Carnegie Mellon CyLab
CONFIDENCE FOR A NETWORKED WORLD

SafeSlinger

Easy-to-Use and Secure Public-Key Exchange

Michael Farb (CMU), **Yue-Hsun Lin (CMU)**, Tiffany Hyun-Jin Kim (CMU),
Jonathan McCune (Google), Adrian Perrig (CMU/ETH)

Setting: Key Distribution in Groups

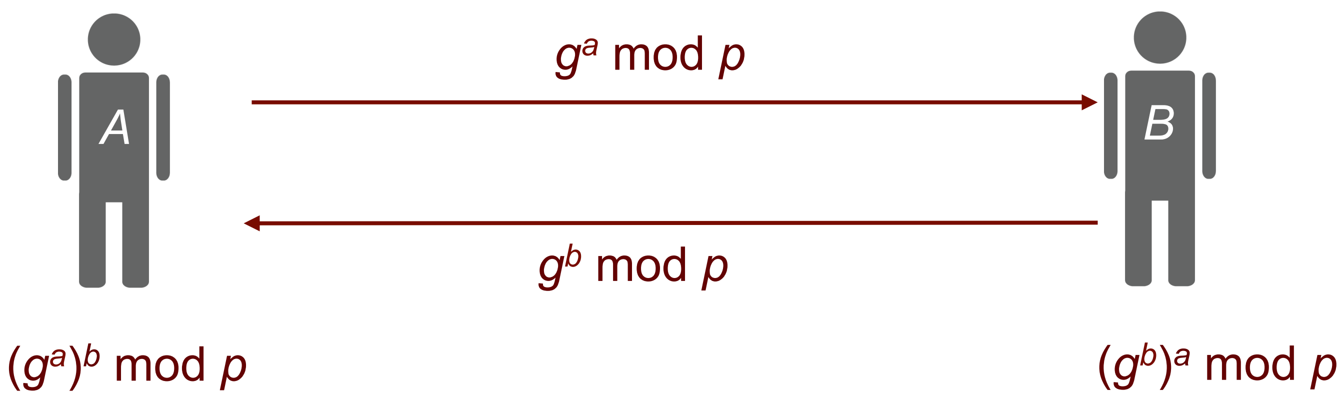
- Exchange information to secure communications
  - Cryptographic Keys
- People meet & want to communicate securely later
  - Researchers at a conference
  - Business people at a lunch
- Challenge: No commonly trusted infrastructure

Prior Solutions

- PKI (Public-Key Infrastructure)
  - Assumptions: TTP (Trust Third Party)
    - Certification Authority (CA)
  - Still vulnerable to Man-in-The-Middle attacks
  - Disconnect between physical & digital world
    - Attacker can likely acquire a certificate for any name
- PGP (Pretty Good Privacy)
  - Sequential broadcast of key and announcement of hash is cumbersome
    - Difficult for people to detect attack
  - A distribution list is cumbersome and insecure
    - Need to count # of people
    - Need to compare lists

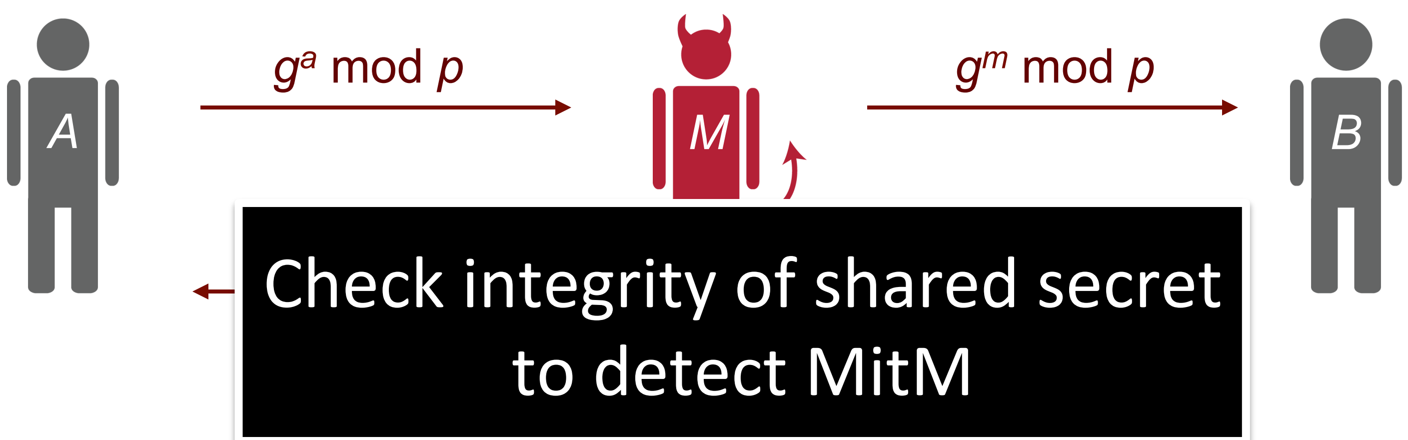
Diffie-Hellman Exchange Protocol

- *Goal*: *Establish shared secret between two parties for further use*
  - Public values: large prime p, generator g
  - Secret values: Alice (A) has secret a, Bob (B) has secret b
  - *Share Secret* $g^{ab} \pmod{p}$

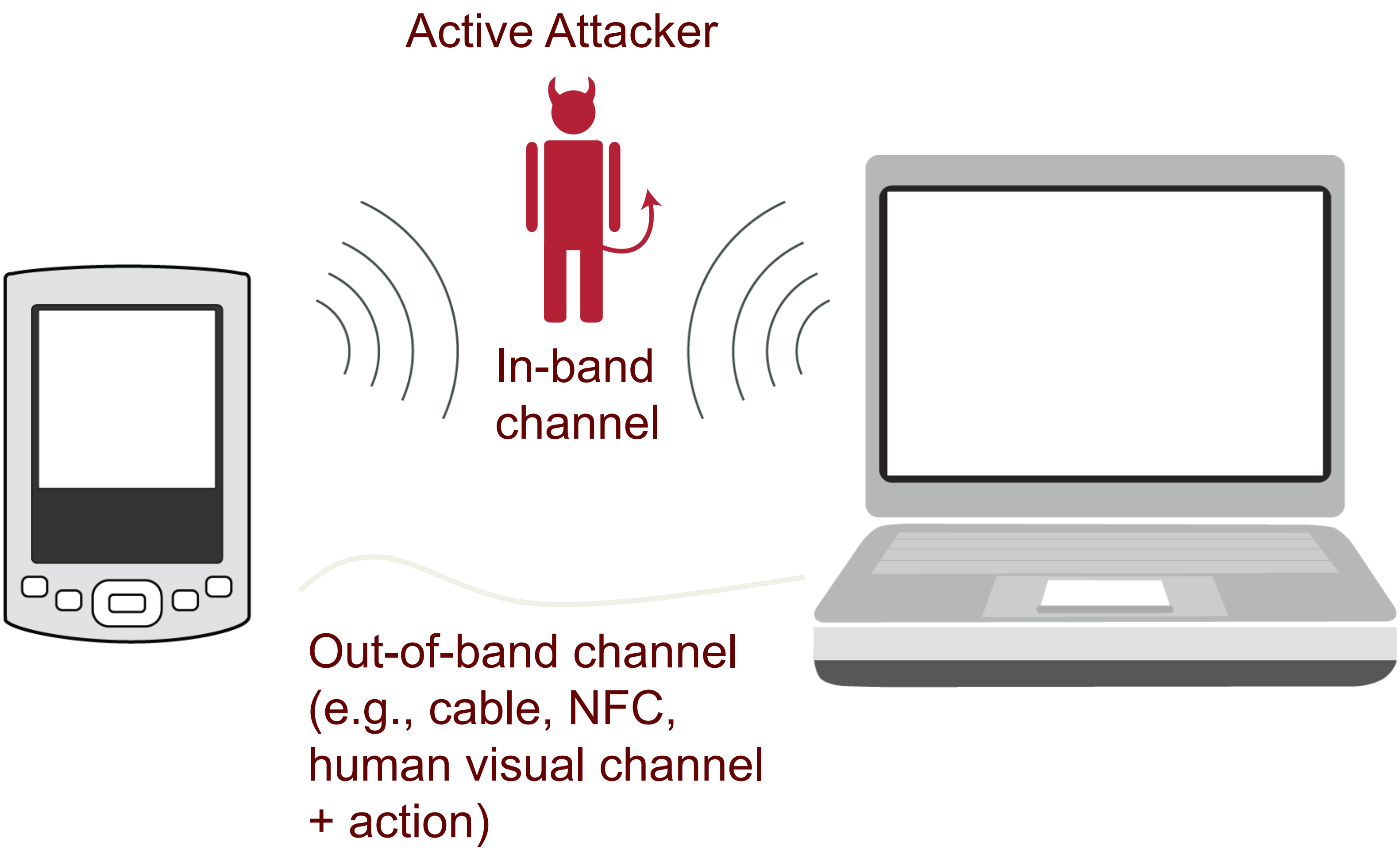


Problem: Man-in-the-Middle Attack

- Problem: Malicious *M* impersonates Alice to Bob and Bob to Alice
  - Wireless is invisible
  - Neighbors can easily launch MitM



Out-of-band Channel to defend MitM

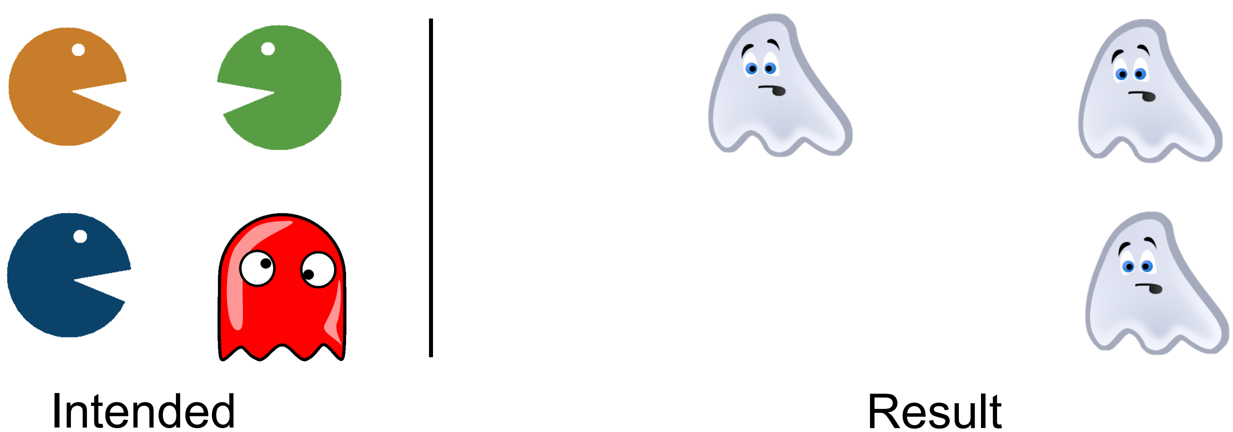


Issues of Out-of-band Channels

- Inconvenient in group settings
  - Scalability: N members must perform $O(N^2)$ interactions
    - Most OOBs are designed for *pairwise* associations
    - For a group of 10, we need 45 interactions
      - i.e., combinations of 2 from 10
  - Efficiency: Most of OOBs are slow

Group-in-the-Middle Attack (GitM)

- Settings
  - All members share secret
  - All members know number of members present
- Problem: Attacker can separate the intended group to multiple groups



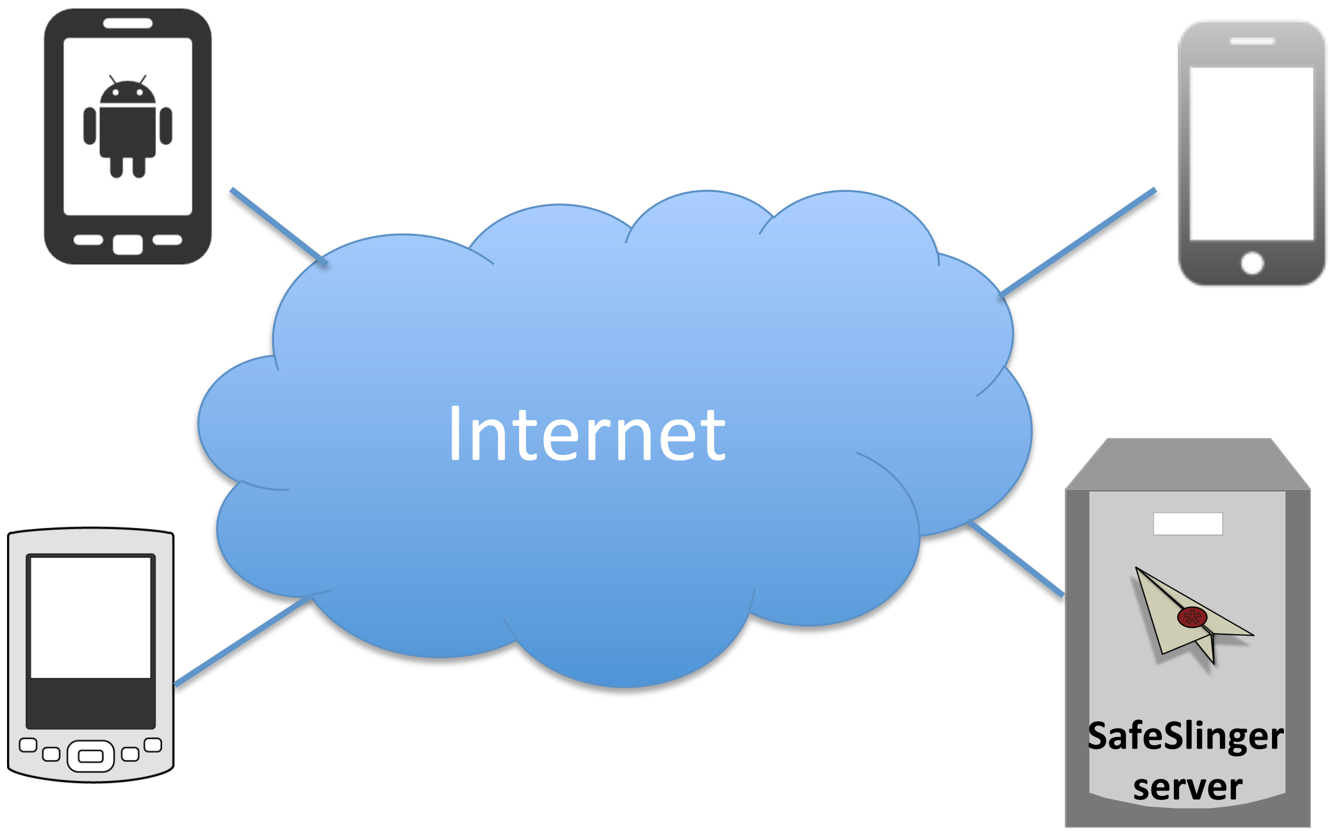
SafeSlinger Goals

- Goal: Exchange authentic information between group members
  - Scalability: Avoid N^2 interactions in a group
  - Authenticity: Each user should obtain the correct contact information associated with each other member
  - Secrecy: Only intended entities receive the information
  - Usability: Easy to use
  - Portability: support heterogeneous platforms

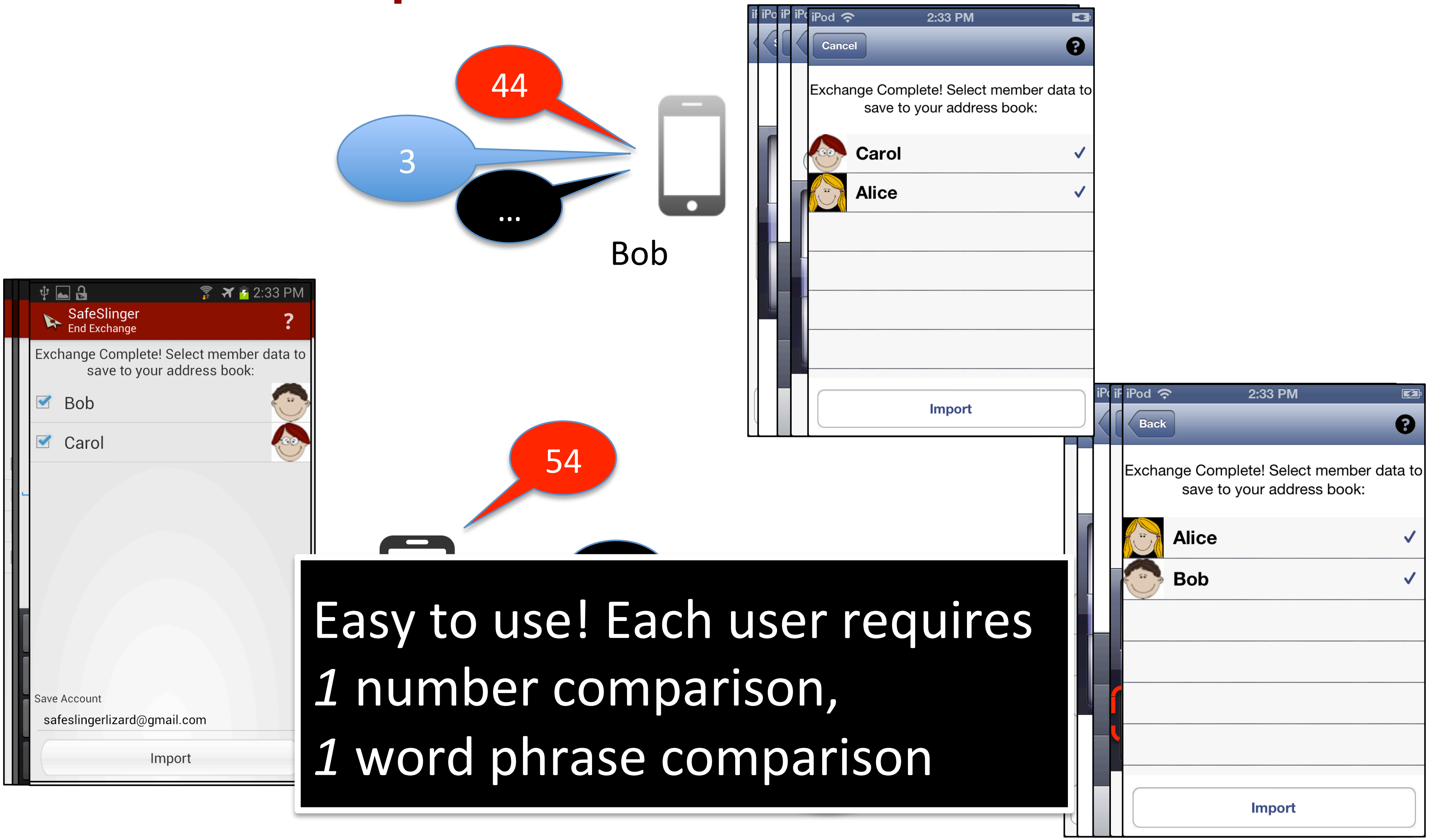
- Provide subsequent mechanisms based on authentic public keys

SafeSlinger Communication

- Devices connect via Internet to SafeSlinger server
- Sidesteps Bluetooth / WiFi communication problems



Simple User Interactions



Easy to use! Each user requires
1 number comparison,
1 word phrase comparison

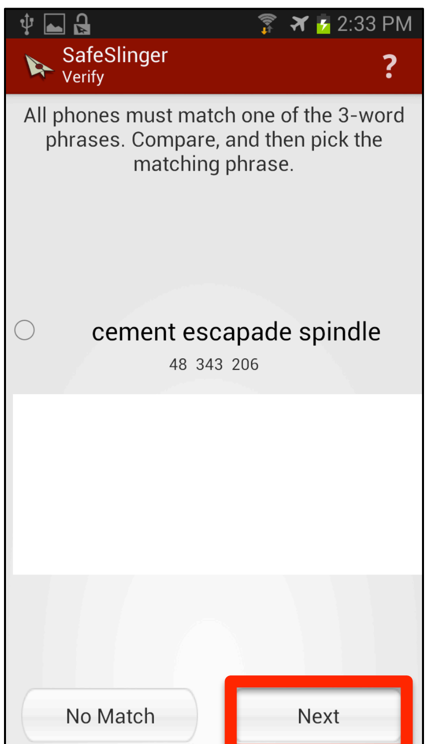
Challenge 1: Private Information Leak

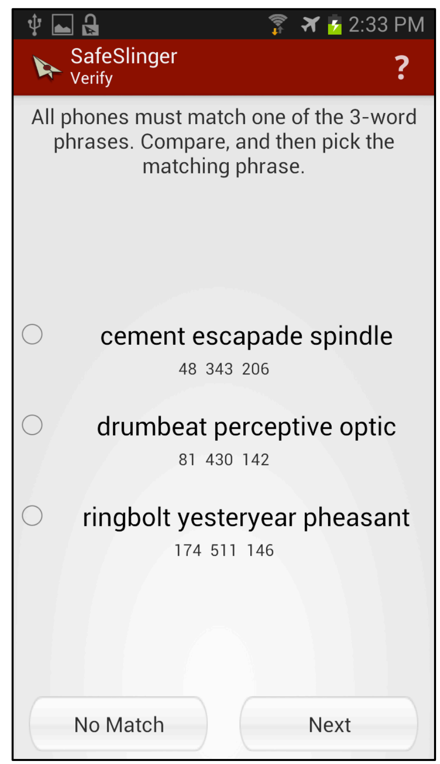
- Server learns contact information of all users
- Approach
  - STR protocol[1] used to create a shared secret key under which all information is encrypted
  - Only if all verifications succeed, decryption key is disclosed to intended individuals

1. Y. Kim, A. Perrig, and G. Tsudik. Group key agreement efficient in communication, *IEEE Transactions on Computers,* 53(7):905–921, July 2004.

Challenge 2: Prevent Dialog Failure

- Users simply click “Next” without checking phrases
- Approach: Make users pay attention!



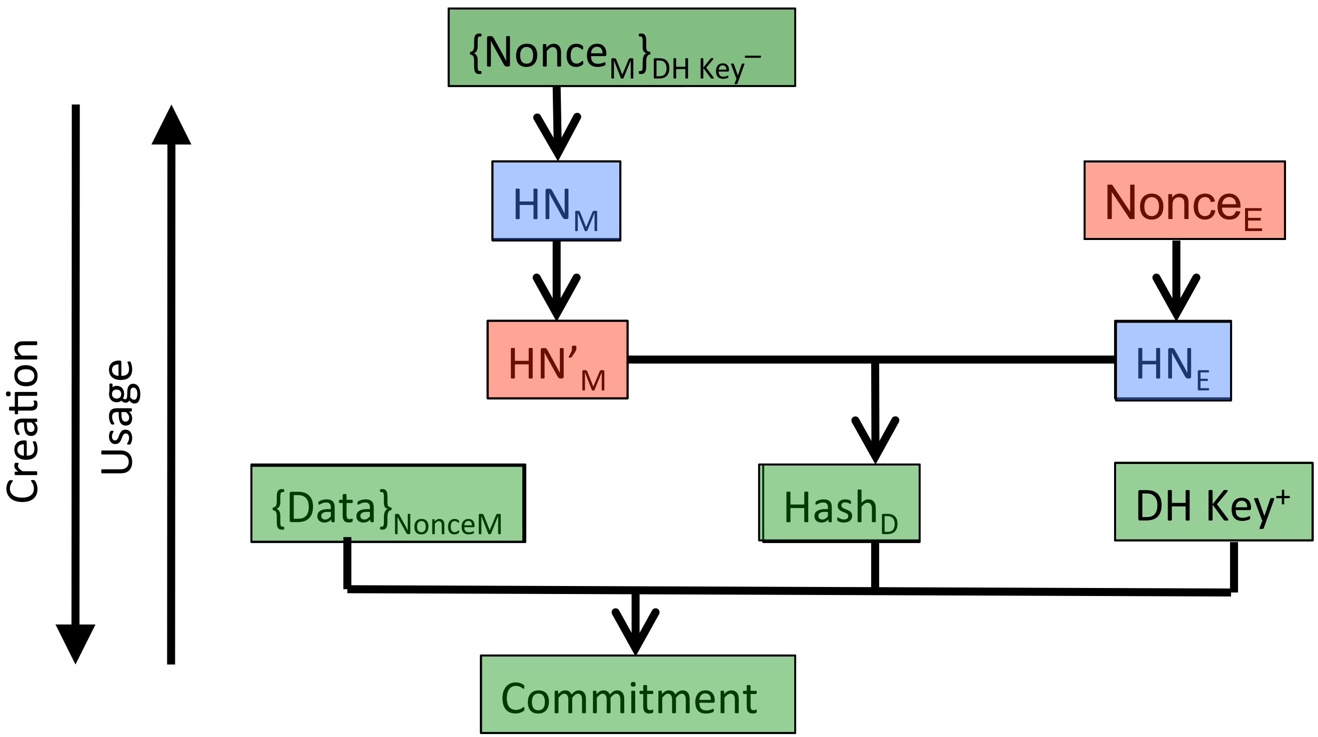


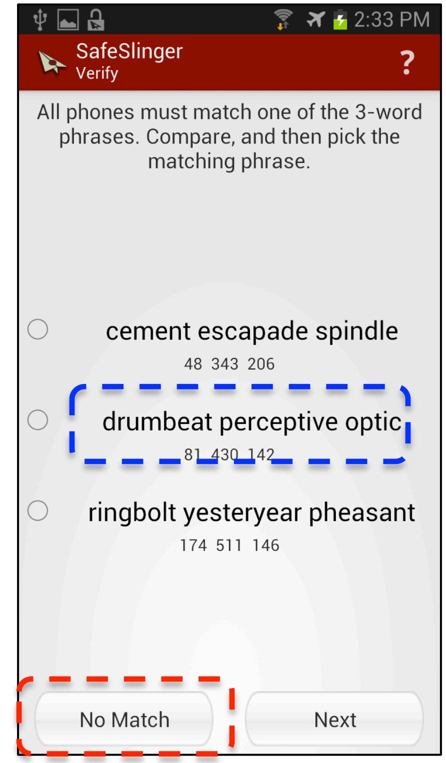
User has to pay attention and select matching phrase!

Challenge 3: No Information Revealed on Protocol Failure

- When protocol fails, no user information is revealed to anyone else
  - All-or-nothing property
- Approach: Commitment tree with several commitment stages

Commitment Tree





- "→" indicates Cryptographic Hash Function (SHA3)
- "$\{x\}_K$" represents encryption with key K

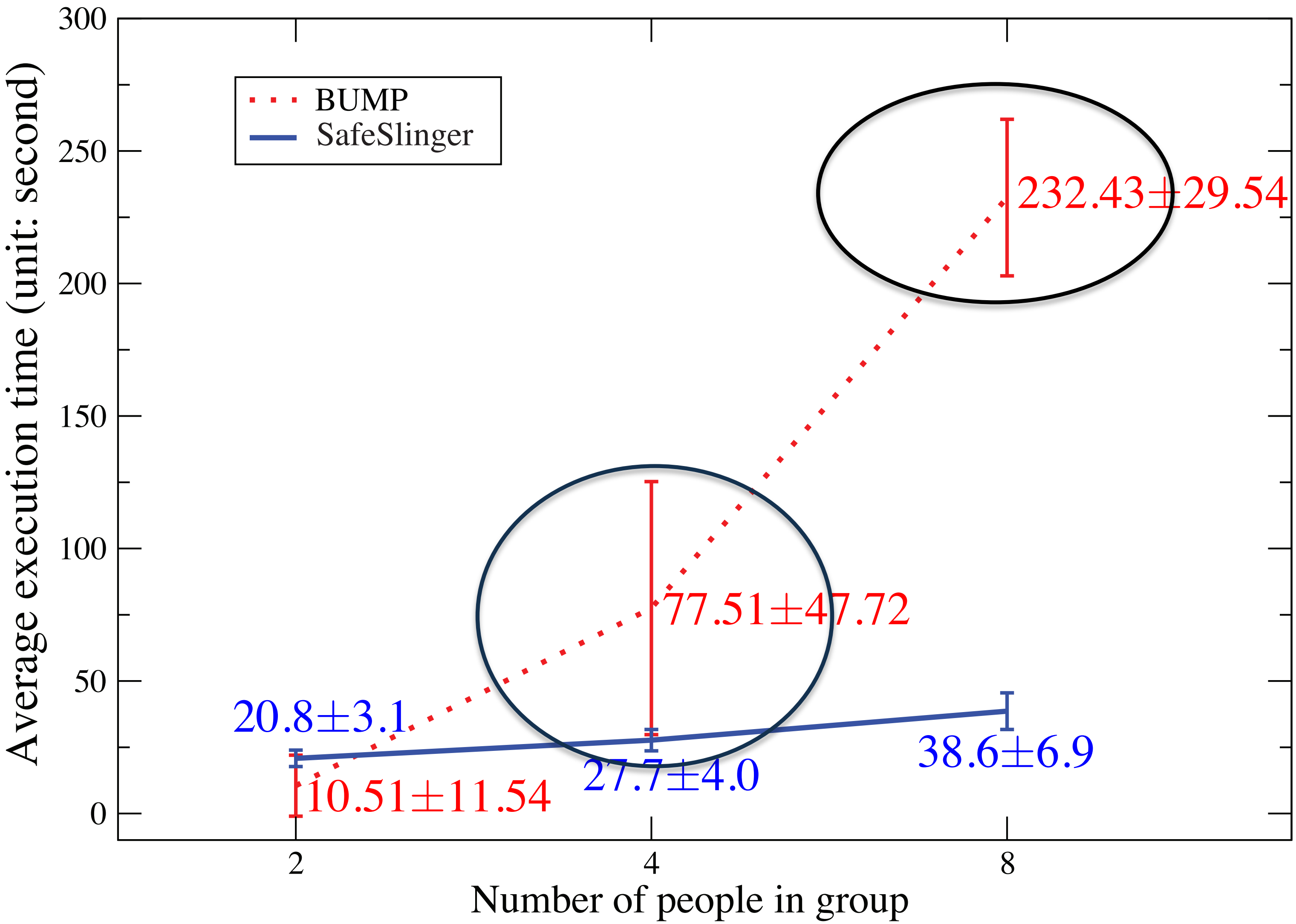
Challenge 4: GitM Attack

- Malicious group member performs Group-in-the-Middle (GitM) attack
- Approach
  - Users enter number of participants
  - All users compare word list with other users (word list simplifies comparison)
  - Commitment tree makes GitM attack a daring attack (success probability = 2^{-24})

Evaluation

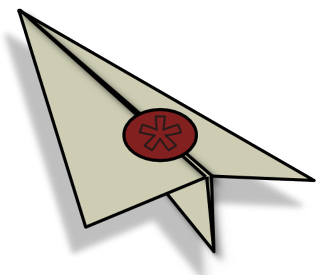
- Goal: measure efficiency of contact exchange
- User study settings
  - Baseline comparison with Bump
  - Recruited 24 users
  - Separate into groups: 2 (small), 4 (middle) and 8 (large)
  - Each group runs either Bump or SafeSlinger in random order to exchange contact information
  - Repeat exchanges multiple times

Performance Results



Summary

- Maintains user privacy
  - Only group members learn exchanged information
  - Server does not learn information
- Simple to use and resilient to user errors
- Supports Rich Applications
  - Secure text and file messaging
  - Secure Introduction
- Webpage: http://www.cylab.cmu.edu/safeslinger/
- Apps are available on Apple Store/Google Play
- Future work:
  - Open source to spur adoption for developers
  - Develop plugins for email and messenger clients



Backup: Group-Diffie-Hellman Key Agreement (STR)

- Notation for each node: (private key, public key)

$$\left(K = g^{z\cdot g^{xy}}, g^{g^{z\cdot g^{xy}}}\right)$$

$$\left(g^{xy}, g^{g^{xy}}\right) \qquad \left(z, g^{z}\right)$$

$$\left(x, g^{x}\right) \qquad \left(y, g^{y}\right)$$

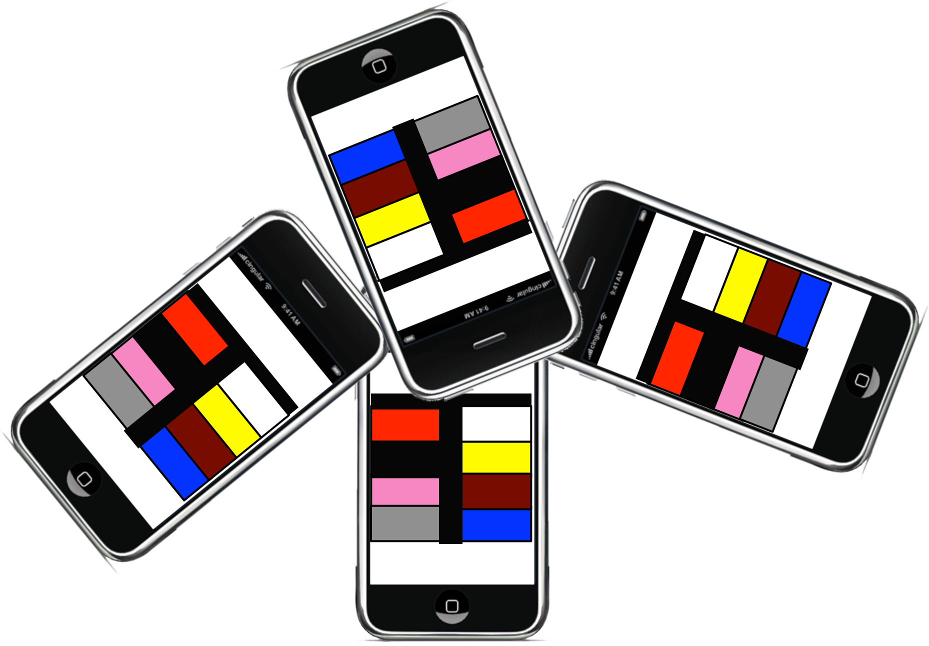
*mod p is omitted to simplify description

Related Work: SPATE [Lin et al. 2009]

Small-group PKI-less Authenticated Trust Establishment

- Efficient
  - Member performs 3 actions
    - Select data
    - Count group size
    - Compare
- Simple comparison
  - Only 1 user needs to pay attention

Verification



- Count the number of people present
- Compare the various checksums (T-Flag)

Issues in SPATE

- T-Flag comparisons makes protocol secure if and only if users are diligent
  - All “Match” signatures: save data
  - “Error” or no signature: discard data
- Dialog failure: Users click “OK” to continue
- What if the slow user found a problem?
- Execute locally (physically presented)

Backup: SafeSlinger Protocol

Multi-Commitment Generation

Data Selection & Counting

1. $U_i \xrightarrow{UI} M_i$: D_i (the data to be exchanged)

   $U_i \xrightarrow{UI} M_i$: $\tilde{N}_i$ (number of people in the group)

Commitment, Group DH Key Setup

2. M_i : $Nm_i \xleftarrow{R} \{0,1\}^{\ell}$ ("match" nonce)

   $Hm_i = H(Nm_i), Hm'_i = H(Hm_i)$

   $Nw_i \xleftarrow{R} \{0,1\}^{\ell}, Hw_i = H(Nw_i)$ ("wrong" nonce)

   $HN_i = H(Hm'_i || Hw_i)$ (multi-value commitment)

   $n_i \xleftarrow{R} \{0,1\}^{\ell'}, G_i = g^{n_i} \bmod p$ (group DH key)

   $E_i = \{D_i\}_{Nm_i}$ (encryption of data)

   $C_i = H(HN_i \,||\, G_i \,||\, E_i)$ (commitment)

3. $M_i \rightarrow S$: C_i

SafeSlinger Protocol (con't)

Authenticity Verification Round

Server Unique ID Assignment, User Grouping

4. $S \rightarrow M_i$: ID_i (unique ID per user)
5. U_i : find lowest unique ID among users $\rightarrow ID_L$
6. $U_i \xrightarrow{UI} M_i$: ID_L (enter lowest ID)
7. $M_i \rightarrow S$: ID_L

Collection and Distribution of Initial Decommitment

8. $S \rightarrow M_i$: ID_j, C_j $(j \neq i)$
(other users' ID and commitment)
9. $M_i \rightarrow S$: HN_i, G_i, E_i
$S \rightarrow M_i$: HN_j, G_j, E_j $(j \neq i)$
(other users' decommitments)
10. M_i : $C_j \stackrel{?}{=} H(HN_j||G_j||E_j)$ $(j \neq i)$ (verify)

Word Phrase Comparison of Integrity of Commitments

11. M_i : WordPhrase($[H(HN_*, G_*, E_*)]_{24}$) (screen)
$U_i \xrightarrow{UI} M_i$: Select Matching 3-Word Phrase
12. $M_i \rightarrow S$: **if** "no match" or wrong phrase selected:
Send Hm'_i, Nw_i, Abort protocol.
13. $M_i \rightarrow S$: **else if** "match" & correct phrase selected:
Send Hm_i, Hw_i
14. $S \rightarrow M_i$: Hm_j, Hw_j $(j \neq i)$
15. M_i : $HN_j \stackrel{?}{=} H(H(Hm_j)||Hw_j)$ $(j \neq i)$ (verify)
Abort if any verification failed

SafeSlinger Protocol

Secret Sharing Round

Group DH Key Establishment

16. M_i : Computation of group DH tree
K = Private key of root node (see Section 3.2)

Distribution and Verification of Data Decryption Key

17. $M_i \rightarrow S$: $\{Nm_i\}_K$
$S \rightarrow M_i$: $\{Nm_j\}_K$ $(j \neq i)$

18. M_i : Decryption of Nm_j $(j \neq i)$
$Hm_j \stackrel{?}{=} H(Nm_j)$ $(j \neq i)$ (verify)

Decryption of Data and Contact Import

19. M_i : Decryption of E_j with Nm_j $(j \neq i) \rightarrow D_j$

20. $U_i \xrightarrow{UI} M_i$: Save user data D_j $(j \neq i)$

Probability Analysis for MitM

- Phrases comparison converts the safe attack to the daring attack
- Analyze MitM attack success probability based on user behavior
  - All users are lazy: randomly pick one phrase to continue
    - $(1/3)^n$ when the group has *n* members
    - Unlikely to happen because decoy phrases makes the protocol aborts in high probability
  - Some users turns to be “partial diligent”

Partial Diligent Cases (1/2)

- At least one word match (upper bound)

$$P_1 \leq P(A \cap B \neq \emptyset) = 1 - \frac{\binom{254}{2} \cdot \binom{255}{1}}{\binom{256}{2} \cdot \binom{256}{1}} \cong 1.94\%.$$

- The first word exactly matches

$$P_2 \leq P(A_1 = B_1) = 1 - \frac{\binom{255}{1}}{\binom{256}{1}} \cong 0.391\%$$

Partial Diligent Cases (2/2)

- The first and second words match

  $P_3 \leq P((A_1=B_1)\&(A_2=B_2))=P_2*(1/256)=1.525878\text{e-}5$

- Whole phrase matches (diligent user)
  $P_4 \leq P((A_1=B_1)\&(A_2=B_2)\ \&(A_3=B_3))=P_3*(1/255)$
  $=5.98383885\text{e-}8$

Comparison: SafeSlinger v.s. Bump

	SafeSlinger	Bump
Scalability (# users)	2-10	2
Exchange Method	Local/Remote	Physical
Privacy	Only IP address	IP Address, Location, Accelerometer information
Security	High	Low
Device Requirement	Internet	Internet, Accelerometer
Additional feature	Built-in secure messaging	Fun to use