The Importance of Physical Security in Networking

Ben Matthews

RMHAM-U/NerdFest
February 2023

So my ISP installed a thing in my apartment (and it wasn't working)

What to do?

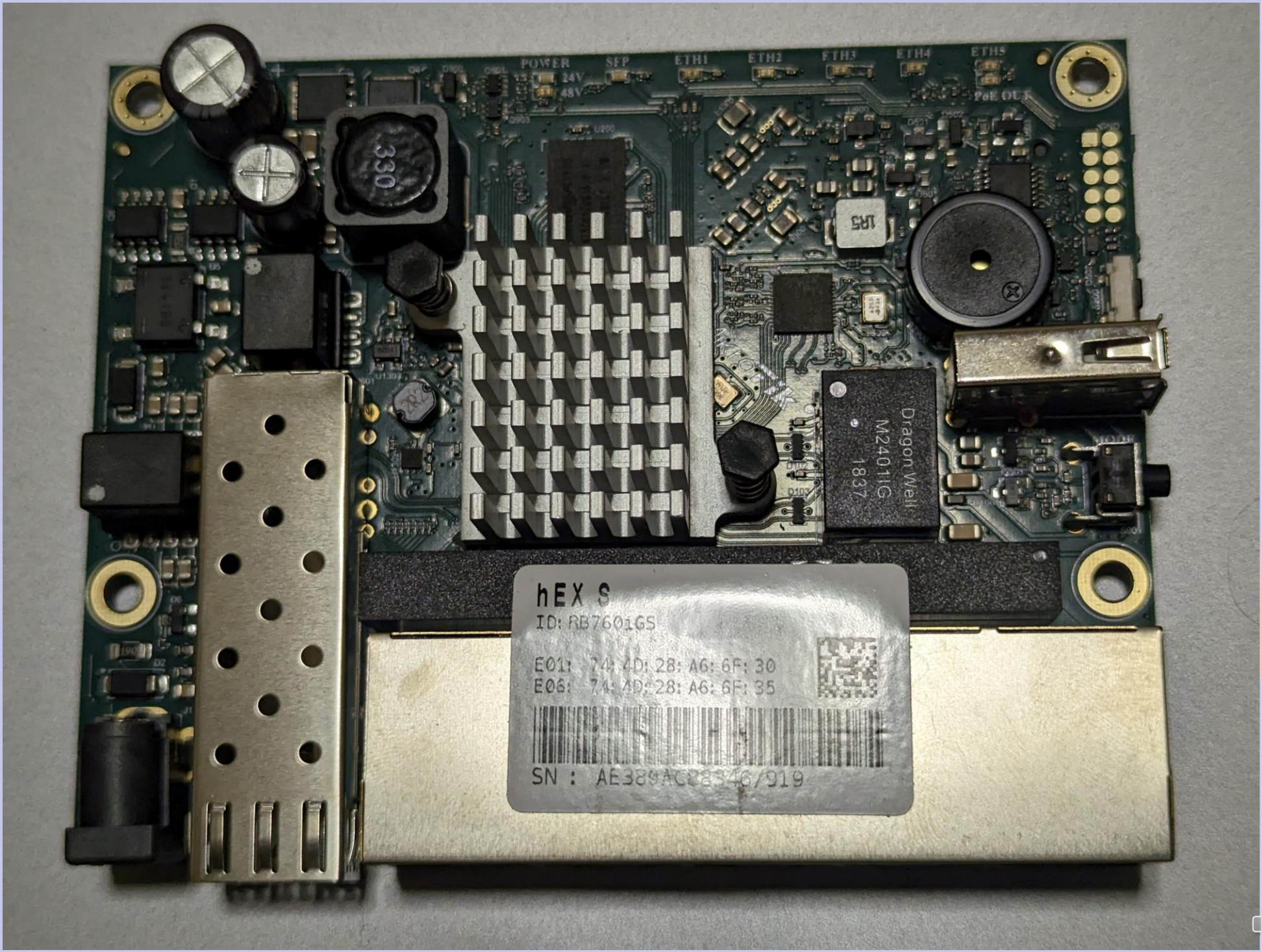
- That looks like a Mikrotik device
- Can we get a shell on it?
  - Don’t have the password
  - Do have permission to mess with it
    - I think they didn’t believe that I could break into it
- Don’t have the full config
- LLDP says the firmware is fully up to date (long term support)

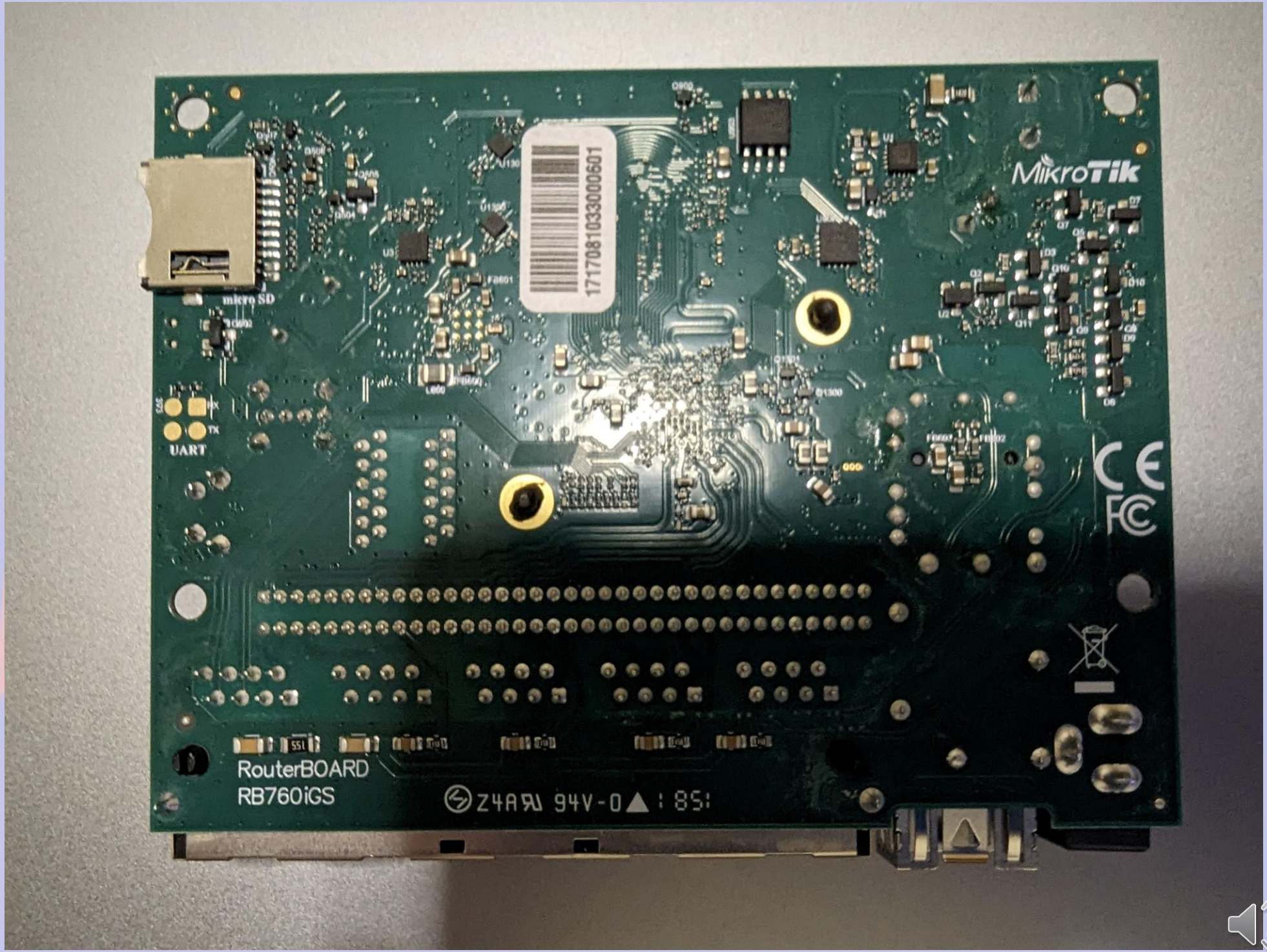
How about off the shelf exploits?

- Mikrotik has a debug shell if you can write a file to the filesystem
- https://github.com/BigNerd95/Chimay-Red works great, but our firmware is too new
- We could try to attack Winbox – there's some documentation for that and people seem to find lots of vulnerabilities
  - That sounds like work and we have physical access

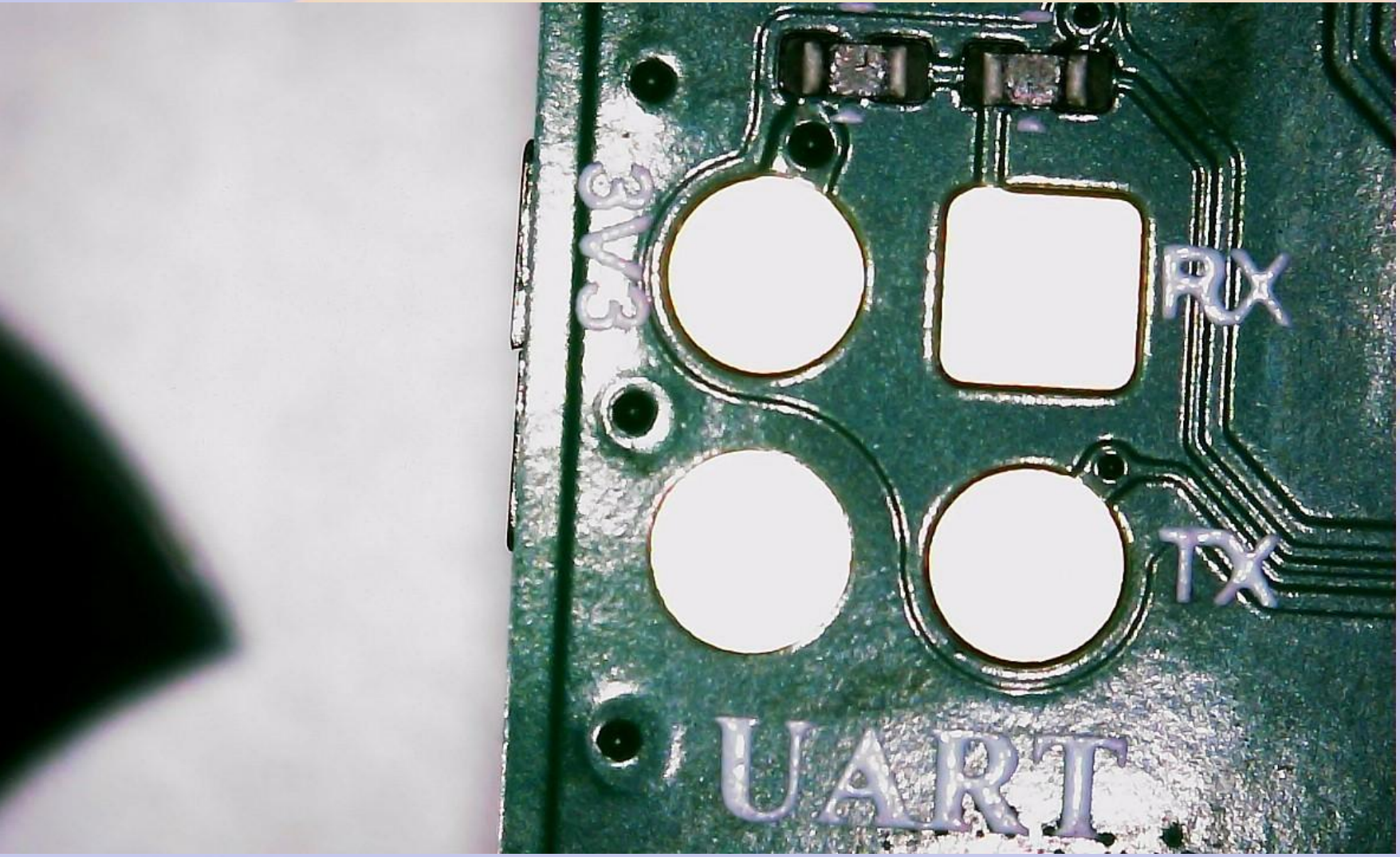
Physical Attack: JTAG

- Can we just overwrite some memory and let ourselves in?
- Can we find test points easily?
- Maybe?

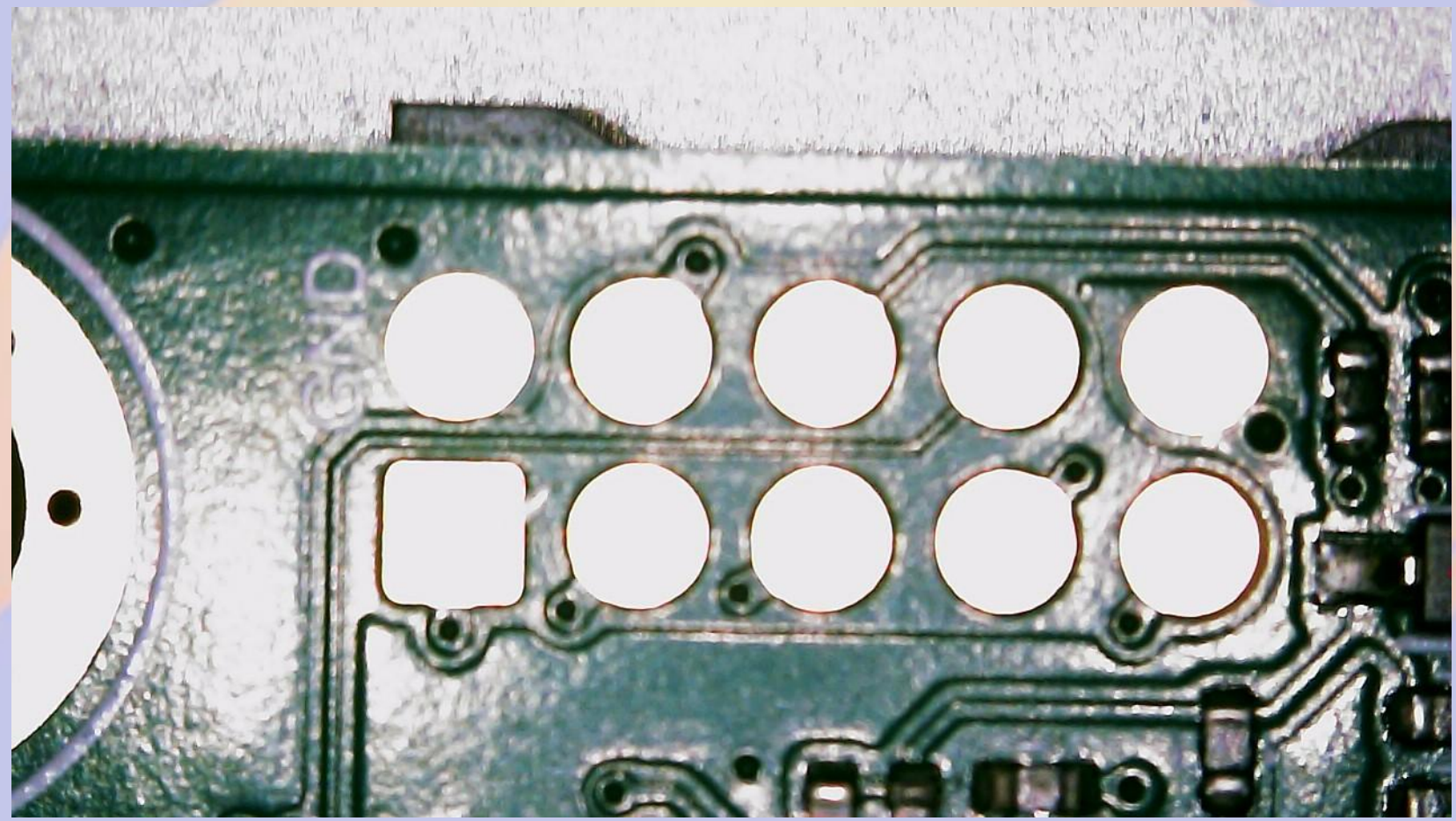

POWER
SFP
ETH1
ETH2
ETH3
ETH4
ETH5
24V
48V
PoE OUT
330
Dragon Well
M2401G
1837
hEX S
ID: RB760iGS
E01: 74:4D:28:A6:6F:30
E06: 74:4D:28:A6:6F:35
SN : AE389AC


MikroTik
micro SD
UART
RouterBOARD
RB760iGS
94V-0

Found a serial port!



JTAG maybe?



My Business Card says “Software” What else can we do?

- Can we boot to something else and copy the flash that way?
- Netinstall == PXE Boot?
- It’s just a Linux box, right?
- Seems a better first thing to try: soldering things isn’t exactly “subtle” if anything happens

Supported devices
Packages
Downloads
Documentation
Quick start guide
User guide
Developer guide
Security
FAQ
Forum
Contributing
Submitting patches
Reporting bugs
Contributing to wiki
Project
About OpenWrt
Rules
Infrastructure
Donate
Merchandise
Website
Trademark policy
License
Contacts

MikroTik RB760iGS (hEX S)

Table of Contents
MikroTik RB760iGS (hEX S)
Supported Versions
Hardware Highlights
Installation
Network configuration
PoE
SFP
Photos
PCB

Supported Versions

Brand	Model	Current Release	OEM Info	Forum Topic	Technical Data
MikroTik	RB760iGS (hEX S)	22.03.3	https://mikrotik.com/product/hex_s		View/Edit data

Hardware Highlights

Model	SoC	CPU MHz	Flash MB	RAM MB	WLAN Hardware	Gbit ports	Comments network ports	USB
RB760iGS (hEX S)	MediaTek MT7621A	880	16, microSD	256	-	5	1x SFP	1x 2.0

Installation

Model	Current Release	Firmware OpenWrt Install	Firmware OpenWrt Upgrade	Firmware OEM Stock
RB760iGS (hEX S)	22.03.3	https://downloads.openwrt.org/releases/22.03.3/targets/ramips/mt7621/openwrt-22.03.3-ramips-mt7621-	https://downloads.openwrt.org/releases/22.03.3/targets/ramips/mt7621/openwrt-22.03.3-ramips-mt7621-	https://mikrotik.com/product/hex_s

Demo Time!

- Live Demos are hard, so I recorded one
- (Recorded demos are hard too -- go easy on me)
- https://youtu.be/LlizkirclZY

That can’t be real, you got the password using just strings?

- I tried binwalk first
- I assumed I was going to have to add an account for myself because surely passwords are hashed
- Mikrotik is using a weird/old/deprecated filesystem that’s hard to work with
- Tried strings just for fun to see if I could find the hashes
- Found the plaintext
- Profit? ¯_(ツ)_/¯

Responsible Disclosure?

- Nah.. The NerdFest organizer wanted (required?) a talk and I'm busy
  - (and tired of yelling at incompetent IT companies for a living)
- The Mikrotik Security policy would seem to me to not want this sort of report anyway
  - They say that they don't accept issues due to configuration
- Did you really expect security from a $70 router anyway?

Wait… is having a password set misconfiguration?

- I’d argue yes, in 2023, yes.
- Physically prevent untrusted people from getting to the config interface
- Firewall untrusted people from the config interface
- Use public key crypto instead
- The untrusted device only knows your public key, which is useless to an attacker
- Note that RouterOS only supports some older cyphers for this – you might have to tweak your client ssh settings (ugh)

How is this relevant to RMHAM?

- Say you knew someone with a big network of Mikrotik gear
- Maybe they leave devices on remote mountain tops for anyone to touch mostly unsupervised (anyone with lockpicks or climbing gear?)
- Maybe they all have an administrative user with the same password
- Break into one, get them all!
- Sound familiar? Of course not ;-)
- [Snark aside, the RMHAM network is pretty great! Who'd want to break it? This is just something that could be possible]

Practical Security Advice

- Don’t use passwords
- Don’t use a single password for multiple things
- Use two factor authentication
- Prefer two part keys/certificates
- **Make sure “secure” hardware can’t be touched by untrusted people**

Questions?

ben@kc2vjw.com