International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Securing the Wireless Network from Jamming Attacks Using Anonymity

T. K. P. Rajagopal, Balaji R, Ravikumar K, Ranjith N. L

Department of Computer Science and Engineering, Kathir College of Engineering, Coimbatore, Tamil Nadu, India

ABSTRACT

Multiple-path source routing protocols allow a data source node to distribute traffic to available paths. We consider the problem of problem-free source routing, in which the source node carries out a traffic allocation based on empirical statistics on individual network nodes. This reduces the efficiency of the blocking attack. In the traditional system, a reactive jammer blocks wireless channels only when sending targets; compared to constant interfering, reactive jamming is more difficult to track and compensate. The transmission of messages by the use of the reaction time of a reactive jamming transmitter. It does not accept a reactive jammer with limited range and transmission power and can therefore be used in scenarios where traditional approaches fail. In this paper, we are investigating the ability of network nodes to characterize the congestion and ability of multiple source nodes to compensate for blocking in the allocation of traffic over multiple routing paths. We formulate the problem of allocating traffic across multiple routing paths in the presence of jamming as a loss-rich network flow optimization problem. We model the problem as a Bayesian game for a single time slot attack and reduce it to solving linear programming problems (LP). We show that in multisource networks, this central optimization problem can be solved with an anti-jamming technique. Finally, we simulate the achievable throughput using our proposed traffic allocation method in several scenarios. We formulate the central traffic distribution problem for several source nodes as a convex optimization problem. We show that the multisource multipath optimal traffic allocation at the source nodes can be calculated using an anti-jamming technique.

Keywords : IMPROVED IDENTITY ATTACKS, IDAS, XML, DIDAS, RePIDAS, LP

I. INTRODUCTION

Wireless networks are vulnerable to sybil attacks due to the broadcast nature of the wireless medium. Location distinction can tell whether or not all identities are originated from the same location, and thus detect such attacks. In wireless networks, location distinction aims to detect location changes or facilitate authentication of wireless users. The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in networks.

In networks, the identity is used as an abstraction so that a remote entity can be aware of identities without necessarily knowing the correspondence of identities to local entities. Wireless signals sent from different locations, the receiver can observe different channel characteristics from these signals

An IDENTITY ATTACKS detection system (IDAS) is an active process or device that analyzes system and network activity for unauthorized entry or malicious activity. The ultimate aim of any IDAS is to catch perpetrators in the act before they do real damage to resources. An IDAS protects a system from attack, misuse, and compromise. It can also monitor network activity, audit network and system configurations for vulnerabilities, analyze data integrity, and more.

A host-based IDAS monitor the detailed activity of a particular host in real-time. The system call traces produced by an auditing mechanism such as the Solaris Basic Security Module (BSM) typically provides the

IDAS with the data needed to search for attack signatures. When an analysis of the BSM data shows signs of an IDENTITY ATTACK, the IDAS alerts the system administrator of an attack. Host-based detection systems can detect attacks that network-based detection cannot see. Attacks that are made at the keyboard of a critical machine do not travel across the network. More information, including machine and process state, is available for host-based methods enabling coordination of multiple data sources in detection.

Distributed IDENTITY ATTACKS Detection System (DIDAS) which generalizes the target environment in order to monitor multiple hosts connected via a network as well as the network itself. The DIDAS components include the DIDAS director, a single host monitor per host, and a single LAN monitor for each LAN segment of the monitored network. The information gathered by these distributed components is transported to, and analyzed at, a central location, thus providing the capability to aggregate information from different sources.

The insights developed in automata theory had a strong impact on numerous scientific areas. Standard applications include pattern matching, syntax analysis, foundations of XML, and hardware and software verification. In recent years, novel applications have emerged from biology, physics, cognitive sciences, neurosciences, control, tomography, linguistics, mathematics, etc. The new developments in information technology have increased the need for formally-based design and verification methods to cope with emerging technical challenges in network security, electronic business, mobile intelligent devices, and high performance computing.

II. METHODS AND MATERIAL

RELATED WORK

Cong Liu and Jie Wu in the year 2011, [] proposed and evaluated a dual Finite Automaton. The dual FA consists of a linear finite automaton (LFA) and an extended deterministic finite automaton (EDFA).It focus on deep packet inspection algorithms in network IDENTITY ATTACKS detection and prevention systems. Inspection programs based on regular expressions are typically implemented by two classic finite automata, non-deterministic finite automata (NFA) and deterministic finite automata (DFA)

Aruna Jamdagni, Zhiyuan Tan, Xiangjian He, Priyadarsi Nanda , Ren Ping Liu in the year October 2012, [2] propose a 3-Tier Iterative Feature Selection Engine (IFSEng) for feature subspace selection and a novel Real-time Payload-based IDENTITY ATTACKS Detection System (RePIDAS) that integrates a 3-Tier IFSEng and the MDM approach. The traffic for Web-based application is considered for validating our model.

SangKyun Yun, Member, IEEE Computer Societyin the year February 2012, proposes a state encoding scheme called a covered state encoding for the efficient TCAM-based implementation of the Aho-Corasick multipattern matching algorithm, which is widely used in network IDENTITY ATTACKS detection systems. System also proposes constructing the modified Aho-Corasick NFA for multicharacter processing, which can be implemented on a TCAM using the covered state encoding.

Yi-Hua Edward Yang and Viktor K. Prasanna in the year July 2012 implemented a dictionary-based string pattern matching (SPM) as Aho-Corasick deterministic finite automaton (AC-DFA). It proposed a head-body finite automaton (HBFA) which implements SPM in two parts, a head DFA (H-DFA) and a body NFA (B-NFA). A branch grafting mechanism is proposed to opportunistically advance the state of the H-DFA with the matching progress in the BNFA.

Sailesh Kumar, Sarang Dharmapurikar, Fang Yu, Patrick Crowley and Jonathan Turner in the year 2006, [13] explained about the deep packet ,which requires multiple default transitions to consume a single character .Careful implementation is required to ensure good, deterministic performance. Embedded memories provide ample bandwidth. Further space reductions are possible by splitting the regular expressions into multiple groups.

Michela Becchi and Patrick Crowley in the year 2007, [9] explained the key characteristics of a hybrid-FA, a modest memory storage requirement comparable to those of an NFA solution, an average case memory bandwidth requirement similar to that of a single DFA solution. Hybrid-FA is capable of evaluating all the regular-expression types found in common NIDAS can be implemented efficiently in practical high-speed systems.

EXISTING SYSTEM

The key idea of the discovered attack is to create a virtual multipath channel as undetectable camouflage to make the receiver believe a specified channel characteristic chosen by the attacker. Virtual multipath attackers are able to make the receiver believe any channel characteristic the attacker chooses. At the receiver, it seems that there is no way to tell whether the signal goes through real or virtual multipath scenario. The detection technique that utilizes an auxiliary receiver or antenna to identify these fake channel characteristics.

Policy Script Interpreter: The Policy Script Interpreter takes the high-level events generated by the Event Engine and compares these with the policy scripts in the system. The events are sorted in a FIFO list which means the first that comes along are the first that is processes. Policy Script Interpreter takes action if it detects any suspicious and dangerous actions or it discards other events not defined in the policy scripts. Traffic that seems like attacks but aren't (false negatives), can be detected at this point, but if the policy scripts are good, this will be minimal. It is written in Bro language.

The distributed and collaborative architecture has a rule that every node in the MANET must participate in IDENTITY ATTACKS detection and response by having an IDAS agent running on them. The IDAS agent is responsible for detecting and collecting local events and data to identify possible IDENTITY ATTACKs, as well as initiating a response independently.

The hierarchical architecture is an extended version of the distributed and collaborative IDAS architecture. This architecture proposes using multi-layered network infrastructures where the network is divided into clusters. The architecture has cluster heads, in some sense, act as control points which are similar to switches, routers, or gate ways in wired networks.

The mobile agent for IDAS architecture uses mobile agents to perform specific task on a nodes behalf the owner of the agents. This architecture allows the distribution of the IDENTITY ATTACKS detection tasks. There are several advantages using mobile agents for IDENTITY ATTACKS detection.

A Local IDENTITY ATTACKS Detection System (LIDAS) is implemented on every node for local concern, which can be extended for global concern by cooperating with other LIDAS. Two types of data are exchanged among LIDAS: security data (to obtain complementary information from collaborating nodes) and IDENTITY ATTACKS alerts (to inform others of locally detected IDENTITY ATTACK). In order to analyze the possible IDENTITY ATTACK, data must be obtained from what the LIDAS detect on, along with additional information from other nodes. Other LIDAS might be run on different operating systems or use data from different activities such as system, application, or network activities; therefore, the format of this raw data might be different, which makes it hard for LIDAS to analyze. However, such difficulties can be solved by using Simple Network Management Protocol (SNMP) data located in Management Information Base (MIBs) as an audit data source. Such a data source not only eliminates those difficulties, but also reduces the increase in using additional resources to collect audit data if an SNMP agent is already run on each node. For the methodology of detection, Local IDAS Agent can use either anomaly or misuse detection. However, the combination of two mechanisms will offer the better model. Once the local IDENTITY ATTACKS is detected, the LIDAS initiate a response and inform the other nodes in the network. Upon receiving an alert,the LIDAS can protect itself against the IDENTITY ATTACK.

III. RESULTS AND DISCUSSION

Proposed System

The key idea of the discovered attack is to create a virtual multipath channel as undetectable camouflage to make the receiver believe a specified channel characteristic chosen by the attacker. Virtual multipath attackers are able to make the receiver believe any channel characteristic the attacker chooses. At the receiver, it seems that there is no way to tell whether the signal goes through real or virtual multipath scenario. The detection technique that utilizes an auxiliary receiver or antenna to identify these fake channel characteristics.

In our proposed system we model a new robust approach based on physical layer security. In our system periodically monitors nodes behavior and elect leader based on rating value of each node. The selected leader nodes are become monitor node. These nodes start maintaining database about nodes behavior, and verify its rating value with the fixed threshold value. If the rating value is become very low compare to threshold than nodes are classified as malicious misbehavior nodes.

Leader nodes send periodical announcement about the malicious nodes. The leader node maintains blacklist about the misbehavior nodes. The misbehavior nodes eliminated from network once it identified as an attacker nodes.

It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these IDENTITY ATTACKS attempts so that action may be taken to repair the damage later.

A simple firewall can no longer provide enough security as in the past. Today's corporations are drafting intricate security policies whose enforcement requires the use of multiple systems, both proactive and reactive (and often multi-layered and highly redundant). The premise behind IDENTITY ATTACKS detection systems is simple: Deploy a set of agents to inspect network traffic and look for the “signatures” of known network attacks. However, the evolution of network computing and the awesome availability of the Internet have complicated this concept somewhat. With the advent of Distributed Denial of Service (DDOS) attacks, which are often launched from hundreds of separate sources, the traffic source no longer provides reliable temporal clues that an attack is in progress. Worse yet, the task of responding to such attacks is further complicated by the diversity of the source systems, and especially by the geographically distributed nature of most attacks.

These systems are modeled in such a way as to separate the rule matching phase from the action phase. The matching is done according to audit trail events. IDES follows a hybrid IDENTITY ATTACKS detection technique consisting of a misuse detection component as well as an anomaly detection component. The anomaly detector is based on the statistical approach, and it flags events as intrusive if they are largely deviant from the expected behavior. To do this, it builds user profiles based on many different criteria (more than 30 criteria, including CPU and I/O usage, commands used, local network activity, system errors etc.). These profiles are updated at periodic intervals. The expert system misuse detection component encodes known IDENTITY ATTACKS scenarios and attack patterns (bugs in old versions of send mail could be one vulnerability). The rule database can be changed for different systems.

Data communicated via the Secure Communication Module will need to be encrypted in order to ensure that the data received by an IDAS agent is accurate and has not been tampered with. The Secure Communication module is only used by IDAS agents and does not communicate any other type of information between nodes. It must share the bandwidth that the mobile device uses for normal data transmission, so it is required to be efficient, and can only use the amount of bandwidth in needs.

Also, the Secure Communication module must process information coming to the IDAS agent from other agents in the network. For this reason, it must be fast and efficient, so as not to take away from the processing time of the mobile unit.

The Secure Communication Module is necessary to enable an IDAS agent to communicate with other IDAS agents on other nodes. It will allow the MDM s and ADM s to use cooperative algorithms to detect IDENTITY ATTACKs. It may also be used to initiate a global response when an IDAS agent or a group of IDAS agents detects an IDENTITY ATTACK. Basically, any communication that needs to occur from one IDAS agent to another will use the Secure Communication Module.

The LID is a local database that warehouses all information necessary for the IDAS agent, such as the signature files of known attacks, the established patterns of users on the network, and the normal traffic flow of the network. The Anomaly Detection Modules and Misuse Detection Modules communicate directly with the LID to determine if an IDENTITY ATTACKS is taking place.

Each agent must constantly check the audit data to decide that an IDENTITY ATTACKS is not taking place. The Local Audit Trial will consist of specific items out of the network traffic as well as user commands to the node. The Local Audit Trial is responsible for selecting only the items it needs out of the network traffic and system audit data in order to minimize the size of the audit data collected. A audit data is collected by the Local Audit Trial, it is passed to the Misuse Detection Modules and the Anomaly Detection Modules for further analysis. The Local Audit Trial is only responsible for gathering and storing audit data, not processing it.

IV.CONCLUSION

Encryption-based packet protection is energy consuming for battery-powered devices. The showed scheme that selective encryption allows to save energy and to detect attack begin and end. We also showed how the number of encrypted packets can be adapted according to the presence of the attack so that more energy is used only when needed. Since packet transmission consumes energy, adapt transmission rate to instantaneous control performance. The IMPROVED IDENTITY ATTACKS DETECTION SYSTEM using payload and rate mechanism identifies misbehavior nodes and isolates it from the network. In the scheme the IDAS value is estimated are constructed to identify the malicious misbehavior node from the network. Once the misbehavior classification is success then these nodes are isolated from the network.

V. REFERENCES

[1]. Anat Bremler-Barr, David Hay, Yaron Koral (2010),"CompactDFA: Generic State Machine Compression for Scalable Pattern Matching". IEEE INFOCOM Computer Architecture Lett., vol. 7, pp. 33–36.

[2]. Aruna Jamdagni, Zhiyuan Tan, Xiangjian He, Priyadarsi Nanda , Ren Ping Liu (October 2012), "RePIDAS: A multitier Real-time Payload-based IDENTITY ATTACKS Detection System",Centre for Innovation in IT Services and Applications (iNEXT), University of Technology, Sydney, Australia. http://dx.doi.org/10.1016/j.comnet.2012.10.002, Vol. 2, Issue 2, pp.25-39

[3]. Christopher R. Clark and David E. Schimmel (2003) "Efficient Reconfigurable Logic Circuits for Matching Complex Network IDENTITY ATTACKS Detection Patterns". In Proceedings of International Conference on Field-Programmable Logic and Applications (FPL), Lisbon, Portugal. Vol. 2778, pp 956-959.

[4]. Cong Liu and Jie Wu (2011),"Fast Deep Packet Inspection with a Dual Finite Automata", IEEE Transactions on Computers.

[5]. Fang Yu, Zhifeng Chen, Yanlei Diao, Lakshman T.V and Randy H. Katz (2006) "Fast and Memory-Efficient Regular Expression Matching for Deep Packet Inspection", San Jose, California, USA, pp 1-10.

[6]. Hopcroft J. E. and Ullman J. D. (1979) "Introduction to Automata Theory". Addison Wesley.

[7]. Kedar Namjoshi and Girija Narlikar (2010) ,"Robust and Fast Pattern Matching for IDENTITY ATTACKS Detection". In Proc. of IEEE, Vol.3, pp 740-748.

[8]. Lin Tan and Timothy Sherwood (2005),"A High Throughput String Matching Architecture for IDENTITY ATTACKS Detection and Prevention". In Proc. of ISCA, Vol. 18, pp. 93-102.

[9]. Martin Roesch (1999),"Snort: Lightweight IDENTITY ATTACKS Detection for Networks", In Proceedings of LISA '99: 13th Systems Administration Conference Seattle, Washington, USA, November 7–12. Snort: http://www.Snort.org/.

[10]. Masanori Bando, N.Sertac Artan, and H.Jonathan Chao (June 2012), "Scalable Lookahead Regular Expression Detection System for Deep Packet Inspection", IEEE/ACM Transactions On Networking, Vol. 20, No. 3, pp. 699 - 714.

[11]. Mehmet Altinel and Michael J. Franklin (2000),"Efficient Filtering of XML Documents for Selective Dissemination of Information". In Proc. of VLDB Conference.vol.8, pp.53-64.

[12]. Michela Becchi and Patrick Crowley (2007),"A Hybrid Finite Automaton for Practical Deep Packet Inspection". In Proc. of CONEXT, MO 63130-4899+1-314-935-4306.

[13]. Nathan Tuck, Timothy Sherwood, Brad Calder, George Varghese (2004),"Deterministic Memory-Efficient String Matching Algorithms for IDENTITY ATTACKS Detection". In Proc. of IEEE INFOCOM, Vol. 33, pp.333-343.

[14]. Rafael Antonello, Stenio Fernandes, Carlos Kamienski, Djamel Sadok and Judith Kelner (November 2012), "Deep packet inspection tools and techniques in commodity platforms: Challenges and trends" , Journal of Network and Computer Applications, Vol. 35, No. 6, pp. 1863-1878.

[15]. Randy Smith, Cristian Estan, Somesh Jha, Shijin Kong (2008),"Deflating the big bang: fast and scalable deep packet Inspection with extended finite automata" August 17–22, Seattle, Washington, USA. LNCS 5352, pp. 158–172.

[16]. Reetinder Sindhu and Viktor K.Prasanna (2001),"Fast Regular Expression Matching Using FPGAs". Contract no.DABT63-99-1-0004, In Proc. of FCCM, Volume 22, pp. 66–74.

[17]. Sailesh Kumar, Sarang Dharmapurikar, Fang Yu, Patrick Crowley, Jonathan Turner (2006),"Algorithms to Accelerate Multiple Regular Expressions Matching for Deep Packet Inspection". In Proc. of ACM SIGCOMM, pp-339-350.

[18]. Salvatore Pontarelli, Giuseppe Bianchi, Simone Teofili(May 2012), "Traffic-aware Design of a High Speed FPGA Network IDENTITY ATTACKS Detection System", Consorzio Nazionale InterUniversitario per le Telecomunicazioni (CNIT) University of Rome "Tor Vergata" Via del Politecnico 1, 00133, Rome, ITALY,Vol-pp,Issue-99,pp.-13.

[19]. SangKyun Yun, Member, IEEE Computer Society(February 2012), "An Efficient TCAM-Based Implementation of Multipattern Matching Using Covered State Encoding", IEEE Transactions On Computers, Vol. 61, No. 2, pp.213-221.

[20]. Shijin Kong, Randy Smith, Cristian Estan (2008),"Efficient Signature Matching With Multiple Alphabet Compression Tables". In Proc. of Secure communication,Vol. 6307,pp.58-78.