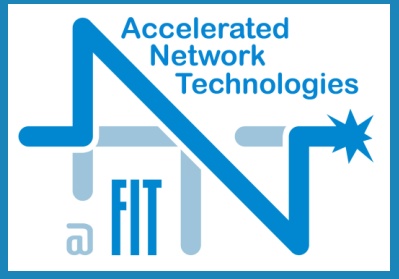
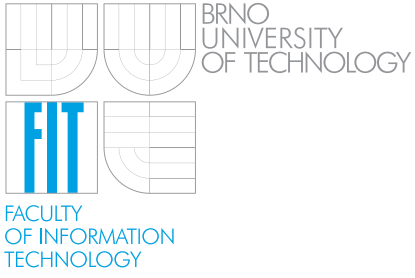
Denial of Service Attacks Targeting a SIP VoIP Infrastructure: Attack Scenarios and Prevention Mechanisms



Jan Kaštil

Brno University of Technology, Faculty of Information Technology
Božetěchova 2, 612 00 Brno, CZ
www.fit.vutbr.cz/~ikastil



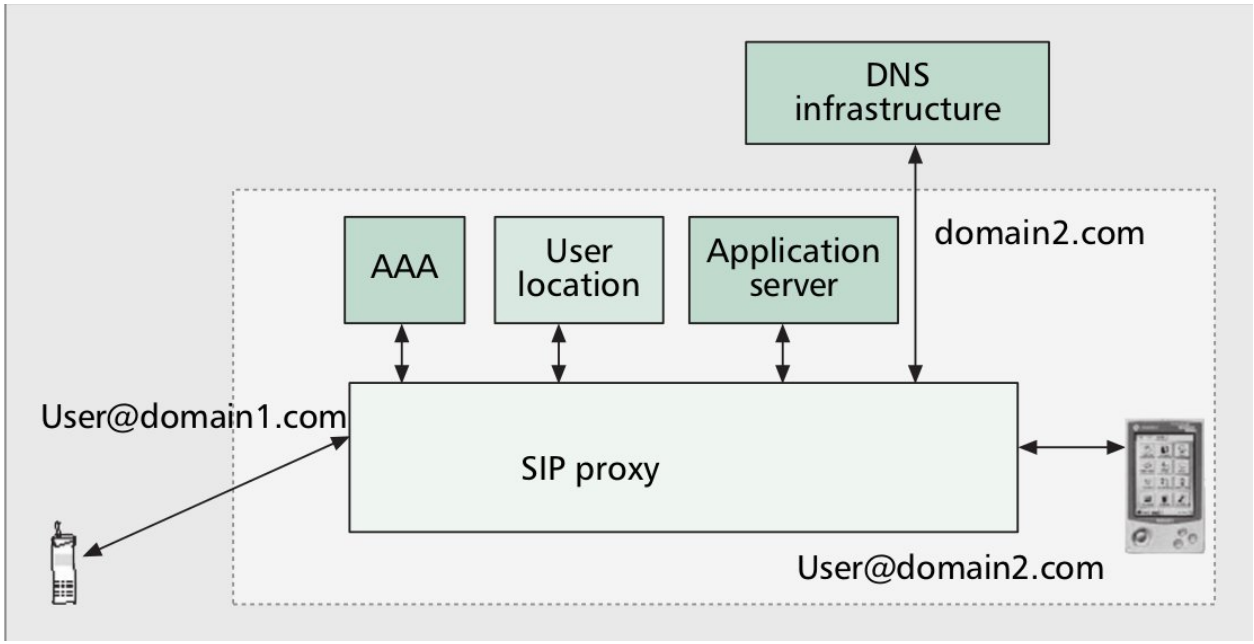
INVESTMENTS IN EDUCATION DEVELOPMENT

DoS útoky

- **chtěné** – aktivita s cílem poškodit systém
- **nechtěné** – například špatná implementace autentizace

Protokol SIP

- Kontrolní textový protokol
- Data hovorů se přenášejí jinými protokoly



Cíle útoku

Paměť

- Bezstavové servery
  - Malé paměťové nároky
  - Specifikace SIP vyžaduje uchovávání stavových informací
- Stavové servery
  - Stav přenosu vs. stav hovoru
  - Důležitá je doba uchování a velikost stavové informace

Procesor

- Dnešní procesory (2006) postačují na bežné zpracování na wire speed
- Možnost aplikovat volitelné hlavičky a uživatelské scripty

Přenosové pásmo

- Klasický DoS útok na TCP
- Nezávislé na SIP

Útoky na paměť

Útok hrubou silou

- Nejjednodušší metoda
- Velké množství požadavků, protože je server rychle ruší

Rozbité spojení

- Útočník potřebuje dva účty
- Jedním posílá požadavky na zahájení hovoru s druhým účtem
- Druhý účet požadavky zahazuje
- Server si musí držet v paměti informaci o spojení až do vypršení časového limitu – více než 3 minuty

Ochrana proti útokům na paměť

Monitorování a filtrování

- Udržováné seznamu podezřelých uživatelů – blacklisty

Autentizece

- Funguje pouze pokud útočník nemá účet
- Standardní proces autentizace vyžaduje uchování stavové informace
  - Snadno zneužitelné uživatelem s přístupem do systému
- Bezstavová autentizace
  - Predictive nonces – IETF draft propadl 2001
  - Doplnění zpráv o kód který je validní jen pro validní zprávy a zvolenou dobu

Bezstavové zpracování

- Velká část funkčnosti může pracovat bezstavově
- Tvoří filtr pro stavové zpracování

Útoky na processor

Šifrování

- MD5 vyžaduje jen malý výpočetní výkon
- Přílišné zatížení šifrováním odpovídá špatné implementaci nebo nedostačujícímu hardware

Aplikační scripty

- Uživatel může přiřadit k příchozím zprávám CGI scripty
- CGI script může svým výpočtem zpomalit procesor
- Pokud je aplikační server umístěn na jiném stroji dojde ke zdržení vlivem čekání na výsledek

Interakce s externím servrem

- DNS dotaz pro určení následující SIP proxy

Přesměrování na neexistujícího TCP příjemce

- Při použití TCP se čeká na ACK

Ochrana proti útokům na processor

Dobrý návrh serveru

- Důležitý je dostatečný výkon CPU a velká paměť
- Software můsí být navržen s ohledem na rychlost a bezpečnost

Kvalitní implementace

- Zaměření na alokaci paměti, zpracování událostí a parsování protokolu

Paralelní implementace

- Implementovat server s podporou vícevláknového zpracování
- Útočník může generovat více zpráv než je vláken a zahltit server
- Procesy musí čekat na DNS odpovědi
- Procesy sdílejí paměť

Posílení útoků

Paketové smyčky a kopírování paketů

- Lze sestavit paket tak, aby jej server přeposílal sám na sebe
- Nutno omezovat počet HOPů požadavku
- Útočník se může registrovat na N místech
  - Jedno spojení se rozgeneruje až na N spojení
  - Útočník si může vygenerovat mnoho účtů

Distribuované DoS útoky

- Stejný princip jako u DDoS útoků ma TCP
- Skrývá identitu útočníka
- Přeposílání odpovědí
  - Vkládáním VIA hlavičky odkazující na oběť
  - Lze řešit zakázáním via hlaviček lišících se od zdrojové IP
  - Diskriminuje klienty za NAT
- Přeposíláním požadavků

Útok na parser protokolu

Příliš dlouhé zprávy

- SIP server musí parsovat celou zprávu
  - Útočník může generovat extrémně dlouhé zprávy
  - Lze nastavit limit délky zprávy

TCP útoky

- Možnost přepnout SIP server na komunikace přes TCP
  - Stává se zranitelným klasickými TCP útoky
  - Přidává stavovou informaci
  - Podpora TCP je vyžadována standardem

Komplikovaná struktura hlaviček

- Více hodnot v jedné hlavičce
  - Lze rozdělit do více hlaviček
  - Nelze tedy zastavit parser po první hodnotě
  - Umístěním důležitých hlaviček na konec lze parser zpomalit

Útok na parser protokolu 2

Stará verze protokolu

- Starší verze SIP je náchylnější k DoS útokům
- Parametr větvení ve VIA hlavičce musí obsahovat magické číslo identifikující protokol

Chybějící TAG

- TAG umožňuje rychlé přiřazení zpráv k hovorům
- Vynechání TAGu donutí server testovat příslušnost zprávy ke všem probíhajícím hovorům

Překvapivé řešení

- Správná implementace
- Přetížení parseru indikuje špatnou implementaci nebo nedostatečný hardware
- Monitorování provozu

Útok na DNS

Popis útoku

- Požadavky se mohou odkazovat na nepřeložitelné doménové jméno
- Server pak musí poslat DNS dotaz a čekat na odpověď
- Při vhodně zvolené doméně nemusí odpověď vůbec přijít

Možnosti obrany

- Omezit používání FQDN
  - FQDN – fully qualified domain name
  - SIP obsahuje hlavičku received
  - Není tedy nutné opakovat DNS dotaz
- Neblokující DNS dotazy
  - Nutné stavové zpracování
  - Náročné na paměť
- DNS caching
  - Snižuje latency DNS dotazů
  - SIP DNS cache má jinou politiku vyhazování než cache OS

Zvýšení odolnosti proti DoS útokům

Správné pořadí zpracování SIP paketu

1. Pokud požadavek patří aktivnímu spojení, zpracuj jej.
2. Jestliže v poslední VIA hlavičce je DNS jméno, použij pro odpověď zdrojovou IP adresu.
3. Pokud je to možné, proveď bezstavovou autentizaci.
4. Proveď rutiní kontroly:
   - Vyhledání virů
   - Vyhledání vzorů známých útoků
   - Pokud je maximální hodnota přeposlání příliš vysoká, sniž ji.
   - Podezřelé pakety zahoď.
5. Volitelně je možné vytvožit stavovou informaci přenosu.

Závěr

- DoS útoky jsou velký problém
- Na SIP je možno provést velké množství útoků.
- Problém nechtěných útoků.
- Vysoký výkon a kvalitní implementace jsou základem pro ochranu před DoS útoky.
- Neexistuje žádný ideální obraný mechanizmus
- Obrana před jedním útokem se může stát slabinou pro jiný.
- Bezstavová implementace je dobrý základ.