Contents

SURVEY AND ANALYSIS OF HARDWARE TOOLS USED IN CYBERCRIME INVESTIGATIONS

SIGNIFICANCE [1]:

TOOLS	TO INVESTIGATORS	TO SUBJECTS
ACCESS CONTROL DEVICES[1]	• Investigators can use these devices to monitor any malicious activity according to the pattern of use. • The presence or absence of an individual at a controlled location may be established.	• These may be hacked by the subject and used to gain unauthorized access to a physical location. • Get access to sensitive data like how a building or a specific site is being used such as frequency and time trends. • In worst case it may be used to create a false alibi implying a that people were somewhere where they were not.
ENCRYPTION TOOLS[1]	• Encryption is used by the law enforcement agencies to protect evidence and other sensitive information. • Decryption by law enforcement may be required to achieve the following: ➢ Recover evidence from hidden/ encrypted logs. ➢ To prove the intent of the criminal/ suspect.	• Criminals can use encryption to circumvent law enforcement detection Contraband or evidence such as: ➢ Child pornography. ➢ Details of counterfeit currency. ➢ The stolen credit card number. ➢ Email or chat file. ➢ Intellectual property information. • Organizations use cryptographic tools to do the following: ➢ Protect yourself from theft of your intellectual property. ➢ Protect customer data from unauthorized access due to network intrusion or hardware theft.
ANSWERING MACHINES[1]	• Acquire record of call content and date/time stamp Listen to the message to determine if the message was heard. • Identifies the caller based on the content of the incoming message. • Identify the owner in a pre-recorded outbound message. • Identify covert identities.	• Modifying or deleting the original recording to distract or mislead investigators. • Promote and give credit to criminal enterprises. • Communicate with each other.

[1] Detailed Definitions, Investigative scenarios and Case study have been included in the Appendix.

SPECIAL INVESTIGATORY CONDITIONS AND LIMITATIONS [1]:

TOOLS	KEY POINTS TO REMEMBER
ACCESS CONTROL DEVICES	• The logs for a device may be unreliable as the key fobs, smart cards, and passwords may be stolen or compromised. These also have a high probability of getting demagnetized. • Biometrics have defined failure rates and may also be affected by physical injury and alteration (e.g., retinal patterns change during pregnancy) so these may or may not establish presence/ absence of an individual. • If the database is hacked the data may be easily overwritten and remotely purged even if suspect is at large.
ENCRYPTION TOOLS	• While carrying out an investigation, the purpose for using encryption tools must be carefully examined as possession of these tools may be legally allowed but their use may/ may not be. • Detection of encryption of encryption tools at the scene may lead to seizure of original hardware carefully without damaging or losing data in the process. Further necessary actions must be taken to recover the key/ passphrase which may require a more detailed search so a search warrant may be required. Also, high tech tools to bypass passphrase may be required in case the passphrase is not known.
ANSWERING MACHINES	• Information can be deleted or changed remotely, anyone with the password can access the system, and there is an automatic wipe policy. • If investigators are looking for voicemails in your company, they will have long-term access to secure data. • Remove the phone cord from the local answering machine to prevent remote wipe. • Voicemail data can be lost if the device is disconnected from power. Consider using a tape recorder to record your message before you turn it off. • The device day, date, and time settings should be compared with the actual date, date, and time.

APPENDIX

DEFINITIONS AND INVESTIGATIVE SCENARIO:

ACCESS CONTROL DEVICES [1]

Access control is a security method that controls access both physically and virtually until and unless the correct credentials are provided. The access control devices are typically located near locked doors gates or barriers and allow them to open only after the identity of the person is authenticated. Authentication may be based on the following elements:

- Something you have e.g., RFID access cards
- Something you know e.g., Pin or password
- Something you are e.g., assessing a person's physical characteristics like face recognition or fingerprints

Examples of such devices are: Key fobs, keypads, smart cards, biometric devices etc.

Figure 1 Keypad and Access Card [2]

Figure 2 Biometric Device [3]

SCENARIO

The murder suspect provided an alibi to police and claimed to have been at home during the murder. Police officers have determined that the suspect has a home alarm system. They received information about when the alarm was set and when the alarm was disarmed. That time confirmed the suspect's alibi.

ENCRYPTION TOOLS AND PASSPHRASE PROTECTION [1]

Encryption is a way to keep data sent and received over the Internet secure and private. Encryption involves the use of mathematical algorithms used to scramble user data, ensuring that only the intended recipients have access to the content.

Cryptographic tools are hardware-based, software-based, or a combination of both, and protect your data by making it inaccessible without using one or more of the following: a password, a passphrase, a "software key," or a physical access device.

EXAMPLES OF ENCRYPTION TOOLS:

- Dongles, key cards, or biometric devices are examples of encryption tools that can be employed on physical devices.
- Tools that are features of the media itself include the following:
  - Integrated drive or device electronics linked to a specific motherboard.
  - Encryption built into the disk that automatically encrypts data.
  - BIOS or boot passphrases.

** Encryption tools may also be a feature of common application software or may also be a standalone software

SCENARIO

A messaging app is providing user with end-to-end encryption so the messages or chat exchanged between two parties may not be read by a third party.

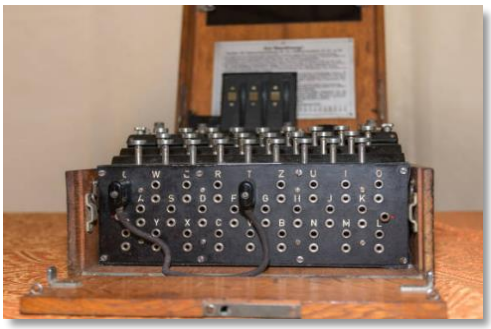

Figure 3 The ENIGMA machine [3]

Figure 4 Typical Dongle containing decryption key [3]

ANSWERING MACHINES AND VOICE MAIL SYSTEMS [1]

An answering machine is a device used to respond to and record a caller's message when no one can answer the call directly. Unlike voicemail, which is a network or centralized system that provides the same functionality but is usually available as a service anywhere, an answering machine is a local device that is connected to or directly integrated with a physical landline. An answering machine is also known as a telephone answering device, telephone answering machine, answerphone or message machine. Answering machines often store date and time stamp information. They can contain several settings, users, or mailboxes and can be incorporated into the phone. Alternatively, they can be a different device. Voicemail messages can also be stored on the communication service provider's local or remote device.

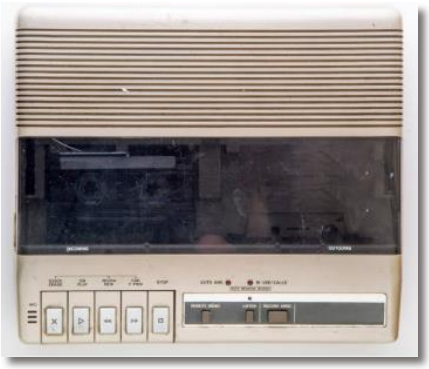

Figure 5 Answering Machine with Tape [3]

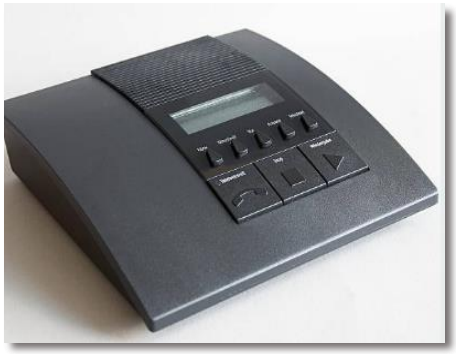

Figure 6 Digital Answering Machine [3]

SCENARIO:

During the murder investigation, the suspect provided an alibi with a voicemail message stamped with the date and time. A subsequent examination of the company's voicemail system revealed that the time setting did not match the actual time because the system was not set to daylight savings time. Therefore, the suspect's alibi was invalidated.

CASE STUDY: ENCRYPTION TOOLS AND THEIR IMPACT DURING WW2

ENIGMA [4]

The main source of secret communication for the Germans during World War II was the ENIGMA machine. It was invented by Arthur Scherbius in 1918. Enigma's encoding process began by typing plaintext characters into the keyboard. A current is passed through the three rotors, hits the reflector then bounces off and passes through the rotor in reverse order and illuminates a lightbulb inscribed with the appropriate letters to be written down to obtain the ciphertext. The plugboard acted like a transposition cipher, providing additional security for encrypted messages. To increase complexity, each rotor shifts its position by one place after a certain number of key presses, creating a cipher similar to the Vigenere cipher. Rings were placed on the left and center discs to determine how many keys had to be pressed before the next rotor was shifted one place. This shift in position meant that certain characters were not always encoded the same way. Attacks by frequency analysis are therefore almost impossible.

The ADFGX cipher, a cryptosystem previously used in Germany, was broken by Allied cryptographers During World War I. Germany was unaware of the work of Allied cryptographers and the German cryptographers thought they still had a secure system. It was only after the war had ended and the British Prime Minister Winston Churchill announced that his army had seized a German codebook containing a list of keywords and algorithms for finding the 5→5 grid used for encoding all German news. The cryptographer was able to read all intercepted messages from Germany. German cryptographers realized they needed a new cryptosystem that could not be compromised even if their codebook is captured.

Enigma became their Primary source for encrypting and decrypting messages. The German government made copies of the codebook and the Enigma and distributed them to the military. The codebook contained the rotor and breadboards initial settings. Every message sent started with a three-letter keyword, which was not encoded. This keyword was used to indicates the rotational position of each rotor. The next 6 letters were scrambled to include a 3-letter codeword that was repeated twice to ensure accuracy. When the target audience received the message, the operator typed the following six characters into the machine after the key to reveal the codeword. This codeword tells the operator the specific initial position of the rotor to decode the rest of the message.

The Germans thought their machines were indestructible, and it seems that was the case for some time. France was the first country to attempt to defeat the Enigma. Cryptographers thought that buying a commercial Enigma could give them insight into how the German military encrypted their messages. This was of little use as the commercial version had different number of rotors and moreover had no plugboard. In 1931 France finally got the help it needed when Hans-Thilo Schmidt, a German working with a German cryptographer, sold the Enigma Machine documents and keys to France. The extreme number of possible settings for the Enigma that the Germans had to cooperate with Indicates that the Germans had a system that was almost impossible to break. But the Germans didn’t make the most of this machine. German troops usually had rotors in the same position with each other for up to 3 months. Allied cryptographer could determine the position of the rotors and need not recalculate them for up to three more months.

In 1939 Poland knew that Germany would soon invade the country. Polish cryptographers and the government decided to hand over all the knowledge they had about Enigma and the replicas they made to France and the British government. The British government soon hired the best math, science and engineering personnel to work at the Bletchley Park facility to deciphers German messages. Alan Turing has planned to simplify Polish machinery. He believed that the machine would work more efficiently if it was built to check the expected text patterns. Many of the intercepted messages contained cilies, allowing Allied cryptographers to guess what the first three characters were decrypted by the Enigma. A cryptographer who knew this only had to check the settings to encrypt his first three letters of the suspicious key. Instead of looking at hundreds of thousands of possible settings, cryptographers need to test a few settings to determine the key. Once that is done, the cryptanalyst can replica the settings and decrypt the rest of the message. Designed by Alan Turing and known as a bombe, this machine worked by circulating hundreds of possible settings at once. Bombe rotor spins at high speed and checks All positions that encode an encrypted 3-character key into an expected 3-character key. If a possible match is found, the rotor will stop spinning.

The messages that the Allies were able to intercept resulted in several major victories that contributed to the outcome of the war.

Bibliography

[1] D. W. Hagy, "Investigative Uses of Technology: Devices,Tools, and Techniques," U.S. Department of Justice Office of Justice Programs.

[2] [Online]. Available: https://safeguardsystems.co.uk/.

[3] [Online]. Available: https://www.istockphoto.com/.

[4] K. Callahan, "The Impact of the Allied Cryptographers," 14 december 2013. [Online]. Available: https://www.gcsu.edu/. [Accessed 30 july 2022].

[5]