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]

SIGNIFICANCE OF ACCESS CONTROL DEVICES

TO THE SUBJECT:

- 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.

TO THE INVESTIGATORS:

- 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.

SPECIAL INVESTIGATORY CONSIDERATIONS AND LIMITATIONS

- 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.

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

Figure 3 The Turing machine [3]

Figure 4 Typical Dongle containing decryption key [3]

SIGNIFICANCE OF ENCRYPTION TOOLS:

TO THE SUBJECTS:

- 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.

TO THE INVESTIGATORS:

- 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.

SPECIAL INVESTIGATORY CONSIDERATIONS AND LIMITATIONS

- 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.

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.

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.

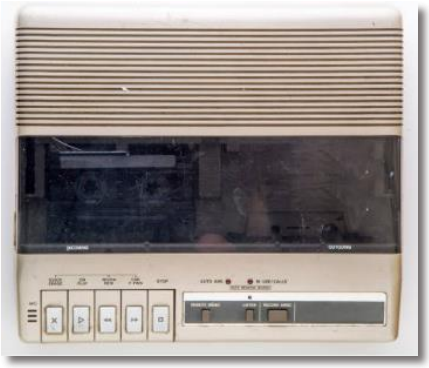

Figure 5 Answering Machine with Tape [3]

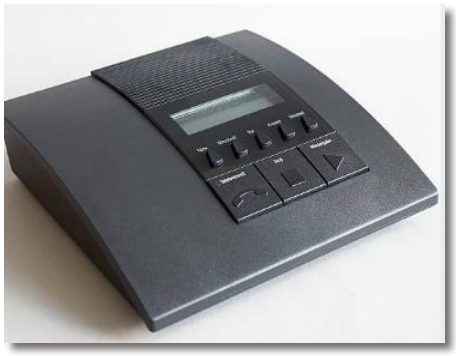

Figure 6 Digital Answering Machine [3]

SIGNIFICANCE OF ANSWERING MACHINES AND VOICE MAIL SYSTEMS

TO THE SUBJECTS:

- Modifying or deleting the original recording to distract or mislead investigators.
- Promote and give credit to criminal enterprises.
- Communicate with each other.

TO THE INVESTIGATORS:

- 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.
- Covertly monitor incoming calls for threat and stalking investigations.

SPECIAL INVESTIGATORY CONSIDERATIONS AND LIMITATIONS

- 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.

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.

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/.