Authentication I

Cryptographic Hardware for Embedded Systems ECE 3170

Fall 2025

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Reading Assignment

- Please read Chapter 3 of the course textbook by Schneier

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 – in other words, even if the message is from you, if the destination is changed to an adversary's bank in transit, then message integrity has been violated

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 #1: receive an email from a foreign country claiming some kind of difficult personal situation
  - Example #2: 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
    - …

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

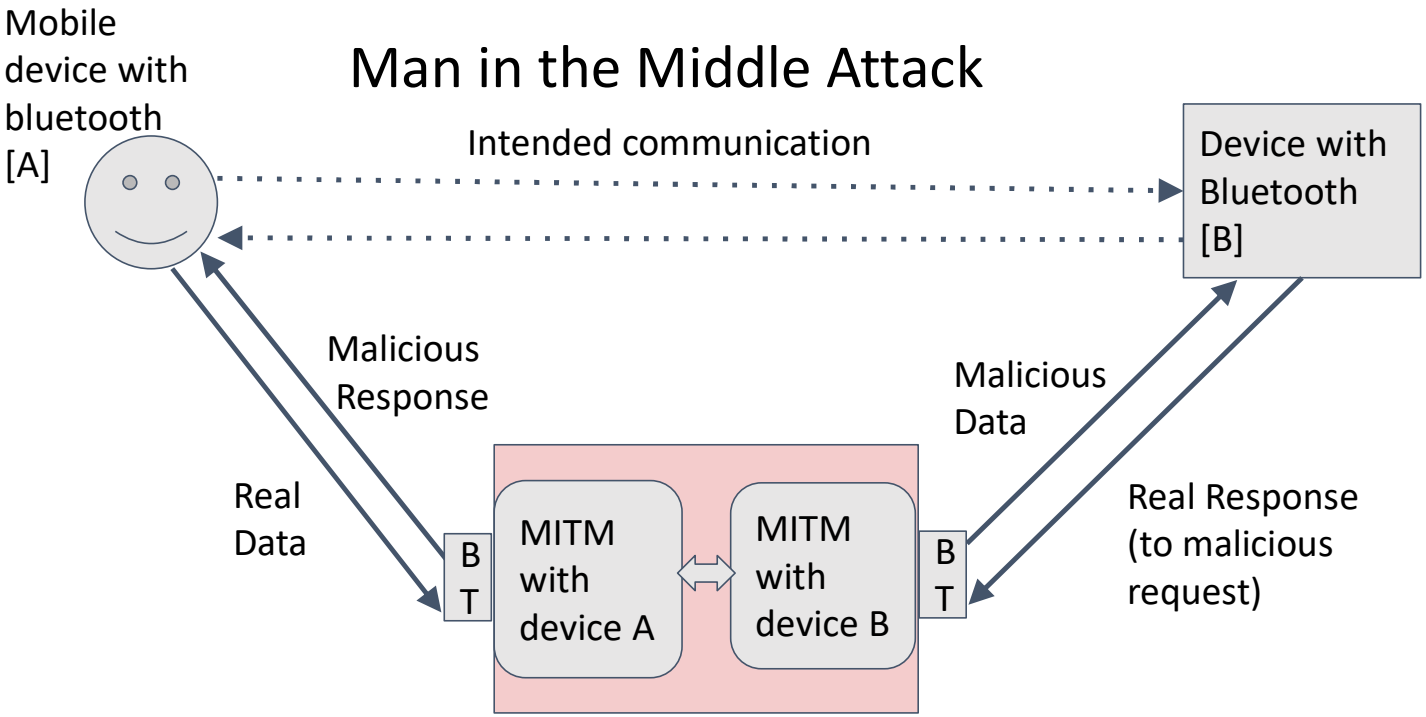
Protocols

- A protocol is a series of steps involving two or more parties designed to accomplish a task.
  - Everyone involved in the protocol must know the protocol and all of the steps to follow in advance
  - Everyone involved in the protocol must agree to follow it
  - The protocol must be unambiguous, the steps must be well defined, and there must be no change of misunderstanding
  - The protocol must be complete, i.e., there must be a specified action for every possible situation

First Attempt to Communicate Securely

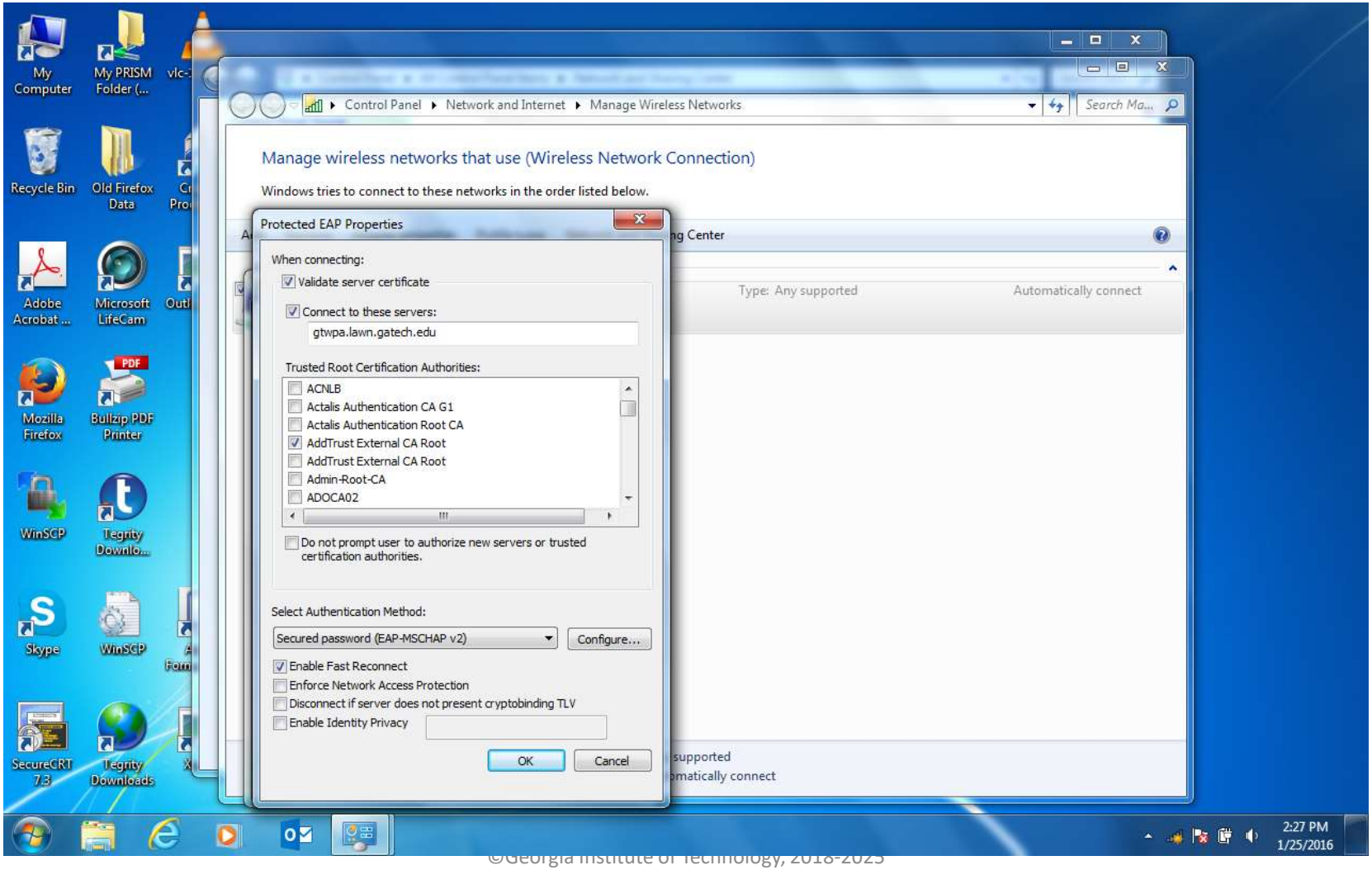
- Alice and Bob agree on a cryptosystem
- Alice and Bob agree on a symmetric key
- Alice takes her plaintext message and encrypts it using the encryption algorithm and the key, creating a ciphertext message
- Alice sends the ciphertext to Bob
- Bob decrypts the ciphertext message with the same algorithm and key and reads it

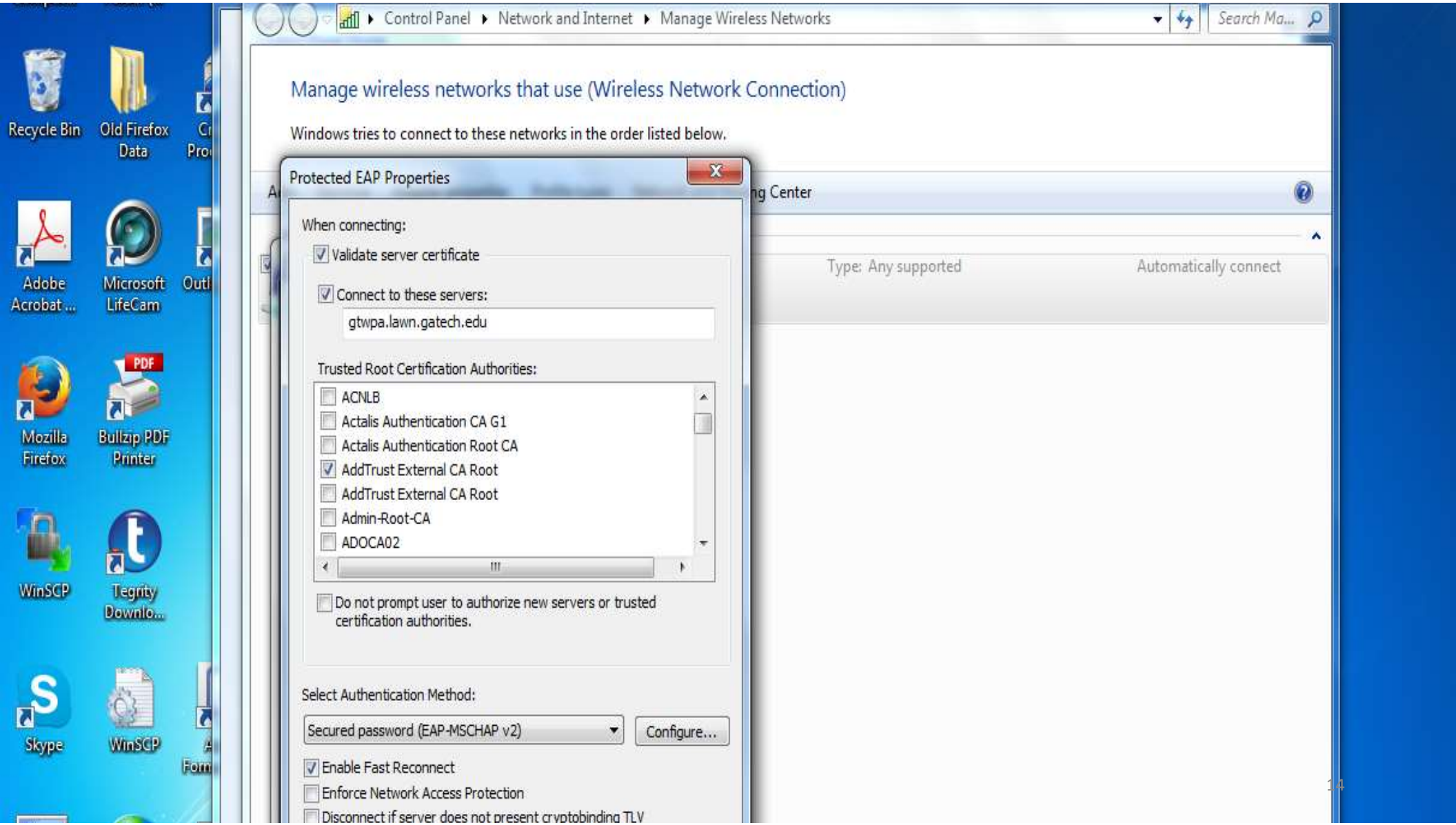
Threat Scenario

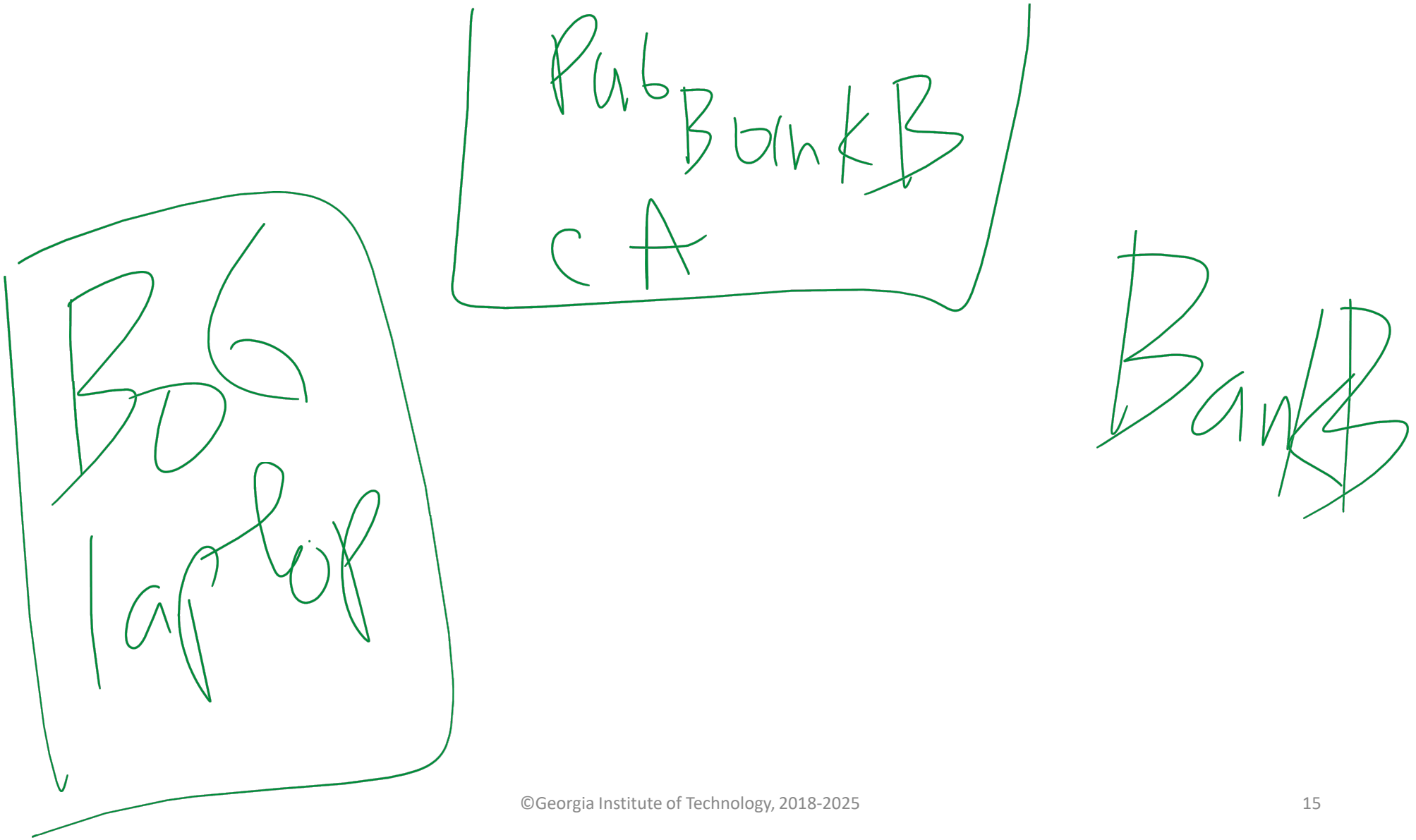


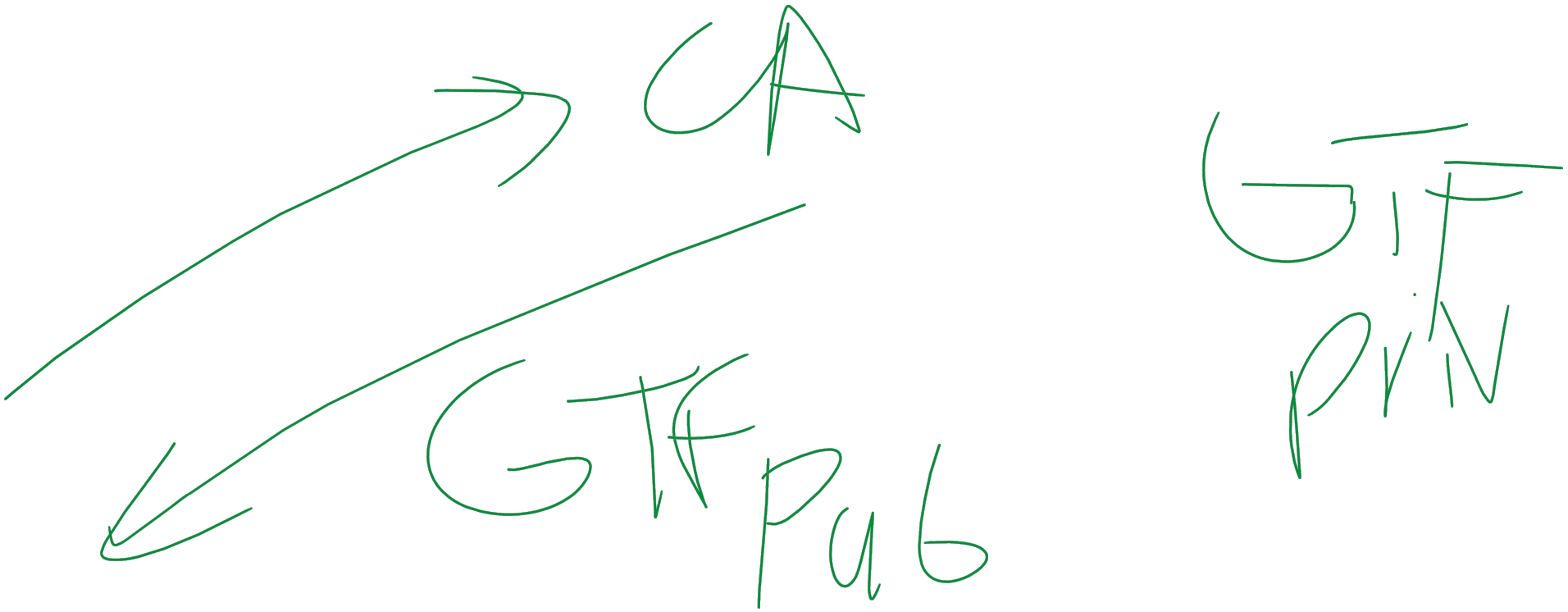
A Second Attempt to Communicate Securely

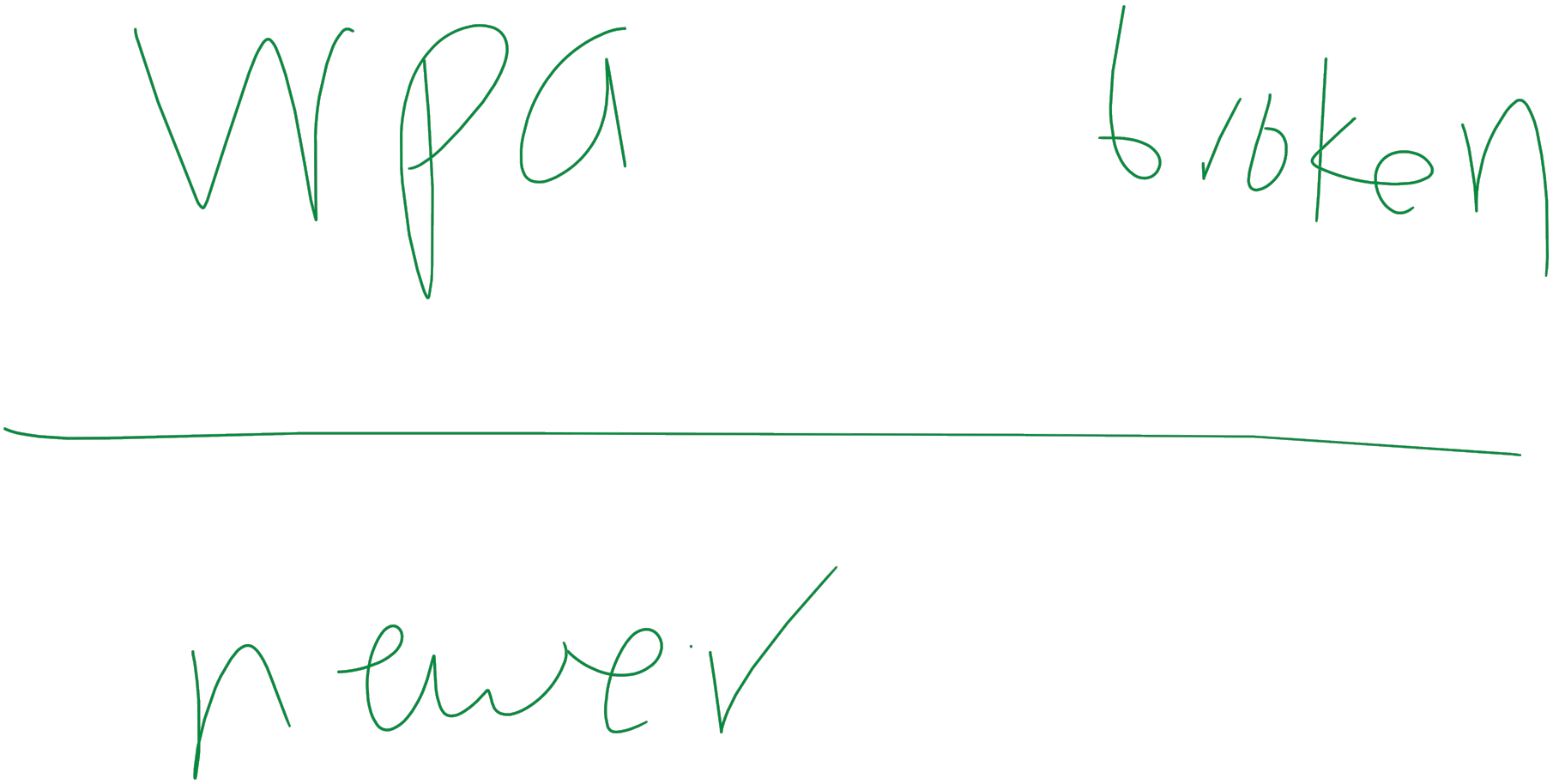
- A public key cryptosystem infrastructure is made widely available
- Alice obtain's Bob's public key from the infrastructure
  - E.g., using a certificate authority (CA)
- Alice encrypts her message using Bob's public key and sends the message to Bob
- Bob then decrypts Alice's message using his private key




Control Panel ▸ Network and Internet ▸ Manage Wireless Networks
Search Ma...
Manage wireless networks that use (Wireless Network Connection)
Windows tries to connect to these networks in the order listed below.
Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
gtwpa.lawn.gatech.edu
Trusted Root Certification Authorities:
ACNLB
Actalis Authentication CA G1
Actalis Authentication Root CA
AddTrust External CA Root
AddTrust External CA Root
Admin-Root-CA
ADOCA02
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Enforce Network Access Protection
Disconnect if server does not present cryptobinding TLV
Type: Any supported
Automatically connect
Recycle Bin
Old Firefox Data
Adobe Acrobat ...
Microsoft LifeCam
Mozilla Firefox
Bullzip PDF Printer
WinSCP
Tegrity Downlo...
Skype
WinSCP





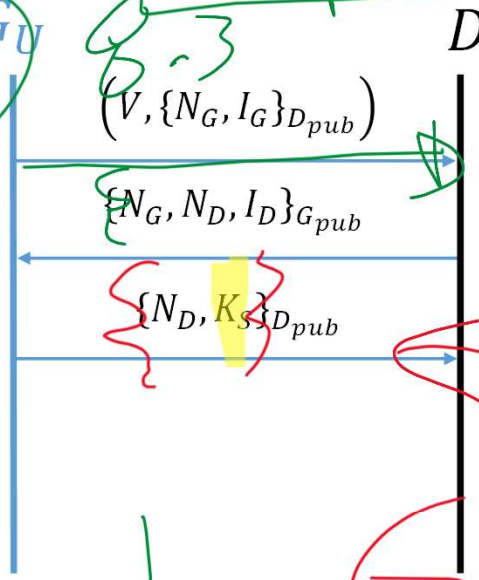


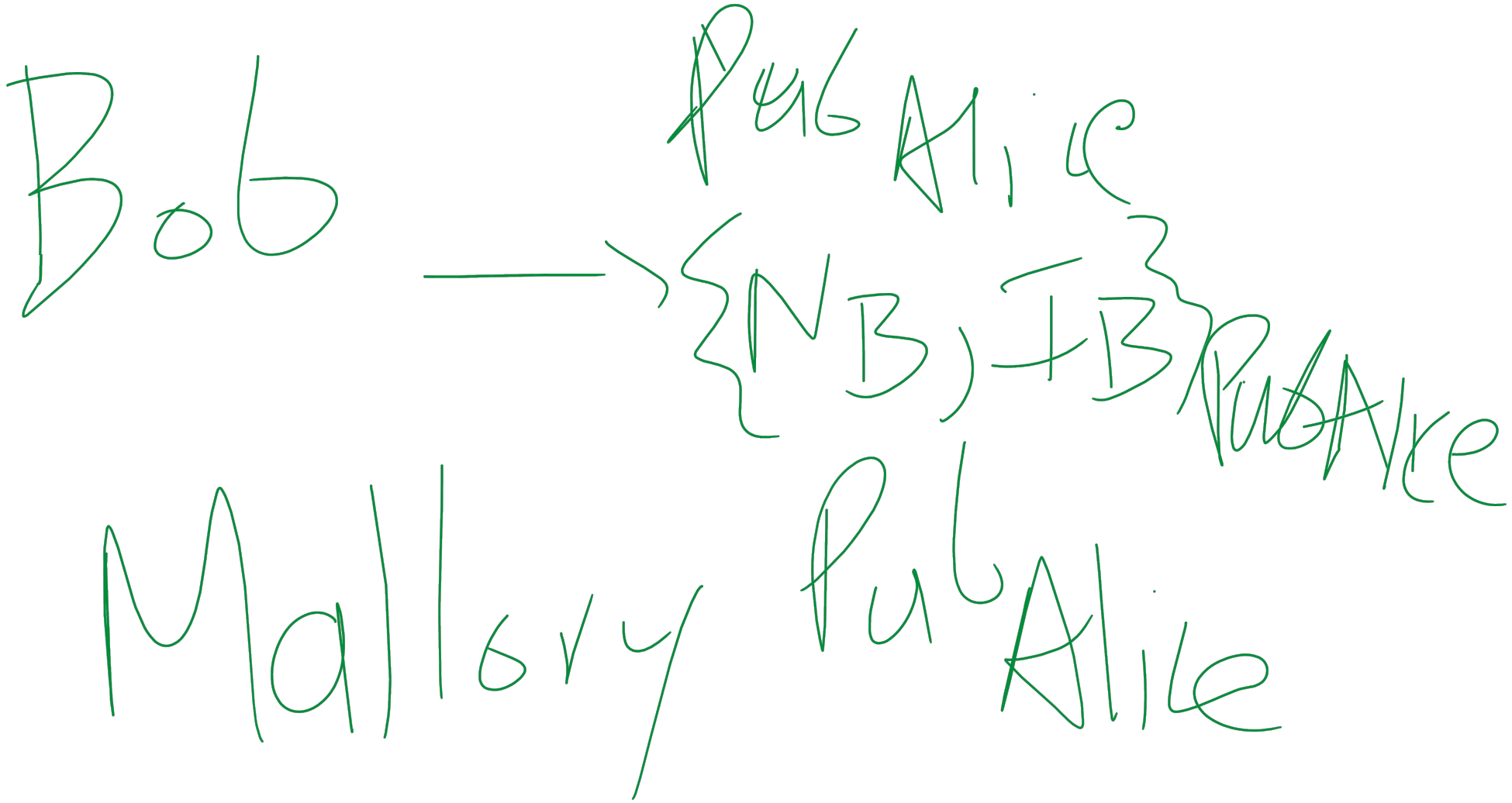
Notation

- D: target device
- G_U: updating organization
- (G_{pub}, G_{prv}): updating organization key pair
- (D_{pub}, D_{prv}): device key pair
- N_G, N_D: organization and device nonces
- I_G, I_D: organization and device identifiers
- V: incoming update version number
- K_s: symmetric key
- U: update image
- H: hash of the update image
- H_U : update hashes sent by G_U
- $\{M\}_{D_{pub}}$: message M is encrypted using key D_{pub}
  - Notation is common to both symmetric and asymmetric encryption (e.g., $\{M\}_{K_s}$)
- $(G \rightarrow D : M)$: organization G sends M to device D
- $(G \leftarrow D : M)$: device D sends M to organization G

Authentication Phase Using Public Key Crypto

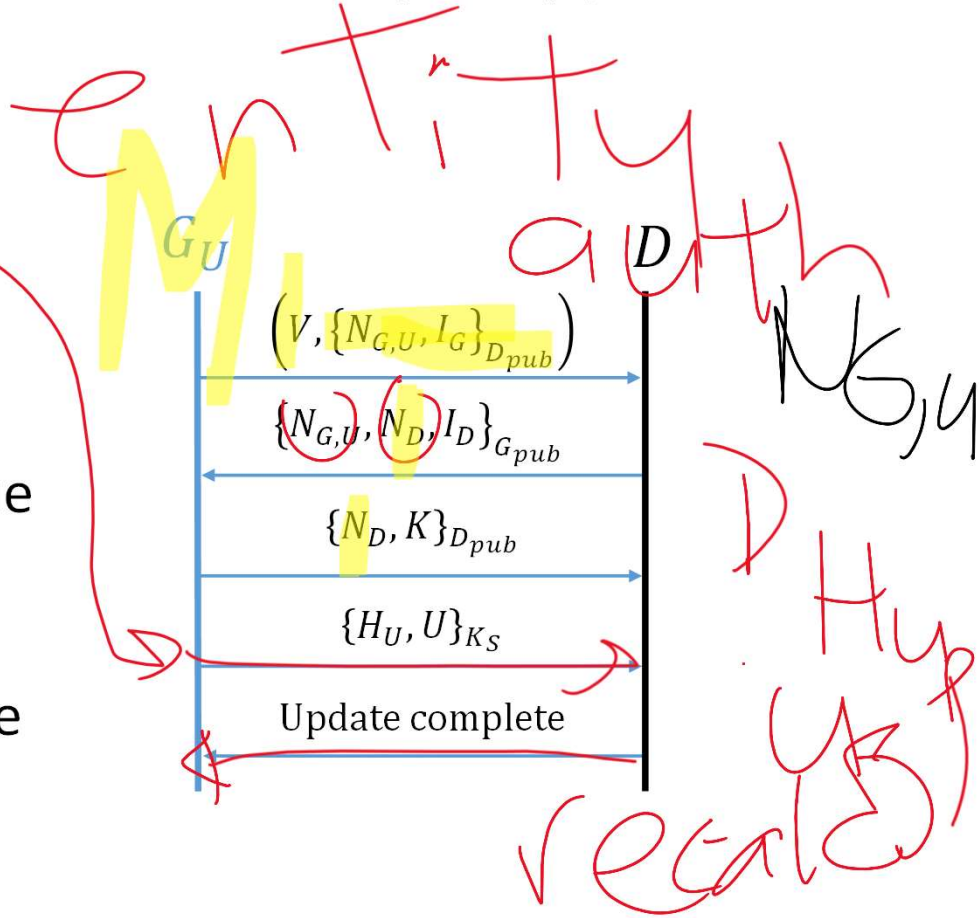
1. Organization nonce N_G and identifier I_G sent to device
2. Device retrieves N_G, then appends its own nonce N_D and identifier I_D
3. Finally, organization responds with N_D and symmetric key K_S

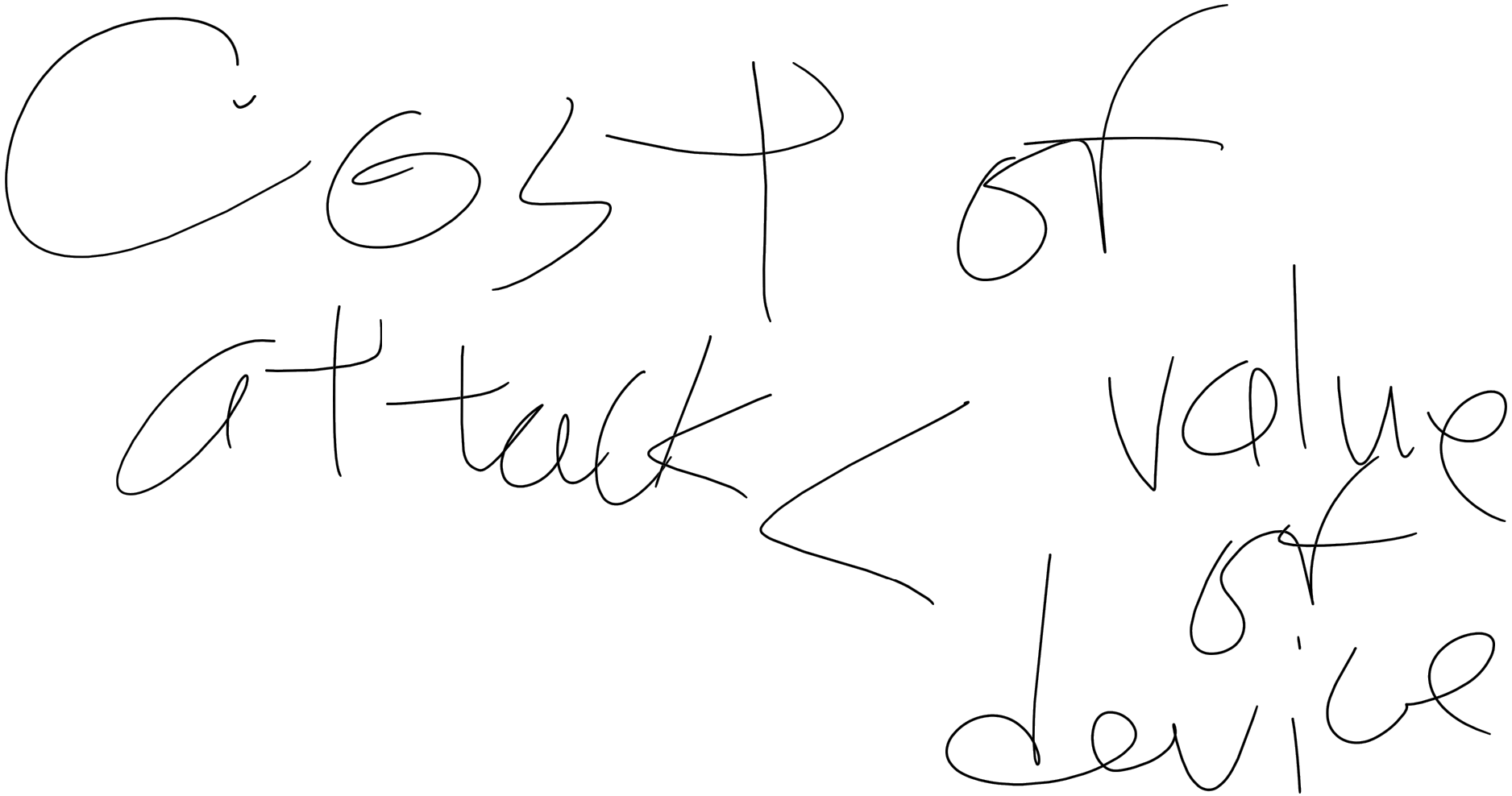




Update Phase Using Symmetric Key Crypto

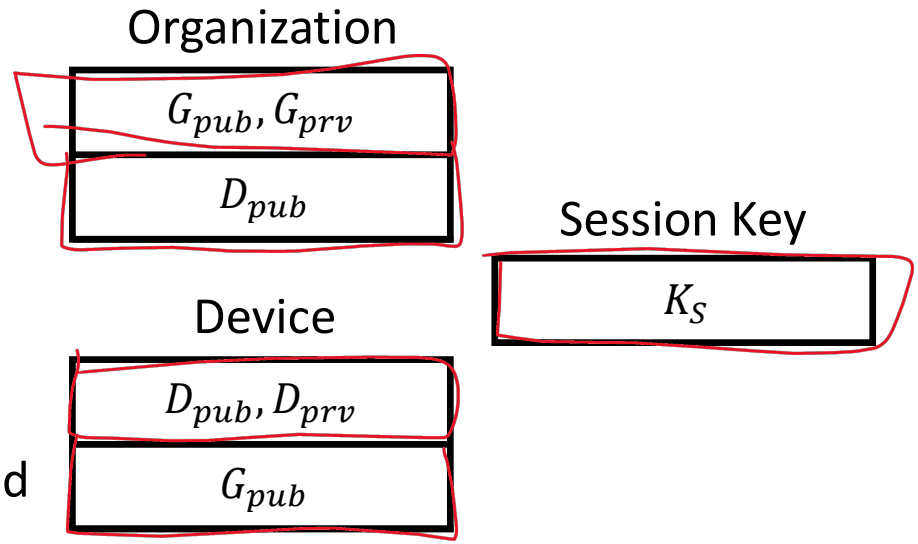
4. Organization sends update U and hash of the update H_U using the and symmetric key K_S
5. Device decrypts the message and checks that the (keyless) hash value H_U is obtained on the update U
6. Finally, D sends an encrypted message indicating that the update is complete





Long Term Asymmetric Keys, Short Term Symmetric Session Key

- New symmetric session key generated by updating organization on every update
  - Shared during authentication phase
- Advantages
  - Decryption of update code faster than asymmetric
  - Higher security
- Disadvantages
  - Device has a higher implementation overhead in order to support asymmetric as well as symmetric crypto

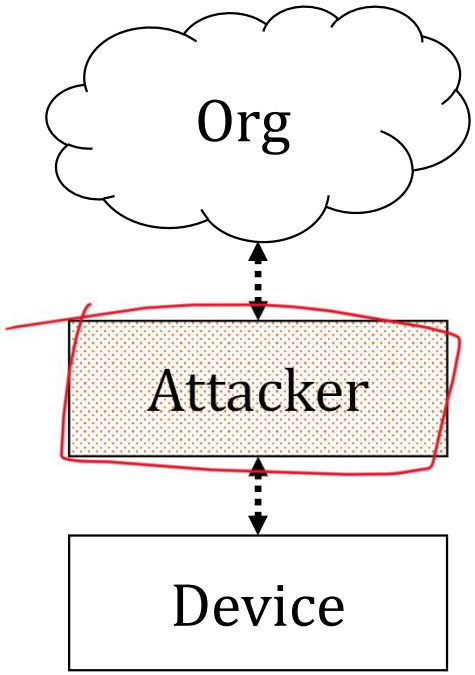


Security Analysis

1. Man in the middle
2. Replay attack
3. Organization spoofing

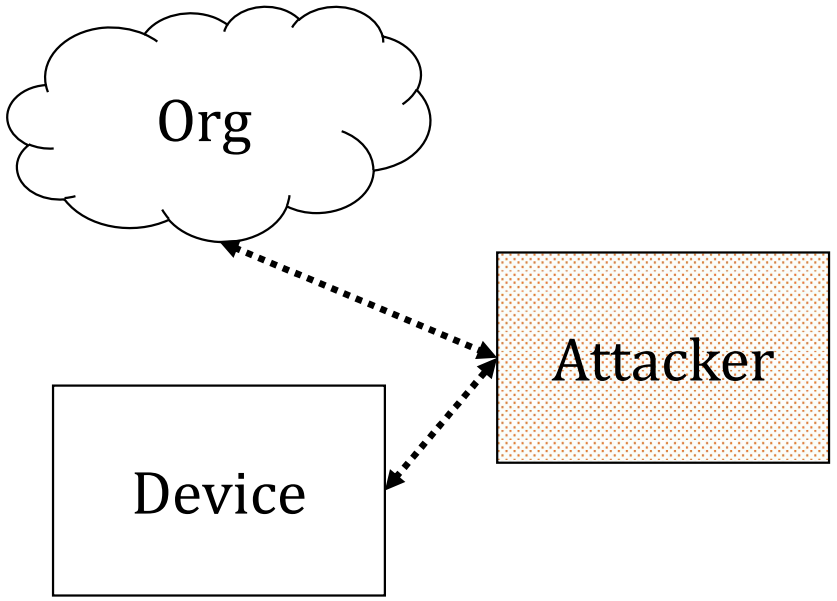
Man in the Middle

- Attacker tries to place himself between the updating organization and the device
- Attack fails because
  1. Authentication requires possession of private key
  2. All communication is encrypted
- Note that the assumption is that the public keys are correct



Replay Attack

- Attacker saves previous authentication and replays it
- Replay will be denied
  - Nonce used prevents successful replay



Organization Spoofing

- Attacker claims to be the updating organization
  - Pushes out malicious update
- Authentication will fail
  - Organization public key statically stored on Device
- Device will deny the update