# 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.