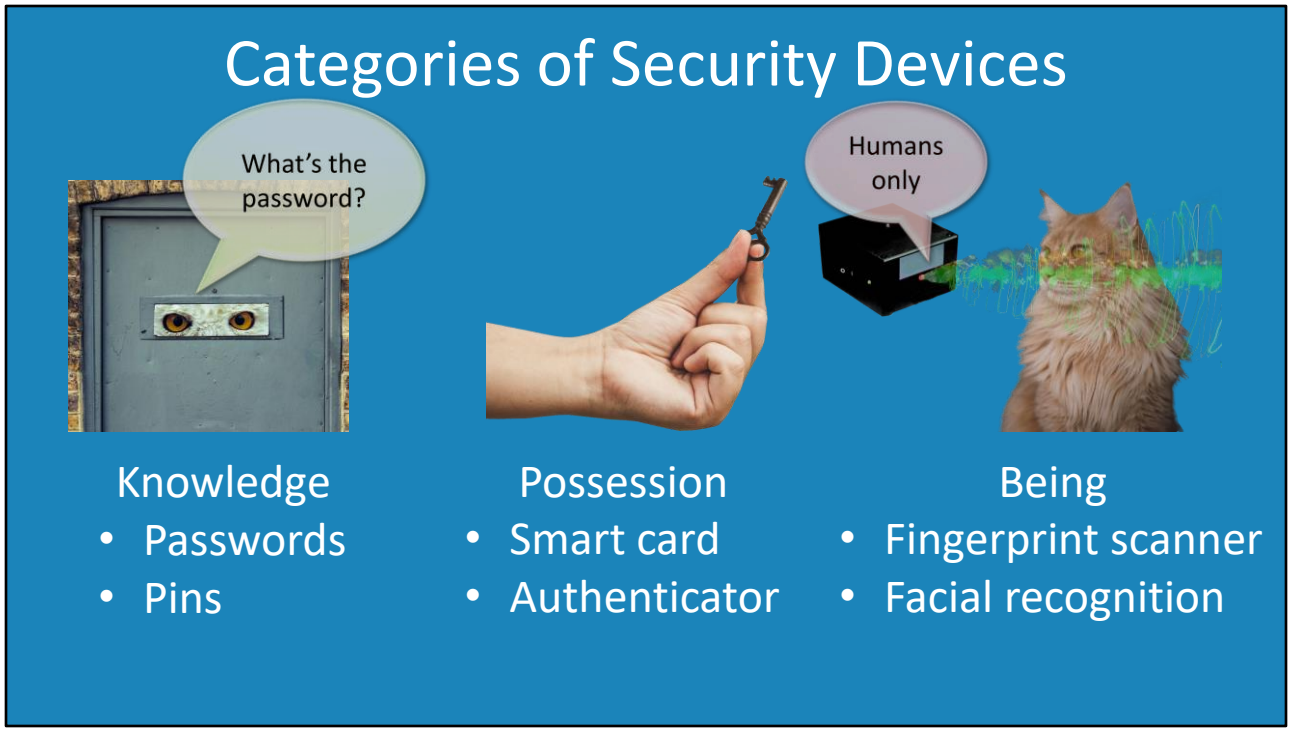
In this video from ITFreeTraining, I will look at Security Input Devices. Security devices are important, as they help protect against unauthorized access to computing devices and resources in your organization.



0:12 Before I start looking at some of the security devices that are available on the market, I will first look at the different categories security devices fall under. The first category is 'Knowledge'. Essentially this is knowing something like the password or a pin number. Only the people who require access should know the password or the pin number.

In this video, I won't be looking at these types of security devices since they are pretty self-explanatory. Whenever you type a password or enter a pin on a number pad this is a knowledge type of security device.

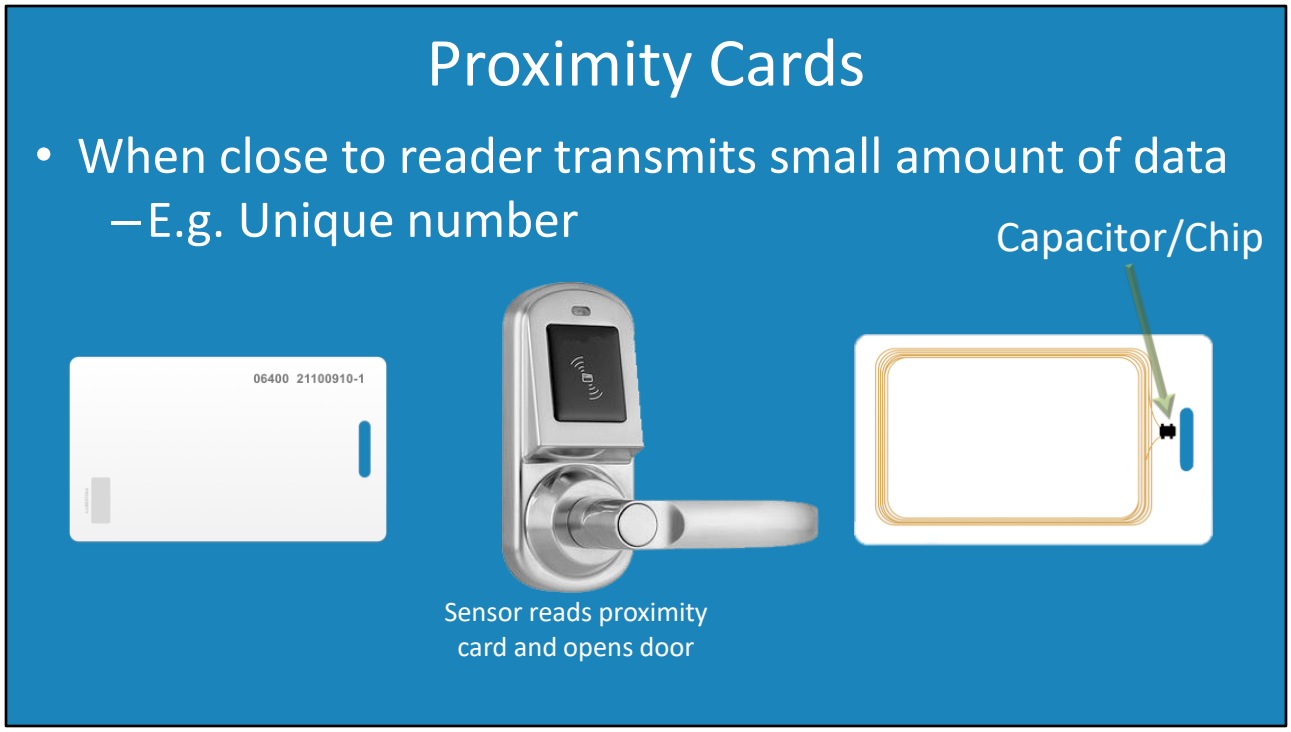
The next category is 'Possession'. This means that you need to have something in order to obtain access. In the old days this would have been a key, but nowadays security devices like these require physical items like smart cards or authenticators. If you need to be holding something in order to gain access, it is part of this category.

The last category is 'Being'. This is something physical about the person attempting access. For example, a fingerprint scanner or facial recognition. Essentially the device tests for something physical about the person. If the device does not detect the required physical characteristics then the person is denied access.

This covers the three basic categories. These are commonly referred to as 'Factors'. You may hear the term two-factor authentication. This is when two factors are used together. The most common is a password and a device like an authenticator. You could use all three categories at once which would essentially give you three factors of authentication; however, generally this

does not give much more security than two-factor authentication. For that reason, you generally only ever see three-factor authentication used in the movies.

To start with, I will look at some of the security devices that fit into the possession category of devices.



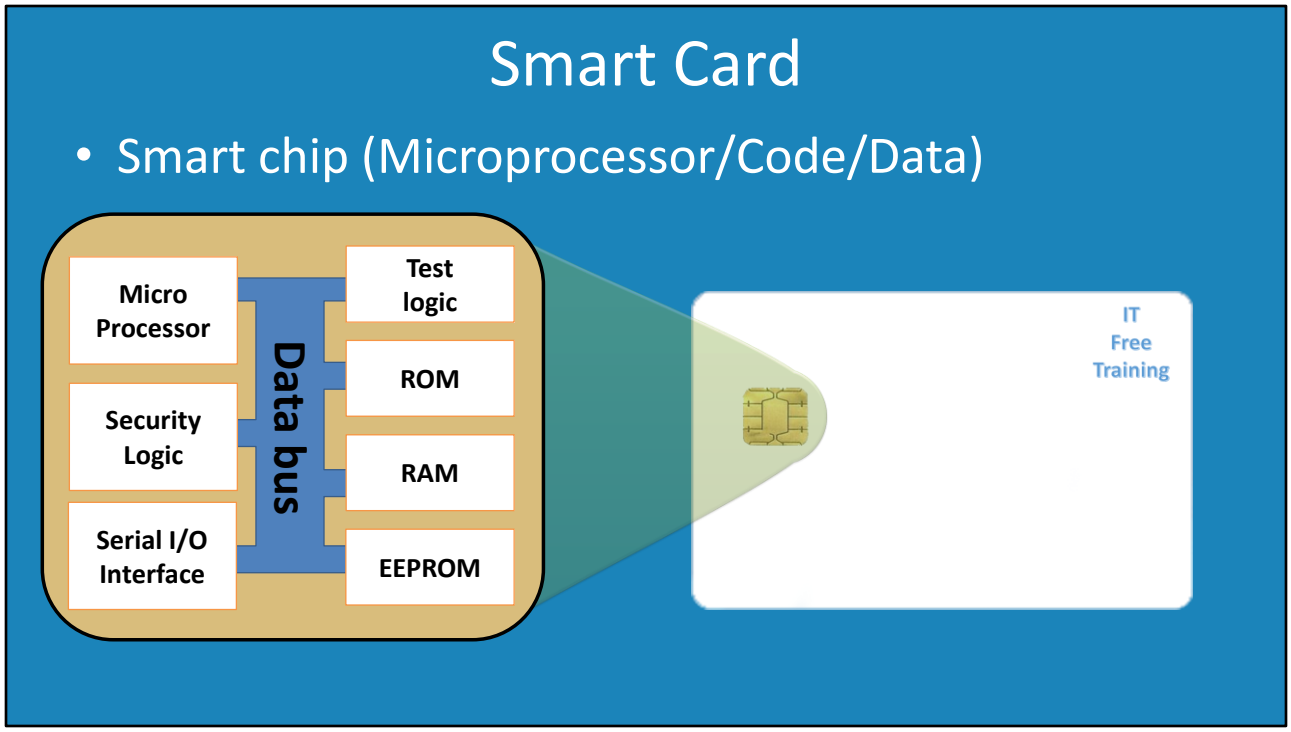
2:12 The first security device I will look at is a proximity card. A proximity or proxy card is a small plastic card. When the plastic card is put next to a sensor, commonly used to unlock doors, the proxy card transmits a small amount of data. This small amount of data is generally a unique number. The unique number identifies the proxy card and thus allows access. The basic idea being that the person who has the proxy card is allowed to have access.

For the CompTIA exam, you don't need to understand the inner workings of the proxy card, but I think knowing this helps you understand its uses and limitations.

The basic proxy card has wires wound in a circle or square called an antenna coil. When the proxy card is moved past the sensor, these wires pick up and store energy from an electric field. The electrical energy is stored using a capacitor. The capacitor stores electricity to power a small chip. Essentially a capacitor works like a battery which holds electricity for a very short amount of time. Once there is enough power, the chip can operate and transmit data so the sensor can read it.

Basic proximity cards are not very secure because you can make copies of them very easily. To make them more secure, more advanced proximity cards implement a password-like system on the card. In simple terms, the door sensor needs to supply a code in order to access the data on the proximity card. This prevents unauthorized copying since the attacker won't have the code to access the proximity card.

If you are planning to implement a proximity card system, it is a good idea to see how secure the system you are planning to implement is. Proximity cards are good for providing access, but since they only contain data, they are limited in what they can achieve. Let's have a look at a more advanced system.



4:09 One of the most common security devices that you will come across is the Smart Card. A smart card is essentially a piece of plastic. Nothing special about that, except the plastic contains a smart chip. The smart chip is a microprocessor containing code and data for the microprocessor, all in one chip.

To understand how this works, let's have a look inside the chip itself. For the CompTIA exam, you won't need to understand how the inside of the chip works, but I think having a basic understanding of the chip will give you a better understanding of what they can be used for and what they can achieve.

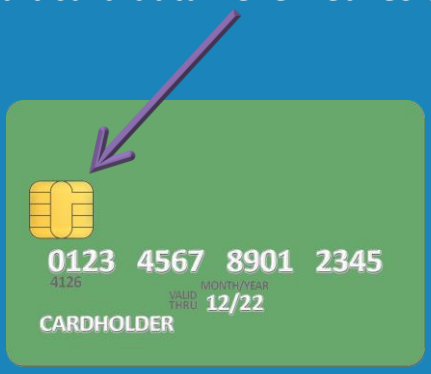
You can see, inside the chip, it contains many different parts. This provides the processing, data and interface to the chip just like how a microprocessor in a computer works; however, nowhere near as powerful. This essentially means that the chip can run small programs and return results. This raises the question, do different smart cards have different processing, memory and abilities. The answer is yes they do. Let's have a look at some of the different ways they are used.

Credit Cards

- Chip provides unique code for each transaction

Magnetic strip details can be copied

Credit card data never leaves chip



5:16 One of the more common examples of where you will find a smart card used is with a credit card. Traditionally, a credit card was read by a magnetic strip on the credit card being scanned. The problem with this approach is that the data on the magnetic strip can easily be copied and thus it is not very secure.

To get around this, a chip was added to the credit card. The process of how this works is quite complex. To explain it in the most basic way, the chip provides a unique code for every transaction. If an attacker was able to get hold of this code, as essentially this code is a one-use code, the code has already been used and it is of no value. Important information like the credit card data used for security never leaves the chip. This helps keep this information secure. In order to use a credit card or smart card you need some kind of device to read the data on the card.

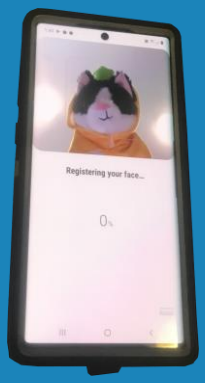
6:12 Traditionally, smart cards were read using a smart card reader or similar device. If I take the example of a credit card, the credit card has a number of contact points on the card. Inside the card reader are a number of contact pins which connect directly to these contact points when the card is inserted into the card reader.

You don't see as many card readers used as much nowadays. Devices like mobile devices still use a smart card reader to read the sim card inside the device. It makes sense to use them as the device will often store security codes, data and thus needs to access it all the time.

Nowadays you see a lot of contactless card readers instead of the traditional card readers. These devices work by using Near Field Communication (or NFC) to communicate with the smart card. Essentially, if the card is within close proximity to the reader, the electromagnetic signal generated by the reader powers the smart card and is also used to transfer data to and from the smart card. These are a lot easier to use then the smart card readers, so you can see why they have become popular.

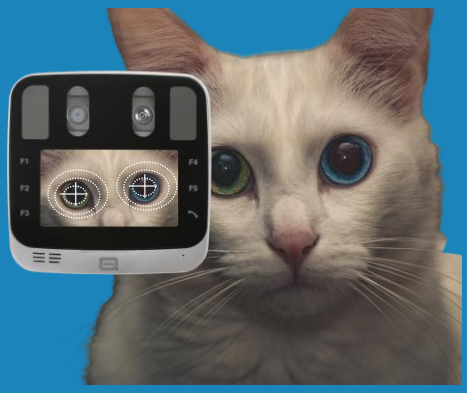
Biometric Devices

- Detect unique aspects of the human body



Face recognition

Fingerprint scanner



Iris recognition

7:21 The next security devices that I will look at are Biometric devices. Biometric devices detect unique aspects of the human body. For example, biometric devices exist that detect faces. This is becoming common place with mobile devices. The device will scan the face, and if it matches what it has saved, it will unlock the device.

The older devices did this by simply taking a photo and comparing it to what it had saved previously. The problem with this approach was that you could place a photo of the person in front of the device and the device would be tricked into providing access.

Nowadays, face recognition has improved to the point where it can look at the face in front of the device in 3D. This means the device cannot be defeated by simply putting a photo (of the person) in front of the device. Sometimes the device will not recognize the person even when the correct person is in front. This could come down to things like too little or too much light. If the person is wearing glasses, this can affect the device. On some devices there may be an option to improve face recognition, but this may reduce the security of the device.

The next device that I will look at is a Fingerprint Scanner. This device works by taking a scan of your fingerprint and matching it against what it has recorded in order to grant access. This can be affected by cuts on your finger or dirt on your hands or on the sensors. Fingerprints are developed while in the womb and thus even in the case of twins are different. It is very unlikely that two people will have the same set of fingerprints. Fingerprint scanners can have problems, if the person does a lot of manual labor. Long term manual labor can wear down the fingerprints making them harder for the fingerprint scanner to read them. Fingerprint scanners

have improved a lot and are commonly used on mobile devices.

The last biometric device that I will look at is Iris Recognition. This works by looking at the iris of the person. Not to be confused with retina scanners that scan the blood vessels at the back of the eye, iris scanners look at the iris of the eye itself. Basically, the part between the black pupil and the white of the eye. Irises are good for authentication because unlike fingers, they are protected by a highly transparent and sensitive membrane. This helps prevent them from getting damaged. Like fingers, since they develop in the womb, even in the case of twins, it is very unlikely that they will be the same.

Biometric devices are getting better but can sometimes not authenticate correctly even when the right person is using them. Depending on the type of sensor, too little or too much light can affect them, injuries like cuts, or wearing glasses can also affect them. Generally, if you are installing these devices, you would install them, so they are in a well-lit area, but not in direct sunlight.

Signature Pads

- Uses signature recognition to identify person

10:21 The last device that I will look at is a Signature Pad. A signature pad uses recognition to detect if the signature is the same as the one it has recorded previously for that person. You don't tend to see these used that much.

The problem with this approach is that the signature pads are often difficult to write on when compared to a piece of paper. As time goes on, a person's signature can change. A signature can also potentially be forged by another person. Generally, signature pads are not used so much for authentication, but more for recording a signature. For example, when you receive a package your signature may be recorded on such a device. A signature pad may also be used to record your signature on an electronic document. The point being most uses for a signature pad nowadays are not for authentication. Authentication is generally done using other methods, as they are more reliable than a signature.

That concludes this video on Security Input Devices. I hope this video helped you understand how these devices work, and may assist you developing them in your organization. Until the next video, I would like to thank you for watching.

References

"The Official CompTIA A+ Core Study Guide (Exam 220-1001)" Chapter 3 Position 13340-14046
"CompTIA A+ Certification exam guide. Tenth edition" Pages 406 – 409
"Multi-factor authentication" https://en.wikipedia.org/wiki/Multi-factor_authentication
"Picture: Door" https://unsplash.com/photos/x8ondX_bTpg
"Picture: Owl" https://unsplash.com/photos/c1fFv08N7qE

“Picture: Hand in the wilderness” https://unsplash.com/photos/uCOd7GEjJvk
“Picture: Key” https://unsplash.com/photos/CiMITAJtb6I
“Picture: Cat” https://unsplash.com/photos/13ky5Ycf0ts
“Smart card” https://en.wikipedia.org/wiki/Smart_card
“Proximity card” https://en.wikipedia.org/wiki/Proximity_card
“File:Fingerprint scanner in Tel Aviv.jpg” https://commons.wikimedia.org/wiki/File:Fingerprint_scanner_in_Tel_Aviv.jpg
“Picture: Close up picture of a cat” https://www.pexels.com/photo/close-up-photo-of-cat-2031419/

Credits
Trainer: Austin Mason http://ITFreeTraining.com
Voice Talent: HP Lewis http://hplewis.com
Quality Assurance: Brett Batson http://www.pbb-proofreading.uk