# PV210 Bezpečnostní analýza síťového provozu

## Útoky podle vrstev sítě I

RNDr. Jan Vykopal, Ph.D.

24. 9. 2014

# Rozvrh I

- 17. 9. Úvod. Opakování TCP/IP. ~~Vykopal~~ Čeleda
- 19. 9. Cvičení odpadlo.
- **24. 9. Útoky podle vrstev sítě I. Vykopal**
- 26. 9. Cvičení sk. PV210/01 – Wireshark a hloubková analýza paketů. Vykopal

# Rozvrh II

- 1. 10. Útoky podle vrstev sítě II. Vykopal
- 3. 10. Cvičení sk. PV210/02 – Wireshark a hloubková analýza paketů. Vykopal
- 8. 10. Základní prvky zabezpečení sítě. Zadání 1. domácího úkolu. Vykopal
- 10. 10. Cvičení sk. PV210/01 – První úkol – hledání útoku v PCAPu (Wireshark). Vykopal
- 15. 10. Úvod do bezpečnostního monitorování sítě. Jirsík
- 17. 10. Cvičení sk. PV210/02 – První úkol – hledání útoku v PCAPu (Wireshark). Vykopal
- 22. 10. Jednoduché metody zpracovávající síťové toky Odevzdání 1. úkolu. Vykopal

# Požadavky na bezpečnost

- **Důvěrnost** (confidentiality) – k datům mohou přistupovat pouze oprávněné strany.
- **Nedotčenost** (integrity) – úpravu dat mouhou provést pouze oprávněné strany.
- **Dostupnost** (availability) – data jsou dostupná oprávněným.
- **Pravost** (authenticity) – existuje možnost ověřit identitu uživatele.

# Rozdělení útoků

- **Pasivní** vs. **aktivní**.
- **Zevnitř** vs. **zvenku**.
- Zdroj: RFC 2828.

- **Centralizované** vs. **distribuované**.

# Rozdělení útoků – jiný pohled

- Čtyři dimenze, každá dimenze obsahuje více kategorií.

- **Vektor** – fyzické útoky, síťové, na hesla, . . .
- **Cíl** – hardware, OS, aplikace, síť
- **Zneužité zranitelnosti** – návrhové, implementační, konfigurační
- **Vedlejší projevy** – jiné útoky, poškození či vyzrazení informace, zneužití
- Zdroj: *A taxonomy of network and computer attacks*, Hansman, Hunt, 2005.

# Pasivní útoky

- Odposlech a využití přenášených dat bez zásahu do systému.
- Únik informací.
- Analýza provozu (např. hledání vzorů komunikace v šifrovaném provozu).

- Detekce velmi obtížná, ale lze jim poměrně dobře předcházet.
- Příklad: odposlech linky (wiretapping – více např. v RFC 2804, ale i RFC 3924).

# Aktivní útoky

- Úprava přenášených dat, generování „nového” provozu.
- Obecně lze rozdělit:
  - Maškaráda (masquerade).
  - Opakování (replay).
  - Úprava (modification).
  - Odmítnutí služby (denial of service).
- Detekce možná, prevence obtížná.
- Příklady: phishing, Man-In-The-Middle (MITM), web defacement, TCP SYN flood.

# Útoky zevnitř

- Nebezpečné, protože často nečekané. Organizace se zaměřují na prevenci vnějších útoků.
- Příklad: zpřístupnění zdrojů neoprávněným subjektům, zneužití autorizace na základě IP adresy.

# Útoky zvenku

- Pochází z vnějšku spravované sítě.
- Některým útokům lze velmi snadno předcházet.
- Příklad: IP spoofing, kdy do sítě přichází paket se zdrojovou IP patřící do rozsahu sítě.

# Útoky na spojové a fyzické vrstvě

- Bagr.
- Odposlech (na L1 fyzicky, na L2 v době hubů).
- Souvisí s fyzickou bezpečností.

- Kradení MAC adres síťových rozhraní.
- Kradení portů switche (port stealing). Nástroj ettercap.

# Kradení portů podrobněji I

- Switch (přepínač) si s **každým** příchozím paketem aktualizuje tabulku přiřazení portu a MAC adres(y).
- Útočník pošle rámec s cílovou MAC adresou, která je nastavena na jeho MAC adresu, zdrojová MAC adresa rámce je adresa oběti.
- Switch si poznačí, že na portu X switche je nyní oběť (nejspíš proto, že došlo k fyzickému přepojení). Ve skutečnosti je na portu X útočník.
- Každý příchozí paket pro oběť je pak “ukraden“ a poslán útočníkovi.

# Kradení portů podrobněji II

- Pokud chce útočník přenést paket k oběti (a to typicky chce, aby nebylo nic poznat), musí opravit tabulku switche do “původního stavu” – pošle požadavek ARP na IP adresu Y oběti.
- Oběť odpoví, že má adresu Y a pošle svou MAC. Switch si aktualizuje mapování portů a adres.
- Útočník pošle “ukradený“ paket oběti.
- Jakmile ale začne oběť vysílat, tabulka switche se přepíše a je nutno celý útok opakovat. Stejně tak v případě dalšího příchozího paketu pro oběť.

# Útok na CAM aktivních prvků

- Záplava MAC adres, např. pomocí nástroje macof.
- Donucení prvku k přepnutí do režimu hubu.
- Následně pasivní odposlech celé (pod)sítě.
- Obrana: statické MAC adresy, limit na počet naučených MAC adres.

# Podvržení odpovědi ARP

- Jinak také ARP poisoning/spoofing, druh maškarády.
- Ukázka na YouTube: `http://www.youtube.com/watch?v=VjlQny3LNlA`
- Útok: arpspoof, obrana: arpwatch, DHCP snooping.
- Stále aktuální hrozba, viz `http://isc.sans.edu/diary.html?storyid=11650`

# Útoky na Spanning Tree Protocol

- Připomenutí: `http://www.samuraj-cz.com/clanek/cisco-ios-9-spanning-tree-protocol/`
- Viz `http://seclab.cs.ucdavis.edu/papers/Marro_masters_thesis.pdf`.
- Další zdroj: `http://www.sanog.org/resources/sanog7/yusuf-L2-attack-mitigation.pdf`.

# Útoky na síťové vrstvě

- Odposlech.
- **Podvržení (spoofing) zdrojové IP**
  Bývá kombinováno s útoky na vyšších vrstvách.
  Obrana proti vnějším útokům: filtrování na hranici sítě.
- **Útok na směrování (RIP)** – podvržení informace o kratší cestě.

# Útoky na síťové vrstvě: ICMPv4

- Protokol nepočítá s autentizací. Zneužití ICMP zpráv.
- **Time exceeded, Destination unreachable** – typ DoS útoku.
- **Redirect** – cílem je odposlech.
- **Echo request** (smurf attack) – DoS útok.
  Zneužití broadcastu, zfalšování adresy odesílatele.
  Více na `http://www.cert.org/advisories/CA-1998-01.html`.
- **Ping of Death** – poslání většího paketu než 65 535 B a fragmentace, dnes už historie.
- **Tear drop** – zneužívá chyby v implementaci fragmentace (překrývající se offsety), také historie.

# Útoky síťové vrstvě: ICMPv6 - útoky na autokonfiguraci

- **DAD DoS** – Neighbor Discovery Protocol (NDP) umožňuje Duplicate address detection, což může zneužít útočník a posílat zprávy, že adresa je již použita
- **RA flood** – DoS záplavou Router Advertisements (RA) protokolu NDP
- **podvržení směrovače a DHCPv6 serveru** – útočník se pomocí RA prohlásí za směrovač a podvrhne odpověď DHCP

- Nástroj: thc-toolkit[1]
- Zdroj: slidy *Security challenges in IPv6* ve Studijních materiálech předmětu

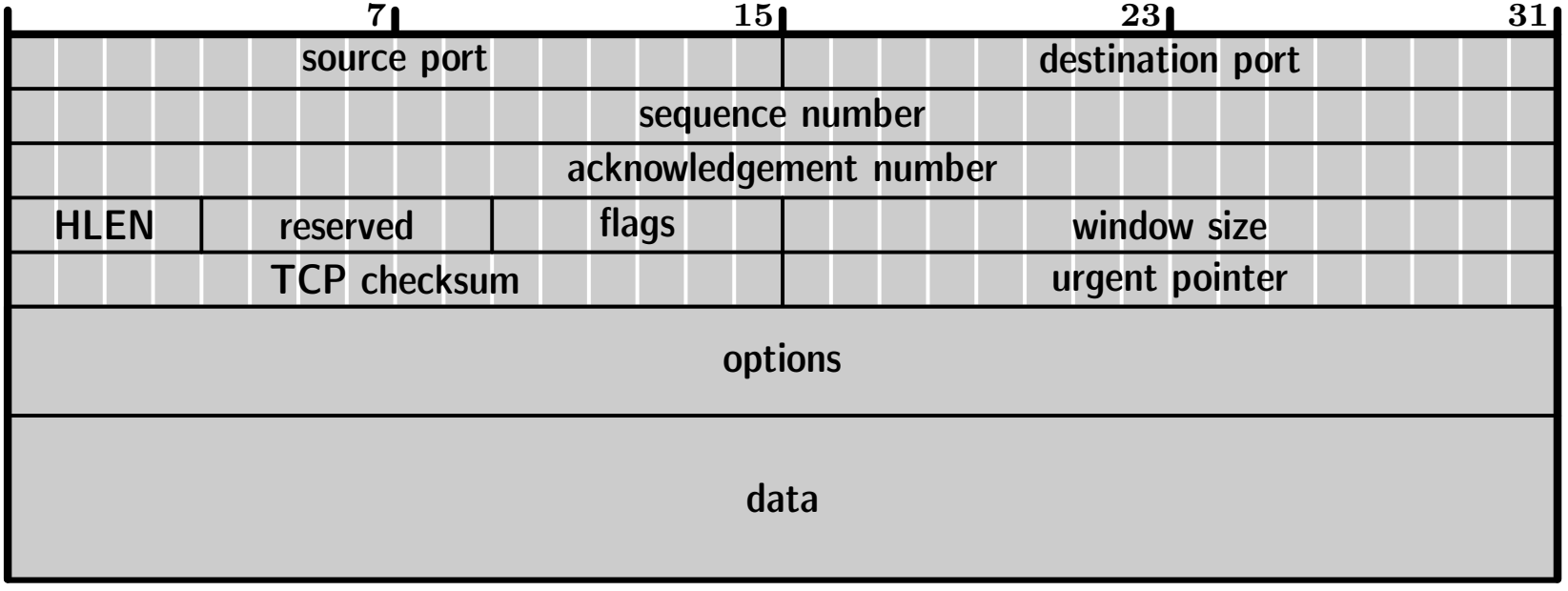
[1] `http://thc.org/thc-ipv6/`

# Shrnutí

- Je známo poměrně dost útoků na protokoly nižších vrstev, nástroje k jejich realizaci jsou volně dostupné.
- Útoky na nižších vrstvách jsou často prvním krokem útočníka.
- Dnes lze předcházet většině z těchto útoků vhodným nastavením aktivních prvků. Např. standard IEEE 802.1X řeší autentizaci uživatele při přístupu do sítě.
- Detekce většiny útoků je možná, taktéž existují volně dostupné detekční nástroje.

- Další multimediální zdroj: videotutoriály YouTube, stačí vyhledat `iefd`.
- Layer 2 Network Protections against MITM Attacks
  `http://isc.sans.org/diary.html?storyid=7567`

# Protokol TCP: opakování I




Příznaky (flags): SYN ACK RST FIN PSH URG

# Protokol TCP: opakování II

## Navázání spojení

- Server „poslouchá” na určitém portu – čeká na zahájení spojení.
- Klient posílá TCP segment s příznakem SYN, nastavuje sekvenční číslo, velikost okna a obvykle také max. velikost segmentu.
- Server odpovídá segmentem SYN+ACK, potvrzuje (SN klienta + 1) a nastavuje vlastní parametry (SN, WS a volitelně MSS).
- Klient odpovídá segmentem ACK, potvrzuje (SN serveru + 1).

- Ukázka provozu ve Wiresharku.

# Protokol TCP: opakování III

## Ukončení spojení

- Ukončuje se zvlášť každý směr spojení, vyvolává buď klient nebo server.
- V praxi se ale většinou ukončí obě poloviny spojení bezprostředně za sebou.
- Ukončující strana: segment s příznakem FIN
- Druhá strana: segment s příznakem ACK