RESEARCH PAPER | Engineering | Volume : 5 | Issue : 4 | April 2015 | ISSN - 2249-555X

Xsd Technique for web Application to Overcome Denial of Service Attacks

KEYWORDS: Dos attack, Feedback controller, prioritize scheduling, Xsd technique

N.R.Sindhuja	C.Balakrishnan	C.Kavitha
PG Student, S.A. Engineering College, Chennai.	Associate Professor, S.A. Engineering College, Chennai	PG student, S.A. Engineering College, Chennai.

ABSTRACT *Denial of service (DoS) is a vulnerable attack and it attempts to make a machine or network resource unavailable to its intended or legitimate user. It comprises of a single system that is infected with a type of virus application known as a Trojan. The most common type of Denial of service attack is done by flooding the target resource with external communication requests. The request overload prevents the resource from responding to legitimate traffic, or slows down its response and makes the system unavailable for the user. This situation is said to be degraded situation where the overloaded vulnerable request to the server transfers the control to the legitimate user. The proposed system focuses on the unwanted request access of clients by blocking them from further data accessing. An automated feedback is introduced in the system which provides a prioritized scheduling concept in reducing the DOS rate and redirects the request to the server. This model serves as a supporting tool for the web application for tracing the vulnerability measured and visualized graphically.*

INTRODUCTION

Now-a-days internet has become an important medium for conducting business and selling and buying services. The web thus provides a convenient interface for a better performance. The attainment of these guarantees is especially difficult due to the unpredictable nature of the Internet and overload. These applications require stringent performance from the web server. Internet security is a catch-all term for a very broad issue covering security for transactions made over the Internet. Generally, Internet security encompasses browser security, the security of data entered through a Web form, and overall authentication and protection of data sent via Internet Protocol.

Internet security relies on specific resources and standards for protecting data that gets sent through the Internet. This includes various kinds of encryption such as Pretty Good Privacy (PGP). Other aspects of a secure Web setup includes firewalls, which block unwanted traffic, and anti-malware, anti-spyware and anti-virus programs that work from specific networks or devices to monitor Internet traffic for dangerous attachments. Internet security is generally becoming a top priority for both businesses and governments. Good Internet security protects financial details and much more of what is handled by a business or agency's servers and network hardware. Insufficient Internet security can threaten to collapse an e-commerce business or any other operation where data gets routed over the Web.

Web sites are unfortunately prone to security risks setting aside risks created by employee use or misuse of network resources, your web server and the site it hosts present your most serious sources of security risk. Web servers by design open a window between your network and the world. The care taken with server maintenance, web application updates and your web site coding will define the size of that window, limit the kind of information that can pass through it and thus establish the degree of web security you will have.

DOS AND ITS TYPES

A "denial-of-service" attack is an explicit attempt by attackers to prevent legitimate users of a service from responding to that service. Some examples of such attack are attempts to flood a network, thereby legitimate network traffic attempts to disrupt connections between two machines are prevented, attempts to prevent an individual from accessing a service, attempts to disrupt service to a specific system or person.

Types of Dos Attack

SYN Attack

When a session is initiated between the Transport Control Program (TCP) client and server in a network, a very small buffer space exists to handle the usually rapid "hand-shaking" exchange of messages that sets up the session. The session-establishing packets includes a SYN field that identifies the sequence in the message exchange. An attacker can send a number of connection requests very rapidly and then fail to respond to the reply.

Teardrop Attack

This type of denial of service attack exploits the way that the Internet Protocol (IP) requires a packet that is too large for the next router to handle be divided into fragments. The fragment packet identifies an offset to the beginning of the first packet that enables the entire packet to be reassembled by the receiving system. In the teardrop attack, the attacker's IP puts a confusing offset value in the second or later fragment. If the receiving operating system does not have a plan for this situation, it can cause the system to crash.

Smurf Attack

In this attack, the perpetrator sends an IP ping (or "echo my message back to me") request to a receiving site The ping packet specifies that it be broadcast to a number of hosts within the receiving site's local network. The packet also indicates that the request is from another site, the target site that is to receive the denial of service The result will be lots of ping replies flooding back to the innocent, spoofed host. If the flood is great enough, the spoofed host will no longer be able to receive or distinguish real traffic.

INTERMEDIATE OR FEEDBACK CONTROLLER

A classic example is the performance controller in a web server, which adjusts the server's configuration (e.g., admission rate) in response to the difference between the current and desired states for meeting expected performance (e.g., throughput and service time) [1]. Feedback control is also a central element in QoS-aware systems (e.g., cloud computing, high performance computing [8], [9], virtualized servers [10], cyber-physical systems [11], and autonomic computing). Recent studies have demonstrated that Low-Rate DoS (LRDoS) attacks can degrade the performance of some feedback-control based applications Different from flooding-based DoS attacks, LRDoS attacks send out intermittent high-volume requests to force the victim away from the desired state, thus deteriorating its performance.

The web presents a convenient interface for the emerging performance-critical applications. These applications require stringent performance guarantees from the web server. The concept of the feedback loop to control the dynamic behavior of the system: this is negative feedback, because the sensed value is subtracted from the desired value to create the error signal, which is amplified by the controller. A feedback loop is a common and powerful tool when designing a control system. Feedback loops take the system output into consideration, which enables the system to adjust its performance to meet a desired output response.

Positive feedback has the property that signals tend to reinforce themselves, and grow larger. In a positive feedback system, noise from the system is added back to the input, and that in turn produces more noise. As an example of a positive feedback system, consider an audio amplification system with a speaker and a microphone. Placing the microphone near the speaker creates a positive feedback loop, and the result is a sound that grows louder and louder. Because the majority of noise in an electrical system is high-frequency, the sound output of the system becomes high-pitched.

OVERALL DESIGN

The architecture mainly contains a legitimate client and an attacking client. The legitimate user involves in direct access of a web server. When the client is seems to be an attacking client the control goes to the feedback controller. The feedback controller takes care of evaluating the access between the clients. Also the feedback controller involves in prioritizing the request between the attacking client and the normal client. This system involves a direct site.

When the attacking client tries to inject the xml data into the site, the feedback controller involves in validating the request in the database, whether the user is an already logged in user or not. If he is a valid user, then the control goes to the server, if not the client is alerted with a message as evaluation restricted. There are many different control mechanisms that can be used, both in everyday life and in chemical engineering applications. There are two broad control schemes, both of which encompass each other are feedback control and feed-forward control. Feedback control is a control mechanism that uses information from measurements to manipulate a variable to achieve the desired result.

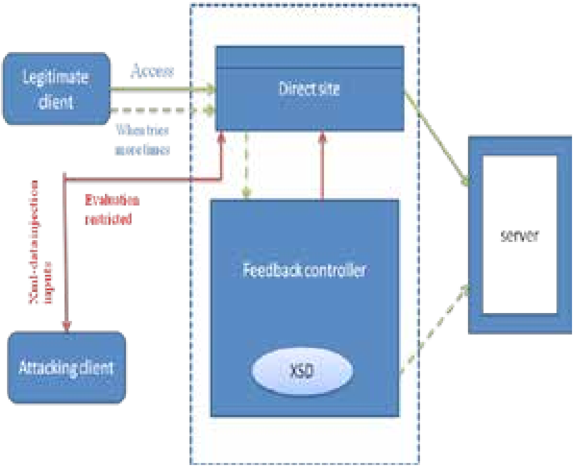

Figure 1: System Architecture

Feed-forward control is also called as anticipative control which is a mechanism that predicts the effects of measured disturbances and takes corrective action to achieve the desired result. In feedback control, the variable being controlled is measured and compared with a target value. This difference between the actual and desired value is called the error. Feedback control manipulates an input to the system to minimize this error. This difference is used to control the system inputs to reduce the error in the system. The feedback control obtains data at the process output. Because of this, the control takes into account unforeseen disturbances such as frictional and pressure losses

PROPOSED TECHNIQUES

XSD technique

XSD (XML Schema Definition), a Recommendation of the World Wide Web Consortium (W3C), specifies how to formally describe the elements in an Extensible Mark-up Language (XML) document. This description can be used to verify that each item of content in a document adheres to the description of the element in which the content is to be placed. XSD provides you with mechanisms to customize the generated type system in the C++/Tree mapping. Common customization examples include:

using a different type for one of the XML Schema built-in types

adding a member function or a data member to a generated type

Adding virtual functions to the base type of a hierarchy and implementing them in the derived types.

XSD provides two command-line options, --custom-type and --custom-type-regex that allow you to specify which types should be customized and how these types will be customized.

Initial Procedure

1. Create a state for each element.
2. Create a separate initial and final state
3. Construct an edge from the initial state to each element name and an edge from each element name.
4. Validate the elements based on the schema defined.

Congestion Participation Rate

A CPR-based approach to detect and filter LDDoS attacks by their intention to congest the network. The major innovation of the CPR-based approach is its ability to identify LDDoS flows. A flow with a CPR higher than a predefined threshold is classified as an LDDoS flow, and consequently all of its packets will be dropped. CPR-based approach is substantially more effective compared to an existing Discrete Fourier Transform (DFT)-based approach - one of the most efficient approaches in detecting LDDoS attacks.

The CPR based approach is used to identify the TCP targeted LDDoS attacks. It is a novel metric approach which denies the fact that TCP flows avoids network congestion and LDDOS induce network congestion. It means that TCP will send fewer packets during network congestion and LDDOS will not reduce the number of packets during network congestion.

Thus the packet number measured here is for the packets sent by a flow to the router. It is normally larger than the number of the packets from the flow that are forwarded by the router, as some of the packets may be dropped due to congestion.

CONCLUSION

By modeling the system under attack as a switched system, we prove the existence of attacks that can drive the system to a state other than the desired state, and then we propose a novel methodology of XSD customization technique to analyze the impact of such attacks on specific feedback control systems and the websites. Also the unauthorized user can be blocked with the help of MAC address and the login address. The legitimate owner of the site can be alerted with any type of message.

REFERENCE

[1 S.-M. Park and M. Humphrey, “Feedback-Controlled Resource Sharing for Predictable eScience,” Proc. IEEE/ACM Int’l Conf. High Performance Computing, Networking, Storage and Analysis (SC ’08), Nov.2008. | [2]] J. Hellerstein, Y. Diao, S. Parekh, and D. Tilbury, Feedback Control of Computing Systems. Hoboken, NJ, USA: Wiley, 2004. | [3] C. Lu et al., “Feedback Utilization Control in Distributed Real-Time Systems with End-to-End Tasks,” IEEE Trans. Parallel and Distributed Systems, vol. 16, no. 6, pp. 550-561, June 2005. | [4] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, “Reduction of quality (RoQ) attacks on dynamic load balancers: Vulnerability assessment and design tradeoffs,” in Proc. 26th IEEE Int. Conf. Comput. Commun., May 2007, pp. 857–865. | [5] G. Loukas and G. Oke, “Protection against denial of service attacks: A survey,” Comput. J., vol. 53, no. 7, pp. 1020–1037, 2010. | [6] Y. Tang, “Countermeasures on application level low-rate denial of service attack,” in Proc. 14th Int. Conf. ICICS, Oct. 2012, pp. 70–80. | [7] Y. Lu, T. Abdelzaher, C. Lu, L. Sha, and X. Liu, “Feedback control with queueing-theoretic prediction for relative delay guarantees in web servers,” in Proc. 19th IEEE RTAS, May 2003, pp. 208–217. |