



A SMALL ;tool< HANDBOOK FOR
FABMANAGERS WHO WONDER HOW
TO CYBERSECURE THEIR FABLABS

INSPIRED BY: JULIA EVANS

BY: ALINE BÉCQ



Hi, this is me
Aline, a French Fablabmanager
specialized in internal Fablabs

And I have been wondering...
? How to increase the cybersecurity
of a Fablab without compromising
its agility ...

I want to avoid 2 things



Armwrestling with
the IT



Spiraling inside
the tech push tornado



Higher education is a
target of choice, so
is manufacturing

Could internal
fablabs
become
attack
surfaces?



CONTEXT

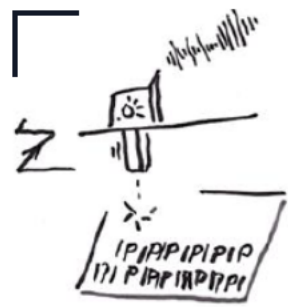
> ifconfig
> ip route
> nmap -sn 10.1.1.1



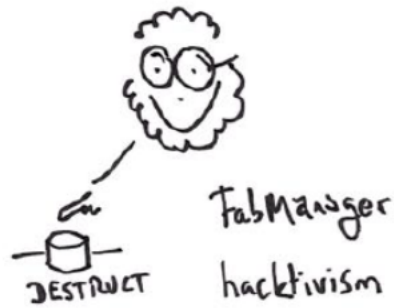
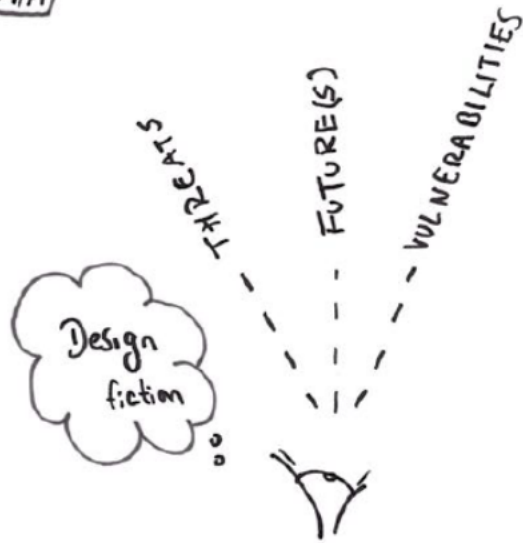
A dry topic,
difficult to apprehend

Wonderful tools in
open-source exist,
waiting to be brought
to light



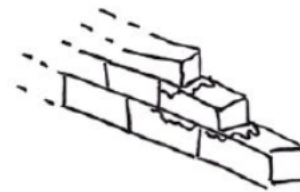


Material / Side channel
data exfiltration



Prevention also relies on imagining
possible threats

This is just the beginning,
the first cyber-bricks,
feedbacks & contributors
are welcome !



Many rabbit
holes are left
to be explored but the clock is
ticking ...



OS tools & projects
mentioned

OpenSSL

WireGuard

VirtualBox

oFRak

OpenSeal

Eurydice

nmap

ncrypt

GPT4All

Wireshark

F5DRAG

Ansible

Inspect

bias.wiki

open v Switch

PrinThor

Hackberry

open CVE

Vulnerable Codes

CRA-ready

Zine maker

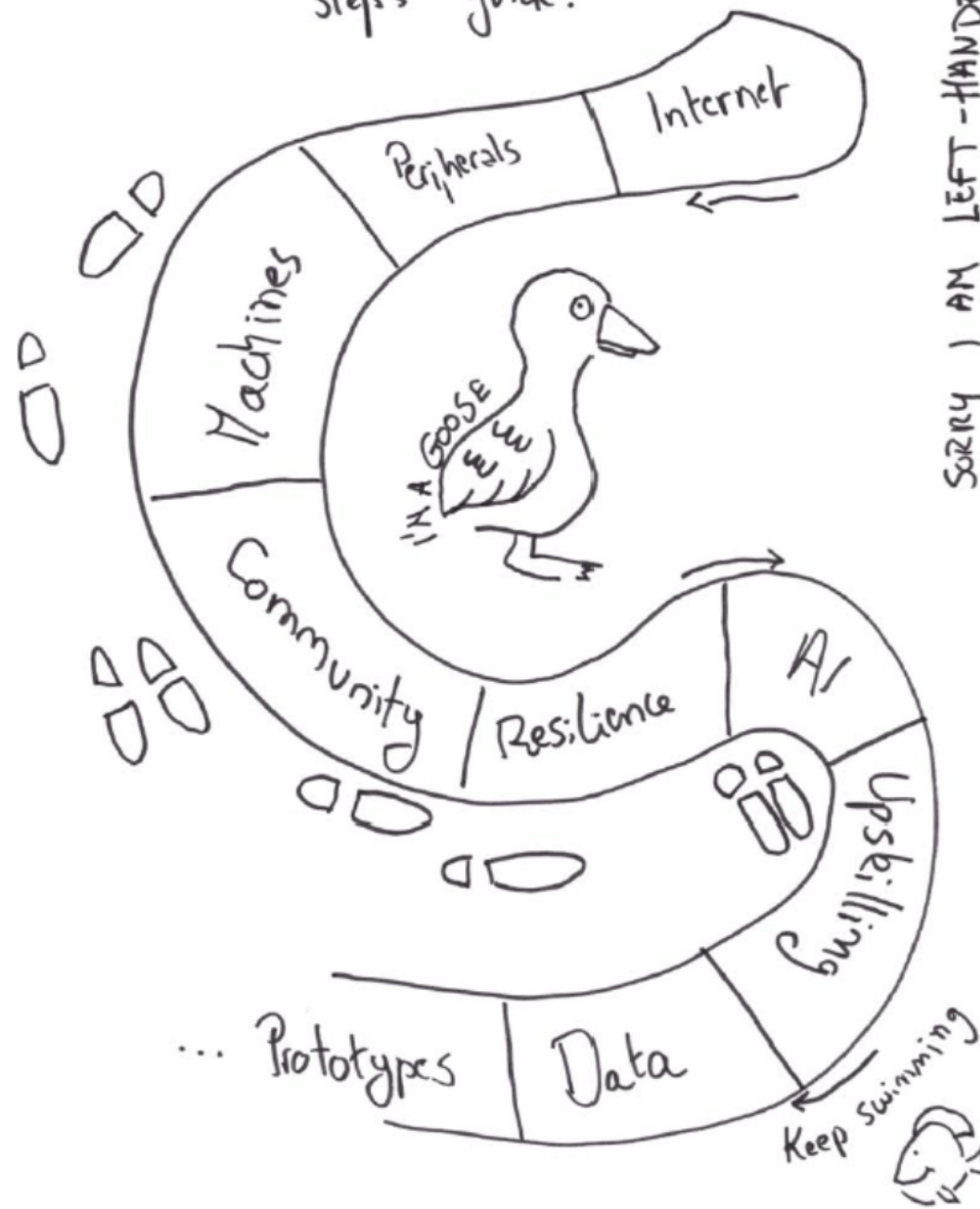
QEMU

egcode

Ludus



I will guide you through a 10-ish
steps guide:



SORRY I AM LEFT-HANDED :)



A first drastic solution

Unplug, decouple networks, become air-gapped
 ! Air-gapped is not airtight as peripherals
 can be vectors of Stuxnet

1. Internet



Use VMs and keep your
 explorations inside a
 sandbox

↳ Virtual Box



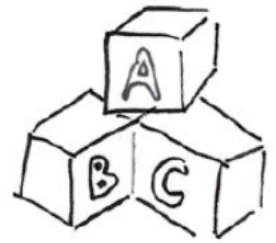
Use VPN tunnels

↳ Wire Guard



Acronyms & Initialisms

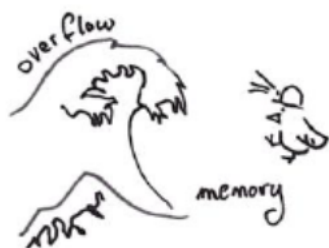
AI: Artificial Intelligence
 BOM: Bill Of Material
 CERT: Computer Emergency Response Team
 CRA: Cyber Resilience Act
 CVE: Common Vulnerabilities & Exposures
 DDOS: Distributed Denial Of Service
 GDPR: General Data Protection Regulation
 IP: Intellectual Property
 IT: Information Technology
 LAN: Local Area Network
 LLM: Large Language Models
 OT: Operational Technology
 RAG: Retrieval Augmented Generation
 VLAN: Virtual LAN
 VM: Virtual Machine
 VPN: Virtual Private Network



Many other cyber-related acronyms on:

app.xmind.com/gYrF6Twv

Let's prevent the Fablab productions to become
new attack surfaces or harming devices



Share vulnerable codes
and ways to protect
them

↳ VulnerableCodes



↳ Install parties

Remind your community
of the legal
framework

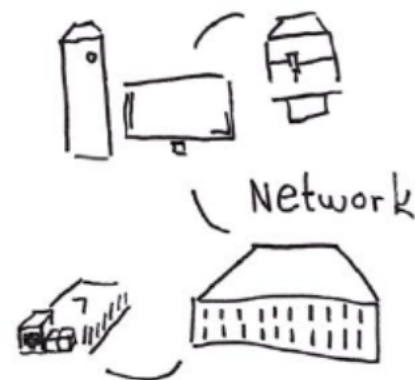


↳ CRA-ready

Organize distros &
RUST IDE parties



Map the topology
of your network
↳ nmap

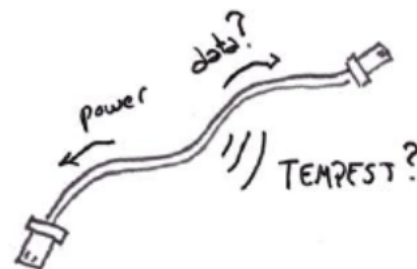


listen to its
traffic



↳ Wireshark

Assess your equipments
& the reputation of
the manufacturer



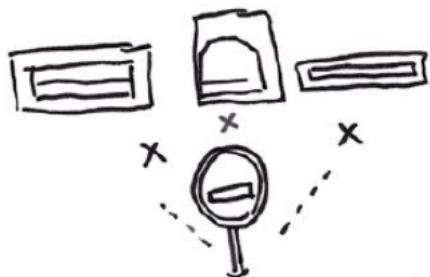
Use segmentation or
(V)LAN to contain
usage types

↳ Open vSwitch



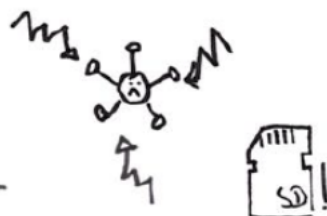
Protect the ports

- ↳ 3D models to print



If using peripherals
consider a decontamination

Station



3. Machines

Consider a firmware retrofit rewritten in RUST

↳ Printhor



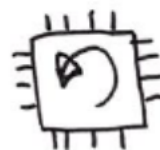
If managed with
a cloud service
good luck 😊



Decompose your equipments (Bom)

• build a tailored CVE watch (hardware & software)

L Open CVE



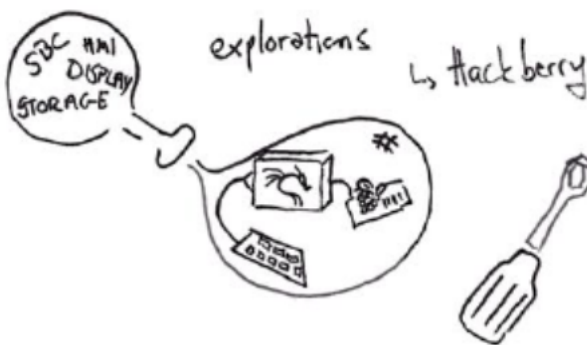
EQUIPMENTS



Build a cyberdeck
dedicated to cyber

explorations

↳ Hack berry



Simulations & emulations
can be used to test
architectures

L, QEMV

↳ ludus

E
 M
 U
 L
 A
 T
 O
 O
 O
 N

When using AI there is a risk of data leak, your data could be used to train the model and become public.

✓ Check the risks of your LLM
↳ Inspect



Build a RAF locally
(Retrieval Augmented Generation)

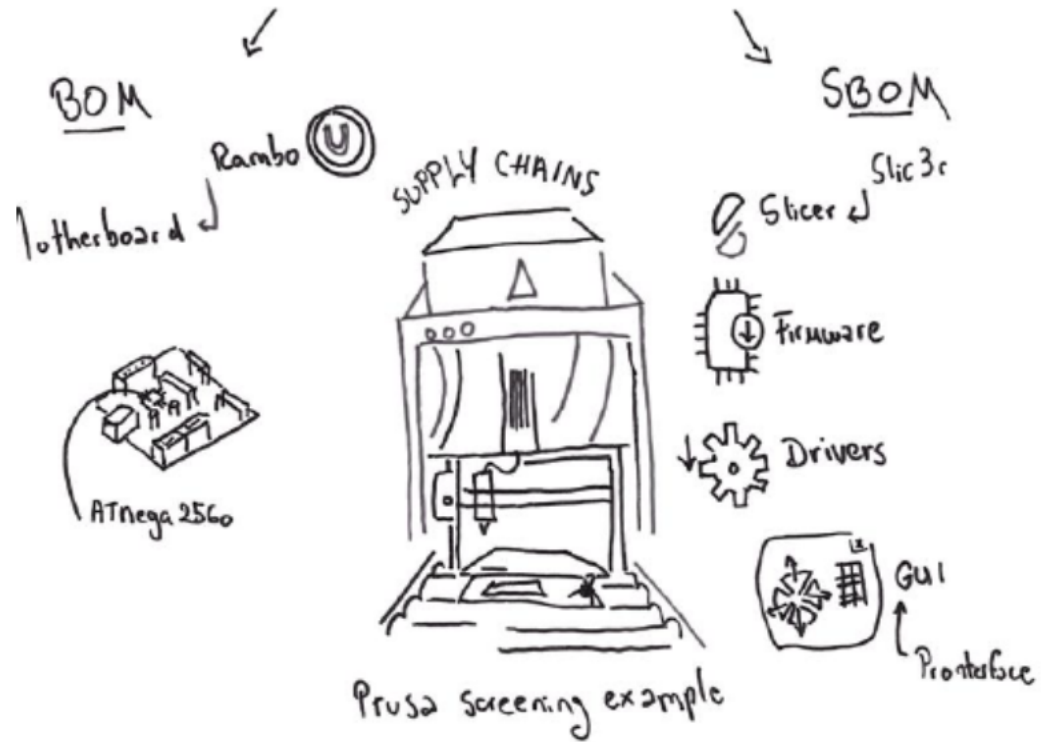
↳ GPT4All

↳ FaBRAF

Keep your distance with your LLM to avoid personification & overtrust!

↔ LLM it's like
↳ bias.wiki

Let's reveal hidden dependencies



COMMUNICATION

Vectors: USB B cable, SD, Bus
Protocols: SPI
Formats: ASCII plain text
Languages: Gcode, C++
Serialization: ecode (project)

> M82
> G21
> G90
> M82
> M104 s200...

DATA STORAGE

Localization: Fat32, caches
Memory types: NAND Flash, RAM
Serialization: Encryption, WriteProtect, Sanitization

Humans represent the bigger vulnerability of your lab.

Promote

ACCOUNTABILITY
over POLICING

Set an example by
applying GDPR
↳ encrypt



4. COMMUNITY

Digital signature

implementation on repos & files

↳ Open Seal

e.

Check credential
leaks on repos
↳ GitLeaks



Save the network topology of
your lab in case you need to redeploy



↳ Ansible



Resilience

Do you apply the
3-2-1
rule?



Document and
share



3 copies of data



1 off-site



2 different storage types