

## **New Approaches to Mitigate Network Denial-of-Service Problems**

Denial-of-Service issues take a distinguished place among the open Internet problems. The problem of DoS has close relation to many other current Internet attacks, like spamming. During my research I tried to find a comprehensive solution for the problem. Since there is no single general solution, I had to carry out in-depth analysis of the problem, like analyzing the protocol DoS-specific behavior and using the extra information of the protocol to enhance protection.

The results of my research can be divided into the following three claims:

In the first claim I tried to deal with the general form of DoS problems, where I analyzed and enhanced the protection of application-level protocols against general DoS problems. My results show that the outcome of this approach is not sufficient to handle every type of the problem and it has certain limitations.

**Claim 1 - Protection against DoS problems with client-side puzzle approach combined with game theoretical methods**

**I propose a novel game theoretical approach for the analysis of the client-side puzzle technique against DoS attacks. I determined the optimum of the game depending on the cost parameters. I constructed a novel client-side puzzle challenge, which uses multiplications of prime numbers. The advantage of the proposed algorithms is that its computational complexity can be precisely computed.**

In the second claim I concentrated on the problem of Denial-of-Service attacks against Internet STMP (e-mail) servers. Not considering the very service-specific solutions there are only a few available methods against this threat. I proposed a method to protect against DoS attacks by observing and analyzing the traffic to a particular system.

**Claim 2 – Protection based on traffic analysis against Denial-of-Service problems in Internet e-mail environment**

**I propose a new protection method against DoS attacks based on network traffic analysis. The proposed method does not need the modification of the network elements outside the victim server and minimizes the number of legitimate sources blocked by the server.**

No matter how excellent a general solutions we manage to come up with, specific solutions against DoS problems utilizing special properties of the protected system or service can be more useful than general protection. In my third claim I focused on the prevention of DHA attacks, which also can cause DoS conditions. This section contains the analysis of Directory Harvest Attacks (DHA) (a type of attack to collect e-mail addresses). By giving countermeasures against DHA attacks, I also enhance the protection against other problems, like DoS.

**Claim 3 – Protection against DoS preparation attacks**

**In this claim I propose new methods to counter some DoS preparation attacks, such as preventing the Directory Harvest Attack and identifying malware infected computers. Concerning Directory Harvest Attacks I propose a new architecture and method to protect against the attacks and I define an optimal algorithm of the DHA attack. My proposed protection method is analyzed by simulations and I also created a software prototype.**

## **Új védekezési módszerek hálózati szolgáltatásmegtagadásos problémák ellen**

### **(New Approaches to Mitigate Network Denial-of-Service Problems)**

A megoldatlan internetes problémák között a szolgáltatásmegtagadásos támadások igen különleges helyet foglalnak el. Ez a terület ugyanis összefüggésben van rengeteg más támadásfajtaival. Lehetőség szerint megoldást kerestem általános protokollok védelmére. Nem mindig adható azonban általános megoldás, így figyelembe kell venni azt is, hogy mélyebb ismeretek, pl. a protokoll specifikálása mellett milyen többletinformáció áll rendelkezésre a védelem javítása érdekében.

Kutatásaimat három fő csoportba foglaltam.

Első tézisemben a szolgáltatásmegtagadásos támadások általános sémájával foglalkoztam, amelyben általános alkalmazás szintű protokollok DoS védetségét elemeztem és növeltem. Kutatásaim azt igazolták, hogy az általános megoldások hatóköre szűk, és noha egyes esetekben megoldást jelenthetnek, alkalmazásuknak számos gátja van.

#### **1. Tézis – Szolgáltatás-megtagadásos támadások (DoS) elleni védekezés client-side puzzle technika és játékelméleti módszerek együttes alkalmazásával**

Újszerű, játékelméleti módszereket felhasználó megközelítést javaslok a DoS védelmet szolgáló client-side puzzle megoldások vizsgálatára és javítására. Megállapítom a szerver és támadó között levő játék optimumát a költségparaméterek függvényében. Új client-side puzzle rejtvényt mutatok be, amely prímszámok szorzatán alapul. A javasolt algoritmus előnye, hogy számítás-igénye pontosabban meghatározható, mivel egyszerű műveletekre épül.

Második tézisemben a internetes e-mail szerverek szolgáltatásmegtagadásos támadásaival foglalkozom. A specifikus támadásoktól eltekintve itt is szűk a mozgástér: A vizsgálataimat a hálózati forgalom analízisen alapuló módszerekre koncentráltam. Ez az SMTP szerverek esetében jelenthet általánosabb megoldást a problémákra.

#### **2. Tézis – Szolgáltatás-megtagadásos támadások elleni védekezés forgalom analízis segítségével internetes levelezési környezetben**

Új, a hálózat forgalomanalízisen alapuló védelmi módszert javaslok a DoS támadások kezelésére. A javasolt módszer nem teszi szükségessé a megtámadott szervereken kívüli hálózati elemek módosítását és minimalizálja a hibásan kiszűrt legális felhasználók számát.

Bármilyen általános megoldással szemben sokkal hatásosabbak lehetnek (és néha csak ezek lehetnek hatásosak) azok a megoldások, ahol a konkrét támadást, támadó szándékot, célt és módszert is figyelembe vesszük a védekezés során. Harmadik tézisemben DoS támadások előkészítése ellen mutatok be speciális védekezési módszert. A fejezetben egy speciális problémával, az ún. Directory Harvest Attack (DHA), azaz SMTP szerverek címki gyűjtést célzó támadásaival foglalkozom. A probléma elleni védekezés segíti azt, hogy megelőzzünk internetes támadásokat, köztük a DoS támadást.

#### **3. Tézis – DoS előkészítő támadások elleni védekezési módszerek**

A 3. tézisben új megoldásokat javaslok a DoS előkészítő támadások elleni védekezésre. Az ún. Directory Harvest Attack (DHA, címki nyerést célzó támadás) elleni védekezésre új módszert és architektúrát javaslok és megadom az optimális DHA támadás algoritmusát is. A javasolt védelmi módszer prototípusban is megvalósítottam és szimulációkkal is elemeztem.