' privacy. Moreover, we need officials that can also interact with technology companies to help improve software security all around. Ultimately, it's our government, our privacy, and our national security so we ought to be playing a part.

Additional Resources:

I have created a demo backdoor-hunting program that I uploaded to the following public GitHub repository: https://github.com/lholde02/backdoor-hunting-demo. The purpose of this demo is to help developers and other security professionals think seriously about what software they have for monitoring their own computers and networks. Backdoors can often be detected by looking for strange open ports, which is a fairly straightforward process. All code is heavily commented to make it easier for readers to follow along.

Works-Cited

"Answers to your questions about Apple and security." *Apple*, https://www.apple.com/customer-letter/answers/. Accessed 5 Dec. 2017.

Ball, James, et al. "Revealed: how US and UK spy agencies defeat internet privacy and security." *The Guardian*, 6 Sept. 2013, https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security. Accessed 5 Dec. 2017.

Hern, Alex. "Kaspersky Lab denies involvement in Russian hack of NSA contractor." *The Guardian*, 6 Oct. 2017, https://www.theguardian.com/technology/2017/oct/06/kaspersky-lab-denies-involvement-russian-hack-nsa-contractor-moscow. Accessed 5 Dec. 2017.

Kharpal, Arjun. "Apple vs FBI: All you need to know." *CNBC*, 29 Mar. 2016, https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html. Accessed 5 Dec. 2017.

Levy, Steven. "Battle of the Clipper Chip." *The New York Times*, 12 June 1994, http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all. Accessed 5 Dec. 2017.

Mimoso, Michael. "Attackers Backdoor Another Software Update Mechanism." *Threatpost*, 15 Aug. 2017, https://threatpost.com/attackers-backdoor-another-software-update-mechanism/127452/. Accessed 5 Dec. 2017.

Rosenberg, Matthew, and Ron Nixon. "Kaspersky Lab Antivirus Software Is Ordered Off U.S. Government Computers." *The New York Times*, 13 Sept. 2017, https://www.nytimes.com/2017/09/13/us/politics/kaspersky-lab-antivirus-federal-government.html. Accessed 5 Dec. 2017.

Thomson, Iain. "Creepy backdoor found in NetSarang server management software." *The Register*, 15 Aug. 2017, https://www.theregister.co.uk/2017/08/15/netsarang_software_backdoor/. Accessed 5 Dec. 2017.

Volz, Dustin. "U.S. Senate votes to ban Kaspersky Lab software from government networks." *Reuters*, 18 Sept. 2017, https://www.reuters.com/article/us-usa-cyber-kasperskylab/u-s-senate-votes-to-ban-kaspersky-lab-software-from-government-networks-idUSKCN1BT2PW. Accessed 5 Dec. 2017.

Zetter, Kim. "Hacker Lexicon: What is a Backdoor?" *Wired*, 11 Dec. 2014, https://www.wired.com/2014/12/hacker-lexicon-backdoor/. Accessed 5 Dec. 2017.