Sesame: A Secure and Convenient Mobile Solution for Passwords

Dr. Mehrdad Aliasgari,
Nick Sabol, and Ashutosh Sharma
California State University, Long Beach
MobiSecServ Feb. 2015

Passwords

Most Popular Passwords of 2014*

- 123456
- password
- 12345
- 12345678
- qwerty
- 123456789
- 1234
- baseball
- dragon
- ……

* Compiled by SplashData

Password Managers Cont.

- Three types
  - Desktop: No mobility
  - Mobile : Trust third party
  - Device based: Have to carry them
- Have to set a master password
  - All passwords are encrypted using one single key phrase.
- If master password is compromised….

Our Work

- Biometric and Phone-based, online password manager
- Data distributed in parts. All parts need to come together to read data
- Our choice of biometric: Voice (Speech and Speaker recognition)

Sesame

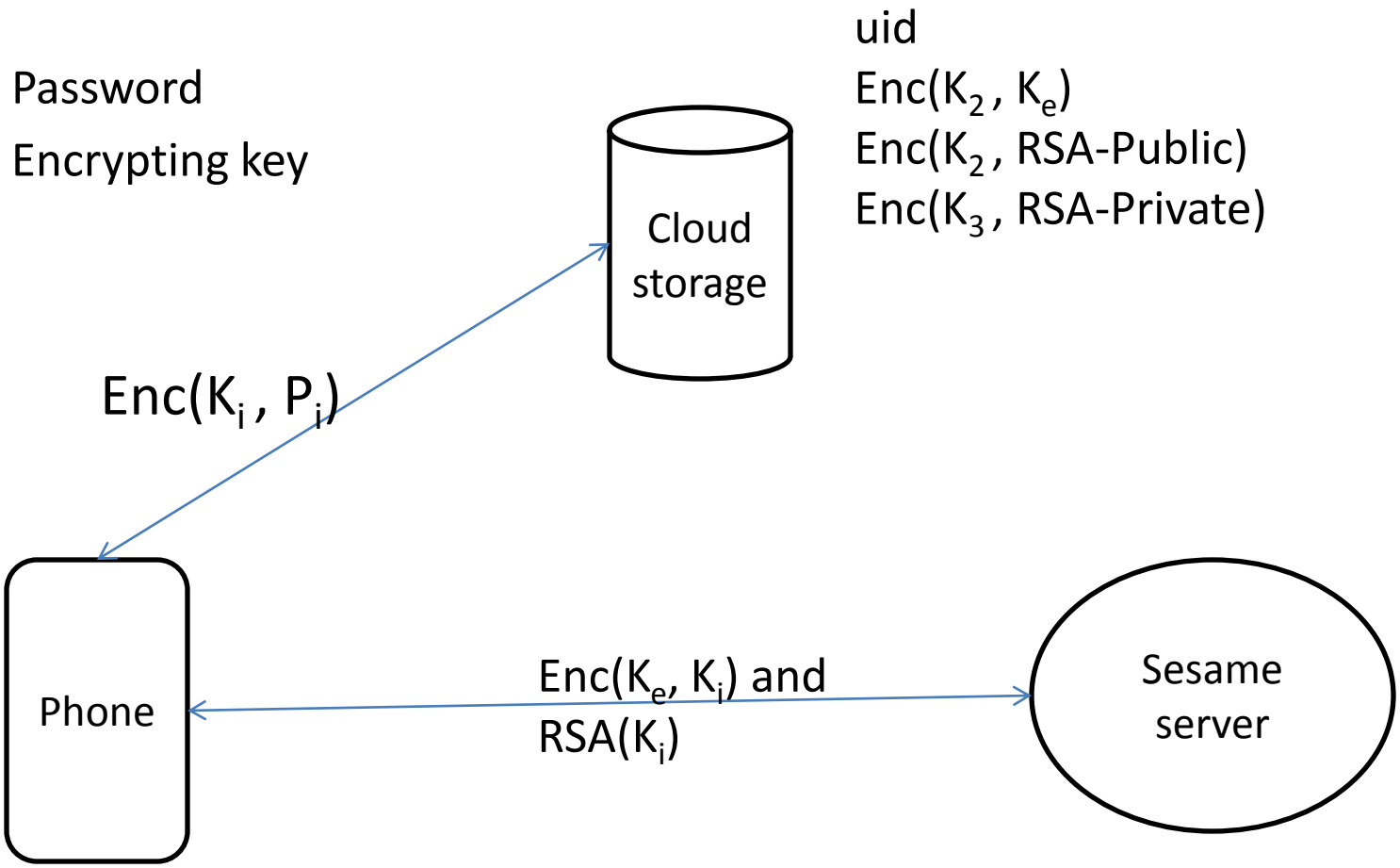
- Idea:
  - Encrypt each password with a **fresh** key
  - Backup the encrypted passwords in the cloud
  - Encrypt the fresh keys and store them on Sesame server
  - If the user passes authentication then release the encrypted key
- Neither the cloud nor Sesame knows anything about your passwords

Sesame (Cont.)

- User Authentication:
  - Voice (Speaker recognition)
  - Speech recognition to extract the requested entry
- Master passwords are used as an alternative but users don’t have to type them every time.
- If master password is compromised user is still safe (better change it soon)

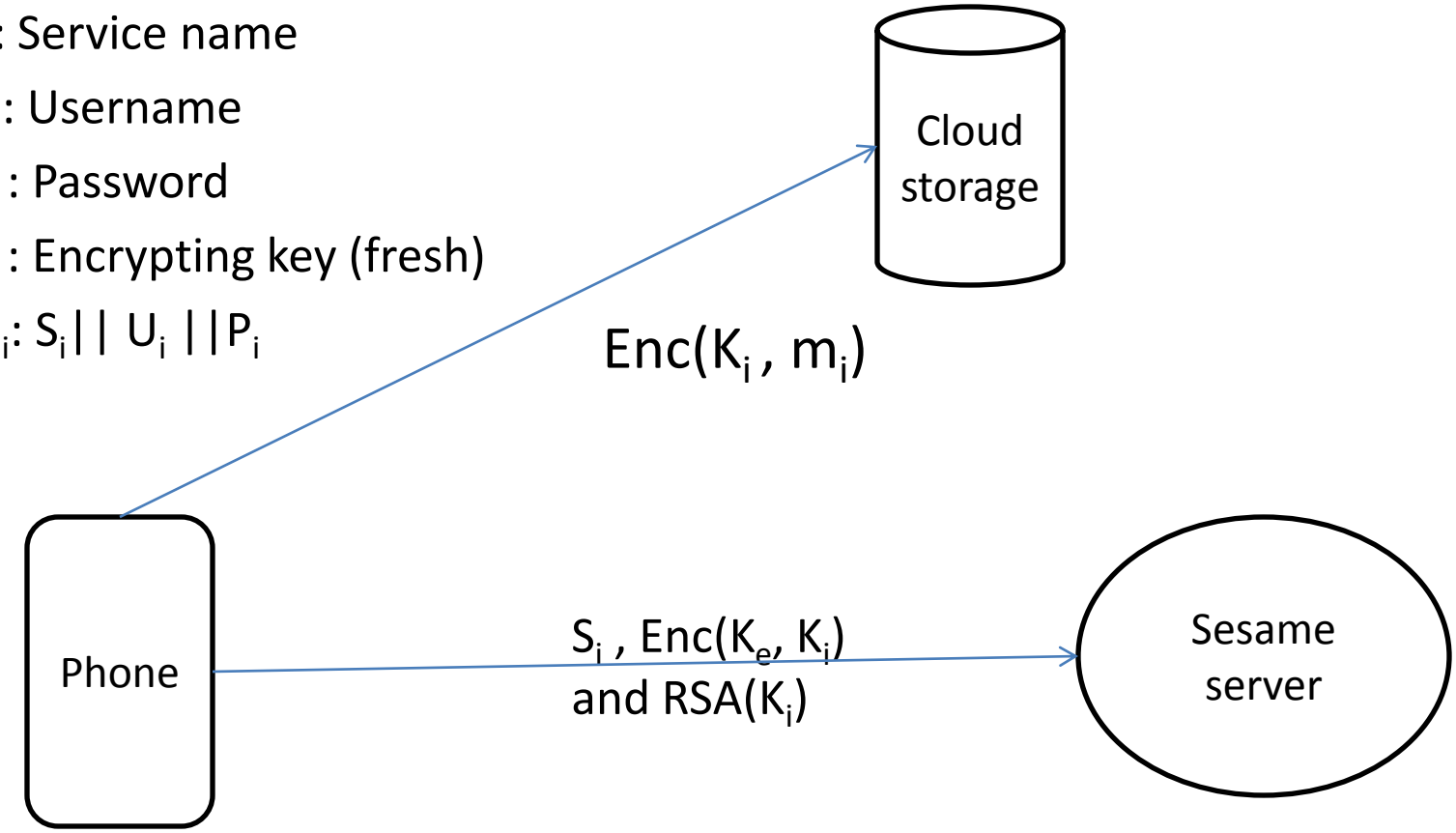
System Overview

- P_i : Password
- K_i : Encrypting key



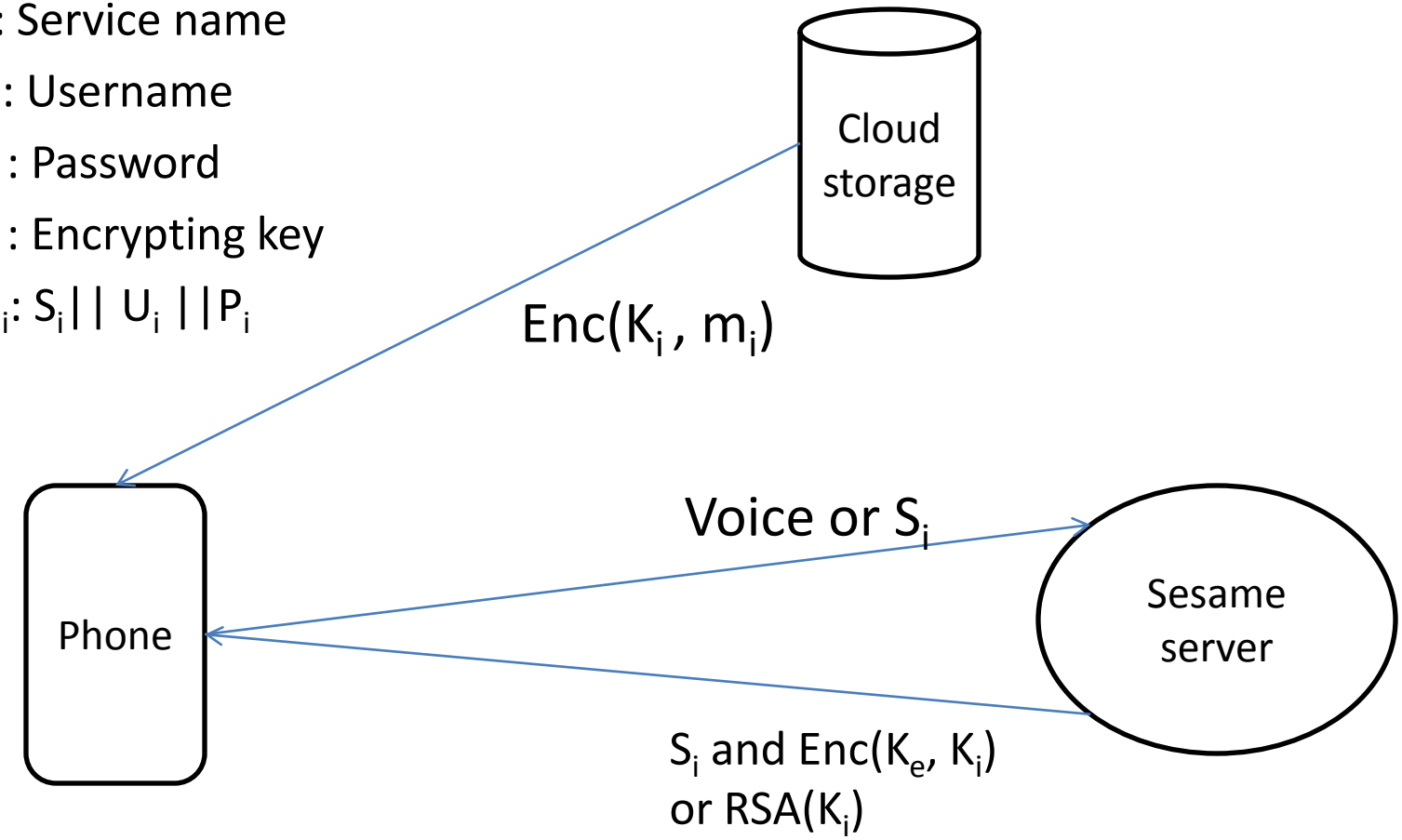
Adding a New Password Entry

- S_i: Service name
- U_i: Username
- P_i : Password
- K_i : Encrypting key (fresh)
- m_i: $S_i || U_i || P_i$



Retrieving a Password Entry

- S_i: Service name
- U_i: Username
- P_i : Password
- K_i : Encrypting key
- m_i: $S_i || U_i || P_i$



Cryptographic Tools

- Master password is used to generate K_1, K_2 and K_3 using KDF (Key Derivation Function)
  - 4096 iterations
  - uid is used as a salt
- Symmetric Encryption: AES 256 bits with CBC mode
- Asymmetric: RSA-OAEP 2048 bits

Symmetric vs Asymmetric

- Why we have both Enc() and RSA()?
- It depends on what method of authentication the users chooses
- When speaker recognition is used
  - Enc(K_e, K_i)
- When master password is used
  - RSA(K_i)

Encryption and Distribution

- All passwords are encrypted with a new key
- Encrypted passwords are backed up
- The keys encrypted and stored in Sesame server
- To recover a password you need:
  - The backed up data in the cloud
  - The encrypted keys
  - The key to decrypt keys

Security Analysis

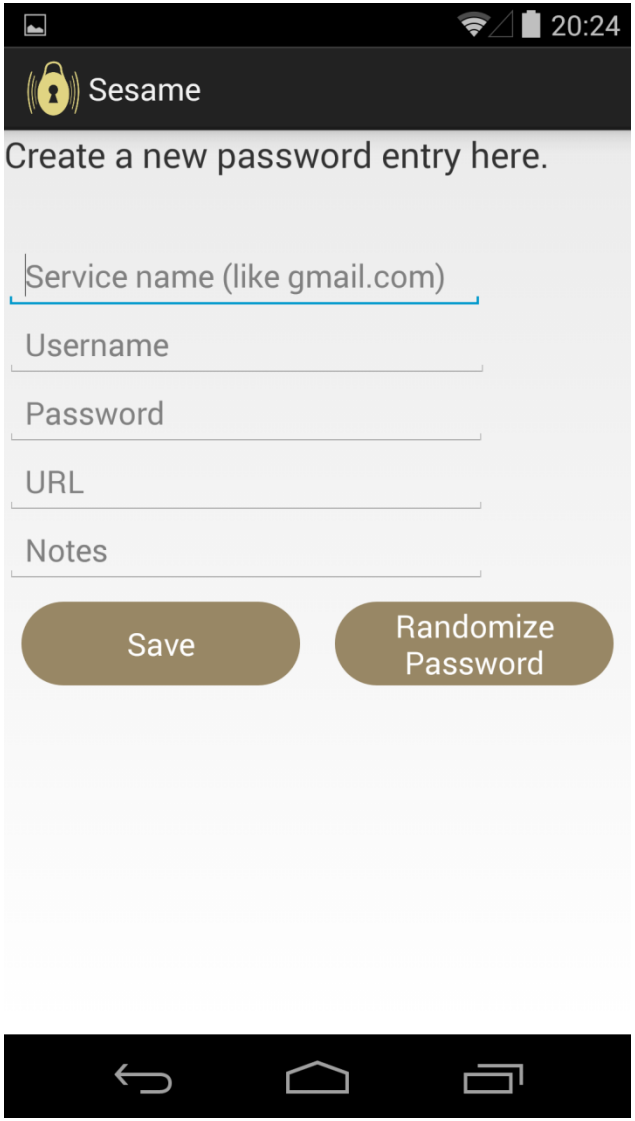
- No one party has all necessary pieces
- Collusion attack:
  - Sesame serve and the cloud collide
    - Best they can do is to brute-force masterpassword
    - Exponential
    - No offline dictionary attack due to use of salt (uid)

Other Capabilities

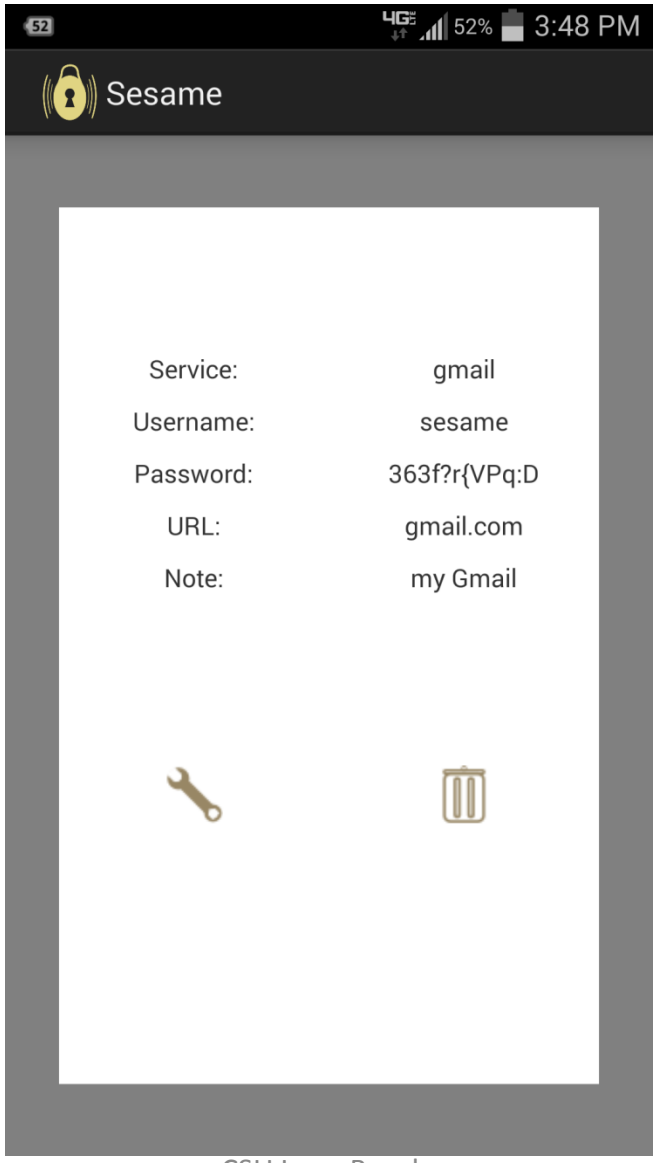
- You can use the application on multiple devices
  - at the installation on second device:
    - Connect with your cloud
    - Enter the master password
    - Respond to the prompted speaker recognition challenge
- Users can change their master password

Android App


20:23
Sesame
Press the microphone below and start speaking to authenticate.


20:24
Sesame
Create a new password entry here.
Service name (like gmail.com)
Username
Password
URL
Notes
Save
Randomize Password


20:26
Sesame
Press the button below and say the prompted word to see all of your password entries.
"Gorgeous"
Alternatively, enter your master password below.
Password
Submit


52
52%
3:48 PM
Sesame
Service:
gmail
Username:
sesame
Password:
363f?r{VPq:D
URL:
gmail.com
Note:
my Gmail

Conclusion

- Secure method of distributing sensitive data
- Can be applied to secure cloud storage of any type of data
- Other biometric modalities can be used
  - Handwriting