BLAZE: A MOBILE AGENT PARADIGM FOR VOIP INTRUSION DETECTION SYSTEMS

Kapil Singh, Son Vuong
University of British Columbia,Vancouver, Canada

Keywords: Intrusion Detection, Voice over IP, RTP, Megaco

Abstract: IP telephony—also known as Voice over IP or VoIP—is becoming a key driver in the evolution of voice communications. VoIP technology is useful not only for phones but also as a broad application platform enabling voice interactions on devices such as PCs, mobile handhelds, and many other application devices where voice communication is an important feature. As the popularity of the VoIP systems increases, they are fast becoming a subject of a variety of intrusions. Some of these attacks are specific to VoIP systems, while others are general attacks on network traffic. In this paper, we propose an intrusion detection system framework for VoIP applications, called BLAZE. BLAZE has the capability to detect a variety of already known attacks, including Denial-of-Service attacks and media stream attacks and is novel enough to detect new attacks. It uses the mobile agent framework for collection and correlation of events among various network elements. The biggest advantage of using mobile agents in this framework is that we are not required to develop any new protocol for the intrusion detection support. Also, the functionality to perform the required recovery can be dynamically added to the mobile agents without changing the underlying VoIP protocols. We also present the concept of developing user profiles based on the user's call behaviour. These profiles form the baseline against which any future behaviour of the user can be mapped to detect any new attack.

1 INTRODUCTION

With the rapid expansion of computer networks during the past few years, transferring voice over the data network has gained quick popularity. Voice over Internet Protocol (VoIP) is a rapidly emerging technology for voice communication that uses the ubiquity of IP-based networks to deploy VoIP-enabled devices in enterprise and home environments. VoIP-enabled devices, such as desktop and mobile IP phones and gateways, decrease the cost of voice and data communication, enhance existing features, and add compelling new telephony features and services. VoIP systems are projected as the technology of the future for transmitting voice traffic over IP networks. VoIP applications have grown rapidly and continue to enjoy exponential growth. According to the 2003 report of InStat/MDR Research, US customers of IP telephony in 2007 will be five times more than the estimate of 1.08 million in 2002, and the business users will increase by nearly ten times from the estimate of 0.26 million in these 5 years (Vuong, 2003).

As the popularity of the VoIP systems increases, they are fast becoming a subject of a variety of intrusions. Some of these attacks are specific to VoIP systems, while others are general attacks for network traffic. A considerable amount of research has been done in the field of intrusion detection systems (IDS) to develop security solutions for different components of the network infrastructure. IDS are the last line of defense against computer attacks behind firewalls, secure architecture design, secure program design, carefully configured network services and penetration audits. In spite of the availability of a large variety of intrusion prevention techniques, the intrusion problem still remains challenging as there is no fool-proof way of reading the attacker's mind and the attackers are still successful in finding system loopholes in order to compromise the system resources. However, most computer attacks are made possible due to poorly configured services or bugs in the software.

Intrusion detection methods are broadly classified into two categories: misuse detection and anomaly detection. Misuse detection methods, also known as signature-based detection, use information

Singh K. and Vuong S. (2004).
BLAZE: A MOBILE AGENT PARADIGM FOR VOIP INTRUSION DETECTION SYSTEMS.
In *Proceedings of the First International Conference on E-Business and Telecommunication Networks*, pages 238-245
DOI: 10.5220/0001406002380245

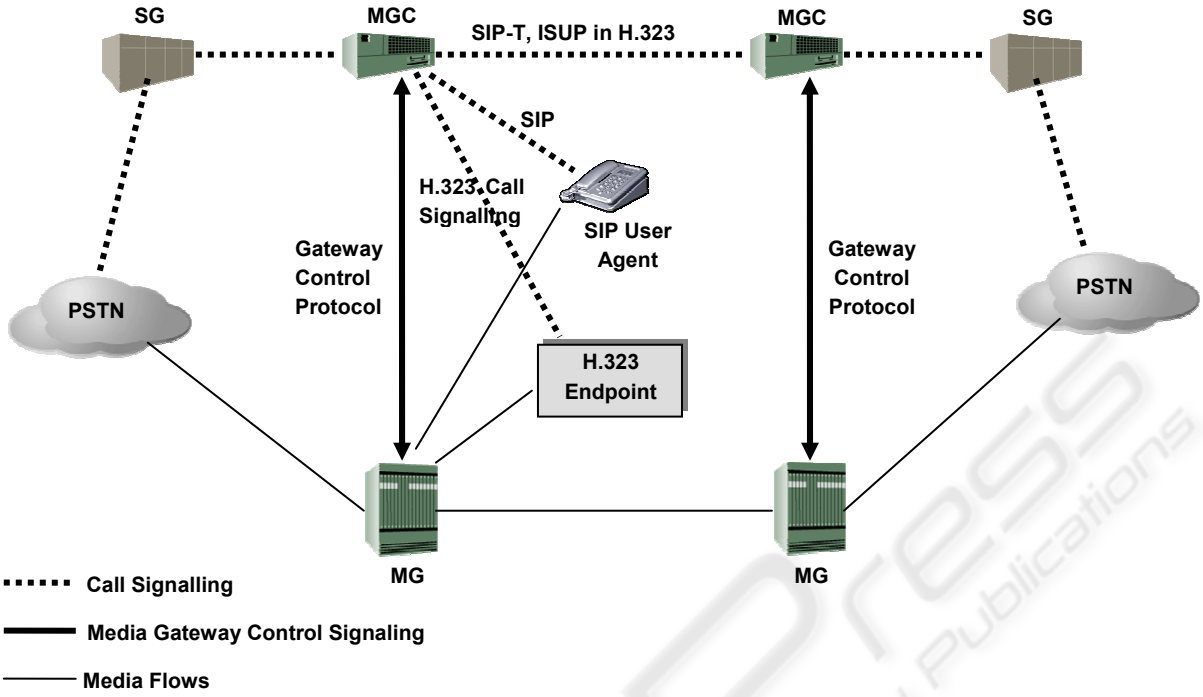

Figure1: Overview of VoIP protocols

about a known security policy, known vulnerabilities and known attacks on the systems they monitor. This approach compares network activity or system audited data against a database of known attack signatures or other misuse indicators, where pattern matches produce alarms of various sorts. A lot of work is being done by researchers to find intelligent ways to map the dynamically changing attack patterns to known attacks. On the other hand, anomaly detection methods, also called behaviour-based intrusion detection, use information about repetitive and usual behaviour on systems and attempt to detect intrusions by detecting significant departures from normal behaviour.

Many IDS tools are available in the market that can detect general IP network intrusions. For example, Snort (Roesch, 1999) is a network-based IDS that can log network traffic; Ethereal (Orebaugh, 2004) can provide the application-level view of that network traffic; and some host-based tools like The Coroner's Toolkit (Farmer, 2000) can summarize the time at which files were last modified, accessed, created and even can recover deleted files. VoIP systems pose several challenges for IDS design. First, these systems use multiple protocols for call signaling and data delivery. Second, the components of the system are distributed in nature making it difficult for an IDS to have a centralized view of the situation in case of a distributed attack. Third, the systems are heterogeneous and the components can be under different domains having different security and billing policies. Finally, there is a large range of attacks specific to such systems such as denial of service attack or billing fraud attack.

In this paper, we propose a novel IDS architecture for VoIP based on mobile agent technology. This architecture delegates the task of making user profiles to mobile agents and any major deviation from user's normal behavior can be flagged as anomaly.

The rest of the paper is organised as follows. Section 2 gives an overview of some VoIP protocols and some general information about mobile agents relevant to our context. Section 3 gives a list of out design objectives. Section 4 presents the architecture for our system. Section 5 presents the implementation of our system and analysis of the system in view of some kinds of attacks scenarios specific to VoIP systems. Section 6 reviews the related work followed by conclusions in Section 7.

2 BACKGROUND

2.1 VoIP protocols overview

IP telephony — also known as voice over IP or VoIP — is becoming a key driver in the evolution of voice communications. VoIP technology is useful not only for phones but also as a broad application platform enabling voice interactions on devices such as PCs, mobile handhelds, and many vertical-specific application devices where voice communication is an important feature.

VoIP traffic over the internet is composed of the signalling protocols and the media transfer protocols. Of all the protocols developed over the years, two have found worldwide acceptance: H.323 (ITU-T, 1998) and SIP (Handley, 1999). H.323 puts all the signalling intelligence in the core of the network keeping the endpoints simple. On the other hand, SIP requires the User Agents at the endpoints to handle the signalling process. Both H.323 and SIP provides for call setup, management and media delivery. The endpoints, which may be physical phones or software entities, send and receive RTP packets over UDP/IP that contain encoded voice conversations. While H.323 uses a set of complex protocols for call setup and management, SIP relies on much simpler set of request messages. Due to its simple design and implementation, SIP is increasing in popularity, but still H.323 is the most widely deployed standard.

Since voice traffic can flow between the IP network and the Public Switched Telephone Network (PSTN), gateways are needed to perform translation between the two networks. Such gateways implement media gateway management protocols such as MGCP (Arango, 1999) and Megaco/H.248 (Cuervo, 2000). Figure 1 shows a converged VoIP network architecture. H.323 and SIP still remain the base protocols for call management, while Megaco is the protocol between the Media Gateway Controller (MGC) and the Media Gateway (MG). Unlike H.323 or SIP which uses a peer-to-peer architecture, Megaco adopts a master/slave architecture for distributed gateways, in which MGC is the master server and MGs are the slave clients. The MG terminates PSTN lines and packetizes media streams for IP transport. The MGC coordinates setup, handing and termination of media flows at the MG. The endpoints could be a PSTN phone, a SIP phone or an H.323 endpoint.

2.1.1 Vulnerabilities in VoIP system

IP telephony-related protocols were not designed with security as prime design goal. However, some of these protocols have added security features in their recent versions. Unfortunately, the security mechanisms offered by these protocols are not secure enough or are impractical and hence failed to achieve worldwide acceptance. It makes it possible for the attacker to easily forge a packet to launch attacks such as call hijacking, terminating the calls abnormally, or toll frauds. Furthermore, denial-of-service attacks on MGs or misbehaving MGCs are unavoidable.

Apart from the aforementioned security problems in signalling, media security is another issue. Though some protocols allow for encryption of the media stream, but this solution introduces extra delay for encryption and decryption. It is, therefore, not very applicable for VoIP applications because they are delay and case-sensitive. In absence of such security mechanism, the packets can be easily captured and replayed. Also, any garbage media packets can be directed to the IP address and UDP port used by the connection. The attacker can also fake his/her identity by changing the source of the RTP packets by changing their header.

2.2 Log correlation using mobile agents

Log correlation refers to the process by which an IDS combines data captured by multiple sensors, or the same sensor at different points in time, and tries to extract significant and broad patterns. A similar type of attack detected at different points in time, for example, may indicate an automated, coordinated attack. In general, the more data that can be collected related to a specific event, the easier it is for a security administrator to respond in an effective manner.

The conventional approach to the log correlation process involves the collection of distributed sensor data into a central location, and the application of searching and data aggregation techniques to discover patterns. In the context of intrusion detection, one of the major advantages of the mobile agent paradigm is the simple model it offers for distributing computational tasks. Instead of following the centralized approach, a mobile agent-based IDS uses agents with analysis capabilities to perform queries and searches remotely. This is commonly known as the remote evaluation technique, which saves bandwidth by taking advantage of the difference in size between the data being analyzed, and the code (the analysis agent) needed to perform the analysis.

2.3 Making User Profiles

The primary problem in detecting anomalous behavior is to determine what constitutes a normal behavior. The motivation behind user-based approach is the belief that the user leaves a 'print' while using the VoIP system. Different machine learning mechanisms can be used to learn this print and identify each user much like using fingerprints to identify the culprit at the crime scene. For IP telephony usage, different users tend to exhibit different call behavior, depending on the requirements. Some prefer calls during the day, while others prefer talking in the nights. Even two users that prefer the same call time may not have the same call trends. For e.g., some make a lot of long distance calls, while others talk locally most of the time. In computer systems security, user profiles have been built based on characteristics such as resources consumed, typing rate, login location, counts of particular commands (Denning, 1987; Smaha, 1988; Lunt, 1990; Frank, 1994). Also, other approaches use causal behavior of human/computer interaction, i.e., based on the idea that a user has a goal to achieve when using the computer, which causes the person to issue certain commands, causing the computer to act in a certain manner. Some characteristics that have been modeled based on the causal behavior are the sequence of commands, distribution of a user's commands over a period of time.

All these user-based techniques are based on building user profiles for individual users as the task of characterizing regular patterns in the behavior of an individual user is an easier task than trying to do it for all users simultaneously. For our system, we use the time of call and call duration as the basis of making user profiles. This requires collecting data for each new user over a period of time and then using that data to make our system learn the user call behavior.

3 DESIGN OBJECTIVES

In our work we aim to develop an IDS system for VoIP environments that has the following characteristics:

- The system should be able to detect normal network traffic attacks as well as the attacks specific to VoIP.
- Intrusion detection should not only include attacks specific to one VoIP protocol, but should also be able to detect intelligent attacks that are distributed across multiple protocols.
- The system should be able to detect both known attacks as well as new, novel attacks.
- Similar type of information from distributed network elements should be combined to give a broader view of a distributed attack on the system.
- The whole detection process should be protocol independent i.e. no change should be needed to the existing VoIP protocols. Also, no new protocol should be defined.
- Data collection and analysis tasks are distributed, allowing for efficient usage of computing resources, as well as minimal bandwidth overhead.

4 SYSTEM ARCHITECTURE

Figure 2 shows the various components of BLAZE. The network flow is passed through the *Packet Filter* that separates out the incoming packets into different protocol streams or signatures. Basically, Packet Filter is responsible for fragmentation, reassembly of IP packets and generating the protocol dependent signatures as the result. For example, a sample signature could be a stream of SIP messages or RTP packets.

The *Event Generator* forms the events from these signatures based on a predefined set of rules. An event is an indication of an attempted intrusion. For example, an incorrectly formatted SIP packet received in the SIP signature stream is a description of an intrusive event, as it describes the attempt to exploit the vulnerability in the SIP proxy.

The *Event Correlation* reports significant related/repeated events instead of individual occurrences. It triggers an alarm when an intrusion detection rule is met. For example, three possible attack events can be (i) an incorrectly formatted SIP message; (ii) an accounting transaction that does not have a corresponding call initialization message; (iii) the source or destination IP address of the RTP packet does not match that of the SIP packet. A typical billing fraud attack can be detected correlating the three events. It is clear that relying on these events individually as the trigger for the billing fraud might generate false alarms. Thus, correlation of the relevant events significantly reduces the number of false positives and gives a better view of the attack scenario in case of a coordinated, distributed attack. Finally, the alarm is created and is sent to the relevant network component by the *Alarm Generator*.

The heart of our IDS design is the *Policy Engine*. This component provides the set of rules to the

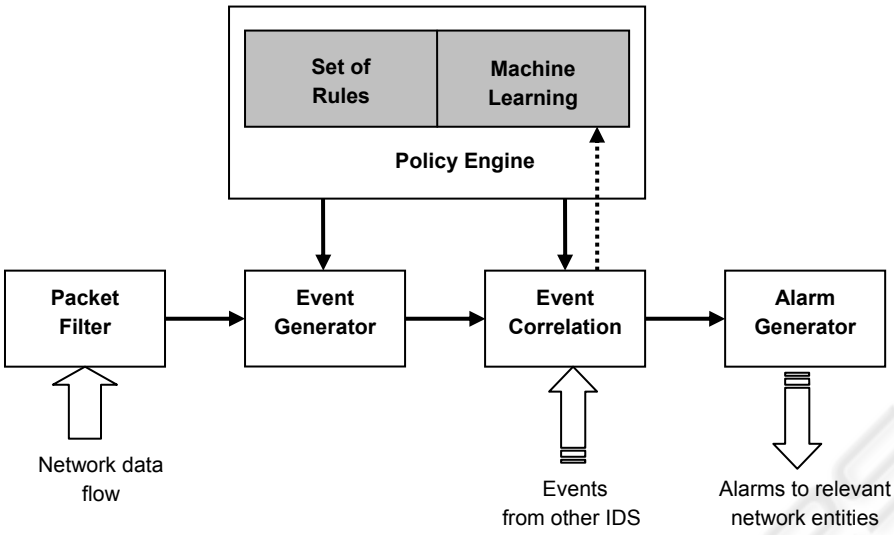

Figure 2. System Architecture for BLAZE

Event Generator and the Event Correlation for detecting the intrusion. Apart from having pre-defined set of rules for typical VoIP attacks, it is responsible for making the user profiles and dynamically generates the set of rules for that user. For example, user A's profile shows that all calls made by user A are typically shorter than 30 minutes. Then the *Machine Learning* component of the Policy Engine can generate a rule that any calls longer than 1 hour made by user A should be further investigated. This clearly has an advantage over the hard coded set of rules in terms of determining new attacks.

Detection of some distributed attacks requires coordination between different IDS deployed at different VoIP components. An event generated at one network entity could be useful to detect an intrusion at some other entity. This distributed event data collection and correlation is done by mobile agents. Mobile agents are protocol independent entities and hence we use them for sending the generated alarm to relevant VoIP network component. The corresponding required recovery tasks are also done by the agents.

5 PROTOTYPE

5.1 Rule-based Attack Scenarios

As part of our analysis, we have investigated few possible attacks and tried to determine the possible detection policies in such scenarios. Two of these attacks demonstrate the vulnerabilities in the signalling protocol while one is a media flow attack.

5.1.1 Service tear-down attack

In this scenario, we have two users X and Y and one attacker (Figure 3). We also have two sets of MGC and MG, one each for the two user ends for making the VoIP call. This attack is targeted to tear down the connection prematurely, thus resulting in a Denial-of-Service attack. As seen in Figure 3, User X is having a conversation with User Y. At this time, the attacker sends a fake BYE message to the MGC, requesting to end the call from the end of User X. So, User Y will stop sending RTP packets immediately, while User X will continue to send the packets to the MG, since User X has no idea that the connection has been terminated.

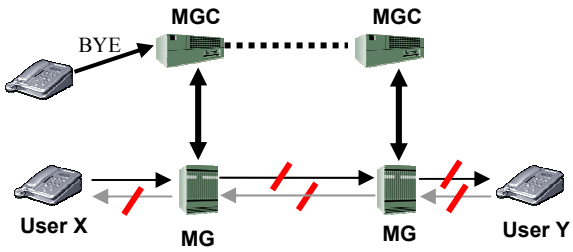

Figure 3. Service tear-down attack

Service tear-down attack can be detected at the MG. If the connection is stopped by User X, then the MG should not receive the RTP flow from User X after receiving the BYE message at the MGC. Therefore, a rule is created in the IDS that signals an alarm if any new RTP packets are received by the MG from User X after MGC has already seen the

BYE message from the same user. Specifically, a Service tear-down attack can be detected by looking for orphaned RTP flow at the MG.

5.1.2 Call Hijacking

In Call Hijacking attack, the attacker can redirect the RTP media stream that is supposed to go to User X to another location, usually the IP address of the attacker machine. In order to launch this attack, the attacker, faking as User X, sends a REINVITE message to the MGC (Figure 4). The REINVITE message is used for call migration when a user wants to change his/her end point location. For example, the user might want to transfer the call from one landline phone to another, or to even a mobile phone. The consequence of this attack would be that user X will not be able to receive the packets from User Y and hence would experience a continued silence. This attack results in serious breach of privacy for User Y, as the attacker is able to listen what User Y is saying.

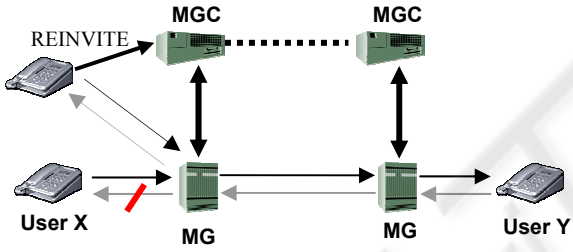

Figure 4: Call Hijacking

This can also be seen as a Denial-of-Service attack for User X, as User X is not able to receive any RTP stream from User Y. This attack can be detected by looking for the orphaned RTP flows, as done in case of Service tear-down attack. If the MG continue to receive RTP stream from User X (to the MG, this is now the old location of User X), then the behaviour is flagged as intrusive and an alarm is raised.

5.1.3 Garbage Packet attack

The Garbage Packet attack takes advantage of the vulnerabilities in the RTP media stream. As part of this attack, the attacker sends garbage RTP packets (filled with random bytes) to one of the MGs taking part in the conversation. As seen in Figure 5, the attacker sends junk RTP packets to the MG for User X. These garbage packets will affect the jitter buffers at the MGs and the phone client at User Y. This will lead to the garbled conversation or may

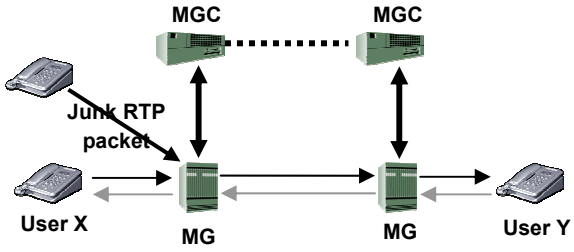

Figure 5: Garbage Packet attack

even result in crashing of the system.

This attack has serious consequences resulting in degradation of the voice quality. To prevent this attack, the IDS at the MG checks whether the packet came from the correct IP address before sending it across. If the attacker is successful in faking the IP address, then the packet would reach User Y. In this case, the attack is detected based on the rule that the sequence number in successive packets should increase regularly. So, if the IDS at User Y sees two consecutive packets whose sequence numbers differ by more than 100 (this number is selected based on average round trip time of the RTP packet), then the IDS raises an alarm.

5.2 Anomaly-based Attack Scenarios

All the scenarios discussed in the previous section make use of some fixed rules or signatures in order to detect an attack. These are quite successful in detecting the already-known intrusion in an effective manner, but cannot look for new novel attacks. In order to detect such new attacks, we first form the user profiles based on the call usage for some initial time. Any major deviation in the user's call usage from this normal behaviour is flagged as anomaly and further investigated by getting feedback from the user. We plan to use some machine learning algorithms to dynamically learn the user profiles over the period of time. For our simple prototype, we have just developed the user profile once during the initial time of user subscription.

5.2.1 Detection based on abnormal call duration

If the attacker is able to fake as a valid user, then he/she can make any number of calls and all the billing would be made to the valid user. To detect this type of intrusion, we keep the statistics for the normal call durations of the user and any major deviation from this normal duration is flagged as anomaly. For example, if a user talks for maximum of 30 minutes long distance and some day he/she is talking for 3 hours, then it can be classified as

anomalous behaviour and further investigation needs to be done. The user could be asked for confirmation after that maximum limit is crossed. The maximum call duration is calculated based on the call records for the user.

Besides keeping track of the duration of each call, the total duration of calls made during a day or a month can also be a criterion for describing the normal behaviour.

5.2.2 Detection based on abnormal time of call

The time of call is another criterion for the formation of user profiles. The call patterns show that users have preference for some specific times while making calls. For example, a user might prefer making long distance calls during the nights when the call rates are at the minimum. So, if the user starts making a large number of long distance calls during the daytime, then that behaviour is abnormal for the user. A user feedback can be taken before raising the alarm for that anomalous behaviour.

5.3 Mapping to mobile agents

Detection of some distributed attacks requires coordination between different IDS deployed at different VoIP components. An event generated at one network entity could be useful to detect an intrusion at some other entity. This distributed event data collection and correlation is done by mobile agents. For example, in case of call hijacking (Figure 4), if the MG receives orphaned RTP packets then it can act as a trigger for an analysis task. A mobile agent is sent from the MG to the MGC to investigate any received REINVITE message from the user. If any such message was received, then whole behaviour can be flagged as intrusive and an alarm is raised. The corresponding required recovery tasks are also done by the agents.

The biggest advantage we achieve by using mobile agents here is that we are not required to develop any new protocol for the intrusion detection support. Also, the functionality of perform the required recovery can be dynamically added to the mobile agents without changing the underlying VoIP protocols. Mobile agents are really useful in collecting the user call data from different network elements to have a centralized view of the user profile. This relevant data is much smaller the billing data actually collected at the network element and hence saves precious bandwidth.

6 RELATED WORK

To our knowledge, not much work has been done to develop IDS specific to VoIP. IDS solutions developed for general network traffic can be handy to some extent in detecting attacks for VoIP traffic too. Snort is one such network based IDS that looks for pre-defined signatures in the network traffic arriving at the host. These network IDSs have proved very effective for detecting most network based intrusion. However, for VoIP traffic these suffer from some limitations. First, VoIP traffic is a combination a number of protocols. The current network IDS do not correlate events between different protocols to give a broader view of an attack and hence can lead to large number of false positives. Second, they only look for a limited set of signatures and are ineffective in case of a new attack.

The concept of using user profiles to check for abnormal behaviour has been used effectively in host-based IDS. In earlier research, user profiles were built based on characteristics such as resources consumed, typing rate, login location, counts of particular commands (Denning, 1987; Smaha, 1988; Lunt, 1990; Frank, 1994). Most of the later research concentrated on the sequence of commands as the characteristics to define user behavior (Lane, 1997). Different machine learning algorithms have been developed to learn the normal user behavior in all the mentioned works. Any deviation from this normal behavior can be flagged as anomaly. BLAZE is the first IDS to use this concept of user profiles to detect anomalous user behavior in VoIP environment.

There exist several published reports regarding the application of mobile agents to intrusion detection. Helmer (Helmer, 2000) presents a complete mobile-agent based IDS, using agents for tasks ranging from monitoring to data collection and distributed analysis. The related project at Iowa State University has also investigated distributed versions of artificial intelligence algorithms to discover network anomalies. This system, however, intends to provide a complete IDS with mobile agents implementing all but the lowest level. Our approach differs in that it focuses on using agents to tie together IDS deployed at different VoIP network components.

7 CONCLUSIONS

In this paper, we have presented a mobile-agent based architecture of an intrusion detection system called BLAZE. BLAZE shows great promise in Voice-over-IP environments in detecting both known attacks and new novel attacks. It tries to map the strengths and flexibility of mobile agent technology to the requirements of the VoIP environment. The ability of the system to detect typical known attacks is demonstrated through three attack scenarios. But the strength of our system lies in its ability to detect new, novel attacks. For that purpose, we introduce the concept of developing user profiles based on the call usage. This is used as a baseline for a user's behaviour in call usage and any major deviation from this behaviour is flagged as an anomaly. We have demonstrated this by means of two examples.

Our next direct step will be to complete our prototype implementation of the BLAZE system. Though we have developed the concept of user profiles, we are still using them to develop static rules for intrusion detection. We plan to investigate machine learning techniques that would allow our system to dynamically update the user profiles and the corresponding set of intrusion detection rules over time.

We also plan to investigate the effectiveness of our system through simulation of other VoIP specific attacks. But the lack of literature describing the attack scenarios for VoIP environment is a major bottleneck. We would also like to look into the possible recovery procedures after the attack. We anticipate that this would not require much change in our system, as the mobile agents can be dynamically updated with new procedures. This explains the logic behind having a mobile-agent architecture that is protocol independent.

Lastly, we plan to explore the various security measures for the mobile agents themselves. The movement of the mobile agents through the networks makes them vulnerable to attacks. Some research has been done to provide some security to the agents using protocols like IPSec, but we still need to add the feature to our implementation to make it complete.

REFERENCES

Vuong S., Bai Y., 2003. A Survey of VoIP Intrusions and Intrusion Detections. *Technical Report, Department of Computer Science, the University of British Columbia*.

ITU-T, 1998. Packet-based multimedia communication systems. *Recommendation H.323*, February 1998.

Handley M., 1999. SIP: Session Initiation Protocol. *RFC 2543*.

Arango M., 1999. Media Gateway Control Protocol (MGCP) Version 1.0. *RFC 2705*.

Cuervo F., 2000. Megaco Protocol Version 1.0. *RFC 3015*.

Roesch M., 1999. Snort – Lightweight Intrusion Detection for Networks. In *Proceedings of USENIX LISA'99*.

Farmer D., 2000. What are MACtimes? *Dr. Dobb's Journal*, October 2000.

Orebaugh A., Morris G., Warnicke E., Ramirez G., 2004. *Ethereal Packet Sniffing*, Syngress Publishing.

Denning D.E., 1987. An intrusion-detection model. In *IEEE Transactions on Software Engineering, 13*, pages 222-232.

Smaha S.E., 1988. Haystack: An intrusion detection system. In *Proceedings of the Fourth Computer Security Applications Conference*, pp. 37-44.

Lunt T.F., 1990. IDES: An intelligent system for detecting intruders. In *Proceedings of the Symposium: Computer Security, Threat and Countermeasures*.

Frank J., 1994. Machine Learning and intrusion detection: Current and future directions. In *Proceedings of the 17th National Computer Security Conference*.

Lane T., Brodley C.E., 1997. An Application of Machine Learning to Anomaly Detection. In *Proceedings of the 20th NIST-NCSC National Information Systems Security Conference*.

Helmer G., Wong Johnny S.K., Honavar V., Miller L., Wang Y., 2000. Lightweight Agents for Intrusion Detection. *Journal of Systems and Software*, Volume 67, Issue 2, August 2004, pages 109-122.

Mobile Agent Intrusion Detection System. Iowa State University. http://latte.cs.iastate.edu/Research/Intrusion/