Project Turris

http://www.turris.cz/en

Zuzana Duracinska
• zuzana.duracinska@nic.cz
• TF-CSIRT
• Rome
What is Turris? Why its logo looks like “microphone”? Why to design and make another router? What is shared cyber defense? How can CSIRT team be involved?
Turris

Latin word for tower Developed from scratch by CZ.NICService helping to protect a user's home network Not-for-profit research project
End user security:
Adaptive firewall based on collected data
Regular updates

Security research
Probes close to end users
Distribution in different networks
Anomaly detection
Turris...(more than a research project)

SOHO routers

Bad support of IPv6, DNSSEC

Many problems with DNS

Limited security features

Measurements

IPv6 DNSSEC
Can we design a SOHO router?

Yes, we can (and it's working)
Hardware
Software
Security
Privacy

PROJECT: TURRIS
Turris...hardware

Wifi 802.11 a/b/g/n – 3x3 MIMO 2x USB 2.0 UART, SPI, I2C, GPIO Free microSD HC slot ATSHA204 – crypto chip Low power consumption Open source - CERN Open HW License
Freescale PPC 1.2GHz dual core2GB DDR memory – slot256MB NAND + 16MB NOR flash5x LAN Gbps ports (2Gbps to CPU)1x WAN Gbps port (directly to CPU)2x miniPCIe (1 occupied by wifi)
Open source – based on OpenWRT
Own configuration wizard – based on NETCONF
Automatic updates
Crypted communication with central server
Turris...software

IPv6, DNSSECData collection- firewall logs- router logs (SW problems)- anomaly detection- modular system for data collection and reporting- real time network traffic monitoring (framework called uCollect)
Turris...privacy

Agreement with end users
Separate DB for accounts and data
ISO 27001
Consulted with personal data protection authority
POSITIVE
Big Brother Awards CZ 2013
Focus on a security of a home network

1. Collection of input data (from end users devices)
2. Analysis of data on central server
3. Preparation of firewall rules
4. Update of end devices

Automatic updates
Distributed adaptive firewall

Turris...security
Turris... the point when CSIRT.CZ comes in

Data, data, data... Help with data analysis Usage of other data sources to update firewall rules Help with firewall updates
Distribution to end users?
Turris

Approx. 4000 requests
Leasing 3Ys + selling off
Leasing for 1 crown (0,04 EUR)
User selection based on provider and location (to ensure diversity)
Main router connecting to the Internet
Non-stop operation
Future plans

Batch of 800 improved routers coming out at the end of the year...Software improvementsMobile apps using the netconf interfaceMake firewall rules available for other platformsExtend the OS to more routers