Something You Have: Smart Cards

- The smart card issues a “challenge” to the reader.
- The user is required to enter a PIN into the reader, and the reader computes a response to the challenge.
- If the smart card receives a correct response, the user is then considered authenticated, and access to use the secret information stored on the smart card is granted.
- One problem with using smart cards for authentication is that the smart card reader (into which the PIN is entered) must be trusted.

Something You Have: Smart Cards

- A rogue smart card reader that is installed by a bad guy can record a user's PIN, and if the bad guy can then gain possession of the smart card itself, he can authenticate himself to the smart card as if he were the user.

- While such an attack sounds as if it requires quite a bit of control on the part of the attacker, it is feasible.

Something You Have: Smart Cards

- For example, an attacker could set up a kiosk that contains a rogue smart card reader in a public location, such as a shopping mall.
- The kiosk could encourage users to enter their smart cards and PINs by displaying an attractive message such as “Enter your smart card to receive a 50 percent discount on all products in this shopping mall!”
- Such types of attacks have occurred in practice.

Something You Have: Smart Cards

- Attacks against smart cards have also been engineered by experts such as Paul Kocher, Cryptography Research-(www.cryptography.com)
- By studying a smart card's power consumption as it conducted various operations, Kocher was able to determine the contents stored on the card.
- While such attacks are possible, they require a reasonable amount of expertise on the part of the attacker.

Something You Have: ATM Cards

- ATM card is another example of a security mechanism based on some secret the user has.
- On the back of an ATM card is a magnetic stripe that stores data—namely the user's account number.
- This data is used as part of the authentication process when a user wants to use the ATM.