

Paranoid Habits

Part 1: Security Tips

What's this about?

Topics:

- Authentication
- Phishing
- PGP
- SSH
- USB
- Networking

“Can I trust you, Denis?”

- Trust no one, remember how this talk is called
- I just share what I do myself
- I do my best to follow all the latest infosec topics
- I'm familiar with basic pen-testing, [CTF](#) is my hobby
- I reported 6 serious vulnerabilities in my career
- People around me think I'm paranoid

Authentication

Passwords — most common authentication method

- Passwords must be long (>8 characters in 2019)
- Can not contain words, must be random
- Must contain numbers and special characters
- Must be different for each service/web-site/access
- Must be securely stored
- Otherwise, they can be cracked

Passwords — how do people crack passwords?

- It's not under your control
- Depends on how websites store your password/hash
- Some old hash functions like MD5 are easily crackable with modern hardware and software ([hashcat](#))
- Can be found in dictionaries or brute-forced (up to 8 characters)
- Databases with hashes [often get leaked](#)

Passwords — how do people crack passwords?

Some services just fail to protect our passwords:

- [Twitter](#) was logging plain-text passwords till May 2018
- [GitHub](#) was logging plain-text passwords till May 2018
- [Facebook](#) stored plain-text passwords for years

These companies have hundreds or even thousands of employees, how can we trust all of them not to sell it?

Passwords — we're only humans

- Most humans are not capable to satisfy the requirements
- Please use password managers — still can leak your passwords but it's better than not having them
- And please, don't write them down anywhere

I recommend [pass](#) —
Standard Unix Password
Manager, that is based on
[GPG](#) and [Git](#)

Demo (pass)

Passwords alone are not
secure

2FA — 2 Factor Authentication

- I've never heard of anyone saying
“My 2FA-protected account got hacked”
- So, **USE 2 FACTOR AUTHENTICATION!**

2FA — Options

- SMS — the most insecure, can be intercepted
- Authentication App — bound to your phone that can die, be hacked or stolen
- **Security token** (e.g. Yubikey) — U2F (Universal 2 Factor)

Demo (U2F)

Passwords?

Where we're going we don't need passwords

“One of the primary weaknesses of password-based authentication is that a password is a shared secret”

webauthn.guide

WebAuthn

- Is based on asymmetric cryptography
- You need a security token (e.g. Yubikey)
- Server stores only the public key,
so if it leaks it's useless for an attacker
- Works in mobile and desktop browsers except Safari
(still under the experimental flag)

Demo (WebAuthn)

Phishing

Do you remember “[Celebgate](#)”?

“Collins [person responsible for the attack] allegedly gained access by setting up emails designed to look like official accounts associated with the Google or Apple services used by his celebrity targets.”

[Washington Post](#)

Check the URL!

PGP

PGP — Pretty Good Privacy (GnuPG)

- In my opinion, the most reliable tool
- 2 modes:
 - Asymmetric — private/public keys
 - Symmetric — encryption with a password
- You can store your keys on a Yubikey and use them for SSH, encryption, signing data (e.g. Git commits)

PGP — Pretty Good Privacy (GnuPG)

The tool itself is reliable but plugins for mail clients that use the tool can be vulnerable.

Sebastian Schinzel gave a talk at 35c3 how they found some vulnerabilities in email client plugins.

Demo (GPG + Yubikey)

SSH

SSH — Secure SHell

- Don't use passwords to access your servers
- It's better to forbid passwords at all:

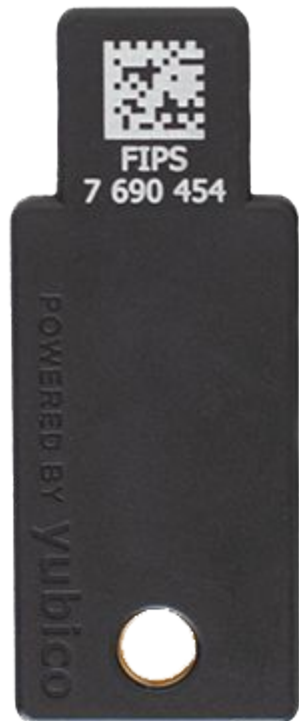
in /etc/ssh/sshd_config

PasswordAuthentication no

- Use public/private key pair
- [Store the key pair on a Yubikey](#) and use from there

Demo (SSH + Yubikey)

Buy this Yubikey already!



Yubikey

- It's a write-only security token device
- 2FA (U2F/OTP)
- GPG (Smart Card mode), can store your keys
- SSH via GPG
- FIDO2 (WebAuthn)
- USB-A, NFC, USB-C
- PIN-protected, requires a touch

USB

USB is vulnerable

- Exploiting a device via USB is easier than you think
- There are many ways to hack you via USB
- Don't use public USB sockets/charging stations, they can be compromised

If you still want though...



Use protection!

Networking

Networking — Rules

Use a firewall

- iptables for Linux
- Built-in for Mac or [LuLu](#) for advanced control

Networking — Observe

Look for suspicious traffic:

- iftop for Linux (*nix systems)
- netstat -atulp

Demo (iptables, iftop)

Links

- [have i been pwned?](#)
- [pass — the standard unix password manager](#)
- [Four embarrassing password leaks on live TV](#)
- [WebAuthn Guide](#)
- [Yubico](#) (Yubikey manufacturer)
- [Guide to using YubiKey for GPG and SSH](#)
- [Attacking end-to-end email encryption](#)

“Sorry, my account got hacked”
is the new
“The dog ate my homework”

[Linus Sebastian](#)

Thank you!
Q/A