Authentication

- Authentication is the act of declaring something (e.g., a person, a message, or an item such as a car) to be authentic.
- An identity is said to be authentic if the claimed identity truly corresponds to the thing (person, message, car, etc.).
  - Example: a car for sale where the owner claims that the car is a Model T Ford.
- In our daily lives, we authenticate on a regular basis!
  - With our friends, we recognize their faces.
    - Sometimes we make mistakes, e.g., at a long distance from our “friend’s” face.
  - We also provide evidence (e.g., a driver’s license) to allow others to authenticate our claims.
Integrity

• Integrity
  • Whole; complete

• Message integrity
  • Verification that a message has not been altered after being sent
  • Example: you want to transfer funds from bank account 1 to bank account 2, and bank 1 needs to verify that the destination bank account has not been changed
Old Fashioned Identity Authentication: Signatures

• Handwriting one’s name has been used for millennia
  • Difficult for others to copy
  • Once a contract is signed, the parties are held responsible
Message Authentication

- Message authentication is the act of declaring a message to be authentic
  - Example: receive an email from a foreign country claiming some kind of difficult personal situation
  - Financial example: log in to a secure bank web page and access your account to pay a bill
    - Step 1: https://bankname.com
    - Step 2: enter username
    - Step 3: enter password
    - Step 4: click on billpay and enter amount you want to pay to company X
    - ...

©Georgia Institute of Technology, 2018
Message Authentication (continued)

• A message is authenticated if the identity of the sender is authenticated and the integrity of the message is verified
  • Step 1: identity authentication
  • Step 2: integrity verification
Authentication and Repudiation

• Once a sender is authenticated, nonrepudiation does not allow the sender to later claim that the sender did not send the authenticated message

©Georgia Institute of Technology, 2018