


Unlock the Door to my Secrets, but don't Forget to Glitch

Marc Schink
Speaker: Silvan Streit

August 19, 2023 @ CCCamp

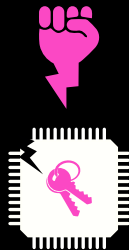


About Me

- Hardware security research
 - Embedded system security
 - Fault- and side-channel attacks
 - Work @ Fraunhofer AISEC
 - Open source contributor
 - OpenOCD
 - libjaylink
 - ...
 - Blog @ blog.zapb.de
- 

Motivation

- Microcontrollers are omnipresent
 - Authentication Tokens, Crypto Wallets, ...
- Their flash memory contains assets
 - Cryptographic keys
 - Intellectual property
- Investigation of new (hardware) attack vectors
- Improved security in future products



Debug Protection

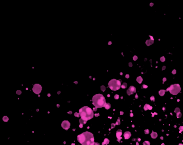
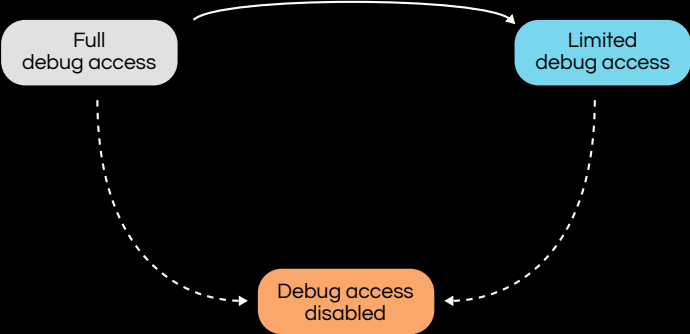
Full
debug access



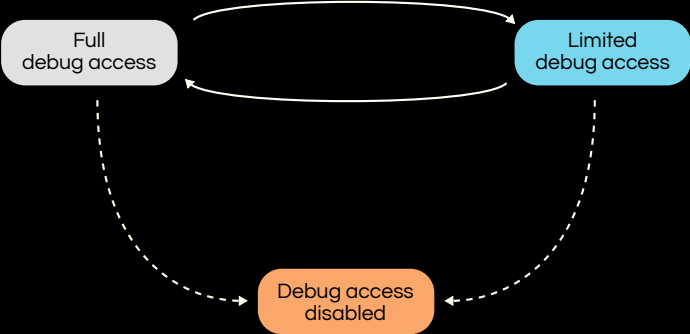
Debug Protection



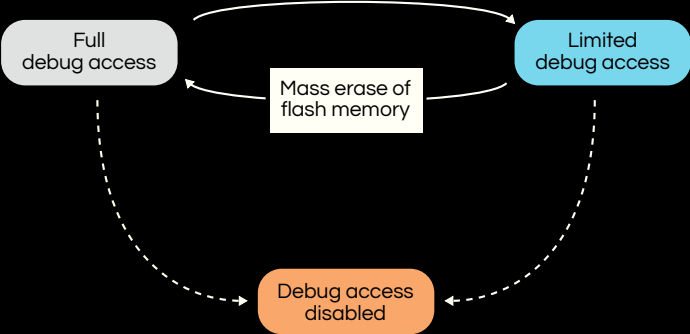
Debug Protection



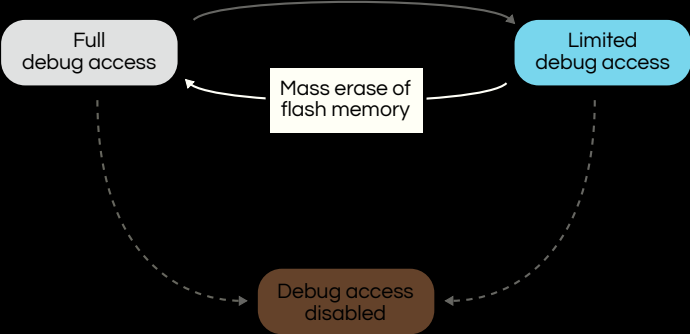
Debug Protection



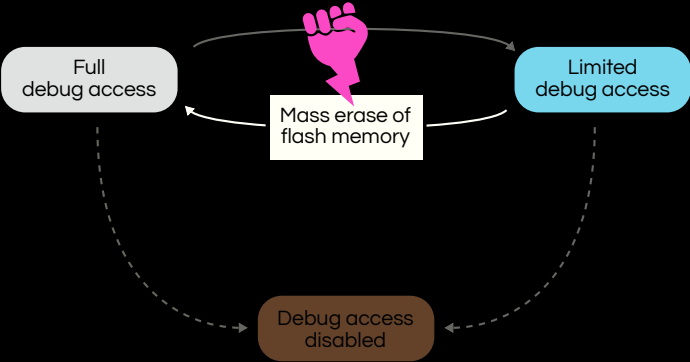
Debug Protection



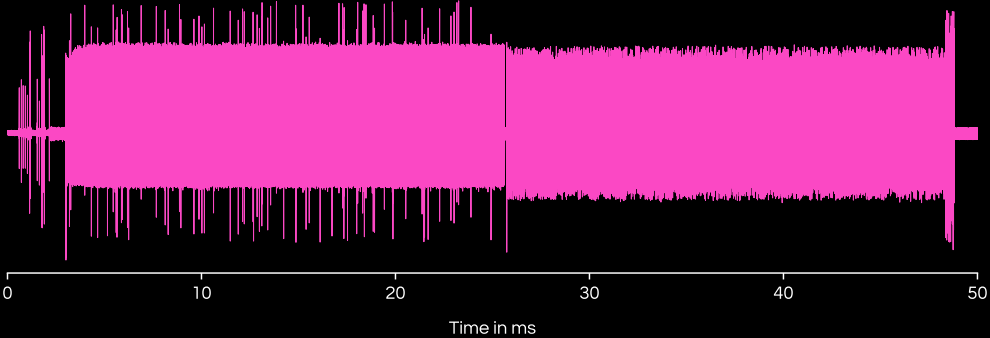
Debug Protection



Debug Protection



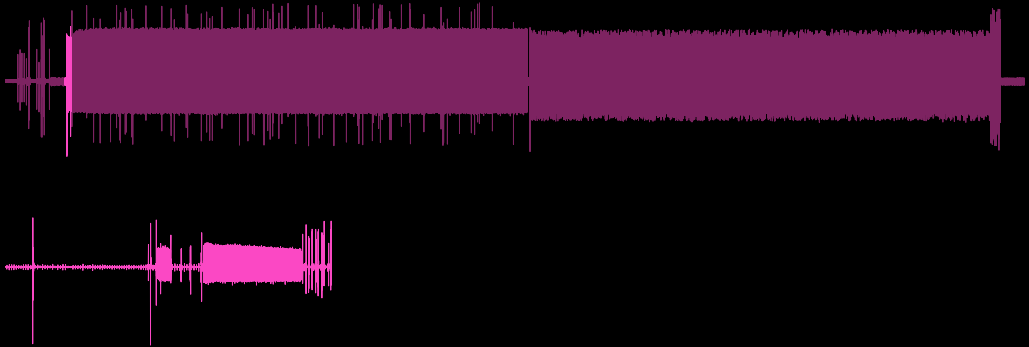
Flash Erase Suppression



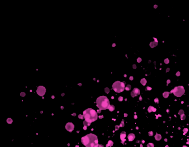
Flash Erase Suppression



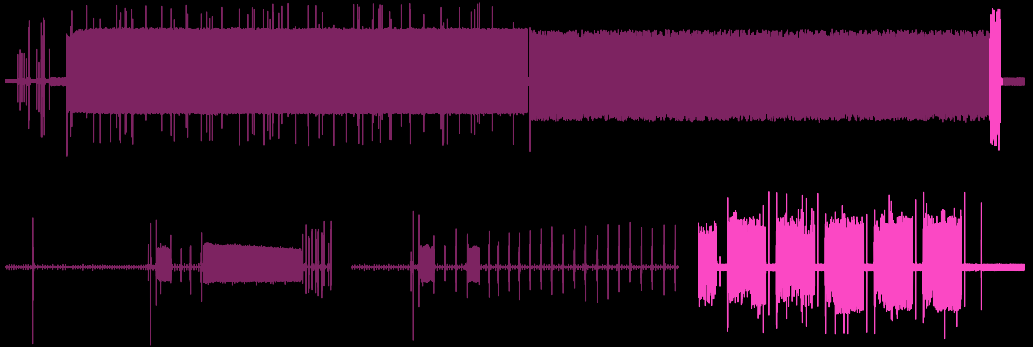
Flash Erase Suppression



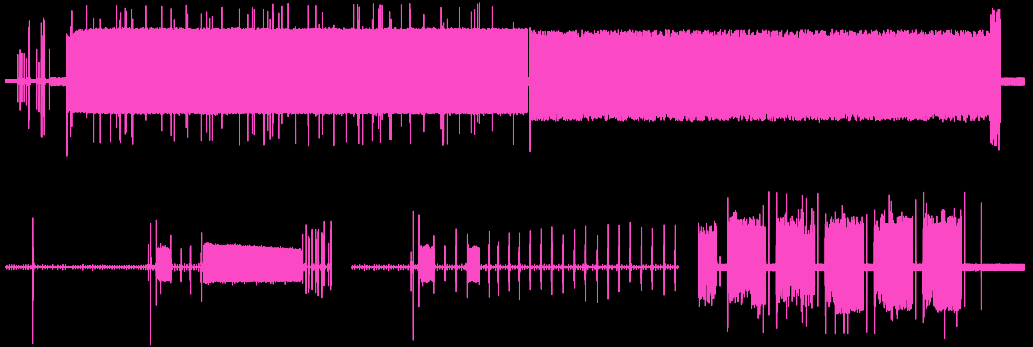
Flash Erase Suppression



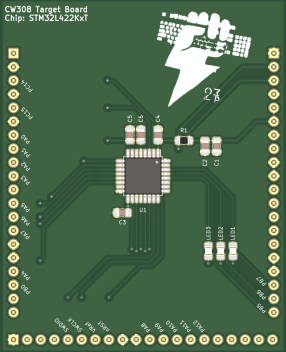
Flash Erase Suppression



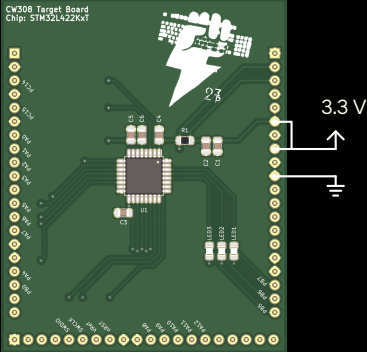
Flash Erase Suppression



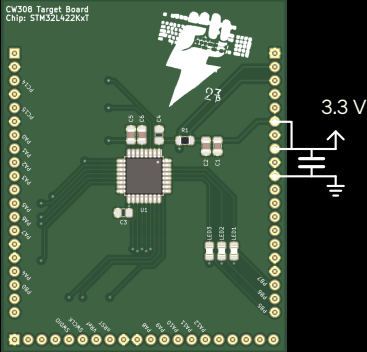
Demo: Setup



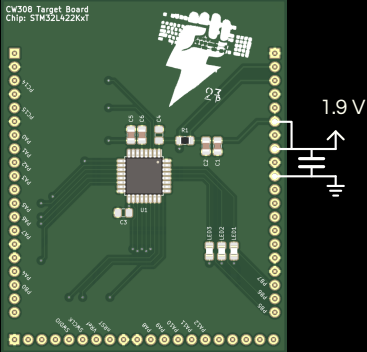
Demo: Setup



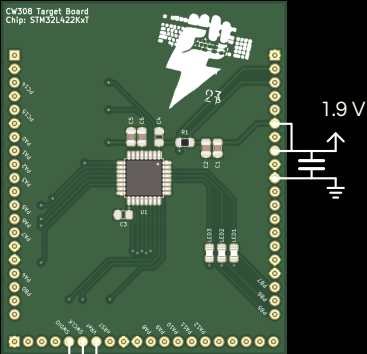
Demo: Setup



Demo: Setup



Demo: Setup



Debug access



Demo

Let's roll!



Conclusion

- Glitch flash mass erase to gain full debug access
 - Access to all assets in flash memory
- Multiple microcontrollers and manufacturers are affected
 - Results will be public soon
 - Paper currently under review
- How to protect yourself?
 - Only application-specific mitigations possible
 - Root cause must be fixed in hardware

