Final Notes on Authentication

- There are other factors that can be taken into account when conducting authentication. E.g. Alice’s location.
- Alice may carry around a cellphone that has a GPS chip inside of it.
- When Alice stands in front of an ATM requesting to withdraw money, Alice’s bank could ask her cellphone company’s computer system where she currently is.
- If the cellphone company’s computer responds with a latitude and longitude that corresponds to the expected location of the ATM, the bank can approve the withdrawal request.

Final Notes on Authentication

- However, if Alice’s ATM card and PIN were stolen by a bad guy who is trying to withdraw money, then taking Alice’s location (or specifically, the location of her cell phone) into account could help thwart such a fraudulent withdrawal request.

Final Notes on Authentication

- If Alice’s cellphone is still with her, when an attacker attempts to use her card at an ATM, the location of the ATM will not correspond to the location of Alice’s cell phone, and the bank will deny the withdrawal request (unless, of course, Alice and her cell phone are being held captive in front of the ATM).

- In this example, it is advantageous for Alice to keep her cellphone and her ATM card in different places; she should not, say, keep both of them in her purse.

Final Notes on Authentication: Internet

- In all the examples discussed so far, we have talked about people authenticating people or people authenticating themselves to computers.
- In Internet, computers are also interacting with other computers. The computers may have to authenticate themselves to each other because all computers cannot be trusted equally.
- There are many protocols that can be used to allow computer-to-computer authentication, and these protocols will, in general, support three types of authentication: client authentication, server authentication, and mutual authentication.

Final Notes on Authentication: Internet

- *Client authentication* involves the server verifying the client’s identity,
- *Server authentication* involves the client verifying the server’s identity, and
- *Mutual authentication* involves the client and server verifying each other’s identity.
- TLS/SSL used in https support client, server, and mutual authentication over the internet.

Final Notes on Authentication: Internet

- Whether client, server, or mutual authentication is done often depends upon the nature of the application and the expected threats.

- Many e-commerce web sites provide server authentication once a user is ready to make a purchase because they do not want the client to submit a credit card number to a spoofed or impostor web site.

- Spoofed web sites are a significant security threat because they do not cost much to set up.