Security patterns for Voice over IP Networks

Eduardo B. Fernandez, Juan C. Pelaez and Maria M. Larrondo-Petrie
Florida Atlantic University, Department of Computer Science & Engineering, Boca Raton, Florida
Email: ed@cse.fau.edu, jpelaez@ieee.org, petrie@fau.edu

***Abstract*—Voice over IP (VoIP) has had a strong effect on global communications by allowing human voice and fax information to travel over existing packet data networks along with traditional data packets. The convergence of voice and data in the same network brings both benefits and constraints to users. Among the several issues that need to be addressed when deploying this technology, security is one of the most critical. We give an overview of VoIP and provide UML models of some aspects of its infrastructure, including architectures and basic use cases. We present some security patterns that describe mechanisms that can control many of the possible attacks and which could be used to design secure systems.**

***Index Terms*—security patterns, Voice over IP, network architecture, software architecture**

I. INTRODUCTION

Voice over IP (VoIP) is defined as the transport of voice as packets over IP based networks. Therefore, VoIP can be achieved on any data network that uses IP, such as the Internet, intranets, and Local Area Networks (LAN), where digitized voice packets are transmitted over the IP network. Existing network infrastructures can be used to carry both data and voice traffic, which is very attractive to new users. Savings come from eliminating the need to purchase new Private Branch Exchange (PBX) equipment, and from reducing staff and maintenance costs, as only one network needs to be supported [1]. The possible savings from the cost of long distance per minute charges of sending voice traffic via existing carriers provide extra incentives for moving to VoIP. In addition to delivering voice, the IP protocol performs some of the related functions of the voice network which are necessary to convert the whole network into a full system. Some of these functions include special features, collect calling, gateways into the public voice network, and associated actions.

We present first architectures and use cases for some aspects of the VoIP infrastructure. We then present security patterns that describe mechanisms that can control many of the possible attacks and which could be used to design secure systems. Patterns have shown their value in developing good quality software and we expect that their application to VoIP will also prove valuable to build secure systems. A security pattern describes a recurring security problem that arises in a specific context and presents a well-proven generic scheme for its solution [2]. We present four security patterns which provide a collection of good practices for VoIP. They should be helpful to system's designers in identifying and understanding the mechanisms needed to protect this type of systems. They will also enable the rapid development and documentation of new methods for preventing future attacks against VoIP networks. The patterns include Network Segmentation, VoIP Tunneling, Signed Authenticated Call, and Secure VoIP Call. These patterns were proposed in [3] and are elaborated here. Only one other paper has shown this type of patterns [4], who also describe a Secure VoIP Call pattern as well as three other different patterns. Current VoIP products are still weak and there is a need to improve their security [5]; we expect that the use of patterns will contribute to this purpose. To make our patterns more precise and easier to implement, we use the Unified Language Model (UML) to describe the solutions implied by each pattern.

We start with an overview of VoIP in Section 2 and present UML models for its architecture, while Section 3 introduces the main actors and use cases of a VoIP system. Section 4 presents our security patterns. Finally, Section 5 provides some conclusions.

II. VOIP ARCHITECTURES

When using the IP protocol, there are three different types of connections for setting up a call: (1) PC-to-PC, where individuals talk online through their PCs, (2) PC-to-Telephone, where individuals make and receive voice calls and messages while on the Internet, and (3) Telephone-to-Telephone, where calls are made and receive using regular phones connected to Public Switched Telephone Network (PSTN) or IP-telephones connected to a data net.

VoIP uses the Real-Time Protocol (RTP) for transport, the Real-Time Transport Protocol (RTCP) for reporting Quality of Service (QoS), and H.323, SIP, MGCP (Media Gateway Control Protocol/Megaco) for signaling. These protocols operate in the application layer; that is, on top of the IP protocol. Most current VoIP implementations use the H.323 protocol, the same protocol used for IP video. Until now, users prefer H.323 over SIP, but this may be primarily due to the earlier release of H.323 (in

Based on "Security Patterns for Voice Over IP Networks", by Eduardo B. Fernandez, Juan C. Pelaez and Maria M. Larrondo-Petrie which appeared in the Proceedings of the Second International Multi-Conference on Computing in the Global Information Technology (ICCGI 2007) on March 4-9, 2007, Guadaloupe, French Caribbean.

© 2007 ACADEMY PUBLISHER

the 90's) [1]. This situation may change in the near future. We present below UML models for the architectures implied by these standards, more detailed descriptions in the form of patterns are presented in [6].

A. H.323

H.323 is a family of protocols specified by the ITU research group. The standard provides a foundation for transporting (i.e. signaling) voice, video and data communications in an IPbased network. H.323 supports Secure Real-Time protocol (SRTP) for media confidentiality, and Multimedia Internet Keying (MIKEY) for key exchange. It is important to emphasize that the signaling is only protected up to the gateway.

Fig. 1 shows a class diagram describing how an IP telephony system integrates with the **PSTN** using H323. The components inside the dotted lines indicate the specific units of the standard while the external units are the network components that participate in the whole system This model shows the elements needed to place a call from a regular telephone number to a PC running an H.323 client (and vice versa). The **PBX** which supports the standard analog phone (caller), formats caller and callee numbers and forwards them to the VoIP **gateway** via the PSTN network. The gateway, which connects different PSTNs, takes the voice call from circuit-switched PSTN and places it on the IP network. The gateway queries the **gatekeeper** via the IP network with caller/callee numbers (note that the Voice packets do not go through the gatekeeper; only the call signaling goes through it) and the gatekeeper translates them into a routing number based upon service logic. Gatekeepers act like central managers providing call setup and routing the calls throughout the network to other voice devices. Likewise, the **IP-PBX** server provides call control and configuration management for IP telephony devices. Finally the gateway routes the call to called party (callee).

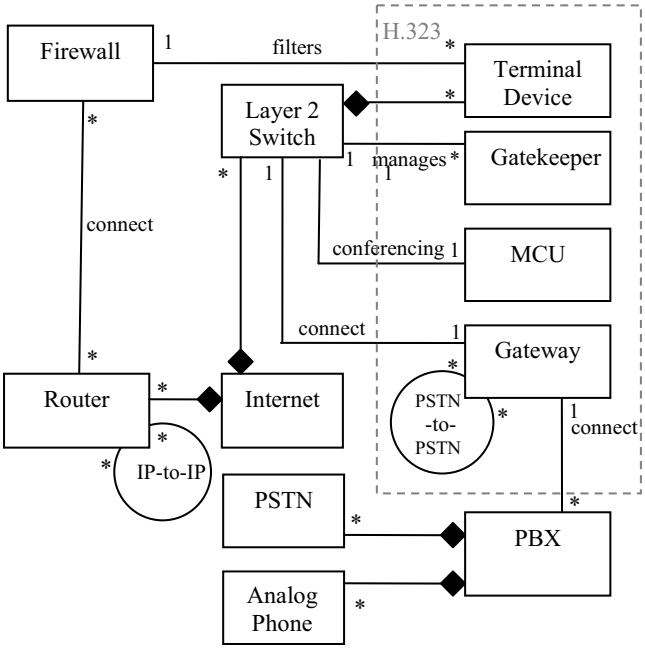

Figure 1. Class diagram for an H.323 architecture

The **Layer 2 Switch** provides connectivity and network availability between H.323 components. The **Internet (**IP network**)** contains **Routers** that connect to each other and **Firewalls** to filter traffic to the **Terminal Devices** (i.e. where users interact with the system). The **MCU** (Multipoint Control Unit) is used for conferencing. **Softphones** are applications installed in Terminal Devices (e.g. PCs or wireless devices) used to send/receive calls.

Fig. 2 shows a sequence diagram for a telephone-to-telephone connection. In this case, the model presented in Figure 1 could be altered to have analog telephones as **terminal devices**, rather than PCs in order to provide all types of connections for setting up a call.

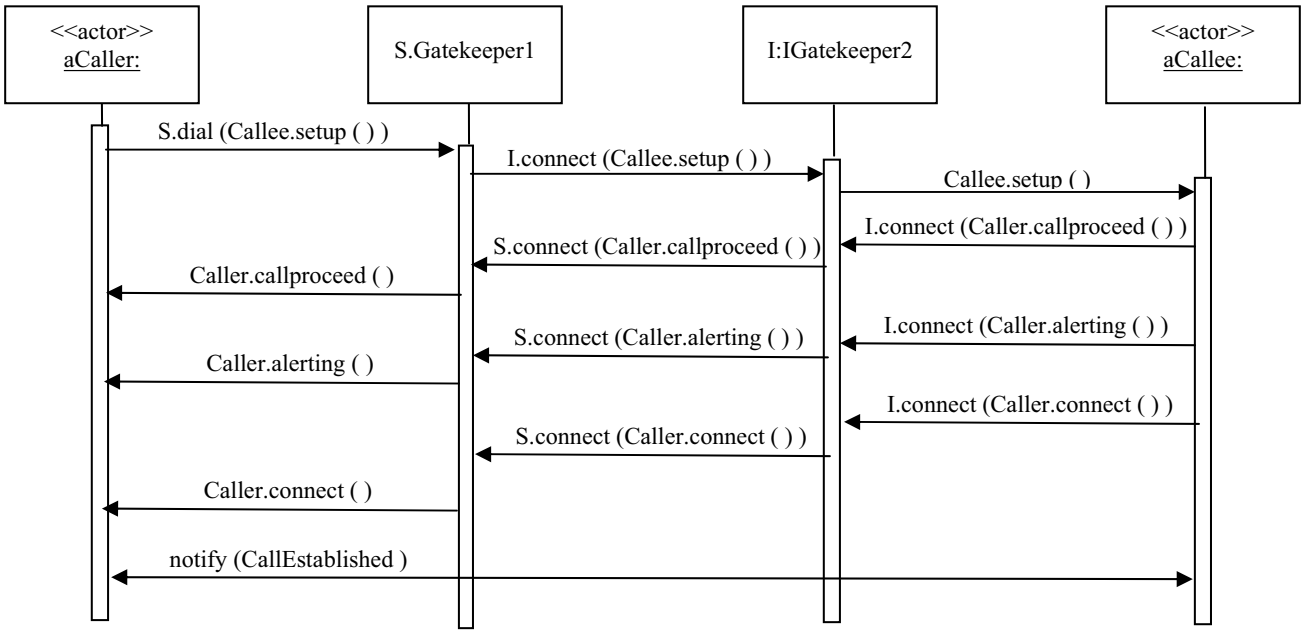

Figure 2. Sequence diagram for call connection in H.323

© 2007 ACADEMY PUBLISHER

B. SIP

Session Initiation Protocol (SIP) is the IETF's standard for multimedia conferencing over IP. SIP is an application-layer control (signaling) protocol used for creating, modifying and terminating sessions with one or more participants. These sessions can include Internet multimedia conferences, Internet telephone calls and multimedia distribution. SIP is a less complicated protocol, and it is more flexible than H.323.

Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call. SIP supports IP mobility for VoIP WLAN applications by providing handoff capabilities at the application layer. SIP can make direct use of Dynamic Host Control Protocol (DHCP) when connecting to an 802.11 AP for binding an IP address [7].

SIP supports SRTP for securing media traffic and TLS and S/MIME for signaling protection. Although most VoIP implementations today use the H.323 protocol for IP services, SIP is gaining more acceptance in the network telephony market due partly to its flexibility and lower implementation costs. It is possible to use each protocol alone or both protocols within the same network in order to provide universal connectivity.

The main components of SIP-based systems are user agents and servers:

User Agents (UAs), are combinations of User Agent Clients (UAC) and User Agent Servers (UAS). A UAC is responsible for initiating a call by sending a URL-addressed INVITE to the intended recipient. A UAS receives requests and sends back responses.

Servers can be classified as:

- **Proxy servers**, which operate on behalf of users and are responsible for routing and delivering messages.
- **Redirect servers**, which keep a user database which allows them to inform proxy servers of a user location.
- **Location servers**, which are used by a Redirect server or a Proxy server to obtain information about a called party's possible location.
- **Registrar servers**, which save information about where a party can be found.

Fig. 3 shows the components for a SIP-based network. The proxy server is connected to a VoIP gateway (to make possible a call from a regular telephone to an IP phone) and to other proxy servers. The rest of the VoIP architecture is similar to Fig. 1 and represented by a UML package. Once the call has been established, the RTP media streams flow between the end stations directly.

III. ROLES IN A BASIC VOIP MODEL

Because VoIP networks are vulnerable to attacks from external and internal sources, the human actors of this system can be classified as described below. We show the participation of these actors in use cases. Another set of use cases can be found in [2].

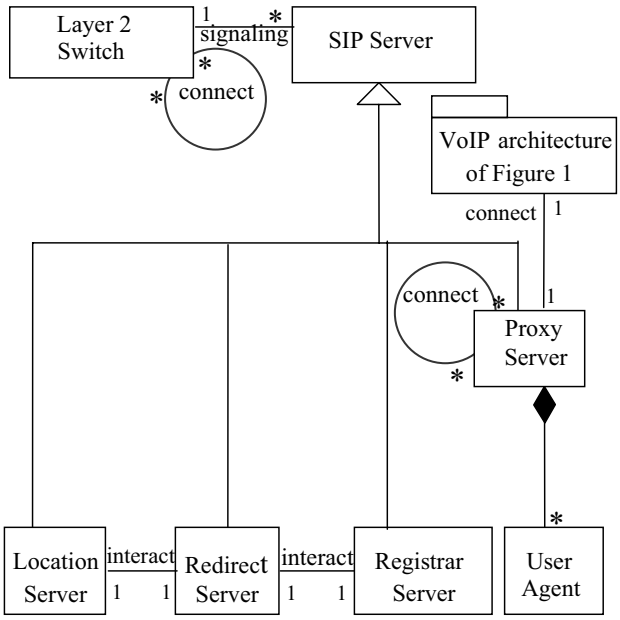

Figure 3. Class diagram of the SIP architecture

Internal Roles

- **Internal subscriber** is a VoIP user, such as an employee in a company. Internal subscribers are allowed to make and receive voice calls by either using standard or IP phones (hardphones and softphones). They also have access to data services by using terminal devices (e.g. PCs).
- **Administrator**. This role is responsible for maintaining the VoIP network perimeter and auditing the VoIP system in order to monitor user activities. The network security administrator is also responsible of properly configuring security mechanisms and reacting in the presence of attacks.
- **Auditor.** This role is responsible for performing audit logs to verify the integrity of the VoIP system. Auditing is especially useful for identifying potential security breaches or break-in attempts.
- **Operator** is responsible of protecting the system from being compromised, so that each voice call can be accounted to the appropriate user. He is also responsible for booting and shutting down the system, performing routine maintenance of servers, performing system performance metering and on-line tests, and in general responding to various relevant user requests.

External Roles

- **Remote** subscriber are users such as employees who occasionally work from home. They are given access to voice and services only from their homes.

© 2007 ACADEMY PUBLISHER

- **Law** Enforcement **Agent** is a legal agent who redirects duplicated media packets to law enforcement, for the purpose of wiretapping. If legally authorized, the agent has access to corporate servers in order to intercept data and voice packets.

In addition to these roles, the use case diagram (Fig. 4) can be used to systematically analyze the different types of attacks against the VoIP network, following the approach in [8].

IV. Attacks against the VoIP Network

Based on the Use Case Diagram of Fig. 4, we can determine the possible attacks against the VoIP infrastructure.

A. Attacks when making/receiving a VoIP Call

Many of the already well-known security vulnerabilities in data networks can have an adverse impact on voice communications and need to be protected against. The attacks when making/receiving a voice call can be classified as follows:

Theft of service is the ability of a malicious user to place fraudulent calls. In this case the attacker simply wants to use a service without paying for it, so this attack is against the service provider. There are numerous methods the hacker can use to accomplish this task. In a basic case of toll fraud, an unauthorized user places calls using an unattended IP phone or assuming the identity of the legitimate user of the telephone. In a more complex attack, a rogue IP phone may be placed on the network or a breached gateway may be used to make unauthorized calls. As mentioned before, gateways are used for routing packetized voice between the source and the destination within the IP network.

Masquerading, occurs when a hacker is able to trick a remote user into believing he is talking to his intended recipient when in fact he is really talking to the hacker. Such an attack typically occurs with the hacker assuming the identity of someone who is not well-known to the target. A masquerade attack usually includes one of the other forms of active attacks [9].

IP Spoofing, occurs when a hacker inside or outside a network impersonates a trusted computer. There are two methods of doing this. The hacker can use either an IP address that is within the range of trusted IP addresses for a network or an authorized external trusted IP address that has access to specified resources on a network. As in Caller ID Spoofing attacks (i.e. Masquerading), IP spoofing attacks can be used to launch other types of attacks. A typical example is to launch a denial-of-service (DoS) attack using spoofed source addresses to hide the hacker's identity. Without some defense a hacker might be able to spoof the address of the IP-PBX and flood the entire voice segment with UDP packets.

Call Interception is the unauthorized monitoring of

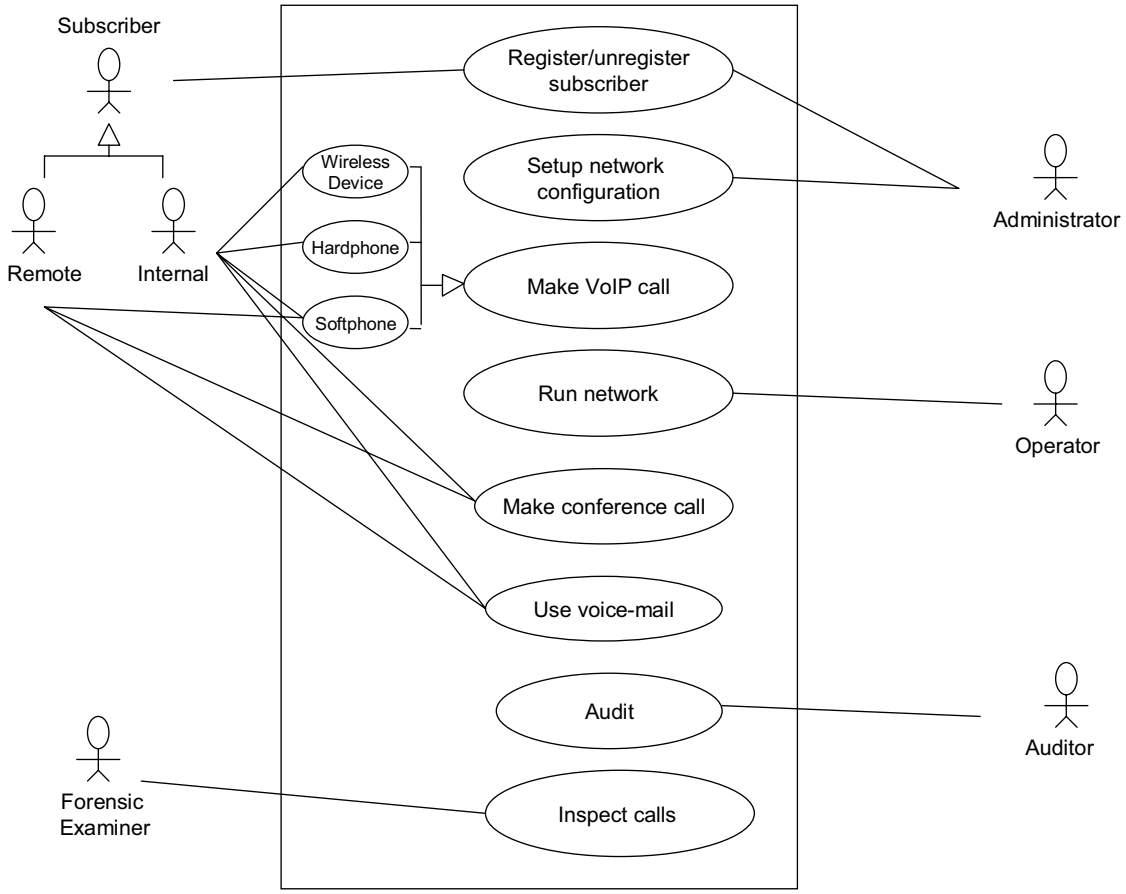

Figure 4. Use Case Diagram for a VoIP System

© 2007 ACADEMY PUBLISHER

voice packets or RTCP transmissions. Hackers could capture the packets and decode their voice packet payload as they traverse a large network. This kind of attack is the equivalent of wiretapping in a circuit-switched telephone system. Due to the fact that voice travels in packets over the data network, hackers can use data-sniffing and other hacking tools to identify, modify, store and play back unprotected voice communications traversing the network, thus violating confidentiality.

A packet sniffer is a software application that uses a network adapter card in promiscuous mode (a mode in which the network adapter card sends all packets received on the physical network wire to an application for processing) to capture all network packets that are sent across a particular collision domain. This packet sniffer application can reside in a general-purpose computer attached, for example, in a corporate's local area network. For example, the tool "voice over misconfigured Internet telephones" (a.k.a. "vomit"), takes an IP phone conversation trace captured by the UNIX tool tcpdump, and reassembles it into a wave file which makes listening easy [10]. Figure 7 shows the sequence of steps that hackers use to monitor a VoIP conversation. With tcpdump, hackers can identify the IP and MAC address of the phone to be attacked By using an Address Resolution Protocol (ARP) spoofing tool, the attacker could impersonate the local gateway and the IP phone on the network, creating a default gateway [10]. This allows IP traffic to and from the target IP phone to be monitored by the attacking workstation. Likewise, the FragRouter tool would have to be enabled on the attacking machine so the data packets would reach their ultimate destination. The tools used for this purpose can be downloaded freely on the internet. Also, if the hacker has access to the local switched segment, he may be able to intercept a call by inserting a phone into the voice segment with a spoofed Media Access Control (MAC) address, and assuming the target phone's identity.

A hacker breaking into a VoIP data stream has access to many more calls than he would with traditional telephone tapping. Consequently, he has a much greater opportunity of obtaining useful information from tapping a VoIP data stream than from monitoring traditional phone systems. The risk of experiencing Call Interception is somewhat limited because it would require physical access to the local network or remote access to a compromised host on the local network. Intercepting voice traffic as it crosses the Internet is more difficult because once the packetized voice hits the carrier, it becomes much harder to single out among other traffic.

Repudiation attacks can take place when two parties talk over the phone and later on one party denies that the conversation occurred.

Call Hijacking or Redirect attacks could replace a voice mail address with a hacker-specified IP address, opening a channel to the hacker [11]. In this way, all calls placed over the VoIP network will fail to reach the end user. The tools used to launch this kind of attack are similar to those used in call interception.

Denial-of-service (DoS) attacks prevent legitimate users of a network from accessing the features and services provided by the network. One method to launch this type of attack is to flood the server with repeated, requests for legal service in an attempt to overload it. This will cause severe degradation or complete unavailability of the service.

A flooding attack can also be launched against IP phones and Gateways in an attempt to interrupt communications. Often the Ping command is used to carry out such flooding attacks. Ping uses ICMP (Internet Control Message Protocol). Attackers can also use the TCP SYN Flood attack to obtain similar results. Since these kinds of attacks can be originated from a wide variety of persons and locations, they are very difficult to mitigate. Similarly, out-of-sequence voice packets (such as receiving media packets before a session is accepted) or an excessively long phone number could open the way to buffer overflows. VoIP spam might paralyze a number through repeated calling [11].

Signal protocol tampering occurs when a malicious user can monitor and capture the packets that set up the call. By doing so, that user could manipulate fields in the data stream and make VoIP calls without using a VoIP phone [10]. The malicious user could also make an expensive call, and mislead the IP-PBX into believing that it was originated from another user.

Attacks against Softphones occur because as they reside in the data VLAN, they require open access to the voice VLAN in order to access call control, place calls to IP phones, and leave voice messages. Therefore, the deployment of Softphones provides a path for attacks against the voice VLAN. VoIP systems are capable of handling large volumes of calls using both IP phones and Softphones. Unlike traditional phones, which must be hardwired to a specific PBX port, IP phones can be plugged into any Ethernet jack and assigned an IP address. These features not only represent advantages but also they may make them targets of security attacks.

Note that all these attacks apply also to conference calls and some may apply to the use of voice mail.

B. Registration attacks

Brute Force attacks are simply an attempt to try all possible values when attempting to authenticate with a system or crack the crypto key used to create ciphertext. For example, an attacker may attempt to brute-force attack a Telnet login, he must first obtain the Telnet prompt on a system. When connection is made to the Telnet port, the hacker will try every potential word or phrase to come up with a possible password.

Reflection attacks are specifically aimed at SIP systems. It may happen when using http digest authentication (i.e. challenge-response with a shared secret) for both request and response. If the same shared secret is used in both directions, an attacker can obtain credentials by reflecting a challenge in a response back in request. This attack can be eliminated by using different shared secrets in each direction. This kind of attack is not a problem when PGP is used for authentication [12].

© 2007 ACADEMY PUBLISHER

The **IP Spoofing** attacks described earlier can also be classified as registration attacks.

We have analyzed in detail some of these attacks using the concept of "attack pattern", where we consider also forensic aspects [13,14].

V. VOIP SECURITY PATTERNS

The pattern diagram of Figure 5 shows the relationship between our security patterns and related (more general) cryptographic patterns. The patterns presented here are indicated with a double line.

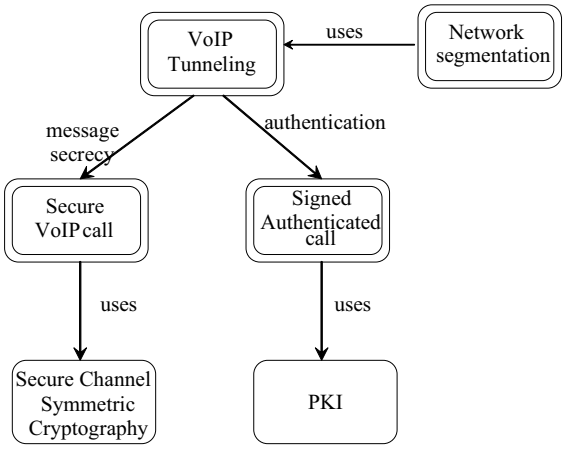

Figure 5. Relatonships between VoIP security patterns

A. Network Segmentation

The Network Segmentation pattern performs separation of the voice and data services to counter possible attacks against the voice VLAN by an attacker in the data VLAN. Using network segmentation, an attack aimed at the data network won't impact critical voice traffic and vice versa.

Context

Two or more VoIP remote users on different private networks need to establish a voice call.

Problem

How to prevent data network attacks from affecting voice traffic in a VoIP environment?

The solution to this problem is affected by the following forces:

- Data and voice have different characteristics and can be attacked in different ways. For example, voice has real-time requirements.
- If an attacker takes control of the data segment he could also overcome the voice section of the system because they use the same units.
- Softphones by their nature reside in the data section and are vulnerable to a variety of attacks, e.g. operating system attacks, application attacks, service attacks, etc.

Solution

Technologies such as virtual LANs (VLANs), and access control, provide the Layer 2 with segmentation necessary to keep the voice and data segments separate at the access layer. In a VoIP network, terminal devices (i.e. IP phones) must be located in VLANs that support only IP telephony services, but not existing data services. Likewise, VoIP servers must be placed on a separate segment protected by a VoIP-aware firewall. Alternatively, packet filtering can be easily configured on the existing router or routing switch connecting the voice and data VLANs. The solution can be optimized by adding a stateful firewall to protect the VoIP VLANs from the data VLANs. Fig. 6 shows a segmentation technique in VoIP that is achieved by sending voice and data on separate VLANs. A **stateful firewall** is used in the data VLAN in order to prevent attacks against the voice VLAN when using PCIPPs (i.e. **softphones**). On the other hand, the voice VLAN uses a proxy firewall to solve the firewall/NAT traversal issue.

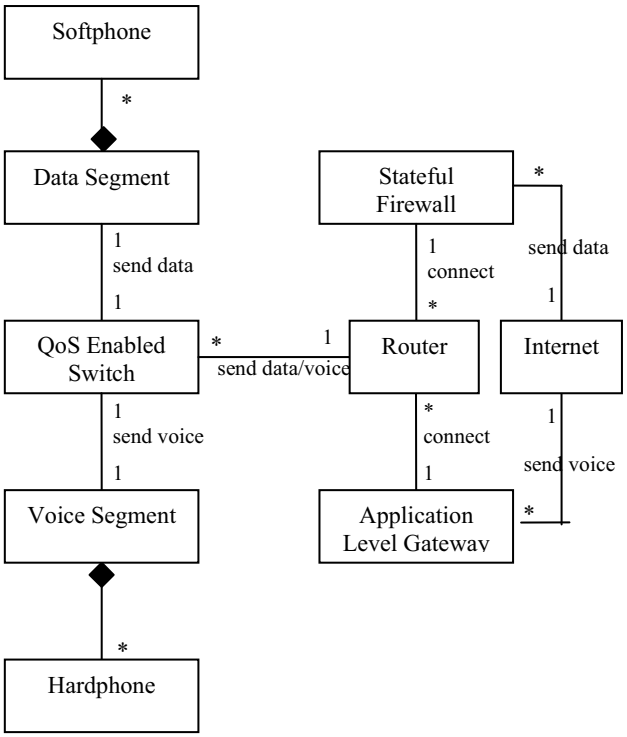

Figure 6. VoiIP Segmentation

Consequences

The advantages of this pattern include:

- Critical voice traffic will remain unaffected if an attack occur on the data network and vice versa.
- Segmentation will minimize disruption in the event of an attack.
- The addition of another IP segment to host VoIP is a simple task, which requires only slight reconfiguration of existing network elements.

Related patterns

VoIP Tunneling can be used for segmentation.

B. VoIP Tunneling

The VoIP Tunneling pattern provides a way of guaranteeing the confidentiality and integrity of calls in IP telephony by the encapsulation of data from one protocol into the protocol stream of another.

Context

© 2007 ACADEMY PUBLISHER

Two or more VoIP remote users on different private networks need to establish a voice call.

Problem

Voice traffic will be exposed to hackers when traversing a public network such as the Internet. How to counter Call Interception and other related attacks against VoIP services when voice packets traverse an external network?

The solution will be affected by the following forces

A VoIP network has potential problems when sending IP voice through a firewall (i.e., the firewall/NAT traversal problem).

VoIP users need to establish secure communication over public networks (i.e. the Internet).

Both endpoints must be authenticated before a voice call is established.

Softphones need to establish a secured channel for communication with terminal devices.

Solution

The simplest method to counter Call Interception and other related attacks is to route the voice traffic over a private network using either point-to-point connections or a carrier-based IP VPNs. Tunnels are virtual connections between a network ingress point and a network egress point. At the ingress point, data is encapsulated using encryption, while at the egress point, data is returned to the original source format. VPNs create private end-to-end pipes or "tunnels" out of the public bandwidth of the Internet providing secure links between distinct locations on the public network. In order to establish such a secure channel one endpoint of the tunnel initiates the connection. The combined use of IP Security (IPSec) tunneling and data encryption to protect from intruders accessing information is also a good alternative for the use of firewalls.

Implementation

These tunnels use encryption and other security mechanisms to ensure confidentiality and data integrity in VoIP networks. Due to performance requirements a symmetric encryption algorithm should be preferred for the data transport. For this encryption algorithm, a single key is necessary. This key has to be distributed to the involved terminal devices. Tunneling uses an Authentication Protocol to establish a trust relationship between network terminal devices prior to establishing a connection.

Consequences

The advantages of this pattern include:

- Tunnels allow secure transport of the VoIP traffic over the external network.
- It eliminates the risk of exposing a network to intruders when opening ports on a firewall to allow VoIP to flow through.
- VPNs are cost-effective solutions because users can connect to the Internet locally and tunnel back to connect to institution resources.
- VPNs improve flexibility and scalability.

The disadvantage of this approach is that end-to-end encryption in VPNs will introduce latency.

Related Patterns

The VoIP Tunneling pattern has direct relationships (see Figure 4**)** to the following security patterns:

- The Secure VoIP Call which will be presented next.
- The Authenticated Call which will be presented later and other similar authentication protocols used to establish trust relationships between the VPN endpoints.
- The Network Segmentation pattern which was previously introduced.

C. Signed Authenticated Call

The Authenticated Call pattern performs both device and user authentication before deciding access to VoIP services.

Context

A VoIP subscriber establishes a voice call over a VoIP channel. The subscriber needs to distinguish whether she is talking with the intended recipient or with an impostor.

Problem

How can an attacker be prevented from masquerading as a VoIP terminal device, either IP or standard, when network subscribers want to establish a voice call? How to guarantee that the caller cannot repudiate a call that the callee believes was made by her?

The following forces affect the solution:

- It is very important to associate a voice call with its legitimate caller.
- Attackers are interested in passing for legitimate users to gain access to the system.
- Users may deny having made specific calls.
- Users may need to make calls through different administrative domains.

Solution

Digital signatures is an authentication method where subscribers can tie the identity of a caller with a voice call made by him. In this way, the sender of a signed voice call is authenticated and cannot deny having sent it.

Implementation

Participants in a VoIP call agree on the use of a mathematical method to prove identities such as the public key digital signature protocol. Public key cryptography is typically used for mutual authentication and key agreement. The call can be established after it is first encrypted, using the caller's private key and the public key of the remote user (callee). The caller sends the signed voice call to the callee who also has caller's public key. He deciphers the signed voice call with the caller's public key in order to verify it. If the enciphered call makes sense to the callee, since only the caller's private key could have been used to generate a meaningful call after decipherment by the callee, both parties can trust each other and are successfully authenticated.

Public key cryptography-based authentication is the only means of authentication that scales up to arbitrarily large networks by making it possible to securely distribute keys relatively easily through unsecured networks [12].

© 2007 ACADEMY PUBLISHER

Fig. 7 shows a sequence diagram (Refer to the class diagram of Figure 1) illustrating an authenticated call. This solution uses PKI for user authentication combined with hash between two phones either IP or standard.

Consequences

The advantages of this pattern include:

- Digital signatures provide a convenient way for authentication of messages in VoIP, because verifying the authorship of a message is based solely on the secrecy of the author's private key.
- Authentication is also the best countermeasure for theft of service attacks where stolen user identification details may be use to charge calls to someone else's account.
- VoIP systems with a global PKI are able to manage trust relationships across multiple administrative domains.

The disadvantage of this approach is that PKI requires significant amount of infrastructure.

Known Uses

IPSec-based connection and TLS are authentication mechanisms that can be specified as those to be used with SIP. IPSec uses either The Authentication Header (AH) or The Encapsulating Security Protocol (ESP) for providing cryptographic authentication to IP (v4 and v6) datagrams. The authentication data is computed by using any of the standard message digest algorithms such as HMAC-MD5 and HMAC-SHA. [15].

Related Patterns

The Authenticated Call pattern is related to other cryptographic authentication patterns such as the Sender Authentication [16] and Authentication [2]. It is also related to the PKI pattern that describes the necessary cryptographic infrastructure.

D. Secure VoIP call

The Secure VoIP call pattern hides the meaning of messages by performing encryption of calls in a VoIP environment.

Context

Two or more subscribers are participating in a voice call over a VoIP channel. In public IP networks such as the Internet, it is easy to capture the packets meant for another user.

Problem

When making or receiving a call, the transported voice packets between the VoIP network nodes are exposed to interception. How to prevent attackers from listening to a voice call conversation when voice packets are intercepted on public IP networks?

The solution will be affected by the following forces:

- Packets sent in a public network are easy to intercept and read or change. We need a way to hide their contents.
- The protection method must be transparent to the users and easy to apply.
- The protection method should not significantly affect the quality of the call.

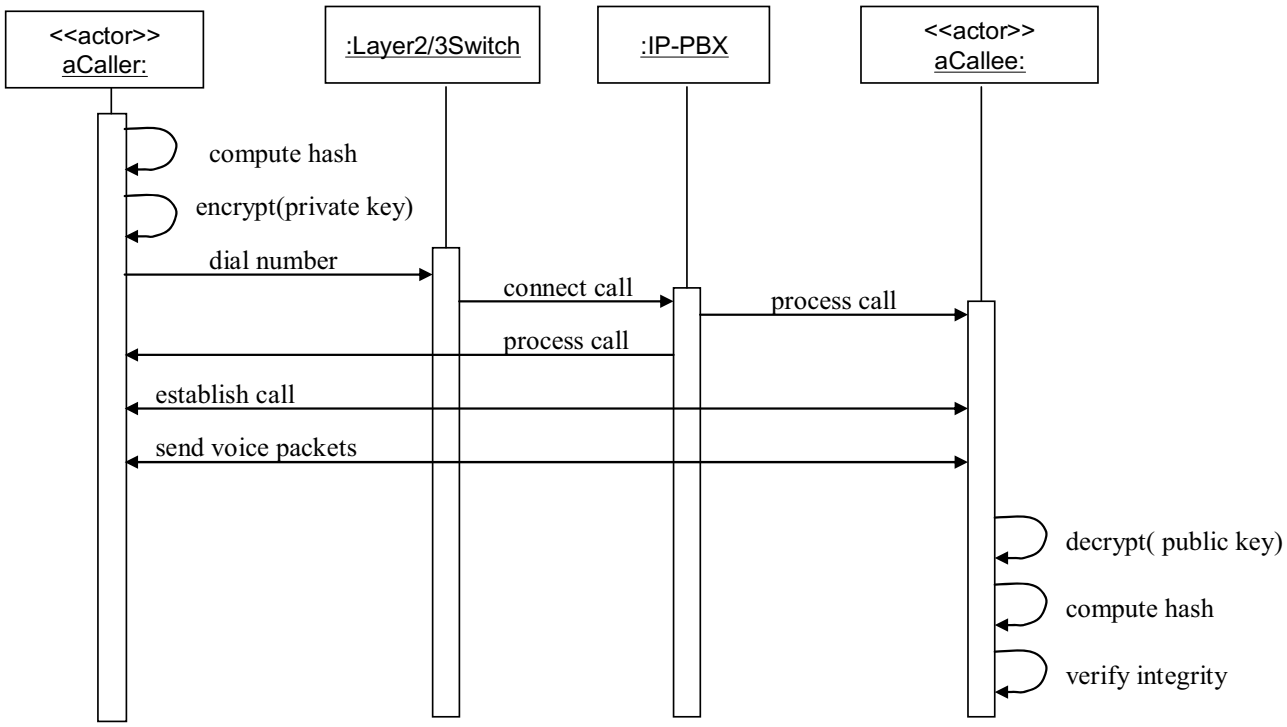

Figure 7. Sequence diagram Authenticated Call

© 2007 ACADEMY PUBLISHER

Solution

To achieve confidentiality we use encryption and decryption of VoIP calls.

Implementation

In cases where performance is an important issue, symmetric algorithms are preferred. Such algorithms require the same cryptographic key (a shared secret key) on both sides of the channel.

If the IPSec standard is used, it is necessary for participants in a call (i.e. Caller and Callee) to agree previously on a data encryption algorithm (e.g. DES, 3DES, AES) and on a shared secret key. The Internet Key Exchange (IKE) protocol is used for setting up the IPSEC connections between terminal devices. The caller encrypts the voice call with the secret key and sends it to the remote user. The callee decrypts the voice call and recovers the original voice packets.

Additionally, the Secure Real Time Protocol (SRTP) can be used for encrypting media traffic and the Multimedia Internet KEYing (MIKEY) for exchanging keying materials in VoIP.

If public key cryptography is used, the callee must obtain the caller's public key before establishing a connection. The caller encrypts the voice call with the callee's public key and sends it to her. The callee decrypts the voice call and recovers the original voice packets.

The class diagram of Fig. 8 shows a Secure-channel communication in VoIP (adapted from the Cryptographic Metapattern in [16]).This model uses the Strategy pattern to indicate choice of encryption algorithems. Both the Caller and Callee roles use the same set of algorithms although they are shown only in the caller side.

Consequences

The advantages of this pattern include:

- Symmetric encryption approaches provide good confidentiality.
- Encryption is performed transparently to the user's activities.
- The need to provide separate VLANs for VoIP security could possibly be removed.
- It may no longer be necessary to use IPSec tunneling that was previously required in the MAN/WAN.

Possible disadvantages include:

- The quality of the call can be affected if encryption is not performed very carefully [17].
- It is hard to scale because of the need for shared keys.
- CALEA (Communication Assistance for Law Enforcement Act) allows the US government to intercept communications for law enforcement purposes. This means that a site needs to provide the encryption keys to the government if required.

Related Patterns

This Secure VoIP pattern is related to the Cryptographic Metapattern [16] and other similar encryption protocol patterns.

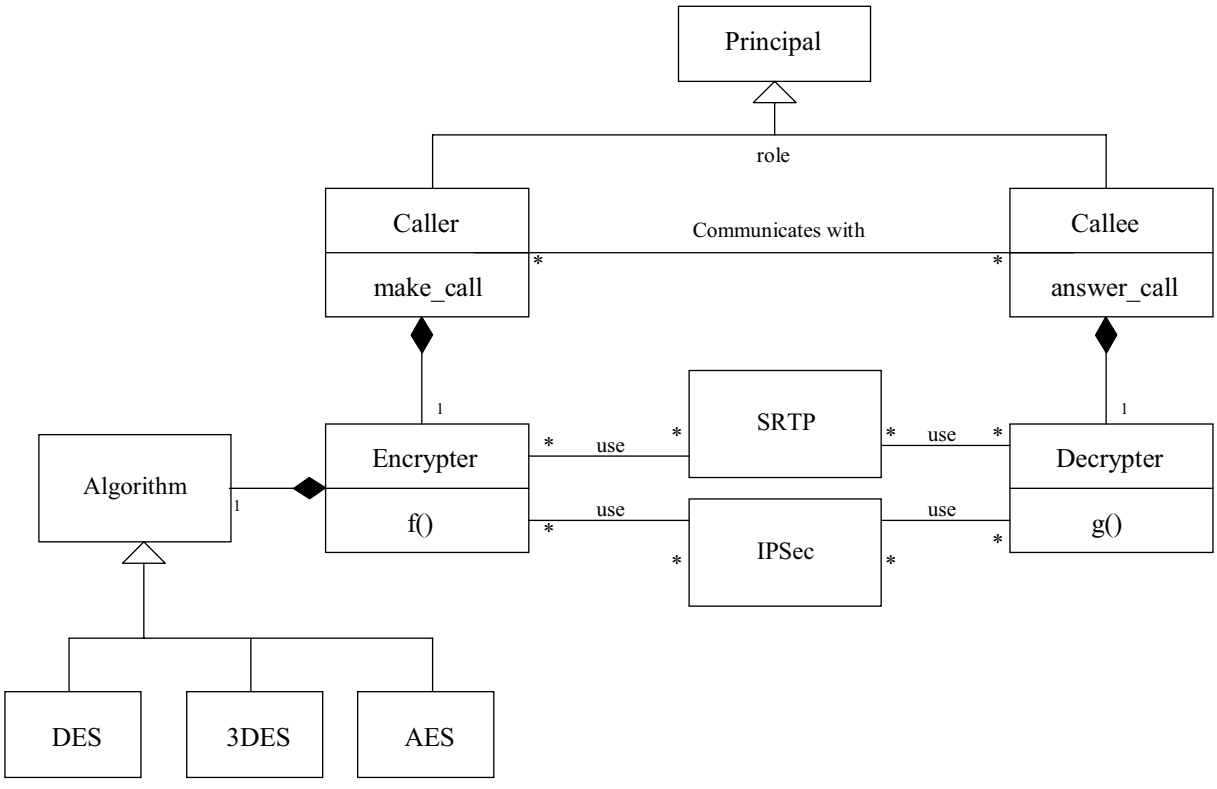

Figure 8. Class Diagram for a VoIP Secure Channel

© 2007 ACADEMY PUBLISHER

VI. Discussion

Our patterns consider only some aspects of security, those involved with signaling. Other aspects are also (maybe more) important for the overall security of the system:

- The general security of the platforms, including hardware and operating systems. The platform affects all applications running in the system.
- Server to server signaling. Important for their coordination. This is done at the IP or TCP levels.
- Logging and intrusion detection. General security mechanisms for any system.
- Use of firewalls in the network. To control external attacks such as denial of service and traffic from/to malicious sites.

As mentioned earlier, another paper [4], has considered other patterns.

VII. Conclusions

We have discussed existing VoIP architectures and provided UML models for them. This approach provides a precise framework where to apply security. We also considered possible security attacks and related them to the ways the system is used. Finally, we considered some defense mechanisms and provided patterns for them.

In conclusion, the best security approach in VoIP is to encrypt all voice traffic and to use VPNs to separate VoIP from data traffic in order to increase security and performance; even though it may not be appropriate for all environments. This would ensure that the critical voice traffic would be unaffected if an attack did occur on the data network. Security on VoIP networks can be better implemented using filtering and/or firewalls to control the traffic between the voice and data VPN.

Acknowledgements

Jose Ortiz-Villajos provided valuable comments which improved this paper.

References

[1] E. Weiss, “Security concerns with VoIP” August 20, 2001, IP Telephony (VOIP) Threats, Defenses and Countermeasures, Core Competence, Inc., http://www.sans.org/rr/papers/index.php?id=323

[2] M. Schumacher, E. B.Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad, *Security Patterns: Integrating security and systems engineering*, Wiley 2006.

[3] J. C.Pelaez. *Security in VoIP networks*. Master’s thesis, Florida Atlantic University, August 2004.

[4] Z. Anwar, W. Yurcik, R. Johnson, M. Hafiz and R. Campbell. “Multiple Design Patterns for Voice over IP (VoIP) Security”, in *Proceedings of the IEEE Workshop on Information Assurance (WIA 206*), Phoenix, AZ, April 2006.

[5] C. Wieser, J. Roning and A. Takanen, “Security analysis and experiments for Voice over IP RTP media streams”, *Proceedings of the 8th International Symposium on System and Information Security (SSI’2006*), Sao Jose dos Campos, Sao Paolo, Brazil, 8-10 November 2006.

[6] J. C. Pelaez, E. B. Fernandez, and C. Wieser, "Patterns for VoIP signaling protocol architectures", in *Proceedings of the 12th European Pattern languages of Programs Conference* (EuroPLoP 2007), Bavaria, Germany, 4-8 July 2007. http://hillside.net/europlop/home.html

[7] Bastermagian N., “Including VoIP over WLAN in a Seamless Next-Generation Wireless Environment”, Whitepapers, Texas Instruments, March 8, 2004. International Engineering Consortium. http://www.iec.org/online/tutorials/ti_voip_wlan/

[8] E. B. Fernandez, M. VanHilst, M. M. Larrondo Petrie, S. Huang, "Defining Security Requirements through Misuse Actions", in *Advanced Software Engineering: Expanding the Frontiers of Software Technology*, S. F. Ochoa and G.-C. Roman (Eds.), International Federation for Information Processing, Springer, 2006, 123-137.

[9] W. Stallings, *Network Security Essentials: Applications and Standard*s, Prentice Hall, Upper Saddle River, 2002, 5 – 21

[10] Pogar, Joel, “Data Security in a Converged Network”, Siemens Whitepaper, 2003, http://whitepapers.techrepublic.com.com/whitepaper.aspx?docid=57980

[11] D. Greenfield, “Securing The IP Telephony Perimeter”, Network Magazine, April 5, 2004. http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=18900070

[12] M. Marjalaakso, “Security requirements and Constraints of VoIP”, Department of Electrical Engineering and Communications, Helsinki University of Technology, September 17 2001, http://www.hut.fi/~mmarjala/voip

[13] E. B. Fernandez, J. C. Pelaez, and M. M. Larrondo-Petrie, "Attack patterns: A new forensic and design tool", in *Proceedings of the Third Annual IFIP WG 11.9 International Conference on Digital Forensics*, Orlando, Florida, USA, January 29-31, 2007.

[14] J. C. Pelaez, E. B. Fernandez, M. M. Larrondo-Petrie, and C. Wieser, "Attack patterns in VoIP", to appear.

[15] M K. Ranganathan and L. Kilmartin. “Investigations into the Impact of Key Exchange Mechanisms for Security Protocols in VoIP Networks,” in *Proceedings of the First Joint IEI/IEE Symposium on Telecommunications Systems Research,* 27 November 2001, Dublin, Ireland. http://telecoms.eeng.dcu.ie/symposium/papers/D2.pdf

[16] A. Braga, C. Rubira, and R. Dahab. “Tropyc: A Pattern Language for Cryptographic Software”, in *Proceedings of the 5th Pattern Languages of Programming Conference,* PLoP 1998, Washington University Technical Report WUCS-98-25, 1998. http://citeseer.ist.psu.edu/braga99tropyc.html

[17] T.J. Walsh and D.R. Kuhn, “Challenges in security Voice over IP”, *IEEE Security and Privacy*, vol. 3 no. 3, May/June 2005, 44-49.

Eduardo B. Fernandez (Eduardo Fernandez-Buglioni) is a professor in the Department of Computer Science and Engineering at Florida Atlantic University in Boca Raton, Florida. He has published numerous papers on authorization models, object-oriented analysis and design, and security patterns. He has written four books on these subjects, the most recent being a book on security patterns.. He has lectured all over the world at both academic and industrial meetings. He has created and taught several graduate and undergraduate courses

© 2007 ACADEMY PUBLISHER

and industrial tutorials. His current interests include security patterns and web services security. He holds a MS degree in Electrical Engineering from Purdue University and a Ph.D. in Computer Science from UCLA. He is a Senior Member of the IEEE, and a Member of ACM. He is an active consultant for industry, including assignments with IBM, Allied Signal, Motorola, Lucent, and others. More details can be found at http://www.cse.fau.edu/~ed/

Dr. Fernandez's areas of expertise include: Data security, including distributed systems and database security, Object-oriented design methodologies, Patterns, including security patterns

Juan C. Pelaez recently completed his PhD in Computer Science at Florida Atlantic University, Boca Raton, Florida, USA, where he is part of the Secure Systems Research Group. He is a research scientist for the U.S. Army Research Laboratory in Adelphi, Maryland, USA.

Dr. Pelaez specializes in VoIP and network forensics. The topic of his doctoral dissertation is "VoIP Network Security and Forensic Models using Patterns". He is an IEEE Member.

Maria M. Larrondo-Petrie is a Professor and Associate Dean in the College of Engineering and Computer Science at Florida Atlantic University in Boca Raton, Florida, USA. She has a PhD is Computer Engineering, a Master in Computer Science and a Bachelors in Mathematics.

She has published more than 150 refereed papers and has led more than $2.5M in sponsored research funded by the U.S. Department of Defense, U.S. Office of Naval Research, Nato, IBM, NSF, and the South Florida Water Management District. Her current research interests focus on security, complex systems modeling and pedagogy.

Dr. Larrondo-Petrie is on the board of the International Federation of Engineering Education Society where she co-chairs the steering committee for the 1st IFEES Global Engineering Education Summit, and also is part of the IFEES Strategic Planning Committee. She is also on the boards of the American Society of Engineering Education's International Division, Minorities in Engineering Division and Women in Engineering Division. She is the Executive Vice President of the Latin American and Caribbean Consortium of Engineering Education and has served as Conference Chair for several LACCEI Latin American and Caribbean Conference for Engineering and Technology, as Vice President of Research Collaboration, and as organizer of two Organization of American States sponsored workshops on Engineering Accreditation and Program Recognition for Latin America and the Caribbean. She has served as past President of the Upsilon Pi Epsilon International Honor Society for the Computing and Information Disciplines, and is a Member of Engineering for the Americas, IEEE and IEEE Computer Society, and ACM. She has received several teaching and leadership awards.

© 2007 ACADEMY PUBLISHER