How to protect mobile application? Case: Nordea Codes

Michael Peltonen
Senior Business Developer, CISSP

11/10/2016

Making it possible

Michael Peltonen
Senior Business Developer, CISSP

Job History:

- Information Security Specialist / Global Product and Process Manager / Senior Business Developer at Nordea 2011 ->

- Security Consultant at Ericsson 2008 – 2011

Education / Certifications:

- Certified Information Systems Security Professional 2013 ->

- M.Sc.(Tech) from Helsinki University of Technology 2003 - 2009

Hobbies:

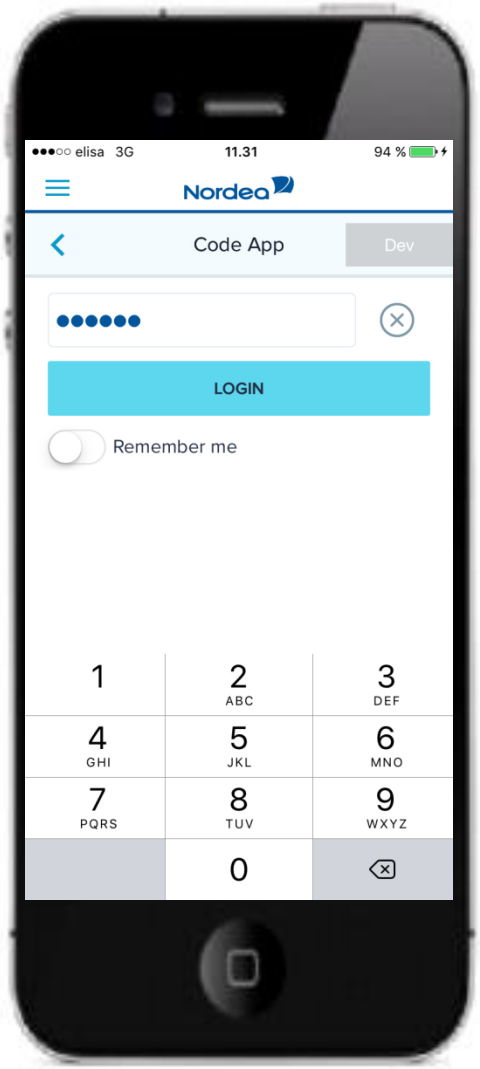
- Disc Golf
- Basketball
- Movies
- Technology
- Travelling

- Nordea Codes
- What threats are out there?
- How to protect against them?
- What about Nordea Codes?
- What about the future?
- Questions & Answers

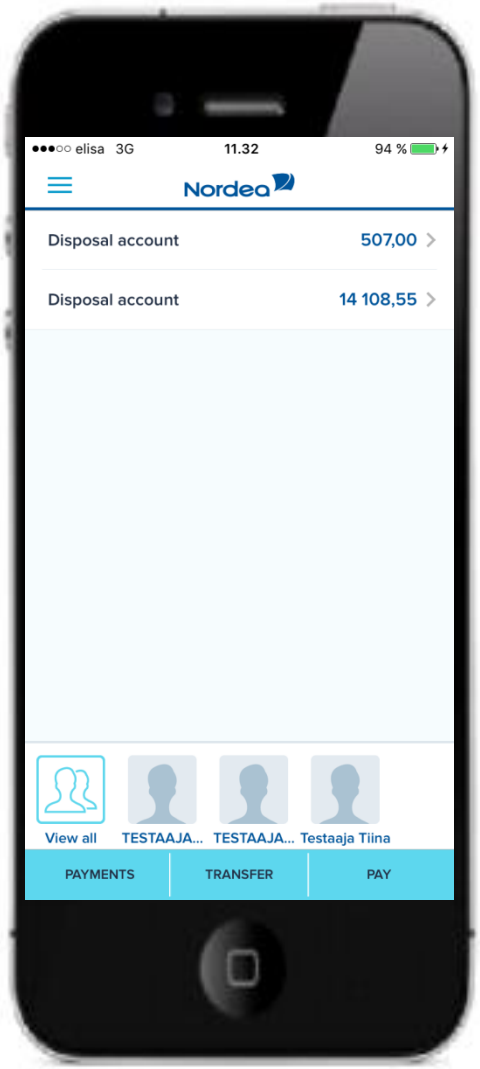
Nordea Codes

- An authentication and signing app released in June 2015
- A replacement for the paper based one-time-code card used by Nordea customers
- Can be used in all Nordea services

Demo


elisa 3G
11.31
94 %
Nordea
Code App
Dev
LOGIN
Remember me
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0


elisa 3G
11.31
94 %
Cancel
Nordea
Do you want to log in?
To private customer's Mobile bank.
PIN
1
2
3
4
5
6
7
8
9
0


elisa 3G
11.32
94 %
Nordea
Disposal account
507,00
Disposal account
14 108,55
View all
TESTAAJA...
TESTAAJA...
Testaaja Tiina
PAYMENTS
TRANSFER
PAY

950 m
vaaras
TEKNIIKKA 28.7.20
Ruut Tolonen HE

Iso hyö
Haittaohjelma
TALOUS 22.9.2015 2:00
Juhani Saa

Suu
jout
Van
vält
Osa vanh
TALOUS 20.
Juho-Pekka

Apple siirtyy uuteen käyttöjärjestelmään – iPhone 4S:n ja muiden vanhojen laitteiden riskit kasvavat

Apple ei tuo uutta iOS 10 -käyttöjärjestelmää esimerkiksi vanhoihin iPhone 4S -älypuhelimiin. Vanhoja puhelimia voi käyttää entiseen tapaan, mutta niistä voi paljastua tietoturvapuutteita.

TALOUS 6.9.2016 19:31

Juhana Rossi HELSINGIN SANOMAT

Turvaris
Hai Androic
tur kertoo,
mä älypuhe
tun
Android-puhelimis
monipuolistumises
TEKNIIKKA
Ville Eloran
TEKNIIKKA 20.3.2016 14:1
Juho-Pekka Pekonen H

Yli 900 miljoonaa Android-laitetta altistunut haittaohjelmalle – Suomalaisasiantuntija: Vanhojen puhelimien tiedot ehkä vaarassa

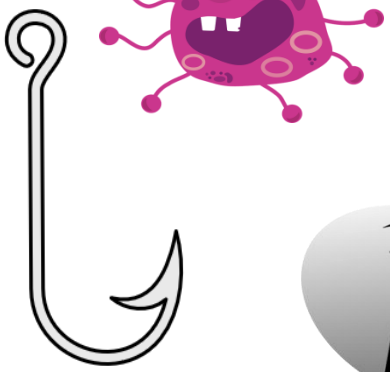
Tietoturvayhtiön ilmaisen puhelinsovelluksen avulla voi tarkistaa, onko Android-puhelin altistunut nyt löydetyille tietoturvariskeille. Ilmeisesti ainakin valtaosa Suomessa myydyistä Samsungeista on turvallisia, selviää HS:n lukijan testistä.

TALOUS 8.8.2016 12:00 Päivitetty: 8.8.2016 19:25

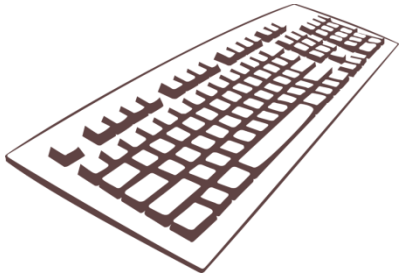
Paavo Teittinen HELSINGIN SANOMAT

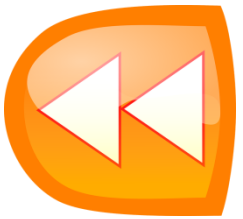
What threats are out there?

- Phishing
- Mobile malware
- Shoulder surfing
- Physical theft
- Bruteforcing
- Altered Android OS
- Cloning
- Man-in-the-middle
- Reverse engineering
- Data Leakage

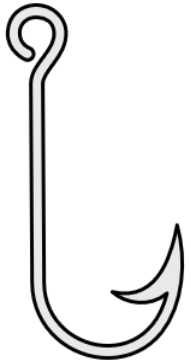





Phishing

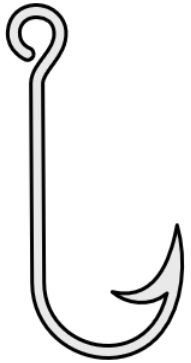


"The total number of unique phishing sites observed in the second quarter of 2016 was 466,065. This was 61% higher than the previous quarterly record in Q4, 2015." [1]

- Same threats on mobile as on PC
- Performed mainly by e-mail, SMS and phone calls
- Credit card information, banking credentials, usernames and passwords

[1] APWG Phishing Attack Trends Report - 2Q 2016

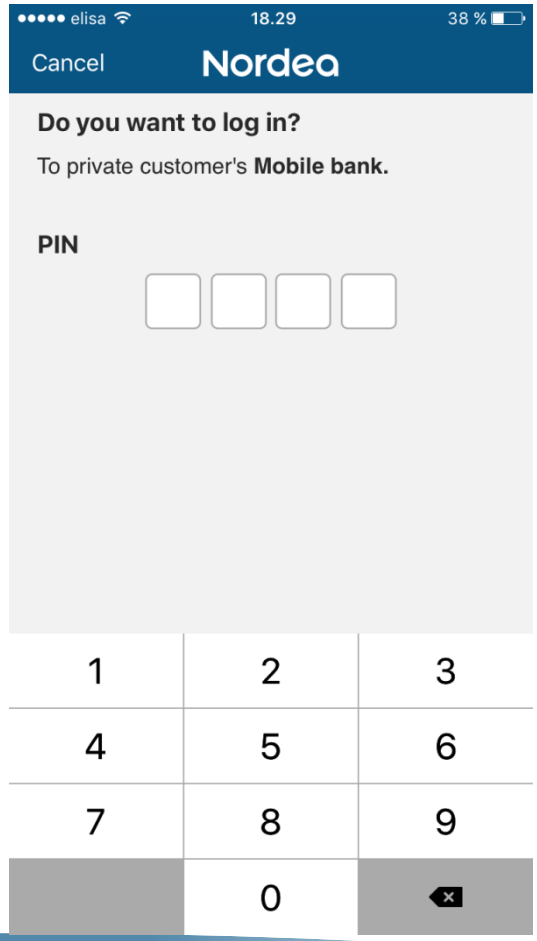
How to protect against phishing?

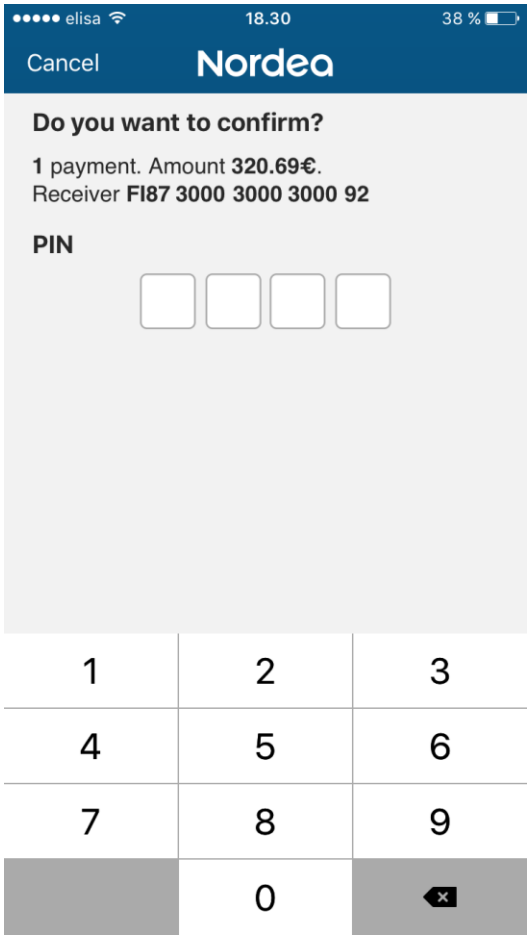


- Time based one-time-codes. As the codes are valid for only a short period of time, the window of opportunity shrinks.
- Content based one-time-codes. The codes contains the context of the code, so that it can only be used for a specific action or purpose.
- Not displaying the code to the end user. If the end user can't see the code, they can't give it out to an attacker.

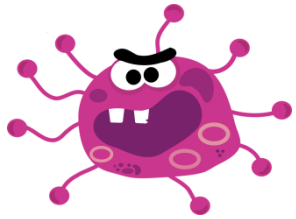
How is Nordea Codes protected against phishing?

- The app implements all protection methods making phishing of credentials impossible. All texts displayed in app is signed.





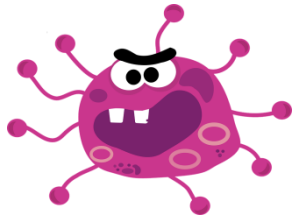
Mobile malware



- Utilizing vulnerabilities in Android and iOS
  - iOS 10 fixed 49 vulnerabilities [1]
  - October Android security bulletin listed 78 vulnerabilities [2]
- Same type of malware as on PC
  - Rootkits, spyware, adware, ransomware, etc.
- Malware usually root or jailbreak the phone

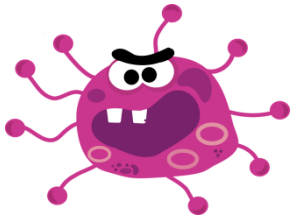
[1] Apple security updates
[2] Android security bulletins

How to protect against mobile malware?

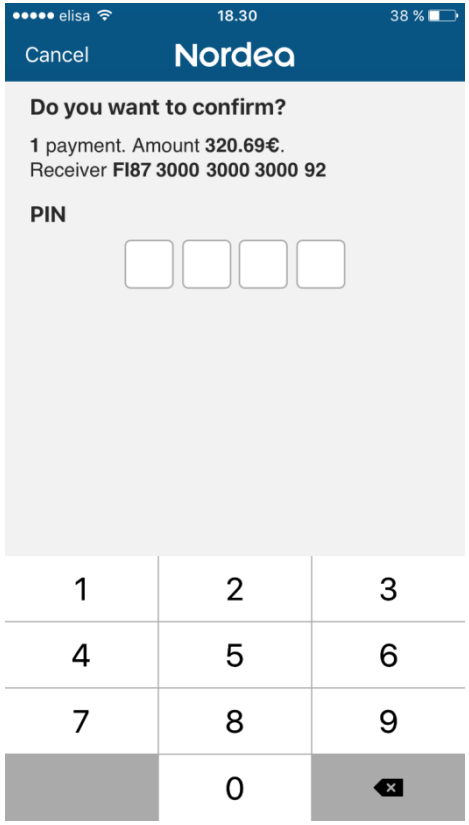


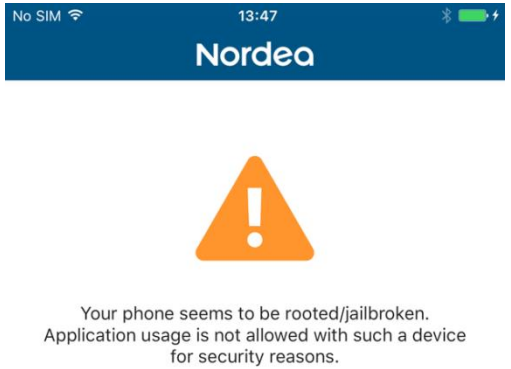
- Root or jailbreak detection
- Custom keyboard, no feedback from key presses, not allowed to take screenshots, scrambling keyboard for PIN entry
- Not storing customers credentials and wiping them from random access memory immediately after use. Don't store them as strings.
- Application integrity protection, hooking protection
- Publish your app only in the official app stores
- Download the platform SDKs from its official source

How is Nordea Codes protected against mobile malware?



- The application do not run on a rooted/jailbroken phone. If the application detects that phone is rooted/jailbroken it deletes all end user data
- The app uses a custom keyboard that gives no feedback about the keypresses
- On Android screenshots has been disabled
- The PIN is wiped immediately from RAM after use





Shoulder surfing

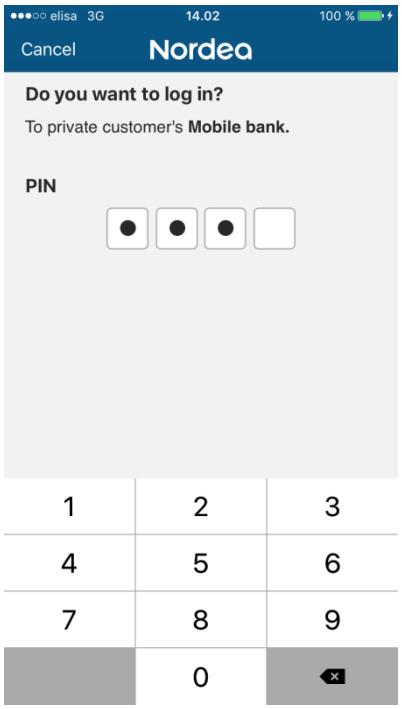
- Mobile devices are used in public places like busses, stores and bars
- More likely that credentials are shoulder surfed

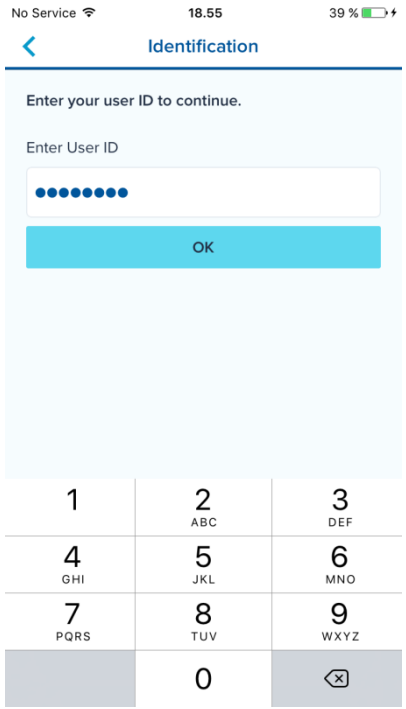
How to protect against shoulder surfing?

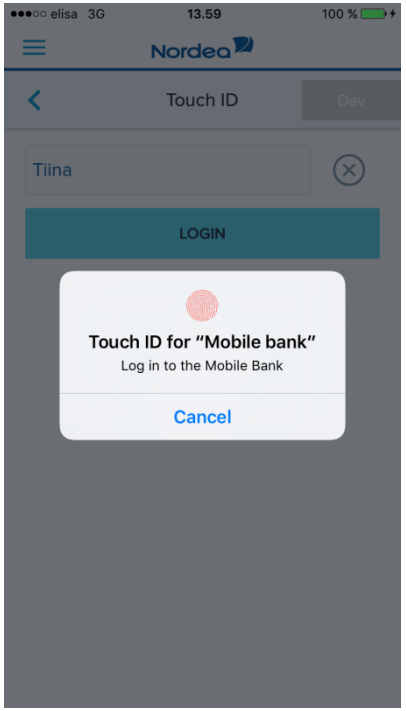
- Protect username, password and PIN entries
- Not showing a glimpse of the user entry nor giving any visual feedback
- Don't use too short secrets
- Use biometrics

How is Nordea Codes protected against shoulder surfing?

- In the Nordea Codes app the PIN code is never displayed and the keyboard gives no feedback
- In Mobile Bank before confirmation of actions your User ID is asked. You can also use fingerprint for log in.







Physical theft

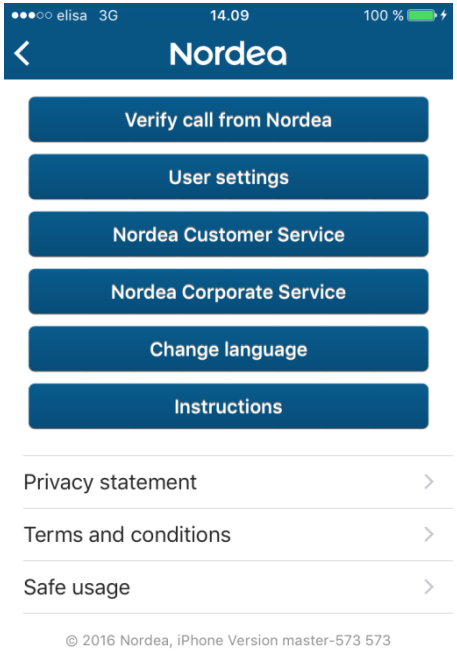
- Smart phones are expensive and contain a lot of valuable information
- Phones can be pick pocketed, snatched, lost or burgled
- Unprotected phones secrets can be acquired, sold and misused

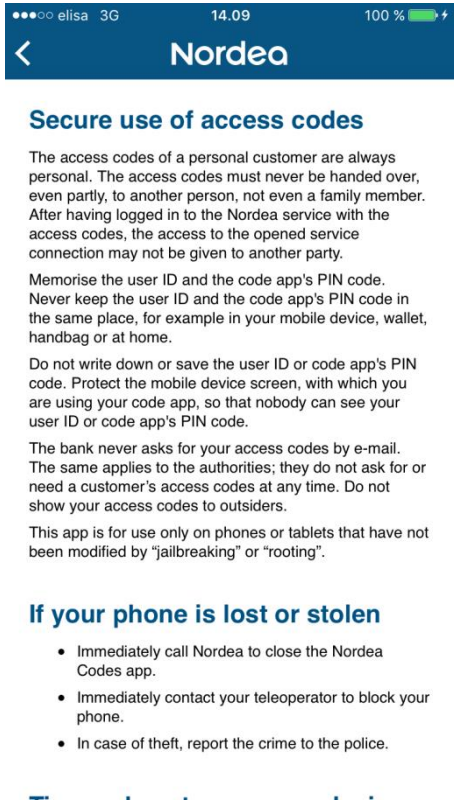
How to protect against physical theft?

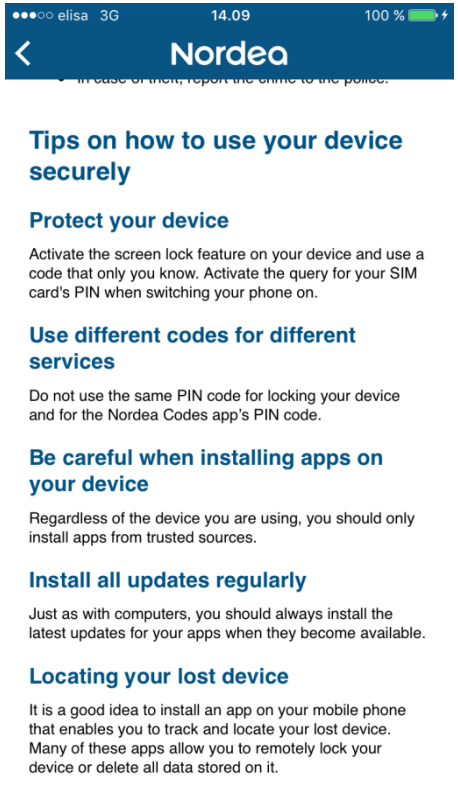
- Always ask for user identification in your application
- Don't store personal information on client side
- Advice people to use phone's lock screen

How is Nordea Codes protected against physical theft?

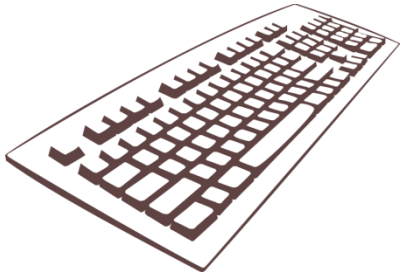
- The application does not store the PIN code and it’s immediately wiped from RAM after use
- We advise the end users on how they can protect their phone





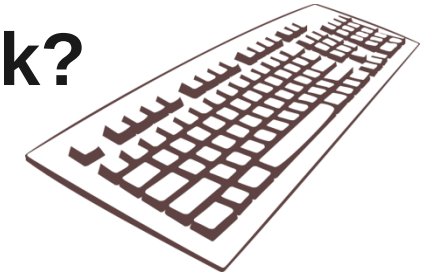


Brute-force attack



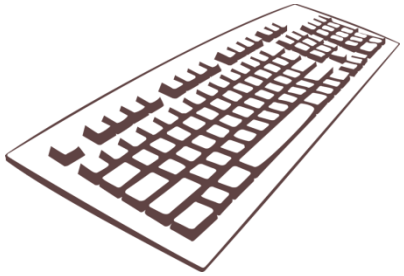
- As processing and memory capacity increases, brute force attacks can crack longer and more complicated passwords
- People don't tend to remember long and complicated passwords

How to protect against brute-force attack?

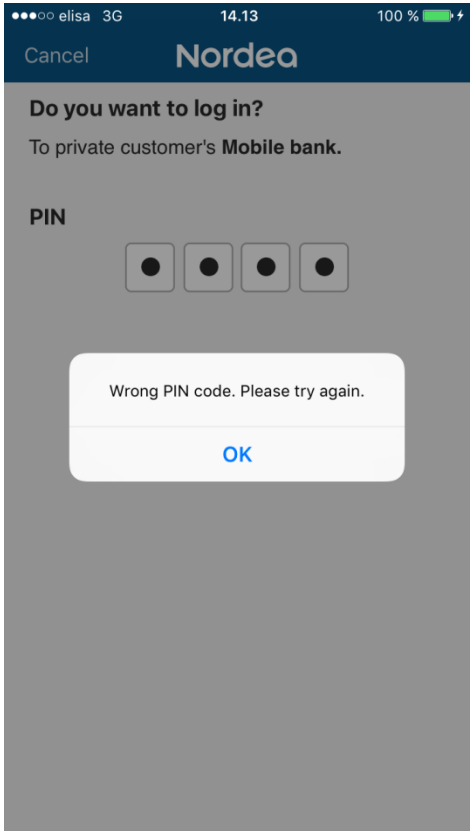


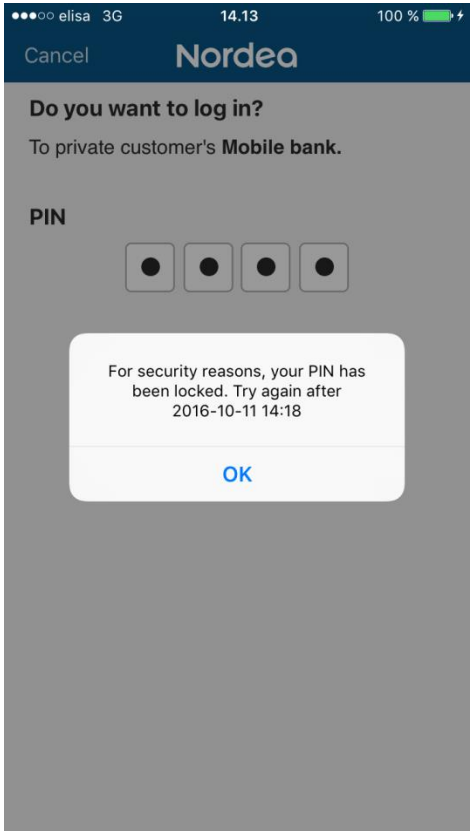
- Don't store secrets on the mobile client
- Limit the amount of tries on server side
- CAPTCHA
- Delays

How is Nordea Codes protected against brute-force attack?



- PIN not stored in client
- After 5 wrong PIN attempts the application is locked for 24 hours on server side
- After a certain amount of wrong PIN tries the application will be locked forever





Altered Android OS

- An altered Android OS could be used to log sensitive operations performed by an application, e.g. AES cryptographic operations

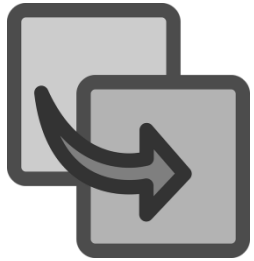
How to protect against altered Android OS?

- Provide own obfuscated libraries inside of the application for all sensitive operations, e.g. an own cryptographic library

How is Nordea Codes protected against altered Android OS?

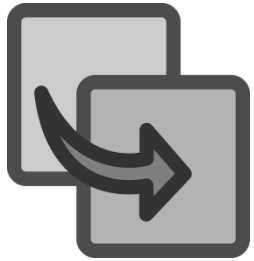
- The Nordea Codes app uses the Gemalto Ezio Mobile SDK that includes own libraries for all sensitive operations

Cloning



- By cloning an application an attacker could try to make a working copy of the application on their own device
- An attacker could either try to copy the application and its data from the device or a cloud backup

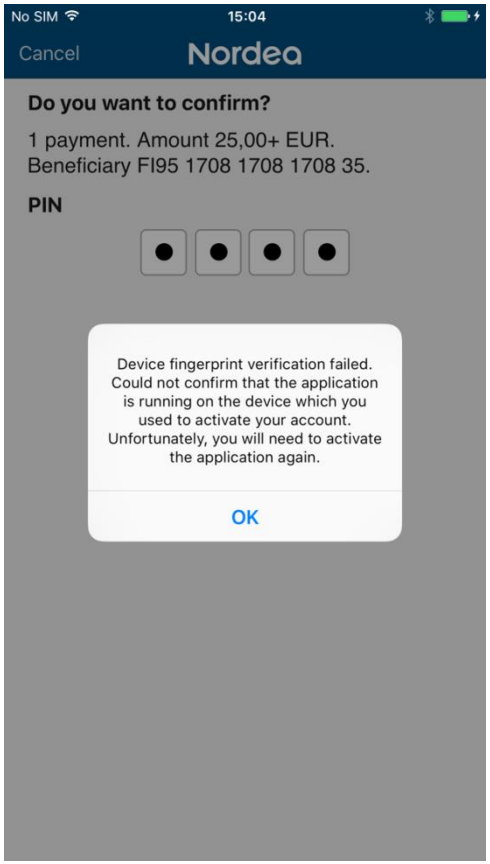
How to protect against cloning?



- Device binding
  - Hardware device information (e.g. IMEI/ESN, Mac address)
  - Soft information (e.g. ANDROID_ID, UID)
  - Service information (e.g. IMSI)
  - Custom fingerprint data
- Back-up to cloud is not possible

How is Nordea Codes protected against cloning?

- During the activation of the Nordea Codes application the application is bound to the hardware and software. Addition to this we are using custom fingerprinting data
- Back-up to cloud has been disabled, as any back-ups would not work



Man-in-the-middle attack

- Rogue wireless access points that offer free Wi-Fi can steal your credentials and data by a man-in-the-middle attack
- The rogue access point can tamper with or forward the traffic between the application and the server

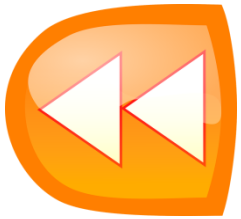
How to protect against a man-in-the-middle attack?

- Protecting the communication channel just with TLS is not enough for preventing the attack
- You need to do certificate pinning in the application so that it refuses to communicate to any other than genuine servers
- Add another layer of encryption inside the TLS communication path

How is Nordea Codes protected against man-in-the-middle attack?

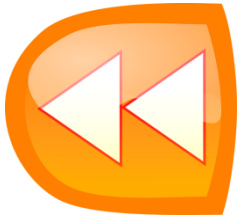
- The communication channel is protected with TLS and additional encryption
- The certificate is pinned on client and server side, so that nothing can be added in-between

Reverse engineering



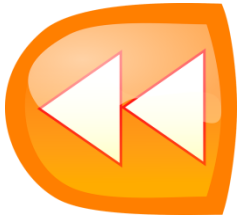
- Mobile application binaries can be reverse engineered back to readable code
- This gives potential attackers insight into how the application works and where it can be attacked
- It also enables attackers to tamper with the code and make their own malicious binaries

How to protect against reverse engineering?



- Code obfuscation. The source code is transformed into unreadable code in the binary build chain.
- Code expansion. The source code is made more complicated and unreadable by adding useless paths, methods and variables.

How is Nordea Codes protected against reverse engineering?



- The Nordea Codes application is obfuscated on all three platforms (iOS, Android and Windows Phone) with commercial obfuscation tools

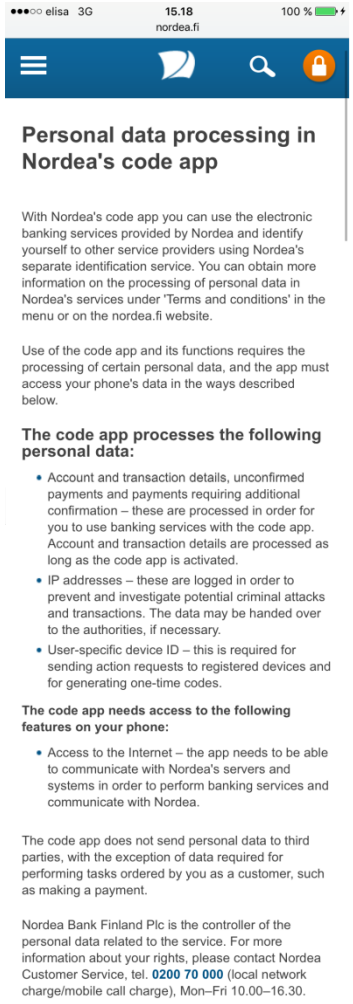
Data Leakage

- Storing data about the end user on the mobile device risks the data being leaked
- The data can be stolen from the device or from a cloud backup

How to protect against data leakage?

- Store only data in the mobile client that is absolutely needed for the application to work
- Never store data in clear text
- Use the secure storage and encryption services provided by the platform (iOS KeyChain, Android Keystore)

How is Nordea Codes protected against data leakage?



- Minimum amount of information is stored and processed
- The keys are stored in the secure storage provided by the platform. The keys are useless without the end users PIN code and the device binding data.

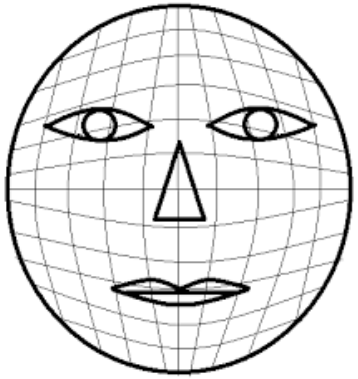
I have protection against all threats, what now?

- Use a third party security company to do:
  - security audit on the source code
  - perform penetration testing
- Ensure that secure coding practices are followed
  - E.g. use the OWASP Secure Coding Practices Quick Reference Guide

Future considerations: Biometrics

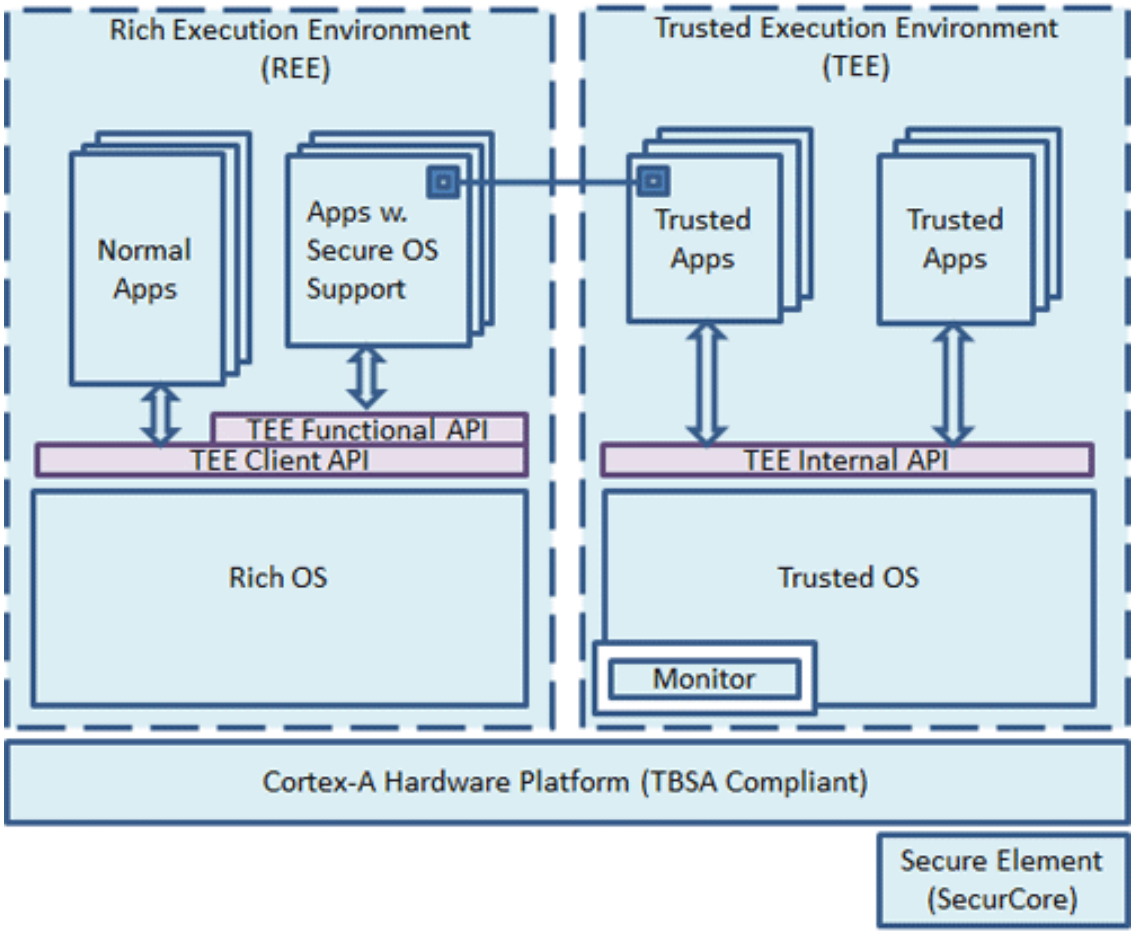
- Fingerprint authentication
  - Apple: Touch ID introduced 2013 in iPhone 5S [1]
  - Samsung: first fingerprint scanner 2014 in Galaxy S5 [2]

- Facial recognition
  - Mastercard: selfie payment available in Europe Oct 2016, worldwide in 2017 [3]



[1] Use Touch ID on iPhone and iPad
[2] Samsung Galaxy S5 unveiled
[3] Mastercard selfie payment

Future considerations: Trusted Execution Environment



https://www.arm.com/products/processors/technologies/trustzone/tee-smc.php

Q&A


elisa 3G
12.44
74 %
Nordea
Tunnuslukusovellus odottaa tapahtumia...
Aloita kirjautuminen, tunnistautuminen tai vahvistaminen sähköisissä palveluissa.

Thank you!