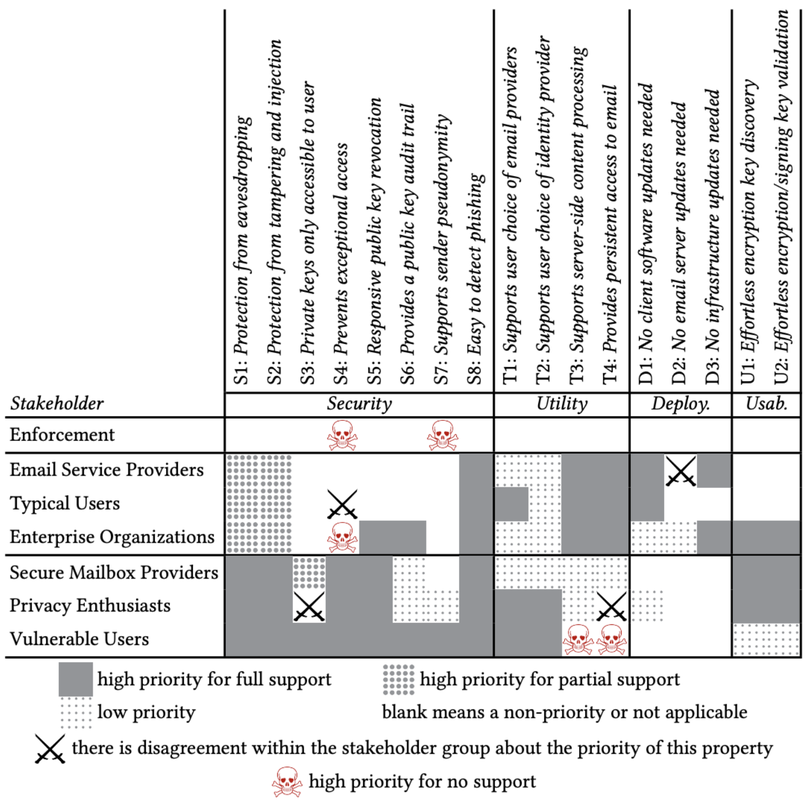
SaTC: CORE: Small:

Usable Key Management and Forward Secrecy for Secure Email

Kent Seamons and Daniel Zappala, Brigham Young University
https://www.nsf.gov/awardsearch/showAward?AWD_ID=1816929

Why don't more people use secure email?

Stakeholder approach shows conflicting goals, resulting in fragmented solutions



"SoK: Securing Email—A Stakeholder-Based Analysis." International Conference on Financial Cryptography and Data Security, 2021

Challenge: Can we make secure user authentication easy to use and easy to deploy?

Tackle a wider range of applications to increase impact

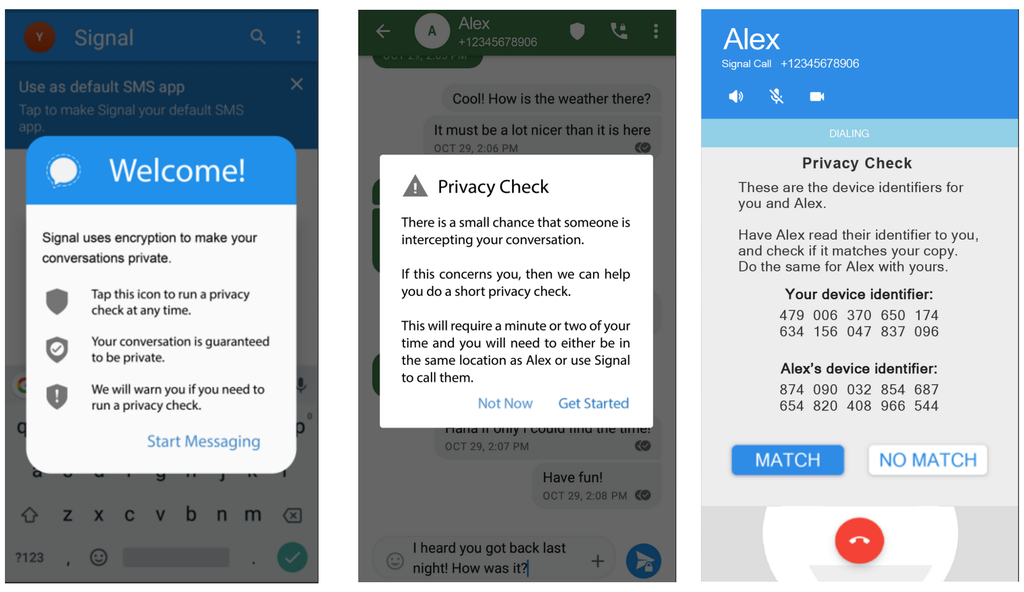
Scientific Impact

Authenticating users is applicable to a wide range of problems in security. Our work demonstrates how a focus on usability leads to automating key management and simplifying user interactions.

Secure Messaging

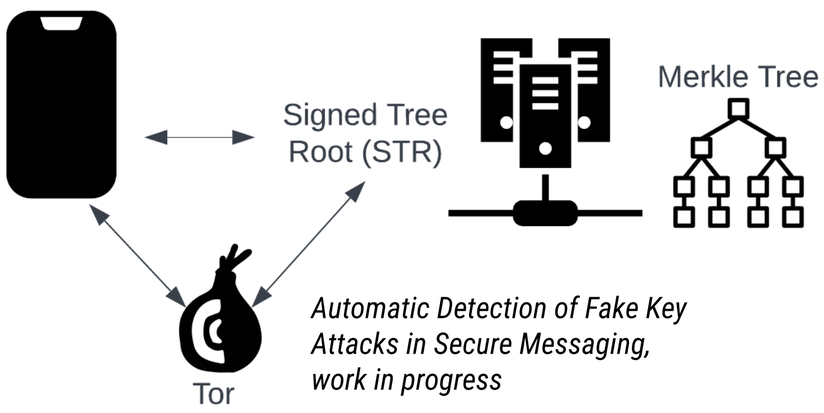
Challenge: A malicious key server could provide fake public keys for users, leading to a man-in-the-middle attack

Approach #1: Improve the usability of the authentication ceremony



"Something isn't secure, but I'm not sure how that translates into a problem": Promoting autonomy by designing for understanding in Signal, SOUPS, August 2019.

Approach #2: Detect fake key attacks using key transparency and anonymous client auditing



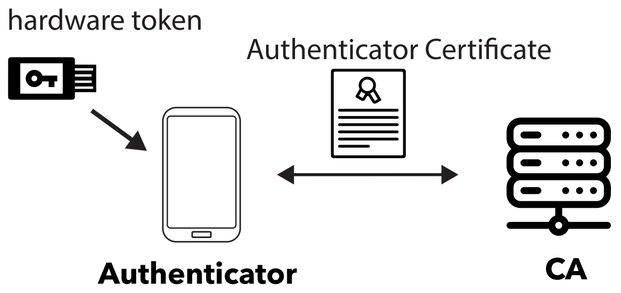
Automatic Detection of Fake Key Attacks in Secure Messaging, work in progress

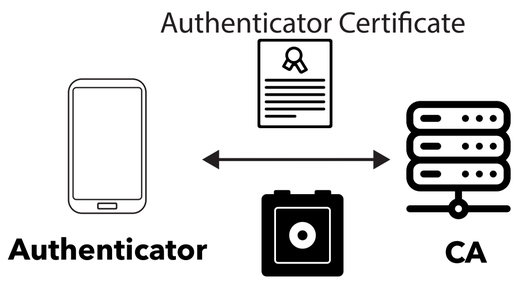
Web Authentication

Challenge: Replace passwords with a system that provides greater security while maintaining high usability

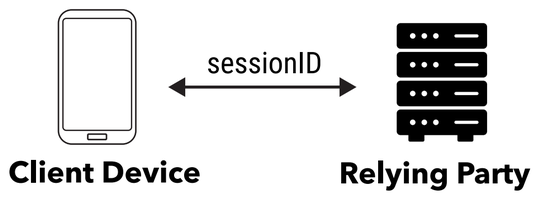
Approach: Automated and centralized management of keys and certificates with Let's Authenticate

1. Use a FIDO2 hardware token to authorize or revoke authenticator access to your account with the CA.
2. Only authorized devices can download the vault, which contains cryptographic keys needed to login to websites.

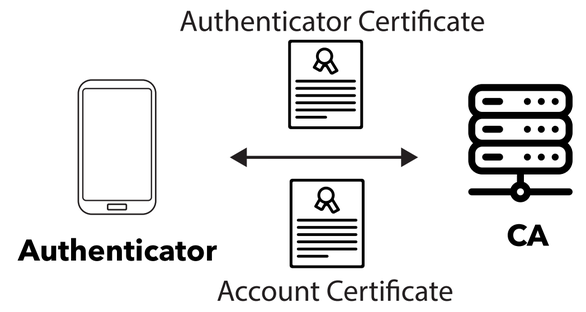




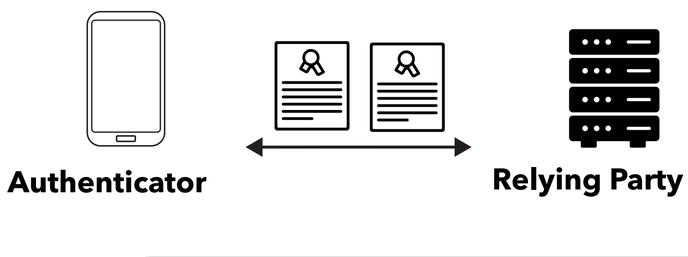
3. Visit a website and obtain a session ID



4. Obtain an Account Certificate to prove ownership of a random ID@letsauth.org



5. Create a session key and sign a Session Certificate authorizing the sessionID to login using ID@letsauth.org
6. Send the Account Certificate and the Session Certificate to the website to register or login



- no trusted third party and no need to carry hardware tokens
- simple account recovery when users lose a device
- portability among multiple authenticators

Let's Authenticate: Automated Certificates for User Authentication, NDSS 2022

Other Authentication Research
2FA Usability Studies (SOUPS 2019, EuroUSEC 2019)
Scalable Certificate Revocation (NDSS 2020, ACSAC 2019)

Broader Impacts

- Billions of users of secure messaging applications can use automated detection of attacks.
- Vulnerable users have clear methods to manually check fingerprints of public keys to guarantee their safety.

34 undergraduates
16 as authors on papers
11 from marginalized communities
1 as lead author (NDSS 2020)

Broader Impacts

- Users will have an easy-to-use method of authenticating to websites and applications that is more secure than passwords.
- Eliminates password breaches and phishing