J Digit Imaging (2017) 30:117–125
DOI 10.1007/s10278-016-9913-x

Cyber-Security Issues in Healthcare Information Technology

Steve G. Langer[1]

Published online: 11 October 2016
© Society for Imaging Informatics in Medicine 2016

Abstract In 1999–2003, SIIM (then SCAR) sponsored the creation of several special topic Primers, one of which was concerned with computer security. About the same time, a multi-society collaboration authored an ACR Guideline with a similar plot; the latter has recently been updated. The motivation for these efforts was the launch of Health Information Portability and Accountability Act (HIPAA). That legislation directed care providers to enable the portability of patient medical records across *authorized* medical centers, while simultaneously protecting patient confidentiality among *unauthorized* agents. These policy requirements resulted in the creation of numerous technical solutions which the above documents described. While the mathematical concepts and algorithms in those papers are as valid today as they were then, recent increases in the complexity of computer criminal applications (and defensive countermeasures) and the pervasiveness of Internet connected devices have raised the bar. This work examines how a medical center can adapt to these evolving threats.

Keywords Computers security · Computers in medicine · Computer communication networks

Introduction

In 1999–2003, SIIM (then SCAR) sponsored the creation of several special topic Primers, one of which was concerned with computer security [1]. About the same time, a multi-society collaboration authored an ACR Guideline with a similar plot [2]. The latter has recently been updated [3]. The motivation for these efforts was the launch of Health Information Portability and Accountability Act (HIPAA) [4]. That legislation directed care providers to enable the portability of patient medical records across *authorized* medical centers, while simultaneously protecting patient confidentiality among *unauthorized* agents. A concomitant requirement was that data availability and veracity had to be assured. These policy requirements resulted in the creation of numerous technical solutions which the above documents described. While the mathematical concepts and algorithms in those papers are as valid today as they were then, recent increases in the complexity of computer criminal applications (and defensive countermeasures) and the pervasiveness of Internet connected devices have raised the bar. This was made clear at the recent SIIM annual meeting in Portland OR where several speakers regaled the audience with tales of possessed car auto-pilots and homicidal infusion pumps [5, 6]. Unfortunately, faced with such a complex topic, the typical medical center management response in employee training stresses complex passwords (changed quarterly) and being careful about what emails they open. This has led leaders in the field to define "security theater" [7].

To understand the complexity of the issues requires a structured treatment. Towards that end (and with a nod to Mr. Schneier), this paper treats cyber-security as dramatic play with actors, their motivations, and plot arcs. Thus, the following sections can be considered as the parts of a screenplay.

(a) The human cast of characters involved in the cyber-security drama—and their motivations
(b) The props used by those actors, noting that some can be used by different groups for diametrically opposed purposes

✉ Steve G. Langer
langer.steve@mayo.edu

[1] Mayo Clinic, Rochester, MN, USA

(c) Illustrate the above cast and props with a couple of real-world scenarios
(d) Conclude with some recommendations

Finally, the gritty details about some of the tools are relegated to Appendix A. In addition, capitalized terms that are not defined in the text body are defined in a Glossary

The Cast

Computer security, and more generally all Internet connected devices (cars, refrigerators, home heating and air conditioning, phones, etc.), is subject to competing interests—both innocent and otherwise. It helps to enumerate the various actors in the drama:

(a) Black hats: Are human agents that seek to gain control over other persons computers or devices for nefarious purposes
(b) White hats: Are human agents who seek to thwart Black Hats. They may be employees in your organization, contractors, or if at home—you.
(c) Users: The average person who is just trying to do their job at work or relax on their home computer (and/or other Internet connected devices) using the available software. They are not seeking to write new applications or subvert other person's devices.
(d) Developers: The authors of the software used by all the above.
(e) Service Providers: Your employer, the companies that host cloud services, or the broadband providers that we all use to reach the Internet.

Now, as intimated above, each of these actors has one or more motivations. It is helpful to consider them in more detail.

… and their Motivations

Black Hats

Black Hats come in three main types. The Thief wants to steal data, be it intellectual property, passwords, or credit cards. The Vandal seeks havoc and destruction—often via something called a Denial of Service Attack that stops a service from functioning or a defacement attack that alters the appearance of a company website [8]. The Soldier/Assassin goes the Vandal one step better and seeks to cause death/damage via attacks on critical infrastructure, by either disabling it or altering intended behavior (think remotely opening the flood gates on a large dam). It is important to realize that the same prop (i.e., a computer virus) can be used singly (or in combination with other props) to satisfy any or several of the above-mentioned motivations.

A basic principle in successfully mitigating risk is to make sure the risks are worth the prize [9]. In symbolic terms, we have

```
if ( difficulty + risk < reward) then
        attack                                  (1)
else
        don't_attack
```

"Difficulty" here means how much time, money, and effort the Black Hat will have to invest to conduct the attack. "Risk" means how likely it is that the Black Hat will be discovered—by law enforcement, other criminals, or the victim. "Reward" can be many things depending on the Black Hat's objective: money, revenge, trade secrets, terrorism, etc. Predators that often ignore Eq. 1 either end up in jail or are removed from the gene pool. Equation 1 is also important because it helps a White Hat think about how to make a given computer less attractive to Black Hats; devalue the reward of the target or make it difficult and risky enough to persuade the Black Hat to move elsewhere.

It is helpful to organize the types of attacks used by Black Hats. Some are related to the "difficulty" term of Eq. 1, others are related to the "risk" term of Eq. 1. They can basically be summed up in the following groups [10, 11].

Cryptographic Attacks The purpose of this class of attack is to reveal the content of a victim's encrypted transactions: either messages sent over the wire, files at rest on a server, or User passwords via a password cracker (i.e., LophtCrack L0pht Holdings, LLC Burlington MA). Alternately, the crypto-attacker may seek to encrypt the User's unencrypted files, thereby rendering them inaccessible to the User—the so-called *ransom-ware* attack [12, 13].

Cybercrime Broadly is the term for all crimes committed on computers, but it also includes a more specific item not addressed elsewhere. That is, as a term for methods used to remove any trace that crime has been committed—the realm of anti criminal forensic-software (i.e., BCWipe, Jetico Inc, Espoo Finland).

Denial-of-Service Attacks The goal of the DOS is to stop or hobble access to services or data on the target machine(s). Depending on the severity, this class of attack can be the domain of either the Vandal (who seeks to embarrass a victim) or the Soldier/Assassin if the service denied is critical to life support. *Ransom-ware* is an example of a DOS attack that uses cryptographic methods to deny access to data.

Injection Exploits Use intentionally bad data or code input into a service that subverts the intended operation of the system. Usually, these exploits target vulnerabilities resulting from insufficient data validation on input; they are most often used against web servers and databases [14]. This is often due to Developers creating software that does not validate and effectively deal with rogue inputs.

Malware Simply, any software that is installed without the User's informed consent that alters the normal behavior of the computer in a way that the User would not allow if they knew (think Trojan Horse programs that capture keystrokes, credit cards, etc.). While the Denial-of-Service attack seeks to actually stop access to a service or data, the objective of much Malware is to *take over* a service for either immediate reward or as an intermediate step towards a larger goal (like privilege escalation). Users often infect themselves unknowingly via opening bad emails are visiting bad web sites.

Privilege Escalation As hinted above, the goal here is to elevate a normal User account on a system to one with administrative rights—usually as a precursor to installing Malware that a modern operating system would prevent a normal User account from doing.

Web Security Exploits Often when a User points their web browser at a web site, a lot more is going on then the User is aware of. The web server can learn a great deal about the User's computer by exploiting browser weaknesses, and if scripting is enabled on the browser, the Black Hat can even execute arbitrary software on the User's computer [15].

White Hats

The aforementioned SCAR Primer and ACR documents extolled at length the goals and motivations of the White Hat and Providers. The bias for those actors in all these documents was due primarily to the HIPAA concerns surrounding the duties and responsibilities of medical center staff. To the authors' credit, the content of all those works was very similar and not surprisingly sought to negate the Black Hat's goals. The high-level goals are as follows:

(a) Audits

  a. Of devices (what is running what service, and where)
  b. Of Users (who touched what patient record, when, and did what)
  c. Of policies and procedures (including downtime plans)
  d. Of network traffic

(b) Authentication

  a. Is the User who they claim to be?
  b. Non-repudiation (is there a strict chain of evidence to make claiming "I didn't do it" an unsustainable claim?)

(c) Authorization (is the User approved to access this service or data?)

(d) Data privacy

  a. If data contains PHI, is it transferred and stored as an encrypted payload?
  b. If possible, PHI should be de-identified (i.e. for research)

(e) Reliability and performance (are services/data available when needed)

(f) Data reliability

  a. Integrity (has data been altered in nefarious ways)
  b. Recoverable in event of failures

It is worth noting that while White Hats do several things mainly to thwart Black Hats (i.e., authentication, authorization, encrypting PHI), they are also tasked with broader concerns. For example, server downtime is not always caused by DOS Black Hats; they may also be caused by hardware failure, software upgrades gone awry, or acts of God. Similarly, data can be lost if steps are not taken to prevent it. This broader mission is often overlooked by White Hat IT professionals whose only motivation is information security; often a point of contention in a medical center.

Further, it is interesting to note that similar props can be used by both Black and White Hats for opposing goals; the Black Hat may use some decryption tools to alter data and then re-encrypt it to fool Users, but the White Hat could detect such alterations with another encryption tool (a digitally signed message digest—described in the Appendix).

Users

Put simply, the user just wants things to work. If they can do their job, go home on time, and watch Netflix on their tablet without any hiccups—that is a good day (Netflix Inc, Los Gatos CA). Multi-factor authentication is a nuisance to them. And yet, a large part of the exploits that are launched into our medical centers are enabled by Users just doing what they do: visiting web sites and opening inviting emails.

Developers

This group of characters is fairly nuanced. Depending on the applications they are developing, they can be thought of as Black or White Hats (if they are developing the kinds of props described below) or more like Users if they are developing the next word processor. This distinction is important. A

Developer who identifies with one or the other color of Hat is acutely aware of programming practices that lead to security issues (aka exploits). The User application Developer may be completely ignorant of basic secure coding programming practices (e.g., what a buffer overrun is and why it should be avoided) [16].

Providers

As customers of the Providers, most Users rarely have direct contact with the Developers or White Hats. Rather, we have chats with the faceless "Help Desk" and the public face(s) of the corporation represented by the C-suite (CEO, CFO, etc.). These are the dramatic leads of the play, and as in any good drama, they bear the nail-biting responsibility to answer to the shareholders/customers if the services go offline or a database breach has exposed a million patient histories to Black Hat identity thieves. Too much security enrages Users with slowness and causes customers to go elsewhere. Too little, and the medical center ends up as front page news [17].

Props for the Play

This is where the plot thickens. It is difficult to defend against attacks one has never seen, the mantra "know thine enemy" is particularly relevant to cyber security; without knowing Black Hat methods, one cannot take effective countermeasures. This leads to the question, "What are we doing today?" Most medical centers have a policy about having complex and routinely changed passwords; but are they effective? Many of us have heard of "rooting" or "jailbreaking" a smartphone to gain administrative access and install software the cellular Providers never intended [18]. Those rooting exploits never need a password to function, yet they gain administrative access. In addition, most hospitals have a firewall which prevents the agents on the Internet from connecting to devices within the hospital firewall. But, does that mean the only way medical center devices can be attacked is for a Black Hat to walk in the door, plug into a network connection, and try to guess thousands of account passwords? No. Certainly some of that occurs, but the vast majority of medical centers are penetrated by Trojan Horses that the employees themselves brought inside the fortress—and the Black Hat never needs a password for this to happen. How? By Users naively opening outside emails and visiting compromised web sites.

To build an effective defense, it is useful to see the statistics on penetration methods the Black Hats are actually using. The Computer Emergency Response Team (CERT) at Carnegie Mellon University ranks the Top 30 exploits by frequency. Table 1 summarizes these data for May 2015 [19]. It is also interesting to note in Table 1 that none of the listed exploits rely on cracking passwords, and 15 of the 30 are browser related.

The Remote Black Hat Penetration Process

Consider the following steps a Black Hat would take to attack a large, firewalled corporate target (medical center, bank, etc.) remotely. In general, the process is as follows:

1. Establish a presence on the target's network. We assume a firewall exists, so an external Black Hat achieves this by a User visiting a compromised web site (and downloading a Trojan Horse) or opening an email that installs the "beachhead" agent on the User's device.
2. Black Hat then begins an inventory scan of the corporate network; identifying the devices and what they do. High value targets are as follows: the User account credential store (think Microsoft domain controllers), the Electronic Medical Record servers, treatment devices, and the Billing systems. This information can be inferred from a network scanning tool [20].
3. Once high value targets have been identified, Black Hat scans the identified services for vulnerabilities (e.g., Nessus, Tenable Network Security Inc., Columbia MD). Also, it begins monitoring the network traffic to them.
4. Exploit the vulnerabilities seen in 3 and either

   a. Begin harvesting data (the Thief)
   b. Cripple them (the Vandal)
   c. Exploit them and alter their behavior (the Soldier/Assassin). All the above missions are accomplished using a suite of penetration tools (e.g., Metasploit Framework, Rapid7, Boston MA).

Table 1 Carnegie Mellon's Computer Emergency Response Team track the most often reported computer exploits. The top 30 in May 2015 are given in this table broken out by: vendor, total exploits related to that vendor, and then application category

	Total exploits	Browser	Browser-based applications	Database	Misc office applications	Operating system, language
Microsoft	16	7	1	1	6	1
Oracle	2					2
Adobe	11		6		5	
OpenSSL	1	1				

White Hat Countermeasures

For each step above, we listed potential props (tools) that the Black Hat could use to "penetrate" the target. Below, we list props the White Hat could use to thwart it.

A. First, it is critical to deny Black Hat a beachhead on any network with PHI. Several methods can be used for this.

   (a) The simplest, and likely unpopular method with Users, is firewall outbound web access to only white listed sites that are known to be free of Web Security Exploits; there are appliances with annual subscriptions that can achieve this (e.g., Barracuda Web Security Gateway, Barracuda Networks Inc., Campbell CA).
   (b) Similarly limit incoming email to white listed sources (e.g., Barracuda Essentials for Email Security, Barracuda Networks Inc., Campbell CA).
   (c) To avoid a User revolt the above may cause, a site could segregate the PHI devices to a network segment that is not directly accessible to any computer that can reach the Internet. Then Users on the Internet side could browse and email with less restraint, but be unable to pass an agent onto the PHI network.
   (d) Restrict what devices can connect to the cooperate network to only those known to the network itself (Cisco Identity Services Engine, Cisco Systems Inc., San Jose CA). While this is a laudable goal, the agent installed in Black Hat Penetration Step 1 is on an already approved User computer. Thus …
   (e) White Hats must implement policy controls on computers that do not allow a User account access to the privilege escalation required to install applications.

B. White Hat should also have an accurate inventory of approved devices, so new devices can be detected and investigated [20]. White Hat can detect Black Hat scans with network surveillance, intrusion prevention, and detection tools (e.g., FireEye Inc., Milpitas CA).

C. White Hats should also perform vulnerability scans on their own equipment and strive to mitigate them (Nessus *op cit*, Rapid7 *op cit*).

D. Detect compromised systems via deviations from known reference baselines (e.g., Tripwire File Integrity Monitoring, Tripwire Inc., Portland OR).

Scenarios

In "Remote Black Hat Penetration Process," we outlined the potential steps used by Black Hats to compromise systems. Note that we did not mention a password cracker to get a User's account credentials. Depending on how vulnerable the User's computer is, it may be possible for the Black Hat agent to install itself using just the User accounts rights (which it inherits) if it was pulled down from a Web Security Exploit-infected web site. This is worth mentioning because if that agent can run vulnerability scans on other systems—the Black Hat can exploit site assets without ever knowing any User credentials!! This dramatically lowers the "difficulty" term in Eq. 1 because decryption of strong passwords is a very computationally intense exercise. If it can be avoided, it radically increases the likelihood that the Black Hat will choose to attack a target.

Screenplay 1

User Downloads a file conversion program to turn Word documents into PDFs from a compromised web site. Unknown to them the converter program is a Trojan Horse containing Malware that installs a beachhead on their computer [21]. The Malware now has the credentials and rights of the User account.

Black Hat Agent installed itself and reports "home." Black Hat instructs agent to replicate by sending fake email to all User's Outlook Contacts

User2-N: Open the email and spread agent

Black Hat Instructs agent to Monitor the site's network and send reports to home. Black Hat finds critical business documents and attempts to encrypt them with the privileges of all the User accounts it has compromised.

Providers Realizing several thousand documents are inaccessible, they are hopelessly lost and pay the ransom via BitCoin. Clinical care was impacted for a week. The IT leadership is fired.

Screenplay 2

As above, but when Provider realizes the problem …

White Hats

Kill the site's Internet access and start rebuilding all PC's and file servers from write once media (like CD-ROMs). Once rebuilt, off-site encrypted backups are restored onto the file servers, and the new workstation policy disables normal Users from having the administration rights to install programs.

Providers Public relations nightmare, cost in millions, lost 2 business days; final scene White Hat going to board room sweating

Screenplay 3

White Hat Workstation policies prevent normal User's from installing software. User still downloads the program, but cannot install it. Threat averted.

Epilogue No angst, no explosions. No one comes to see the movie based on screenplay 3

Admittedly, the above screenplays are somewhat contrived. They were constructed to illustrate the threat/countermeasure steps as the White Hat learned more about the Black Hat methods. In reality, the Black Hats also adapts and the exploit used in later attacks would likely not require the User to have local administration rights to install software. Rather, weaknesses in the Browser itself could be used to run the Malware (often scripting engines and media players). The agent would run in the browser, survey the local machine for vulnerable services, and exploit them to form the beachhead.

Discussion and Recommendations

As has already been said, much of employee training regarding cyber-security revolves around complex passwords that are regularly changed. That is of some value, but brute force password cracking is slow and computationally expensive. Dictionaries of commons password hashes (called Rainbow tables) can accelerate this a bit, but it is still a difficult process [22]. It is much easier to trick Users into opening infected emails (aka *phishing*) or visiting compromised web sites and having them download Trojan Horses which in turn bootstrap up more sophisticated Malware.

Given that any corporation has thousands of devices to defend, one has to adopt some triage algorithm to assign risk and assign surveillance resources accordingly. A useful model to facilitate this was described in [2 op cit]. Table 2 recreates the concept here with suggested categorizations. Clearly, a double HIGH item (RIS or EMR) merits greater attention then a double LOW (a data-mining system with only de-identified data). The National Institute for Standards and Technology has a similar multi-parameter view of risk assessment [23].

Table 2 A two parameter matrix to assign risk to various components in the medical center; in this case the two parameters are Protected Health Information (PHI) and criticality of the system to the business. In this model a HIGH/HIGH is seen as a high-value target to Black Hats, whether their motivation is to steal patient data or cripple the business

	System mission criticality	
PHI risk	High	Low
High	RIS, EMR	Scanner
Low	Modality Worklist server	Research systems

The following steps can harden systems from the vast majority of even experienced Black Hats:

A. Install network firewalls, segregate PHI networks from ones that can reach the Internet directly, and implement network auditing (to detect if the PHI network is reaching the Internet).
B. Set policies on computers that prevent ordinary Users from being able to install software.
C. Remove unneeded services from all servers; wrap remaining services to both restrict traffic and log traffic (incoming and outgoing).
D. Write system logs to "append only" media that cannot be wiped by Black Hats
E. Perform regular checksums of all critical server files, store results on append only media, and cross-check with the live system (e.g., Tripwire—Tripwire Inc., Portland OR).
F. Penetration test critical servers to test for exploits using tools like Nessus/Metasploit. Given the results, consult with the Developers to mitigate the vulnerabilities, and learn programming practices that avoid them in the future (i.e., defend against Injection Exploits).

Bear in mind, while one can raise the bar significantly, to a determined Black Hat willing to pit significant resources against a single target, and given the likelihood that some required service has an undocumented and exploitable bug, no networked computer can ever claim to be completely bulletproof. Constant vigilance is required. To that point, the single best action that any site can take is to conduct information security drills. Several important points to consider on those drills are as follows [24, 25]:

(a) Creation of a "Red Team" made up the sites own information security IT staff, assume the role of Black Hats for the exercise, and attack the site's network
(b) A "Blue Team" which are just the other employees: Users, Developers, and other IT staff.
(c) Some example drills

   a. Patient data has gone poof: rebuilding the file-systems or databases
   b. Bad software rollout: either a commercial or custom developed program has been upgraded and is now broken
   c. Unauthorized device on network: How long to locate and neutralize?
   d. Building on c), a device that sniffs PHI traffic on the network and sends out to persons unknown on the Internet.

e. Phishing expeditions: how many Users are fooled?

(d) Perform post-drill reports that are shared with IT, Providers and the C-suite. Re-test the scenario in a couple of months to assess if mitigations have been deployed.

Initially, these exercises should be broadly communicated to the entire site staff to avoid panic. But as the site gains maturity and resilience in handling the “attacks,” they should be shared with a minimum of staff to increase realism.

Unfortunately, cyber-security is not a movie; it’s more like a deadly serious arms race, with Black and White hats alternately countering each other’s moves. There is unlikely to be a cease-fire anytime soon.

Glossary

Authentication	Is the agent who they claim to be
Authorization	Does the agent have rights to the resource
Confidentiality (data)	Is data secure from the eyes of unintended agents
Cyphertext	The encrypted version of an unencoded “clear” text
Denial of service	An attack that incapacitates a service running on a computer
Encryption	A reversible process to converts a clear text message that can be read by anyone into a cipher-text message that can be read by no one, unless they possess the decryption key(s).
Firewall	A device that contains two network cards on two different networks, and uses a rule base to select what data is passed through and in what direction
Hashing	An algorithm to generate a unique value from a unique text input
Integrity (Data)	Is data unaltered from its original sent state
Internet	The big “I” internet is the world wide network connecting the millions of private local area networks.
Local Area Network	Generally applied to a local Ethernet subnet where all computers have the same address suffix (i.e. xxx.corporationX.com)
Non-repudiation	Can an agent send/alter a message, then later deny having sent/altered it
One/two-factor authentication	One factor authentication may require only one piece of data, perhaps a password. Two factor methods use an additional item, perhaps a biometric (fingerprint, voice, etc.) to perform authentication.
Public Key Infrastructure	A trusted means of distributing individual’s public keys. Required in a large scale implementation of a public key encryption system.
Reliability	Is a service or system available and accurate when needed
Sniffing	Using a network interface card in a promiscuous mode to capture all data on the network, even if it is not meant for the local machine
Spoofing	Faking the Internet address of packets emanating from one’s computer so as to assume the identity of another computer and hide one’s true identity
Switched networks	As opposed to shared networks (which act like a party line in the telephone world), switched networks create private links momentarily between computers
Tripwire	A program that can detect intruder’s changes to a computer system’s critical files
Trojan Horse	A program that masquerades as something benign but actually contains Malware.
Virtual Private Network	A method of encrypting data passed on the open Internet so it is as if the users share a private link

Appendix A

To preserve readability, the body of this paper glossed over many details; for those inclined, this Appendix (and the following Glossary) address some of them. For a solid grounding on the topic of cryptography and encryption, the reader is directed to [26]. As mentioned in the section on “White Hat—Motivations” there are six goals the White Hat has to address. Of those, three are fully addressed by encryption and hashing: Authentication, Data Privacy, and Data Integrity. The other three areas (audits, authorization and reliability, and performance) will be addressed in turn.

Audits

As mentioned previously, auditing involves several categories of things to audit. Auditing *devices* means knowing what devices are on the network, what they do, and who they talk to. These points can be solved with numerous tools [27]. Auditing *Users* typically means looking at a time window of applications and data they used, and this is typically addressed by looking at HIPAA audit logs. Auditing of cyber-security *policies and* *procedures* should be done at least annually to see what is working, what is not, and with an eye to close that gap. Finally, *network auditing* should be done continuously and automatically to restrict network access to known agents (e.g., Cisco Firepower and ISE, Cisco Systems Inc, San Jose, CA).

Authorization

Authorization relies on tying a User or group of Users to a role, and defining access privileges for resources to that role. For example, members of the Finance Department would have access to the *finance* folder on the network, but other Users would not. As such, authorization depends critically on accurate authentication. In modern computing systems (i.e., Microsoft environments, Microsoft Corporation Redmond WA), the two areas are linked using a protocol based on LDAP (Lightweight Directory Access Protocol) [28].

Reliability and Performance

As mentioned before, not all service failures are due to Black Hats. The White Hats are also expected to maintain service uptime, at acceptable performance, in the face of hardware, software, and Acts of God failures. The methods for maintaining application uptime are referred to High Availability and are aimed at avoiding single points of failure. The methods to assure that data are never lost are referred to Disaster Recovery. The combination of methods to maintain both application and data availability are referred to as Business Continuity [29].

Authentication, Data Privacy, and Data Integrity

Encryption helps: authentication, data privacy, and data integrity (non-repudiation)

First consider data confidentiality. The goal is to transfer the “clear text” of the message (say “Patient Name Richard Nixon”) to some cipher-text like “sgsgsdfWE%#%@#$F.” The exact mechanics of the encryption process vary from algorithm to algorithm, but the bottom line is that without the right key(s), non-authorized Users cannot read the message. Tools exist to perform such encryption over the Internet as data is transferred [30]. They also exist to encrypt data at rest on a server [31]. Authentication and non-repudiation make use of both encryption and “hashing” as we will now see.

Hashing helps: authentication and data integrity (digital signing and non-repudiation)

A reversible encryption algorithm can be used to secure a message from prying eyes. However, the recipient of the message has no way of knowing the absolute identity of the person

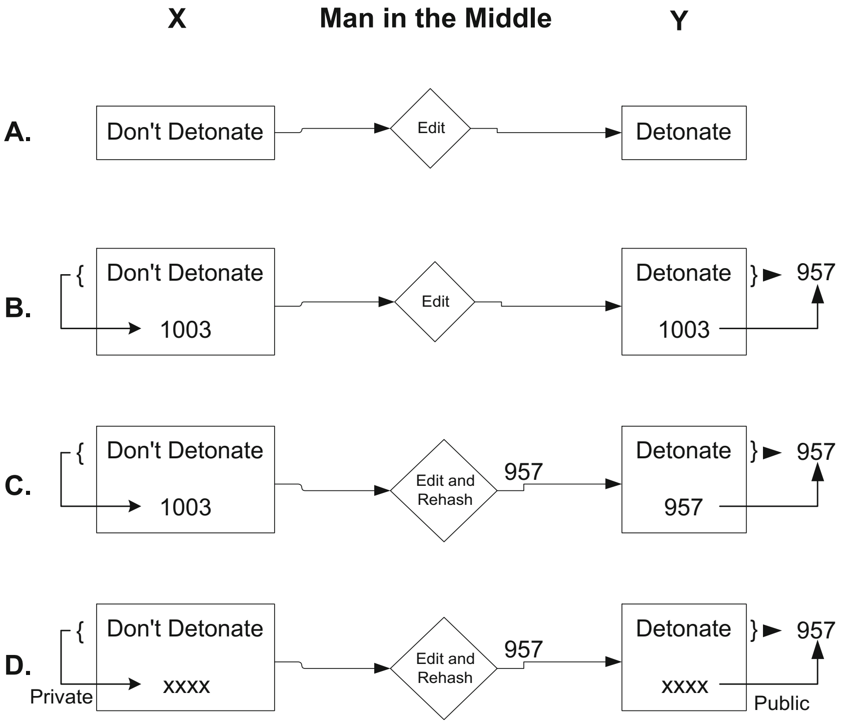

Fig. 1 (*A*) X sends a message, and it is altered by M. Y cannot discern the alteration. (*B*) X computes the document’s message digest (MD) and sends its value (1003) with the document. M alters the message. Y recomputes the MD of the message and detects an alteration, because the MDs do not match (957 ≠ 1003). (*C*) This time, M recomputes the MD and sends it with the altered message. Now when Y recomputes the MD and checks against the sent MD, the two match, and Y is fooled. (*D*) X digitally signs the MD, and M cannot reproduce X’s signature without X’s private key. Nevertheless, M alters the message. When Y decodes the MD signed by X and compares it with the recomputed MD of the altered message, Y detects the substitution (957 ≠ 1003)

who sent a message or that the message arrived uncorrupted. With a combination of public key encryption and a process known as "hashing," all these ends can be achieved.

A hash is a one-way, irreversible process guaranteed to generate a unique number for a unique data input. The importance of this process is that any change to the text document will result in a new value from the hashing algorithm. The two different values (called message digests "MDs") indicate that the input text has been changed. However, even this is not enough. If an enterprising Black Hat can intercept a message, they may well recompute the MD themselves and send it along with a modified document to the intended User. The User checks the sent MD against the MD they compute from the received message, finds that the numbers match, and has no way of detecting the modification.

This is where digital signing enters the picture. The real author computes the MD and encrypts it (in effect signing it) with their private key. If an intermediate Black Hat intercepts the message, throws out the real MD, falsifies the message, and supplies their own MD, the recipient will not be able to decode the MD with the public key from the presumed author. If the intended recipient User has faith that their public key is correct for the intended author, they will know that something is wrong (see Fig. 1). A side benefit of digital signing is that a document, once digitally signed, can only be repudiated by the signer by claiming one of two things: either that their private key has been stolen or that the public key claimed to be theirs has been forged by Black Hats. The latter argument is mitigated by the existence of trusted third-party PKI certifying authorities (e.g., Entrust DataCard, Entrust Inc., Minneapolis, MN).

References

Note: All web references were last viewed July 2016.

1. Langer SG, Stewart BK: Computer security: a primer. J Digit Imaging 12(3):114–23, 1999
2. Seibert T, Andriole K, Langer S, Siegel E, Morin R: Practice Guideline for Electronic Medical Information Privacy and Security. American College of Radiology Practice Guideline. 2004; 2004(Res. 12):471–77. PMID: 0
3. Morin et al: "ACR-AAPM- SIIM Practice Parameter for Electronic Medical Information Privacy and Security " http://www.acr.org/~/media/419A8512DBDB4FDE99EC75B3C68B01CF.pdf, 2014
4. "Health Insurance Portability and Accountability Act: Final Rule". Federal Register, 2013; 78(17): 5566–5698. https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
5. Felice RW et al: "Taking Back Control of Our Pacemakers and OnStar Vehicles" SIIM Annual Meeting, 2016, Portland, OR. http://siim.org/page/16it_security
6. Reel M and Robertson J: "It's Way too Easy to Hack the Hospital" Bloomberg Businessweek, 2015: 11. http://www.bloomberg.com/features/2015-hospital-hack/
7. Schneier B: "Beyond Security Theatre" https://www.schneier.com/blog/archives/2009/11/beyond_security.html, 2014
8. Zargar ST: A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE Commun Surv Tutorials 11:2046–2069, 2013
9. Hegan DG. "Risk and Reward Analysis". Expert Program Management. http://www.expertprogrammanagement.com/2011/07/risk-and-reward-analysis/
10. Lippmann R, Haines JW, Fried DJ, Korba J, Das K: "The 1999 DARPA Off-Line Intrusion Detection Evaluation". Comput Netw 34(4):579–595, 2000
11. Wikipedia "Computer Security Exploits" https://en.wikipedia.org/wiki/Category:Computer_security_exploits
12. Becher M, Freiling FC, Hoffmann J, Holz T, Uellenbeck S, & Wolf C: Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices." *Security and Privacy (SP), 2011 I.E. Symposium on* (pp. 96–111). IEEE 2011
13. Foster B, & Lejins Y: Ehealth security Australia: the Solution Lies with Frameworks and Standards. *Proceedings of the 2nd Australian eHealth Informatics and Security Conference*, 2–4 December 2013, Edith Cowan University, Perth, Western Australia, 2013
14. Maydanchik A: "Data Quality Assessment", Technics Publications, LLC, Bradley Beach, NJ, 2007
15. Open Web Application Security Project (2005) "OWASP Developers Guide V2.0". OWASP Publishing, Bel Air, MD
16. Computer Emergency Response Team (CERT). "Top 10 Secure Coding Practices" https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices
17. LA Times: "Hollywood Hospital Pays $17,000 in Bitcoin to Hackers". http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html, 2016
18. Esser S: "iOS Kernel Exploitation". Blackhat Annual Meeting, Las Vegas NV. https://media.blackhat.com/bh-us-11/Esser/BH_US_11_Esser_Exploiting_The_iOS_Kernel_Slides.pdf, 2011
19. CERT Top 30 (May 2015). "Top 30 Targeted High Risk Vulnerabilities" https://www.us-cert.gov/ncas/alerts/TA15-119A
20. The Honeynet Project (Gordon Lyon, 2001). "Know Your Enemy: Revealing the Security Tools, Tactics and Motives of the Blackhat Community". ISBN-10: 0321166469 Addison Wesley, New York, NY
21. Easy doc. Hacket R: "Do not Download This Scam Mac App! It's Nasty Malware" Fortune 2016: 7. http://fortune.com/2016/07/06/mac-malware-backdoor-app/, 2016
22. Oechslin, Philippe (2003-08-17). "Making a Faster Cryptanalytical Time-Memory Trade-Off". Advances in Cryptology: Proceedings of CRYPTO 2003, 23rd Annual International Cryptology Conference. Lecture Notes in Computer Science (*Santa Barbara, California*, USA: Springer). ISBN 3-540-40674-3
23. Takai TM, et al: "Guide for Conducting Risk Assessments", National Institute of Standards and Technology-Computer Security Division, Gaithersburg, MD, 2012
24. Scarfone K, et al: "Technical Guide to Information Security and Assessment". NIST Special Publication 800–115. National Institute of Standards and Technology-Computer Security Division, Gaithersburg, MD, 2008
25. Sons S: Under the sink: security exercises. Linux J 276:42–58, 2016
26. Schneier B: Applied Cryptography". Wiley and Sons, Hoboken, NJ, 1996
27. Schoen D, Kumar N: Getting Started with Spiceworks". Packt Publishing, Birmingham, UK, 2013
28. Carter G: LDAP System Administration". O'Reilly Media, Sebastopol, CA, 2003
29. Snedaker S: Business Continuity and Disaster Recovery Planning for IT Professionals, 2nd edition. Elsevier Publishing, Amsterdam, Netherlands, 2013
30. Davies J: Implementing SSL/TLS Using Cryptography and PKI". Wiley and Sons, Hoboken, NJ, 2011
31. Garfinkel S: Pretty Good Privacy". O'Reilly Media, Sebastopol, CA, 1994