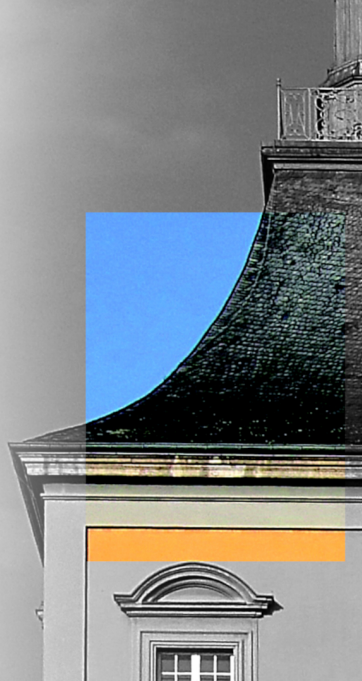
UNIVERSITÄT BONN

Web Authentication Schemes

Melina Hoffmann
hoffmann@cs.uni-bonn.de
University of Bonn | Institute of Computer Science 4

Lecture IT Security | Uni Bonn | WT 2024/25



UNIVERSITÄT BONN

About Me

- 2023 Master Computer Science in Bonn
- since 2023 Researcher WG IT-Security
- Project „DARIA“
  - collaborative and privacy preserving fraud prevention
  - online identities and authentication

UNIVERSITÄT BONN

Contents

- Why do we need different web authentication schemes?
- German eID
- FIDO2
- Browser Fingerprinting
- Risk Based Authentication
- Conclusion

Why do we need different web authentication schemes?

UNIVERSITÄT BONN

Motivation: Classic Username and Password Schemes

Historically, web applications typically use an authentication scheme that is based on a username and password combination. The user chooses username and password on registration. The credentials are stored by the online service and should be securely hashed and salted. During a login attempt, the stored credentials are compared to the user input.

Disadvantages and security risks:

- Users needs to remember credentials for all online services
- Passwords may be weak and easy to guess or reused
- Users may need to enter their personal data multiple times
- Online service may use weak security measures when storing the credentials

German eID

UNIVERSITÄT BONN

German Electronic Identity (Online-Ausweis)

- introduced in 2010
- chip on german identity documents, e.g. identity card, passport, residence permit
- stores personal data of the holder, analogous to the printed information on the document
- can be used for online identification and authentication

https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/online-ausweisen/online-ausweisen-node.html

UNIVERSITÄT BONN

Typical Use Cases

- online identification and authentification linked to a state issued and verified offline identity
  - official administration services
  - private companies that require strong authentication of their customers for legitimzing certain transactions
- can also generate a pseudonym which can be used to recognize and reidentify customers or users without learning any of their actual personal data

German eID

Components

UNIVERSITÄT BONN

User Environment

- identity document
  - stores personal data of the card holder analogous to the printed information on the document, e.g. name, date of birth, expiry date, nationality
  - stores eID system specific data, e.g. cryptographic keys used in the authentication process
- card reader
  - e.g. dedicated reader device or NFC-compliant smartphone
- 6-digit PIN
- eID client
  - software on local device
  - manages authentication process on the client side and communicates between the user, card reader and eID service
  - e.g. AusweisApp by Governikus

UNIVERSITÄT BONN

eID Service

- online service that uses the online authentication via eID
- can request only user and service specific pseudonym for user reidentification
  - simple implementation via official login plugins for wordpress, nextcloud and TYPO3
- if the eID service wants to request personal data, infrastructure and official certification is required

eID Service

Process for certification

- service concept including list of required data fields that should be read from the eID
- state issued authorization certificate
  - official paperwork permitting the operation of an eID service
  - vetting the declaration on data protection and data security as well as the necessity of the requested personal data fields
- technical authorization certificate
  - electronic certificate
  - i.a. specifies which data fields are allowed to be requested by the service
  - requirement: state issued authorization certificate

UNIVERSITÄT BONN

eID Server

- hard- and software-component of the eID service infrastructure
- undertakes secure communication between eID client, id card chip, eID service
- also communicates with central backend structures

German eID

Online Authentication Process

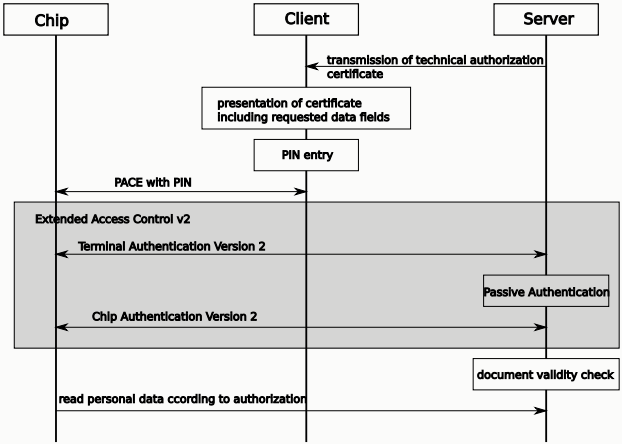
UNIVERSITÄT BONN

Online Authentication Process

1. user visits the eID service's website requiring online authentication
2. the eID service sends an authentication request to the eID server and activates the eID client via the user's application
3. General Authentication Procedure between eID server, eID client and the chip on the user's document

UNIVERSITÄT BONN

General Authentication Procedure



PACE

- Password Authenticated Connection Establishment
- verifies that user has knowledge of the PIN corresponding to the presented eID card
- mutual authentication between eID client and the chip

UNIVERSITÄT BONN

Extended Access Control v2

mutual authentication of eID service and the eID document via the eID server and eID client

- Authentication of the eID service (Terminal Authentication Version 2)
  - proof of authenticity and access rights (required data fields) of the eID service
  - uses the eID services technical authorization cerfiticate and therefore requires the eID server to communication with the authorization PKI
- Authentication of the German eID's public key (Passive Authentication)
  - uses a digital signature from the card manufacturer to authenticate the data stored on the chip
  - eID server communication with the document PKI
  - part of the stored and authenticated data: static public key of the chip used in the next step

UNIVERSITÄT BONN

Extended Access Control v2

- Authentication of the document (Chip Authentication Version 2)
  - Diffie-Hellman based protocol to further authenticate the chip
  - verification that the chip contains the private key that corresponds to the verified public key from the previous step

UNIVERSITÄT BONN

Online Authentication Process

1. user visits the eID service's website requiring online authentication
2. the eID service sends an authentication request to the eID server and activates the eID client via the user's application
3. General Authentication Procedure
4. eID server transmits the result and personal data to the eID service and redirects the eID client back to the web session
5. eID service checks the response and, if satisfactory, grants access to the user

German eID

Revocation

UNIVERSITÄT BONN

Revocation

The eID system needs an option to revoke a stolen or lost identification document. The card holder typically issues the notification through the issuing authority, the police or a revocation hotline, which then needs to make this information electronically available in the eID system.

Complication: service specific pseudonyms
If there is a global revocation list that uses card serial numbers or that allows linking to one revocation entry with all service specific pseudonyms, the pseudonymity is lost.

Solution: eID service specific revocation lists and revocation service to manage these lists

UNIVERSITÄT BONN

Preparations

Preparations during identity card manufacturing

- revocation key
  - public/ private key pair
  - public key send to revocation service
  - private part stored on the chip
- revocation password
  - clear text password, randomly chosen from a word list
  - send to the card holder with the PIN in the PIN letter
  - send to resident register
- revocation code
  - hash over the first name, last name, birth date and revocation password
  - send to the resident register
  - send to the revocation service

UNIVERSITÄT BONN

Preparations

Preparations of the revocation service and eID service

- revocation sector
  - key pair of the revocation service
  - private key used to „activate“ the revocation key of an id card
  - public key base point for the generation of the terminal sectors
- terminal sector
  - key pair specific to one eID service and one revocation service
  - generated by the authorization CA based on the revocation sector
  - public key part of the authorization certificate of the eID service
  - private part used by authorization CA to convert „activated“ revocation keys to eID service specific revocation tokens

UNIVERSITÄT BONN

Revocation Process

User revokes an indentification document

1. user notifies the authorities or the hotline
2. authority/ hotline generates the revocation code from the users personal information and revocation password from the PIN letter, or looks it up in the resident register
3. revocation code is send to the revocation service
4. revocation service looks up the corresponding revocation key and makes an entry in the revocation list

UNIVERSITÄT BONN

Revocation Process

eID service specific revocation list is generated from the card specific revocation keys

1. the revocation service uses its own private key from the revocation sector to convert the card specific revocation key into an „activated“ revocation key
2. the authorization CAs retrieve the list of „activated“ revocation keys
3. the authorization CAs convert the lists of „activated“ revocation keys to service-specific lists of revocation tokens using the private part of the eID service specific terminal sector
4. eID servers or service providers retrieve the lists of eID service specific revocation tokens from their authorization CA

UNIVERSITÄT BONN

Revocation Process

Future authentication attempts with the lost or stolen document

1. during the online authentication process, the chip generates eID service specific revocation token from its own private part of the revocation key (stored on the chip since maufacturing) and the public part of the eID service specific revocation sector (derived from eID service specific certificate during authentication process)
2. chip and eID service specific revocation token is checked against the eID service specific list of revocation tokens

The revocation process can be reversed and the revocation status can be retrieved via the issuing authority.

German eID

Usage and Limitations

UNIVERSITÄT BONN

Limitations

- linked to and requires state issued documents and identities
- complex setup, including certification process
- complex system with a lot of components and background infrastructure that needs to be run by trusted parties
- as of today seen as quite secure, although not entirely without risks or attacks vectors

UNIVERSITÄT BONN

Usage

- 39% percent of citizens have the eID PIN activated
- 22% have used the eID functionality before
- Personalausweisportal lists over 250 eID services, including various municipalities and goverment services as well as private companies
- not limited to german citizens, thanks to the eIDAS scheme and the german eID card for citizens of the EU and the EEA

https://initiatived21.de/publikationen/egovernment-monitor/2024

https://www.personalausweisportal.de/SiteGlobals/Forms/Webs/PA/suche/anwendungensuche-formular.html?gts=14626016_list%253DunifiedDate_dt%2Bdesc&gtp=14626016_list%253D2

FIDO2

UNIVERSITÄT BONN

FIDO2

FIDO2 is an authentication standard specified by the W3C (World Wide Web Consortium) and FIDO Alliance (Fast IDentity Online).

Goal: replace password-based schemes or enhance them with public key cryptography based authentication that is

- more secure than passwords
- simple to use
- simple to deploy and manage

UNIVERSITÄT BONN

Components

Authenticator

- hardware based token that stores/ generates private-public key pairs
- client device with internal FIDO2 authenticator, dedicated external hardware or software

Relying Party

- service using FIDO2 authentication, containing a web application and FIDO2 server

Client

- bridge between authenticator and relying party, typically the users web browser or operating system subsystem

Communication Protocols

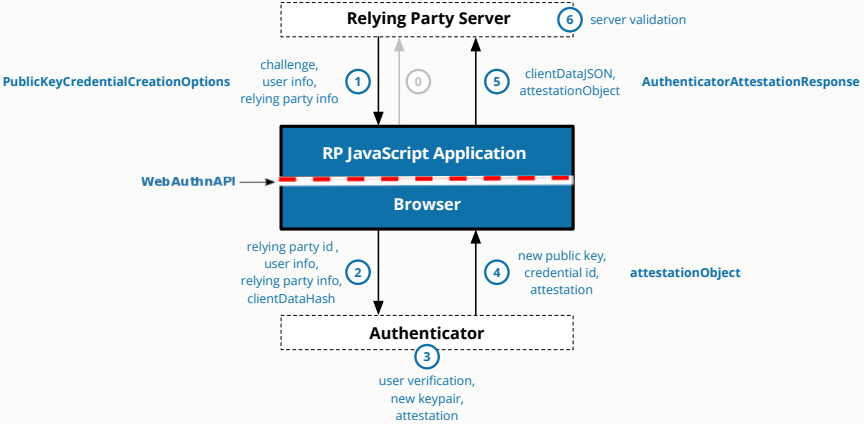
- CTAP (Client to Authenticator Protocol) for communication between client and authenticator
- WebAuthn between client and relying party

FIDO2

Registration and Authentication

UNIVERSITÄT BONN

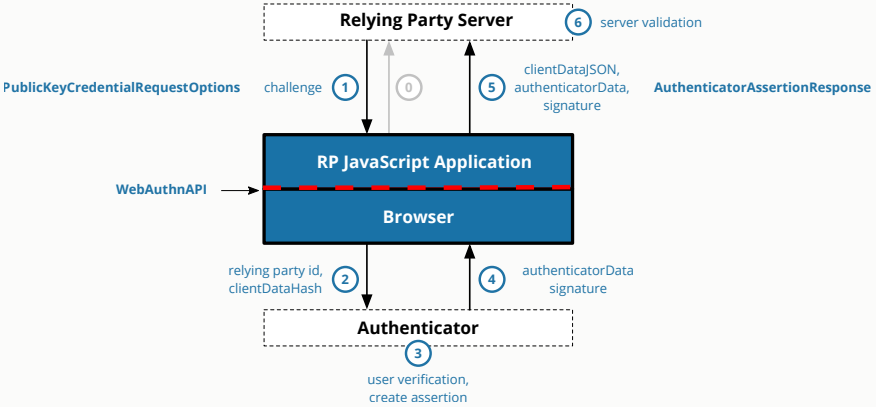
User Registration



https://developers.yubico.com/WebAuthn/WebAuthn_Developer_Guide/WebAuthn_Client_Registration.html

UNIVERSITÄT BONN

User (Re-)Authentication



https://developers.yubico.com/WebAuthn/WebAuthn_Developer_Guide/WebAuthn_Client_Authentication.html

FIDO2

Usage and Limitations

UNIVERSITÄT BONN

Usage and Limitations

- in the basic version, the credentials are tied to a single authenticator device
- more complex setup than simple password based scheme
- needs additional background infrastructure
- used by numerous companies and services, e.g. discord, dropbox, ebay, facebook, github

Browser Fingerprinting

UNIVERSITÄT BONN

Browser Fingerprinting

> A browser fingerprint is a set of information related to a user's device from the hardware to the operating system to the browser and its configuration.

> Browser fingerprinting refers to the process of collecting information through a web browser to build a fingerprint of a device.

Browser Fingerprinting: A Survey - Laperdrix et al. - 2020

Browser Fingerprinting

User Agent

UNIVERSITÄT BONN

HTTP User-Agent Request Header

- request header: HTTP header that can be used in an HTTP request to provide information so that the server can tailor the response
- HTTP User-Agent request header is a characteristic string that lets servers identify the application, operating system, vendor, and/or version of the requesting user agent
- originally meant to prevent incompatibility problems

General syntax:

```
User-Agent: <product>/<product-version><comment>
```

UNIVERSITÄT BONN

Example: Firefox

Common format for web browsers:

```
Mozilla/5.0 (<system-information>) <platform>(<platform-details>)
<extensions>
```

Example for Firefox:

```
Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0)
Gecko/20100101 Firefox/47.0
```

Browser Fingerprinting

Additional Features

UNIVERSITÄT BONN

Additional Features Used for Browser Fingerprinting

Examples of further attributes:

- content language as specified in HTTP header
- list of installed plugins
- timezone
- screen resolution and colour depth
- use of an ad blocker
- canvas

UNIVERSITÄT BONN

Example: Canvas Fingerprinting

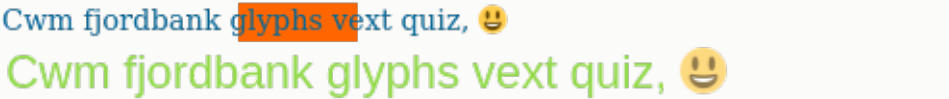
The Canvas API can be used to draw and manipulate graphics via JavaScript and the HTML <canvas> element. The final user-visible bitmap is influenced by operating system, browser version, graphics card, installed fonts and more. Therefore, different devices render the same canvas drawing as defined in HTML and JavaScript slightly differently.

Canvas Fingerprinting:

- render invisible picture in the users browser
- collect the characteristic rendering as part of the fingerprint

UNIVERSITÄT BONN

Example: Canvas Fingerprinting



https://amiunique.org

Browser Fingerprinting

Usage and Limitations

UNIVERSITÄT BONN

Usage and Limitations

- not an actual precise authentication method
- usage in study results varies by an order of magnitude depending on the method and definition of fingerprinting
- used in literature and companies for fraud detection and prevention by searching for anomalies in user behaviour patterns

Risk Based Authentication

UNIVERSITÄT BONN

Risk Based Authentication

RBA (Risk Based Authentication) is an adaptive security measure to strengthen password-based authentication. With RBA, an online service monitors additional features during password entry to asses the risk of identity theft. If a certain risk level is detected, additional authentication factors are requested. The goal of RBA is to effectively and efficiently combine different concrete authentication schemes.

Risk Based Authentication

Login Process

UNIVERSITÄT BONN

Login Process

Attacker model: knows the correct credentials or can guess them with a low number of tries

During login process:

1. during password entry, additional features are being monitored in the background
2. from these features, the service calculates a risk score
3. depending on the risk score, different additional authentication measures are required
   - e.g. none when score low, additional authentication factor when medium (e.g. e-mail verification, SMS verification), block access when high

Risk Based Authentication

Usage and Limitations

UNIVERSITÄT BONN

Usage Study

„Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild“ - Wiefling et al. 2019

- investigated 8 online services: Amazon, Facebook, GOG.com, Google, iCloud, LinkedIn, Steam and Twitch
- used virtual identities and user accounts and simulated „typical“ user behaviour
- then changed features from the assumed rba feature list and recorded the behaviour of the online services
  - feature list: IP address, user agent string, language, display resolution, login time

UNIVERSITÄT BONN

Study Results Example: Google

Features Used in RBA:

- either IP address, user agent or screen resolution changed: e-mail security alert
- strong variation in IP address: request for additional authentication factor
- all combinations of 2 factors except language+time: e-mail security alert
- three features changed: security alert
- IP address, user agent, and time parameters: additional authentication factor

Additional authenticaton factors:

- enter name of city you usually sign in from
- verification code over various channels, e.g. email, app, text message
- press confirmation button on secondary device

UNIVERSITÄT BONN

Study Results Summary

- used parameters, risk threshold(s) and triggered actions vary significantly between services, including no detected RBA for some services
- all discovered feature sets contain IP address
- all discovered RBA schemes us verification codes of some kind as an additional authentication factor

UNIVERSITÄT BONN

Limitations

- not an authentication scheme in and of itself
  - security depends on the utilised fingerprinting and authentication methods
- risk of inconveniencing legitimate users that just happen to deviate from their usual behavioral patterns
- might add security and privacy risks, e.g. by leaking legitimate user's data

Conclusion

UNIVERSITÄT BONN

Conclusion

- overview over different web authentication schemes for different needs and scenarios
- balance between different factors like security requirements, user experience, ease of installation and maintenance determine the best setup for a specific service

Thank you for your attention!
Questions?

Melina Hoffmann

University of Bonn | Institute of Computer Science 4

hoffmann@cs.uni-bonn.de