2015 16th IEEE International Conference on Mobile Data Management

A Logic-based Security Framework for Mobile Perimeter

Mahesh Nath Maddumala
Advisor: Vijay Kumar
Computer Science and Electrical Engineering
University of Missouri - Kansas City
Kansas City Missouri 64110, USA
E-mail: mnmg2d@mail.umkc.edu

I. Introduction

Mobile communication has become an essential information exchange platform for today's enterprise and government organizations. Their employees extensively use mobile devices to support their job activities while they are on the move. Organizations need to secure mobile devices as they secure wired devices. Organizations while securing mobile devices, also have to secure themselves from mobile devices as these devices are easily prone to attacks. Today, it is common for these organizations to have multiple external mobile and wireless connections to the outside world to provide high bandwidth and tolerate connection failures. One way to protect the network perimeter is to use border gateways that impose a uniform static policy on network traffic entering through its borders and by installing effective security schemes and policies on mobile devices itself. While being simple, such a static policy has many disadvantages and may not provide necessary protection to mobile perimeter. They are (a) unable to react to changes in its external environment, (b) they have physical limitations and differences in trust relationships, and (c) completeness among a non- communicating set of policies is problematic. Firewalls for mobile systems (mobile database systems, PDA, etc.) protect mobile clients from external attacks. Unlike wired systems, a mobile node (a) can issue a request from any location, (b) connects to many service providers that may have different security requirements, (c) can slip into doze mode, powered off or fail, and (d) is vulnerable to attacks. It is possible that a mobile client's valid request from one location may be denied at another location. The existed security framework provide engineering solutions to firewall protection and appear highly system-dependent. They are not scalable and not dynamically self-adjusting.

II. Our Approach

To protection policies that react to dynamic changes (quite frequent in mobile perimeter) and respect organizational objectives such as preferential treatment, yet enforce overall security objectives of organizations, requires that individual policies enforced at each border gateway be (a) dynamic and flexible, and (b) be a part of a global policy such that taken together enforce common security objectives in mobile infrastructure. In this proposal we achieve this by a logic-based security framework. Our solution has the potential to improve the security while reducing the management costs. We introduce the idea of "location-attack protection" where traffic from high cyber-crime locations (country, state, city, etc.) can be completely blocked. The proposed research will produce the following contributions:

1. A flexible, policy and implementation independent framework for protecting perimeters of networked environment where:

- Local policies at gateways are enforced in consultation and permission with a global policy base.
- Local policies export provisional permissions from the global policy base to admit the next packet of a progressing stream.
- Local policies are in-turn obligated to update statistics relevant for the global policy base to maintain the network health of the protected system.
- A sound stratified logic programming based semantics for all specifications.
- Consistent and complete permissions for all requests (i.e., every access request will be answered yes or no).

2. A two-stage optimization strategy for optimizing the implementation of distributed perimeter protection policies. The first stage uses folding/unfolding rules in the policy and the second stage consists of materialization (caching). In this respect, Etalle and Gabbrielli [1] developed fold/unfold transformations for constrained logic programs, Seki [2] developed the same for stratified programs. In addition. We propose to combine these techniques to develop an appropriate notion of program transformations to optimize our local and global perimeter protection policies.

978-1-4799-9972-9/15 $31.00 © 2015 IEEE
DOI 10.1109/MDM.2015.53

3. Algorithms that translate optimized policies to access-lists used by current firewalls and an appropriate secure communication fabric.

4. A uniform framework for provisions, obligations, and delegations where distributed collections of policies (including these) can be logically checked for consistency and completeness. The local policies depend upon having provisions approved by the global policy base and in turn, local policies are obliged to update their local statistics with the global policy base. This two-way exchange of data enables the global policy to respond to perimeter wide changes in an accurate and timely manner. We will suitably modify Delegation Logic of Li, Feigenbaum and Grosof [4, 5]. By examining fixed point semantics of our extended logic programs for provisions, obligations and delegations, we propose to develop a first order theory of provisions, obligations and delegations. The advantage of this proposal would be to have a theory of provisions, obligations, and delegations that go beyond Horn clauses. To the best of our knowledge, such a theory has not been developed.

5. An algebra for policy compositions that may result in inconsistent, ambiguous or non-deterministic policies being specified, and algorithms to determine such compositions. Our proposed solution consists of two levels of abstractions. The propositional level considers policies as abstract symbols that are interpreted as state transformers, where the state consists of a finite dimensional vector of finite length streams, and transformers specify which extensions of streams are accepted and which others are rejected. We use a countable collection of propositions to reason about such states. The predicate level enriches the propositional level with two kinds of details. The first enrichment defines atomic policies. These accept or deny to admit stream bundles and add or delete accepted or rejected streams to/from a bundle. The second enrichment is to replace propositions with predicates. We propose to explore the expressiveness of our formulation in three ways. First, we propose to include a collection of operations on policies that are used in policy formulations. Common ones are conjunctions, disjunctions, negations, differences, sequential compositions, closure under Kleene, restricting the scope, inverting policies (where accepted and rejected streams are swapped) taking lattice maximas and minimas under some pre-defined lattice of operations and adding and removing provisions and obligations. Second, we show a sense of completeness of the operations by showing how diverse policies can be modelled in our algebra. Third, we propose to explore the expressive power and the complexity of deciding if a modelled policy is complete and consistent.

6. A logic to reason about these policy compositions in the realm of Floyd-Hoare rules and Dynamic Logic to ensure that the policy composition is efficient and error-free.

7. A revised set of predicates for local and enterprise-wide policies for protecting mobile systems

8. Ability to stop attacks from high cyber-crime locations by including geographical locations in the predicates used to specify local and enterprise-wide policies. The firewall policy in mobile systems will depend upon the location from where a packet originates (location-specific attacks). One of the requirements of this project is to discover the location of an attack. We have developed a scheme using cell global identity to discover attacker's location even if the attacker is hiding behind a proxy. We published this work in special issue of IEEE journal Secure Cloud Computing for Big Data [3]. The discovery of attack location helped us to develop a location-based attack prevention scheme. This is covered in detail in Achieved Contributions section.

Once composed, our policies can be imported into access control rule lists that exist in today's Firewall.

III. Achieved Contributions

We started our research with location-based attack prevention scheme. Allocation of IP addresses is dynamic and not bound to any specific location. Also IP addresses can be spoofed in internet communication. Using this an attacker can exploit IP addresses to hide his/her identity which makes it hard to identify the attacker's location based on IP address. In order to reach to the attacker hiding behind the proxy, we propose the following approach. The location of a mobile phone in a cellular network can be identified by knowing its *cell global identity*. The scope of this approach is limited to the mobile devices which uses cellular network to access Organization's network.

A. Perimeter protection in Cellular Network

The location of a mobile device in a cellular network is given by *cell global identity*. For example, if the *cell global identity* is MCC = 310, MNC = 410, LAC = 3450 and CI = 118541125, then it represents a Cell in Kansas City of Missouri in United State of America. Here MCC (310) represents the country United States of America, MNC (410) represents AT&T network and LAC and CI codes represents a unique cell area in United States of America (Fig. 1).

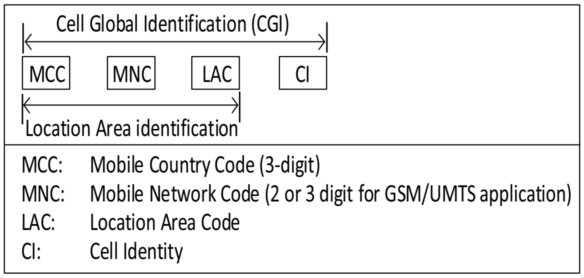
Cell Global Identification (CGI)
MCC
MNC
LAC
CI
Location Area identification
MCC: Mobile Country Code (3-digit)
MNC: Mobile Network Code (2 or 3 digit for GSM/UMTS application)
LAC: Location Area Code
CI: Cell Identity

Figure 1. Cell Global Identity structure.

B. *Extended IP Header*

At present cell global identity information is not available in IP packets coming from mobile devices. Our proposal is to extend the structure of an IP packet and include *cell global identity* information in IP packets. IP packet header contains optional field. It can be used to store the *cell global identity*. This will help us to identify the location of the mobile unit mounting the attack; directly or through a proxy. This will help us to program the firewall accordingly which then can block the attack from an unsafe location.

The IP Header format has an option field which is used whenever it is necessary. As per RFC791 standard [6], option field is of variable length and two types of formats are available: (a) a single octet of option type and (b) an option-type octet, an option-length octet, and the actual option-data octets. In this proposal, we consider second type of option field format with one octet of type, one octet of length and 6 octets of data which forms the *cell global identity.* Fig. 2 presents the format of the extended IP header.

<table>
<tr><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="2">Type</td><td>Length</td><td colspan="2">MCC</td></tr>
<tr><td colspan="3">MNC</td><td colspan="2">Location Area Code</td></tr>
<tr><td colspan="5">Cell Identity</td></tr>
</table>

Figure 2. Extended IP Header

As per RFC 971 standard, the option-type octet is viewed as having 3 fields: 1 bit-copied flag, 2 bits-option class and 5 bits-option number. In type field of proposed option header has the values of 1 as flag, 1 as class and 1 as the number. So, Option type = 10100001, i.e. 161. MCC is Mobile Country Code which is of 2 octets, MNC is Mobile Network Code which is of 2 octets, LAC is Location Area Code which is of 2 octets and Cell Identity is of 4 octets.

C. *Firewall Logic*

Initially when packet arrives, location area code will be read and verified in the HUL (Hard Unsafe Location) list. If there is a match then the packet will be discarded, otherwise packet will be analyzed by firewall for any malicious content apart from the firewall policies. If any malicious content is found, then LAC of the packet is recorded in MUL (Mild Unsafe Location) list. A separate counter is maintained for each entry of LAC in MUL and will be incremented whenever a new attack is detected from the same location.

When the counter value reaches the threshold limit T, it will be removed from MUL list and moved to HUL list. Thereafter packets from these HUL are completely blocked. Note that HUL is the final list of unsafe locations which we want to avoid.

Fig. 3 illustrates the entire process of determining unsafe locations. It is an ongoing process of finding unsafe locations based on number of attacks originating from a specific location.

LAC is a Location Area Code from where packet originates and

T is Threshold limit of attacks from a particular location.

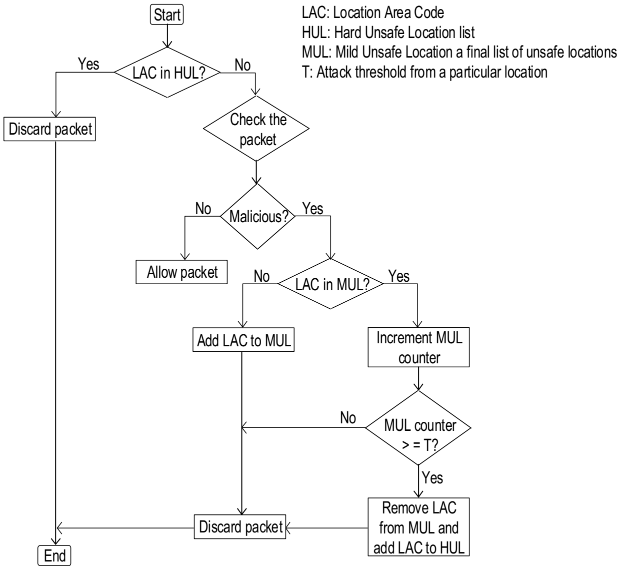

Figure 3. Firewall logic flowchart

How to geo-locate the attacker? Once an attack is identified by the Firewall then attacker's geolocation can be identified by converting the cell global identity to the

GPS coordinates. Google provides the APIs to convert Cell Global Identity information the GPS coordinates. It can also be mapped on the Google Maps.

D. Mobile Client Implementation

The Client at Mobile side is responsible for integrating *cell global identity* information with the IP packet. This information should be encrypted to safeguard the privacy of the user and to protect from the man-in-the-middle attack. Encryption technique is incorporated in the mobile client implementation logic. The Cell Global Identity information should be made available in every packet that is going to the Firewall. Fig. 4 presents the integration of an extended IP header to a typical IP packet.

Ethernet Header	IP Header + CGI	IP Data

Figure 4. Integration of CGI with IP Header.

Another approach is to make the *cell global identity* available in the IP packets only at the time of authentication of user by Organization's Firewall that is while mobile client sending credentials to the Firewall in the authentication process. This reduces the size of the total length of the packets sent to the Firewall compared to the previous approach. Also on the other side, firewall does not have to check and compare the Location Area Code for every packet. This reduces the load on the Firewall. However there is a disadvantage to this approach. When user moves from one location to another or one location area to another location area then this new location area information is not made available to the firewall until user logins again. There is an inconsistency between user's Location Area known to the Firewall and actual user's Location Area. So, by making Cell Global Identity available in every outgoing packet reduces these inconsistencies and avoids any loop holes which can be exploited by the attacker.

E. Current Results

We evaluated our approach by developing a mobile app which acts as mobile client and implemented the firewall logic in python on a Linux server which acts as a Firewall. We loaded mobile app on various android devices and tried accessing server which has our Firewall program running on that server. Firewall program able to extract the IP packets and reads the Cell Global Identity information of various locations and compared against the existing list of Location Area Codes. This implementation also verified the algorithm presented in the section Fig. 3.

We implemented mobile application in android and loaded on various android devices to verify our approach. We read the MCC, MNC, LAC and Cell Identity from the Phone and we modified the IP packet to add options field which is filled with the above Cell Location values. We included Cell Location details in every packet sent from mobile to data center. However we have not implemented the encryption part that encrypts the *cell global identity* values in an IP header.

IV. Expected Contributions

The research issues and the solution approaches proposed in this project are highly innovative and will change the conventional approach of building, implementing and managing firewalls for providing strong security to mobile (wireless) streams. The idea to stop attacks through location-specific approach is quite innovative. The main deliverables of this proposal are a reference architecture, mathematical framework to specify policies for coordinating and dynamically adjusting filters, their efficient implementation, location-specific message filtering, and an algebra for composing and propagating changes to such policies for wired and mobile systems.

V. Acknowledgment

I would like to thank my advisor professor Vijay Kumar for his support and guidance. This project is funded by a grant from NSF.

References

[1] Sandro Etalle and Maurizio Gabbrielli. Transformations of clp modules. Theoretical Computer Science,166: 101–146, 1996.

[2] Hiroshisa Seki. Unfold/fold transformation of tratified programs. Theoretical Computer Science, pages, 107–139, 1991.

[3] Chetan Jaiswal, Mahesh Nath, and Vijay Kumar "A Location-Based Security Framework for Cloud Perimeter," Special issue of IEEE journal Secure Cloud Computing for Big Data, Vol-1, Issue03, 2014: pp. 56-64.

[4] Ninghui Li. Delegation Logic: A Logic-based Approach to Distributed Authorization. PhD thesis, NewYork University, September 2000.

[5] Ninghui Li, Benjamin N. Grosof, and Joan Feigenbaum. A practically implementable and tractable delegation logic. In IEEE Symposium on Security and Privacy, pages 27–42, 2000.

[6] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[7] 3GPP TS 23.003: "Numbering, addressing and identification".