Digital Security
Research Group

ETAA 2022 Copenhagen

Protecting FIDO Extensions against Man-in-the-Middle Attacks

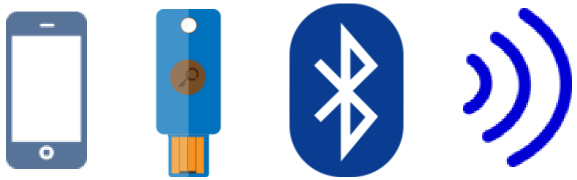
Andre Büttner and Nils Gruschka

University of Oslo

30th September 2022

UNIVERSITY
OF OSLO

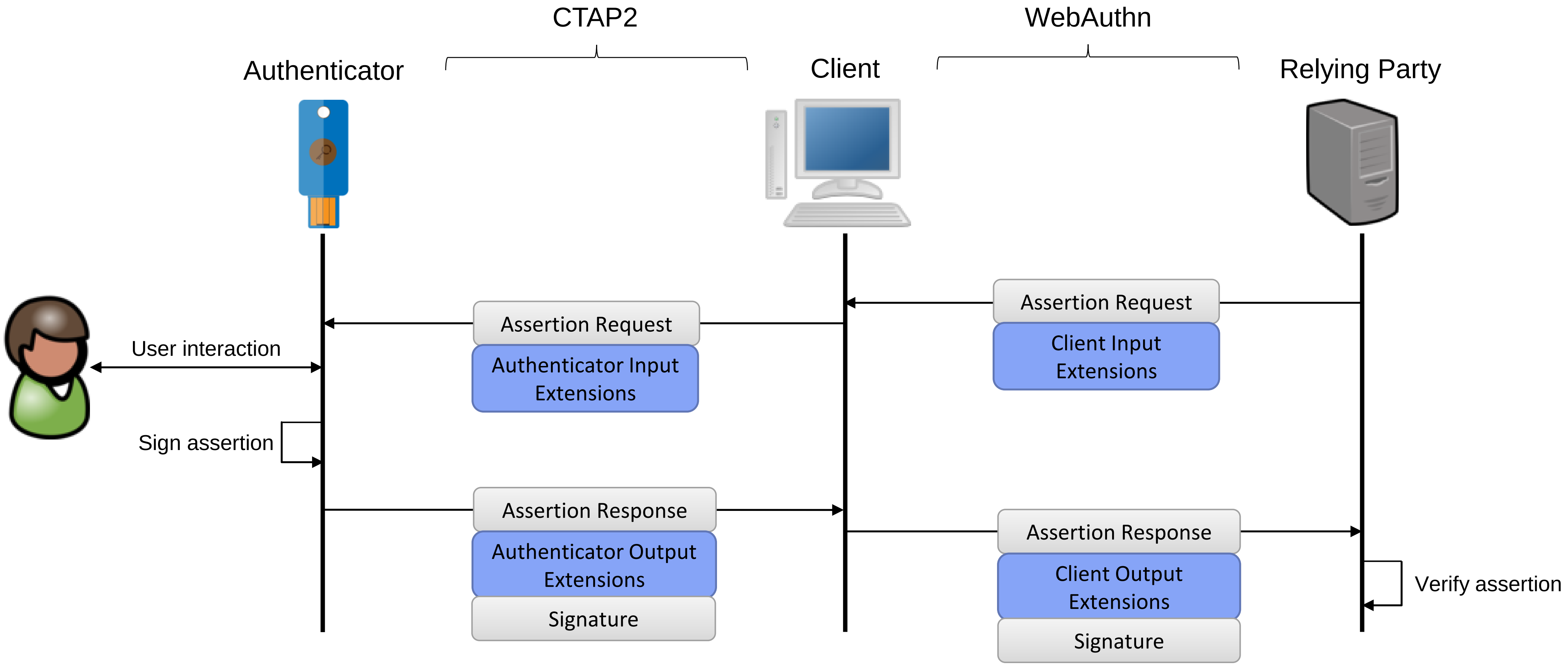
FIDO Authentication



- Used for MFA or passwordless authentication
- Roaming / platform authenticators
- Based on public-key cryptography
- Phishing resistant
- FIDO2 Standards
  - W3C WebAuthn[1]
  - Client-to-Authenticator Protocol 2 (CTAP2)[2]

1. https://www.w3.org/TR/webauthn
2. https://fidoalliance.org/specs/fido-v2.1-rd-20210309/

FIDO Authentication



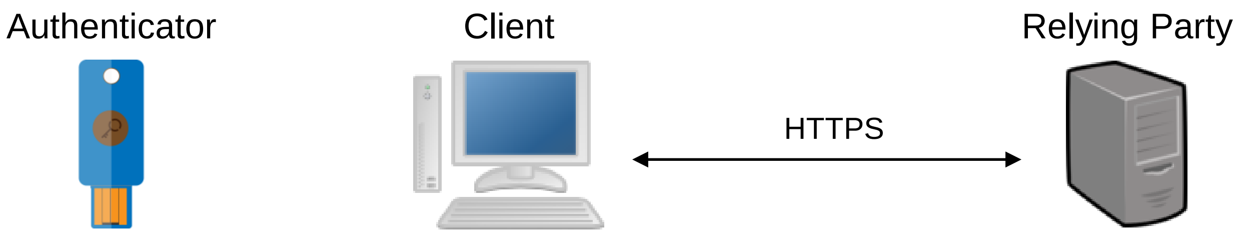
FIDO Authentication

Extensions

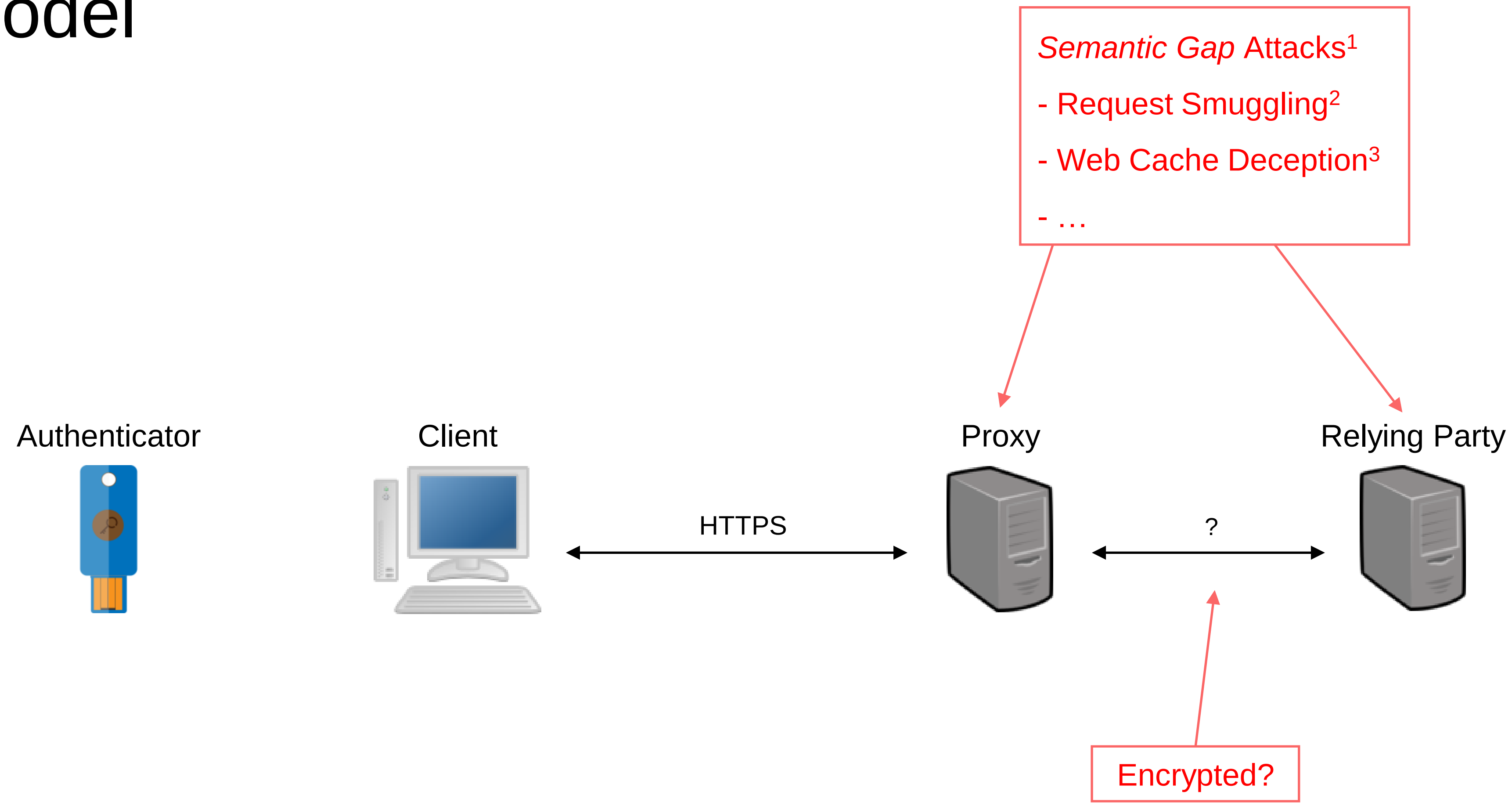
- Transactions:
  - Transaction Confirmation[1] (deprecated)
  - Secure Payment Confirmation (SPC)[2]
- Other examples[3]:
  - HMAC Secret
  - Large blob storage

1. https://media.fidoalliance.org/wp-content/uploads/2020/08/FIDO-Alliance-Transaction-Confirmation-White-Paper-08-18-DM.pdf
2. https://www.w3.org/TR/secure-payment-confirmation/
3. https://www.w3.org/TR/webauthn

Attacker Model

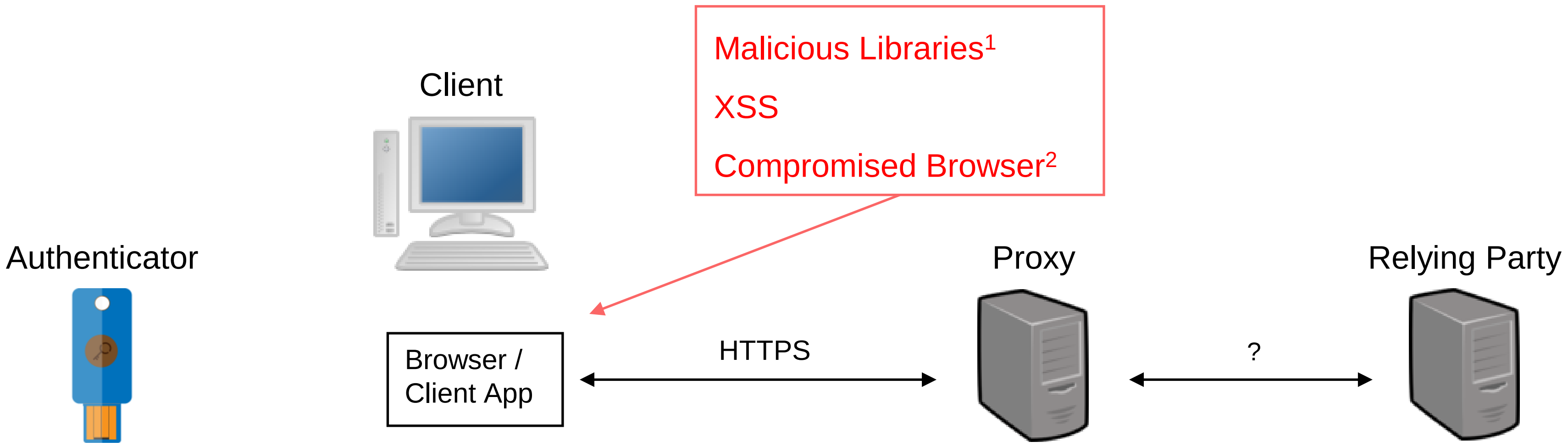


Attacker Model



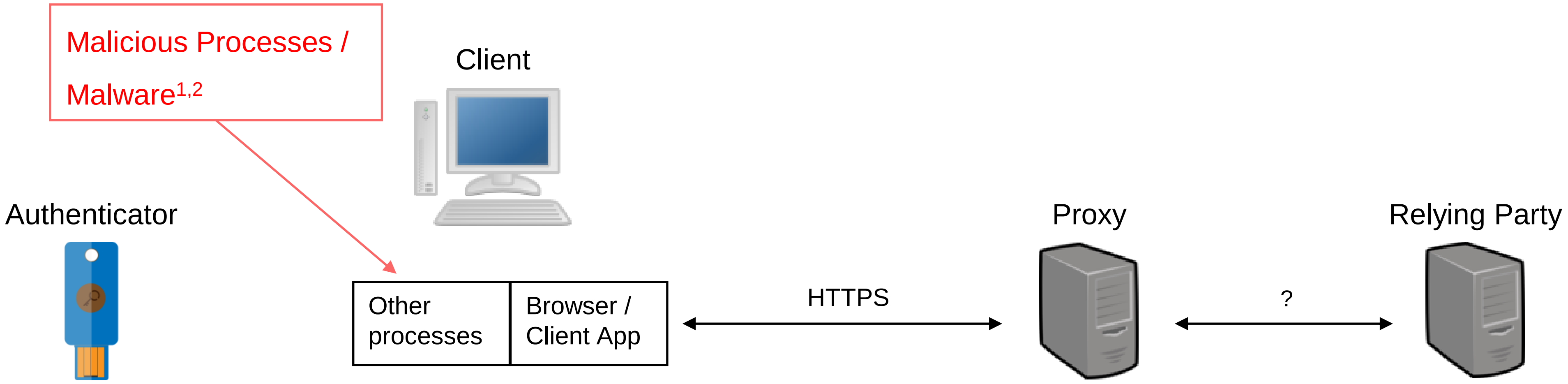
1. Büttner, A, *et al.* "Less is Often More: Header Whitelisting as Semantic Gap Mitigation in HTTP-Based Software Systems." IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, Cham, 2021.
2. Linhart, C., *et al.* "Http request smuggling" (2005).
3. Gil, O. "Web cache deception attack." Black Hat USA 2017 (2017).

Attacker Model



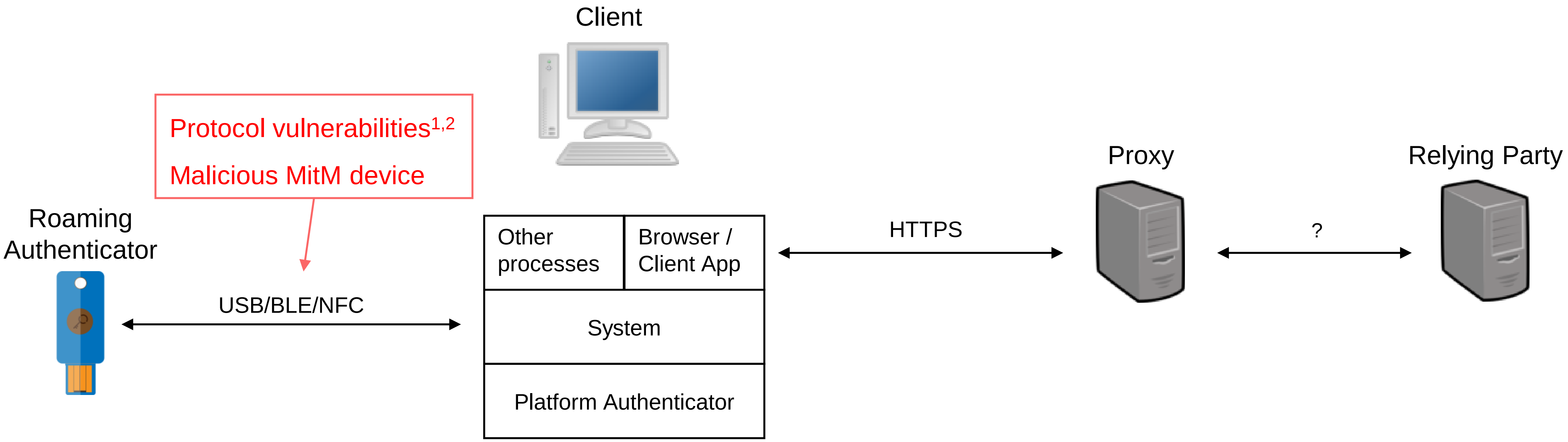
1. Arshad, S, *et al*. "Include me out: In-browser detection of malicious third-party content inclusions." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2016.
2. Dougan and Curran. "Man in the browser attacks." International Journal of Ambient Computing and Intelligence (IJACI) 4.1 (2012): 29-39.

Attacker Model



1. Bui, T., et al. "Man-in-the-Machine: Exploiting {Ill-Secured} Communication Inside the Computer." 27th USENIX security symposium (USENIX Security 18). 2018.
2. Zhang, Y., et al. "Secure display for FIDO transaction confirmation." Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. 2018.

Attacker Model



1. Sun, D., *et al*. "Man-in-the-middle attacks on Secure Simple Pairing in Bluetooth standard V5. 0 and its countermeasure." Personal and Ubiquitous Computing 22.1 (2018): 55-67.
2. Lahmadi, *et al*. "MitM attack detection in BLE networks using reconstruction and classification machine learning techniques." Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Springer, Cham, 2020.

Protocol Design

Security properties

- Confidentiality
- Authenticity
- Integrity

Challenges

- Key exchange
- Encoding
- Displaying user information
- Low-resource devices
- FIDO2 standard compliance

Protocol Design

Authenticated encryption

- E.g. AES-GCM
- Key wrapping for multiple authenticators

Key exchange

- Diffie-Helman Key Exchange during registration
- Require attestation

Data format

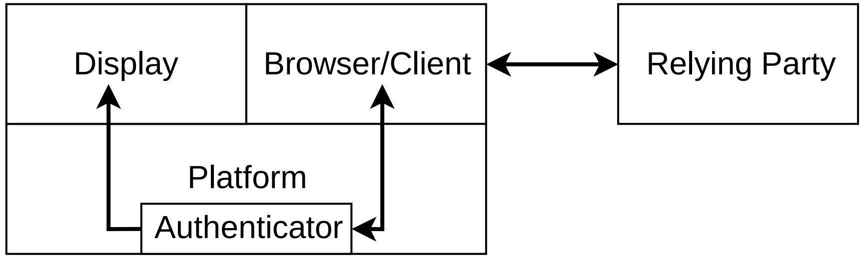
- CBOR Object Signing and Encryption (COSE)[1]
  - Binary format
  - CBOR used in FIDO2
  - Standardized encryption, signature and message authentication algorithms and data structures

1. RFC 9052 https://datatracker.ietf.org/doc/rfc9052/

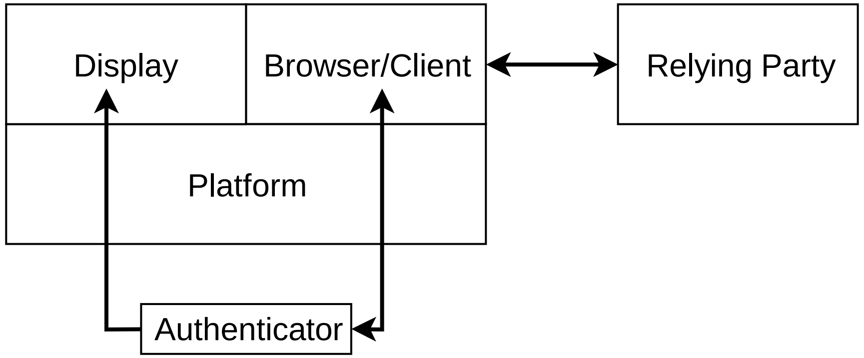
Protocol Design

Displaying user information

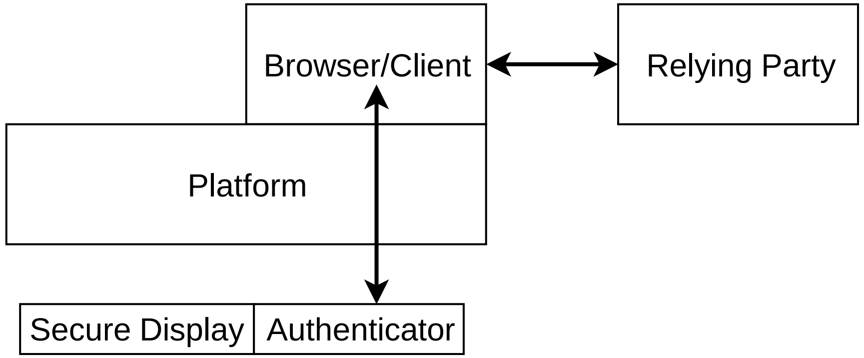
Platform Authenticator



Roaming Authenticator



Roaming Authenticator with Display



Security Evaluation

Methodology

- ProVerif[1]
- Creating models of the protocol
  - Registration
  - Authentication

1. Blanchet, B. "Modeling and verifying security protocols with the applied pi calculus and ProVerif.“ Foundations and Trends® in Privacy and Security 1.1-2 (2016): 1-135.

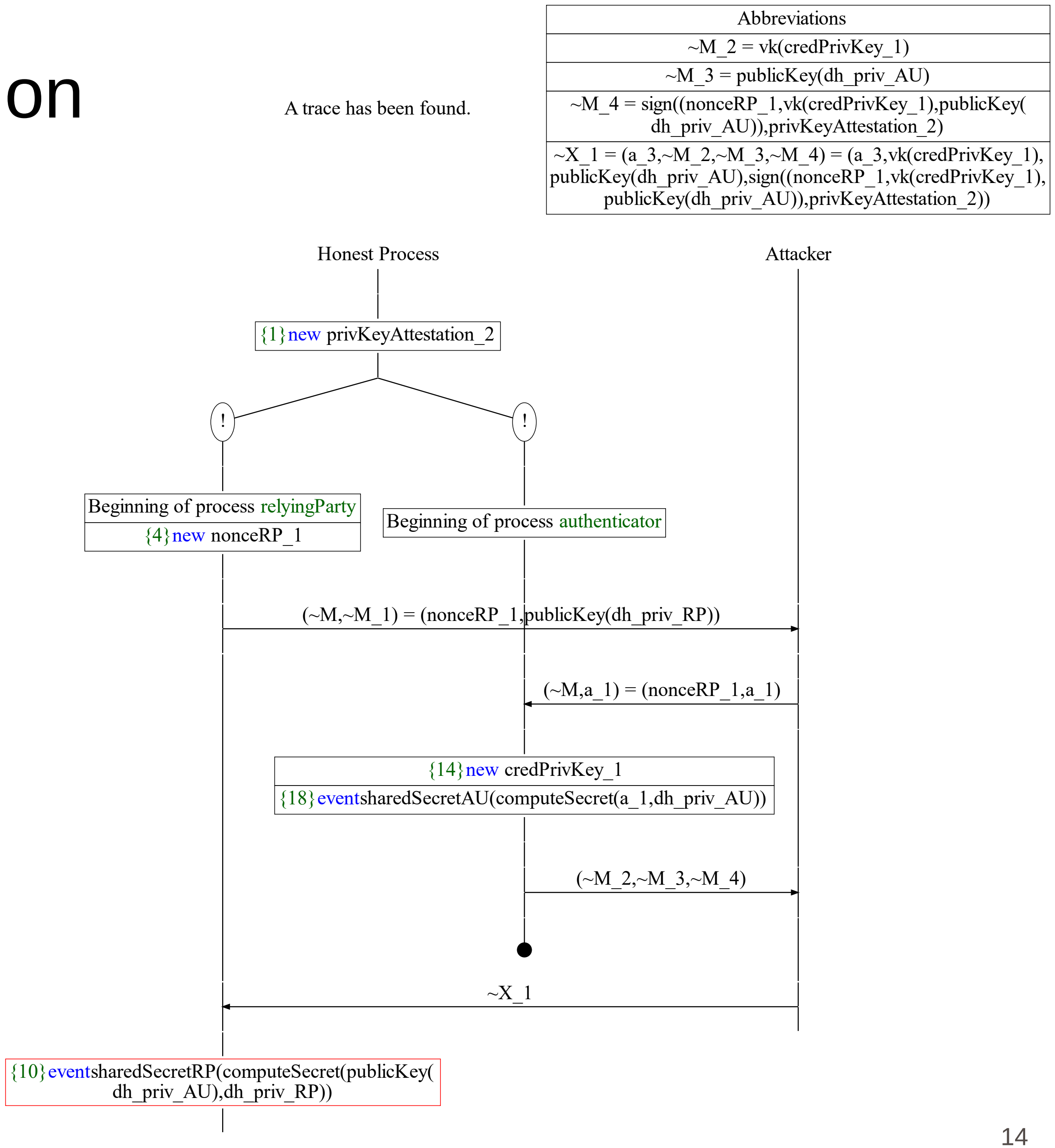
Security Evaluation – Registration

Security properties tested

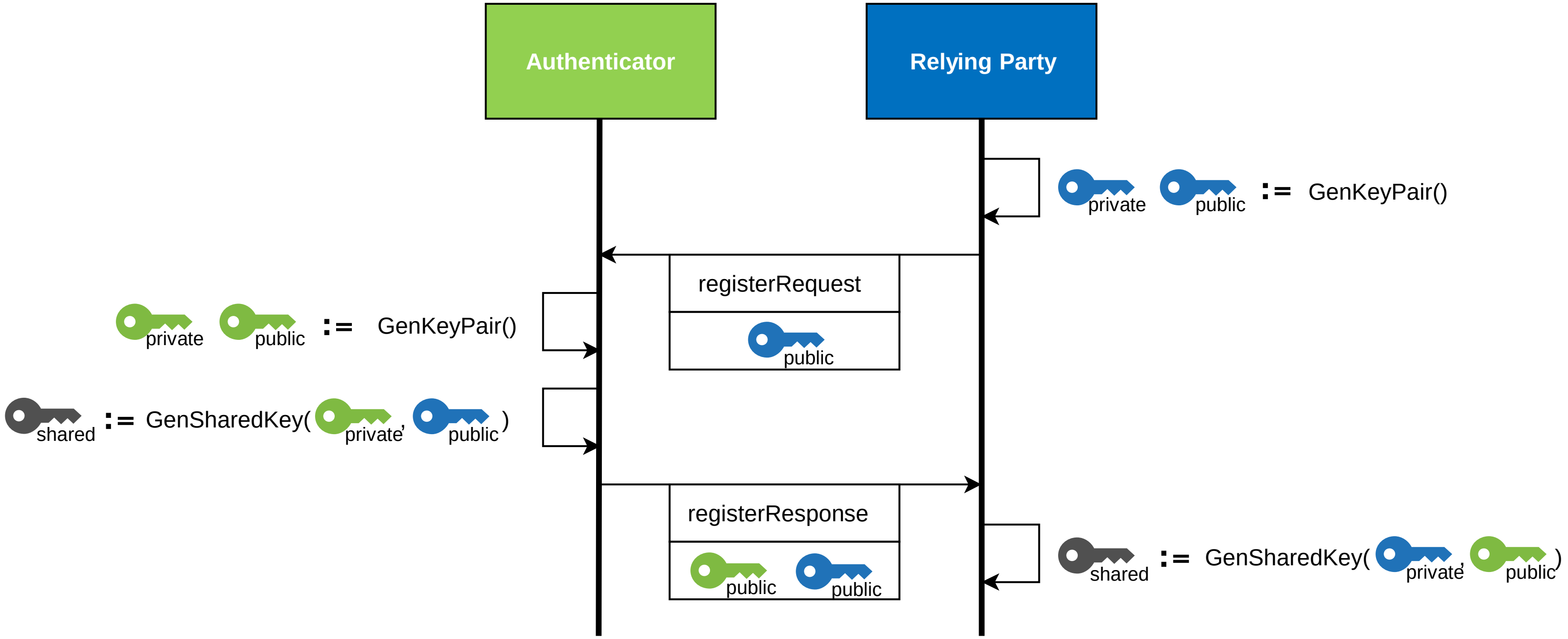
- Secrecy of the shared secret
- Authenticity of the shared secret

Results

- First version → Attack discovered
- Second version → No attacks



Protocol Design – Registration



Security Evaluation – Authentication

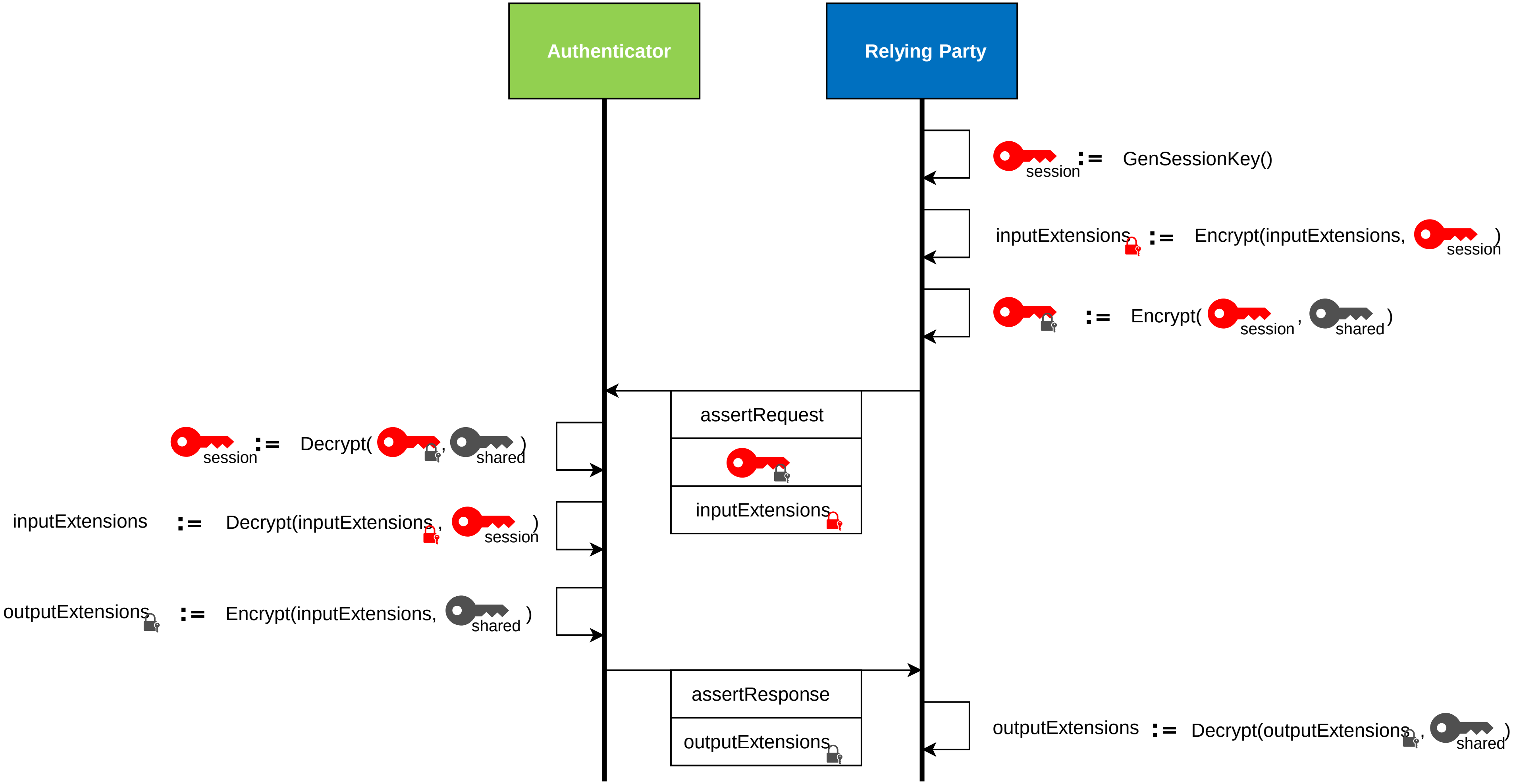
Security properties tested

- Secrecy of the input and output extensions
- Authenticity of input and output extensions

Results

- No attacks discovered ✓

Protocol Design – Authentication



Discussion

Security

- FIDO extensions require further security measures
- Key exchange only secure with proper attestation (otherwise trust-on-first-use)
- Depends on cryptographic algorithms used

Implementation

- Relatively complex protocol
- Compliant with FIDO2 specifications
- Easy to implement using the proof-of-concept implementation[1]

1. https://github.com/Digital-Security-Lab/protecting-fido-extensions-poc

Discussion

Usability

- Important especially in the case of FIDO authentication
- Protocol is unnoticed by the user
- Delay neglectable
  - Measurements on Raspberry Pi Pico
    - Registration: 250 ms
    - Assertion: 5 ms

Conclusion

- No application level encryption for FIDO extensions
  → Vulnerable to MitM attacks

- Not many extensions used yet
  → But relevant extensions like SPC are about to appear soon

- The proposed protocol can effectively prevent attacks
  → Security of the protocol formally verified

Additional Material

- COSE C-library
  https://github.com/abuettner/cose-lib

- Proof-of-concept implementation
  https://github.com/Digital-Security-Lab/protecting-fido-extensions-poc

- Formal evaluation
  https://github.com/Digital-Security-Lab/protecting-fido-extensions-proverif

Thank you!

Contact

Andre Büttner

University of Oslo

Email: andrbut@ifi.uio.no

https://www.mn.uio.no/ifi/english/people/aca/andrbut