TRAFICOM
National Cyber Security Centre

Mobile Authn AppSec

Verification Criteria

OWASP Helsinki, September 3rd

Petteri Ihalainen, NCSC-FI

Who?

- Finnish Transport and Communications Agency, Traficom
  - National Cyber Security Centre
    - eIDAS division – we supervise, consult and help to the best of our abilities
      - Senior Specialist, Petteri Ihalainen

- www.kyberturvallisuuskeskus.fi/en & https://www.kyberturvallisuuskeskus.fi/fi/sahkoinen-tunnistaminen

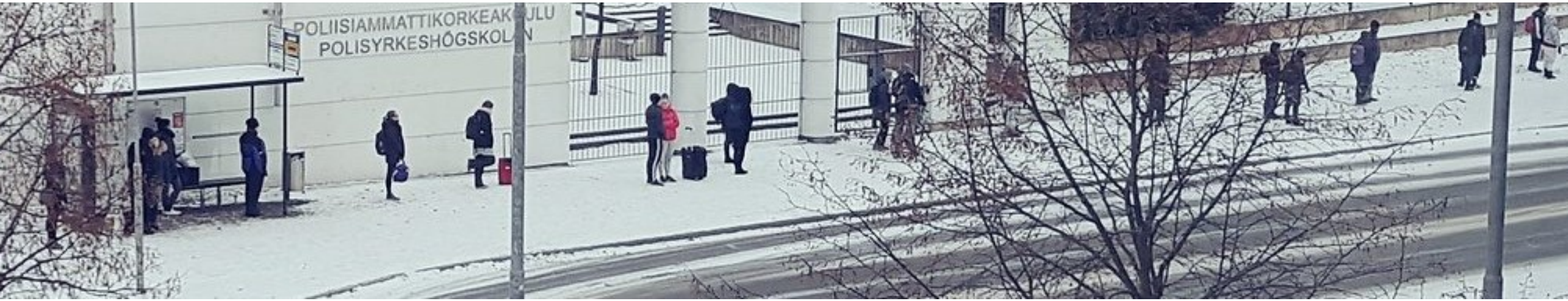
- LinkedIn: www.linkedin.com/in/door
- Twitter: @ihalain

Agenda

- Background
- LoA
- Why
- What
- How
- When
- Q&A

We Are Geek

- Technogeek nation with heavy emphasis on personal privacy (leave me alone, don’t talk to me, do NOT come within 1m of me...)
  - Mobile phone: To avoid F2F personal contacts (customer service)
  - SMS, (äm) Internet Relay Chat: To avoid actually speaking to someone
  - Mobile data usage 2018: nr 1 in the world: DNA Finland: 19,8GB / user / month



Europe & Finland

- eIDAS regulation in 2014
- Our local law (Tunnistuslaki, TunnL) 2016 that transports eIDAS into local legislation
  - Strong Authn (& trust services)
  - Federation ← something unique in the EU/world as we created the Finnish Trust Federation Network or Finnish Trust Network
- The ”perfect” storm conditions for Auth providers
  - 2016 law with 2+1 year transition for the old bank auth protocol (end of Sept 2019)
  - PSD2 and Strong Customer Authentication (mid Sept 2019)

➔ NEW COOL STUFF FROM BANKS

Level of Assurance

- EU LoA → COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502
  - Low
  - Substantial
  - High
- FI
  - Low → not supervised, example: password, social
  - Substantial → supervised, almost all transactions in FI, example: OTP list, dongle, Mobile App, Mobile ID
  - High → supervised, 1 IdP (Government), smart card, heavy use in the public sector / organisations. Citizen use, not so much...

Why an App – Educated Guessing Session

- Economics & security
  - Print-out OTP lists do not comply with PSD2 RTS SCA (copying)
  - Overall improved security with apps compared to previous ”technologies”
  - Price?
- Mobile banking on the rise
- OTP devices to edge case users only

The 6 step program

1. Establish a bank, MNO or similar...
2. Get loads of customers (optional)
3. Buy/build the infrastructure including authn solution (this could also be nr 2, depends if you are marketing oriented or dev oriented)
4. Audit the authn solution
5. Notify Traficom eIDAS department through the website about:
   - New authn solution
   - LoA
   - Include audit report(s) ”it really is secure”
6. Sit back & relax and wait for us to process your application
   - If ok – Join FTN as a distinguished member of a unique network

Why develop a (national) criteria?

- Smart cards != Mobile Apps

- 3 rules
  - The user is not in control of his/her environment
  - The user is clueless
  - The OS is broken
  - → Abandon all hope and run? No – you do your best to protect the secret

- Security is at the core of the organisations selling mobile authn apps... Right?

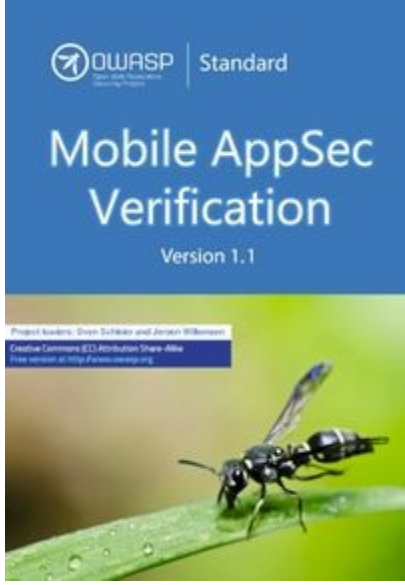
What?

- Building on existing work by the security community & international experts: OWASP Mobile AppSec Verfication Criteria (first released in 2018). Other sources include e.g. FIDO security reference
- Extending the chapter 4 (Authentication) of the OWASP criteria
- Working group consists of
  - Finnish & Nordic Banks
  - Mobile Network Operators (Elisa, Telia, DNA)
  - Commercial vendors (Gemalto, Inside Secure, Ubisecure)
  - Finnish Police Board
  - Companies offering audit services (Nixu, F-Secure)
  - Identity Brokers (NETS, Signicat, Fujitsu)
- Together with the financial authority to ensure compatibility with PSD2 RTS SCA

OWASP Model – 3 layer approach

- Basic (L1)
  - Dum dum level – but still we see some of these fail when we review audit reports
- Advanced (L2)
  - More resistance against attacks, perhaps making it possible to create a method (means) at eIDAS level ”Substantial” or even ”High”?
  - Traficom view: All L2 criteria will be included, but does not guarantee an automatic approval of ”Substantial” nor ”High” – after all, the whole system needs to be evaluated to determine the LoA
- Resilience (R) - chapter 8
  - OWASP: For sensitive mobile applications, Traficom: adopted and modified in our criteria
  - Resistance against reverse engineering and tampering

What’s that OWASP thing?



- Application Security Verification framework & guides
- Mobile – now at version 1.1.3
  - Chapter 1: Architecture, Design and Threat Modelling (10 criteria)
  - Chapter 2: Data Storage and Privacy (12 criteria)
  - Chapter 3: Cryptography (6 criteria)
  - Chapter 4: Authentication and Session Management (OWASP: 11 criteria → AuthnAppSec : 30+ criteria)
  - Chapter 5: Network Communication (6 criteria)
  - Chapter 6: Platform Interaction (8 criteria)
  - Chapter 7: Code Quality and Build Setting (9 criteria)
  - Chapter 8: Resilience (12 criteria)

What are the new things? Examples (HOW?)

- Chapter 4…
  - eIDAS LoA mapping for **each ~100 criteria**
  - Authentication cannot be based on shared secret only
  - Hard fail certificate pinning must be used (Trusted Path) – not a liked feature perhaps in the enterprise environment
  - The available security features of the platform (phone) should be used in full
  - The user must be informed to delete/remove other biometric data than his own from the device (iPhone TouchID/FaceID problem), or additional methods must be used to uniquely identify the user
  - No biometric data shall be transmitted outside the app
  - The secret(s) must NOT be included in any form in a backup (cloud backup, ”desktop” backup, etc)
  - If a hardware component becomes vulnerable, the solution can compensate

Example from the Authn chapter

6.4 Authentication, characteristics of the authentication method; session management

This chapter employs the OWASP standard and chapter 4 where applicable. Additional criteria relating to the characteristics of the authentication method are also provided.

Criterion	Justification	Additional information / comment
432. The procedure used for the personalisation of the app at registration phase ensures that the app is linked to the holder of the identification means.	LOA, section 1 (definitions), point 2 LOA, section 2.2.1, point 2	
433. The secret used for implementing the identification is protected against unauthorised use and can only be accessed using a predefined, secure method.	LOA, section 2.4.6, point 3 LOA, section 2.4.6, substantial M72A, section 6, paragraph 3	Example: private key.
434. Secrets/identification keys are unique.	M72A, section 5.1, paragraph 2g)	
435. Asymmetric secrets that implement the identification are created in the mobile device (key pair, other secret key/secret).	M72A, section 5.1, paragraph 2g) M72A, section 5.1, paragraph 3b)	Cf. RTS.
436. If secrets used to implement the identification are created outside the device, they are provisioned to the device using a secure method.	LOA, section 2.4.6, point 2 LOA, section 2.4.6, substantial M72A, section 5.1, paragraph 3b)	Cf. RTS.

Challenges

- How to treat biometric methods? Can they stand on their own as a factor?
  - FaceID –type of scenarios especially on Android devices?
  - iOS biometric does not identify the user
  - Twins, siblings etc
  - Attack potential considering all the various devices & sensors in the market

    ➔ Depends...
- Remote registration?
- Are your rooted? ”No I’m not – trust me...”
- Stakeholders request LoA guidance: ”If we implement this feature A, can we get High?”
  - We need to evaluate the whole system, not just the fancy mobile app
- Mobile AuthnApp & (Remote) signing?

When

- Work started end of 2018
- 6 working group meetings (4 were concentrated mostly on the mobile criteria)
- Request for comments ended 2 weeks ago
- Draft FI/SE/EN versions of the 176 page doc is available through our site
  - Less than 20 pages for the mobile authn appsec verification...
- We hope to have this adopted into the official OWASP portfolio
- Promoted at EU level to other member states
- ... And push this down to the vendors and have them integrate this to their own development frameworks

  → This will become a selling point in their PPTs???

  → We will all be safer... Who has got the guitar? Let's make a fire and sing songs of...

Why should You care???

- Because you are trying to protect an asset with the authn solution – don't use a strong looking styrofoam door, use the real thing
- Ask yourself again – do you know that the mobile tech you just bought / are about to buy is secure?
- Ask your vendor for proof on how they determine the security of their app technology – if they say "We use the best of the best of the best methods in our dev&products – we are 110% secure" – RUN (or at least give them a chance to prove they're worthy – hint: they're not)

TRAFICOM
National Cyber Security Centre

Thank You – Questions?

petteri.ihalainen (@) traficom.fi

Twitter: @ihalain

LinkedIn: www.linkedin.com/in/door