Getting Physical
Meet Local Hackers Near $AREA

Kirils Solovjovs
26.10.2022.

possible.lv

IT drošības risinājumi

Introduction

- Possible Security lead researcher
- White hat hacker
  - Network flow analysis
  - Reverse engineering
  - Social engineering
  - Consulting clients
- https://kirils.org/
- twitter / @KirilsSolovjovs

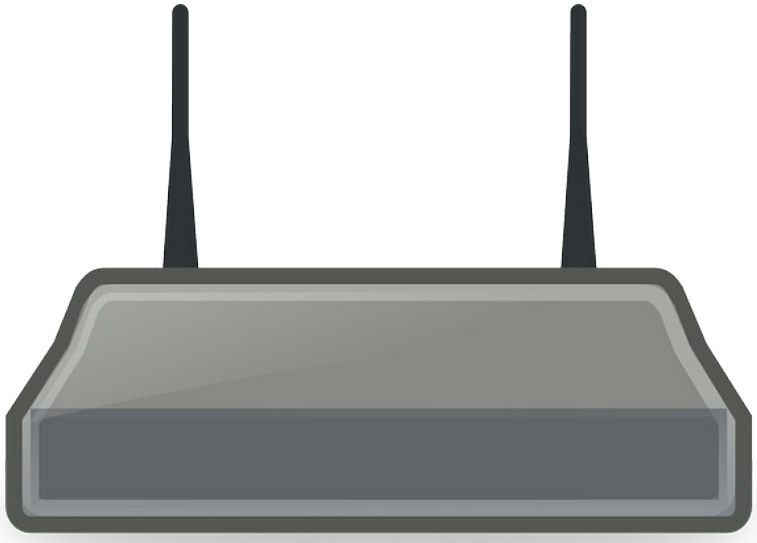
This story is based*

— based? based on what?

— true events

Guest network

Guest network misconfiguration



Access card database

Unauthorized editing of access card database

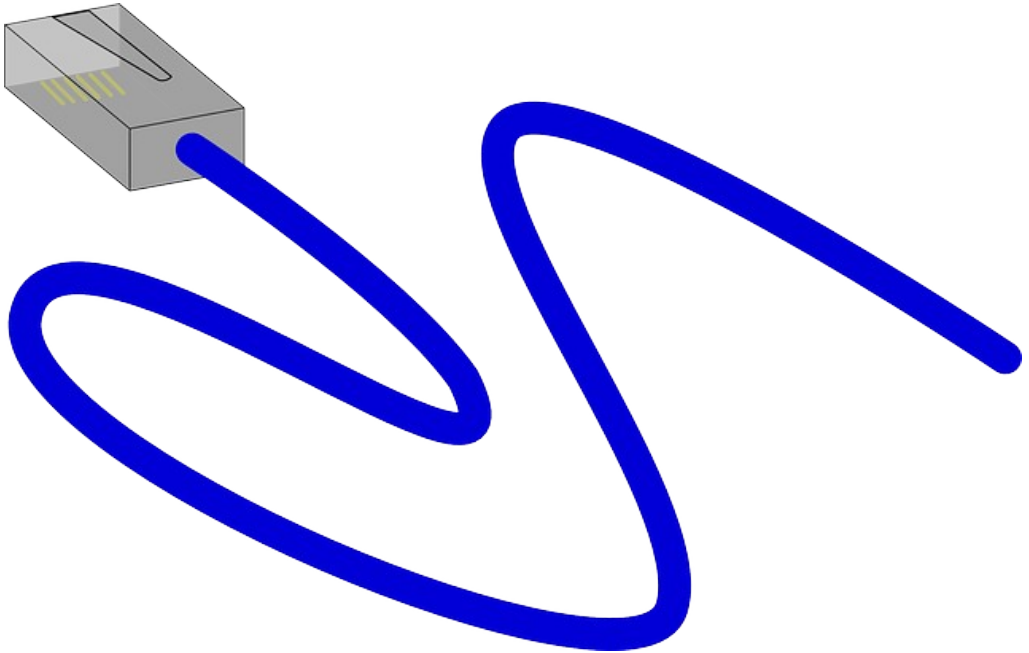
Domain administrator access

- Unattended PC
- Local administrator password
- Domain administrator access

This is another story

Alone in the conference room

Dropping a network remote access device



MAC address filtering

- MAC address spoofing

“Unclonable” card

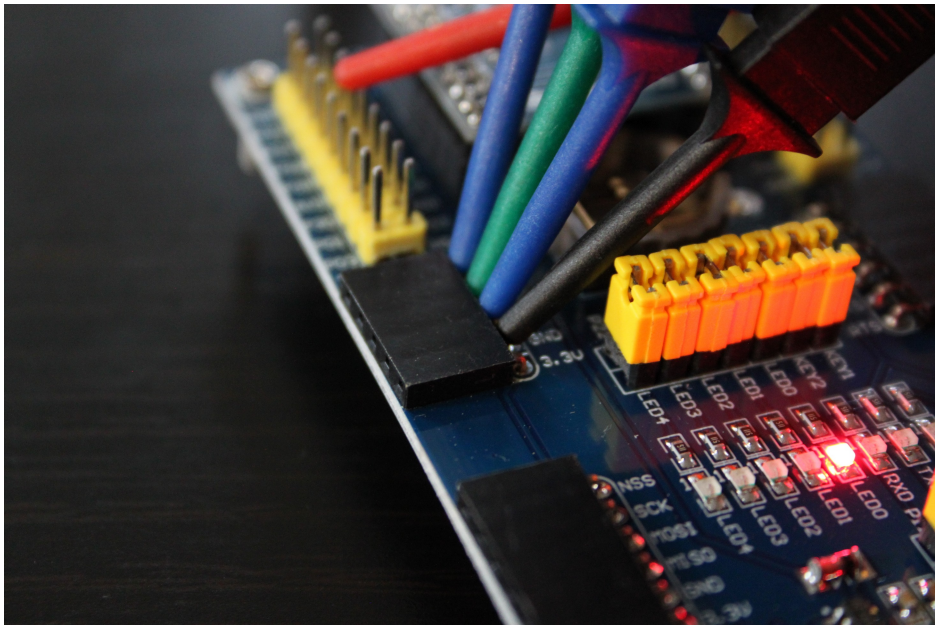
RFID card cloning

Recommendations

Recommendations

- Correctly configure client **and** network isolation
- Unattended computers should be protected with password (*bonus points: lock the room*)
- Physical connections to network should be limited, monitored and protected
- Key cards should be kept safe by using a RFID blocking sleeves

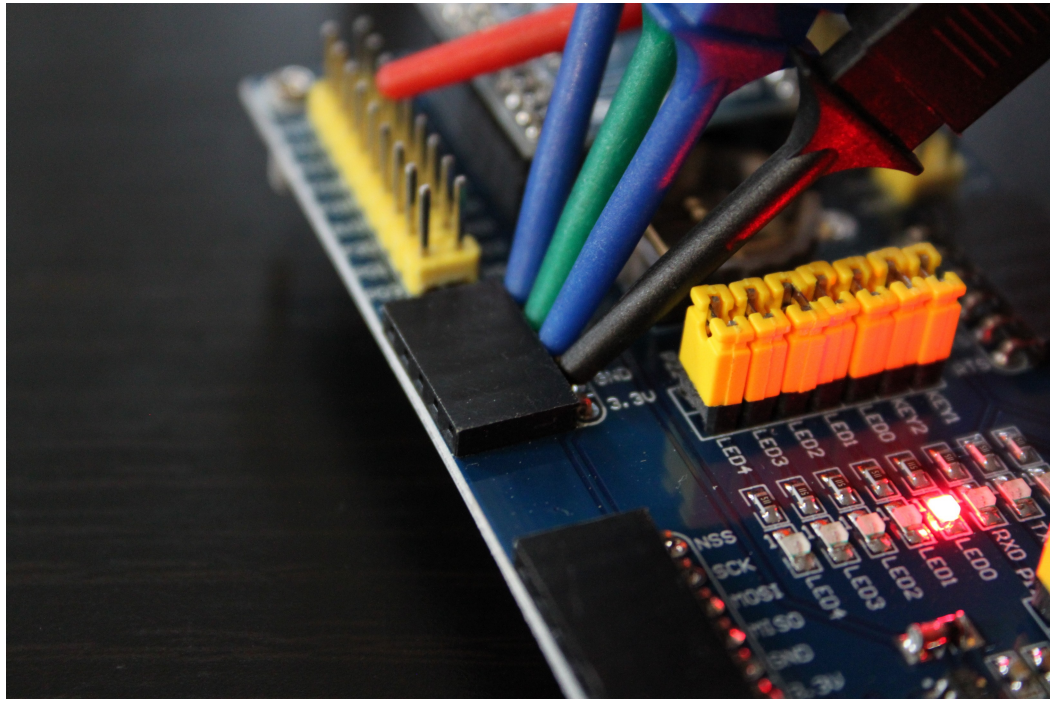
Possible Security



- Penetration tests and audits
- Hardware and software security
- Consulting
- Premium-level service

Possible Security services

- Penetration tests and audits
- Red team tests (attack simulations)
- Incident response
- Vulnerability research
- Reverse engineering
- Consultations
- IT security trainings



Thank you for your attention!

@KirilsSolovjovs
https://kirils.org/

possible.lv

IT drošības risinājumi