Journal of Computer Applications ISSN: 0974 – 1925,
Volume-5, Issue EICA2012-4, February 10, 2012

STRAB: Sensing and Tracing Back Attackers Against Encrypted Protocols

Thangarani S
Assistant Professor
Dept of IT,
Angel College of Engineering and Technology
Tirupur

Poornima K
Dept of IT,
Angel College of Engineering and Technology
Tirupur
E-mail: poornimakalimuthu@gmail.Com

Priyadharsini C
Dept of IT,
Angel College of Engineering and Technology
Tirupur
E-mail: priya20c@Gmail.Com

Rathna Rajeswari V
Dept of IT,
Angel College of Engineering and Technology
Tirupur
E-mail: rathna1991@gmail.Com

Abstract- The Uncontrolled Growth Of The Network Based Applications Has Contributed To Enormous Security Leaks. Though The Encrypted Protocols Are Used To Provide Secure Communication, Intrusion Detection Systems (Idss) Are Often Employed To Monitor Network Traffic And Host Activities That May Lead To Unauthorized Accesses And Attacks Against Vulnerable Services. Anomaly Based IDS, It Is A System For Detecting Computers Intrusions And Misuse By Monitoring System Activity And Classifying It As Either Normal Or Anomalous. To Detect And Trace Back Attacks Against Encrypted Protocols, We Use An Anomaly-Based Intrusion Detection System By Using Deliberately Distributed Monitoring Stubs (Mss). The Mss By Monitoring The Encrypted Traffic, Extort Features For Detecting These Attacks And Construct The Network Profile Of The Users. By Detecting Suspicious Activities Due To The Deviations From These Normal Profiles, The Mss Alert The Victim Servers, Which May Then Take Necessary Actions. In Addition To Detecting Attacks, The Mss Can Also Trace Back The Originating Network Of The Attack. We Call Our Unique Approach STRAB Since It Focuses On Both Sensing And Traceback In The MS Level. The Effectiveness Of The Proposed Sensing and Traceback Methods Are Verified Through Extensive Implementation In Internet Datasets.

Keywords *Computer Security, Encryption Algorithm, Cryptographic Protocol, Monitoring Stub(MS), Intrusion Detection System(IDS), DES(Data Encryption Standard).*

I. INTRODUCTION

Cryptographic Protocols Rely Upon Encryption To Provide Secure Communication Between Involved Parties. A Wide Range Of Cryptographic Protocols Are Employed By Popular Applications And Services To Ensure Data Confidentiality, Integrity, And Authentication. For Example, Secure Socket Layer(SSL) And Its Successor Transport Layer Security (TLS) Are Extensively Used To Provide Authentication And Encryption In Order To Transmit Sensitive Data. Secure Shell (SSH) Has Become Highly Popular For Providing

Password-Based Authentication And Remote Logins. Cryptographic Protocols Have Also Been Developed For The Network Level , Such As Ipsec, Which Is Extensively Used In Virtual Private Networks (Vpns). The Purpose Of All These Encrypted Protocols Is To Resist Malicious Intrusions And Eavesdropping. It Is, However, Ironic That The Network Services And Applications Become Vulnerable Once The Underlying Encrypted Protocols Get Compromised. The Functionality Of The Mss In Order To Detect And Trace Back The Attacks Against Cryptographic Protocols Is Then Illustrated In Four Modes, Namely Learning, Sensing, Alert, And Traceback Phases. The Performance Of DTRAB Is Evaluated With The Aid Of Simulations. Due To Difficulties In Obtaining Real Encrypted Traces That Are Rather Sensitive In Nature, This Section Also Demonstrates The Application Of DTRAB For Detecting Nonencrypted Attacks In Internet Datasets. Finally, Section V Concludes The Paper.

II. SENSING ATTACKS AGAINST ENCRYPTED PROTOCOL USING TRIPLE DES

Intrusion Detection Has Been An Active Field Of Research For Over Two Decades, And Most Conventional Idss Operate By Inspecting The Contents Of The Networking Packets. Once Encrypted, The Packet Contents Are Garbled And The Intrusion Detection Systems (Idss) Fail To Recognize Whether The Payloads Are Normal Or Potentially Malicious. Intrusion Detection Systems Can Be Broadly Categorized In Two Ways, Namely Signature-Based And Anomaly Based Detection Techniques. A Signature-Based (Also Known As Rule-Based Or Misuse-Based) IDS Uses Previously Stored Attack Descriptions To Compare If A Portion Of The Monitored Network Packets Is Malicious. Signature Based IDS Monitors Packets In The Network And Compares With Pre-Configured And Pre-Determined Attack Patterns Known As Signatures. The Issue Is That There Will Be Lag Between The New Threat Discovered And Signature Being Applied In IDS For Detecting The Threat. During This Lag Time Your IDS Will Be Unable To Identify The Threat Having Said This, The Signature-Based Detection Schemes Are Inherently Incapable of Detecting Truly Novel Attacks And Suffer From High Rates Of False Alarms When Attack Signatures Match Both Intrusive And Non Intrusive Patterns. The Limitation Is That, It Is Not Uncommon For The Number Of Real Attacks To Be Far Below The False-Alarm Rate. Real Attacks Are Often So Far Below The False-Alarm Rate That They Are Often Missed And Ignored.

On The Other Hand, An Anomaly-Based Intrusion Detection System, Is A System For Detecting Computer Intrusions And Misuse By Monitoring System Activity And Classifying It As Either *Normal* Or *Anomalous*. The Classification Is Based On Heuristics Or Rules, Rather Than Patterns Or Signatures, And Will Detect Any Type Of Misuse That Falls Out Of Normal System Operation. This Is As Opposed To Signature Based. The Primary Strength Of An Anomaly-Based Detection Scheme Is Its Ability To Recognize Novel Attacks. Recent Research Efforts Have Been Devoted Toward Detecting Various Attacks Against Encrypted Protocols Such As SSL/TLS And SSH. For Instance, An Attacker Launching The Infamous Remote Timing Attack Against An Openssl Server Could Extract The Private Key Stored In The Server Within 6 H. All The Attacker Had To Do Was To Measure The Time The Openssl Service Took To Respond To Decryption Queries On A Trial-And-Error Basis. Access Information In Terms Of Data Size And Timing For Every Web Client Was Extracted From The Encrypted Web Traffic By Reconstructing The TCP

Sessions And The Headers Of The Encrypted Sessions. Based On The Low Access Frequency Of Malicious Activities, The Encrypted Traffic Analysis Statistically Detected Rare Events As Anomalies And Reported The Same As Suspicious Attacks.

An Overlay-Based Architecture Called Websos , Comprising Access Points, Beacons, And Servlets, Has Been Conceived To Enable A Web Server To Function Even Under A Dos Attack. The End-To-End Communication Between A Client And The Server Is Secured By SSL Sessions. When An Access-Point Is Attacked, Websos Chooses Another Access Point So That Traffic From Legitimate Clients Can Still Enter The Overlay. On The Other Hand, If A Node Is Under Attack, The Overlay Topology Is Modified By Computing New Paths To Other Nodes In The Overlay. Protomon, An Anomaly-Based IDS For Both Cryptographic And Application-Level Protocols, Includes The Use Of Lightweight Authorized Licensed Protocol Monitors To Detect Deviation From A Previously Constructed Normal Behavior Profile. Protomon Functions In Three Modes, Namely Learn, Sense, And Prevent Modes. First In The Learn Mode, A Monitoring Stub Per Server Constructs Normal Usage Patterns For The Monitored Protocols. In The Sense Mode, Protomon Constantly Compares The Online Observations With The Acceptable Threshold Of Normal Profiles. Once The System Sense An Anomaly, It Switches To The Third And Final Mode, In Which The Monitor Stub Slows Down The Protocol Response So That The Anomaly May Not Go Beyond The Threshold Level.

III. TRACING BACK ATTACKERS AGAINST ENCRYPTED PROTOCOLS

Traceback Approaches Require The Routers To Generate Additional Packets For Each Packet That Passes Through The Routers. The Victim Host Receives Both The Original Packets And These Extra Packets, Which Provide Identification Of The Originating Routing Devices. The Obvious Disadvantage Of This Approach Is An Increase In The Network Traffic. In Order To Deal With This, We Proposes An Extra “Trace-Packet” To Be Generated On A Probabilistic Basis, For Instance Approximately One Trace-Packet For Every 20 000 Packets. One Of The Most Common Techniques To Evade Detection Is The Use Of “Stepping Stones”, Where An Attacker Often Masks His Identity By Launching Attacks From Intermediary Hosts That Were Previously Compromised. This Enables The Attacker To Use A Chain Of Interactive Connections Using Protocols Such As SSH To Dispatch Malicious Commands Over The “Stepping Stone” Chain To Gain Access To The Victim Machine.

It Is, Indeed, Difficult To Trace Back The Trail Of The Attacker Owing To The Sheer Volume As Well As The Chaotic Nature Of The Traffic On The Internet. The Final Victim Can, At Best, See The Traffic From The Last Hop Of The Chain Of The Stepping Stone. In Quest of Tracing A Stream of Attack Packets Through A Number Of “Stepping Stones,” Content-Based Stream-Matching Approaches Came Into Use. One Notable Example Of Such An Approach Is “Thumb-Printing”, Which Shows Good Performance In Tracing Back Stepping-Stone Attacks Involving Nonencrypted Protocols Only. Alternate Approaches Include Correlation Methods Based On Interpacket-Delay (IPD), For Tracing Back Attacks Against Encrypted Connections. IPD Remains As A Distinctive Feature In Normal Interactive Connections That Employ Encrypted Protocols Such As SSH. Blum *Et Al.* Proposed An Algorithm Based On The Distinctive Characteristics Such As Packet Size And

Timing Information Of The Interactive Traffic Rather Than The Packet Contents. Using The Algorithm, It Was Possible To Find Stepping Stones Even When The Traffic Was Encrypted. The Timing-Based Algorithm Performed More Efficiently Compared To The Traditional Context-Based Techniques. Blum *Et Al.* Investigated Not Only The Detection Of Interactive Stepping Stones, But Also Made Attempts To Determine An Algorithmic Bound Over The Detection Approach. The Stepping- Stone Detection Problem Sheds Some Light On The Difficult Ordeal Of Tracing Back Attacks Against Encrypted Protocols.

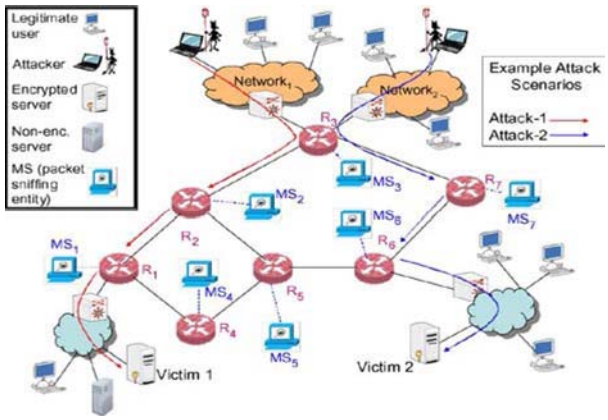

Figure 1: Attack Scenarios

A Number Of Servers Running Services Based On Both Encrypted And Application-Level Protocols. Users From An Untrusted Network Or From The Internet May Connect To Any One Of These Servers. Seven Mss Are Placed Aside The Network Elements. The Mss, By Sniffing, Monitor The Traffic Headers But Do Not Inspect The Payloads. When An Attack Is Launched By A Host (In Network-1), Say From The Untrusted Network To Victim Server 1, , , And Consequently Observe An Influx In Abnormal Protocol Operations Interpreted As An Attack Feature. In The Remainder Of This Section, We Shall Describe How The Mss Effectively Detect Attacks Against Encrypted Protocols And Try To Trace Back The Attacker. Furthermore, By Specifying The Normal Operation Modes And Request-For-Comments (Rfcs) Specifications Of Different Protocols In The MS' Databases, This Approach May Also Be Extended To Detect Attacks Against Standard Application-Level Protocols.

At First, A Client Attempts To Establish A Connection To The Server By Sending A SYN Packet. The Server Acknowledges This By Sending An ACK And A SYN Packet Of Its Own. If The Client Manages To Successfully Log Onto The Server And Wants To Quit, The Client Will Initiate The FIN Packet First. This Is A Normal Mode Of Operation In SSH. On The Contrary, If The Server Initiates The FIN Packet First, It Indicates That The Server Is Shutting Down The Connection Because Of Either An Invalid Attempt To Access The Service Or A Timeout. A MS Monitors Such Connection Flows, And When It Discovers That The Server Is The First Originator Of The FIN Packet Soon After The Connection Attempt, It Recognizes A Deviation In The Protocol's Normal Mode Of Operation And Deems That Event As A "Failed Session.

IV. DATA ENCRYPTION STANDARD

Most Widely Used Block Cipher In The World. Based On The Feistel Cipher Structure With 16 Rounds Of Processing. Block Is 64 Bits And The Key Is 56 Bits. What Is Specific To DES Is The Design Of The F Function And How Round Keys Are Derived From The Main Key. To Achieve High Degree Of Diffusion And Confusion. Diffusion Means Making Each Plaintext Bit Affect As Many Ciphertext Bits As Possible. Confusion Means Making The Relationship Between The Encryption Key And The Ciphertext As Complex As Possible. As A Temporary Solution To DES's Security Problem, One May Encrypt A Message (With DES) Multiple Times Using Multiple Keys 2DES Is Not Much Securer Than The Regular DES. So, 3DES With Either 2 Or 3 Keys Is Used.3 DES Is More Secure And Reliable And Is Used here.

V. PROBLEM DEFINITION

The Sensing Approach Adopted In STRAB Involves Detecting Anomalies. This Relies On Detecting The Point Of Change In The Encrypted Protocol Behavior As Quickly As Possible Under An Attack. For This Purpose, We Employ The Nonparametric Cusum Algorithm, Which Is A Statistical Tool. We Realize That It Is Expensive To Employ The Classical Version Of The Cusum Algorithm And Other Change-Point Detection Algorithms Due To The Manner In Which They Demand To Learn About Statistical Probabilities Of Hypotheses Of The Normal And Abnormal Events *A Priori*. Such Hypotheses Are Referred To As Parameters. This Is Why We Choose To Adopt The Nonparametric Version Of Cusum, Which Is A Lightweight Algorithm Applicable To The Traffic In The Internet, Including The Scope Of Encrypted Traffic. We Employ The Nonparametric Cusum Algorithm At The Mss To Detect Points Of Changes In The Network Behavior At The Advent Of An Anomaly.

VI. CONCLUSION

The Client Knows The Data Loss After It Reached The Intruder Level. Client May Trace Back It But It Is Inefficient, Because It Takes More Time To Trace. The Receiver Checks The Count Of The Packets And Received Packets If It Is Differed Then They Know That Data May Hacked. The Existing System Is Less Flexible, Less Secure And Also Less Compatible. Monitoring Stub Will Helps To Improve The Efficiency Of The Trace Back Mechanism. Behavioral Distance Used To Find Out The Hacking Of Information Before The Data Corrupted Or Updated By The Intruder. The Proposed Detection Scheme Manages To Avoid False Alarms When The Flash Crowd Occurred. It Is Used To Find Out The Hacking Of Information Before The Data Is Hacked By Using DES.

REFERENCES

1. C. E. Landwehr And D. M. Goldschlag, "Security Issues In Networks With Internet Access," Proc. IEEE, Vol. 85, No. 12, Pp. 2034–2051, Dec. 1997.

2. Z. M. Fadlullah, T. Taleb, N. Ansari, K. Hashimoto, Y. Miyake, Y. Nemoto, And N. Kato, "Combating Against Attacks On Encrypted Protocols," In Proc. IEEE ICC, Glasgow, Scotland, Jun. 24–28, 2007, Pp. 1211–1216.
3. J. P. Anderson, Computer Security Threat Monitoring And Surveillance. Fort Washington, PA: Anderson, 1980.
4. Bivens, C. Palagiri, R. Smith, B. Szymanski, And M. Embrechts, "Network-Based Intrusion Detection Using Neural Networks," In Proc. ANNIE, St. Louis, MO, Nov. 2002, Pp. 10–13.
5. Stavrou, D. L. Cook, W. G. Morein, A. D. Keromytis, V. Misra, And D. Rubenstein, "Websos: An Overlay-Based System For Protecting Web Servers From Denial Of Service Attacks," Comput. Netw., Vol. 48,n No. 5, Pp. 781–807, Aug. 2005.
6. K.Poornima, Currently Pursuing Her B.Tech Degree In Information Technology, Anna University, Coimbatore.
7. C.Priyadharsini, Currently Pursuing Her B.Tech Degree In Information Technology, Anna University, Coimbatore.
8. V.Rathna Rajeswari, Currently Pursuing Her B.Tech Degree In Information Technology, Anna University, Coimbatore.