# TEARDROP DOS ATTACK

Roman MICHEL, Master Degree Programme (5)
Dept. of Information Systems, FIT, BUT
E-mail: xmiche01@stud.fit.vutbr.cz

Supervised by: Daniel Cvrček

**ABSTRACT**

Denial of service (DoS) attacks represent the simplest and the most effective network attacks when used to attack non-prepared systems. Their behaviour exploits vulnerabilities in IP communication architecture. By generating and sending particular IP packets they cause unavailability, congestion collapse or restart of network hosts. Purpose of this paper is to show how to prepare and launch a Teardrop attack, how to detect it and what defense strategies are available to prevent this type of attack.

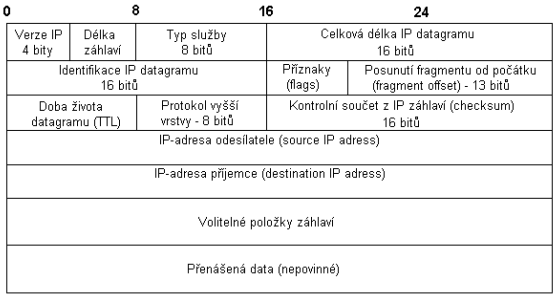
## 1 ÚVOD

Útoky typu DoS (Denial of Service – odepření služby) představují útoky na vzdálené systémy prostřednictvím síťového připojení. Můžeme je rozdělit na 4 základní typy: útoky způsobující obsazení přenosové linky, obsazení systémových zdrojů, útoky na DNS a útoky na chyby v implementaci protokolů TCP/IP. V případě že útok probíhá z více míst najednou, označují se tyto útoky jako DDoS (Distributed DoS – distribuované odepření služby). Více [1]. Teardrop využívá chybu v implementaci TCP/IP na některých systémech. Úpravou IP hlaviček v paketech a jejich odesláním můžeme dosáhnout přetížení vzdáleného systému, případně jeho zatuhnutí nebo restart.

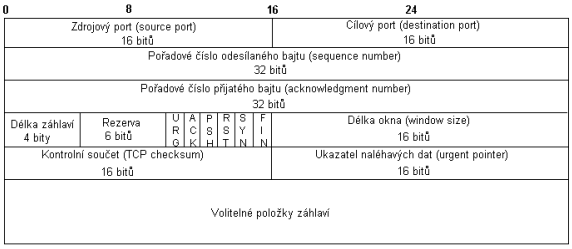
## 2 VYUŽITÍ NEDOSTATKŮ V IMPLEMENTACI PROTOKOLŮ TCP/IP

### 2.1 PROTOKOL IP

Protokol IP slouží k zajištění komunikace a přenosu dat mezi dvěma počítači v Internetu. Základní přenosovou jednotkou je IP datagram, který je přenášen nezávisle na ostatních datagramech. Každý datagram obsahuje hlavičku (Obrázek 1) [2], ve které nás bude v našem případě zajímat hodnota délky datagramu a jeho offsetu. Právě odesíláním datagramů se změnou v těchto položkách můžeme docílit kolaps vzdáleného systému.




Obrázek 1: Záhlaví IP




Obrázek 2: Záhlaví TCP

## 2.2 PROTOKOL TCP

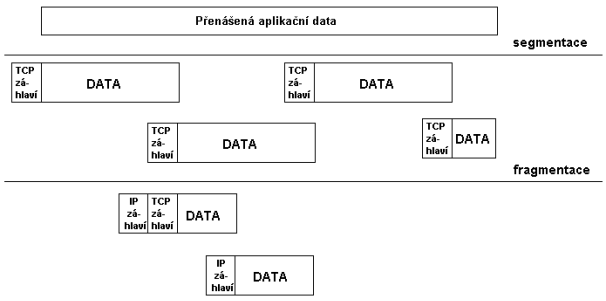
Zatímco protokol IP přenáší data mezi počítači, protokol TCP přepravuje data mezi dvěma konkrétními aplikacemi na těchto počítačích. Pokud použijeme analogii s běžnou poštou, pak IP adresa představuje adresu domu a číslo portu odpovídá jeho konkrétnímu obyvateli [2].

Protokol TCP se označuje jako spojově orientovaný (connection oriented) – na začátku se vytvoří plně duplexní spojení. Posílané TCP segmenty se číslují, ztracený nebo poškozený segment (paket) si příjemce může znovu vyžádat.

## 2.3 SEGMENTACE A FRAGMENTACE DAT

Pokud aplikace potřebuje přenést data, musí je rozdělit nejprve na TCP segmenty. Ty se poté zabalí do IP datagramů. Protože pro hodnotu maximální délky IP datagramu je v hlavičce vyhrazeno číslo o velikosti 16 bitů, může být velikost TCP segmentů nejvýše 65535 bajtů (včetně záhlaví). Rozdělení dat na segmenty vkládané do TCP se nazývá segmentace.

TCP segmenty se vkládají do IP datagramů, ty se poté vkládají do linkového rámce. Pokud se vytváří příliš velké TCP segmenty, vznikají následně IP pakety které jsou větší než maximální velikost přenášeného linkového rámce (MTU). Tuto hodnotu může mít obecně každý směrovač, kterým rámce po své cestě k adresátovi prochází, nastavenu jinak. V případě že je potřeba IP datagramy zmenšit, musí se provést fragmentace (Obrázek 3).




Obrázek 3: Segmentace a fragmentace

Při fragmentaci se začíná využívat položka Fragment offset v hlavičce IP datagramu. Její hodnota určuje, jaké množství dat je uloženo v předchozích datagramech. Například při MTU = 1500 budou datagramy rozděleny tak, že jejich hodnota Fragment offset bude 1500, 3000 a 4500. Poslední datagram který vznikl fragmentací původního bude mít navíc v hlavičce nastaven příznak označující poslední fragment.

### 2.4 PRINCIP ÚTOKU TEARDROP

Teardrop využívá chybu v implementaci při opětovném sestavování IP datagramu z jednotlivých fragmentů. Pokud vytvoříme fragmenty s hodnotou *Fragment offset* v hlavičkách tak, aby na sebe při sestavování jednotlivé fragmenty nenavazovaly, případně se překrývaly, bude cílový systém plně zaneprázdněn pokusy o znovusestavení paketu, nebo dojde k restartu. Díky tomu že se toto sestavování dělá až na straně adresáta, nebude zbytek sítě ohrožen.

Výhodou tohoto útoku je, že existují volně dostupné programy NewTear, Boink, Bonk, kterými může zaútočit prakticky kdokoliv. Teardrop hackeři často po proniknutí do systému změní některé konfigurační soubory a potřebují donutit server k restartu.

## 3 DETEKCE ÚTOKU A OBRANA

Protože jsou na Internetu dostupné už hotové implementace útoků, většina hackerů se pokusí použít už hotový program. Tyto programy ovšem zanechávají typické stopy, díky kterým je možné útok snadno odhalit. Pro DoS útokům obecně jsou nejdůležitější preventivní opatření: administrativní (definice zodpovědnosti a postupů v případě napadení), aktualizace systému a instalace záplat, zavedení QoS pravidel, zavedení anti-spoof pravidel.

Dalším základním kamenem obrany je důsledné logování – následným prohlížením logů z firewallu, směrovače a dalších zařízení je možné určit původ útoku. Doporučuje se přesměrovat všechny logy na jedno zařízení, které tak může průběžně kontrolovat stav všech komponent systému a vyhledávat situace typické pro útok. Centralizovaná analýza umožňuje nastavit prahové hodnoty, či specifické podmínky při kterých je administrátor informován o podezření z útoku.

## 4 DALŠÍ POSTUP

Po dokončení implementace samotného nástroje pro útok Teardrop budeme provádět pokusy s vlivem útoku na systém a vliv různých parametrů na následky útoku. Poslední fází bude návrh možných protiopatření založený na provedených testech.

## REFERENCE

[1] McClure, S., Scambray, J., Kurtz, G.: Hacking bez tajemství, Brno, Computer Press 2003, ISBN 80-7226-948-8

[2] Dostálek, L. a kolektiv: Velký průvodce protokoly TCP/IP: Bezpečnost, Brno, Computer Press 2003, ISBN 80-7226-849-X