SAFE SLINGER

Easy-to-Use and Secure Public-Key Exchange

Gian Poltéra

Student, Master of Science in Engineering

Biel, 17. Dezember 2013

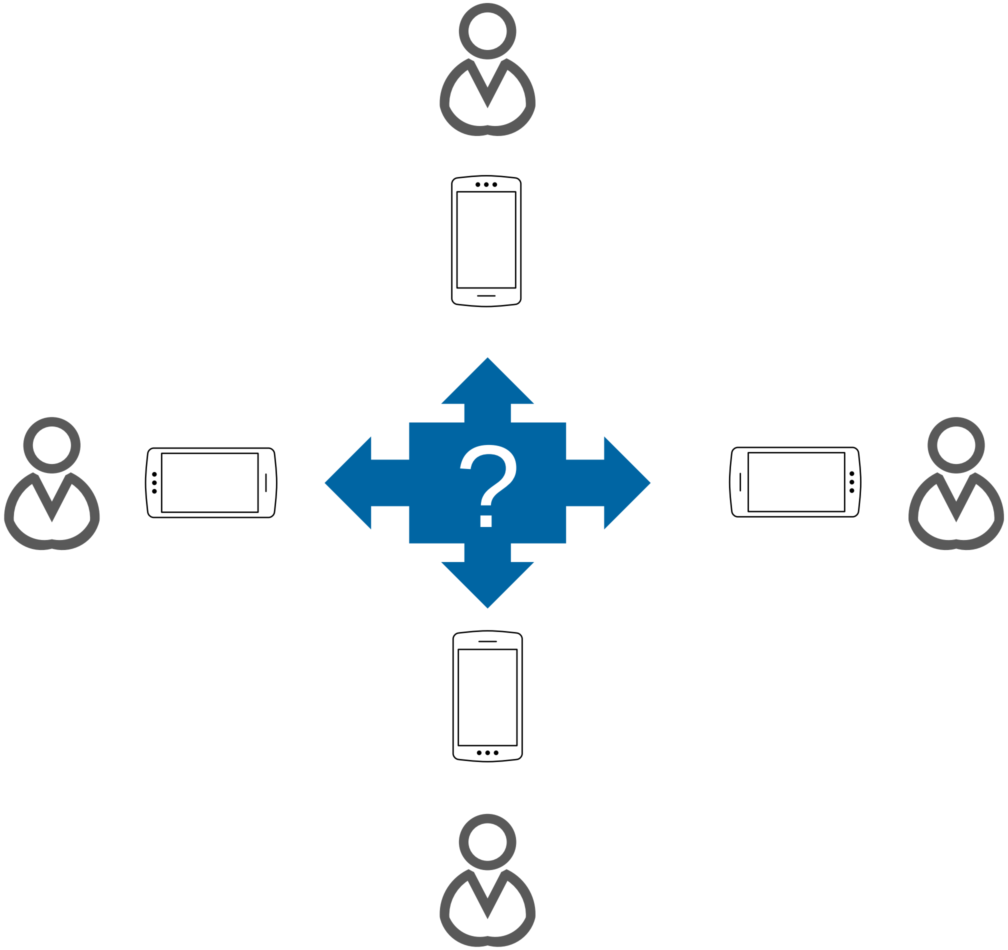
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

Agenda

- **Introduction**
- Basics
- SafeSlinger Protocol
- Security
- Alternatives
- Conclusion

Introduction



Introduction

- **Problem**
  - Unknown sender
  - Problem with authentic public key exchange
- **SafeSlinger**
  - Physical Interaction to establish digital trust
  - Secure exchange of public keys (groups)
  - Secure data exchange
  - Provides an API for importing applications public keys into a user's contact information
  - First complete system without external trusted parties
- **Secure exchange protocol**
- **SafeSlinger Video**

Introduction

- **Goals**
  - Scalable
  - Easy to use
  - Portability
  - Authenticity
  - Secrecy

Introduction

- **Attacks**
  - Man-in-the-Middle (MitM) attack
  - Impersonation attack
  - Sybil attack
  - Group-in-the-Middle (GitM) attack
  - Malicious Server
  - Information leakage after protocol abort
  - Collision attack on low-entropy hash

Introduction

- **Applied Cryptographic Protocols**
  - AES (256 bit)
  - RSA (2048 bit)
  - SHA3 (256 bit)
  - DH-Key Exchange (512 bit) ??
  - Multi-Value-Commitment
  - Group DH-Key Agreement
  - PGP Word-List

Agenda

- Introduction
- **Basics**
- SafeSlinger Protocol
- Security
- Alternatives
- Conclusion

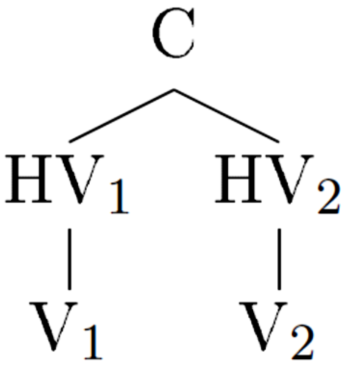
Multi-Value Commitments

- **Cryptographic Commitment**
  - A Commitment is used to lock an entity to a Value V without disclosing V:

$$\boldsymbol{C = H(V, R)}$$

  - On the commitment C, the decommitment can be validated
  - Ensures that the correct value V is disclosed
  - R, V cannot be inferred from C
- **Unpredictable Value**
  - If $\boldsymbol{V}$ is unpredictable, the additional R is not needed:

$$\boldsymbol{C = H(V)}$$



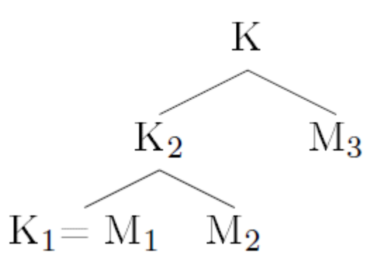
- **Multi-Value Commitment**
  - In case we want to commit more Values with a single commitment:

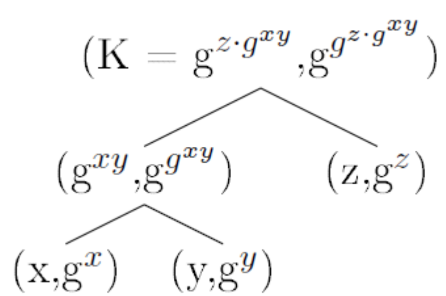
$$\boldsymbol{C = H(HV_1 \parallel HV_2)}$$

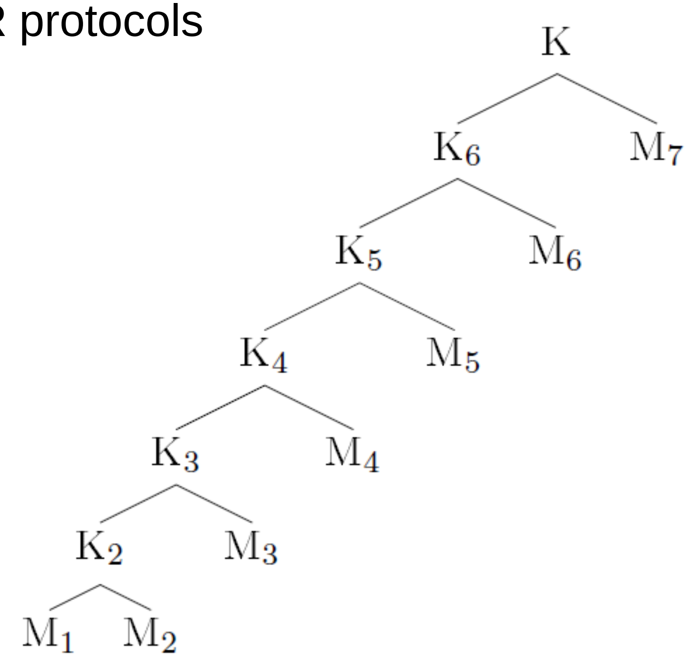
  - Decommitment of either V_1 and V_2 without disclosing the other

Group DH Key Agreement

- **Diffie-Hellman DH key Agreement**
  - Secure Exchange of keys over a unsecure channel
- **Group DH Key Agreement**
  - Multiple parties participate to a common group key
  - Examples are the Cliques, TGDH and STR protocols
- **STR**
  - Tree-based group DH protocol
  - Similar to TGDH
  - Maximally unbalanced tree







Agenda

- Introduction
- Basics
- **SafeSlinger Protocol**
- Security
- Alternatives
- Conclusion

SafeSlinger Protocol

- **Multi-Commitment Generation**
- **Authenticity Verification Round**
- **Secret Sharing Round**

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. $M_i \to S$: C_i

Authenticity Verification Round

Server Unique ID Assignment, User Grouping

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

Collection and Distribution of Initial Decommitment

8. $S \to M_i$: ID_j, C_j $(j \neq i)$
   (other users' ID and commitment)
9. $M_i \to S$: HN_i, G_i, E_i
   $S \to M_i$: 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($\lfloor H(HN_*, G_*, E_*) \rfloor_{24}$) (screen)
    $U_i \xrightarrow{UI} M_i$: Select Matching 3-Word Phrase
12. $M_i \to S$: **if** "no match" or wrong phrase selected:
    Send Hm'_i, Nw_i, Abort protocol.
13. $M_i \to S$: **else if** "match" & correct phrase selected:
    Send Hm_i, Hw_i
14. $S \to M_i$: 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

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)

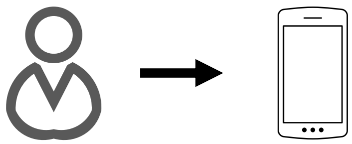
Distribution and Verification of Data Decryption Key

17. $M_i \to S$: $\{Nm_i\}_K$
    $S \to M_i$: $\{Nm_j\}_K$ $(j \neq i)$
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 $(j \neq i) \to D_j$
20. $U_i \xrightarrow{UI} M_i$: Save user data D_j $(j \neq i)$

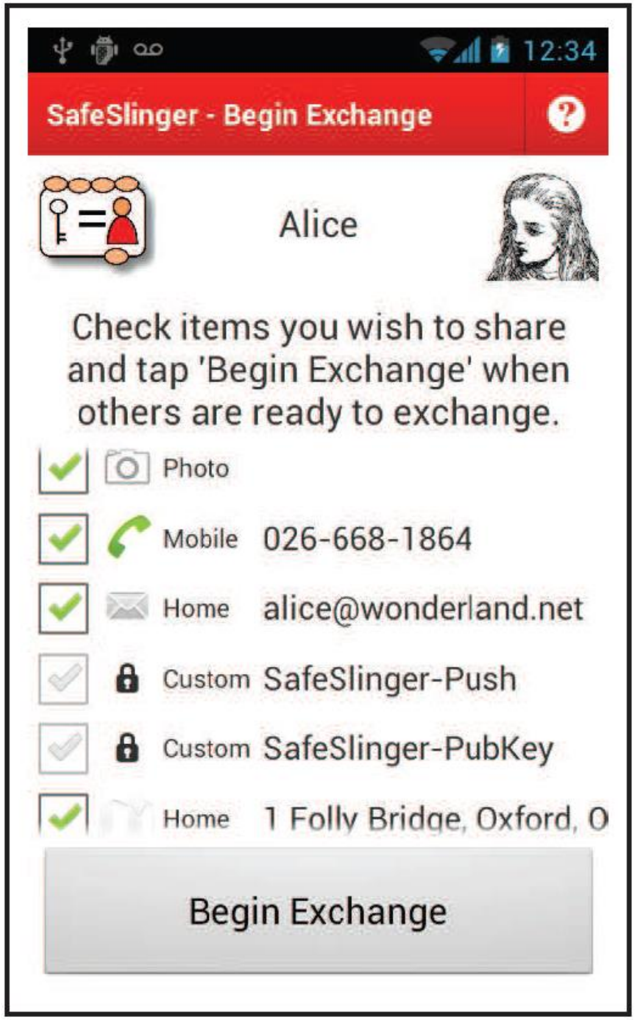
Data Selection & Counting

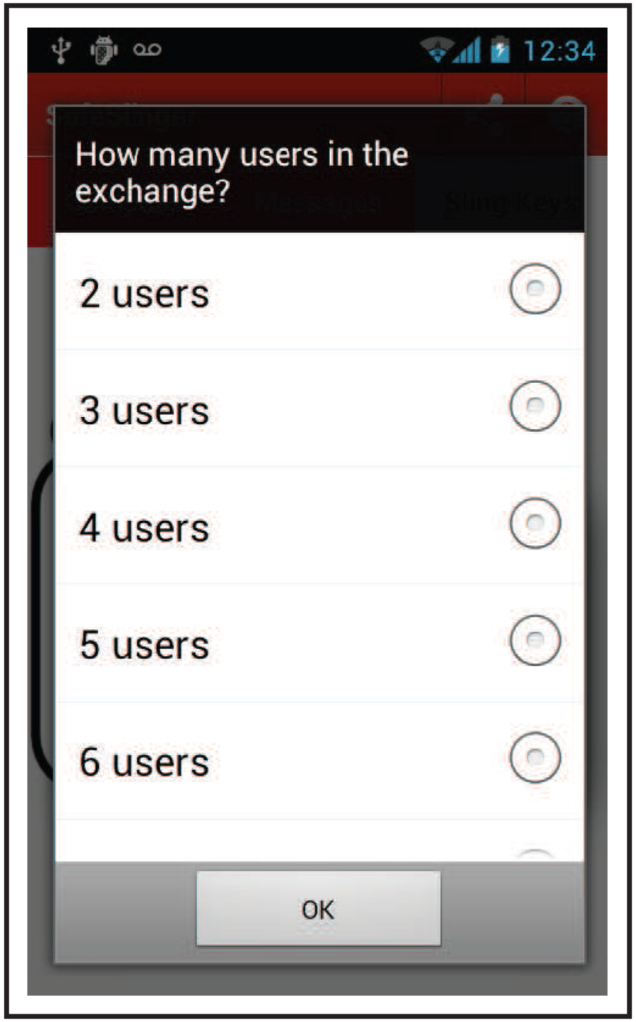
1. 

D_i (the data to be exchanged)

$\widetilde{N}_i$ (number of people in the group)

Multi-Commitment Generation





Multi-Commitment Generation

Commitment, Group DH Key Setup

2.

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

$$Hm_i = H(Nm_i),$$

$$Hm_i' = H(Hm_i)$$

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

$$Hw_i = H(Nw_i)$$

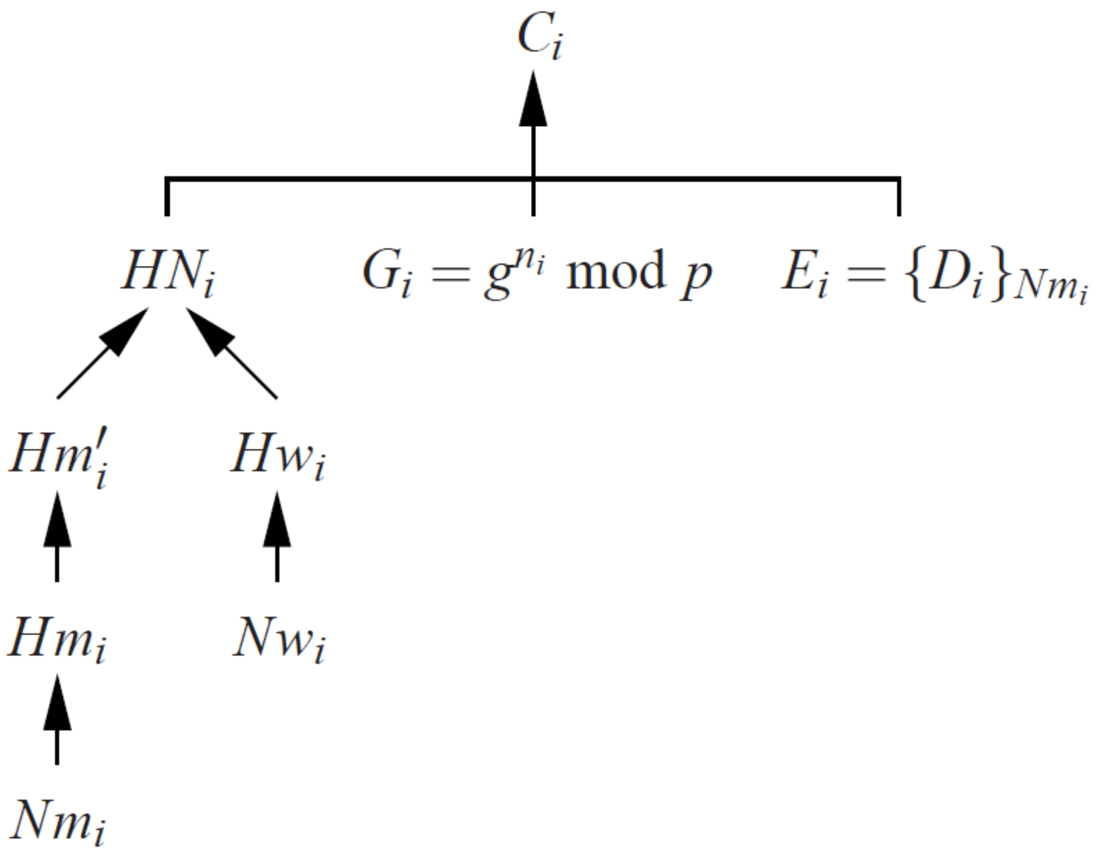
$$HN_i = H(Hm_i' \parallel Hw_i)$$ (multi-value commitment)

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

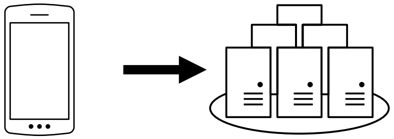
$$E_i = \{D_i\}_{Nm_i}$$ (encryption of data)

$$C_i = H(HN_i \parallel G_i \parallel E_i)$$ (commitment)

Multi-Commitment Generation

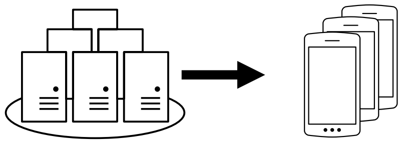


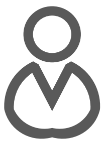
Multi-Commitment Generation

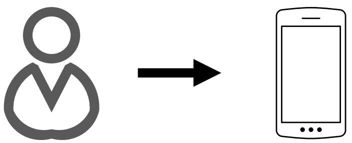
3.  C_i (send the commitment to the server)

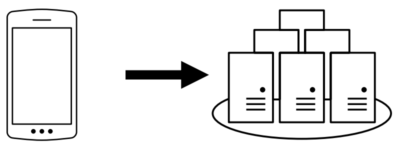
Authenticity Verification Round

Server Unique ID Assignment, User Grouping

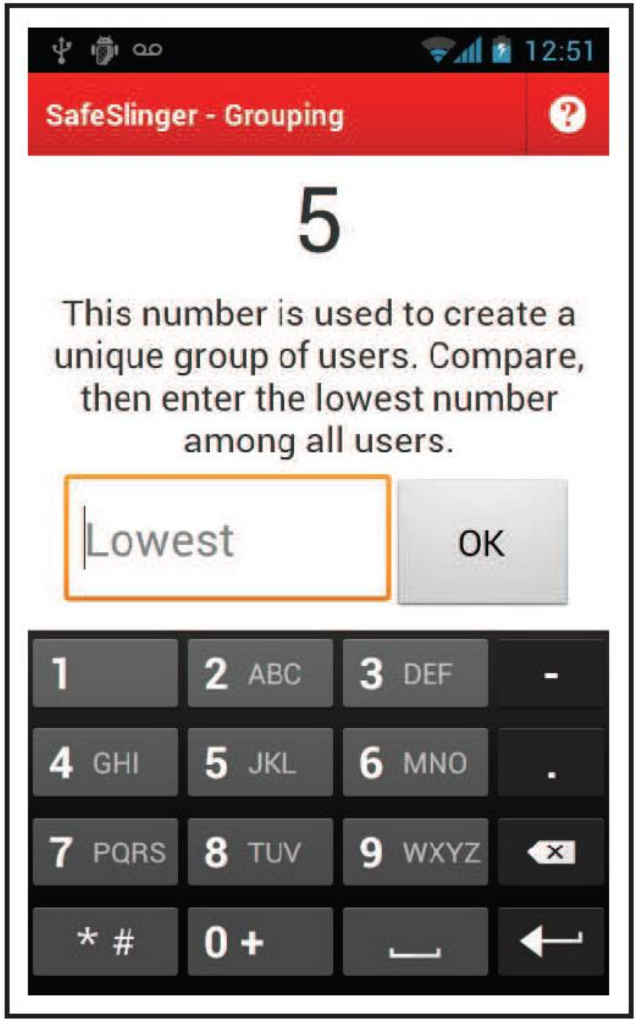
4.  ID_i (unique ID per user)

5.  ID_L (find lowest unique ID among users)

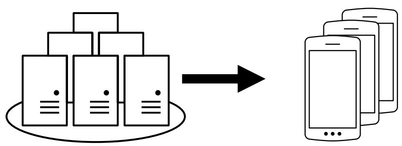
6.  ID_L (enter lowest ID)

7.  ID_L (transfer to the server)

Authenticity Verification Round

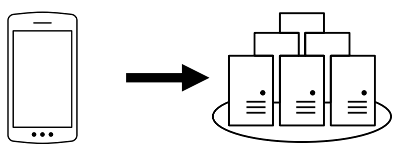


Collection and Distribution of Initial Decommitment

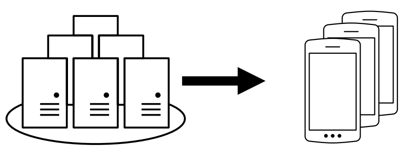
8. 

ID_j, C_j

(other users ID and commitment)

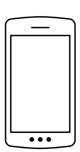
9. 

HN_i, G_i, E_i



HN_j, G_j, E_j

(other users decommitment)

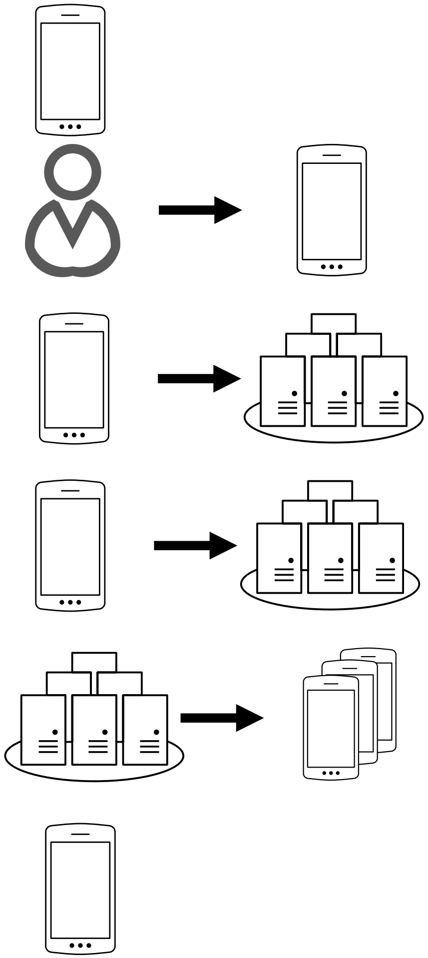
10. 

$$C_j = H\left(HN_j \parallel G_j \parallel E_j\right)$$

(**verify**)

Authenticity Verification Round

Word Phrase Comparison of Integrity of Commitments



11. $([H(HN_*, G_*, E_*)]_{24})$ (WordPhrase, screen)

Select Matching 3-Word Phrase

12. Hm'_i, Nw_i If no match/ wrong phrase

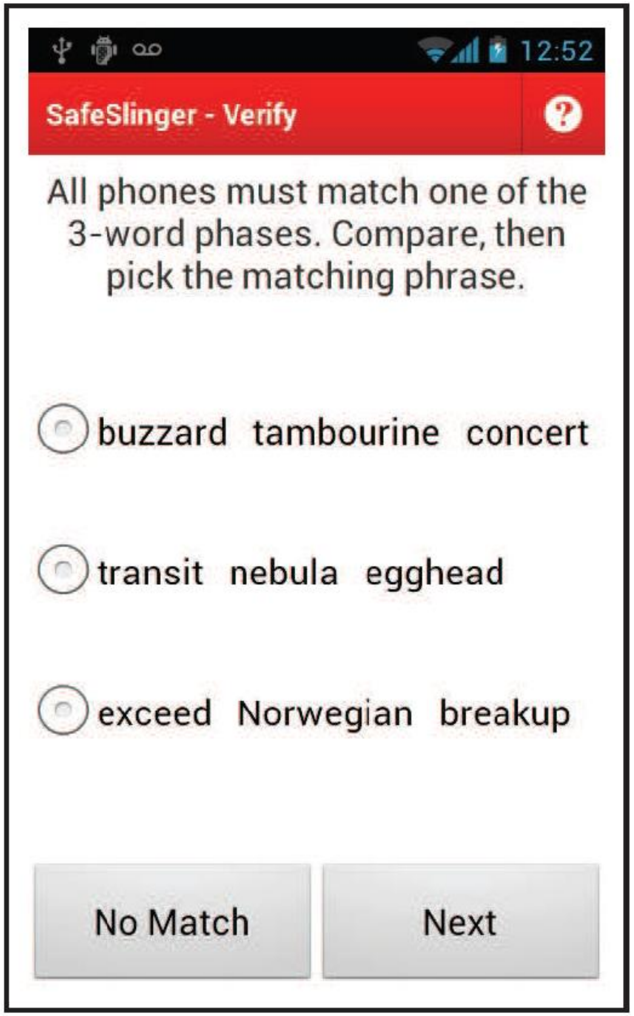
13. Hm_i, Hw_i Else if match/correct phrase

14. Hm_j, Hw_j

15. $HN_j = H\big(H\big(Hm_j\big) \parallel Hw_j\big)$ (**verify**)

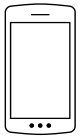
Authenticity Verification Round

- **PGP Word List**
  - Even and odd list with 256 words
- **Word Phrase Verification**
  - Hash-Value from step 11
  - Truncated the first 24 bits
  - Standard PGP approach to convert into 3 words
  - First 8 bits select from even list
  - Second 8 bits select from odd list
  - Final 8 bits select from even list
- **Word Phrase Collision Avoidance**
  - No correct word is in the decoy phrases
  - Each decoy word is unique across all decoy phrases in the group

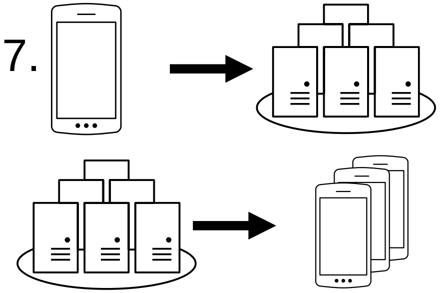


Secret Sharing Round

Group DH Key Establishment

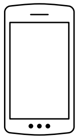
16.  K — Computation of group DH tree

Distribution and Verification of Data Decryption Key

17. 

$\{Nm_i\}_K$ — Encryption of Nm_i

$\{Nm_j\}_K$

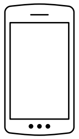
18. 

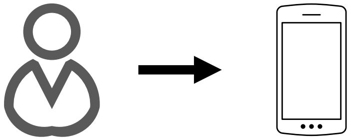
Decryption of Nm_j

$Hm_j = H(Nm_j)$ (**verify**)

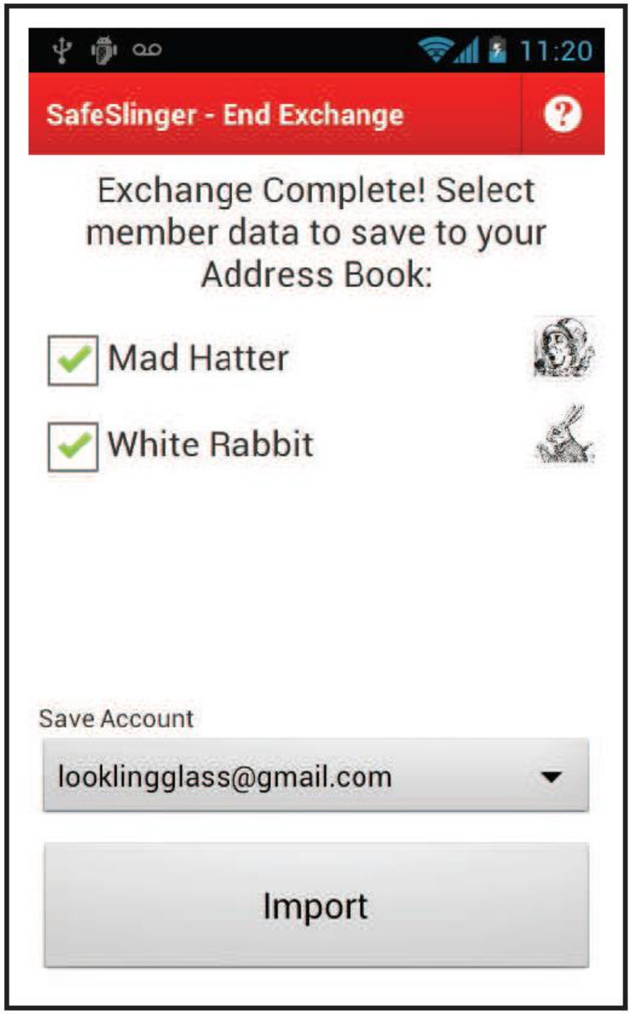
Secret Sharing Round

Decryption of Data and Contact Import

19.  Decryption of E_j with Nm_j

20.  Save user data D_j

Secret Sharing Round



Agenda

- Introduction
- Basics
- SafeSlinger Protocol
- **Security**
- Alternatives
- Conclusion

Security

Malicious outsiders (not legitimate group members)

- **Adversary joins arbitrary group**
  - Too many commitments
- **Local adversary jams communication of one of the local devices, and attempt to join the group in place of the jammed user**
  - Hash comparison with all other users
- **Malicious server splits the group up into different subsets of users**
  - Hash comparison with all other users
- **Participate as a user and inject a commitment**
  - Number of members is larger than the user has entered

Security

Malicious legitimate participant of the group

- **Sybil attack, adversary attempts to infiltrate additional virtual members into the group**
  - Number of virtual members is larger than the user has entered
- **Group-in-the-Middle attack**
  - Hash comparison, different groups = different hashes
- **Impersonation attack, adversary send malicious contact information for himself**
  - Users verify which of their contact entries they actually import into their address book

- **Information leakage**
  - No Information is revealed unless all members reveal their “match” nonce
- **Collision attack on low-entropy hash**
  - Multi-commitment, not changeable
- **Man-in-the-Middle attack**
  - Only least one matching word, without confirming its position
    - $P[A \cap B \neq \emptyset] = 1 - \frac{\binom{254}{2} \cdot \binom{255}{1}}{\binom{256}{2} \cdot \binom{256}{1}} \cong 1.94\%$
  - Only the first word
    - $P[A_1 = B_1] = \frac{1}{256} \cong 0.391\%$
  - All words, with confirmation of their position
    - $P[A = B] = \frac{1}{256 \cdot 256 \cdot 256} = 2^{-24} \cong 0.00000596\%$

$\leq 1.94\%$

Agenda

- Introduction
- Basics
- SafeSlinger Protocol
- Security
- **Alternatives**
- Conclusion

Alternatives

- **Bump**
  - The users are grouped by “bumping” their phones
  - Bump reveals the user location to the server
  - Malicious bystander can simultaneously simulate the bump
  - Not scalable to multiple users
  - No remote users support
  - Device position unreliable
  - Often delay of 10 seconds or more
  - Often fails to pair
- **Ambient noise**
  - Privacy-sensitive sound to the server
  - Unreliable in many circumstances

Agenda

- Introduction
- Basics
- SafeSlinger Protocol
- Security
- Alternatives
- **Conclusion**

Conclusion

- **New approach**
- **Simple operability**
- **Current cryptographic protocols**
- **Weakness 24 bit word phrase and 512 bit large DH-key**

References

- AMIR, Yair, et al. On the performance of group key agreement protocols. *ACM Transactions on Information and System Security (TISSEC)*, 2004.
- DAMGÅRD, Ivan. Commitment schemes and zero-knowledge protocols. In: *Lectures on Data Security*. Springer Berlin Heidelberg, 1999.
- DIFFIE, Whitfield; HELLMAN, Martin. New directions in cryptography. *Information Theory, IEEE Transactions on*, 1976.
- FARB, Michael, et al. *SafeSlinger: Easy-to-Use and Secure Public-Key Exchange*. Technical Report of the CyLab, Carnegie Mellon University, 2012.
- KIM, Yongdae; PERRIG, Adrian; TSUDIK, Gene. Tree-based group key agreement. *ACM Transactions on Information and System Security (TISSEC)*, 2004.
- STEER, David G., et al. A secure audio teleconference system. In: *Proceedings on Advances in cryptology*. Springer-Verlag New York, Inc., 1990.
- STEINER, Michael; TSUDIK, Gene; WAIDNER, Michael. Key agreement in dynamic peer groups. *Parallel and Distributed Systems, IEEE Transactions on*, 2000.