mobile business

Lecture 02

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Information & Communication Security (WS 2016/17)

Authentication

Prof. Dr. Kai Rannenberg

Deutsche Telekom Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.

mobile business

Agenda

- Introduction
- What you know
- What you have
- What you are
- Where you are
- Multi Factor Authentication
- Authentication protocols

Introduction

- **Definition:** Authentication is the binding of an identifier to a subject.
- The subject must provide information to enable the system to confirm the relation between subject and identifier.
- The goal of an authentication system it to ensure a correct identification of entities.

[Bi05, modified]

Authentication Information

- The information comes from one (or more) of the following:
  - What the subject knows
    - PIN, passwords, pass-phrases, secret information
  - What the subject has
    - Keys, tokens, smart cards
  - What the subject is
    - Fingerprints, iris, retinal characteristics
  - Where the subject is
    - In front of a particular terminal, located by a particular radio receiver

[Bi05]

Authentication Process

- The authentication process consists of:
  - Obtaining authentication information from the subject
  - Analyzing the data
  - Determining if data is associated with that subject
- The computer must store some information about the subject.
- A mechanism for data management is required.

mobile business

Agenda

- Introduction
- What you know
- What you have
- What you are
- Where you are
- Multi Factor Authentication
- Authentication protocols

mobile business

Passwords

- Passwords are the typical example of an authentication mechanism based on **what you know.**
- A password is information associated with an entity that confirms the entity's identity.
- **Example:** each user chooses a sequence of 8 digits as a password. Then A (the set of possible passwords) has 10^8 elements (from "00000000" to "99999999").

Attacking a Password System

- Threatening the subject
- Password guessing
- Password spoofing
- Compromise of password file
- Social engineering

mobile business

Threatening the Subject

Password Guessing

- **Exhaustive search (a.k.a. brute force):** try all possible combinations of valid symbols, up to a certain length.
- **Intelligent search:** search through a restricted name space, e.g. try passwords that are somehow related with a user or generally popular.
  - Example: Dictionary attack

User Side Defenses

- Set a password:
  - If no password is set, the attacker is even spared the trouble of guessing one.
- Change default passwords
- Password length
  - To thwart exhaustive search, a minimal password length should be prescribed.
- Password complexity
  - Mix upper and lower case symbols and include numerical and non alphabetical symbols.
- Avoid obvious passwords
- Do not re-use passwords on different systems

System Defenses

- Proactive password checkers
  - Search for weak passwords by administrator
- Password generation
  - Computer produces random passwords
- Password ageing
  - Set expiry date for passwords
- Limit login attempts
  - Lock account after multiple unsuccessful login events
- Inform user
  - Show time of last login, after a successful login.

Password Spoofing

- Identification and authentication through username and password only provide *unilateral authentication*.
- Does the user know who has received the password? -> No
- The user has no guarantees about the identity of the party at the other end of the line.

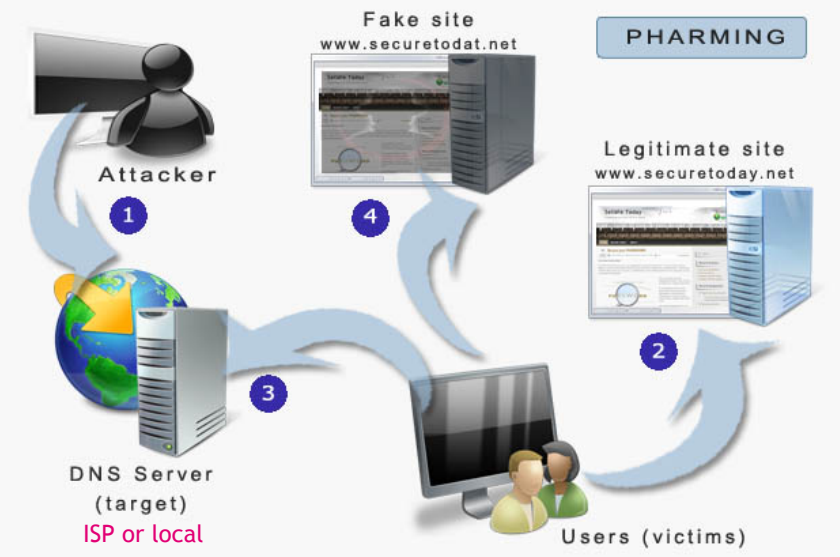
mobile business

Password Spoofing

- The attacker runs a program that presents a fake login screen.
- An unsuspecting user tries to login at that terminal.
- The victim is asked for username and password.
- These are then stored by the attacker.
- Login is aborted with a (fake) error message and the spoofing program terminates.
- Often, the user is then redirected to the real login screen.

Example: Pharming

- When users ask for an IP address to match a URL, a wrong one is provided.
- Attack against DNS server or user's PC.



Source: http://www.securetoday.net/

- When users try to access the attacked website they are redirected to the fake site

Countermeasures

- Displaying the number of failed logins:
  - If your 1st login fails but you are told at the 2nd attempt that there has been no unsuccessful login attempt, you should become suspicious.
- Trusted path:
  - Example: CRTL+ALT+DEL in Windows XP
    Guarantee that the user is communicating with the operating system and not with a spoofing program.
- Mutual authentication:
  - The system could be required to authenticate itself to the user.

Compromise of Password File

- To verify a user‘s identity, the system compares the password against a value stored in the password file.
- This password file is naturally an extremely attractive target for an attacker.
- Even if password file is encrypted, an offline dictionary attack can occur.

mobile business

How to Protect Your Password File

- To protect the password file, we have the following options:
  - Cryptographic protection
  - Access control enforced by the operating system
  - A combination of both, possibly with even further advancements to slow down dictionary attacks

Social Engineering

social engineering: n.

Term used among crackers (…) for cracking techniques that rely on weaknesses in wetware rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a mark who has the required information and posing as a field service tech or a fellow employee with an urgent access problem. (…)

The Jargon File,
http://catb.org/jargon/html/S/social-engineering.html

Staff give up passwords for chocolate bar

A new survey has discovered just how unconcerned employees are about IT security, with more than 71% of those questioned wiling to divulge their computer password for nothing more than a chocolate bar.

The survey asked workers a series of questions including "what is your password?" at which 37% immediately gave it up. A further 34% revealed their password after some minor additional interrogation. Of the 172 office workers surveyed, the vast majority had passwords based on some easily uncovered aspect of their lives, such as family name or favourite football team, but the most common password was found to be 'admin.'

Hot on the heels of these revelations came a DTI survey, which revealed security breaches are, unsurprisingly, on the increase. One third of all UK businesses and two-thirds of large businesses had a security incident that involved loss of data (excluding viruses), with the average cost to a business of a serious security incident set at £7,000 to 14,000 and a loss of four days of productivity.

Another serious concern was the discovery businesses were spending less than 3% of their IT spend on security and, though the majority of businesses understand the need for anti-virus software, most of them did not update the software often enough.

Stephen Timms, government minister for e-commerce, announced the results with the caveat that the context of the survey had changed. "UK companies are now using the internet as a routine part of business, but with the rapid adoption of e-business comes huge risks, and those risks are not being managed."

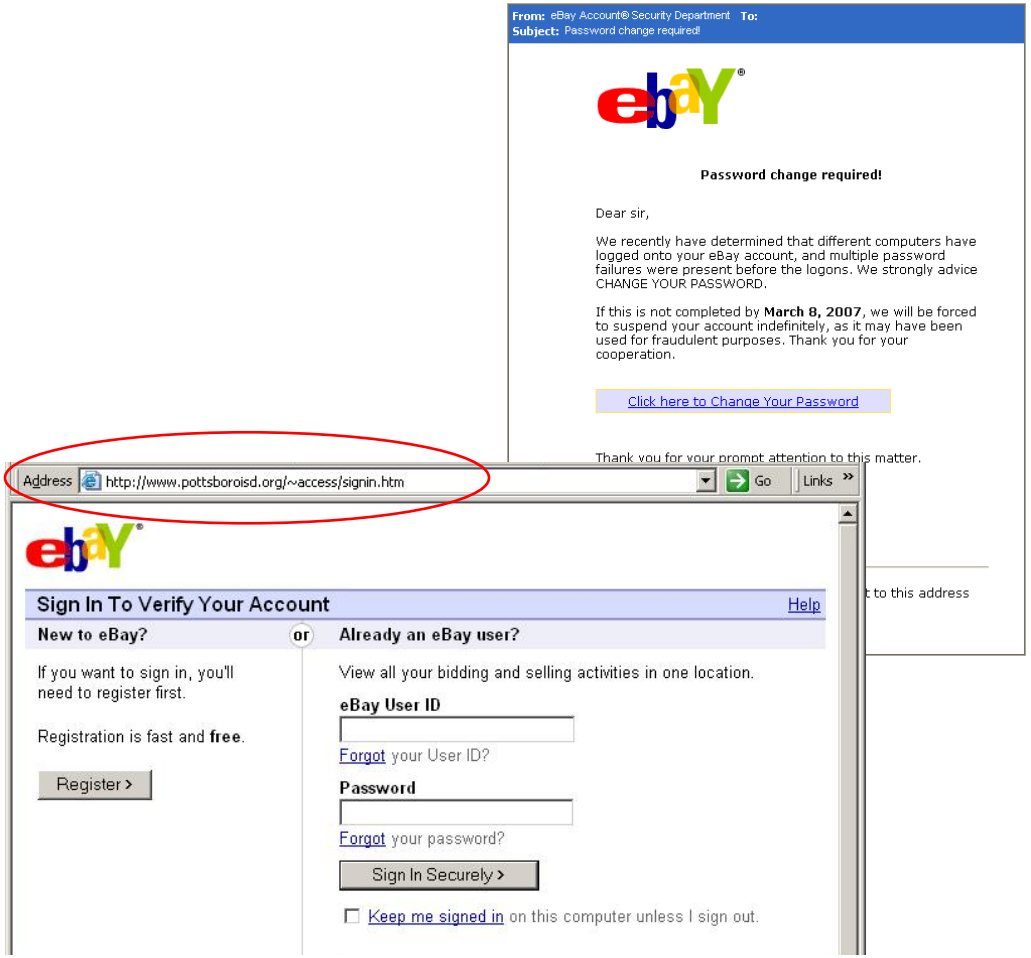
A full copy of the findings – and we urge you to read them – can be found at www.security-survey.gov.uk

Growing Business, May 2004

19

Example: Phishing

- Scam e-mail
- Link to fake login form
- Fake address visible in URL



mobile business

Agenda

- Introduction
- What you know
- What you have
- What you are
- Where you are
- Multi Factor Authentication
- Authentication protocols

mobile business

What You Have

- The user has to present a physical object to be authenticated.
- Classic example: a key

- A card or identity token used to control access are examples of such a key.

What You Have (II)

Hardware Token

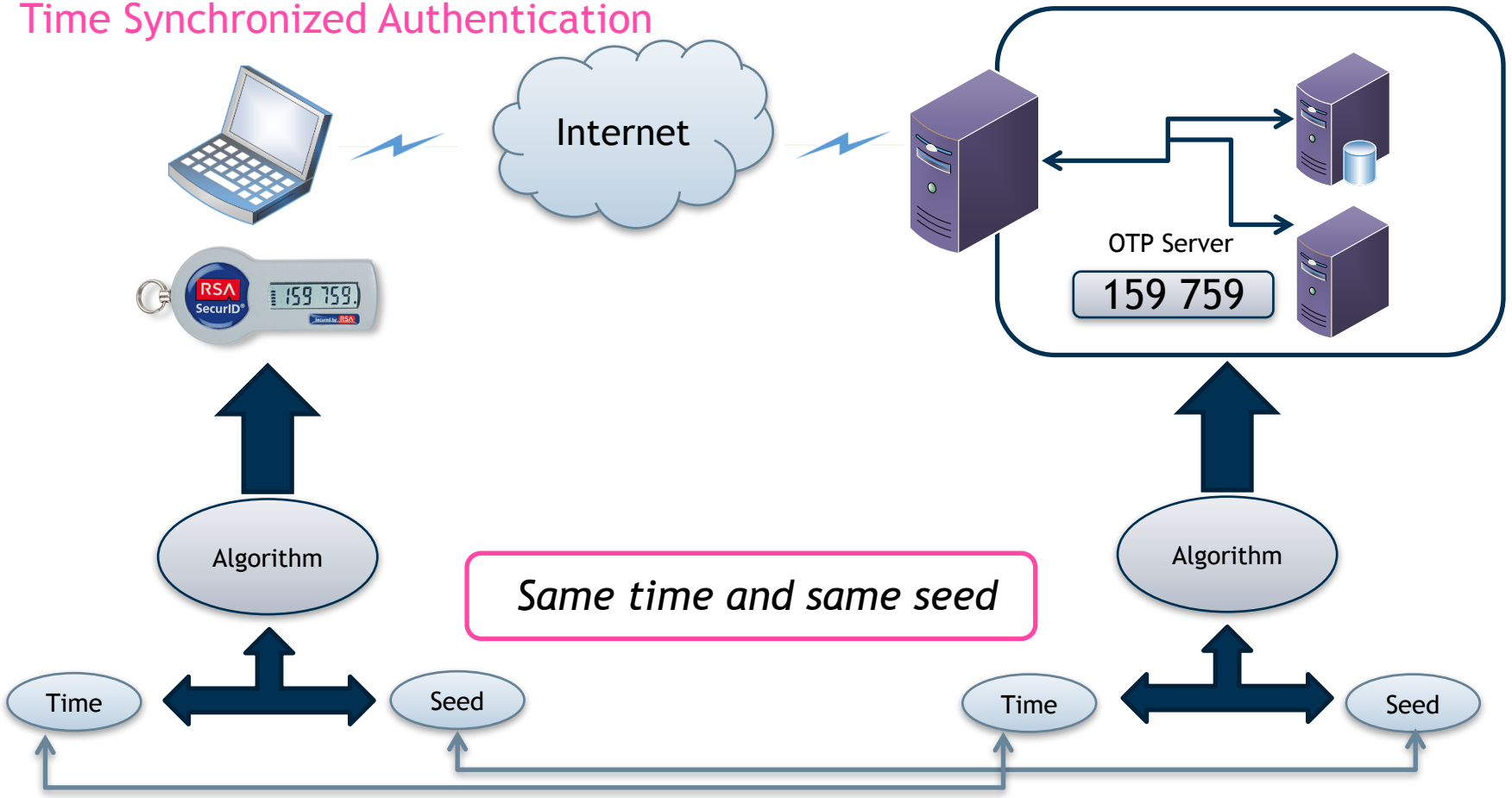
- Known also as Security Token, Authentication Token.
- Widely used as *unconnected* tokens

Smart Card

- Smart cards are an example of *connected* tokens.
- Low cost, strong security mechanisms

Security Tokens
One-time Passwords (OTP)

Time Synchronized Authentication



mobile business

Security Tokens

- **A physical token can be lost or stolen.**
- Anybody who is in possession of the token has the same rights as the legitimate owner.
- Combinations with PIN or other information about the legitimate owner are used.
- However, this does not eliminate the risk.

mobile business

Agenda

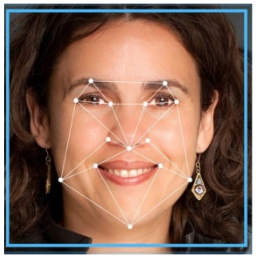
- Introduction
- What you know
- What you have
- What you are
- Where you are
- Multi Factor Authentication
- Authentication protocols

Biometrics

- Identification by physical attributes is as old as humanity.
- Biometrics is the automated measurement of **biological** or **behavioural** features.
- Biometric systems provide a percentage of similarity between samples, i.e., an individual's identity is confirmed only if the resulting percentage is above a **predefined threshold.**
- Biometric errors: "false rejection rate" (FRR) or false non-match rate (FNMR), and the "false acceptance rate" (FAR) or false match rate (FMR)

Physiological Biometrics

Fingerprint



Facial

DNA

Hand

Lip print

Iris & Retina

mobile business

Fingerprint

- It distinguishes the unique impressions of **ridges and valleys** made by an individual's finger.
- The uniqueness can be determined by the pattern of ridges and valleys, as well as minutiae points.
- **High accuracy:** although spoiled readings occur from time to time.
- Fingerprint features can be obtained with a fingerprint sensor.

mobile business

Iris Scan

- It identifies the location, shape and size of random patterns in the external iris of the eye; it transforms the iris rim into a rectangular shape texture
- **High accuracy:** The probability of two irises producing the same code is nearly impossible.
- Iris patterns are obtained through a video-based image acquisition system.

Face Recognition

- It captures a sequence of images, and extracts distinct individual features such as **eye socket position** (upper outlines), **space between cheek bones**, etc.
- **Medium accuracy:** other features such as hair and glasses and non-controlled scenarios (e.g., low light) make the recognition harder.
- Facial features can be obtained through simple store-bought camera.

mobile business

Fingerprints

Behavioral Biometrics

Voice

Keystroke Dynamics

Signature

Gait

Voice Recognition

- Authentication by voice, also called *speaker verification* or *speaker recognition* involves recognition of a speaker‘s voice characteristics.
- It analyses **power and spectral samples** of the speech, building a statistical pattern from them.
- **Low to medium accuracy:** the system needs to be trained first, it is susceptible to noise and changes in the voice.
- Voice features can be obtained with a microphone.

Keystrokes

- It identifies user's typing pattern. It measures and compares the series of user specific timing events also known as “typing *signature*” based on
  - Keystroke intervals
  - Keystroke pressure
  - Where the key is stuck (on the edge or in the middle)
- Two different approaches
  - *Static* – happens once in the beginning of authentication
  - *Dynamic* – happens continuously (more secure)
- Samples could be taken either from conventional keyboards or from touch screens (key tap dynamics).
- **Low to medium accuracy:** FRR/FAR can be adjusted by changing the acceptance threshold **at the individual level**

[Bi05]

Biometrics Issues and Risks

- Patterns will hardly ever match precisely.

  false positives - incorrectly allow access to an unauthorized user (FAR) and *false negatives* - incorrectly deny access to an authorized user (FRR)

  - If data can be copied by a potential attacker, identity fraud can occur.
  - Replay attacks are possible.
  - Biometric attribute can not be **revoked** easily.

mobile business

Agenda

- Introduction
- What you know
- What you have
- What you are
- Where you are
- Multi Factor Authentication
- Authentication protocols

Location Based Authentication

- Geodetic location, as calculated from a location signature, adds a fourth and new dimension to user authentication and access control.
- The physical location of a particular user or network node at any instant in time is uniquely characterized by a location signature.
- This signature is created by a location signature sensor (LSS) from the microwave signals transmitted by the twenty-four satellite constellation of the Global Positioning System (GPS).
- An entity in cyberspace will be unable to pretend to be anywhere other than where its LSS is actually situated.

[DeMa96]

mobile business

Agenda

- Introduction
- What you know
- What you have
- What you are
- Where you are
- Multi Factor Authentication
- Authentication protocols

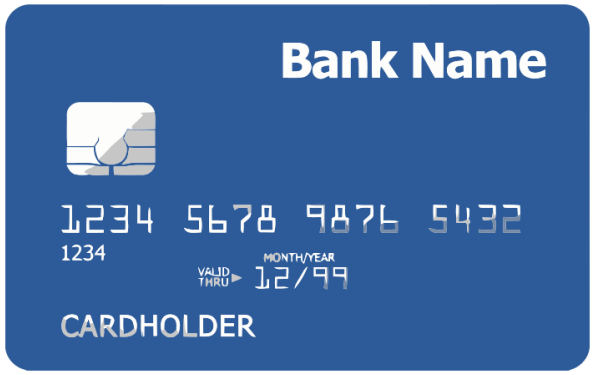
Multi Factor Authentication

- Authentication mechanisms can be combined, or multiple methods can be used (Multi Factor Authentication).
- The multiple layers of authentication require an attacker to know more, or possess more, than is required to spoof a single layer.

Example: Automatic Teller Machines (ATM)

- Combination of security token (e.g. girocard, ATM card) and password (PIN)

girocard



mobile business

Agenda

- Introduction
- What you know
- What you have
- What you are
- Where you are
- Multi Factor Authentication
- Authentication protocols

mobile business

Challenge/Response

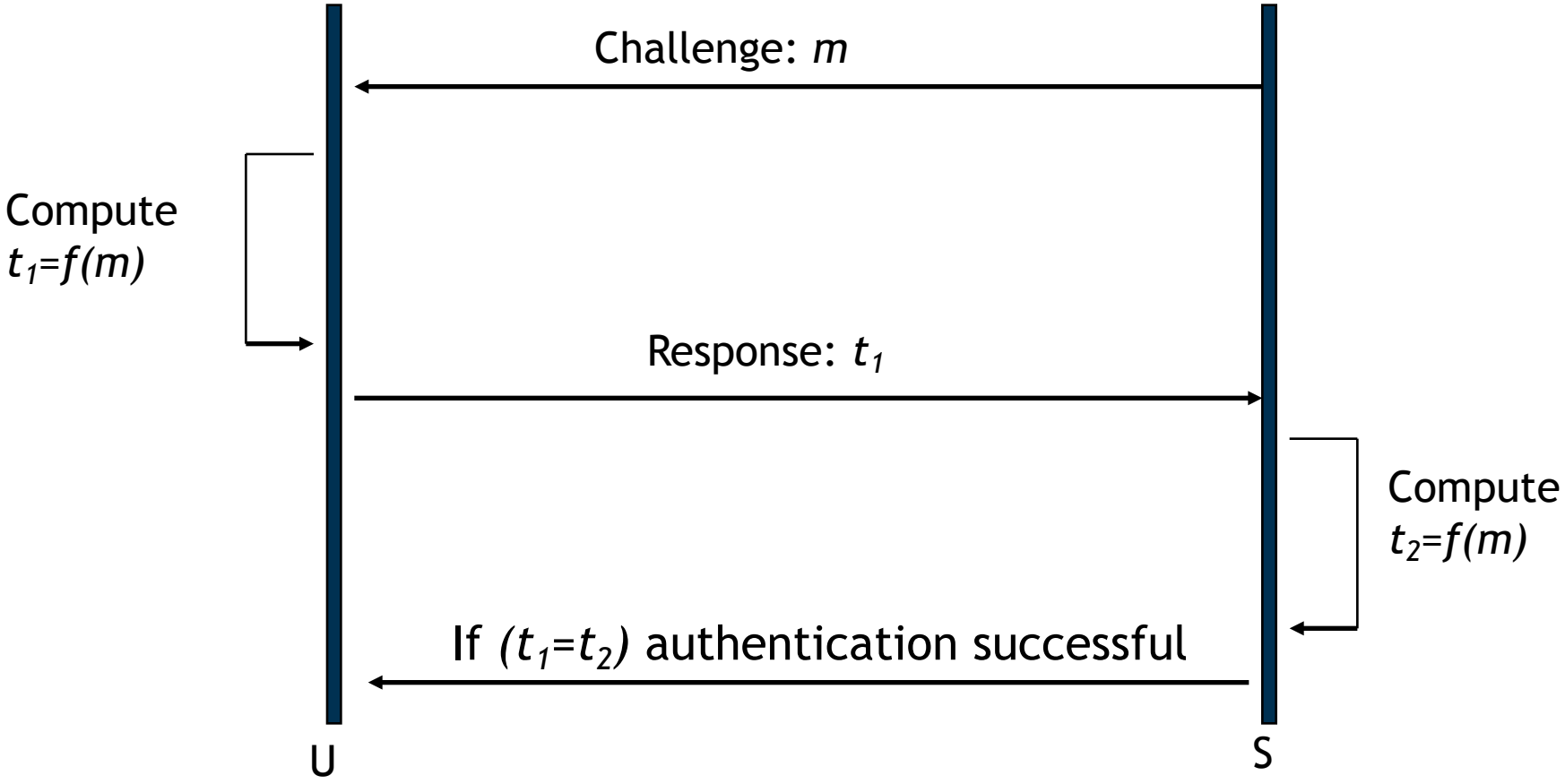
- Passwords have the fundamental problem, that they are reusable.
- If an attacker sees a password he can later replay the password.
- The system can not distinguish between the attacker and the legitimate user and allows access.
- An alternative is to authenticate in such a way that the transmitted password changes each time.

mobile business

Challenge/Response

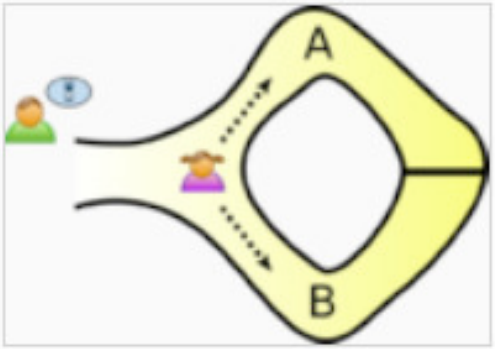
- User U wants to authenticate himself to System S.
- U and S have agreed on a secret function f.
- When authentication is needed S sends a random message m to U (challenge).
- U replies with the transformation t=f(m) (response).
- S validates t by computing it separately.

Challenge/Response

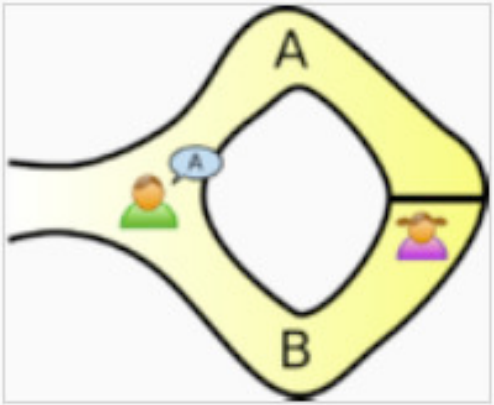


Zero Knowledge Proof

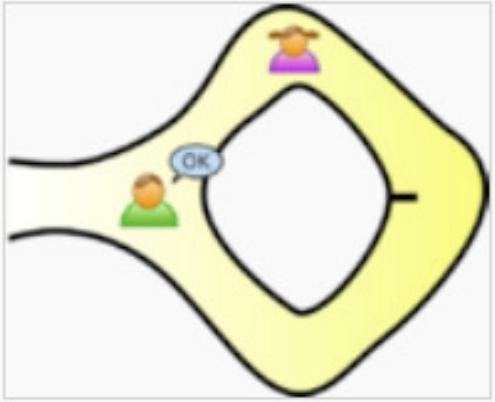
- How can Alice prove to Bob that she knows a secret S without disclosing the secret to Bob or a third person?



Peggy randomly takes either path A or B, while Victor waits outside



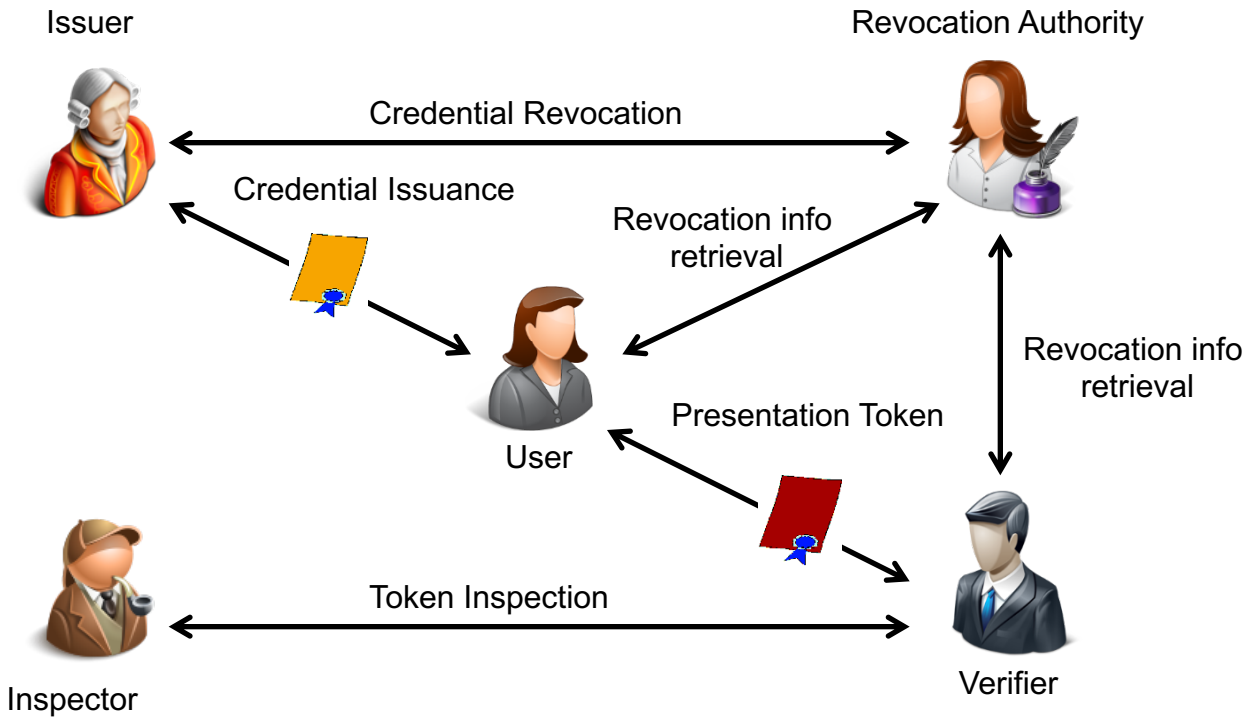
Victor chooses an exit path



Peggy reliably appears at the exit Victor names

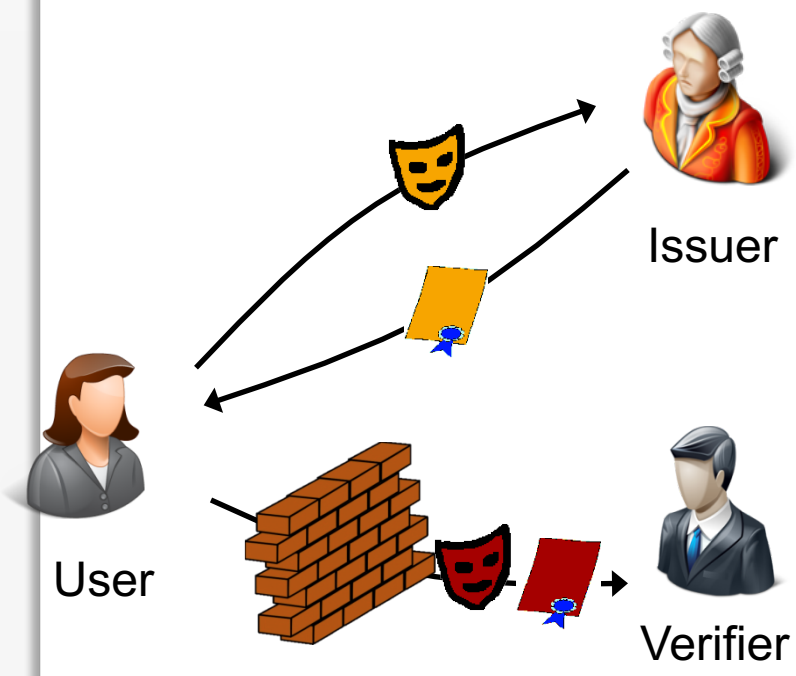
[Qu89]

ABC4Trust architecture
Interactions and Entities



Existing Privacy-ABC Technologies

Zero-Knowledge Proofs

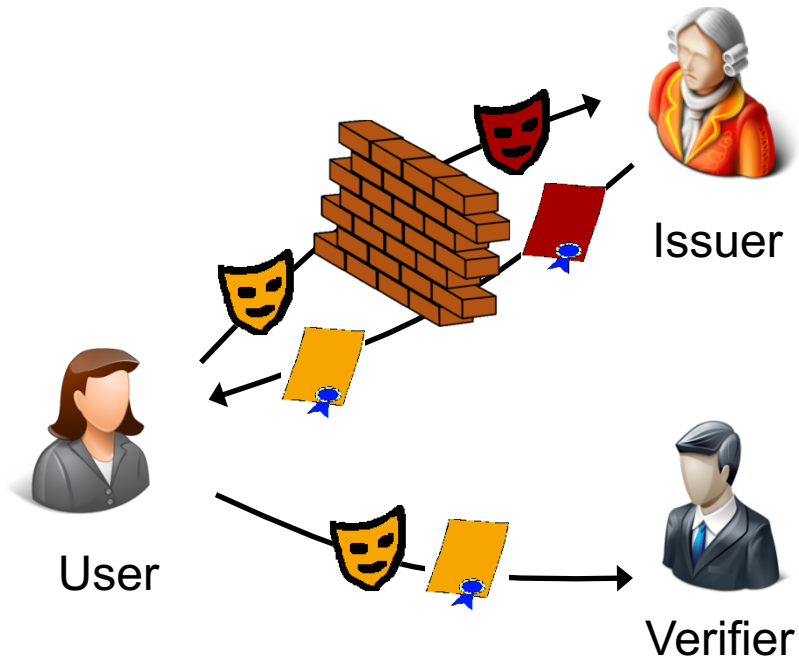


Idemix (Identity Mixer)

Damgard, Camenisch & Lysyanskaya

Strong RSA, pairings (LMRS, q-SDH)

Blind Signatures



U-Prove

Chaum, Brands et al.

Discrete Logs, RSA,…

mobile business

References

- **[ABC4Trust]** ABC4Trust website: www.abc4trust.eu
- **[Bi05] Bishop, Matt.** *Introduction to Computer Security.* Boston: Addison Wesley, 2005. pp. 171-198.
- **[DeMa96] D. E. Denning and P. F. MacDoran**, "Location-Based Authentication: Grounding Cyberspace for Better Security," Computer Fraud &Security. vol. 1996.
- **[Go06] Gollmann, Dieter.** *Computer Security, 2nd Edition.* Chichester, New York, Weinheim, Brisbane, Singapore, Toronto: John Wiley & Sons, 2006.
- **[Qu89] Quisquater, Jean-Jacques, et al.** *How to explain zero-knowledge protocols to your children*, Conference on the Theory and Application of Cryptology. Springer New York, 1989.