Routers...

Household's sleeping evil

Zuzana Duračinská • **zuzana.duracinska@nic.cz** •
17.06.2016

CZ.NIC | CZ DOMAIN REGISTRY

- Internet domain registry operator
  - CcTLD **.CZ**

- National CSIRT in Czech Republic

- Established within academic environment as a part of research project (2007-2010)

- Work later formalized by memorandum(s) with Ministry of Interior and National Security Authority

- Since December 2015 public contract for indefinite duration

SCHOOL

LIBRARY

Come In We're OPEN

cz.nic | CZ DOMAIN REGISTRY
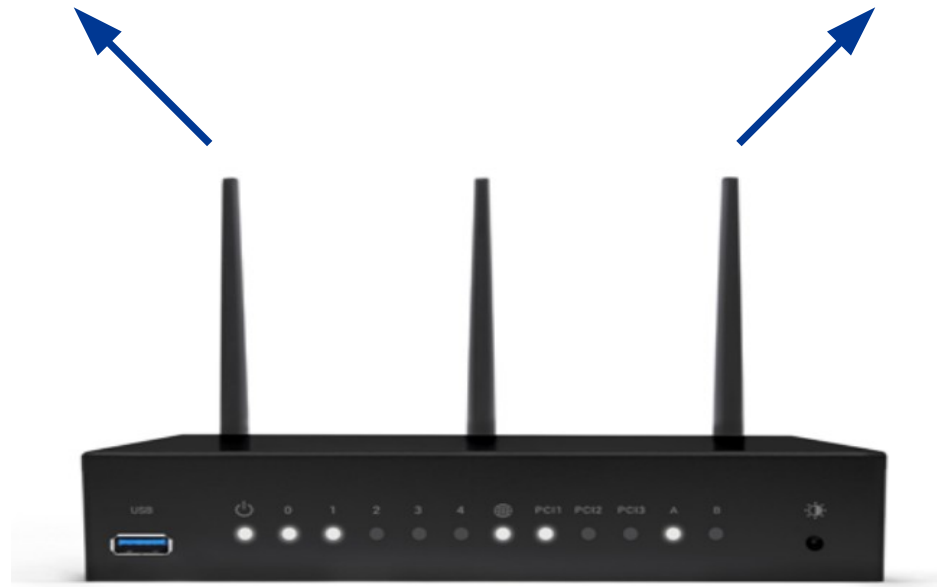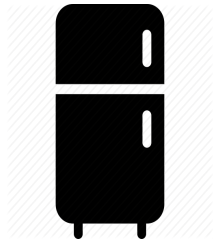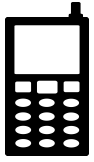
Regular End User

IT Specialist

Where to buy (get) a router?

- Internet Service Providers

- Electronics

- E-shops...

vs.

Where to get support?

Manufacturer…transport…supplier…transport…ISP…in stock…customer
=
xy months

CZ.NIC | CZ DOMAIN REGISTRY

Weaknesses

- Outdated SW
- Default passwords
- Remote administration
- UPnP on by default

Responsibility?

- Manufacturer
- ISP
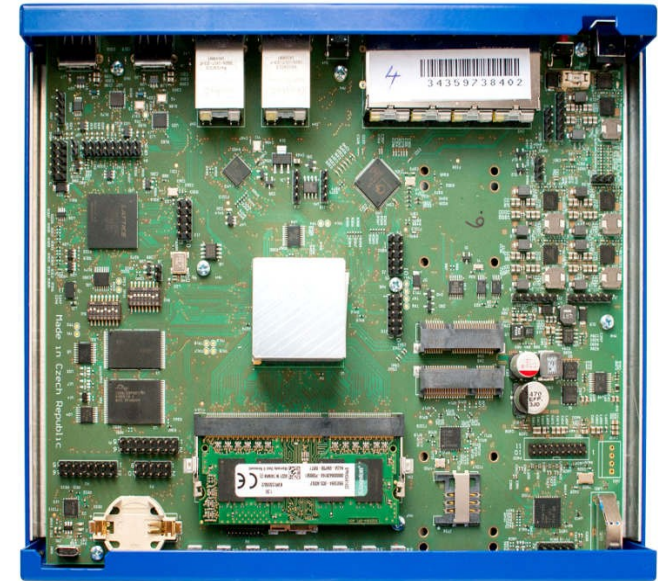- Sales companies
- Producers
- CSIRTs...?

**$$$ vs. performance vs. security
Secure by default???**

Turris

- Motivation: situation on the market

  of SOHO routers :(

- Open source (fork of OpenWRT)

- Open hardware

- Not-for-profit and **RESEARCH** project

- 2000 routers distributed in Czech republic

- Automated updates

- Strong demand especially from Czech IT community

- Assembled in Czech republic :)

Another added security value

- **Collection** of input data (most importantly monitoring of end devices)

- **Analysis** of obtained data on central server

- Preparation of **firewall rules** based on data analysis

- **Update** of end devices

- CSIRT.CZ feeds distributed adaptative firewall

- Provision of generated greylists as a feed to IntelMQ

https://youtu.be/3ATAFufg_pY

- **Enhanced** HW part
- Possibility to buy the Turris router
- Funding? - we have tried crowdfunding (to see wheather there would be an interest)

Honeypots

With Omnia, you can observe network attackers' activity from the safety of your home.

Cryptochip

10010
00101
110101

Not having enough entropy may be a security weakness. This is why we include an extra cryptochip.

Extensibility

There are many things you can use Omnia for besides connecting to the Internet.

mSATA

If you want extra fast storage in your Omnia, connect an SSD via the mSATA interface.

Additional features

4 GB flash

Turris Omnia has two orders of magnitude more flash memory than common routers.

RTC with battery backup

Missing time information may be a security problem when cryptography is involved.

Wi-Fi

Turris Omnia has dual band Wi-Fi with 802.11ac and 802.11b/g/n.

Dimmable RGB LEDs

LEDs are an important source of information in a router. But they might not be so nice at night.

	Regular router	Turris	Turris Omnia
CPU	500 MHz MIPS	2x1.2 GHz PowerPC	2x1.6 GHz ARM
RAM	32-64 MB	2 GB	1-2 GB
Storage	8 MB	256 MB	8 GB
Extension connectors	USB	USB, miniPCle, GPIO	USB, miniPCle, GPIO, mSATA
Internal network connection	LAN and WAN share the same line to the CPU	LAN and WAN are connected to the CPU using dedicated lines	LAN and WAN are connected to the CPU using dedicated lines
Power consumption	3-6 W	9 W	5 W
Firmware updates	NO	YES	YES

Article | Talk

List of highest funded crowdfunding projects

From Wikipedia, the free encyclopedia

101	Turris Omnia	Router	Indiegogo	Ongoing	$100,000	$1,116,258

=

People are interested in **powerful, open source, secure** routers with lifetime support they can trust :)

Conclusion...?

- Can we encourage routers manufactures to focus on routers security more?

- Can we talk to local ISPs about the routers they provide (sell) to their customers?

- Can CSIRTs do awareness activities on "routers in households"?

- What will be the role of routers in coming IoT age?

What kind of router would you buy your parents (or kids:) ?

@turris_cz