Ultrablue
Remote attestation over Bluetooth

Gabriel Kerneis, Loïc Buckwell, Nicolas Bouchinet
French National Cyber Security Agency

February 4 – FOSDEM 2023
Bootchain

UEFI → execute → Bootloader → execute → Kernel → execute → Initramfs → execute → Init

passphrase: $ _

Disk decryption
Bootchain with TPM
Bootchain with TPM and remote attestation
Ultrablue – User-friendly lightweight TPM remote attestation over Bluetooth
Ultrablue Stack

server (laptop)

clients (smartphone)
Ultrablue Workflow - Enrollment

- Use a QR code to share channel encryption key
- Get the reference state
- Boot state trusted on first use
Ultrablue Workflow - Attestation

- Get new boot state
- Inspect changes easily
- Control attestation result
Ultrablue Demo
Ultrablu is versatile

- Embeddable in initramfs, or runnable at a later stage
- Usable as a second factor for disk decryption (via PCR extension and LUKS TPM slot)
- Sample `mkosi` scripts to build a test VM demonstrating those features
- We welcome use-cases, suggestions and contributions!
Ultrablue protocol
Protocol overview

Server

Enrollment – QR code pairing

Authentication

Enrollment – EK exchange

Credential activation

Attestation

Client

Off the network

Fully encrypted
Enrollment – QR Code and UUID generation

Server (attester)

TPM

Server

Client

Enrollment specific

Generate encryption key

Connection/Encryption materials

Generate random UUID
Authentication – Mitigate DoS attacks

Server (attester)

TPM

Server

Client

UUID

Generate auth nonce

Auth nonce challenge

Auth nonce response

Nonce validation

February 4 – FOSDEM 2023
Enrollment – Endorsement key exchange

Server (attester)

TPM

Server

Client

Enrollment specific

Generate EK and fetch EKpub/EKcert

EKpub + EKcert + flags
Credential activation – Generate an Attestation Key

Generate AK and fetch AKname

AKname

Generate secret
MakeCredential(EK, AK, secret)

MakeCredential challenge

ActivateCredential(challenge)

Challenge response

Validate challenge response
Attestation – Validate boot state

Server (attester)

TPM

Server

Client

Generate anti-replay nonce

GenerateQuote(AK, anti-replay nonce) and fetch quote + event log

Anti-replay nonce

quote + event log

Validate quote signature

Validate quote anti-replay nonce

Apply PCR policy

Replay event log (optional)

Attestation response

What’s next?

- Integrate with external projects to ease setup
- Get more users and contributors
- Test our FOSDEM release!
  github.com/ANSSI-FR/ultrablue/releases
https://github.com/ANSSI-FR/ultrablue