Austin Andres

Section: 4001

Homework 01 (SY308)

(10 pts: 20 mins) Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give at least three examples of pillars of cybersecurity requirement associated with the system. Give at least two examples of fundamental security design principles that would be helpful for the system.

Pillars of cybersecurity:

1. Authentication: The ATM requires customers to use their unique card with their unique pin to access money. This is a two-factor authentication example.
2. Confidentiality: The ATM keeps its users' banking account information confidential from other unauthorized users.
3. Availability: ATMs are a common machine that can be found everywhere and are a simple computer. Additionally, ATMs' two-factor authentication is quick to use. This allows for timely, reliable access for authorized users.

Fundamental security design principles:

1. Least Common Mechanism: If one ATM is compromised via a bug, the unauthorized user should not be able to gain further access into the system of other ATMs or other user's accounts.
2. Open Design: The security of the ATM should remain secure even if the security architecture and design of a system are publicly available. This way if a hacker obtains how the ATM works, they still cannot compromise the system due to keeping the cryptologic keys secret.

(4 pts: 10 mins) For each scenario, identify the security design principle (by Saltzer and Schroder) that the scenario violates, and briefly explain how the principle is violated.

BigMoney is a local bank providing ATM service. Normally, when a customer inserts his ATM card, the ATM will contact the BigMoney central server to validate the ATM card and check that the corresponding account has sufficient funds before allowing the user to withdraw money. However, if the server does not respond, or the network connection is down, the ATM will assume all is well, allow the customer to withdraw up to $300, and upload the transaction data later when connectivity is restored.

Principle: Fail-safe default

Explanation: BigMoney is allowing access to users without explicit access. For example, if the customer does not have 300$ in the bank they are able to steal money. The system needs to shut down until the issue is resolved rather than assuming.

Alice once heard about a kiosk at one airport that lets you access the web, for a fee. To use the kiosk, you had to enter your credit card information. However, some hackers discovered that if you press F1, the Windows help subsystem would pop up a window with generic help information. The help text happened to contain a link to an external web site with more help information, and if you click on that link, the kiosk would open the Internet Explorer web browser to display that web page. At that point, one could change the URL in the IE address bar and gain full access to the web, without paying.

Principle: Complete Mediation

Explanation: It is clear that this kiosk did not have control and did not monitor every access point. There is a relatively simple back-door to circumvent the protocols in place to access the internet, which allows hackers to bypass them and get free internet access. This kiosk needs to act to ensure that the access and control mechanism cannot be circumvented.

Title: Sealed U.S. Court Records Exposed in SolarWinds Breach

URL: https://krebsonsecurity.com/2021/01/sealed-u-s-court-records-exposed-in-solarwinds-breach/

First paragraph (summary):

CISA believes the SolarWinds attack began at least as early as March and is still ongoing. It's not clear exactly what the attackers have done beyond accessing top-secret U.S. government networks and monitoring data. However, it was stated that the breach is affecting thousands of organizations that relied on backdoored products by network software firm SolarWinds may have jeopardized the privacy of countless sealed court documents on file with the U.S. federal court system. It is believed that the attacker has a high level of sophistication, complex tradecraft, and is an advanced persistent threat actor, all signs pointing towards Russia. The source said the intruders behind the SolarWinds compromise seeded the AO's network with a second stage "Teardrop" malware that went beyond the "Sunburst" malicious software update that was opportunistically pushed out to all 18,000 customers using the compromised Orion software. This suggests the attackers were targeting the agency for deeper access to its networks and communications. The data is valuable to the Russians because it has data about ongoing criminal investigations. Officials are investigating whether the company, founded by three Russian engineers in the Czech Republic (JetBrains) with research labs in Russia, was breached and used as a pathway for hackers to insert back doors into the software.

Second paragraph (Violation of fundamental security design principles and pillars of cybersecurity):

The number one pillar of cybersecurity that was compromised here was confidentiality. This attack led to the unauthorized disclosure of possibly thousands of classified records. The attack is still ongoing so more data could be stolen each day. Further, no one is sure what data was actually stolen. This ties into the second pillar of cybersecurity that was compromised: non-repudiation. No one knows who the actor is, what exact path they used, nor what they took. The first violation of fundamental security design principles prevalent in this attack is complete mediation. It is clear that the attackers were able to gain entrance through a backdoor, thus SolarWinds did not have complete mediation of all access points. The second violation of fundamental security design principles was Least Common Mechanism. The attackers gained entrance through a single-entry point, yet they were able to gain access to thousands of files because they were grouped together rather than isolated.

Third paragraph (Countermeasures):

The judicial branch agency said it will be deploying more stringent controls for receiving and storing sensitive documents filed with the federal courts, following a discovery that its own systems were compromised as part of the SolarWinds supply chain attack. The companies severely affected by this breach need to implement a defense-in-depth system. If an attacker is able to gain access into a system there should be additional security practices in place to ensure the least amount of data can be accessed. Something as simple as two-factor authentication to files within the database could have mitigated the effects of the breach. Additionally, on an obvious note, the US Government should not be utilizing third-party vendors with ties to Russia to secure their systems. Finally, there needs to be better mediation with some type of an intrusion system. The attackers had access to the database for almost a year until the breach was actually discovered. With a proper intrusion system, the effects of this breach could have been drastically mitigated.

(15 pts: 30 mins) The following is a ciphertext from the Vigenere cipher. You will break it by referring to the course notes on how to break Vigenere cipher.

NZRAGNFGSYFPLQCNABHAFNGZUAANSVHUBHXVXWANANFAGSLUULVMLBEW
RJLUYHYUAANWKNZVXVRHXEIENHWNPWFXJBJHRL

(5 pts) Give the plaintext:

THE GOAL OF ENCRYPTION IS TO MAINTAIN CONFIDENTIALITY THAT IS TO KEEP
THE PLAINTEXT HIDDEN FROM AN EAVESDROPPER

(10 pts) Explain the steps that you took to obtain the plaintext.

Knowing this is a Vigenere Cipher we need to know what the key is to decrypt the ciphertext. We are not given the key or its length so there are a couple of things to try. I figured out that the most common letters in the ciphertext were N, A, H. These letters might correlate to the most common letters used in words such as E, T, A. But first I looked for reoccurring letter pairs and triplets that had common letters used in the ciphertext, I found that AAN repeated twice. There were a few pairs, but the triplet gave me hope that the key length was 3. My first analysis led me to break up the ciphertext into 3 lines (assuming the key might be 3 characters long). The break up is as follows:

NAFYLNHNUNHHXNFSUMEJYUNNXHIHPXJL

ZGGFQAAGASUXWAALLLWLHAWZVXEWWJH

RNSPCBFZAVBVANGUVBRUYAKVRENNFBR

I took the first line and plugged it into the Caesar-Shift program on the SY110 website, it said that it was 99.9% that it was a shift of 20, which corresponds to “U”. I did the same process for the next two lines. The key came out to be “USN” and sure enough, it worked to decrypt the ciphertext. The technique I used is called frequent analysis.