Undetectable Interception of Network Traffic on LAN Technologies

Dmitry Virovlyanskiy
SUAI, Russia

November, 2013

Introduction

- Traditional hardware key-loggers are no longer work
- Small chances of getting access to networking hardware
- Wired network connections trusted way more then wireless

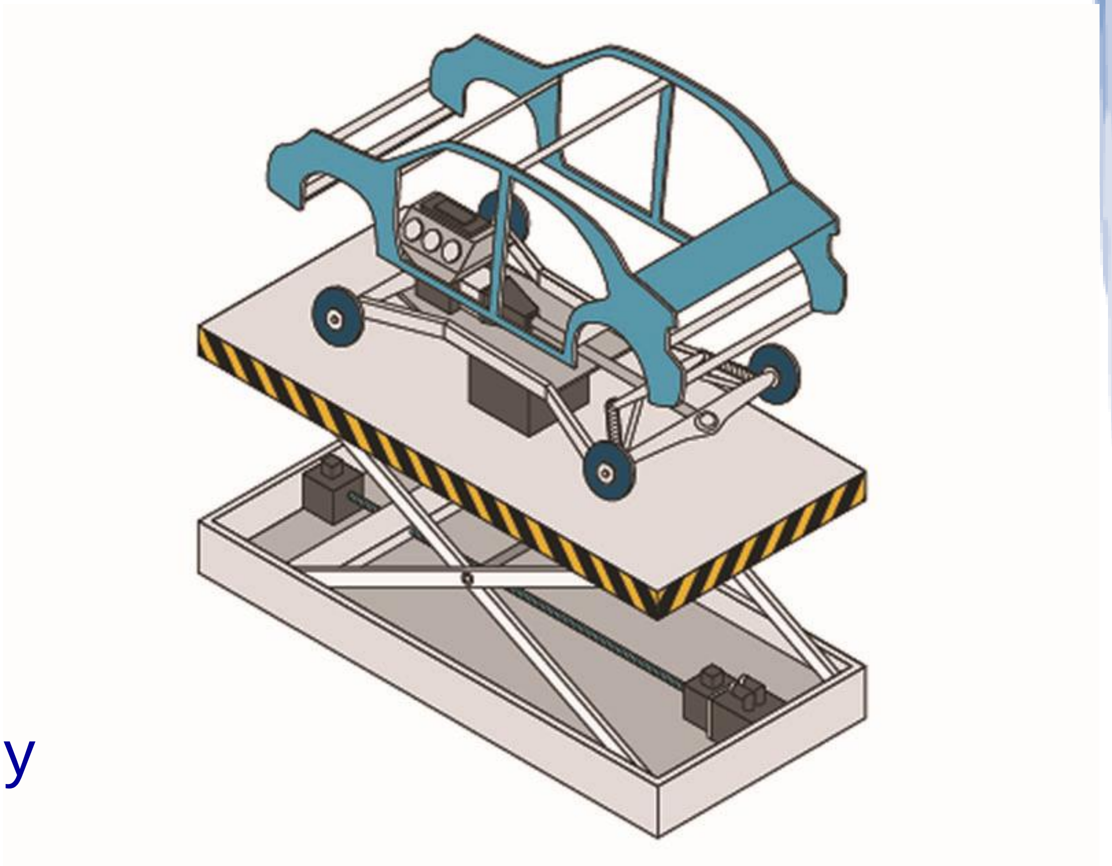
Requirements

Main goal

- Sniffing
- Interception
- Invisibility of device
- Remote access

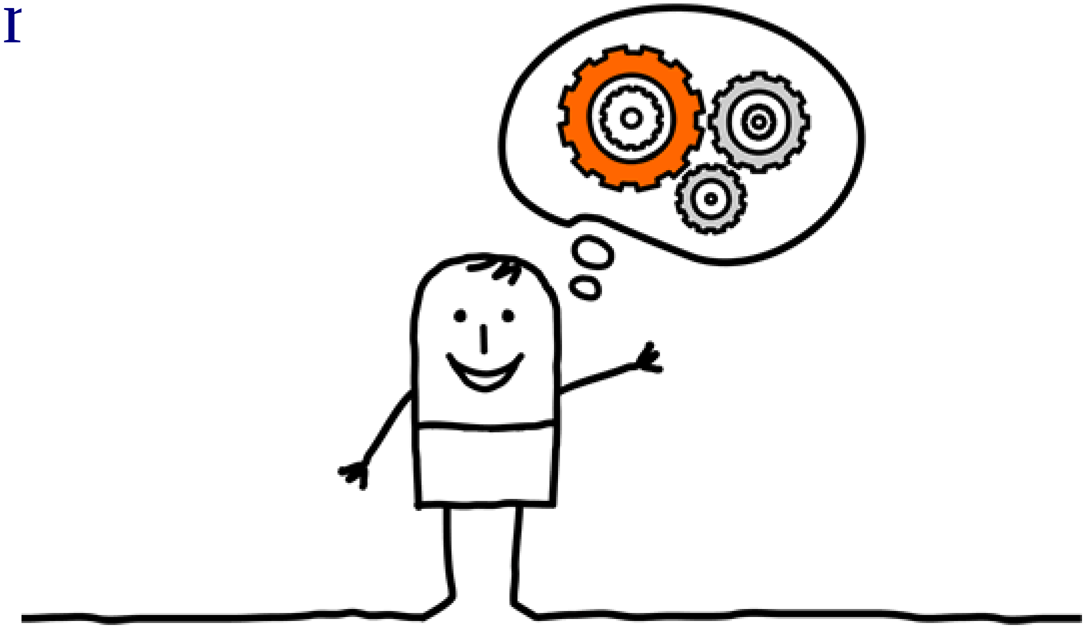
Secondary

- Universal power supply
- Failsafe
- Fast installation and connection



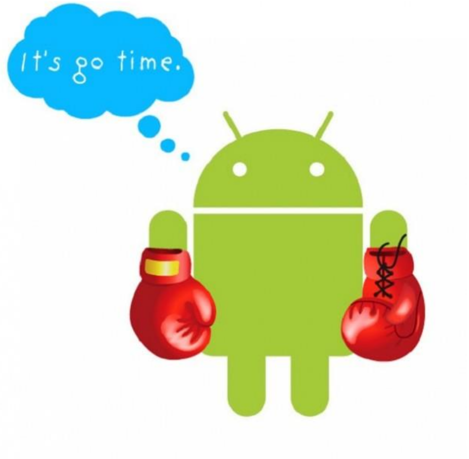
Developing System

- Single-board computer
- Dual ethernet port
- Linux brige
- UART
- Hardware pair swich extention
- Power supply
- Multiple wireless interfaces



Existing solutions

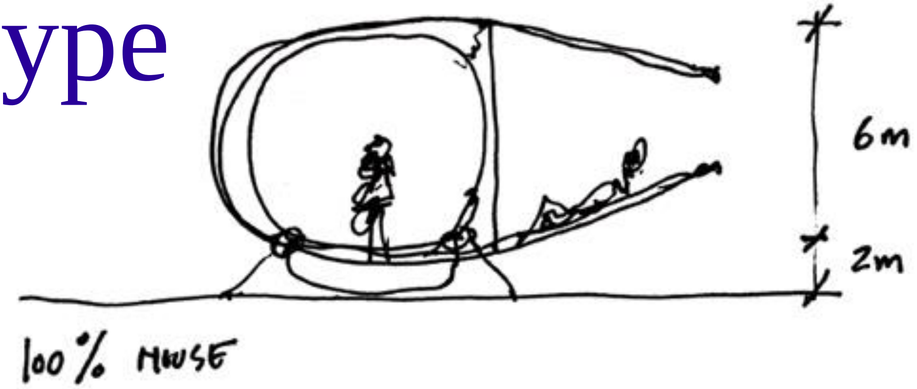
- Modified hardware Wi-Fi router
  - Standalone sniffer
  - Ability to save dump
  - Controlled by Wi-Fi
- Throwing Star LAN Tap
  - Looks like a star
- Pwn Plug Elite
  - Runs the ARM build of Ubuntu Linux
  - Several wireless interfaces



Comparison

	Device 1	Device 2	Device 3
Transparency	-	-	-
Availability MITM	N/A	-	N/A
OS	dd-wrt	-	Debian
Power supply	+	-	±
Remote control (SSH)	+	-	+
Additional tools	±	-	+
RAM usage	8 mb	-	N/A

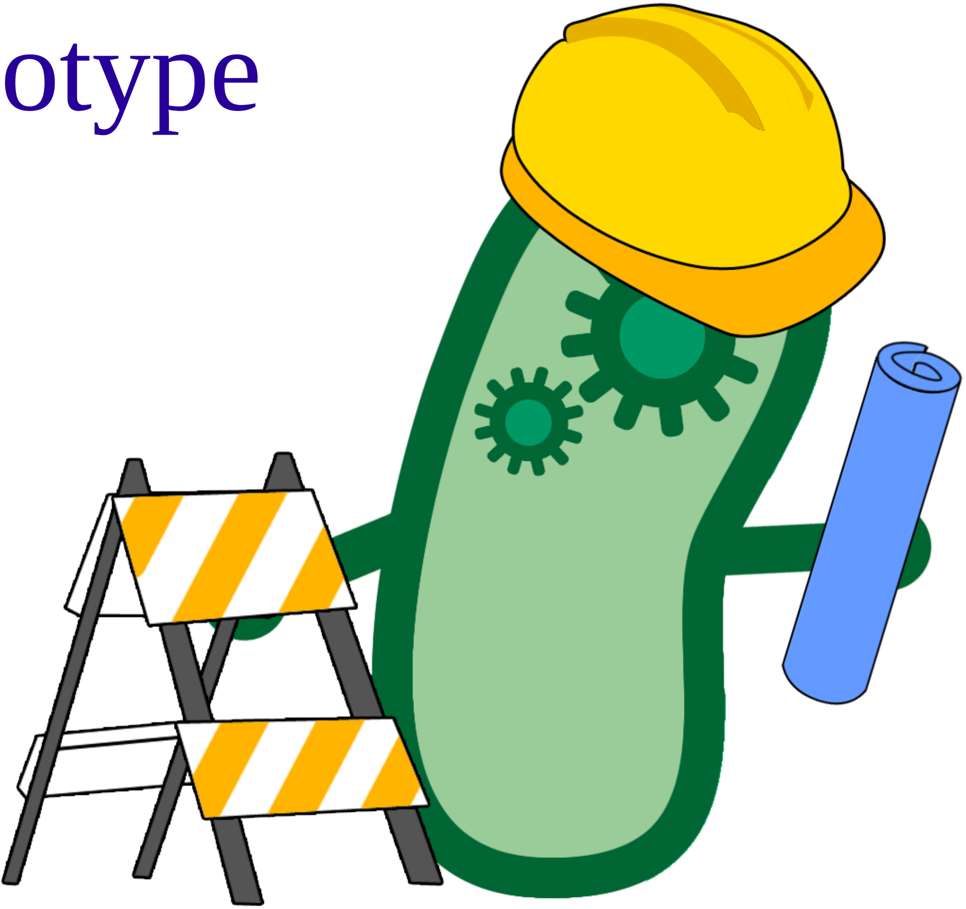
Prototype



- Hardware switch
  - Based on relays
  - 2 modes: active and failsafe
  - UART connection to the main board
  - 5v power
- Current setup
  - Three stand-along workstations
  - Two Ethernet cards
  - Ethernet cables with the RJ-45 connectors

Prototype

- Software
  - Ssltrip
  - Wireshark
  - Tcpdump
  - bridge

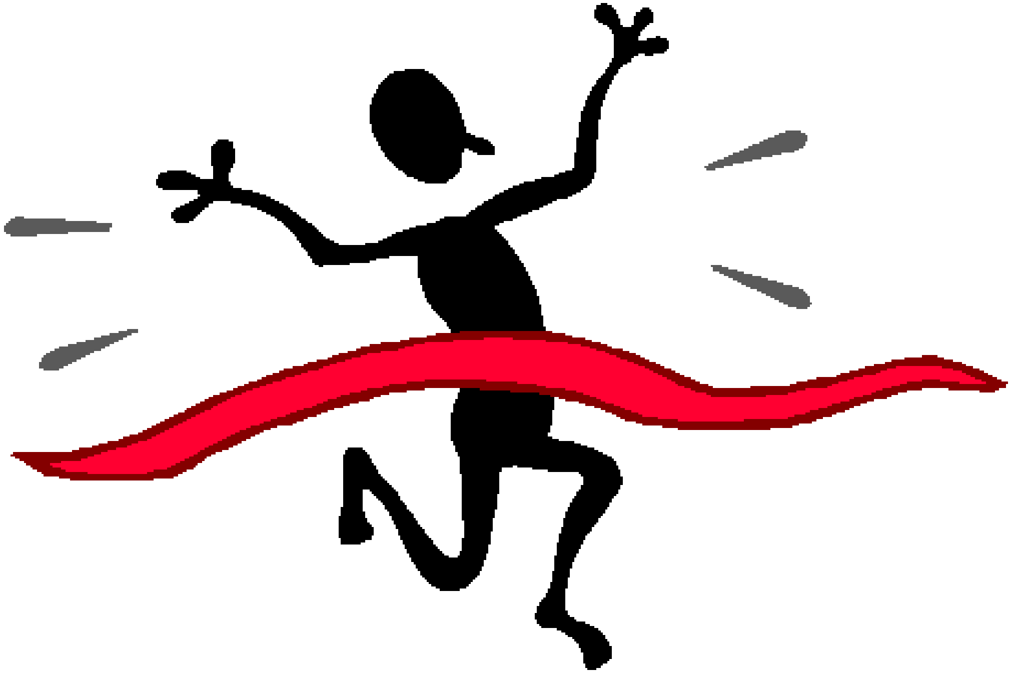


Future research and development

- Hardware switch PCB layout
- Try solid state relays
- Try ARP-proxy
- Active attacks (spoofing, MitM, etc...)
- Porting tools to ARM
- Power supply: Battery and AC
- Self-destruct

Conclusion

- Prototype of device
  - Sniffing
  - Interception
  - Invisibility of device
  - Remote access



- Use such technologies as SSL, SSH, VPN

Q&A

Thank you

Dmitry Virovlyanskiy
SUAI, Russia
e-mail: fr50hz@gmail.com