THE SYSTEM FOR TESTING SECURITY OF THE COMMUNICATION UNIT LAN REMOTE DATA COLLECTION

Petr Mlýnek
Master Degree Programme (2), FEEC BUT
E-mail: xmlyne01@stud.feec.vutbr.cz

Supervised by: Jiří Mišurec
E-mail: misurec@feec.vutbr.cz

ABSTRACT

The aim of this project is testing security of the communication unit LAN against attacks from the Internet. The next aim of this project is testing data communication secure between communication unit and data collection center. Systems for the remote data collection are widely used. One of the area is also data collection in energetic, when the energy consumption can be collected daily and presented to users on-line. The advantage of the remote data collection is possibility of frequent readings without a physical presence at the electrometers. The data transmission in the Internet can be subject of various attacks, which is the disadvantage. The understanding of attack method is the most important thing. The protection against the hackers is not complicated, but requires only lot of attention. This article is focused on the SYN flood attack and ARP spoofing. These attacks were successfully accomplished in our laboratory.

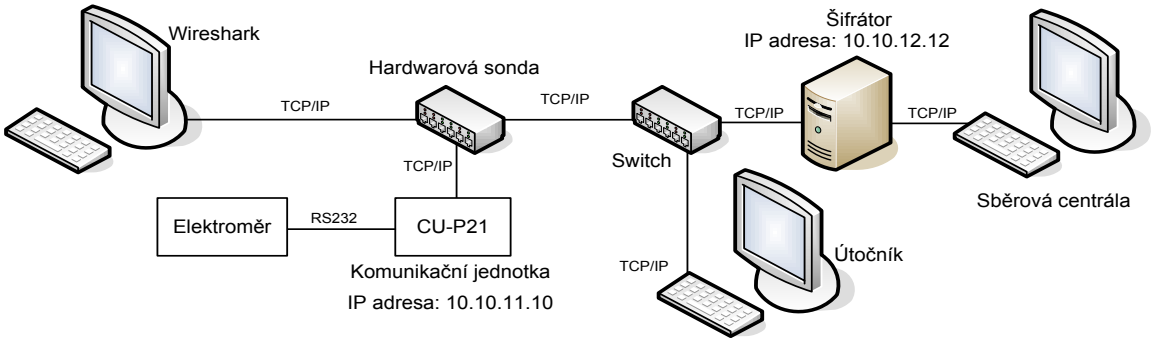
1. ÚVOD

Pro dálkový sběr dat mohou být využity různé komunikační kanály, jako například GSM síť nebo Internet. Tento příspěvek se zabývá dálkovým sběrem dat přes Internet. Internet je v současnosti nejrozšířenější sítí sloužící k datové komunikaci. Snaha o maximální využití při datových přenosech z různých zařízení vyžaduje vytvářet vhodné komunikační jednotky, které umožní připojení různých zařízení, jako například elektroměr. Přenos dat přes Internet však může být předmětem různých útoků. Základem jakékoli obrany je důkladná znalost těchto útoků.

2. SESTAVA PRO SIMULACI ÚTOKŮ

Pro účely simulace útoků a testování odolnosti komunikační jednotky byla vytvořena sestava zapojená podle Obrázku 1.

CU-P21 je komunikační jednotka měřicího přístroje, viz [1]. Komunikaci inicializuje centrála přes šifrátor, který se poté spojí s kryptografickým modulem komunikační jednotky. Po úspěšné oboustranné autentizaci, může začít komunikace centrály s elektroměrem.



Obrázek 1: Schéma zapojení testovacího pracoviště

3. SKENOVÁNÍ

Podstatou skenovaní je nalezení systémů dosažitelných z venkovního Internetu. Základem je zjistit, jestli je cílová IP adresa dosažitelná. To lze například zjistit prostřednictvím hromadného pingu pomocí Linuxového nástroje *nmap*. Dále musíme zjistit, na jakých portech naslouchají síťové služby. To zjistíme rovněž pomocí nástroje *nmap*. Alternativou ve Windows je programu *SuperScan*.

nmap –sP 10.10.11.0/24

```
Host (10.10.11.10) appears to be up.
```

nmap –sS 10.10.11.10

```
Port          State       Protocol
2000          open        tcp
```

4. SYN FLOOD ÚTOK

Výměna dat přes TCP/IP začíná tzv. *three-way handshake*. Jedná se vlastně o způsob, jak se navazuje spojení v rámci TCP protokolu, viz [2].

Z níže uvedené síťové komunikace je patrné, jak šifrátor SYN paketem zahajuje komunikaci s komunikační jednotkou.

```
Source address  Destination address   Protocol      Info
10.10.12.12     10.10.11.10           TCP       1105>2000[SYN]
10.10.11.10     10.10.12.12           TCP       2000>1105[SYN,ACK]
10.10.12.12     10.10.11.10           TCP       1105>2000[ACK]
```

Útok SYN flood využívá špatné implementace začátku tohoto spojení. Útočník posílá posloupnost paketů s příznakem SYN cílovému počítači, ale již dále neodpovídá.

Syn flood útok spustíme pomocí programu *hping* na IP adresu a port zjištěný při skenování sítě : **hping2 -S --flood --rand-source 10.10.11.10 –p 2000**. Takto zahltíme port 2000 SYN pakety, jak vidět na níže uvedené síťové komunikaci.

```
Source address   Destination address  Protocol      Info
174.106.199.13   10.10.11.10          TCP    2204>2000[SYN]
10.10.11.10      174.106.199.13       TCP     2000>2204[RST,ACK]
68.82.171.246    10.10.11.10          TCP     2205>2000[SYN]
10.10.11.10      68.82.171.246        TCP    2000>2205[RST,ACK]
```

Komunikační jednotka odpovídá na záplavu SYN paketu reset paketem. SYN paketů přijde velké množství a tím má jednotka otevřené velké množství spojení a není schopna otevřít další spojení. Po tomto útoku se nemůže šifrátor spojit s komunikační jednotkou, to znamená, že nemůže provést odečet dat z elektroměru, takže útok byl úspěšný.

Útok SYN pakety je nepříjemný, protože útočník si vystačí s velmi skromným připojením k síti, útočník může být i mimo lokální síť, využívá způsobu definovaného pro zahájení TCP relace a pracuje s velkým objemem dat, ale útok funguje jedině tehdy, pokud server alokuje prostředky po obdržení paketu SYN ještě před tím, než obdržel paket ACK.

Základní obranou je zkrátit dobu, po kterou server čeká na pokračování relace vyvolané příkazem SYN, nebo blokovat provoz přicházející z falešných IP adres. Je možné řešení i v podobě SYN a RST Cookie, které odstraňují problém s alokací systémových prostředků.

5. ARP SPOOFING

ARP spoofing je zneužití Address Resolution Protocolu umožňující útočníkovi vydávat se v místní síti za jiný počítač. Útok využívá faktu, že protokol ARP si vůbec nehlídá, jestli o data žádal nebo ne. ARP spoofing funguje pouze uvnitř broadcastové domény, viz [2].

Útok provedeme tak, že nejprve vytvoříme záznamy v ARP Cache. Toto provedeme příkazem *ping* z počítače Útočníka na komunikační jednotku a výchozí bránu. Nyní pomocí Linuxového nástroje *arpspoof* začneme falšovat všechny ARP odpovědi týkající se výchozí brány, takže síťový provoz od komunikační jednotky určený pro bránu skončí u útočníka. Útočník poté musí zajistit přeposlání dat k původnímu adresátovi.

arpspoof -t 10.10.11.10 IP adresa brány

6. ZÁVĚR

Otevřenost a dostupnost veřejné sítě Internet přináší kromě kladů také řadu bezpečnostních rizik. Nechráněná data putující po sítích a je snadné je odposlechnout a zneužít. Naproti tomu stále větší dostupnost veřejné sítě Internet předurčuje k využití pro datové přenosy a sběr dat z měřicích zařízení.

Pomocí ARP přesměrování jsme schopni zachytit komunikaci mezi komunikační jednotkou a sběrnou centrálou. Komunikace je v uvedeném případě šifrována symetrickou šifrou AES. Pro dešifrování bychom museli provést 2^{128} operací, což není v reálném čase proveditelné.

Horší pro tuto komunikaci jsou útoky na dostupnost služeb, kdy pomocí SYN flood útoku zahltíme síťové prostředky. Po tomto útoku nelze realizovat spojení mezi komunikační jednotkou a sběrnou centrálou. Toto přerušení spojení je pouze dočasné, ale i přes to může být nepříjemné.

LITERATURA

[1] KOUTNÝ, M.: Komunikační jednotka koncového měřícího zařízení v energetice. Diplomová práce VUT v Brně, FEKT, Ústav telekomunikací, 2007.

[2] Stuart McClure, Joel Scambray, George Kurtz: Hacking bez záhad, Grada, Praha 2007, ISBN 978-80-247-1502-5