Bezpečnost počítačových sítí v oblasti provozu inteligentníich budov

DTEDI – Příprava tezí disertační práce

Mgr. Radek Krejčí

Fakulta informatiky
Masarykova univerzita
radek.krejci@mail.muni.cz

Brno, 18. litopadu 2010

Obsah

Úvod

vymezení problematiky

Systémy inteligentních budov

- soustava propojených systémů reagujících na potřeby obyvatel za účelem zvýšení jejich pohodlí, bezpečí a snížení nákladů na provoz
- modulární systém s centrálním řízením
- možné součásti:
  - energetický systém, osvětlení, zábavní systém, komunikační systém, bezpečnostní systém, ...
- sítě:
  - senzorová síť, datová síť, audio/video rozvody

Inteligentní dům se sice stará o zabezpečení domácnosti, ale bezpečnost samotného systému je řešena pouze na úrovni fyzické bezpečnosti.

Hrozby počítačových sítí v systémech inteligentních budov

nikdo neví, co se v síti vlastně děje

- problém hlavně u obytných budov
- u průmyslových budov je problém posunut do samostatných senzorových sítí – datová síť bývá kontrolována

syndrom black-boxu

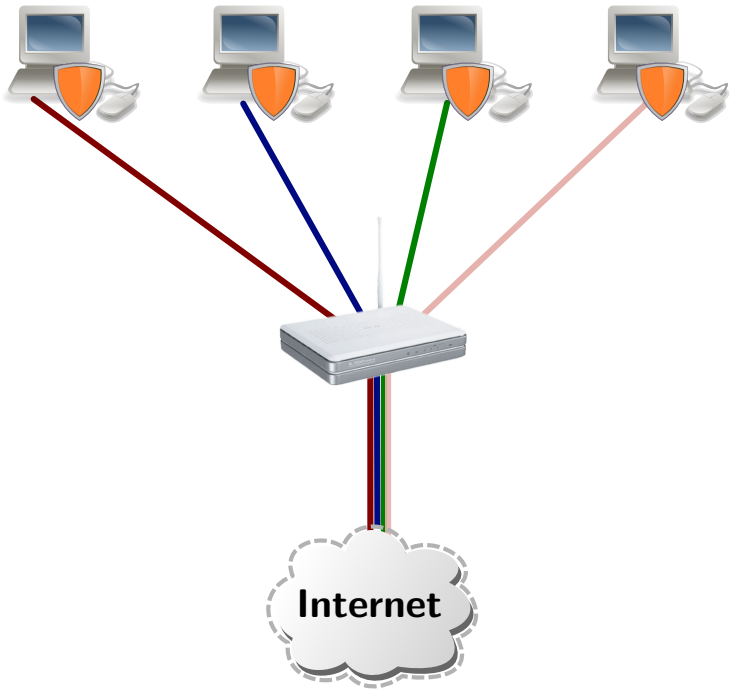
- zařízení mají podobu krabiček, o které se zdánlivě není třeba starat
- vlastnosti sítě včetně bezpečnosti dány výchozím nastavením výrobce jednotlivých zařízení

- bezpečnost je řešena pouze na úrovni fyzické bezpečnosti
- výhodné vlastnosti pro útočníka – narozdíl od běžných PC jsou tato zařízení neustále v provozu

Hrozby počítačových sítí v systémech inteligentních budov

Neviditelný malware

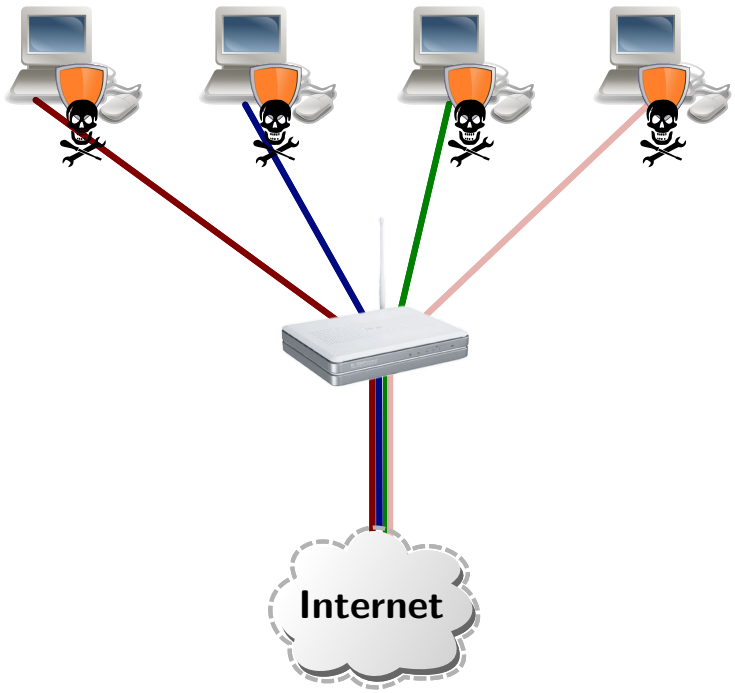
- neútočí se přímo na koncové stanice



Hrozby počítačových sítí v systémech inteligentních budov

Neviditelný malware

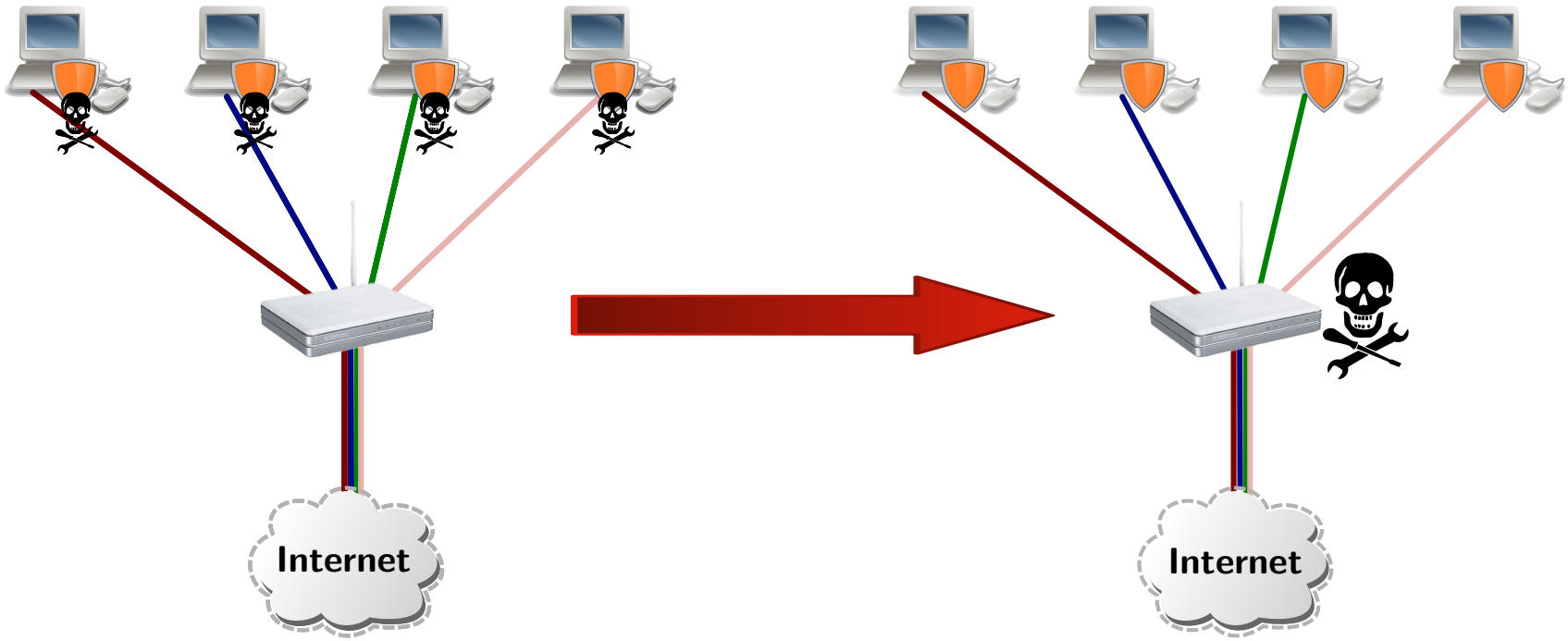
- neútočí se přímo na koncové stanice



Hrozby počítačových sítí v systémech inteligentních budov

Neviditelný malware

- neútočí se přímo na koncové stanice
- útočí se přímo na infrastrukturu



Hrozby počítačových sítí v systémech inteligentních budov

MITM útoky

- odposlech veškeré komunikace
- DNS spoofing
- útoky na HTTPS spojení
- transparentní proxy (SSL Strip)

$\rightarrow$

- krádeže citlivých informací
- zneužití výpočetních zdrojů
- právní důsledky
- ekonomické ztráty

State of the Art

současný stav řešené problematiky

Přístupy k bezpečnosti

- **ISP** – bezpečnost sítě, ochrana infrastruktury ISP (firewally, IDS/IPS systémy, monitoring sítě, . . .)
- **uživatel** – až na koncovém PC (firewall, anti* řešení, . . .)
- **průmyslové systémy** – často se bezpečnost neřeší, protože (zdánlivě) neexistuje připojení k vnější síti

Přístupy k bezpečnosti

- **ISP** – bezpečnost sítě, ochrana infrastruktury ISP (firewally, IDS/IPS systémy, monitoring sítě, . . .)
- **uživatel** – až na koncovém PC (firewall, anti* řešení, . . .)
- **průmyslové systémy** – často se bezpečnost neřeší, protože (zdánlivě) neexistuje připojení k vnější síti

Infrastruktura sítě uživatele zůstává územím nikoho.

Detekce hrozeb

host based

- firewally, anti* řešení
- většinou pattern-matching, heuristiky ($\rightarrow$ deep packet inspection)
- vychází pouze z lokálních informací a mají velkou nevýhodu u zero-day útoků a u škodlivého kódu měnícího svou signaturu

network-based

- z části opět deep packet inspection
- větší důraz na celkový pohled na síť – behaviorální analýza
  - detekce hrozeb na základě (odlišností v) chování sítě a síťových prvků
  - nebezpečí chybného učení
  - využití statistických modelů chování

Behaviorální analýza sítě – sběr informací o tocích

Moderní trend při řešení bezpečnosti (rozsáhlých) počítačových sítí.

IP tok – proud IP paketů se shodnými klíčovými charakteristikami

- informace o tom, **kdo**, **s kým**, **jak**, **kdy**, **jak moc** a **jak dlouho** komunikuje
- pětice zdrojová a cílová IP adresa, zdrojový a cílový port, protokol tvoří charakteristiku toku, dále se uchovávají časová razítka, množství přenesených dat, TCP flagy, ...
- poskytuje celkový pohled na to, co se děje na síti

Používané protokoly

- bezpečnost komunikačních protokolů se neřeší
- mnoho protokolů původně určeno pro naprosto jiné podmínky
  - BACnet
  - Modbus
  - M-Bus
  - ...

PSYB0T

technické parametry

- IRC botnet útočící na Linuxová zařízení s architekturou MIPSel
- kromě hádání SSH a telnet hesel využívá i mnoho specifických zranitelnosti jednotlivých typů zařízení (Linksys, Netgear, Netcomm, . . .)

časová posloupnost

- verze 2.5L objevena v lednu 2009 a zůstala bez většího zájmu
- verze 2.9L měla na svědomí DDoS útok na server DroneBL v březnu téhož roku
- následně byl botnet vypnut s deklarovanou velikostí 80 000 nakažených zařízení

Stuxnet

technické parametry

- zacílení na SCADA (*supervisory control and data acquisition*) systémy – první objevený červ, který se soustřeďuje na průmyslové systémy
- šíří se pomocí USB zařízení a následně využívá **sadu** zero-day exploitů MS Windows
- dokáže přeprogramovat programovatelné logické kontrolery (PLC) a skrývat svou činnost
- je digitálně podepsán ukradenými klíči důvěryhodných CA
- neobvykle sotisfikovaný

časová posloupnost

- objeven v červnu 2010
- nepozorovaně působil ale již měsíce před tím (červenec 2009)

Záměr

stanovení cílů, očekávané výsledky

Cíle

Detekce nežádoucích zařízení v síti

- detekce NATu
- detekce transparentní proxy
- detekce zařízení v senzorových sítích

Detekce nežádoucího chování v síti

- adaptace sběru informací o tocích – Ethernet, BACnet, ...
- rozšíření/úprava protokolů (NetFlow/IPFIX)
- úpravy nástrojů pro sběr informací o tocích

Analýza použitelnosti konceptů známých z datových sítí

- monitorování na základě informací o tocích
- IDS/IPS systémy
- Deep Packet Inspection

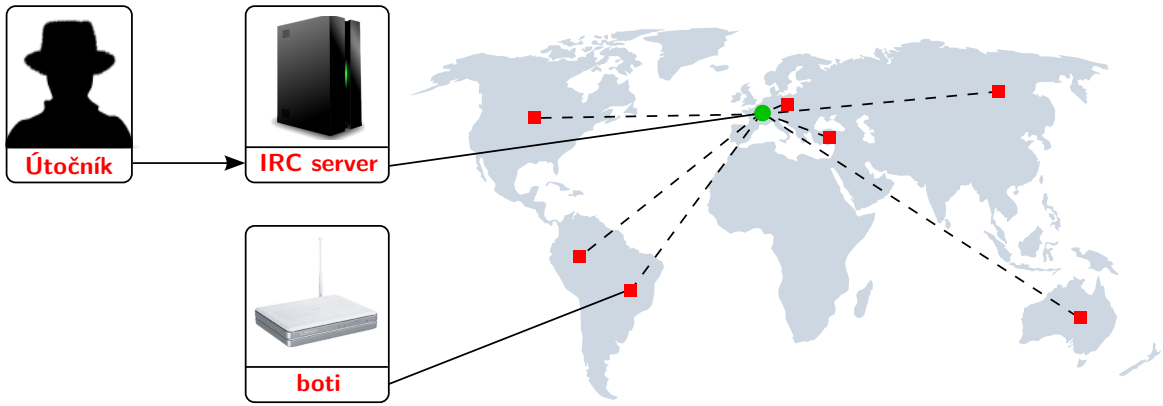
Použití vytvořených nástrojů v technologické síti MU (kampus Bohunice)

Dosavadní výsledky

dosavadní výsledky práce, publikace

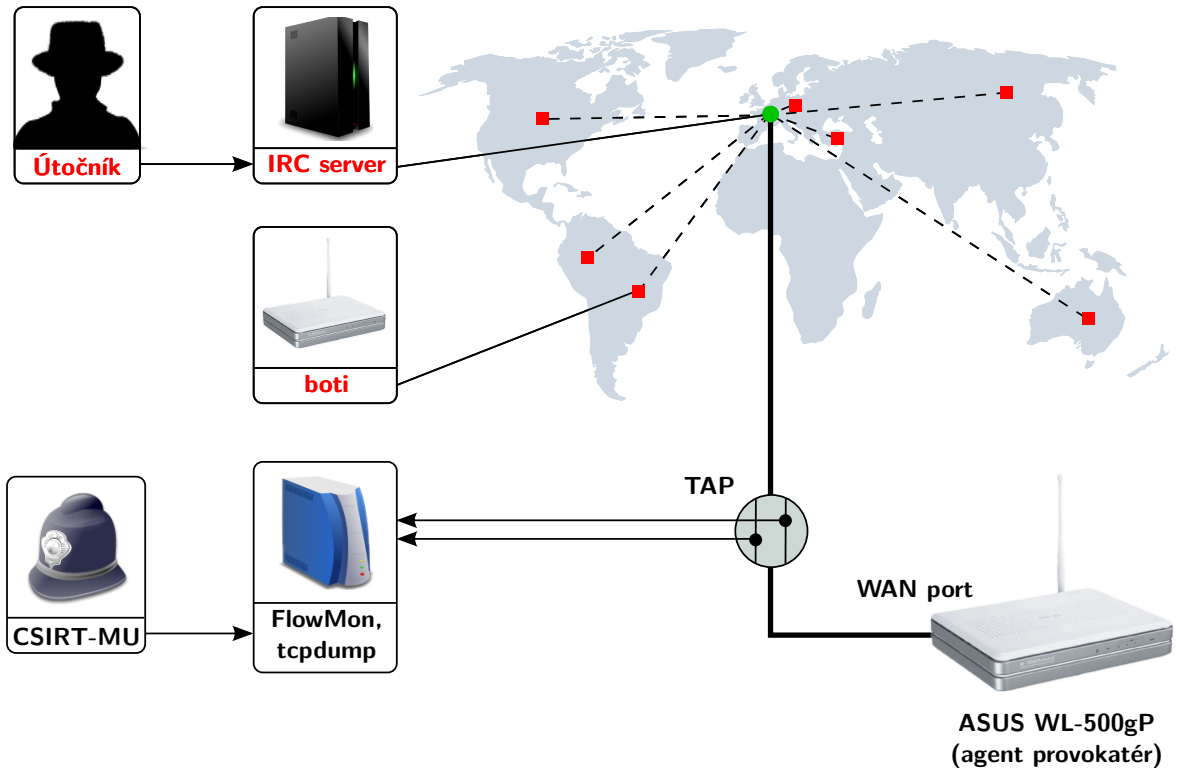
Chuck Norris botnet

- objeven 2. 12. 2009 na MU
- škodlivý software pro Linux – architektura MIPSel
- zranitelnými zařízeními jsou ADSL modemy, routery, ...
- hlavním způsobem nákazy je hádání slabých hesel (TELNET)
- jde o IRC bota s centrálními řídicími servery



Chuck Norris botnet

- objeven 2. 12. 2009 na MU
- škodlivý software pro Linux – architektura MIPSel
- zranitelnými zařízeními jsou ADSL modemy, routery, ...
- hlavním způsobem nákazy je hádání slabých hesel (TELNET)
- jde o IRC bota s centrálními řídicími servery



Modifikace NetFlow/IPFIX

- monitorování sítě na základě toků nelze použít všude
- lze však upravit definici toku podle charakteristiky sítě
- modifikace pro Ethernet, BACnet, ...
- ve stádiu příprav

Publikace I

Drašar, M., Vykopal, J., Krejčí, R. a Čeleda, P.
Aspect-based Attack Detection in Large-scale Networks
Recent Advances in Intrusion Detection, 2010.

Novotný, J., Čeleda, P., Dedek, T. a Krejčí, R.
Hardware Acceleration for Cyber Security
IST-091 – Information Assurance and Cyber Defence, 2010.

Krmíček, V., Vykopal, J. a Krejčí, R.
Netflow Based System for NAT Detection
Co-Next Student Workshop '09: Proceedings of the 5th international student workshop on Emerging networking experiments and technologies, 2009.

Publikace II


Čeleda, P., Krejčí, R., Vykopal, J. a Drašar, M.
Embedded Malware – An Analysis of the Chuck Norris Botnet
Proceedings of the EC2ND Conference, 2010.


Čeleda, P. a Krejčí, R.
Na stopě Chucka Norrise
Data Security Management, 2010.


Krejčí, R. a Čeleda, P.
(Ne)bezpečné HTTPS – část I
Data Security Management, 2010.


Krejčí, R. a Čeleda, P.
(Ne)bezpečné HTTPS – část II
Data Security Management, 2010.