Project Turris


Ondřej Filip • 12 May 2014 • RIPE 68 • Warsaw
CZ.NIC, CZ.NIC Labs

- Domain name registry - .cz
  - 1.1M, 35% DNSSEC
- Project for local and global community

Knot DNS

BIRD
Project Turris - motivation

- Started in 2013 – project of shared cyberdefence
- Main goals
  - Security research
  - End user security
  - Improve the situation of SOHO routers
Project Turris - motivation

- Security research
  - Currently – Honeynet, DNS anomaly detection
  - Probes close to end users
  - Distributed in many networks
  - IP(v4/6) Anomaly detection
- End user security
  - Adaptive firewall based on collected data
  - Feed for CERT team (CSIRT.CZ)
Problems of current CPE devices

- SOHO routers
  - No or very bad support of IPv6
  - Problems with DNS, DNSSEC, no validation
  - No support for third party applications – app store
- Limited security features
- No automated software upgrades
- Current security issues
Data collection - probes

- Distribute 1000 probes - SOHO routers to end users for free (lease for 1 CZK/3Y = 0.03 EUR/3Y)
- Probe – powerful enough to forward 1Gbps of traffic with analysis – no HW found on the current market => HW development
- Additional features to increase value for end users
Router Turris

- Developed from scratch
- 1000 pcs – produced in Czech Republic
  - Freescale 1.2 GHz dual core (PPC)
  - 2 GB DDR memory – slot
  - 256 MB NAND + 16 MB NOR flash
  - 5x LAN – 1 Gbps ports (Ethernet switch with 7 ports - 2 Gbps lines to CPU)
  - 1x WAN – 1 Gbps port (directly to CPU)
Router Turris

- 2x miniPCIe (1 occupied by WiFi)
- WiFi 802.11 a/b/g/n – 3x3 MIMO
- 2x USB 2.0
- UART, SPI, I2C, GPIO
- Free microSHDC slot
- Low power consumption – 9-14 W
- Open source license
Router Turris
Router Turris
Router Turris – killer feature

- LED brightness intensity tunable (!)
  - Software managed (RGB)
  - Button at the back
- :-D
Router Turris - software

- Based on OpenWRT – open source
- Own configuration wizard – based on NETCONF
- Automatic updates – user can avoid certain time periods
- Encrypted communication with central server
- Data collector – only mandatory process
- IPv6, DNSSEC, passwords, ...
- Android application
Router Turris - usage

- Network testing
  - Reachability tests (ping, RTT)
  - Protocol specific
  - Speed measurement
- Other research - planned
  - Discussion with universities, security researchers (agreement limits)
Data collection

- μCollect
  - Basic stats, PCAP stats, anomaly detection
- Firewall logs
- Router logs - upgrade status, SW problems
- Other measures – temperature, load, memory and flash utilization etc.
Data collection - μCollect

- Modular system for data collection and reporting
- Module "count" – TCP/UDP/.. stats - displayed on portal
- Modules “buckets“ - IP anomaly detection
  - Hashed by multiple functions
  - Central server tries to find anomaly
- Send – secure way – crypto HW – into central repository
Data collection - μCollect

109.202.66.4:1194
[fe80::221:5aff:fe94:3818]:546
78.99.191.23:51621
81.201.52.105:1194
78.45.116.59:23608
95.102.219.237:39684
[2001:1488:ac15:ff70::88]:443
77.48.112.9:57298
89.221.210.10:1935
Other
Data collection - μCollect
# Data collection - μCCollect

<table>
<thead>
<tr>
<th>ID</th>
<th>Date</th>
<th>A</th>
<th>A</th>
<th>A</th>
<th>A</th>
<th>A</th>
<th>A</th>
<th>A</th>
<th>A</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000006500001AF3</td>
<td>2014-05-07</td>
<td>7%</td>
<td>7%</td>
<td>7%</td>
<td>7%</td>
<td>7%</td>
<td>7%</td>
<td>7%</td>
<td>7%</td>
<td>7%</td>
</tr>
<tr>
<td>000000050000019DF</td>
<td>2014-05-30</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
</tr>
<tr>
<td>0000000500000C346</td>
<td>2014-05-04</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
<td>70%</td>
</tr>
<tr>
<td>0000000600000E72</td>
<td>2014-05-14</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
</tr>
<tr>
<td>00000005000001CG9</td>
<td>2014-05-07</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
</tr>
<tr>
<td>00000005000001A38</td>
<td>2014-05-07</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
<td>80%</td>
</tr>
</tbody>
</table>
End user portal

- Communication with users
- Graphs
- Tutorials
- End user forum – very active
End user portal

Statistics - IPv4 vs. IPv6 (size)

- IPv4 (12.41 GB - 80.23 %)
- IPv6 (8.19 GB - 39.77 %)
End user portal

Logged firewall packets - Target port

<table>
<thead>
<tr>
<th>Port</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>5678</td>
<td>5678</td>
<td>42,846 - 71.81%</td>
</tr>
<tr>
<td>8080</td>
<td>8080</td>
<td>3,701 - 6.20%</td>
</tr>
<tr>
<td>1433</td>
<td>1433</td>
<td>2,308 - 3.87%</td>
</tr>
<tr>
<td>22</td>
<td>22</td>
<td>1,781 - 2.98%</td>
</tr>
<tr>
<td>23</td>
<td>23</td>
<td>898 - 1.51%</td>
</tr>
<tr>
<td>64153</td>
<td>64153</td>
<td>492 - 0.82%</td>
</tr>
<tr>
<td>80</td>
<td>80</td>
<td>466 - 0.78%</td>
</tr>
<tr>
<td>3306</td>
<td>3306</td>
<td>440 - 0.74%</td>
</tr>
<tr>
<td>5060</td>
<td>5060</td>
<td>434 - 0.73%</td>
</tr>
<tr>
<td>3389</td>
<td>3389</td>
<td>405 - 0.68%</td>
</tr>
<tr>
<td>15701</td>
<td>15701</td>
<td>387 - 0.65%</td>
</tr>
<tr>
<td>5000</td>
<td>5000</td>
<td>336 - 0.56%</td>
</tr>
<tr>
<td>53</td>
<td>53</td>
<td>281 - 0.47%</td>
</tr>
<tr>
<td>1080</td>
<td>1080</td>
<td>248 - 0.42%</td>
</tr>
<tr>
<td>443</td>
<td>443</td>
<td>232 - 0.39%</td>
</tr>
<tr>
<td>6996</td>
<td>6996</td>
<td>201 - 0.34%</td>
</tr>
<tr>
<td>67</td>
<td>67</td>
<td>197 - 0.33%</td>
</tr>
<tr>
<td>25</td>
<td>25</td>
<td>184 - 0.31%</td>
</tr>
<tr>
<td>5900</td>
<td>5900</td>
<td>162 - 0.27%</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td>(3,668 - 6.15%)</td>
</tr>
</tbody>
</table>
End user agreement

- Leasing, 3Ys + selling off
- Main router connecting to the Internet
- No switch off – non stop operation
- Open access – SSH + root
- Free modification except data collection and communication with central servers
Privacy issues

- Agreement
- Separate DB for account an data
- ISO27001
- Consulted with personal data protection authority
- POSITIVE Big Brother Awards CZ 2013
- Open Source
- Packet headers, data retention
Status

- 55% distributed to end users (>4000 requests)
- Distributing about 100 per week
- OS improvements – small incremental updates and one larger (OS version 1.1)
- Central portal improvements
- Tutorials – Turris as NAS, DLNA, VPN concentrator, multi WAN setup, 3G backup, VLAN setup, ...
Status

- Improving detection methods – calibration of the sensors
- Some IP scanners detected – portscanners, NTP, DNS scanners
- Checking flows to well known botnet C&Cs
- Publishing grey and black list
- Filtering some IPs based on CSIRT.CZ information
Future

- Another batch of 800 routers this year
- VDSL interface – small dongle
- SW improvements – OS + collection
- Universal OS for SOHO routers
  - Market
- Sweet to the end users – HW upgrades, tutorials – e.g. camera, smart home
Thank You!

Ondřej Filip  •  ondrej.filip@nic.cz  •  http://www.turris.cz