Information Security

Project (slides & report)

Chapter # 14 (From: Security Engineering by Ross Anderson)

Mam Hina Binte Haq

Course Instructor
CS- 3002
SE- S
Due Date: May 07, 2023

Group Members:

Zeeshan Ali	Hammad Aslam	Ans Zeeshan
20i-2465	20i-1777	20i-0543

Table of Contents

Security Printing and Seals

Abstract:

In this chapter we will be discussing about the Introduction and history of the topic and after that what techniques are used to identify secure printed seals after that we will come to know how the seals are attached on the packages and some vulnerabilities that come across while producing and we will also come to know about some issues that are generated.

Introduction:

We will cover the significance of secure printing, packing, and seals in computer systems in the introduction session to ensure their protection. The user can be reassured that the product hasn't been tampered with since leaving the manufacturer thanks to seals and tamper-evident packaging. Another front has been opened up by how simple it is to create passable forgeries using contemporary color scanners and printers. The history of seals, their application in authentication techniques, and how their significance evolved over time from paper to packaging are also briefly covered in this chapter.

In the Introduction, we have discussed about the **usability of the security** and enlighten the ideas to a person to how he needs more concerns about to recognize the forged notes and it's like that HCI is preventing those forgeries and it has main focus on the usability of the security in this area.

A threat model is required to detect potential sources of threat when evaluating protection technology. According to the industry, a fake banknote or document may or may not pass one of three forms of inspection:

1. Primary inspection: This is carried out by a person who is uneducated and inexperienced, such as a member of the public or a brand-new cashier at a store. A primary inspector might not have the desire to carefully examine the item and might try to pass it off as genuine.
2. Secondary inspection is carried out by a qualified and motivated individual, such as a seasoned bank teller or a factory inspector, who may utilize specialized tools like an ultraviolet lamp, a pen with a chemical reagent, a scanner, or a PC. This equipment can be comprehended by serious counterfeiters, but it is restricted in terms of price and volume.
3. Tertiary inspection: This is carried out in the manufacturer's or issuing bank's laboratory. There will be extensive equipment and assistance available, along with the specialists that created the security printing. If the product and the inspection process have been skillfully developed, it is typically impossible to get a counterfeit past tertiary examination.

Techniques:

Intaglio, letterpress, specialized printing presses including Simultan presses, rubber stamps, embossing and laminates, watermarks, and fluorescent threads are a few examples of conventional security printing methods. These methods are used to make raised impressions, print with both sides aligned, endorse papers, seal images, increase the expense of forgery, make translucent areas, and use special materials for protection.

Inks with magnetic, photochromic, or thermochromic qualities, optically variable inks, printing features visible only with specialized equipment like microprinting, ultraviolet, infrared, or magnetic inks, and metal threads and foils with optically changeable effects like holograms are examples of contemporary approaches. Additionally, digital copyright marks are used to alter images hidden by microprinting their Fourier transforms or by using spread spectrum signals that will be recognized by a color copier, scanner, or printer and cause it to stop. These techniques include screen traps and alias band structures to create details that are too faint to scan properly and digital copyright marks to vary images. Last but not least, a barcode can be used to digitally sign a document and print it on special stock like paper that had magnetic fibers distributed randomly throughout it during manufacturing.

Certain activities, such as copying The Big Issue, committing check fraud, and altering credit cards and travel documents, may currently be difficult and expensive to do. However, it's implying that these activities may become easier and cheaper in the future, possibly due to advancements in technology.

Packaging & Seals:

As tamper-indicating tools intended to leave irrefutable proof of unauthorized access or tampering, seals are defined as such. In this chapter, the author discusses how tags are made and connected to the material that is being safeguarded via security printing on substrates. The chapter also covers substrate characteristics and how systems confer uniqueness on the substrate material by introducing random variability. The next section of the chapter explores the issues with glue and explains how most seals operate by attaching a security-printed tag to the intended object. The chapter ends with a discussion of how seals are typically poorly implemented in items and how many seals can be easily removed directly with some patience and simple hand tools. A "PIN" is your own security code. Personal identification number is referred to as PIN. In order to guarantee security and confidentiality, it is shipped in a tamper-evident package.

Systemic Vulnerabilities:

The wristband system used to control crowding at a nearby swimming pool is linked to system-level threats in this issue. During busy times, different colored waxed paper wristbands are distributed every 20 minutes. One strategy is to call the supplier and place an $8 order for boxes of 100 wristbands. The bracelets can be reused in a more covert attack by being gently pulled off in various directions without noticeable harm. The weaknesses include the following: Enemy is customer; Customer applies seal; Available in market; Inspection is impractical; Manufacturing of counterfeit seals; Seal reuse indistinguishable from failure. The discussion comes to the conclusion that the wristband system is still useful and successful despite these flaws since there is minimal incentive to cheat and the rewards of doing so do not outweigh the drawbacks.

Issues:

1- Peculiarities of the Threat Model:

Depending on the application, the threat model for security printing and seals can change. When a business subcontracts manufacturing, it is common for the client to be the adversary. This is especially true when the business is concerned that the contractor will manufacture more goods than anticipated, resulting in overproduction and counterfeiting. For high-value products with integrated serial numbers and digital signatures, such as cosmetics, there may be a variety of packaging options. The sealing mechanisms must enable agents to go out and make sample purchases in order to discover counterfeits, as distributors who buy counterfeit items might not do so with malicious intent and might unintentionally sell them to customers. Inspection, however, can be difficult. As a result, the audit, testing, and inspection processes must be taken into consideration while designing sealing devices.

2- Staff Diligence

It checks for "seals," or those who claim to have carried out their obligations but haven't. To avoid this, the Los Alamos risk assessment team has created a number of seal designs. In one concept, a tiny CPU houses a cryptographic keystream generator that generates a new number roughly once per minute. The inspector's responsibility is to examine each of the incoming containers and note any numbers that are displayed. The device erases its key and stops producing numbers if a tampering incident is noticed. Such seals are also referred to as "anti-evidence" seals since they keep track of information indicating when a device hasn't been tampered with and destroy it when it has, leaving nothing for a foe to forge. The article also emphasizes how corruption and carelessness can coexist, and how if enough employees are irresponsible, a bribe that results in a fault does not establish dishonesty on its own.

3- Random Failure

The impact of sporadic failures on the security of seals is stated in this topic. Seals can fail for legitimate causes, such as when a truck engine is being steam cleaned, making it challenging for traffic enforcement to demonstrate tampering. A well-sealed envelope can also be opened and then resealed with a fake sticker, which could cause issues during prosecution. The consequences of these failures depend on the protection purpose, and if that goal is to assist prosecutions, spontaneous seal failure can be a major issue that could compromise the seal's admissibility as evidence and result in a miscarriage of justice.

4- Material Controls

Security measures may be weakened by the absence of control over sealing material sources. Corporate seals, for instance, are made of metal embossing plates that are placed into unique pliers and used to crimp significant documents. These plates are produced by a number of suppliers, and no checks are performed when orders are placed. This means that by creating a letter that appears to have come from a law firm, it is simple to have a seal manufactured for nearly any less well-known target. Blister packs, holograms, and color-shifting inks are used by the pharmaceutical industry as security measures, although anybody can access these technologies for a small fee. Similar to how anyone with access to fresh envelopes at the depot may readily replace the plastic envelopes used by courier services. Urban myth: If the flaps are strengthened with adhesive tape, the police and security agencies cannot open the envelopes without leaving a trace. Even if sellotape were guaranteed to leave a noticeable trace on an

envelope, it would be challenging for law enforcement to identify a fake one because desktop color printers have made it simpler for forgers to imitate firm insignia.

5- Cost and Nature of Inspection

The security printing and seals sector faces difficulties with the cost and type of inspection. Holograms, security features, and tamper-evident packaging are all intended to prevent counterfeiting, but it is challenging for anyone to thoroughly inspect them. Forgery is simple due to the wide range of passports, driver's licenses, company seals, and packaging, especially without authentic items for comparison. In research, even tamper-detection experts were unable to identify tampering, which raises questions about how well the typical consumer can spot fraud. Software is a high-value product package that is tougher to safeguard than currencies. Over the past several years, online registration systems have taken on a larger role in software product protection against counterfeiting. One option, however problematic, is to enlist the public as examiners of unique serial numbers.

6- Not protecting the right thing

When organizations fail to safeguard the appropriate items, systemic vulnerabilities may result. For instance, in the late 1980s, when authorization terminals read the magnetic strip and payment draught capturing devices employed embossing, credit cards were susceptible to attacks. Attackers might alter the mag strip but not the embossing, rendering the system vulnerable. Similar to this, attackers could partially alter credit cards by changing the final four numbers because the hologram only covered those digits. The remaining portion of the card could then be flattened, reproduced, and re-embossed using inexpensive tools. While amateurs may find it difficult to fake some packaging measures like shrink-wrap or blister packaging, they may not be sufficient to fend off threats like forgery, alteration, duplication, simulation, diversion, dilution, substitution, or tampering. which call for different safeguards.

References:

https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c14.pdf

https://www.bcsyseal.com/collections/plastic-seal-6?gclid=Cj0KCQjwgLOiBhC7ARIsAIeetVDrFAy6m4fzLXvOoZaGypXIQsNOC8MBhzME5sTQcol0X2oPDHbj8QgaAh_SEALw_wcB

https://www.slideshare.net/anand8095/security-features-of-currency-note

https://slideplayer.com/slide/5090607/

Work Division:

Name	Roll No	Work Division
Zeeshan Ali	20i-2465	Slides, Report
Ans Zeshan	20i-0543	Slides, Report
Hammad Aslam	20i-1777	Slides, Report