Projekt Turris

PROJECT:
TURRIS

Proč a jak?

Ondřej Filip • ondrej.filip@nic.cz
Bedřich Košata • bedrich.kosata@nic.cz
30.11.2013 / IT13.2

CZ.NIC | SPRÁVCE DOMÉNY CZ

CZ.NIC & bezpečnost

- Jedno z hlavních témat
  - DNSSEC, DANE
  - CSIRT.CZ – CZ.NIC-CSIRT
  - Honeynet
  - Malicious Domain Manager
  - Generátor DOS útoků
  - Skener webu

Analýza dat

- Dobré znalosti o útocích díky Honeynetu
- Analýza anomálií v DNS provozu
  - Sledování webcrowleru, spamu, testy volných domén, …
- Žádné znalosti o tocích na okraji sítě, u koncových uživatelů

Stav SOHO routerů

- **Žalostný!**
- Mizerná podpora IPv6
- Časté chyby z implementaci DNS
- Nulová podpora DNSSEC
- Nemožnosti nahrávání vlastních aplikací
- Žádná ochrana při přetížení linky (RED)
- Téměř žádné bezpečnostní funkce
- UPGRADE

Projekt Turris

- Bezpečnostní výzkum
  - Toky u uživatelů
  - Hledání anomálií
- Zlepšení situace u SOHO routerů
  - IPv6, DNSSEC, …
- Bezpečnost koncových uživatelů
  - Publikace firewallových pravidel
  - Podklady pro CSIRT.CZ

Router Turris

- Prostředek, nikoliv cíl!
- Sonda, router, fileserver, printserver, …
- Žádný takový výkonný HW na trhu nebyl
  - Výkon CPU – 1Gbps + analýza
  - Rozměry
  - Porty
- Vše open source

Filipika proti Misoturrisům

- Je to dobrovolné
- Je to open source
- Jasná smlouva
- Nesbíráme více než antivirus, …
- Uvidíte, co sbíráme
- Jasná retenční politika
- Žádný obchodní zájem
- Transparentní český subjekt

Jak na to? Co potřebujeme?

- **Hardware** - koupíme, upravíme a nebo vytvoříme vlastní
- **Operační systém** - vezmeme OpenWrt, doupravíme
- **Bezpečnostní vybavení** - použijeme existující a upravíme nebo napíšeme
- **Analýza síťových anomálií** - musíme napsat
- **Moderní rozhraní** - napíšeme vlastní
- **Vývojový tým** - něco máme, zbytek přijmeme

Vlastní hardware - ano či ne?

- Proti
  - Výrazné zvýšení náročnosti projektu
  - Vyšší cena
- Pro
  - Řešení na míru
  - Optimalizace výkonu
  - Možnost implementace vlastních nápadů

- Zvítězila těžší ale zajímavější varianta

Open hardware made in Czech Republic

hardware

- Výroba v ČR
- Veškerá dokumentace je dostupná ke stažení
  - Zdrojová data pro Altium Designer
  - Schéma zapojení
  - Návrh desky
  - 3D model osazené desky

Vyplatil se vývoj vlastního hardware?

- Nemusíme dělat technologické kompromisy v software
  - 4x rychlejší procesor
  - 16x více RAM
  - 16x větší flash úložiště
- Projekt je zajímavější pro veřejnost
- Skryté benefity
  - Spousta zkušeností s low-level fungováním hardware
  - Další nástroj ve vývojovém arzenálu

Operační systém a jeho zabezpečení

- OpenWrt je optimalizované na routery
- Obsahuje některé kompromisy kvůli parametrům hardware
- K zabezpečení je nutné především bezpečné nastavení (a to i ve výchozím stavu zařízení)
- V některých oblastech je nutné změnit výchozí programové vybavení, případně upravit balíčky (DNSSEC, openssh, atp.)
- Automatické aktualizace jsou základem dlouhodobé bezpečnosti

Analýza síťových anomálií

- Založena na předchozích zkušenostech se statistickou analýzou DNS provozu
- Vytvořeno vlastní řešení - ucollect
- Příprava na budoucí potřebu analýzu rozšiřovat
  - systém zásuvných modulů

Ochrana uživatelských dat

anomálie

- Technologická
  - sbírat minimum citlivých dat
  - ze zařízení jich přenášet ještě méně
  - pokud ukládat, tak po omezenou dobu
  - dlouhodobě neukládat nic citlivého
  - pečlivě navrhovat a spravovat systémy pro práci s daty
- Právní
  - nájemní smlouva specifikuje, co smíme a nesmíme sbírat a dělat

Uživatelské rozhraní

- Nevymýšlet kolo - existuje rozhraní Luci
- Neomezovat rozhraní na webový prohlížeč
- Rozdělení konfigurace na části klient a server
  - Server mohou využívat klienti z různých platforem
- Využití protokolu netconf
  - Standardizované řešení
  - Příspěvek do OpenWrt

Uživatelské rozhraní

PROJECT:TURRIS 6 / 7

Wi-Fi

Pokud chcete používat tento router pro připojování dalších Wi-Fi zařízení k internetu, povolte v následujícím formuláři Wi-Fi a zvolte si SSID (název přístupového bodu) a příslušné heslo.

Mobilní zařízení můžete jednoduše nastavit načtením QR kódu zobrazeného vedle formuláře.

Povolit Wi-Fi	☑
SSID	Turris
Skrýt SSID	☐ ?
Režim Wi-Fi	◉ 2.4 GHz ○ 5 GHz
Kanál	7
WiFi Heslo	●●●●●●●●●●●●●●●●●●●●●●●●●●●● ?

Další

Vývojový tým

- Na začátku roku 3
- Nyní 9 členů
  - Hardware – 2
  - Operační systém a spol. – 2
  - Anomálie, nuci, atp. – 2
  - Webové stránky, UI – 2
  - Management (holka pro všechno) – 1
- Pomáhají kolegové z jiných týmů

Aktuální stav projektu

- Testujeme poslední prototypy routeru
- Ladíme OS a programové vybavení
- Testujeme v ostrém provozu detekci anomálií
- Spustili jsme výrobu 1000 ks routeru Turris - k dispozici budou na přelomu roku
- Máme cca 2500 předregistrovaných
- Plánujeme distribuci

Jak se zapojit

PROJECT: TURRIS

- Předregistrace na https://www.turris.cz/
- V okamžiku dostupnosti routerů Vás upozorníme na zaregistrovaný email
- Vyplnění smlouvy online (mojeID výhodou)
- Za symbolickou 1 Kč dostanete router k dlouhodobému pronájmu (za podmínek smlouvy)

Jaké jsou podmínky účasti

- Využívat router jako hlavní přípojný bod k internetu
- Nezasahovat do sběru bezpečnostních dat
- Nezasahovat do aktualizací zařízení
- Uživatel má právo kdykoli od smlouvy odstoupit a zařízení vrátit
- Uživatel může cokoli instalovat a měnit

Plány do budoucna

- Sběr, analýza a publikace dat o detekovaných anomáliích
- Další vývoj celé platformy
  - Ladění a vylepšování OS
  - Vylepšování detekce síťových anomálií
  - Nové analýzy - rychlost sítě, dostupnost, atp.
  - Vylepšování vzdálené správy a administrace routeru
  - Vývoj směrem k univerzálnímu OS pro domácí routery
- Podle ohlasu případně rozšíření hardware

Spousta dotazů
Děkujeme za pozornost!

http://www.turris.cz

Ondřej Filip • ondrej.filip@nic.cz
Bedřich Košata • bedrich.kosata@nic.cz

CZ.NIC | SPRÁVCE DOMÉNY CZ

Proč Turris?

- Turris = věž