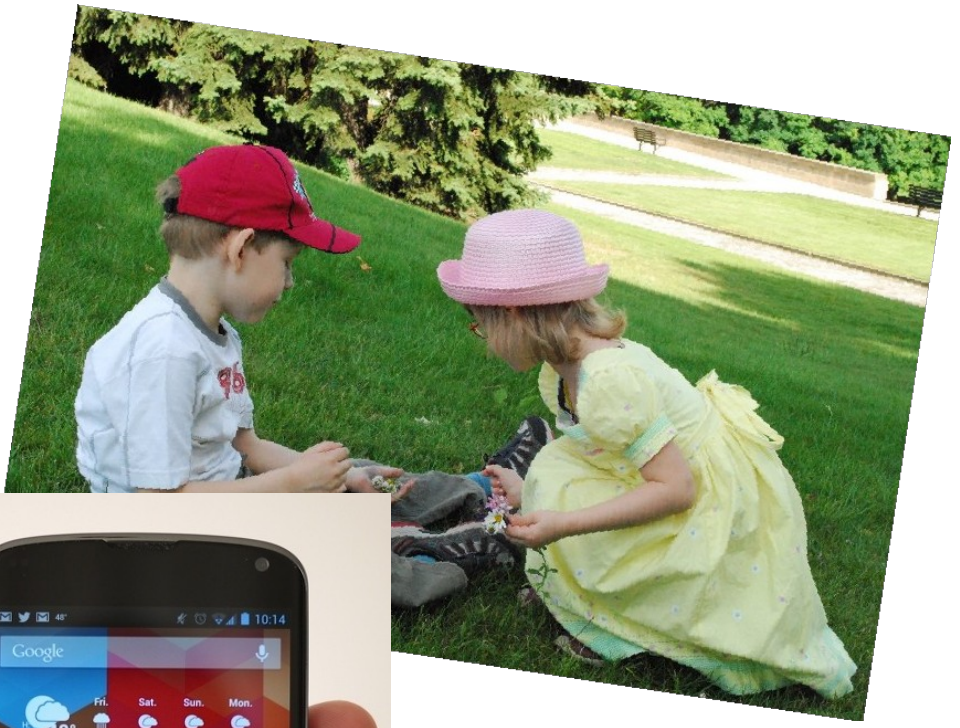
Bezpečný router pro domácí uživatele

Bedřich Košata • bedrich.kosata@nic.cz • 21.05.2013




10:14
Google
Fri.
Sat.
Sun.
Mon.
48°
40°/55°
39°/55°
36°/49°
35°/48°
Play Store
Calendar
Games
Camera
Media
Social
Maps
Settings
Voice
People
Twitter
Google

Je tu co vylepšovat?

- Bezpečnost
  - router je brána mezi poklidnou domácí sítí a divokým internetem
- Moderní technologie
  - podpora IPv6 stále není běžná (http://katalogrouteru.cz/)
  - DNSSEC validace není dostupná snad u žádného výrobce
- Výkon
  - málokterý router zvládne „uroutovat“ 500 Mb/s, výkon výrazně padá s počtem firewallových pravidel, NATováním, apt.
- Dopňkové funkce
  - router typicky běží v provozu 24/7 - ideální místo pro NAS, monitorovací server, atp.

Bezpečnost

- u mnoha domácích routerů je prvotní zapojení zároveň poslední operací s ním
  - bezpečnostní záplaty pomocí updatu firmware mají velké zpoždění
  - často zůstává výchozí heslo pro administrátora (v některých případech i pro přístup z vnějšku sítě)*
- je třeba aktivnější přístup k updatům
  - nelze jej očekávat od uživatelů
  - musí to být vestavěná funkce routeru

* http://census2012.sourceforge.net/paper.html

Aktivní bezpečnost

- co udělá uživatel, když zjistí, že se mu do sítě někdo naboural?
  - Google, Facebook, přátelé, fóra - získávání a výměna informací, hledání lidí se stejným zařízením a/nebo problémem
- proč si nevyměňovat bezpečnostní informace **před** napadením a nechránit tak sebe i ostatní?

Ideální router

- operační systém se schopností automatických updatů
- moderní technologie vestavěné do systému
  - IPv6 včetně přechodových mechanismů, plnohodnotného firewallu, atp.
  - DNSSEC validující resolver jako výchozí volba
- přívětivé a moderní uživatelské rozhraní
- aktivní ochrana uživatelů před bezpečnostními hrozbami
- hardware adekvátní nabízeným funkcím

=> „CZ.NIC router“

CZ.NIC router - operační systém

- Linuxový systém s podporou pro omezené prostředky zařízení
- **OpenWrt**
  - populární alternativní operační systém pro domácí routery
  - obsahuje všechno co potřebujeme (balíčkovací systém, uživatelské rozhraní, podporu IPv6,...)
  - silná uživatelská komunita

=> **využijeme OpenWrt a doplníme do něj, co chybí**

CZ.NIC router - programové vybavení

- IPv6
  - závisí na způsobu sestavení firmware
- DNSSEC
  - není ve výchozím nastavení podporován
  - přizpůsobili jsme balíček resolveru Unbound pro OpenWrt
- uživatelské rozhraní
  - je obsaženo základní webové rozhraní
  - pracujeme na jednotném konfiguračním rozhraní, které umožní přístup z různých „front-endů“

CZ.NIC router - bezpečnost

- Pasivní bezpečnost
  - automatické bezpečnostní updaty
- Aktivní bezpečnost
  - využití celé sítě zapojených routerů pro monitoring
  - centrální vyhodnocení možných hrozeb a útoků
  - přizpůsobení pravidel firewallu detekovaným útokům => **distribuovaný adaptivní firewall**

CZ.NIC router - adaptivní firewall

- Zdroje informací pro firewall
  - monitoring nevyžádaných pokusů o spojení z vnějšku sítě pomocí firewallu
  - detekce anomálií v síťovém provozu pomocí statistických metod (nyní využíváme v DNS monitoringu)
  - vnější zdroje - např. informace o chování a šíření malware ve spolupráci CSIRT.CZ
- Pravidla budou vytvářena odborníky na základě analýzy získaných dat
- V budoucnu automatické vytváření pravidel s dohledovou funkcí odborníka

CZ.NIC router - hardware

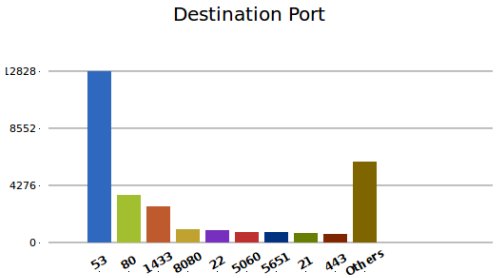
- vlastní hardware
- návrh bude uvolněn pod open-source licencí
- dostatečný výkon na plný Gbit provoz + bezpečnostní analýzu:
  - procesor Freescale P2020 (2 jádra, PPC, 800-1200 MHz)
  - SO-DIMM slot na DDR3 paměť
  - 5x Gbit port
  - WiFi 802.11n
- možnosti rozšíření:
  - 1x miniPCIe (druhý obsazen WiFi kartou) - VDSL karta, záložní 3G připojení, ...
  - 2x USB 2.0 - tiskárna, sdílený disk, kamera, ...
  - GPIO, SPI a další sběrnice vyvedeny do „pinheaderu“ - čidla teploty, tlaku, rosného bodu, ...

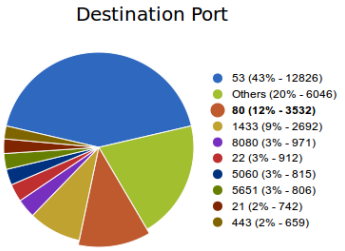
CZ.NIC router - plán na rok 2013

- vyrobit sérii 1000 ks „CZ.NIC routeru“
- připravit operační systém pro bezpečné a komfortní použití
- vytvořit programové vybavení a infrastrukturu pro distribuovaný adaptivní firewall
- nabídnout „CZ.NIC router“ testovací skupině uživatelů
- vytvořit tak síť „monitorovacích stanic“ pro sběr bezpečnostních dat

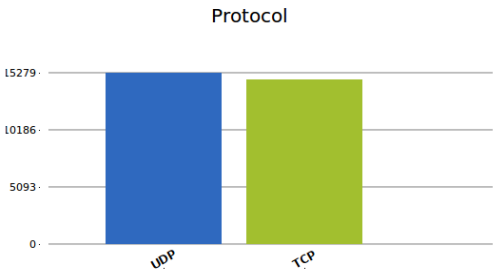
CZ.NIC router - ukázky

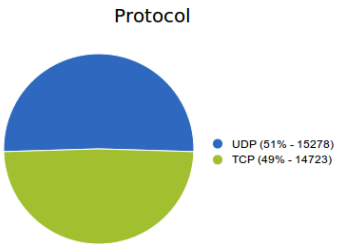
- v testovacím provozu sbíráme data z firewallu a detektoru anomálií z několika testovacích zařízení





Destination Port	Count	First Occurence	Last Occurence
53	12826	2013-03-11 07:14:37	2013-05-08 12:06:16
80	3532	2013-03-11 07:13:27	2013-05-02 09:29:06
1433	2692	2013-03-11 07:37:10	2013-05-09 13:17:50
8080	971	2013-03-11 07:17:48	2013-05-09 12:54:12
22	912	2013-03-11 13:02:39	2013-05-09 12:01:51
5060	815	2013-03-11 08:03:37	2013-05-09 10:49:28
5651	806	2013-03-11 14:22:37	2013-05-09 13:14:48
21	742	2013-03-12 10:10:54	2013-05-09 04:52:54
443	659	2013-03-15 13:53:31	2013-03-15 14:10:42
Others	6046	2013-03-11 07:14:12	2013-05-13 15:38:42

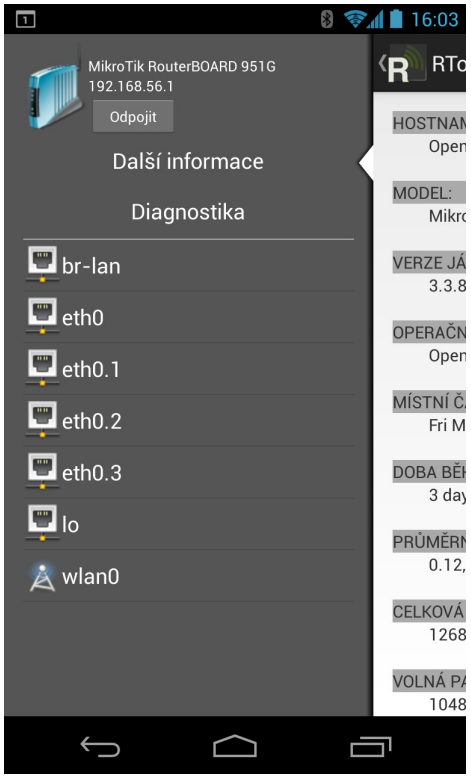


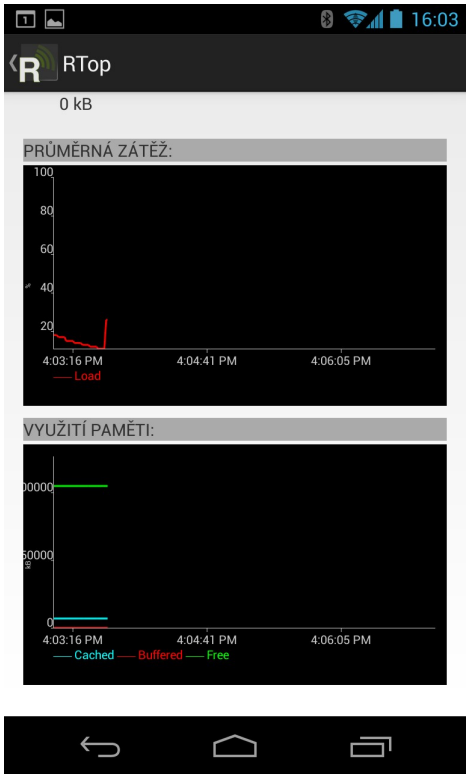


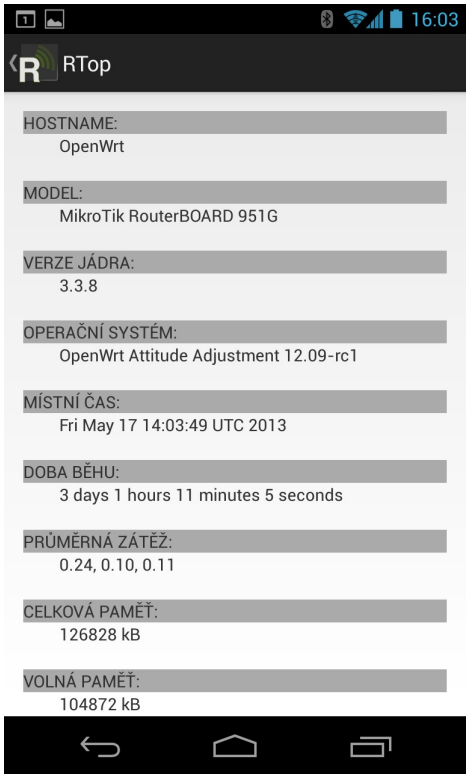
Protocol	Count	First Occurence	Last Occurence
UDP	15278	2013-03-11 07:14:37	2013-05-13 15:38:42
TCP	14723	2013-03-11 07:13:27	2013-05-09 13:17:50

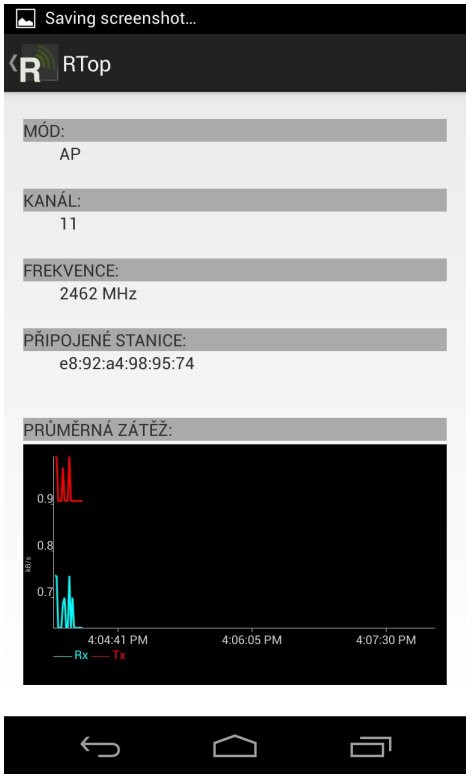
CZ.NIC router - ukázky

- vyvíjíme prototyp aplikace pro monitoring routeru pomocí mobilního telefonu









Vývojový tým

Martin Strbačka

Michal Vaner

Tomáš Rykl

Štěpán Henek

Robin Obůrka

Zbyněk Kos

Bedřich Košata

Děkuji za pozornost

Bedřich Košata • bedrich.kosata@nic.cz