Something You Have: OTP Cards

- OTP products generate a new password each time a user log in.
- One such product, by RSA Security, is the SecurID card
- The SecurID card is a device that flashes a new password to the user periodically (every 60 seconds or so).
- When the user wants to log into a computer system, he enters the number displayed on the card when prompted by the server.

Something You Have: OTP Cards

- Server knows the algorithm that the SecurID card uses to generate passwords, and can verify the password that the user enters.
- Other variations of OTP systems as well:
- For instance, some OTP systems generate passwords for their users only when a personal identification number (PIN) is entered.
- Also, while OTP systems traditionally required users to carry additional devices, they are sometimes now integrated into personal digital assistants (PDAs) and cell phones.

Something You Have: Smart Cards

- New Gen smart cards are tamper-resistant, which means that if a bad guy tries to open the card or gain access to the info stored on it, the circuit within card will self-destruct.

- The microprocessor, memory & other components that make up the "smart" part of the smart card are epoxied (or glued) together such that there is no easy way to take the card apart.

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.