W I S S E N ▪ T E C H N I K ▪ L E I D E N S C H A F T

Android Bluetooth Credential Store

Camilla Reis,
Institute of Applied Information Processing and Communications

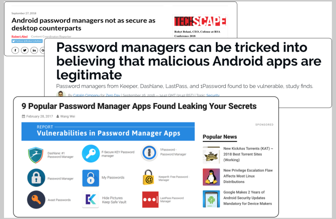
Graz, 7. November 2018

▸ www.tugraz.at

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

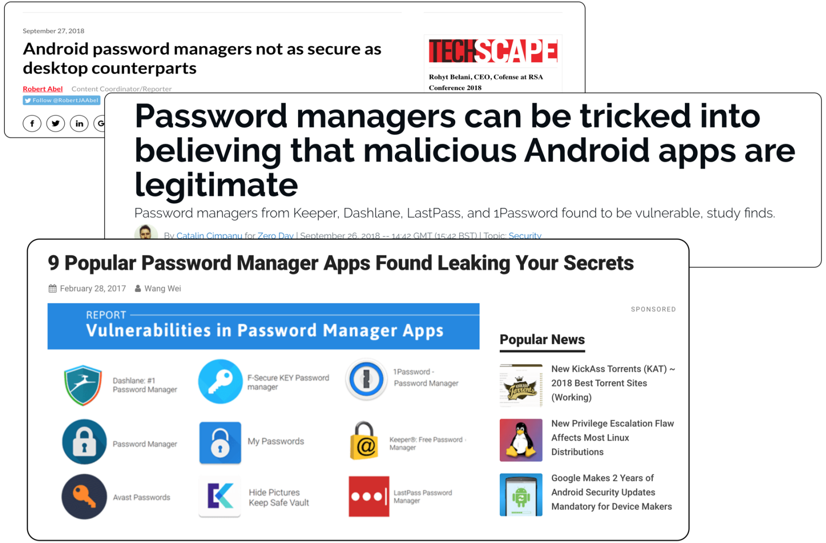
SPONSORED

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



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.

aft. research many sources found that claim password managers are not as secure might seem.
Articles state: andr. pm less secure than desktop & popular pm leaking secrets.
Have researched and found common problem with pm and developed a solution.

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.

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
  - Android Permission System
  - Sandboxing
- Smartphones support our everyday life.

some recent vulnerabilities: popular pm prone exploitation through phishing.
Mali. applications phished cred by misleading the pm with tampered package.
User logs in, communicate backend. pm identifies with package. malic. app mimic legitimate app
MPassword in plain text. In case attack result in compromise of security
Sniffing of the phones clipboard. if not cleaned properly after copied, access credentials
Also web-based pm vulner. to attack cookies to authenticate user.
Although informed & problems resolved, future vulnera. cannot be excluded. (3m)

Motivation of Project

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

Motivation of Project

- The Android platform offers
  - Trusted Execution Environment (TEE)
  - Biometric authentication methods
  - Android Permission System
  - 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.

Now it might seem A. pwm just not secure. Nevertheless, we found Android system offers important sec. mechan. to provide integr, confi, authenti
Including: TEE, provide a secure hardware-backed solution to store sensitive data
Biometric Authentication Methods like Fingerprint.
Andr. Permi.System: most impor. sets restrictions and protects system resouces
Additionally, Sandboxing. offers advan. Linux user-based protection to identify & isolate app resources.
Mobile phones support everyday, make data available. This makes ideal to store data.

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

- 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 transfer
  - Data is stored on device
  - Authentication is done via fingerprint

Availability import. multiple devices. solution: synchronizing w/ cloud services. countless applications offer cloud services. store on servers owned by, access over Internet. cloud services compromise data confidentiality. Conf: accessed only authorized party. storing data on servers, unauthorized access, renounce cloud, avail. challenging.

Depending third-parties lead compromised security. Implementation weaknesses and insecure handling lead vulnerabilities. goal to reduce external dependencies altogether. unexplored approach of sending credentials directly BT. data stored on phone: Authenticity provided. third parties excluded, risk compromised conf. reduced

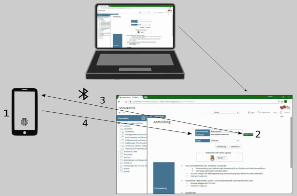
Motivation of Project

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

Motivation of Project

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

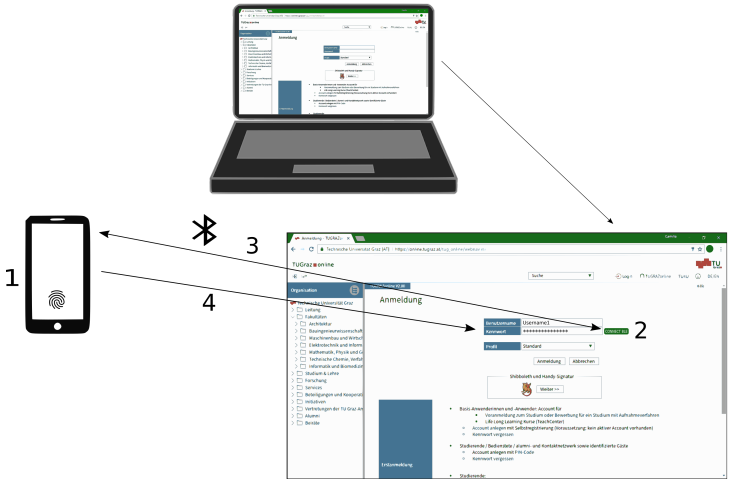
Workflow of Devices



Achieve goal, designed android credential manager, an accompanying Google ext, uses the web bt API: websites communicate BLE devices.
both establish BLE connection to transfer. data on device, selec cred shared on demand. to access/send user authenticate via, this ensures regis. fingerp., extension fills uname and pw into proper forms

7:30

Workflow of Devices



Anmeldung - TUGRAZonline

Technische Universitat Graz [AT] | https://online.tugraz.at/tug_online/webnav.ini

TUGraz online

Suche ▼ | Log in | TUGRAZonline | TU4U | DE/EN | Hilfe

Organisation

- Technische Universität Graz
  - Leitung
  - Fakultäten
    - Architektur
    - Bauingenieurwissenschaft
    - Maschinenbau und Wirtsch
    - Elektrotechnik und Inform
    - Mathematik, Physik und G
    - Technische Chemie, Verfah
    - Informatik und Biomedizin
  - Studium & Lehre
  - Forschung
  - Services
  - Beteiligungen und Kooperati
  - Initiativen
  - Vertretungen der TU Graz-An
  - Alumni
  - Beiräte

TUGRAZonline V2.00

Anmeldung

Benutzername: Username1

Kennwort: ****************

Profil: Standard ▼

Anmeldung | Abbrechen

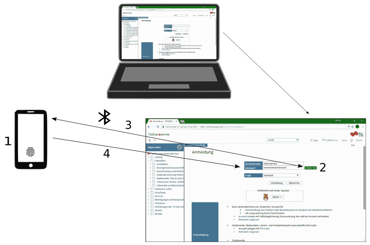
Shibboleth und Handy-Signatur

Weiter >>

Erstanmeldung

- Basis-Anwenderinnen und -Anwender: Account für
  - Voranmeldung zum Studium oder Bewerbung für ein Studium mit Aufnahmeverfahren
  - Life Long Learning Kurse (TeachCenter)
  - Account anlegen mit Selbstregistrierung (Voraussetzung: kein aktiver Account vorhanden)
  - Kennwort vergessen
- Studierende / Bedienstete / alumni- und Kontaktnetzwerk sowie identifizierte Gäste
  - Account anlegen mit PIN-Code
  - Kennwort vergessen
- Studierende:

Workflow of Devices



Requirements

Application requirements:

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

Extension requirements:

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

here see workflow between:
First, selects credential and authenticate via fingerprint. successful, advertising. extension, inject button, step2. button: establish BLE. upon click pairing process step 3.
successful pairing, ext allowed read advertised char. step 4 charac contain username and password. ext inserts uname and pw directly into the forms

Requirements

Application requirements:

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

Extension requirements:

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

Requirements

Application requirements:

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

Extension requirements:

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

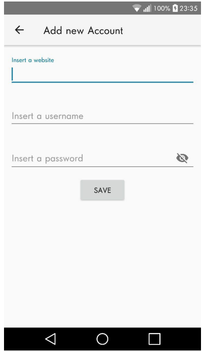
Storage of Credentials

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

Before starting defined requirements
requ. of app:
Secure storage and management like adding, changing and deleting
Encryption and decryption of data
Authentication through fingerprint
requ. of ext:
Injection of a button onto the website
Establishment of BLE Connection upon button click
Reading the advertised characteristics and inserting them into the proper forms

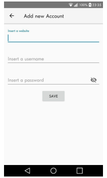
Storage of Credentials

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



Storage of Credentials

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



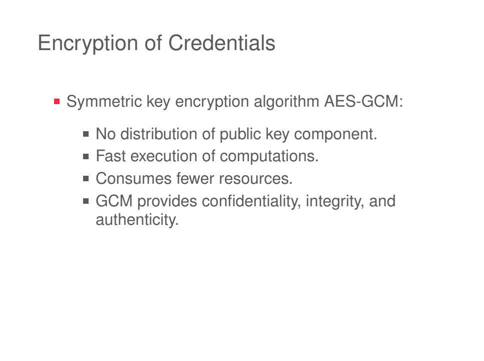
Encryption of Credentials

- 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.

To store credentials needed suitable database structure.
Decided object-relational mapping framew greenDAO. manages all database related tasks: storing, deleting, updating, querying etc. compared other frameworks, straightforward and intuitive to use.
database lies persistent memory and only be accessed from our app.

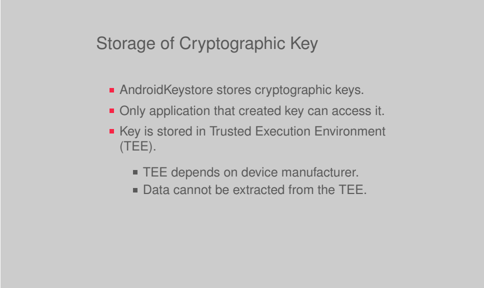
Encryption of Credentials

- 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.



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.



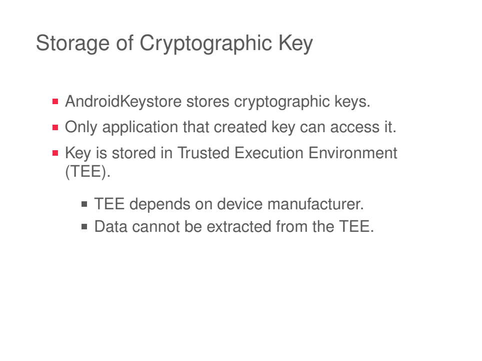
Storage of Cryptographic Key

- 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.

For...decided AES algorithm, GCM as cipher mode.
because all encryption on phone, no distribution of public part. same key used for both
advantages of symmetric key algorithms compared to asymmetric: that it also efficient, secure, provide faster execution of computation, consume fewer such as memory & processor time.
GCM as our cipher mode provides

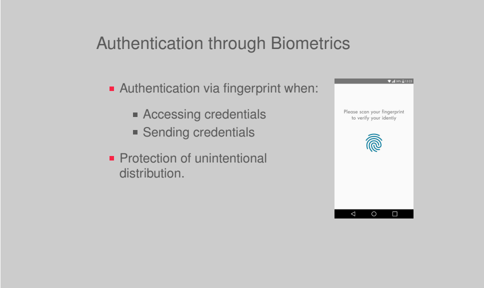
Storage of Cryptographic Key

- 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.



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.



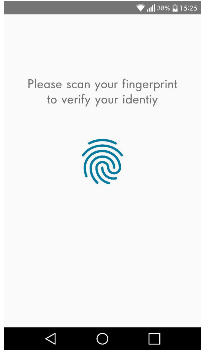
Authentication through Biometrics

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

Store key securely rely on AndroidKeystore system, lets app store/manage keys, no other app access
A specific realization of the AndroidKeystore provides a hardware-based security feature: the Trusted Execution Environment.
availability TEE depends manufacturer.
On devices equipped Qualcomm processor with TrustZone Technology, AKS automatically stored in tee, ensures data not extracted.
Represents sec. option to store keys. tee not supported, the key stored system provided emulated software environment. however, both: keys removed when delete app.

Authentication through Biometrics

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

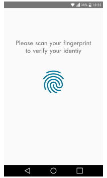


Please scan your fingerprint to verify your identiy

Authentication through Biometrics

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

Please scan your fingerprint to verify your identiy



Chrome Browser Extension

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

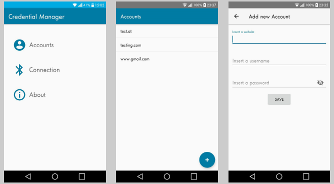
to protect credentials, app requires biometric authentication. as biometric auth: use fingerprint.
whenever access/send cred., fingerprint authentication required. upon each new request - needs to re-authenticate.
mechanism protects unintentional distribution. Risk threatened sec. reduced the user left their phone unattended with open application.

Chrome Browser Extension

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

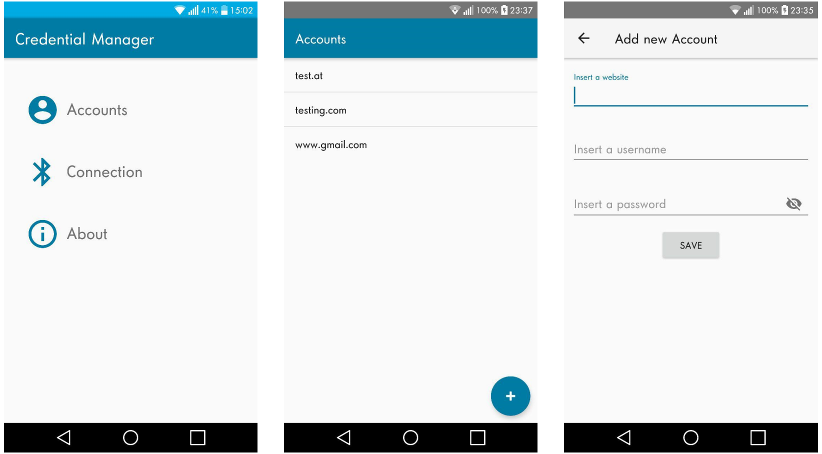
Chrome Browser Extension

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



implemented an extension, chrome introduced dedic. web bt API, support ble conn. website communicate ble devices e.g. heart rate mon.
typically ble device advertise and mobile phone consumes., here roles reversed.
mobile phone is ble device that advertises. acts as server.
extension impl. GATT client retrieve characteristics sent from app.
ext. reads values and fills.
also modifies the document object model. inject button on website.: initiate connection process between
Now guide you through the finished solution of this project:

Architecture of Project



41% 15:02

Credential Manager

Accounts

Connection

About

100% 23:37

Accounts

test.at

testing.com

www.gmail.com

+

100% 23:35

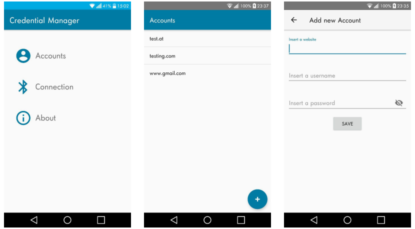
Add new Account

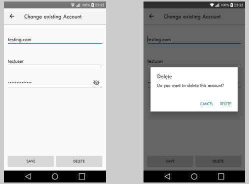
Insert a website

Insert a username

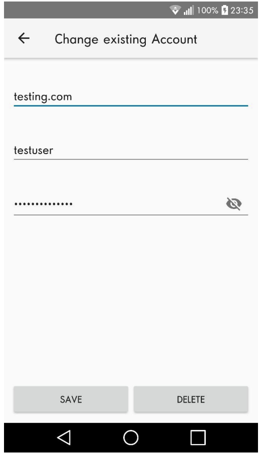
Insert a password

SAVE


Credential Manager
Accounts
Connection
About
Accounts
test.at
testing.com
www.gmail.com
Add new Account
Insert a website
Insert a username
Insert a password
SAVE



Architecture of Project



100% 23:35

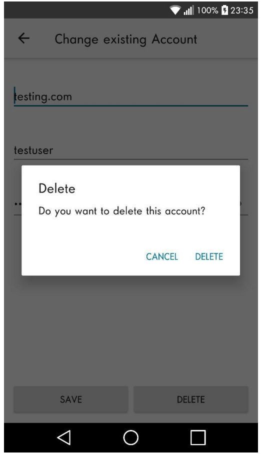
Change existing Account

testing.com

testuser

••••••••••••••

SAVE DELETE



100% 23:35

Change existing Account

testing.com

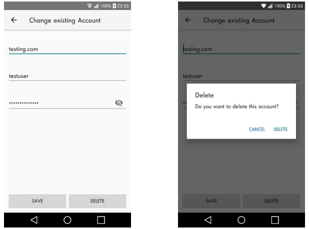
testuser

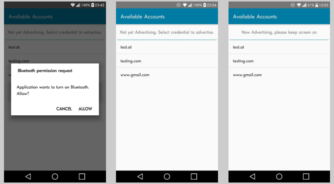
Delete

Do you want to delete this account?

CANCEL DELETE

SAVE DELETE

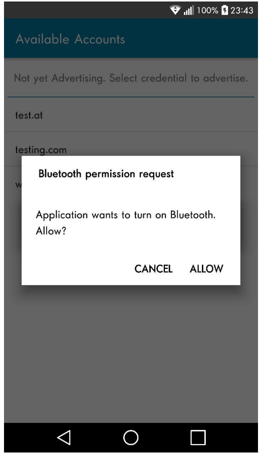



Available Accounts
Bluetooth permission request
Application wants to turn on Bluetooth. Allow?
CANCEL ALLOW

Android Bluetooth Credential Store

Architecture of Project

Architecture of Project


100% 23:43

Available Accounts

Not yet Advertising. Select credential to advertise.

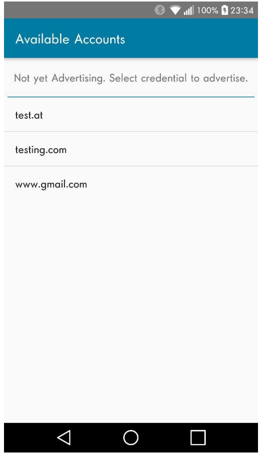
test.at

testing.com

Bluetooth permission request

Application wants to turn on Bluetooth. Allow?

CANCEL ALLOW


100% 23:34

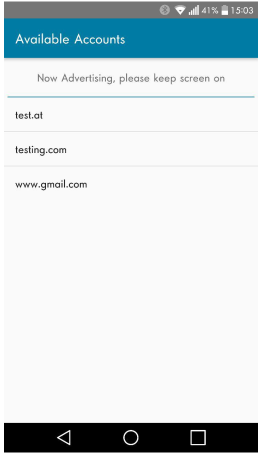
Available Accounts

Not yet Advertising. Select credential to advertise.

test.at

testing.com

www.gmail.com


41% 15:03

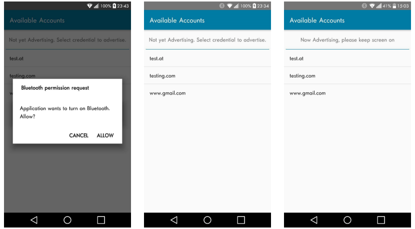
Available Accounts

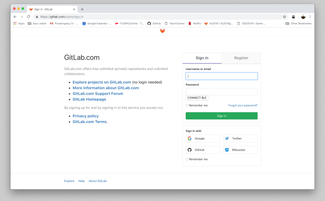
Now Advertising, please keep screen on

test.at

testing.com

www.gmail.com

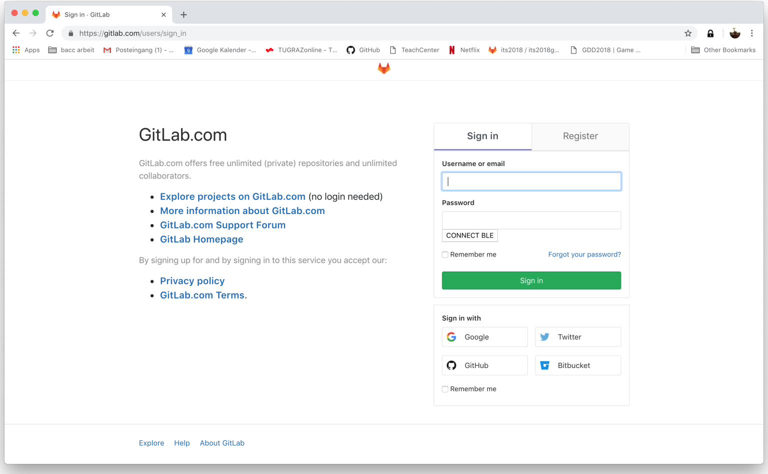




Android Bluetooth Credential Store

Architecture of Project

Architecture of Project



Sign in · GitLab

https://gitlab.com/users/sign_in

GitLab.com

GitLab.com offers free unlimited (private) repositories and unlimited collaborators.

- Explore projects on GitLab.com (no login needed)
- More information about GitLab.com
- GitLab.com Support Forum
- GitLab Homepage

By signing up for and by signing in to this service you accept our:

- Privacy policy
- GitLab.com Terms.

Sign in | Register

Username or email

Password

CONNECT BLE

□ Remember me   Forgot your password?

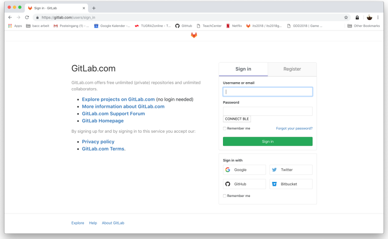
Sign in

Sign in with

Google | Twitter
GitHub | Bitbucket

□ Remember me

Explore   Help   About GitLab

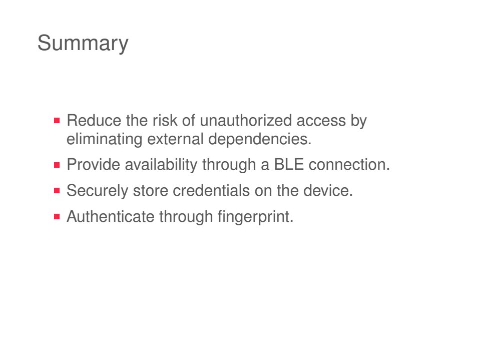


Summary

- 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.

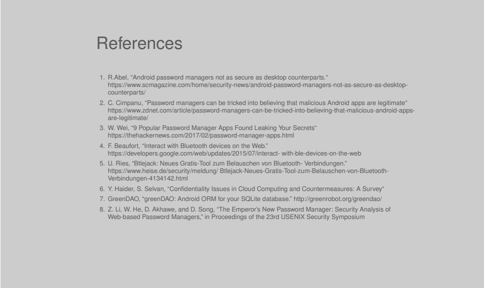
Summary

- 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.



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.



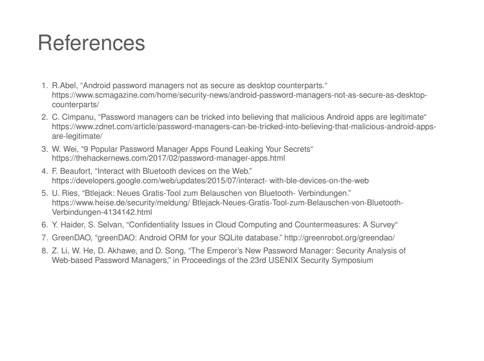
References

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/
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/
3. W. Wei, “9 Popular Password Manager Apps Found Leaking Your Secrets“ https://thehackernews.com/2017/02/password-manager-apps.html
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
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
6. Y. Haider, S. Selvan, “Confidentiality Issues in Cloud Computing and Countermeasures: A Survey“
7. GreenDAO, “greenDAO: Android ORM for your SQLite database.” http://greenrobot.org/greendao/
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

by eliminate exter. depend. we reduced risk unauthorized access
provide availability with ble connection to transfer data to web browser
data stored on device and key in the hardware-backed environment provided by the AKS, where extraction is almost infeasible.
Distribution accomplished BLE connection between. access and transfer of credentials done fingerp. auth.
fingerprint, provide reasonable security maintaining usability. so risk of using insecure PINs and patterns is reduced
would like to thank you for

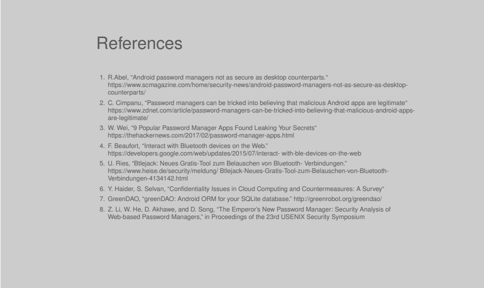
References

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/
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/
3. W. Wei, “9 Popular Password Manager Apps Found Leaking Your Secrets“ https://thehackernews.com/2017/02/password-manager-apps.html
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
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
6. Y. Haider, S. Selvan, “Confidentiality Issues in Cloud Computing and Countermeasures: A Survey“
7. GreenDAO, “greenDAO: Android ORM for your SQLite database.” http://greenrobot.org/greendao/
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



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/
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/
3. W. Wei, “9 Popular Password Manager Apps Found Leaking Your Secrets“ https://thehackernews.com/2017/02/password-manager-apps.html
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
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
6. Y. Haider, S. Selvan, “Confidentiality Issues in Cloud Computing and Countermeasures: A Survey“
7. GreenDAO, “greenDAO: Android ORM for your SQLite database.” http://greenrobot.org/greendao/
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



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/
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/
3. W. Wei, “9 Popular Password Manager Apps Found Leaking Your Secrets“ https://thehackernews.com/2017/02/password-manager-apps.html
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
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
6. Y. Haider, S. Selvan, “Confidentiality Issues in Cloud Computing and Countermeasures: A Survey“
7. GreenDAO, “greenDAO: Android ORM for your SQLite database.” http://greenrobot.org/greendao/
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