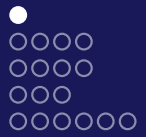
Introduction to authentication

Daniel Bosk

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

5th November 2020



1 Introduction to authentication

- Identification and authentication
- Authenticating
- DIY or trust
- Time of check, time of use

Definition (Identifier)

- An identifier is a piece of data that uniquely identifies some entity.

Example (Identifiers)

- An email address identifies a user uniquely in the email system.
- A username identifies a user in some system.
- A passport number uniquely identifies a passport issued by a country.

Definition (Authentication)

- Some entity claims some attribute of some data.
- *E.g.* identity: 'identifier X identifies me'.
- Authentication is about verification.
- That entity must *convince* us that its claim is true.

Exercise: How can we authenticate . . .

1. the claim of an email address?
2. the claim of a username in some system?
3. the claim of a passport number?
4. the claim of a national identity in some country?

Definition (Authentication)

- Some entity claims some attribute of some data.
- *E.g.* identity: 'identifier X identifies me'.
- Authentication is about verification.
- That entity must *convince* us that its claim is true.

Exercise: How can we authenticate . . .

1. the claim of an email address?
2. the claim of a username in some system?
3. the claim of a passport number?
4. the claim of a national identity in some country?

Example (User authentication)

Identification First you enter your username to *identify* yourself.

Authentication Then you enter your password to *authenticate* that you are truly you.

Exercise

Why does this work?

Example (User authentication)

Identification First you enter your username to *identify* yourself.

Authentication Then you enter your password to *authenticate* that you are truly you.

Exercise

Why does this work?

Example

- Identity is simply an attribute.
- Age is another attribute.
- ‘Authorized to read document X’ is also an attribute.
- ‘Is an administrator’ is an attribute too.

Example (Age limits)

- Bob wants to go see a film in cinema.
- Bob looks very young so Alice who works there wants to have proof of his age.
- Show physical ID; reveals name, exact date of birth, ...

Exercise

- That's a bit overkill, right?
- What does Alice actually need to know?
- In what direction must we move to achieve that?

Example (Age limits)

- Bob wants to go see a film in cinema.
- Bob looks very young so Alice who works there wants to have proof of his age.
- Show physical ID; reveals name, exact date of birth, ...

Exercise

- That's a bit overkill, right?
- What does Alice actually need to know?
- In what direction must we move to achieve that?

Example (Age limits)

- Bob wants to go see a film in cinema.
- Bob looks very young so Alice who works there wants to have proof of his age.
- Show physical ID; reveals name, exact date of birth, ...

Exercise

- That's a bit overkill, right?
- What does Alice actually need to know?
- In what direction must we move to achieve that?

What Alice needs?

She must be convinced that Bob is older than 15.

How can she learn that?

1. She has known Bob since he was born, so she knows.
2. She can ask someone *she trusts* who knows Bob is older than 15.

What Alice needs?

She must be convinced that Bob is older than 15.

How can she learn that?

1. She has known Bob since he was born, so she knows.
2. She can ask someone *she trusts* who knows Bob is older than 15.

What Alice needs?

She must be convinced that Bob is older than 15.

How can she learn that?

1. She has known Bob since he was born, so she knows.
2. She can ask someone *she trusts* who knows Bob is older than 15.

But how can she do that?

1. The trusted person who knows Bob is with Alice.
2. Alice can send a picture to the other person who verifies.
   - This requires an *authenticated* channel.
3. The trusted person made a certificate for Bob showing that he's older than 15.
   - Alice must be able to *verify* the certificate.
   - Bob must not be able to forge such a certificate.
   - Bob must bring this certificate with himself everywhere.

But how can she do that?

1. The trusted person who knows Bob is with Alice.
2. Alice can send a picture to the other person who verifies.
   - This requires an *authenticated* channel.
3. The trusted person made a certificate for Bob showing that he's older than 15.
   - Alice must be able to *verify* the certificate.
   - Bob must not be able to forge such a certificate.
   - Bob must bring this certificate with himself everywhere.

But how can she do that?

1. The trusted person who knows Bob is with Alice.
2. Alice can send a picture to the other person who verifies.
   - This requires an *authenticated* channel.
3. The trusted person made a certificate for Bob showing that he's older than 15.
   - Alice must be able to *verify* the certificate.
   - Bob must not be able to forge such a certificate.
   - Bob must bring this certificate with himself everywhere.

Alice interacts with the trusted person

- Gaah, but Bob doesn't want the trusted person (his parents) to know he's at the cinema right now!
- It's a small cinema so they'll know which film he sees if they learn when he's there.

Alice reads and verifies the certificate

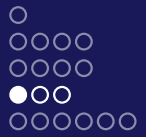
- Phew, she accepted the note from his parents.
- But now Alice learned all those embarrassing things in there.

Alice interacts with the trusted person

- Gaah, but Bob doesn't want the trusted person (his parents) to know he's at the cinema right now!
- It's a small cinema so they'll know which film he sees if they learn when he's there.

Alice reads and verifies the certificate

- Phew, she accepted the note from his parents.
- But now Alice learned all those embarrassing things in there.



- Some attributes we can verify ourselves (*i.e.* DIY).
- For other attributes we rely on someone else (*i.e.* trust).

Example (Verify ourselves)

- I sign a note saying 'Pay 10 SEK for this note'.
- I give you this authentication token if I owe you 10 SEK.
- I can verify the authenticity of the note when you claim the money.

Example (Trust someone else)

- I ask your age.
- You show me your ID card.
- I trust the card issuer and read your birthday.

Example (Verify ourselves)

- I sign a note saying 'Pay 10 SEK for this note'.
- I give you this authentication token if I owe you 10 SEK.
- I can verify the authenticity of the note when you claim the money.

Example (Trust someone else)

- I ask your age.
- You show me your ID card.
- I trust the card issuer and read your birthday.

Remark

- Both methods use ‘authentication tokens’.
- Security depends on forgeability of those.

Remark

- Whenever we authenticate a user, we do this for a purpose.
- When does this authentication take place in relation to when we make use of it?

Example (Bank office)

- Customer shows ID to clerk, clerk verifies account owner (authentication).
- Clerk helps the customer.
- Customer leaves.

Example (Personal computers)

- User starts the computer in the morning.
- User logs in (authentication step).
- User goes for coffee.
- User comes back.
- User goes to lunch.
- User comes back.
- ...
- User turns the computer off.

Remark

- The key difference is that the first (bank) has 'continuous authentication', the clerk notices if the customer changes.
- The computer doesn't see the difference who's at the keyboard.
- We need continuous authentication for the computer too.

Solution

- *We can approximate that with repeated authentication.*
- *We could also authenticate anew when we need to do something requiring more privileges, and if it has been a while since last time.*
- *The computer could monitor the user's behaviour.*

Time of check, time of use