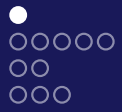
Bootstrapping authentication and recovery

Daniel Bosk

Department of Information and Communication Systems,
Mid Sweden University, Sundsvall

5th November 2020



1 Bootstrapping authentication

- What is bootstrapping?
- Problems and recovery
- Give the problem to someone else

Bootstrapping: A chicken-and-egg problem

- Alice is not registered in our authentication system.
- We want to register her as a user in our system.
- How do we know Alice is actually Alice?
- Since she's not registered, we don't have anything to authenticate her.

Exercise

- Any quick workarounds that comes to mind?
- When is this a problem and when is it not?

Bootstrapping: A chicken-and-egg problem

- Alice is not registered in our authentication system.
- We want to register her as a user in our system.
- How do we know Alice is actually Alice?
- Since she's not registered, we don't have anything to authenticate her.

Exercise

- Any quick workarounds that comes to mind?
- When is this a problem and when is it not?

Bootstrapping: A chicken-and-egg problem

- Alice is not registered in our authentication system.
- We want to register her as a user in our system.
- How do we know Alice is actually Alice?
- Since she's not registered, we don't have anything to authenticate her.

Exercise

- Any quick workarounds that comes to mind?
- When is this a problem and when is it not?

Solution (We don't care who Alice is)

- *We simply set up authentication when Alice creates the account.*
- *Now we can authenticate whoever set up the account.*

Remark

- The attribute here is account ownership.

Example

- This is the solution used by most web services.

Solution (We don't care who Alice is)

- *We simply set up authentication when Alice creates the account.*
- *Now we can authenticate whoever set up the account.*

Remark

- The attribute here is account ownership.

Example

- This is the solution used by most web services.

Solution (We care who Alice actually is)

- *We can require ID checks etc. to set up the authentication mechanisms using a helpdesk.*
- *If we have address etc., then we can send the credentials via mail (be it snailmail or email).*

Remark

- The attribute here is identity.
- ID checks trust in the issuer.
- Sending via mail trusts the mail system.

Solution (We care who Alice actually is)

- *We can require ID checks etc. to set up the authentication mechanisms using a helpdesk.*
- *If we have address etc., then we can send the credentials via mail (be it snailmail or email).*

Remark

- The attribute here is identity.
- ID checks trust in the issuer.
- Sending via mail trusts the mail system.

Solution (We care who Alice actually is)

- *We can require ID checks etc. to set up the authentication mechanisms using a helpdesk.*
- *If we have address etc., then we can send the credentials via mail (be it snailmail or email).*

Remark

- The attribute here is identity.
- ID checks trust in the issuer.
- Sending via mail trusts the mail system.

Exercise

- How is Alice authenticated when she applies for an ID?

Example (Signal, WhatsApp, . . .)

- Relies on ownership of (mobile) phone number.
- Send a text message with a code.

Remark

- Assumes trustworthy phone infrastructure and operator.
- Phone operator can impersonate.
- Government can impersonate (forcing phone provider).

Example (Signal, WhatsApp, . . .)

- Relies on ownership of (mobile) phone number.
- Send a text message with a code.

Remark

- Assumes trustworthy phone infrastructure and operator.
- Phone operator can impersonate.
- Government can impersonate (forcing phone provider).

Remark

- How to recover from failure?

Example

- You sign up for a Google account.
- You forget your password . . .

Example

- You sign up for a Facebook account.
- Someone guesses your password and takes over your account.

- Sometimes this is a continuous process.
- The same bootstrapping procedure can sometimes also be used for *recovery from failure*.
- Make sure the system can handle forgotten, lost or aged authentication means.

Idea

- We could let someone who has solved the problem already do the authentication for us.

Remark

- This make it easier for the user.
- This makes the provider a very attractive target.
- We must trust them to do it properly . . .

Idea

- We could let someone who has solved the problem already do the authentication for us.

Remark

- This make it easier for the user.
- This makes the provider a very attractive target.
- We must trust them to do it properly . . .

Example (We don't care who Alice is)

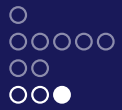
We can use Google, Facebook *etc*.

Example (We care who Alice is)

We can use *e.g.* BankID.

Remark

This third party must have done bootstrapping as rigorously as we would have.



Give the problem to someone else