Gabrielle Sudik
IT1025 CRN 12115 – Spring 2017
Professor Tamerlano
Lab 5
April 3, 2017

Executive Summary

The theme of this week's lab is access to data: Who should have it, how can they get it, how it is protected, how it can safely be shared, and how it might be discovered even when it is protected.

Multi-Factor Authentication

One example of multi-factor authentication I encounter a few times each month is when I log on to an online videogame that I enjoy. Each time I log on, I have to enter my username and password, and about twice a month I have to enter a six-digit code that is sent to me via an electronic dongle. The code is random each time I press the dongle's button, and that is the only device linked to my account, so one without the dongle would be able to know the code. I'm also asked for the code each time I log on to the game from a new computer, or when I need to update payment information.

The multi-factor authentication makes my account (both financial account and in-game "stuff") more secure. I know several people whose accounts were compromised, and unknown persons temporarily took control of the game characters and stuff. All of these people did *not* have multi-factor authentication, but were quick to get it after the game company re-secured their accounts. I personally have never had my account compromised, and I assume that, in part, it is because of the two-level authentication.

The downside of this is, if I don't happen to have my dongle handy when I'm asked for my code, I have to go looking for it. I keep it on my keychain, because I always know where my keys are. This is a small hassle, and it happens rarely. And in my opinion, it is worth it for peace of mind. I would more bothered if the second step of authentication were more troublesome. Or if it required some sort of biometric information. My worry in the latter case would be: What if the company itself was compromised, and hackers now have not only a password, but information about me that might be used to fake me somewhere else (like a fingerprint or iris scan, etc.) Everything is secure until it is stolen, right?

The Information Security Triad

The information security triad consists of confidentiality (giving access to information only to people who are supposed to see it), integrity (assurance that the information is accurate and not tampered with) and availability (info can be access and modified by appropriate people). Say I want to check my bank balance at an ATM. The machine will ensure confidentiality by only allowing someone who has both my bank card and my PIN to check it. (Note the two-step authentication: Something I have and something I know.) Once the ATM has both the card and PIN, it allows me to see my balance. Integrity is a little harder to confirm on a trip to the ATM because the ATM alone cannot demonstrate that the information is accurate, but once the ATM tells me my bank balance, I should be able to compare that amount to my statements and checkbook.

Access to Data

The access control list (ACL) and role-based access control (RBAC) are two ways access to data can be limited only to appropriate people. ACL basically grants permissions (like read, write, delete) to each individual for each set of data. ACLs are very simple, but different ACLs must be set up for each information resource. RBACs assign different roles to each user (like reader, writer, administrator) then each role is assigned to the correct level of access in each information resource. This method allows users and roles to be managed separately, and one RBAC can be used to set permissions for multiple resources.

Cryptology

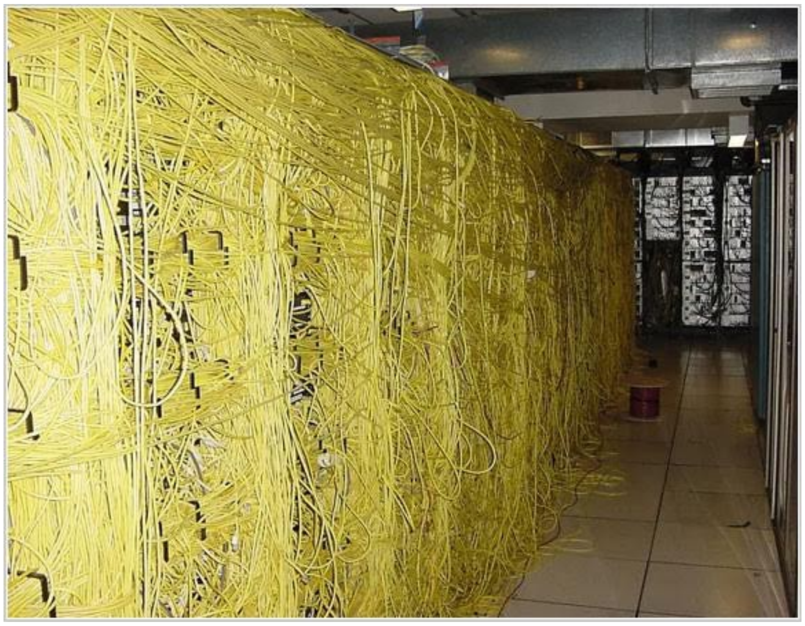
Ciphertext is an old method of scrambling written messages by substituting letters in the original message with other letters a fixed, pre-determined number of letters away in the alphabet. In modern computer encryption, a system of public and private keys are used to create the "secret code." The public key is used by anyone who creates the original message, while the private key is used only by the person intended to read the message (or rather, that person's computer). It works with some math that the computer science major in the video won't get into right now. But here is an example of ciphertext: Using a 5 letter shift, the text "Xjhzwnyd nx pjd ns Nsktwrfynts Yjhmstqtld." becomes "Security is key in information technology."

ICANN and IP Addresses

ICANN is responsible for the top-most distribution of all IP addresses. IP addresses are allocated to five regions around the world (corresponding roughly to the five continental areas) called Regional Internet Registries. Each disbursement to an RIR (called a /8) contains over 16 million IPv4 addresses, and each /12 for IPv6 addresses is significantly larger. The RIRs are then responsible for assigning blocks of IP addresses to regional organizations like ISPs, schools, businesses, etc. ICANN does not have a role in controlling content on the internet, but ICANN will assess requests for more IP addresses in terms of need and size of the grant.

Mesh Topology

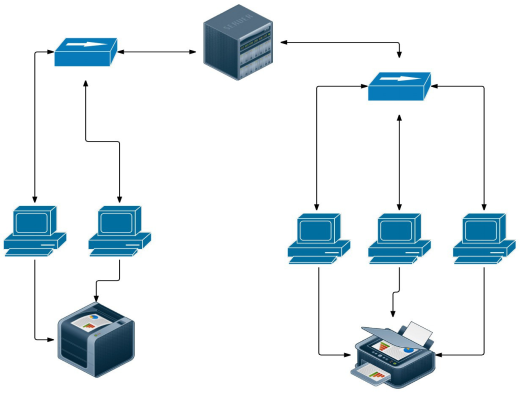
In a mesh topology, each hose connects to at least two other hosts. Sometimes each host connects to all other hosts, and sometimes each host connects to only a few other hosts. This arrangement is most likely to be used where a high level of redundancy is needed (I will speculate that systems like air traffic control and military defense are meshes). Advantages to mesh topology are (1) information can travel via multiple routes; (2) lots of data can be transmitted without slowing down the system; (3) data is more secure because it can travel only where it needs to go; and (4) troubleshooting is easy. Disadvantages of mesh topology include: (1) it is complicated to install because there are so many ports, wires and connections; (2) it is expensive, for the same reasons; and (3) the redundancy can be a little *too* redundant, resulting in server rooms that look like this:



(I got some help from a website at Pace University for this one: http://webpage.pace.edu/ms16182p/networking/mesh.html)

Network Diagrams

Here is my first network diagram, using random pics from Lucidchart: This is a tree topology. The server goes to two distribution points. Perhaps each point is in a different division of the same company, or on different floors. The two computers on the left are connected to one printer, and the three on the right are connected to a different printer.



The National Security Administration

On the NSA website, I read two sections of “What We Do” – Understanding the Threat, and Signals Intelligence. When it comes to Understanding the Threat, NSA is tasked with preventing harm to the United States, whether it’s in the form of other governments, terrorism, or even drug smugglers. Cyber criminals are growing more dangerous, and they can launch a variety of attacks on US, including stealing funds or information from businesses, customer identities and military intelligence. They can also use the internet to spread dangerous propaganda or hate speech, or provide online “safe havens” to connect wrongdoers with one another. The NSA works to keep track of, and prevent, such meddling with the internet.

In Signals Intelligence, the NSA tracks the ability of other governments and organizations to collect and disseminate information. That is, NSA learns about other communication systems, and the intentions and actions of adversaries. (The NSA doesn’t use the word “spy” but I will.) The work involves translators, mathematicians, analysts and engineers.

DDoS vs Surge in Legitimate Traffic

A Distributed Denial of Service (DDoS) attack occurs when a hacker tries to bring a website to a halt by having multiple computers all try to contact the site at one time. There are various reasons a hacker might do this, ranging from attempted theft or ransom to plain old troublemaking. The attack will “look like” an incredible increase in the amount of traffic to the site, slowing it down for everyone else. An easy way for a site or network operator to distinguish between an attack and a natural increase in traffic is to check the metadata of the site, and it might reveal that the traffic is caused by misconfigured load bouncer (ie, an error, not an attack).

My Project

The details of my project will probably reveal themselves once I really get into the research, but I think my general topic will be exploring how information systems – perhaps something specific like crowd sourcing – can be used to compile historical data, educate historians, and in some cases, even reach conclusions on the topic in question. I’m interested in this topic for a number of reasons. First, I was a history major in college. When I wrote my thesis in 1995-96 (a 35-page paper of original research), almost all of the original sources I read were in hard copy. Books, magazines, even newspapers. Some older material was on microfilm or microfiche, but those are just another version of “hard copy” in that I actually had to go to where the film and fiche were housed to read them. How I would have loved having at least some of my material online, both for background research and for access to (e-copies of) the original documents.

Second, I was intrigued a few years ago when I visited the Rembrandt exhibit at the Cleveland Museum of Art. Among other things at the exhibit, I learned that one painting's authenticity assessment was recently changed by art scholars from “attributed to Rembrandt” to “by Rembrandt” because so many people earlier in the exhibit had written to the museum saying they thought it was by Rembrandt himself. Scholars took a closer look, and agreed with the crowds. Obviously, the input of experts was still needed to confirm what the crowds thought, but the experts then had the added benefits of thousands of pairs of eyes to help them assess the piece.

Conclusion

In this lab, I discussed several IT elements related to data security: authentication, access controls, encryption, and the “security triad.” I also discussed the NSA, and how part of its mission is (they hint!) to get around IT security, in order to learn what hostile governments or lone criminals might be up to. I also discussed and diagrammed some network topologies, and explained ICANN's role in distributing IP addresses. Finally, I ruminated about a possible topic for my upcoming class project.