# Yubikey hardware security tokens

## Lunch and learn

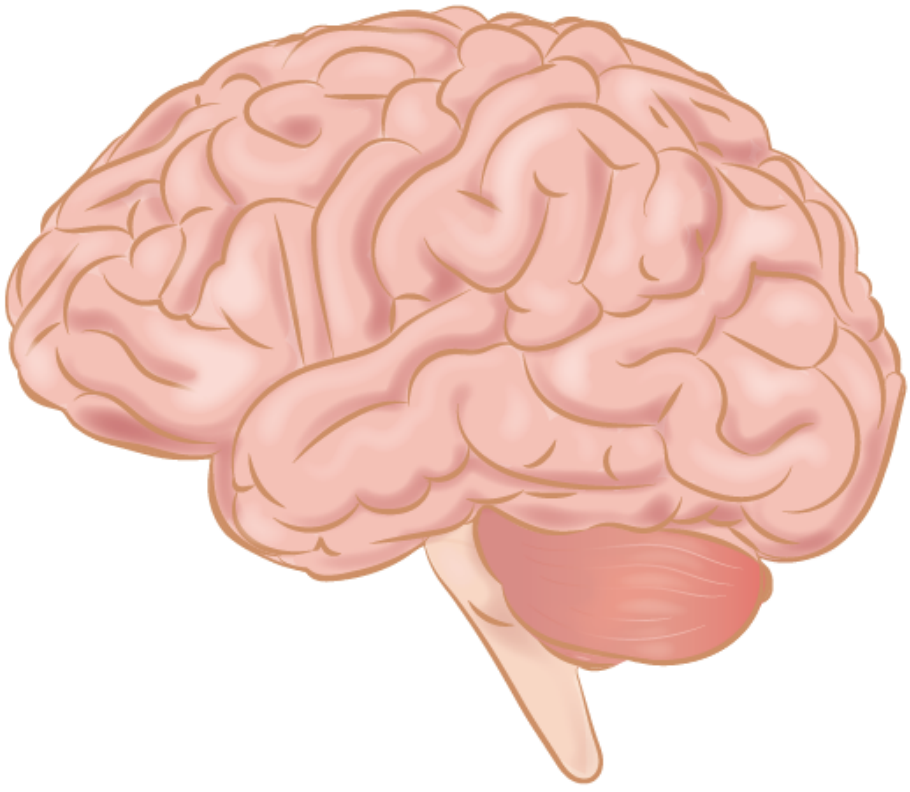
Lars Wirzenius

2020-09-28

# Password strength

- 2010 study: strong passwords need to be at least 12 random characters, 8 will soon not be strong enough.
- 2012: Attackers can brute force every 8 character password in less than 6 hours using 25 GPUs.
- It's 2020. Everything gets more scary now.

# This remembers about 8 random characters



Passwords are passé*

*not entirely true

# What are hardware security tokens?

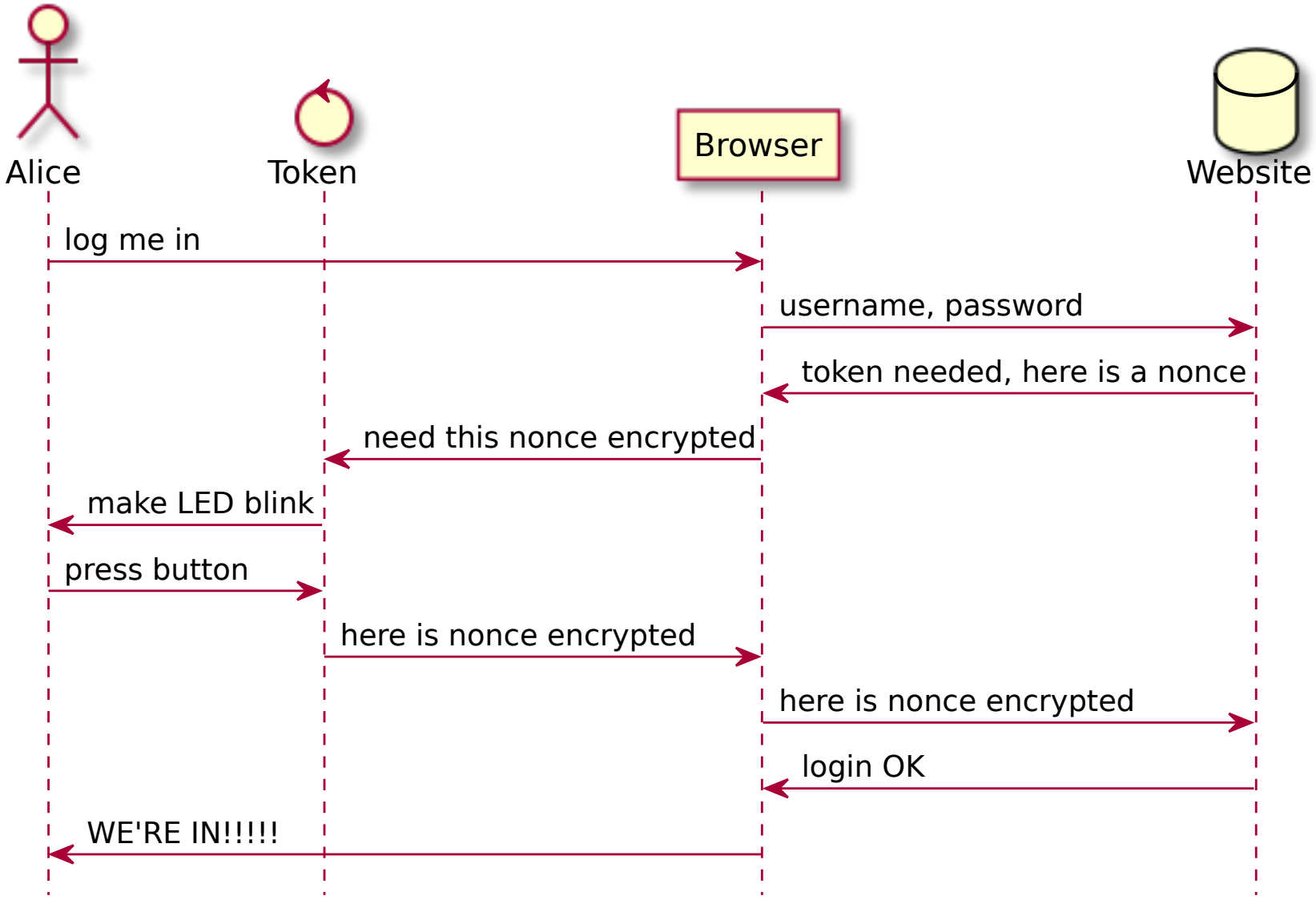
# Why a Yubikey specifically

# Use case: Log into web site

Demo

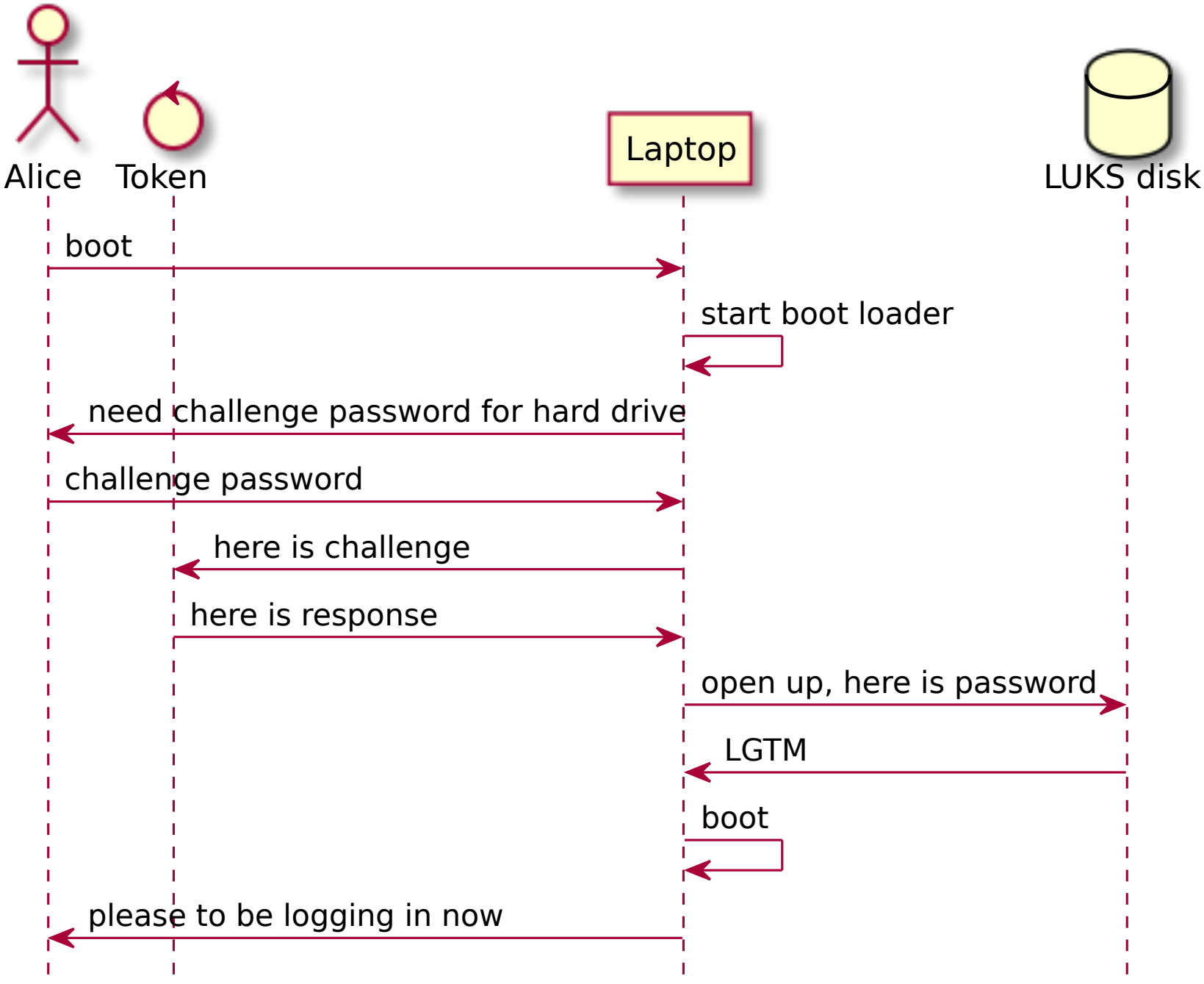
https://demo.yubico.com/

https://gitlab.com/


Alice
Token
Browser
Website
log me in
username, password
token needed, here is a nonce
need this nonce encrypted
make LED blink
press button
here is nonce encrypted
here is nonce encrypted
login OK
WE'RE IN!!!!!

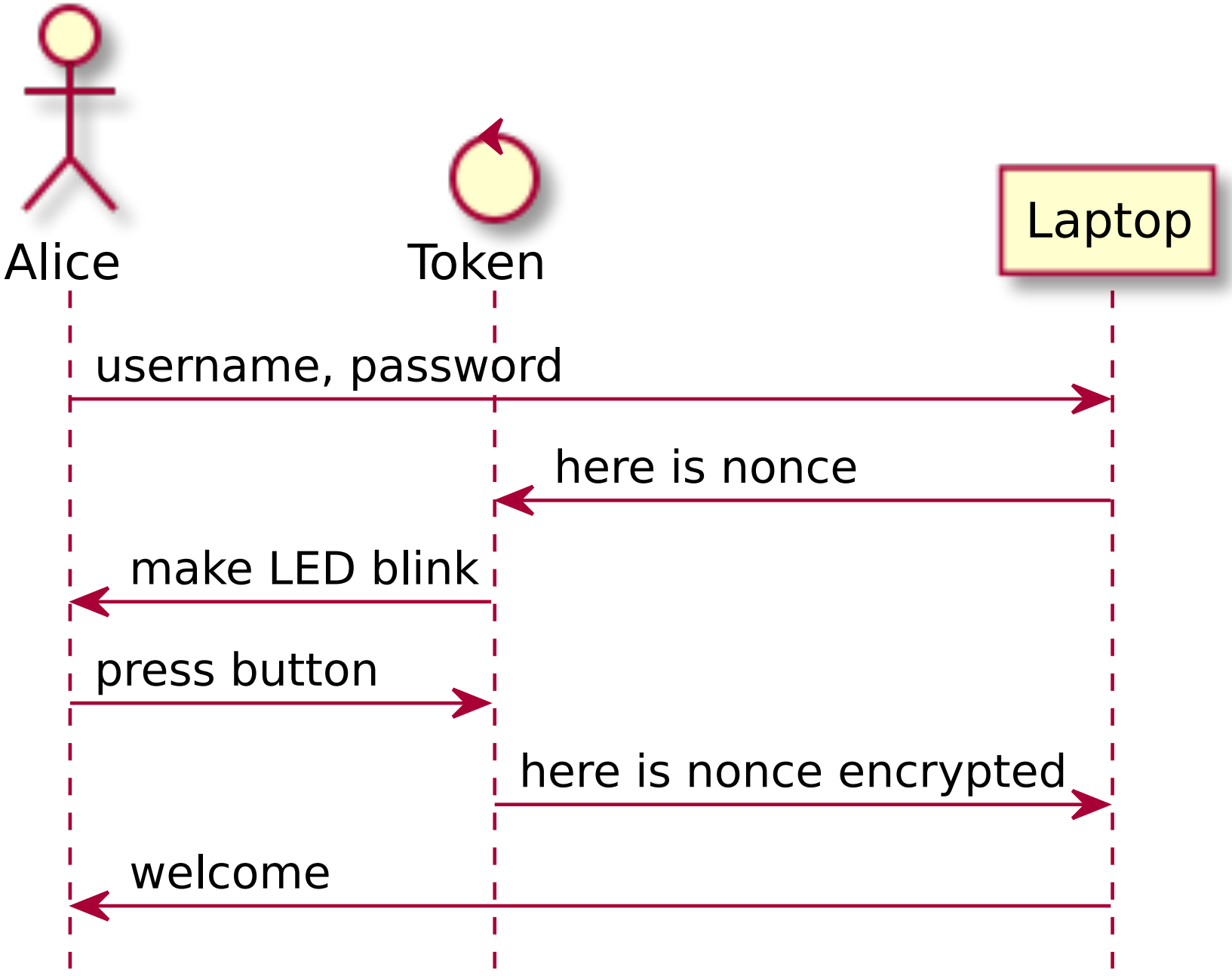
# Use case: Full disk encryption

- Linux: yubico-luks
- Mac, Windows: something, I don't know


Alice
Token
Laptop
LUKS disk
boot
start boot loader
need challenge password for hard drive
challenge password
here is challenge
here is response
open up, here is password
LGTM
boot
please to be logging in now

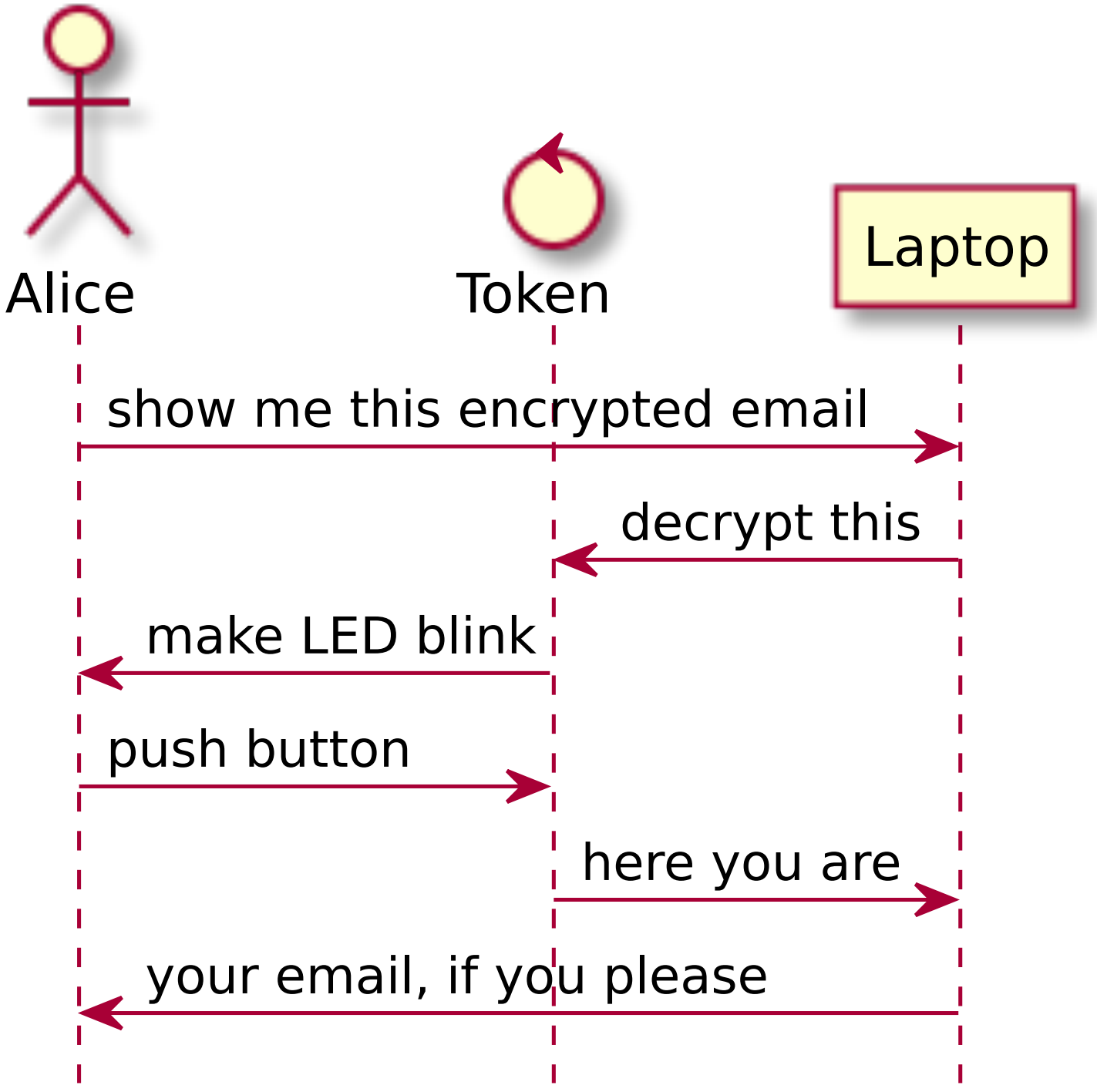
# Use case: Log into system

- can be 1FA or 2FA
- Linux: libpam-u2f, libpam-yubico
- local logins: getty, su, sudo, desktop
- also SSH or any other service


Alice
Token
Laptop
username, password
here is nonce
make LED blink
press button
here is nonce encrypted
welcome

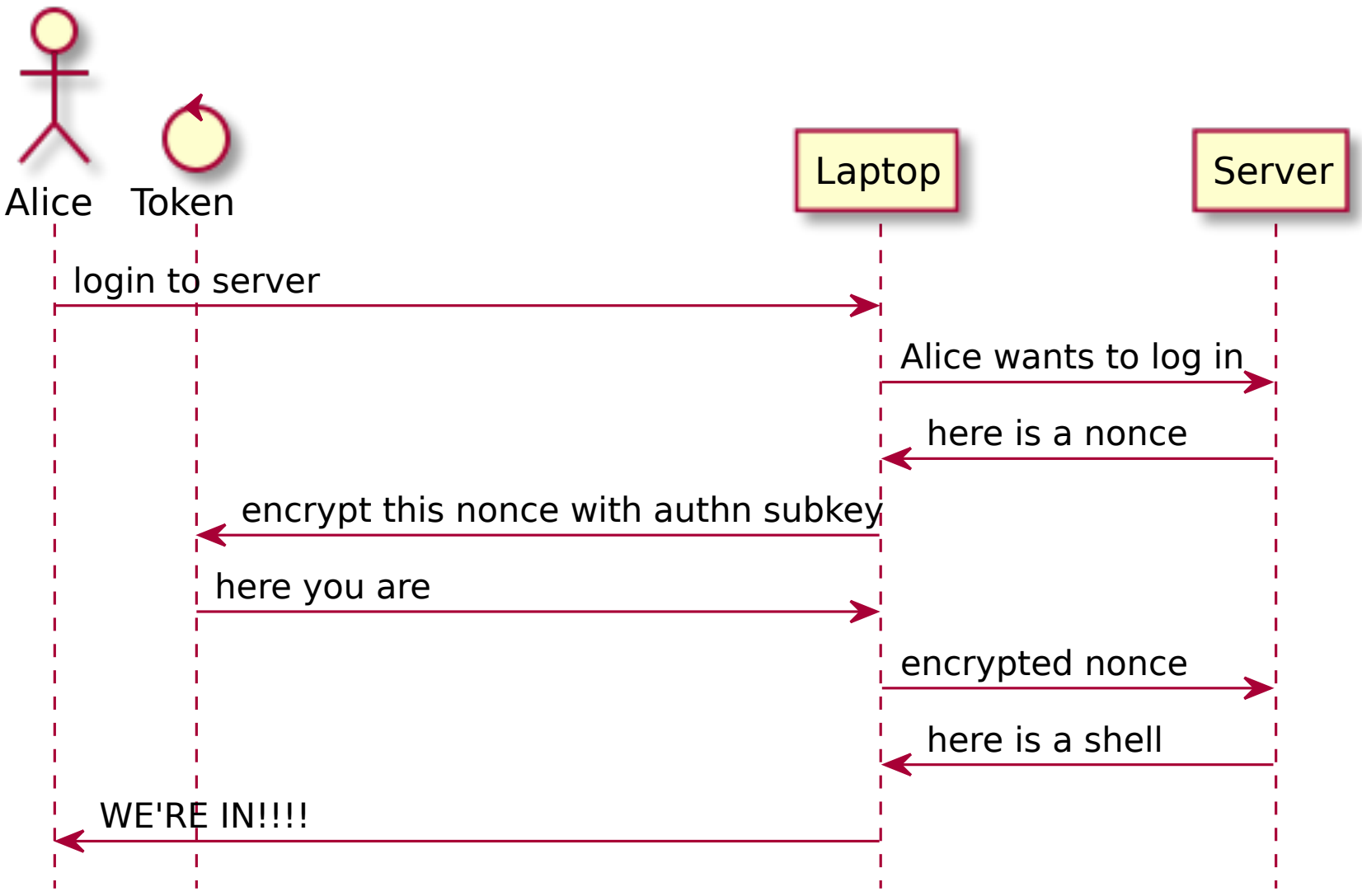
# Use case: OpenPGP

- Private subkeys stored on token
- All operations involving private keys happen on token


Alice
Token
Laptop
show me this encrypted email
decrypt this
make LED blink
push button
here you are
your email, if you please

# Use case: SSH

- OpenPGP authentication subkey on token
- `gpg-agent` acts as an SSH agent


Alice
Token
Laptop
Server
login to server
Alice wants to log in
here is a nonce
encrypt this nonce with authn subkey
here you are
encrypted nonce
here is a shell
WE'RE IN!!!!

# Here how you configure everything

Not part of this talk.

Sorry.

# SEE ALSO

Password strength:

- http://web.cs.wpi.edu/~guttman/cs557_website/papers/passwords/MorrisThompsonPasswordSecurity.pdf
- https://en.wikipedia.org/wiki/Password_strength
- https://arstechnica.com/information-technology/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/
- https://arstechnica.com/information-technology/2013/03/how-i-became-a-password-cracker/

Configure Yubikeys and operating systems:

- https://github.com/drduh/YubiKey-Guide
- https://infosec-handbook.eu/blog/yubikey-luks/
- https://infosec-handbook.eu/blog/yubikey-2fa-pam/

# Legalese



Images from Injurymap, https://www.injurymap.com/free-human-anatomy-illustrations, and Yubico.com.