Safeguarding Personal Health Information: Case Study

1

Holly Gandarilla

Abstract

Password cracking tools have given hackers the ability to solve hashes in minutes. These same tools can also be used for penetration testing to determine weak passwords within our own infrastructure. In using products, such as, Cain and Abel or Ophcrack, organizations can gain insight and awareness that could be the stronghold in keeping accounts and personal health information (PHI) safe. Cain and Abel, and Ophcrack, which are the two password cracking tools tested, can be both useful and very dangerous at the same time. While many can learn from these products, so can their adversaries. In using these products to test our own password strengths we can foresee vulnerabilities that we may have been overlooked. As new software is created, passwords will become easier to crack. Technology knows no boundaries in many aspects, which is why securing our networks, strengthening our physical and logical security, and mitigating every risk possible, becomes of utmost importance in this technology-ridden world.

Keywords

PHI · Personal health information · Password · Cracking · Penetration · Safeguard · Hackers · Study

1.1 Introduction

Technology is ever-advancing and constantly creating new avenues for vulnerabilities in our information systems to be exploited. Midyear 2016, 60% of data breaches were attributed to hacking [1]. An organization's duty to protect their patients' PHI should remain top priority. With a more comprehensive security posture, organizations can barricade these vicious avenues from negatively impacting their patients.

The CIA triad refers to the confidentiality, integrity, and availability of information—in our case, PHI. The confidentiality of information is protected by a system's access controls. Those who require access to the system are granted it, and those who do not are denied. The confidentiality of information is pertinent because it ensures that patient and employee information have not been compromised. The integrity of information is backed by encryption procedures. Per HIPAA Security Rule, medical facilities should be encrypting PHI when deemed appropriate [2]. For many, this means when it is static, or stored in file systems, and while in transmission. While these HIPAA guidelines are addressable, organizations should stress this to employees who handle PHI frequently and implement organizational policies identifying proper procedures. The availability of PHI is maintained by Disaster Recovery and Business Continuity Plans [3]. By making this information constantly available the CIA triad is being enforced.

1.2 Proposed Work

In order to effectively control unauthorized access, the identities of individuals should be validated. It is not enough to impose partial security standards. Multiple methods should be in place to protect the failure of any one of them. For example, if password requirements are that the key must be 14 characters in length, include upper and lowercase letters, and numbers—that's a great first step. Given enough time, passwords could still be compromised via password cracking tools. However, if an account lockout policy were in place after three incorrect attempts, the chances of a brute force attack could be mitigated.

H. Gandarilla (✉)
Department of Cybersecurity, University of Maryland University College, Adelphi, MD, USA

S. Latifi (ed.), *Information Technology – New Generations*, Advances in Intelligent Systems and Computing 738,
https://doi.org/10.1007/978-3-319-77028-4_1

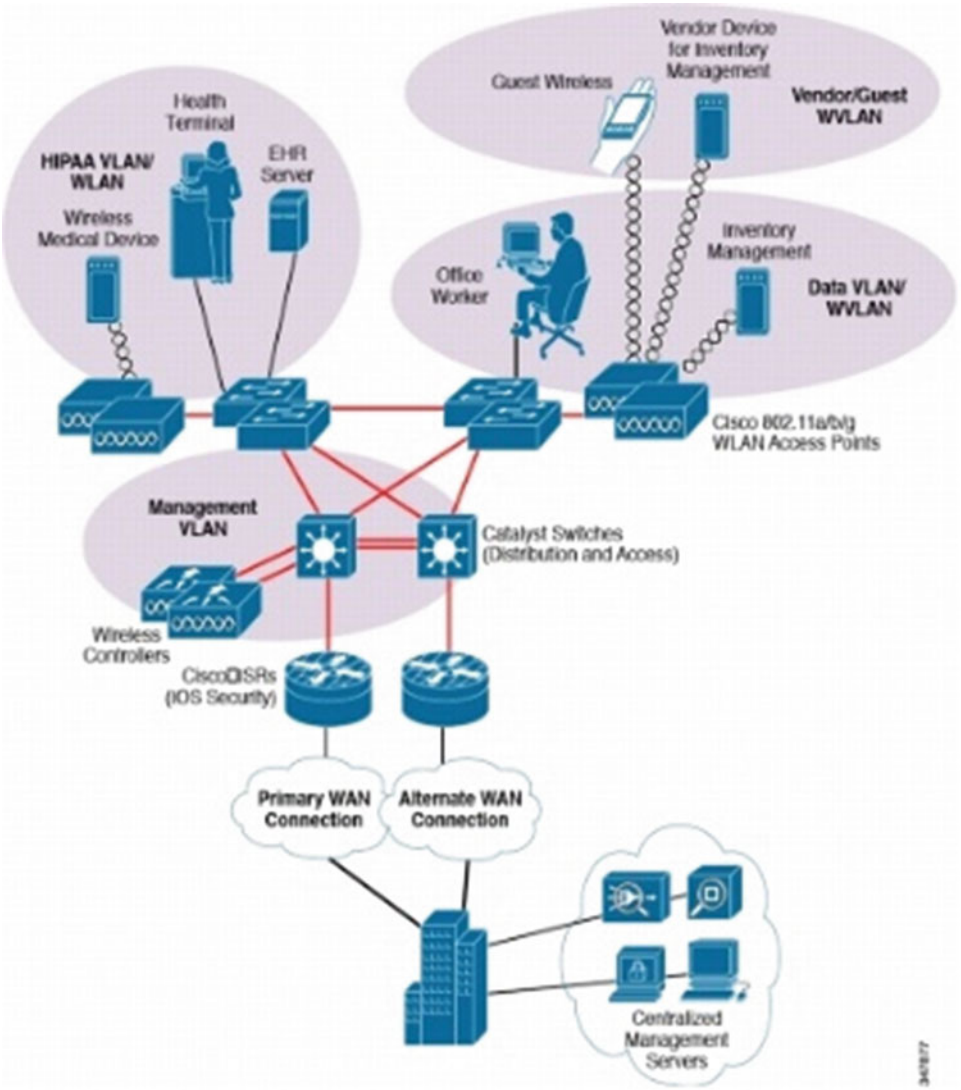

Fig. 1.1 Cisco's recommended network topology for medium-sized clinics

The issuance of identification badges that dual as common access cards (CACs) are perfect examples of authentication. Two-factor authentication is a method of authentication that requires two of the following: something you have, something you know, or something you are (i.e. biometrics). The combination of CAC and password mitigates the risk of losing a badge and systems automatically being compromised. A CAC alone would not be enough to breach the system.

Authorization is the method of permittance to a system. Often times, authentication and authorization are seen as one entity. Authorization is the process in which users are granted or denied access based on their permissions. Controlling access to systems assists in solidifying one's security posture as a whole. Organizations that are partially enforcing these measures should implement multiple methods. Thus, the failure of just one method does not permit access.

Access control lists (ACLs) determine who is authorized access to a network. As opportunity arises through open ports, even settings, such as, access lists can protect against unauthorized traffic. With the settings deny and allow, administrators can dictate who is granted access. Additionally, unused ports should always be turned off to prevent intruders from gaining access to the network (Fig. 1.1).

Role-based access controls (RBAC) are set based upon the role or position an employee holds. If they are a nurse or a doctor, they have access based on what their position requires access to. For example, nurses should be permitted access to levels of PHI that are relevant to the care that they give. In turn, doctors are authorized greater access to view entire records, so that they may better diagnose health issues.

With the influx of mobile platforms, hospitals have become more productive as they can work on the go. However, with easier access for users comes easier access for intruders. Mobile devices are more difficult to secure as they have weaker protocols without being hard wired, not to mention, that wireless access is never as secure as a wired connection.

Nonetheless, mobile devices and their connectivity has become essential to the welfare of patients. This means strong passwords, CAC readers connected via USB or built-in, and implementing protection displays and locks. In 2016, 78% of data breaches in U.S. hospitals were due to the loss or theft of information [1]. These devices, although they are made to be portable, should have emergency procedures in place in the event of loss or theft. Remote wipe should certainly be considered an option. Encrypting PHI is the most secure method in providing confidentiality to this information [4].

The importance of having strong password requirements is paramount. Passwords that are alpha-numeric and short, or contain words from the dictionary are easily guessed and cracked using password cracking tools. Tools, such as, Ophcrack, and Cain and Abel are specifically designed to figure out passwords in as little time as possible. Even more concerning, the word lists that are used to perform dictionary attacks are a dime a dozen.

1.3 Findings and Results

Cain and Abel, and Ophcrack, two password cracking tools tested in this case study, can be both useful and very dangerous at the same time. While organizations can learn from these products, so can our adversaries. In using these products to test internal account password strengths, organizations can foresee vulnerabilities that perhaps may have been overlooked.

Dictionary attacks can be debilitating for users who use full words in their passwords. Word lists can be uploaded to password cracking programs, making it almost effortless to solve hashes. Ensuring that password policies do not allow for words that can be found in the dictionary, this threat can be mitigated. While it may be difficult to remember complex passwords, users can also spell out words using various characters. For example, the password floridagators could be turned into a more secure one by substituting characters that look similar; Fl0R!d@G@t0R5. It does take some extra steps to make a password secure, but if this is what an organization requires to keep PHI safe, users will become more skilled in creating stronger passwords.

"A brute-force attack is a method of defeating a cryptographic scheme by trying a large number of possibilities" [4]. In simpler terms, brute force attacks occur when multiple password entries are sent to overload a system. Sometimes a correct password is guessed, or sometimes a system becomes overloaded. In both scenarios, neither one is particularly good. Limiting the amount of times an incorrect password can be entered before the account locks is one way to keep these types of attacks from debilitating our systems. The most common is the number three—after three incorrect attempts, an account should lock, and administrators can now control access to the user's account. In many cases users are required to verify their identity either in person, via video teleconferencing, or by giving identifying information about themselves. Organizational policies should provide more than one way of validating an individual's identity and should be approved by the Chief Security Officer.

The speed in which these programs cracked passwords was impressive. For simpler passwords, such as xmen and M00n, both programs almost immediately solved the hashes. Ophcrack was easier and faster to use, but only performs by using Rainbow tables. Whereas, Cain and Abel can use a variety of attacks. Cain and Abel was precise in solving hashes when the correct attack was chosen. Being that not all passwords include dictionary words in them, a dictionary attack can certainly be unsuccessful. The good news—Cain and Abel attacks in more than one way. Rainbow tables are easily found for use in Ophcrack and make it easier to solve multiple account passwords in one function. However, for passwords that the hash is unknown, Ophcrack will not be able to find it on its own.

Password strength was the most determining factor for cracking account passwords. The longer the password, the more time consuming it becomes. Likewise, the more difficult a password is by including not just letters and numbers, but also symbols, can be the saving grace or end all in these situations. Requiring passwords to be at least 14 characters in length, with two uppercase letters, two lowercase letters, two numbers and two symbols makes solving them more difficult and time consuming for hackers.

Both programs were successful in solving for simple hashes, dictionary words and short passwords. Essentially, if the password was weak, these programs could crack them in under a minute. While both programs differ in ability, they both can be useful to our organization.

1.4 Conclusions

Both programs were successful in solving for simple hashes, dictionary words, and short passwords. Essentially, if the password was weak, these programs could crack them in under a minute. While both programs differ in ability, they both can be useful to an organization. It is my recommendation that both programs be used for penetration testing. Because they are open source products, this comes at no cost to organizations, but with a plethora of benefits. In using these programs, they will be flagged as malware. The simple solution would be to advise the IT department to download the programs and leave their testing lab equipment offline when not in use. During penetration testing, these machines can be connected to the network to perform their duties,

scanning for weak security and then once again disconnected so that they are not constantly flagged on the network. Deploying both tools on networks for penetration testing will significantly decrease the ability of intruders to hack networks effortlessly. In keeping machines that house these tools offline until weekly testing is done, the chances of false positives in anti-virus software can be mitigated. The ability to know what hackers can do and where the faults lie, will strengthen security posture to the best of our ability. Most importantly, this will show patients that we care about their personal information and we will continue to keep it secure.

References

1. Major 2016 healthcare data breaches: mid year summary. HIPAA J. (2017), [Online]. http://www.hipaajournal.com/major-2016-healthcare-data-breaches-mid-year-summary-3499/
2. R.A. Leo, *The HIPAA Program Reference Handbook* (CRC Press, Boca Raton, FL, 2005)
3. M. Korolov, Healthcare organizations face unique security challenges. CSO Online, (2015), [Online]. https://www.csoonline.com/article/2932978/data-protection/health-care-organization-face-unique-security-challenges.html
4. N. Daras (ed.), *Applications of Mathematics and Informatics in Military Science* (Springer, Berlin, 2014), p. 208