Machine-to-user authentication

Daniel Bosk

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

5th November 2020

1 Machine–user authentication

- What's the problem?
- How to solve?

What's the problem?

Question

- How can a user tell something legitimate from something illegitimate?

Example

- Payment terminal in the supermarket?
- Email from someone?
- Web page?

What's the problem?

Definition (Spoofing/Masquerading)

- Attacker masquerades as authorized.
- To a system: impersonates authorized user.
- To a user: impersonates legitimate system/UI/part of UI.

What's the problem?

Definition (Phishing)

- A masquerading attack trying to collect sensitive data.

Example

- Email from IT department requesting the password.
- See `https://phishingquiz.withgoogle.com/`.

How to solve?

Exercise

How can we prevent spoofed interfaces?

How to solve?

Solution (In general)

- *Must have some trusted interface.*

Example

- The computer and web browser are trusted.
- Web pages are not.
- But the browser tries to aid.

How to solve?

Example

- The computer, browser and web pages are untrusted.
- The mobile phone with BankID is trusted.

Example

- The payment terminal is untrusted.
- The payment card is trusted.
- How to communicate with the payment card? — Through the untrusted terminal.

Example

- The computer, browser and web pages are untrusted.
- The mobile phone with BankID is trusted.

Example

- The payment terminal is untrusted.
- The payment card is trusted.
- How to communicate with the payment card? — Through the untrusted terminal.

Example

- Windows has a trusted path.
- Uses the Ctrl+Alt+Del to bring up the authentication dialogue upon login.
- How many know that?

Example

- Windows has a trusted path.
- Uses the Ctrl+Alt+Del to bring up the authentication dialogue upon login.
- How many know that?

How to solve?

Summary

- Users must have trusted devices.
- Users must not make mistakes setting these up.
- We must do great usability to aid them.

Remark

- This is a very hard problem to solve.

How to solve?

Summary

- Users must have trusted devices.
- Users must not make mistakes setting these up.
- We must do great usability to aid them.

Remark

- This is a very hard problem to solve.

How to solve?