6.6.12 Smart Card Authentication Facts

This lesson covers the following topics:

- Smart cards
- Smart card benefits and weaknesses

Smart Cards

Smart cards are plastic cards similar to credit cards that have an embedded memory chip that contains encrypted authentication information. Be aware that smart cards:

- Use public key infrastructure (PKI) technology to store digital signatures, cryptography keys, and identification codes.
- Can authenticate a user when used in conjunction with a smart card reader connected to a computer system.
- Typically have RAM, ROM, programmable ROM, and a microprocessor integrated within the card itself.
- Have their own processor, allowing the card to perform its own cryptographic functions.
- Use a serial interface to connect to the card reader.
- Are powered externally by the smart card reader.
- Are generally considered to be tamper-proof.
- Can be divided into two categories:
  - Contact smart cards: these cards use a gold-plated contact pad that must physically touch the contact pad on a smart card reader.
  - Contactless smart cards: these cards do not require physical contact with the reader device. Instead, these cards use Radio Frequency Identification (RFID) technology to communicate with the smart card reader. An antenna is wound around the edge of the card and activated when the card is within proximity of the card reader.

Smart Card Benefits and Weaknesses

Key benefits of smart cards include the following:

- They provide tamper-resistant storage for a user's private key and other personally identifying information (PII).
- They isolate security-related operations from the rest of the system.
- They allow security credentials to be portable.

Smart cards are subject to the following weaknesses:

- Microprobing - this is the process of accessing the chip surface directly to observe, manipulate, and interfere with the circuit.
- Software attacks - these exploit vulnerabilities in the card's protocols or encryption methods.
- Eavesdropping - this captures transmission data produced by the card as it is used.
- Fault generation - this deliberately induces malfunctions in the card.