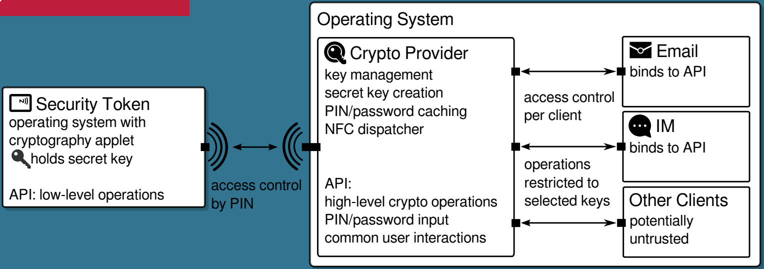
Technische
Universität
Braunschweig

Institute of Operating Systems
and Computer Networks



Security Token
operating system with cryptography applet
holds secret key
API: low-level operations

access control by PIN

Operating System

Crypto Provider
key management
secret key creation
PIN/password caching
NFC dispatcher

API:
high-level crypto operations
PIN/password input
common user interactions

access control per client

operations restricted to selected keys

Email
binds to API

IM
binds to API

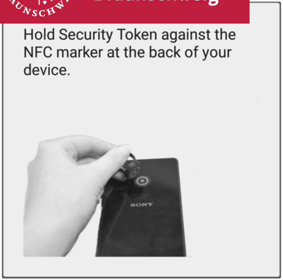
Other Clients
potentially untrusted

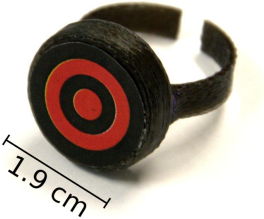
OpenKeychain: An Architecture for Cryptography with Smart Cards and NFC Rings on Android

Dominik Schürmann, Sergej Dechand, Lars Wolf, 2017-09-14

Technische Universität Braunschweig

Institute of Operating Systems
and Computer Networks


Hold Security Token against the NFC marker at the back of your device.



Working Title: “One Ring to Sign Them All”

Dominik Schürmann, Sergej Dechand, Lars Wolf, 2017-09-14

End-to-End Encryption

But let’s start from the beginning...

End-to-End Encryption

But let’s start from the beginning...

End-to-End Encryption on Android

- Messaging: Signal, WhatsApp, LINE, ...
- Cloud Storage: SpiderOak, Boxcryptor, ...
- Email: ?

End-to-End Encryption

But let’s start from the beginning...

End-to-End Encryption on Android

- Messaging: Signal, WhatsApp, LINE, ...
- Cloud Storage: SpiderOak, Boxcryptor, ...
- Email: ?

Issues

- Secret Key is stored on the device
- Android updates rolled out slowly
- Malware
- Bring Your Own Device (BYOD) Policies

Goals

Architecture for End-to-End Encryption

- Easy API (no knowledge of public key crypto required)
- Support for secret keys on external NFC tokens
- Include UI components

Goals

Architecture for End-to-End Encryption

- Easy API (no knowledge of public key crypto required)
- Support for secret keys on external NFC tokens
- Include UI components

Research Goals

- API Design
- Comparison with existing APIs
- Try out new form factors (NFC Ring!)
- User study of UI components

Existing Work

Crypto API Misuse

- Egele et al.: “An Empirical Study of Cryptographic Misuse in Android Applications.” (ACM CCS’11)
- Fahl et al.: “Why Eve and Mallory Love Android: An Analysis of Android SSL (in) Security” (ACM CCS’12)

Usability of **Two Factor Authentication** on Desktop Systems

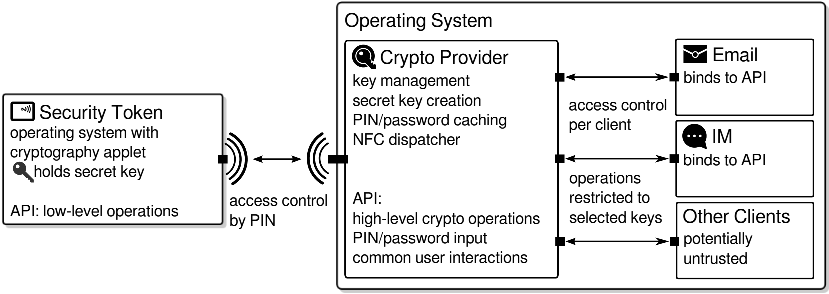
- Strouble et al.: “Productivity and Usability Effects of Using a Two-Factor Security System” (SAIS’09)
- Lang et al. (Google): “Security Keys: Practical Cryptographic Second Factors for the Modern Web” (Financial Crypto’16)

Existing Work

Conclusion

- No App/Library/Architecture on Android for NFC Security Tokens for End-to-End Encryption
- Studies only about Authentication, not Encryption
- No studies on NFC Rings for Crypto

Architecture



Operating System

Crypto Provider
key management
secret key creation
PIN/password caching
NFC dispatcher

API:
high-level crypto operations
PIN/password input
common user interactions

Email
binds to API

IM
binds to API

Other Clients
potentially
untrusted

access control
per client

operations
restricted to
selected keys

Security Token
operating system with
cryptography applet
holds secret key

API: low-level operations

access control
by PIN

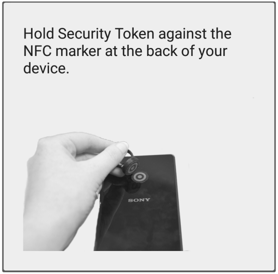
API Specificiation (Simple Version)

Action	Req. Extras	Description
SIGN_AND_ENCRYPT	USER_IDS	Encrypt to email addresses and generate signature
DECRYPT_VERIFY	-	Decrypt and verify signature

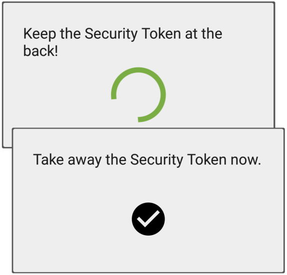
- Typically, APIs only provide low level methods
- In our case it also provides UI components
- Includes secure password/PIN caching

Demo Videos

User Interface Engineering

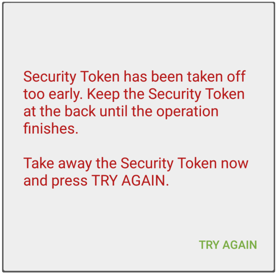


Hold Security Token against the NFC marker at the back of your device.



Keep the Security Token at the back!

Take away the Security Token now.



Security Token has been taken off too early. Keep the Security Token at the back until the operation finishes.

Take away the Security Token now and press TRY AGAIN.

NFC Performance

Table: Mean durations (w/ standard deviation) of cryptographic operations (10 experiments per operation).

Operation	Duration	σ
Signature calculation	787.9 ms	3.18
Decrypt session key	830.9 ms	55.86
Transfer existing secret key	711.9 ms	32.66
Generate secret key on-token[a]	9476.2 ms	2297.71

[a] Roughly, only every third key generation succeeded

User Study

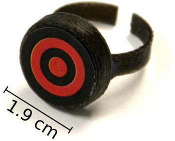
- Try new form factor in comparison to smart cards
- Forge the One Ring in the fires of Mount Doom.

User Study

- Try new form factor in comparison to smart cards
- Forge the One Ring in the fires of Mount Doom.

(a) IC extracted from NXP J3D081.

(b) Circular coil as new NFC antenna.

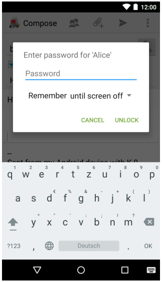


(c) 3D printed ring prototype.

User Study

Study

- 40 participants from a large company in Germany
- Password vs NFC card vs NFC ring

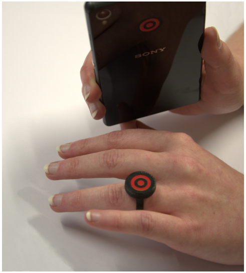


Enter password for 'Alice'

Password

Remember until screen off

CANCEL UNLOCK



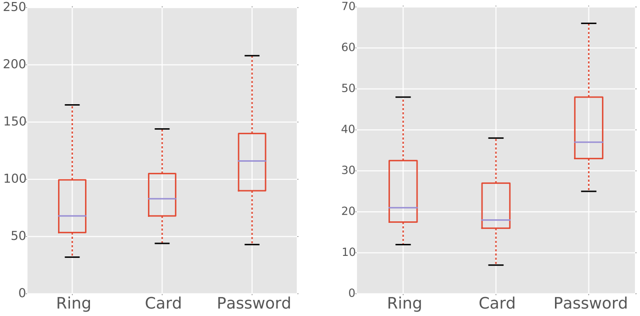
User Study

Design

1. Lab experiment observing setup time, decryption time
2. User survey for analyzing perception

- Within-group design
- No comparison with biometric features

Performance



(a) Setup time.

(b) Decryption time.

Figure: Time measurements (in seconds, no outliers, lower is better).

User Perception

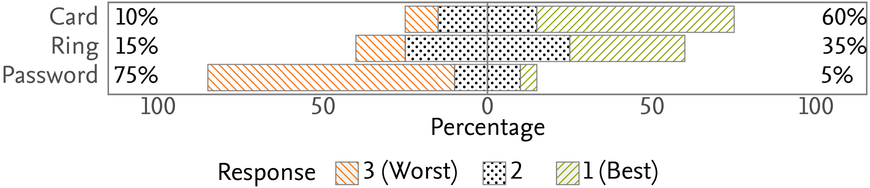


Figure: Aggregated user perception showing the ranking choices in the interview.

Interview

- favor of cards: “easily stored in the wallet”
- “rings are more secure than cards because they are more difficult to steal than wallets”
- “security purpose is not immediately obvious to an outsider”
- “rings can easily be forgotten on a bedside cabinet while not worn at night”
- “cards are easily misplaced as they are not constantly worn on the body”

Conclusion

Summary

- First architecture for end-to-end encryption with NFC tokens
- Study showing the advantage of NFC in comparison to passwords
- Deployed to over 100,000 users on Google Play
- Sufficiently Secure Newsletter: *https://www.sufficientlysecure.com*

Hands-On Demo

- Get a smart card and install OpenKeychain and K-9 Mail from Play
- Yesterday during demo reception
- Come to me after this talk to try out the ring

Conclusion

Summary

- First architecture for end-to-end encryption with NFC tokens
- Study showing the advantage of NFC in comparison to passwords
- Deployed to over 100,000 users on Google Play
- Sufficiently Secure Newsletter: *https://www.sufficientlysecure.com*

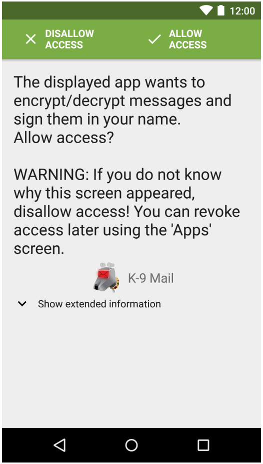
Hands-On Demo

- Get a smart card and install OpenKeychain and K-9 Mail from Play
- Yesterday during demo reception
- Come to me after this talk to try out the ring

Any questions?

Twitter: @domschuermann

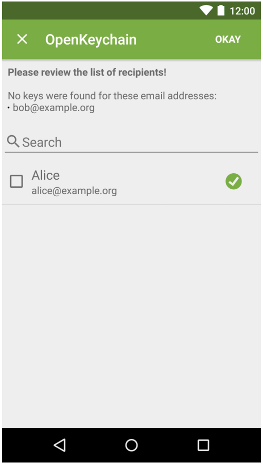
Backup Slides



The displayed app wants to encrypt/decrypt messages and sign them in your name.
Allow access?

WARNING: If you do not know why this screen appeared, disallow access! You can revoke access later using the 'Apps' screen.

(a) Access control per app via user decision.

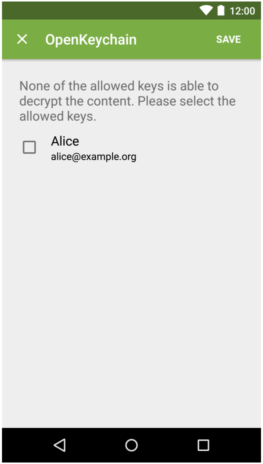


Please review the list of recipients!

No keys were found for these email addresses:
- bob@example.org

□ Alice
alice@example.org ✓

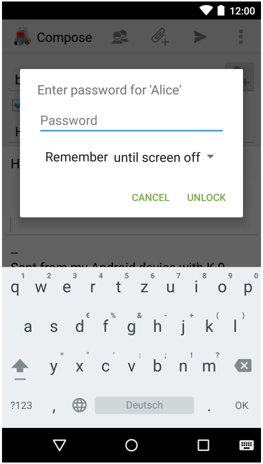
(b) Missing public key.



None of the allowed keys is able to decrypt the content. Please select the allowed keys.

□ Alice
alice@example.org

(c) Restriction of allowed keys per app.

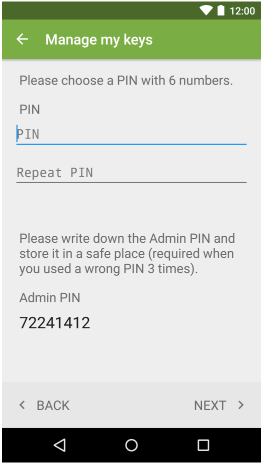


Enter password for 'Alice'

Password

Remember until screen off

(a) Password input for password-protected keys.



Manage my keys

Please choose a PIN with 6 numbers.

PIN

PIN

Repeat PIN

Please write down the Admin PIN and store it in a safe place (required when you used a wrong PIN 3 times).

Admin PIN

72241412

(b) PIN selection during key creation.

		High-Level API w/ Secure Defaults	Supports Security Tokens	Standardized Formats	Cross-Platform	PIN/Password Cache	Key Management	GUI
Low-Level APIs	libcrypto	○	○	●	●	○	○	○
	Bouncy Castle	○	○	●	●	○	○	○
	OpenSC	○	●	●	◐	○	○	○
High-Level APIs	NaCl/libsodium	●	○	○	●	○	○	○
	Keyczar	●	○	○	●	○	◐	○
Fully Integrated Systems	GnuPG	○	●	●	◐	●	●	○
	GNU Privacy Assistant (GPA)[a]	○	●	●	◐	●	●	●
	Kleopatra[a]	○	●	●	◐	●	●	●
	GNOME Keyring[a]	○	●	●	○	●	●	●
	Our work	●	●	●	○	●	●	●

[a] uses GnuPG as its backend