Authentication Part I: Terminology

ECE 4156/6156 Hardware-Oriented Security and Trust

Spring 2024

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Reading

- Handbook of Applied Cryptography, Chapter 1
- Intro to Modern Cryptography, Chapter 1

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

Entity Authentication

- Entity authentication is also known as identification
- Entity authentication is the act of declaring an identity to be authentic
  - Example: receive an email from a person Mira from a foreign country claiming some kind of difficult personal situation
    - Is the person really Mira with the actual difficult situation, or is the person who sent the email an imposter trying to take your money?
  - 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: see an image you preselected (e.g., a specific waterfall) and enter password

Old Fashioned 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
- Form of entity authentication for written documents

Authentication Requires 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
- Handbook of Applied Cryptography, Chapter 1, Table 1.1, page 3 refers to this concept as *data integrity*

Message Integrity is also Referred to as Message Authentication

- Message authentication is the act of declaring a message to be authentic
    - Example: receive an email from Mira claiming some kind of difficult personal situation
        - Mira did send you a message at the time indicated, but did she claim the difficult situation or did someone alter the message without her knowledge/consent?
    - 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
        - …

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

Confidentiality or Privacy

- Keeping information provided only to those intended to or authorized to receive the information

That’s It for Now

- We will add new terminology as needed!