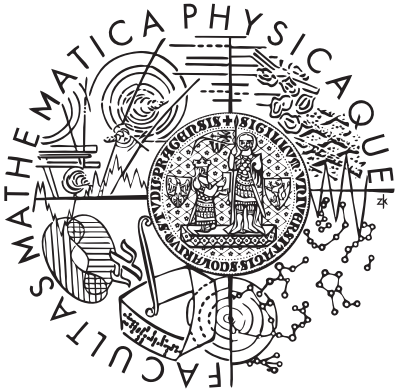
Sítě a bezpečnost

Jiří Setnička a Jan Škoda

Matematicko-fyzikální fakulta Univerzity Karlovy v Praze

Podzim 2012



Náplň přednášky

- Struktura sítí a aktivní síťové prvky
  - Rozbočovač, switch, router
- Pakety a rámce
- Řízení komunikace na síti
  - Spojovaná a nespojovaná komunikace (TCP, UDP)
  - Adresace paketů (IP adresy, ARP)
- Šifrování komunikace
- V průběhu: Praktické ukázky útoků a možnosti obrany

Struktura sítí a jejich dělení

Sítě

Dva druhy sítí:

- WAN – *Wide Area Network* – Internet, CESNET, ...
- LAN – *Local Area Network* – domácí a firemní sítě

Navzájem propojené sítě

- Komunikace v rámci sítě nebo ven

Všechna zařízení zapojená do sítě mají:

- **MAC adresu**
  - *Unikátní* identifikační číslo – `A0-88-B4-9A-09-0C`
  - Vázané na HW
- **IP adresu**
  - Vyjadřuje polohu zařízení v síti – `195.113.27.37`
  - Přidělované dynamicky (pokaždé může být jiná)

Síťový model

Síť se dělí do vrstev

- Výše postavená vrstva využívá nižší vrstvy
  - Aplikace se nestará kudy data jdou – jednoduše je odešle
- Teoretický model **ISO/OSI** – 7 vrstev
- Používaný model **TCP/IP** – 4 vrstvy

Důležité vrsty:

1. Fyzická – „dráty“, fyzický aspekt
2. Linková – spojuje sousední síťová zařízení
   - Adresace fyzickými MAC adresami
3. Síťová – propojuje vzdálené uzly v síti
   - Adresace IP adresami
4. Aplikační – síťové rohraní pro programy

1. Fyzická vrstva

Opakovač (repeater):

- Jeden vstup a jeden výstup
- Jen zesiluje (opakuje) signál, žádná vnitřní logika

Rozbočovač (hub):

- Více připojených zařízení (*víceportový* opakovač)
  - Umožňuje větvení
  - Hvězdicová topologie
- „Vše všem“ – každý obdržený signál pošle všem připojeným zařízením

2. Linková vrstva

Switch (přepínač):

- Podobnost s opakovačem (více připojených zařízení)
- Má už vnitřní logiku
  - Pamatuje si MAC adresy zařízení na svých portech
  - Snižuje zátěž sítě
- Komunikace:
  1. Switch obdrží na nějakém portu data
  2. Přečte si z hlavičky, komu je má poslat (na jakou MAC adresu)
  3. Zároveň si zapamatuje MAC a port odesílatele
  4. Podívá se, na kterém portu je připojený cíl
  5. Pošle data cílovému zařízení

3. Síťová vrstva

Router (směrovač):

- Spojuje alespoň dvě různé sítě (třeba LAN a WAN)
- Provádí *routování* – hledá pro data nejlepší cestu skrz síť
  - Funguje už nad *IP adresami*
  - **Routovací tabulka** – ukládá nejlepší známé cesty pro dosažení cíle
- Rozdíl: *domácími routery* vs. *routery spojujícími rozsáhlé sítě*
- Příklad domácí WiFi router – kombinované zařízení:
  - LAN switch
  - Router mezi LAN a Internetem
  - WiFi AP (principem podobný hubu)
  - Bridge mezi WiFi a LAN

Pakety, rámce a komunikace v síti

Pakety a rámce

Paket:

- Síťová vrstva – IP adresy
- Části: tělo a hlavička
  - Tělo – přenášená data
  - Hlavička – informace o paketu:
    - Identifikátor paketu
    - Zdrojová a cílová IP adresa (port)
    - Kontrolní součet
    - TTL – **Time to live**

Pakety a rámce

Rámec:

- Linková vrstva – MAC adresy
- Obaluje paket, přenáší ho uvnitř dané sítě
  - Žije jen uvnitř této sítě
- Opět tělo a hlavička
  - Tělo – zabalený paket
  - Hlavička – řídící údaje:
    - Synchronizační sekvence – rozpoznání začátku rámce
    - MAC adresa zdroje a cíle
    - Kontrolní součet

Ukázka paketů a rámců

Program Wireshark – analyzér síťového provozu

Schéma posílání dat

1. Aplikace odešle data
2. Síťová vrstva zabalí požadavek do paketu
   - Opatří hlavičkami
   - Předá linkové vrstvě
3. Linková vrstva zabalí paket do rámce
   - Pokud je cíl ve stejné síti, nastaví MAC adresu cíle
   - Pokud je v jiné síti, nastaví MAC adresu routeru
4. Router vybalí paket z rámce
   - Podívá se do routovací tabulky a najde nejlepší cestu
   - Paket opět zabalí do rámce a pošle do správné sítě
5. ...
6. Cíl vybalí paket z rámce a data z paketu – hotovo

Překlad MAC adres

Vím, komu chci poslat data (mám IP adresu), ale nevím fyzickou MAC adresu.

- Potřebuji zjistit MAC adresu
- Vyšlu do sítě dotaz „Kdo má tuto IP adresu?“
  - Posílám na speciální fyzickou adresu `FF-FF-FF-FF-FF-FF`
  - Dotaz dostanou všichni
  - Vlastník dané adresy odpoví „To jsem já, moje MAC je…“
- Pokud se IP adresa nachází v jiné síti, ptám se na MAC routeru
- Neustále dotazy zatěžují síť (všechny uzly)
- Není nutné se ptát stále znovu – data se ukládají do **ARP tabulek**

Ukázka ARP paketů

Wireshark – filtrování paketů

ARP tabulky

Vlastnosti:

- Záznamy mají omezenou životnost – po čase se aktualizují
- Jedna MAC může mít více IP – servery
- Když se přijme nějaký ARP paket, aktualizuje se údaj v tabulce

Zranitelnost:

- Nemám záruku, že odpověď není podvržená
- Kdo víc křičí, vyhrává – **ARP útoky**

Obrana:

- Statické ARP tabulky
  - Problémové přidávání nových zařízení
  - Nutné na všech uzlech zanést novou IP a MAC
  - Používá se jen v rizikových sítích – banky

Útok a obrana

ARP spoofing

Zkusíme přesvědčit ostatní zařízení v síti, že my máme tuto MAC

- Vyhlédneme si oběť – zapamatujeme si MAC a IP
- Začneme zaplavovat síť množstvím ARP dotazů
  - Všechna zařízení postupně aktualizují svoje ARP tabulky
  - Zapíší si, že IP oběti teď sedí na naší MAC adrese
- Data pro oběť začnou proudit přes náš počítač
- Měli bychom je přeposílat oběti, aby nic netušila
  - Přeposíláme na zapamatovanou MAC adresu oběti
  - Stává se z nás „ten uprostřed“ – *Man-in-The-Middle (MiTM)*
- Pokud provedeme oboustranně, kontrolujeme odchozí a příchozí komunikaci oběti

Ukázka ARP spoofingu

Ettercap – analyzování a testování/ovlivňování sítě

Útok MiTM - ovlivňování obsahu paketů

Poté, co data proudí přes můj počítač:

- Mohu číst obsah všech paketů
- Mohu obsah i ovlivňovat

Přepisování paketů I

- Mohu zadržet pakety a ručně je přepsat
- Přepisování mohu ro určité výrazy dělat automaticky

Použijeme program **burp suite**

Přepisování paketů II

Co přepsat přihlašovací dialog? Nebo adresu souboru ke stáhnutí?
Převezmeme emailový účet na Seznamu :)

Obrana

Obrana spočívá hlavně v opatrnosti:

- Statické ARP tabulky
  - Nepohodlné
  - Musí zařídit správce celé sítě – uživatel neovlivní
- Mít vlastní síť, kam nikoho nepustím
- Přistupovat jen přes šifrované spojení (SSL)
  - Ne vše je přístupné přes šifrované spojení
  - Důležité hlavně u citlivých dat (přihlašování)
  - Nesmím „odklepnout“ neplatný certifikát

Šifrování

Symetrické a asymetrické šifry

Symetrické šifry:

- Stejný klíč pro šifrování a dešifrování
- Jsou rychlé – lze jimi přenášet rychle hodně dat
- Nevýhoda: nutnost si předem předat klíč

Asymetrické šifry:

- Soukromý a veřejný klíč
- Data zašifrovaná jedním klíčem lze rozšifrovat jen pomocí druhého
- Výhoda: Veřejný klíč mohu předat nezabezpečeným kanálem
- Nevýhoda: Jsou pomalé, zašifrování trvá dlouho

Použití v praxi:

- Asymetrickou šifrou si vyměníme klíč pro symetrickou šifru
- Symetrickou šifrou šifrujeme zbytek komunikace

SSL a HTTPS

SSL:

- Šifrovací protokol využívající asymetrické šifry
- Navázání spojení:
  - Klient pošle serveru žádost o SSL spojení
  - Server odešle nazpět svůj veřejný klíč asymetrické šifry
  - Klient by si veřejný klíč měl **ověřit**
  - Klient vygeneruje heslo, zašifruje ho veřejným klíčem a odešle serveru
  - Server odpoví, šifrovaná komunikace navázána

HTTPS:

- Rozšíření HTTP o šifrování
- Pro přenos využívá SSL

Certifikáty

Nebezpečí SSL:

- Nějaký asymetrický klíč si může vygenerovat kdokoliv
  - Při útoku MiTM mi může nějaký klíč nabídnout i útočník
- Jak poznat, že klíč je pravý a mohu ho používat?
  - Můžu si otisk klíče ověřit (zavolat, ověřit osobně)
  - Klíč může být podepsaný jiným klíčem – vzniká **digitální certifikát**

Certifikační autority

Ověřování pravosti certifikátů:

- V operačním systému je přednastaveno několik důvěryhodných **certifikačních autorit – CA**
- Pokud je klíč podepsaný důvěryhodnou CA, je důvěryhodný
- Vzniká strom důvěry – nebezpečí, pokud selže některý ze článků
- Při správném použití brání před útoky MiTM
- **Důležité:** Nedůvěřovat neznámým certifikátům.

Co si odnést?

- Vědět o nebezpečích, dávat si pozor ve veřejných sítích
- Při podezřelém chování (náhle delší odezva, problémy s certifikáty) zpozornět
- Pokud si chci být jistý, ověřit stav
  - Wireshark – kontrola ARP provozu
  - Specializované nástroje varující před ARP útoky: *Arpwatch*, *ArpOn*
- Nevěřit, že síť je bezpečná po celé cestě
- Citlivé věci jen přes šifrované spojení (SSL, PGP)
- Neodklikávat neznámé certifikáty
- **Hackování za účelem poškození cizí osoby nebo pro vlastní prospěch je protizákonné!**

Děkuji za pozornost.
Dotazy?