Information Security for the Layperson

Dietrich Lehr

dietrichlehr@gmail.com

East Carolina University

Abstract

I will be covering a multitude of network and personal security measures that can be implemented in order to provide a person or other entity with the means to secure their desired data. I will explain how the practice works and its intended benefit as well as potential limitations that it may impose. Areas of examination will include general network security configuration, network and application security tools, user anonymity tools to keep personally identifiable information private, and some user practices that can reduce exposure or data compromise to unintended parties. The overall intent is to explain measures that can be taken to increase security.

The average user today relies mainly on vendor default security settings or an initial setup wizard in order to secure their devices or profiles. This presents major security vulnerabilities as most devices come configured for convenience rather than security. Allowing users to quickly setup and access their devices allows the layperson quick access but leaves them susceptible to attacks that may have otherwise been easily blocked.

The ideal method to stopping an attack is by blocking it as close to the source as possible. For home users, this begins at the ISP’s (Internet Service Provider’s) demarcation point which is the router for the majority of people. Think of it as the front door to your house. The software that comes on consumer routers provides a startup wizard for users to quickly configure and connect to the internet. The problem with this is that it does not force a user to change the default password, which is consistent across a company's product line most of the time. The United States Computer Emergency Readiness Team (US-CERT) put out alert TA13-174A, Risks of Default Passwords on the Internet, which describes how easily an attacker can obtain factory default credentials through means of product documentation (Alert TA13-175A). Once an attacker accesses a system with privileged credentials, they can modify it or install malware that allows them to intercept and monitor the traffic passing through it.
US-CERT provides recommendations on strong password creation with security tip ST04-02 where they suggest tactics like using passphrases (Security Tip ST04-002).

Home routers are also packed with numerous features, but not all are used. Unused features should be disabled to reduce the exposure to potential threats as attackers cannot attack what isn't there. An example of a vulnerable service on a router was found in the NetUSB bug. The NetUSB driver allows networked devices to access peripheral devices connected to the router's USB port. This can include things like printers or storage devices. The vulnerability allows the attacker to perform a buffer overflow attack to execute code or perform a denial-of-service (DoS) attack (Routers Vulnerable to Attacks). The fix for such a vulnerability is with an update to the NetUSB which was provided by the maker of the driver to the router manufacturers, and then to the customers. This drives home another important aspect of securing a router, which is to apply updates as they come out. Vulnerabilities are found all the time and updates are released as they are found.

Routers come with several encryption options today such as WEP, WPA and WPA2. WEP is no longer considered safe and is recommended to never be used. WEP is vulnerable to several attacks described by Princy Mehta in "Wired Equivalent Privacy Vulnerability". There are several methods one can employ, but the passive attack targets the 24 bit IV based on the knowledge that a key stream will be reused in less than half a day (Alert TA13-175A). There is no real fix for WEP as the system itself is weak. The only true solution is to use an encryption method that has not been broken, such as WPA2.

Another convenient feature we find on today's routers is the Wi-Fi Protected Setup (WPS). This allows users to simply push a button on the router in order to connect a device to the network. While convenient, it has been discovered and put out by the US-CERT in TA12-006A that WPS can be brute-forced using free tools in less than 10 hours (Wired Equivalent Privacy). This would give an attacker the ability to connect to your network and provide them with more attack vectors. The best course of action is to disable WPS and authenticate to the router using the proper credentials, which should include a strong password.

Once your network itself is secure by properly setting up your network's router, you client devices must be secured in order to prevent it from being used to propagate malicious traffic. The US-CERT provides a general guide on how to accomplish this and will be discussed in detail (Alert TA12-006A). One of the easiest methods to increase a computer's security is to segregate user accounts from the administrator, or superuser, account. The premise is that even if the computer is compromised, the malicious payload will not be able to harm the system due to having insufficient permissions to execute harmful payloads.

Unpatched computers are one of the largest security vulnerabilities on a network. Companies routinely provide security patches for their products once it is discovered that they are susceptible to attack. The US-CERT provides a list of 30 high risk vulnerabilities, and in it you can see that most vulnerabilities are things used by the average user (Ten Ways to Improve Comp Sec). This list references numerous Microsoft Security Bulletins that have identified security risk in Excel, Internet Explorer, Word, Java, Adobe Flash, and the Windows operating system itself. MS12-005 describes a Windows 7 x64 bit vulnerability where an attacker can hide a payload in a Microsoft Office file, which when executed, allows the attacker remote control of the system (Microsoft Security Bulletin). It's important to note the importance emphasised in the threat reduction applied by not logging in as an administer by using standard accounts instead. Updating the Operating System (OS) is all that's required to prevent this. The National Institute of Standards and Technology (NIST) put out CVE-2014-1776 which identified a vulnerability with Internet Explorer (IE), which rated as the highest risk possible; a 10 on the (Common Vulnerability Scoring System) CVSS (Vulnerability Summary). This affects IE versions 6 through 11 through the use of an attacker crafting a webpage and a user accessing it. Again, this attack allows remote access but limits the access to those of the user currently logged in. An update is the solution.

Cloud applications and storage solutions are becoming increasingly popular for the average computer user. It is important to understand some of the risk involved as well as the benefits.They allow the transfer or liability to a 3rd party to host and secure your information. There are trade-offs to this, such as the risking the loss of confidentiality if the 3rd party's data centers are breached.

Ease of data access is very appealing, especially for individuals who may travel and like to travel light. Data is accessible anywhere with an internet connection. It is important to keep in mind that when you are not at home, you are on someone else's' network. Cloud providers typically provide the ability to securely access and transfer your data through Transport Layer Security (TLS) which can be indicated by the “https” portion of a web address. Request for Comments 2818 (RFC2818), describes the methods used in order for TLS to secure your data. A session is opened between your browser and the server hosting your data and a handshake processes happens, in which keys are exchange and the session secured (RFC 2818). This can help prevent man-in-the-middle attacks where the attacker is able to sniff traffic and see what is moving across the network using freely available tools, such as Wireshark. It is important to note though, that even things such as TLS must be kept up to date in order to prevent exploitation. One of the most infamous vulnerabilities in TLS was exploited by the vulnerability Heartbleed. The vulnerability is due to the mishandling of heartbeat packets which can allow an attacker to trigger a buffer over-read and read the private session keys that you exchanged with the server to securely transfer your data (Common Vulnerabilities and Exposures) . This really stresses the importance of not only keeping your personal computer up to date with the latest security patches, but for cloud providers to do the same.

Another surfacing threat to data protection is called ransomware. This attack happens when a user unknowingly downloads a program that then encrypts their data, using a key that they do not know. This locks the user out, and a pop-up then demands payment to restore access. This is known as CryptoLocker. The encryption method used to encrypt a user’s data is AES, which uses an algorithm that has not yet been broken (Ransomware). The easiest way to combat this is by backing up data through multiple mediums such as a cloud provider and on your local machine or external drive. There is no guarantee that if you pay the ransom that you will get your data back, so the best course of action is to prevent this from happening in the first place by being aware of what you click and also through the use of a firewall to block threats in real-time.

Some operating systems come with a software firewall by default. If it doesn’t, you should immediately download and install one. Av-comparatives.org provides comprehensive reports where you can view the real-world effectiveness of antivirus programs. Kaspersky is typically among the highest rated, blocking nearly all threats while producing next to zero false-positives (File Detection Test). The antivirus provides security by scanning each file that you open in order to provide real-time security. The scans are based on virus definitions that are frequently updated by the antivirus company in order to keep systems secure. Companies like Symantec provide an active list of threats, risk, and vulnerabilities along with severity levels (Security Response) . One of the most frequent items that show up on list is spyware. Spyware secretly installs itself on the host system and sends personal information to attackers. A current example is the TSPY spyware that is hidden in a downloadable file and installed unknown to the user. It then logs user’s passwords and sends them to the attacker which allows them to access anything from email to bank accounts. The results could be devastating and the only fix is a series of registry edits to regain control of your system. Data theft isn’t the only risk of not running updated antivirus software. Another predominant threat is the recruitment of bots for botnets. Botnets are collections of computers remotely controlled by attackers, usually in the form of distributed denial of service (DDoS) attacks. Malicious payloads are hidden in files downloaded from the internet which enslaved computers to become members of botnets. One a member, the attacker can collectively command the slave devices to perform attacks on the host they specify. One of the largest botnets to date is the Simda botnet which has compromised over 770,000 machines across the world (Security Response). Unpatched computers are the primary target of this malware and contributed to a growing problem with DDoS attacks. The GameOver Zeus botnet is a much larger botnet which is said to have over 3.6 million devices in it (Collaborative Effort). The purpose of this botnet is less about DDoS and more about monetary theft. It is propagated via email and has been the cause of millions of dollars in theft. The command structure of this network is decentralized and spread through a peer to peer network and one quarter of the infected computers in this botnet are located in the United States.

With this information, the average computer user will have a better understanding of security vulnerabilities active in the world and how to mitigate them. Networks should be set up in the most secure means possible so that they can be trusted. Users should routinely update their systems as well as perform regular backups. The implementation of least privilege should be used to mitigate the impact of successful attacks as well as antivirus programs to add to the defense in depth.

References

Alert (TA13-175A). (n.d.). Retrieved November 18, 2015, from https://www.us-cert.gov/ncas/alerts/TA13-175A

Security Tip (ST04-002). (n.d.). Retrieved November 18, 2015, from https://www.us-cert.gov/ncas/tips/ST04-002

Millions of Routers Vulnerable to Attacks Due to NetUSB Bug | SecurityWeek.Com. (n.d.). Retrieved November 18, 2015, from http://www.securityweek.com/millions-routers-vulnerable-attacks-due-netusb-bug

Alert (TA13-175A). (n.d.). Retrieved November 18, 2015, from https://www.us-cert.gov/ncas/alerts/TA13-175A

Wired Equivalent Privacy Vulnerability(n.d.). Retrieved November 18, 2015, from https://www.giac.org/paper/gsec/624/wired-equivalent-privacy-vulnerability/101399

Alert (TA12-006A). (n.d.). Retrieved November 18, 2015, from https://www.us-cert.gov/ncas/alerts/TA12-006A

Ten Ways to Improve New Computer Security. (n.d.). Retrieved November 18, 2015, from https://www.us-cert.gov/sites/default/files/publications/TenWaystoImproveNewComputerSecurity.pdf

Alert (TA15-119A). (n.d.). Retrieved November 18, 2015, from https://www.us-cert.gov/ncas/alerts/TA15-119A

Microsoft Security Bulletin MS12-005 - Important. (n.d.). Retrieved November 18, 2015, from https://technet.microsoft.com/library/security/ms12-005

Vulnerability Summary for CVE-2014-1776. (n.d.). Retrieved November 18, 2015, from https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-1776

RFC 2818 - HTTP Over TLS. (n.d.). Retrieved November 18, 2015, from https://tools.ietf.org/html/rfc2818

Common Vulnerabilities and Exposures. (n.d.). Retrieved November 18, 2015, from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

Ransomware. (n.d.). Retrieved November 18, 2015, from https://www.trendmicro.com/vinfo/us/security/definition/Ransomware

File Detection Test - AV-Comparatives. (n.d.). Retrieved November 18, 2015, from http://www.av-comparatives.org/detection-test/

Security Response. (n.d.). Retrieved November 18, 2015, from https://www.symantec.com/security_response/landing/vulnerabilities.jsp

TSPY_ROVNIX.YPOB. (n.d.). Retrieved November 18, 2015, from https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/tspy_rovnix.ypob

Alert (TA15-105A). (n.d.). Retrieved November 18, 2015, from https://www.us-cert.gov/ncas/alerts/TA15-105A

Collaborative Effort Among International Partners. (2014, June 2). Retrieved November 18, 2015, from https://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted