IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

AN EFFECTIVE ANATOMIZATION OF CRYPTOGRAPHY IN NETWORK SECURITY

[1]BINOOP KUMAR C A
[1]Assistant Professor,
[1]Department of computer science,
[1]Thunchathezhuthachan College Elavanchery

Abstract: **In this technical world, network security is one of the most important thing which protects your network and data from infringement, intrusions and other threats. Inorder to provide secure network and data trasmission via a wireless network, cryptography and network encryption is beign used. The need for protection in network is very critical. Network security includes security for both source and destination as well as for data transmission, to provide high security during data transmission here we are introducing the concept of cryptography**

Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications. In this paper we discuss an effective anatomization of cryptography in network security

This project utilizes game theory to propose a number of puzzle-based defenses against flooding attacks. It is shown that the interactions between an attacker who launches a flooding attack and a defender who counters the attack using a puzzle-based defense can be modeled as an infinitely repeated game of discounted payoffs.

***Reason for using game theory in designing flooding prevention mechanisms is that the underlying assumptions of game theory hold in a network. The main assumption is that the players are rational, i.e., their planned actions at any situation and point in time must actually be optimal at that time and in that situation given their beliefs. This assumption holds in a network, where players are the active entities created and controlled by human beings. Therefore, a defense mechanism that implements the defender's strategy obtained game-theoretic approach assures its designer that the best possible sequence of* actions is performed against a rational attacker.**

I. INTRODUCTION

A DoS attack is characterized by a malicious behavior, which prevents the legitimate users of a network service from using that service. There are two principal classes of these attacks: flooding attacks and logic attacks. In recent years; some researchers have utilized game based approaches to describe but not to design puzzle-based defense mechanisms. In general, reactive mechanisms suffer from the scalability problem and difficulty of attack traffic identification.

The solution concepts of this type of games are deployed to find the solutions, i.e., the best strategy a rational defender can adopt in the face of a rational attacker. In this way, the optimal puzzle-based defense strategies are developed. More specifically, four defense mechanisms are proposed. PDM1 is derived from the open-loop solution concept in which the defender chooses his actions regardless of what happened in the game history.. PDM2 resolves this by using the closed-loop solution concepts, but it can only defeat a single-source attack. PDM3 extends PDM2 and deals with distributed attacks. This defense is based on the assumption that the defender knows the size of the attack coalition. Finally, in PDM4, the ultimate defense mechanism is proposed in which the size of the attack coalition is assumed unknown

NEED OF THE STUDY.

In recent years, a number of puzzle-based defense mechanisms have been proposed against flooding denial-of-service (DoS) attacks in networks. These mechanisms have not been designed through formal approaches and thereby some important design issues such as effectiveness and optimality have remained unresolved. This project utilizes game theory to propose a series of optimal puzzle-based strategies for handling increasingly sophisticated flooding attack scenarios. This study culminates in a strategy for handling distributed attacks from an unknown number of sources.

This project utilizes game theory to propose a number of puzzle-based defenses against flooding attacks. It is shown that the interactions between an attacker who launches a flooding attack and a defender who counters the attack using a puzzle-based defense can be modeled as an infinitely repeated game of discounted payoffs.
Reason for using game theory in designing flooding prevention mechanisms is that the underlying assumptions of game theory hold in a network. The main assumption is that the players are rational, i.e., their planned actions at any situation and point in time must actually be optimal at that time and in that situation given their beliefs. This assumption holds in a network, where players are the active entities created and controlled by human beings. Therefore, a defense mechanism that implements the defender's strategy obtained game-theoretic approach assures its designer that the best possible sequence of actions is performed against a rational attacker.

3. MODULE DESCRIPTION

LIST OF MODULES:
Defender
Puzzle approach
Rational attacker
Unknown sources
Requested Count

3.1 DEFENDER:

The defender takes his part in the solution as an optimum defense against rational attackers. The defender treats incoming requests similarly and need not differentiate between the attack and legitimate requests. Upon receiving a request, the defender produces a puzzle and sends it to the requester.

If it is answered by a correct solution, the corresponding resources are then allocated. As solving a puzzle is resource consuming, the attacker who intends to use up the defender's resources by his repeated requests is deterred from perpetrating the attack. An attacker who knows the defender's possible actions and their corresponding costs may rationally adopt his own actions to defeat a puzzle-based defense mechanism.

For example, if the defender produces difficult puzzles, the attacker responds them at random and with incorrect solutions. In this way, he may be able to exhaust the defender's resources engaged in solution verification. If the defender produces simple puzzles, the mechanism is not effective in the sense that the attacker solves the puzzles and performs an intense attack.

3.2 PUZZLE APPROACH:

A number of puzzle-based defense mechanisms have been proposed against flooding denial-of-service (DoS) attacks in networks. Nonetheless, these mechanisms have not been designed through formal approaches and thereby some important design issues such as effectiveness and optimality have remained unresolved.

This paper utilizes game theory to propose a series of optimal puzzle-based strategies for handling increasingly sophisticated flooding attack scenarios. A method for limiting resource consumption is the use of client puzzles.

It is shown that the interactions between the attacker who perpetrates a flooding attack and the defender who counters the attack using a puzzle-based defense mechanism can be modeled as a two-player infinitely repeated game with discounting.

In this concept of perfect Nash equilibrium is then applied to the game. This leads to the description of players' optimal strategies.

3.3 RATIONAL ATTACKER:

There are two principal classes of these attacks: flooding attacks and logic attacks. A flooding attack sends an overwhelming number of requests for a service offered by the victim.

These requests deplete some key resources at the victim so that the legitimate users' requests for the same are denied. A resource may be the capacity of a buffer, CPU time to process requests, the available bandwidth of a communication channel, etc.

3.4 UNKNOWN SOURCES:

This study culminates in a strategy for handling distributed attacks from an unknown number of sources. The ultimate defense mechanism is proposed in which the size of the attack coalition is assumed unknown.

This notion is applied to a series of increasingly sophisticated flooding attack scenarios, culminating in a strategy for handling a distributed attack from an unknown number of sources.

This reflects those attack-defense circumstances in which the player involved in the defense mechanism knows his opponent's payoff function as well as the actions chosen by his opponent at previous periods. It is worth noting that the puzzles can be designed in such a way that the amounts of resources a machine uses to solve a puzzle are independent of the machine's processing power.

Therefore, except for flooding attacks from an unknown number of sources, it is reasonable to assume that the defender knows the attacker's payoff function.

3.5 REQUESTED COUNT:

In the client-puzzle approach, the defender engages two types of resources, one for producing puzzles and verifying solutions, and the other for providing the requested service.

The defender who counters the attack using a puzzle-based defense mechanism can be modeled as a two-player infinitely repeated game with discounting.

The interactions between an attacker who perpetrates a flooding attack and a defender who counters the attack using a puzzle-based defense is modeled as a two-player infinitely repeated game of imperfect information.

4 RESULTS AND DISCUSSION

This paper utilizes game theory to propose a number of puzzle-based defenses against flooding attacks. It is shown that the interactions between an attacker who launches a flooding attack and a defender who counters the attack using a puzzle-based defense can be modeled as an infinitely repeated game of discounted payoffs. Then, the solution concepts of this type of games are deployed to find the solutions, i.e., the best strategy a rational defender can adopt in the face of a rational attacker.
A complete flooding attack solution is likely to require some kind of defense during the attack traffic identification. The mechanisms of this paper can provide such defenses the mechanisms.

My project "***A PUZZLE-BASED GAME THEORY IN ADVANCED NETWORKS***", Using front end ASP.NET and back end C# has been completed successfully with the guidance and help of staffs and friends. I was able to finish my project to most of my expectations and in a specified time.

REFERENCES

[1] D. Moore, C. Shannon, D.J. Brown, G.M. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity," ACM Trans.Computer Systems, vol. 24, no. 2, pp. 115-139, May 2006.

[2] A. Hussain, J. Heidemann, and C. Papadopoulos, "A Framework for Classifying Denial of Service Attacks," Proc. ACM SIGCOMM '03, pp. 99-110, 2003.

[3] C.L. Schuba, I.V. Krsul, M.G. Kuhn, E.H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a Denial of Service Attack on TCP," Proc. 18th IEEE Symp. Security and Privacy, pp. 208-223, 1997.

[4] Smurf IP Denial-of-Service Attacks. CERT Coordination Center, Carnegie Mellon Univ., 1998.

[5] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms," ACM SIGCOMM Computer Communication Rev., vol. 34, no. 2, pp. 39-53, Apr. 2004.