Android Bluetooth Credential Store

Camilla Reis,
Institute of Applied Information Processing and Communications

Graz, 7. November 2018

September 27, 2018

Android password managers not as secure as desktop counterparts

Robert Abel Content Coordinator/Reporter

Follow @RobertJAAbel

TECHSCAPE

Rohyt Belani, CEO, Cofense at RSA Conference 2018

Password managers can be tricked into believing that malicious Android apps are legitimate

Password managers from Keeper, Dashlane, LastPass, and 1Password found to be vulnerable, study finds.

By Catalin Cimpanu for Zero Day | September 26, 2018 -- 14:42 GMT (15:42 BST) | Topic: Security

9 Popular Password Manager Apps Found Leaking Your Secrets

February 28, 2017 Wang Wei

REPORT

Vulnerabilities in Password Manager Apps

Dashlane: #1 Password Manager

F-Secure KEY Password manager

1Password - Password Manager

Password Manager

My Passwords

Keeper®: Free Password Manager

Avast Passwords

Hide Pictures Keep Safe Vault

LastPass Password Manager

SPONSORED

Popular News

New KickAss Torrents (KAT) ~ 2018 Best Torrent Sites (Working)

New Privilege Escalation Flaw Affects Most Linux Distributions

Google Makes 2 Years of Android Security Updates Mandatory for Device Makers

Existing Solutions

- Android applications prone to phishing attacks.
- Master passwords stored in plain text.
- Sniffing data from uncleaned clipboard.
- Web-based password managers use cookies for authentication.

Motivation of Project

- The Android platform offers
  - Trusted Execution Environment (TEE)
  - Biometric authentication methods
  - Sandboxing
- Smartphones support our everyday life.

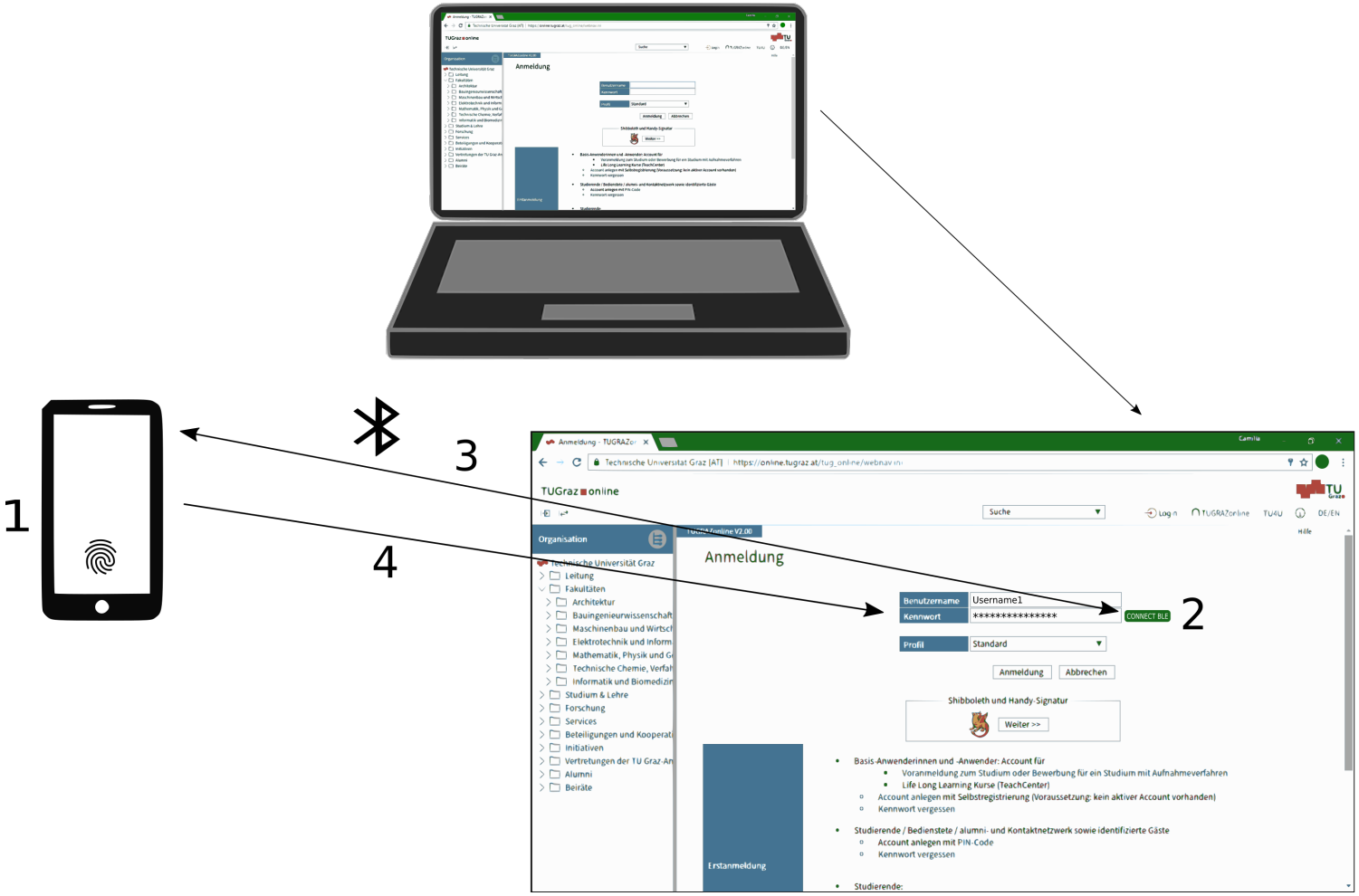
Motivation of Project

- Availability of credentials is important.
- Third parties compromise confidentiality.
- Our goal is to
  - provide secure storage and availability of credentials.
  - reduce external dependencies to increase confidentiality.

Motivation of Project

- Solution:
  - Android credential manager
  - Google Chrome extension
  - Bluetooth LE connection for data exchange
  - Data is stored on device
  - Authentication is done via fingerprint

Workflow of Devices



Requirements

Application requirements:

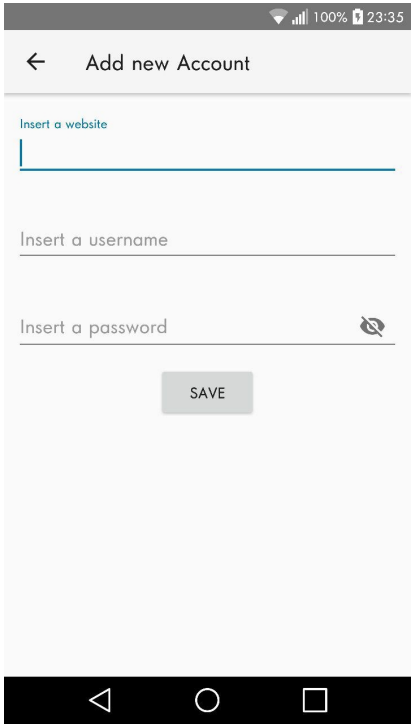
- Storage and management of credentials
- En- and decryption
- Authentication through biometrics

Extension requirements:

- Injection of a button
- Establishing BLE connection
- Read and insert characteristics

Storage of Credentials

- ORM greenDAO
  - Handles storing, deleting, updating tasks.
- Database lies in persistent memory.
- Only application can access data.



Encryption of Credentials

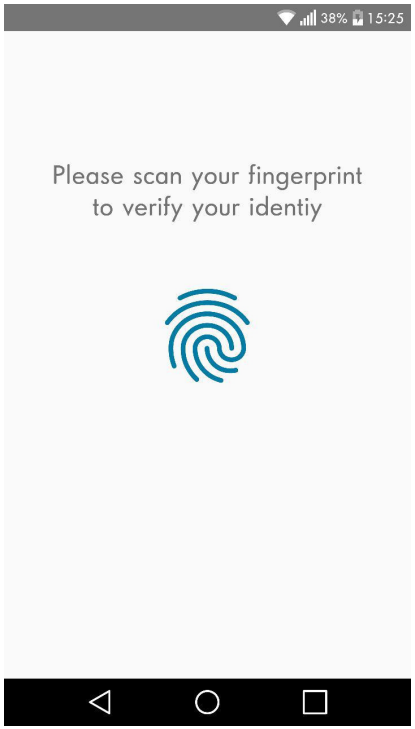
- Symmetric key encryption algorithm AES-GCM:
  - No distribution of public key component.
  - Fast execution of computations.
  - Consumes fewer resources.
  - GCM provides confidentiality, integrity, and authenticity.

Storage of Cryptographic Key

- AndroidKeystore stores cryptographic keys.
- Only application that created key can access it.
- Key is stored in Trusted Execution Environment (TEE).
  - TEE depends on device manufacturer.
  - Data cannot be extracted from the TEE.

Authentication through Biometrics

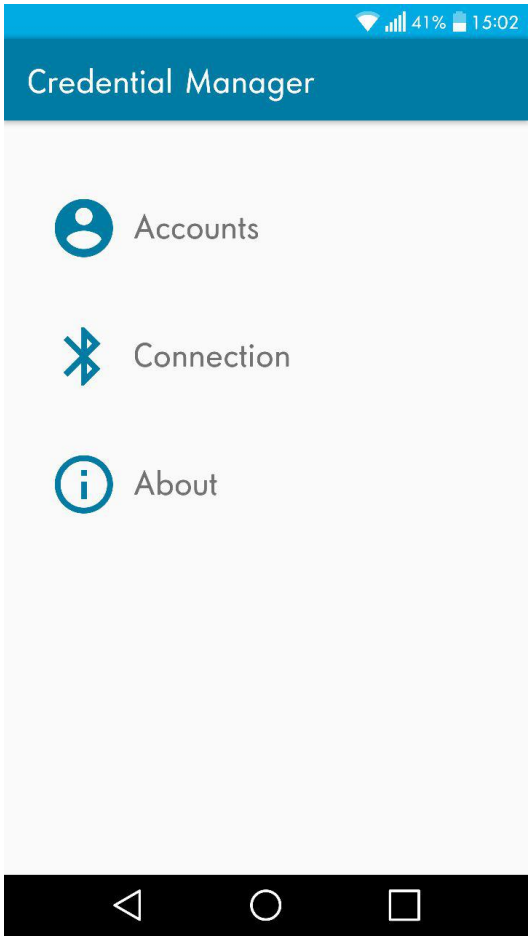
- Authentication via fingerprint when:
  - Accessing credentials
  - Sending credentials
- Protection of unintentional distribution.

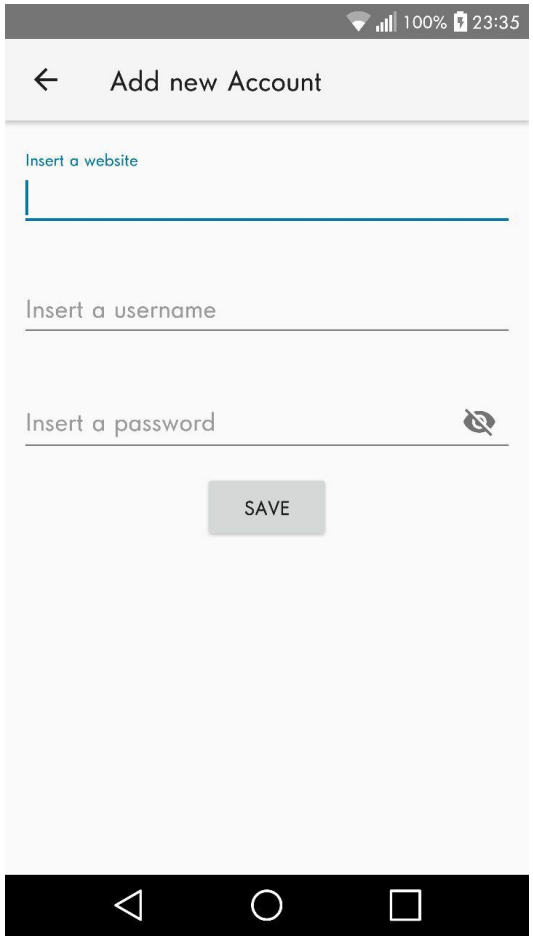


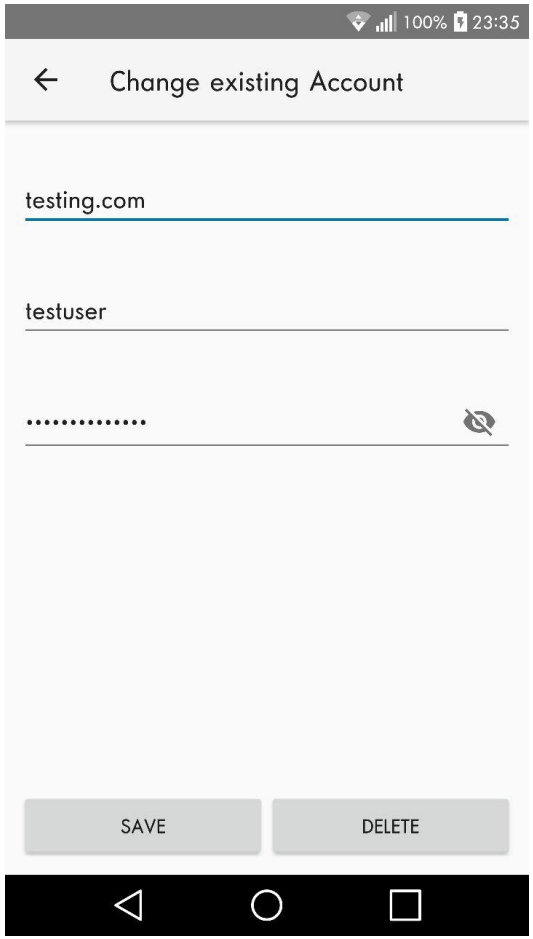
Chrome Browser Extension

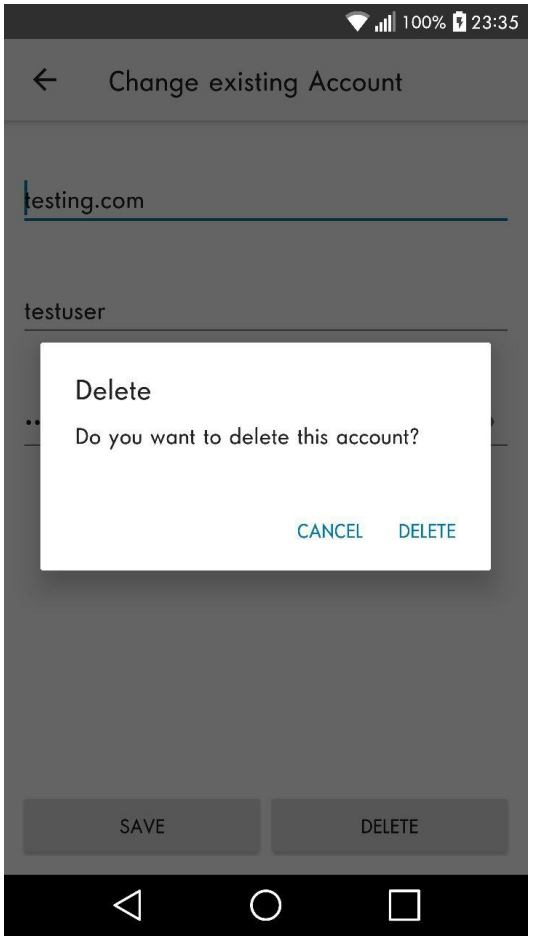
- Establish connection with BLE device.
- Extension acts as client and receives data.
- Insert data into forms.
- Modification of DOM.

Architecture of Project

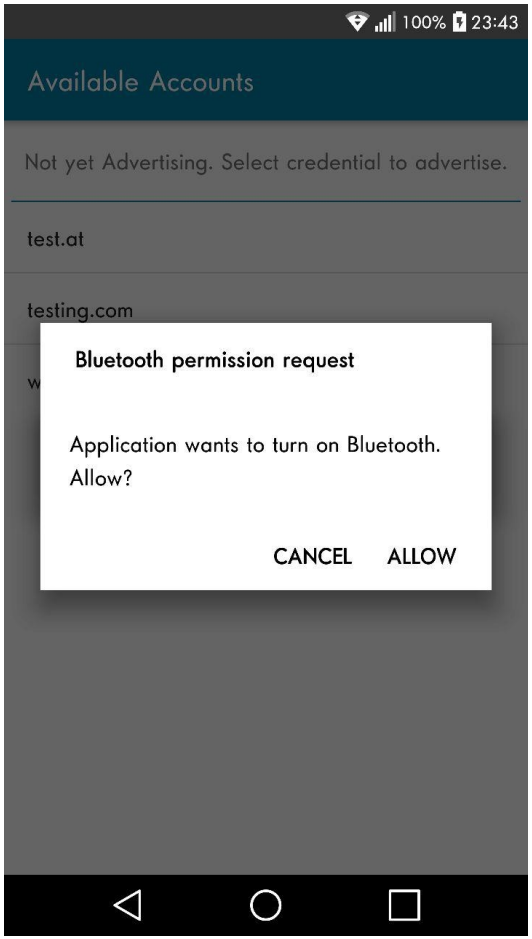




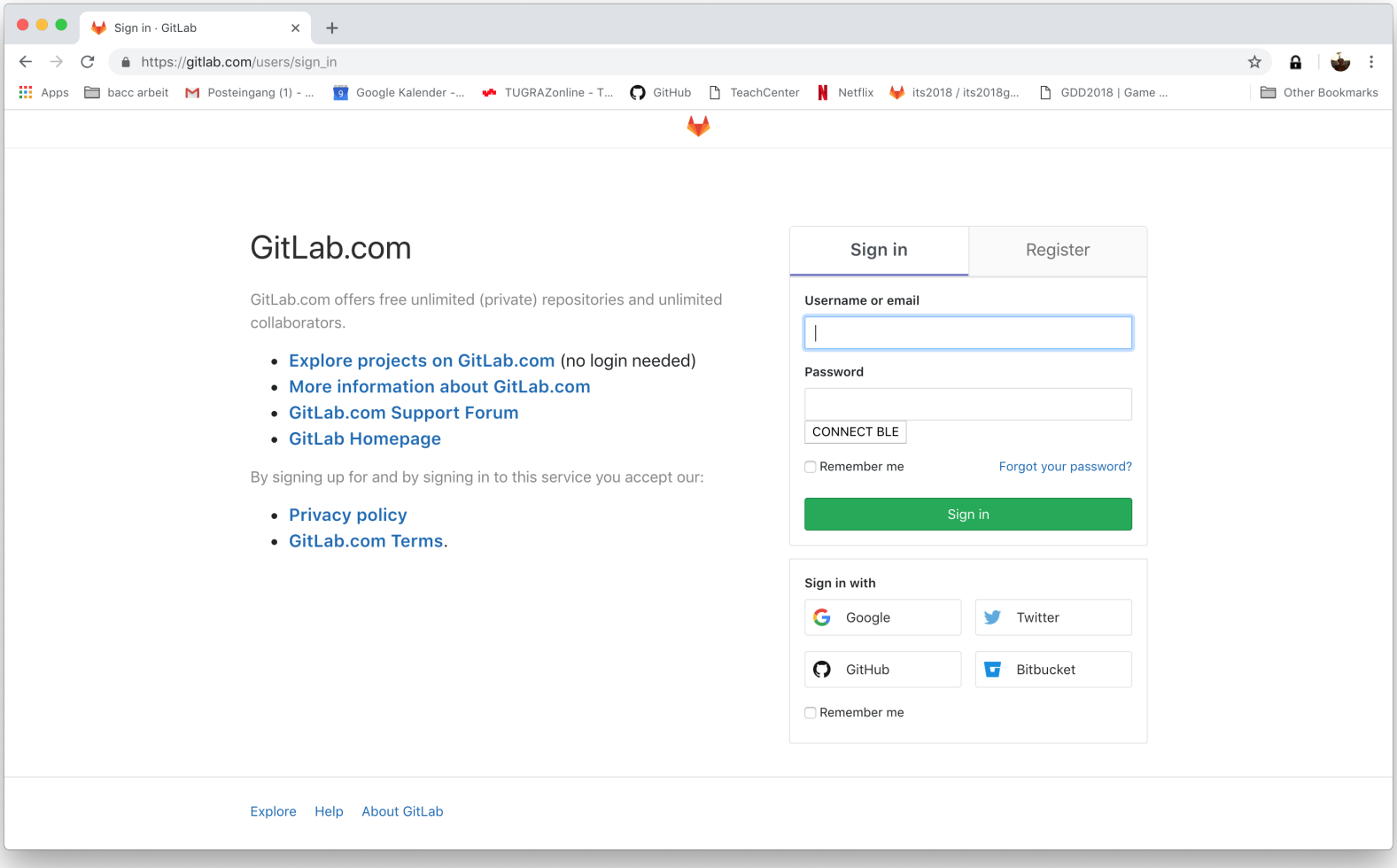

100% 23:35
Change existing Account
testing.com
testuser
SAVE
DELETE


100% 23:35
Change existing Account
testing.com
testuser
Delete
Do you want to delete this account?
CANCEL
DELETE
SAVE
DELETE

Architecture of Project



Architecture of Project



Summary

- Reduce the risk of unauthorized access by eliminating external dependencies.
- Provide availability through a BLE connection.
- Securely store credentials on the device.
- Authenticate through fingerprint.

References

1. R.Abel, “Android password managers not as secure as desktop counterparts.“ https://www.scmagazine.com/home/security-news/android-password-managers-not-as-secure-as-desktop-counterparts/, 2018
2. C. Cimpanu, “Password managers can be tricked into believing that malicious Android apps are legitimate“ https://www.zdnet.com/article/password-managers-can-be-tricked-into-believing-that-malicious-android-apps-are-legitimate/, 2018
3. W. Wei, “9 Popular Password Manager Apps Found Leaking Your Secrets“ https://thehackernews.com/2017/02/password-manager-apps.html, 2017
4. F. Beaufort, “Interact with Bluetooth devices on the Web.” https://developers.google.com/web/updates/2015/07/interact- with-ble-devices-on-the-web, 2018.
5. U. Ries, “Btlejack: Neues Gratis-Tool zum Belauschen von Bluetooth- Verbindungen.” https://www.heise.de/security/meldung/ Btlejack-Neues-Gratis-Tool-zum-Belauschen-von-Bluetooth-Verbindungen-4134142.html, 2018.
6. Y. Haider, S. Selvan, “Confidentiality Issues in Cloud Computing and Countermeasures: A Survey“, 2016.
7. GreenDAO, “greenDAO: Android ORM for your SQLite database.” http://greenrobot.org/greendao/, 2016.
8. Z. Li, W. He, D. Akhawe, and D. Song, “The Emperor’s New Password Manager: Security Analysis of Web-based Password Managers,” in Proceedings of the 23rd USENIX Security Symposium, 2014.