COMPUTERS & SECURITY XXX (2009) I–II

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Issues and challenges in securing VoIP

Ram Dantu[a], Sonia Fahmy[b], Henning Schulzrinne[c], João Cangussu[d,*]

[a]Department of Computer Science, University of North Texas, P.O. Box 311366, Denton, TX 76203, USA
[b]Department of Computer Science, Purdue University, 305 N. University St., West Lafayette, IN 47907-2107, USA
[c]Department of Computer Science, Columbia University, M/S 0401, 1214 Amsterdam Avenue, New York, NY 10027-7003, USA
[d]Department of Computer Science, University of Texas at Dallas, P.O. Box 830688 M/S EC31, Richardson, TX 75083-0688, USA

ARTICLE INFO

Article history:
Received 20 August 2008
Received in revised form
29 April 2009
Accepted 3 May 2009

Keywords:
VoIP security
Threats
Feedback
VoIP attacks
Security solutions

ABSTRACT

Voice over the Internet protocol (VoIP) is being rapidly deployed, and the convergence of the voice and data worlds is introducing exciting opportunities. Lower cost and greater flexibility are the key factors luring enterprises to transition to VoIP. Some security problems may surface with the widespread deployment of VoIP. In this article, we discuss these security problems and propose a high-level security architecture that captures required features at each boundary-network-element in the VoIP infrastructure. We describe mechanisms to efficiently integrate information between distributed security components in the architecture.

1. Introduction

Voice over the Internet protocol (VoIP) is being rapidly deployed and is adding a third dimension to voice communication – with public switched telephone networks (PSTN) and cellular networks being the other two. VoIP can be used to call any PSTN telephone or mobile phone anywhere in the world. Although certain services can only function on a computer or a special VoIP phone; others allow a caller to use a traditional phone with an adapter. VoIP promises to enable migration of the existing circuit-switched, public switching telecommunication network to a packet-switched network. With widespread acceptance by telecommunication markets of all sizes, advanced VoIP features have started emerging. However, the convergence of the voice and data worlds introduces security risks, not just opportunities. Lower cost and greater flexibility are key factors luring enterprises to transition to VoIP. VoIP should not, however, be installed without careful consideration of the security problems that it can introduce.

To facilitate the ensuing discussion, we briefly describe the basic VoIP network architecture. The VoIP infrastructure can be visualized as three layers: end user equipment, network components, and a gateway to the traditional telephone network (Fig. 1). We define each of these layers as follows.

1. End-user equipment:

The end-user equipment provides an interface for users to communicate with other end users. Equipment can be ''hard phones'' with an interface similar to a conventional telephone or a ''soft phones,'' software that emulates a telephone. The security of such end-user components depends on how they are installed. Mostly, this end-user equipment is often

* *Corresponding author*. Tel.: +1 972 883 2193; fax: +1 972 883 2349.
E-mail addresses: rdantu@unt.edu (R. Dantu), fahmy@cs.purdue.edu (S. Fahmy), hgs@cs.columbia.edu (H. Schulzrinne), cangussu@utdallas.edu (J. Cangussu).
0167-4048/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2009.05.003

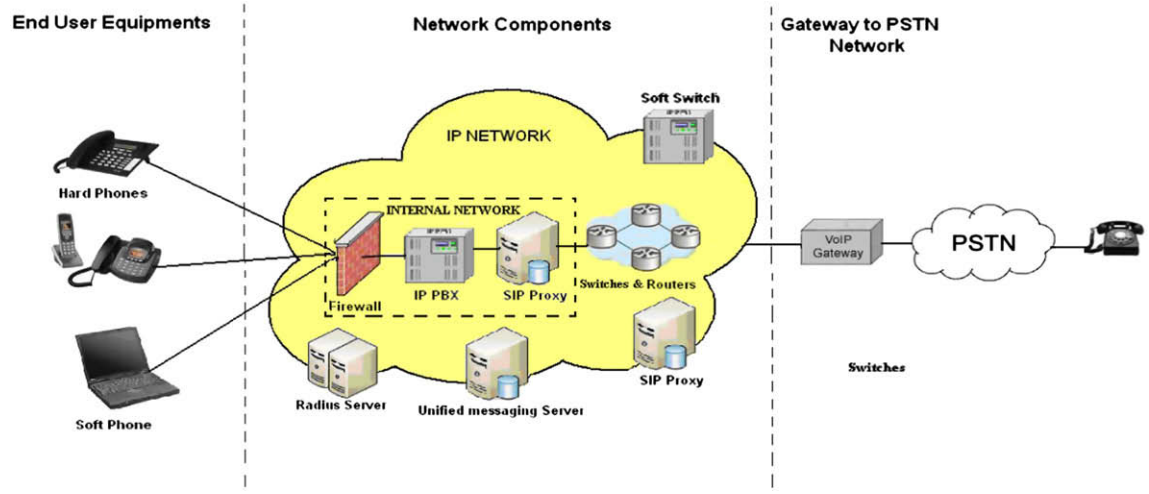

Fig. 1 – VoIP network.

deployed in campus networks, at home, or in hotels. Rarely, however, does the equipment have security features built in, making them vulnerable to exploitable flaws.

2. Network components:

VoIP normally uses the existing IP network and thus inherits its vulnerabilities. Each network component has its own security concerns, which have surfaced over the past few years. Adding voice traffic to these components increases their list of vulnerabilities. The IP network components, including routers, switches, and firewalls, must also be VoIP-aware to provide security features specific to VoIP.

3. VoIP Gateways:

Gateways play an important role in integrating the IP network with the PSTN; thus, care should be taken to ensure that its security policies do not introduce vulnerabilities. The primary functions of a VoIP gateway include voice compression or decompression, signaling control, call routing, and packetization. VoIP gateways interface with external controllers such as session initiation protocol (SIP) proxies, H434 gatekeepers, media gateway controllers (MGCs), network management systems, and billing systems. These interfaces can be a potential weakness because malicious attackers can exploit them to make free telephone calls. Any security framework must counter these attacks quickly and efficiently.

Security issues in VoIP are unique and, in most cases, quite complex. This paper describes each component of the VoIP infrastructure and its corresponding security issues and then outlines a VoIP security framework. In Section 2, we discuss security provisions in the existing VoIP protocols and how effectively these provisions enable secure communication. In Section 3, we enumerate attacks that threaten VoIP networks and follow the enumeration with a discussion of solutions that could mitigate these vulnerabilities. In Sections 4 and 5 we discuss the important topics of soft phone security, PSTN–VoIP interoperability (using for example the Electroninc Number (ENUM) protocol), and intrusion detection (Mukherjee, 1994; Axelsson, 2000). Finally, in Section 6, we outline a VoIP architecture that would address most of these security issues.

2. Security threats in VoIP protocols

We classify VoIP protocols broadly as either *signaling protocols* or *media transport protocols*:

- *Signaling protocols*: These protocols control signaling services such as call setup and termination. They also handle management, establishment, setup negotiation, modification, and teardown of sessions.
- *Media transport protocols*: These protocols control digitizing, encoding, decoding, and ordering of voice samples for real-time communication.

These VoIP protocols were not designed with security as a primary concern. Though their latest versions have incorporated some security features, they are still not fully secure. For example, the SIP is unaware of media misuse. Gupta and Shmatikov (2006) present a structured security analysis of the VoIP protocol stack, which comprises signaling through the SIP; session description protocol (SDP); key establishment, such as session description (SDES), multimedia keying (MIKEY), and real-time transport protocol (ZRTP); and secure media transport protocols such as secured real-time \protocol (SRTP). The authors claim that a replay attack on SDES presents the most serious attack because replay attacks cause SRTP to repeat the key-stream used for media encryption, thus breaking transport-layer security. Clearly, security features built into the protocols need to be enhanced to ensure secure communication and defeat threats such as replay attacks. However, security administrators encounter a large number of diverse protocols available in the market today and need a method to determine whether such protocols address security concerns. To avoid security breaches, VoIP protocols

Please cite this article in press as: Dantu R et al., Issues and challenges in securing VoIP, Comput. Secur. (2009), doi:10.1016/j.cose.2009.05.003

need to address issues such as authentication, integrity, and privacy as follows:

- The authentication function ensures that endpoints participating in the conference are indeed who they claim to be.
- The integrity function provides a means to validate whether the packet contents were tampered with while they were in transit.
- Privacy is provided by encryption to ensure that the data cannot be intercepted by eavesdroppers.

In Table 1, we give a brief description of the primary VoIP protocols and how they address security issues. In the following sections, we examine how attackers can exploit vulnerabilities and some possible solutions for preventing exploitations.

3. Survey of attacks and solutions

Attackers typically target the most popular and well-publicized systems and applications. VoIP has become one such application. Several VoIP weaknesses have been revealed recently, which protocol designers need to address before successfully deploying VoIP on a global scale. In this section, we present a study of attacks on a VoIP infrastructure. We classify attacks into five primary types in Table 2. Further, we discuss approaches that have been adopted to counter attacks. This survey has enabled us to design a high-level architecture (Table 3), which we present in Section 7. Since we have collected the information in this section from a variety of sources, we cannot attest to the accuracy of all the given information. We believe, however, that vendors have patched the security flaws in each instance.

Table 1 – Prominent VoIP protocols and their approaches to security.

Protocol	Brief description	Security
H.323 (Signaling)	→ The H.323 protocol is based on a connection-oriented paradigm that accommodates video conferencing and basic telephony. → As H.323 uses packet communications systems (Goode, 2002), it can be integrated into personal computers and routers or can be implemented in stand-alone devices.	→ H.323 relies on the H.235 standard to provide security (Goode, 2002). The H.235 standard addresses many common security issues, including authentication, integrity, privacy, and non-repudiation. → H.323 can also use a secure socket layer (SSL) for transport-layer security.
SIP (Signaling)	The SIP is an application-layer control protocol that establishes, modifies, or terminates user sessions (Rosenberg et al., 2002). → Within this text-based client-server protocol, the client initiates SIP requests, and a server responds to those requests.	SIP uses two main security mechanisms: end-to-end and hop-by-hop (Salsano et al., 2002). → In end-to-end protection, hypertext transfer protocol (HTTP) digest provides authentication. SIP body encryption utilizes the secure multipurpose Internet mail extension. → In a hop-by-hop mechanism, encryption is supported, and the SDP conveys the SSL keys for media encryption (Kent and Atkinson, 1998). The PROTOS (Oulu University Secure Programming Group) test-suite is a tool available to evaluate implementation-level security and robustness of SIP implementations.
SCCP (Signaling)	The skinny client control protocol (SCCP) is a Cisco proprietary protocol used between Cisco Call Manager and Cisco VoIP phones.	Secure SCCP, which is a newer version of SCCP, uses a TCP connection rather than the user datagram protocol (UDP) and encrypts call control information.
RTP (Media)	The real-time transport protocol (RTP) defines a standardized packet format for delivering audio and video over the Internet. According to RFC1889 (Schulzrinne et al., 1996), the services provided by RTP include the following: → Payload-type identification—indication of the kind of content being carried → Sequence numbering—protocol data unit (PDU) sequence numbers → Time stamping—presentation time of the content being carried in the PDU → Delivery monitoring It is possible to capture legitimate packets and insert them into another RTP stream, which acts as a kind of replay/insertion attack to impersonate a legitimate user (Richard Kuhn et al., 2004).	SRTP (Baugher et al., 2004), a security profile for RTP, aims to provide confidentiality, message authentication, and replay protection. → SRTP does not encrypt RTP headers that include information such as payload type, synchronization source identifier, and time-stamp. → SRTP counters replay attacks by using a sliding window and ''replay list.'' → SRTP mitigates denial or service attacks by using stream ciphers. The challenge when using SRTP is to find a means for provisioning key distribution and management.
RTCP (Media)	The real-time transport control protocol provides out-of-band control information for an RTP flow. The primary function of the RTCP is to provide feedback on the quality of service being provided by the RTP.	The RTCP itself does not provide any flow encryption or authentication means. The SRTCP (Baugher and Carrara, 2006) protocol can be used for that purpose.

Please cite this article in press as: Dantu R et al., Issues and challenges in securing VoIP, Comput. Secur. (2009), doi:10.1016/j.cose.2009.05.003

Table 2 – A Summary of VoIP Attacks and Responses.

Attack type	Attacks reported	Proposed solutions
Denial of Service (DoS)	→ Certain VoIP phones were susceptible to both DoS attacks and communication interception vulnerabilities (Leyden, 2004). → Certain VoIP routers were vulnerable to malicious traffic (Leyden, 2004). → An open-source IP private branch exchange (PBX) and an open-source VoIP client had vulnerabilities that could allow hackers to compromise VoIP networks with DoS attacks (Network computing, 2006). → Another type of virtual private network (VPN) routers allowed remote attackers to cause a DoS (crash) via an IP security Internet key exchange (IKE) packet with a malformed Internet security association and key management protocol (ISAKMP) (National Cyber-Alert System). → Another type of IP phones was rendered unusable by bombarding them with specific IP traffic (Mier et al., 2004; Franklin, 2007).	→ **Firewalls** filter unwanted traffic. However, filtering induces time delay that reduces quality of service. → **Special-purpose hardware** (such as routers and switches) prevents the attacker from gaining unauthorized access. → **VoIP-aware hardware** can distinguish VoIP traffic. → **Effective authentication systems** can prevent unauthorized access to infrastructural components. → **Recovery systems** can recover as quickly as possible after an attack attempt.
Packet Spoofing and Masquerading	→ Recently, a bank and an online payment service were victims of attacks in which the attacker calls a credit-card customer and dupes the customer into revealing account information by claiming that there has been fraudulent activity on their account (Jackson Higgins, 2006).	An effective authentication module combined with encryption would be an effective solution to masquerading and spoofing attacks.
Eavesdropping	→ The Internet Security Systems (ISS) X-Force team discovered VoIP security flaws in a vendor's call manager that would give an attacker the ability to eavesdrop or redirect calls and gain unauthorized access to networks running the VoIP products (VoIP Magazine Editorial Staff, 2005; Wright et al., 2008; McMillan, 2008). If attackers exploited the vulnerabilities, they could set off a heap overflow within the call manager, causing a DoS condition and compromising the call manager.	Long (2002) recommends four strategies to prevent eavesdropping: → Employing flawless hardware. → Ensuring that access to wiring closets is restricted to authorized personnel only. → Implementing port-based MAC address security on any vulnerable network point; for example, on a reception courtesy phone. → Initiating a procedure to regularly scan the network for devices running in promiscuous mode. Encryption of VoIP traffic, although a good method for preventing eavesdropping, adds additional overhead.
VoIP Spam and Phishing	→ Gonsalves (2006) reports an attack in which a con artist sent VoIP spam disguised as if coming from a small bank and collected personal identification numbers. → Recently, an attacker sent e-mails that appeared to come from the account verification team at an online-payment service. Unlike most phishing schemes that direct the recipient to a fraudulent Web site, this scam instructed victims to call a phone number, where they were asked to divulge account information (Ryst, 2006). → A security vendor reported a worm that spreads through the chat feature of a popular VoIP service (Kirk, 2006). Users received a message asking them to download a file called "sp.exe." The executable was a Trojan horse that can steal passwords. If a user runs the Trojan, it triggers another set of code to spread itself. → Dritsas et al. (2007) and Marias et al. (2007) have introduced protocol oriented vulnerabilities specific to SIP.	→ **Filter traffic based on frequency and duration.** A filter can identify calls likely to be spam on the basis of the frequency and duration of the calls. Qovia recently filed two patent applications for this technology designed to thwart spam over Internet telephony (SPIT) (Celeste Biever, 2004). → **Detection and mitigation of SPIT networks using signaling protocol analysis** uses analysis of the VoIP signaling messages which can assist service providers in detecting spam activity targeting their customers. MacIntosh *et al.* proposed this solution (MacIntosh et al., 2005). → Dantu and Kolan (2004, 2005) use a voice spam protection algorithm. They utilize user feedback to calculate a caller's reputation value using a Bayesian inference function, taking into consideration the caller's past history. → **Trust enforcement in peer-to-peer (p2p) VoIP networks** uses a trust enforcement framework consisting of computation and memory bound functions that associate trust implicitly to the p2p VoIP entities (Banerjee et al., 2006). → **Reputation-based spam filtering,** from Rebahi and Sisalem (2005), is a spam-blocking algorithm in which a reputation network manager is built from an SIP repository.

Please cite this article in press as: Dantu R et al., Issues and challenges in securing VoIP, Comput. Secur. (2009), doi:10.1016/j.cose.2009.05.003

Table 2 (*continued*)

Attack type	Attacks reported	Proposed solutions
		→ **Socio-technical defense against voice spamming** is a multi-stage, adaptive spam filter that uses presence (location, mood, time), trust, and reputation to detect spam in voice calls. It was proposed by Kolan and Dantu (2007). → Gritzalis and Mallios (2008) have also identified the need for the identification of spam at the signaling phase and have proposed a framework for spam mitigation in SIP environments. → Soupionis et al. (2008) propose an adaptive policy-based approach for the management of voice spam. The approach is based on the definition of a set of rules along with actions and controls to mitigate the attacks.
Toll Fraud	The financial implications of toll fraud are more profound than perceived by telephone subscribers. The Communications Fraud Control Association (CFCA) conducted a world-wide survey in 2006 (Communications Fraud Control Association) and estimated that telecommunication fraud losses range from US $54.4 to 60 billion—up 52% from the 2003 CFCA survey results. → In a recent scam (Blackwell, 2006), a Spokane resident hacked into an unprotected corporate IP network and into the networks of several VoIP providers. He routed traffic from the company's customer through the corporate network to the VoIP providers. The providers were left with the interconnect charges—as much as $300,000 per victim. → A Miami service provider was reported to have hacked into other provider networks, routing his customers' calls onto their networks and then billing his customers (Teal, 2006).	VoIP providers can prevent toll fraud by properly configuring firewalls and by protecting ports. VoIP providers must also actively monitor their networks, so that they know who is accessing the network and with what frequency and who is generating what kind of traffic.

4. Soft phone security

A soft phone is an application that enables using the computer as a telephone by streaming audio. Most attacks we discussed in Section 3 exploit vulnerabilities when a soft phone is used. In this section, we take a deeper look at security concerns that arise when a soft phone is used.

With the widespread acceptance of VoIP and its price advantage, many leading Web service firms are trying to make their presence known in this field. Skype, one of the first firms to capitalize on VoIP, provides a p2p Internet telephony network. The Skype communications system is notable for its broad range of features, including free voice and video conferencing. Since Skype is closed-code software, there has been a lot of debate about its security features. Yahoo and Google also have similar applications that allow users to make calls for a low cost. Recently, Microsoft unveiled its Office Communicator 2007, a unified communications client with a VoIP soft phone and Web, audio, and video conferencing. We can expect an increasing number of such applications as VoIP becomes more attractive to users, but addressing the security issues discussed in Section 3 will be a challenging task.

As an application, soft phones can have full access to system resources. They can, therefore, take advantage of the privileges of the user who started the soft phone. If the user has administrative rights, the soft phone application can access critical system information. Some of the more common activities that hackers may use to exploit this vulnerability are i) listening to any inputs on the soundcard, ii) reading files and transferring them elsewhere, iii) capturing data being sent to the screen or coming in from the keyboard, iv) scouring your machine to look for passwords, v) disabling antivirus or other protective tools, and vi) monitoring the local area network (LAN) that the computer is attached to and even attacking other machines.

Because the soundcard is always powered on in a personal computer (PC), an attacker's invasive application could switch on the microphone at any time to listen. The soft phone is also a good tool for hackers to send Trojan horses through a network. In addition, soft phones make segregating the voice and data network more difficult. With all these potential attack points, the operating system's security features will determine the success of soft phones. Any weakness in the operating system (OS) will make it easier for attackers to insert malicious applications. This threat to the OS is especially aggravated when soft phones run on devices such as personal digital assistants (PDAs), which lack full-fledged secured OSs. Clearly, the industry must address the security issues related to soft phones before soft phones can be considered reliable means of communication.

Please cite this article in press as: Dantu R et al., Issues and challenges in securing VoIP, Comput. Secur. (2009), doi:10.1016/j.cose.2009.05.003

Table 3 – A high-level security VoIP architecture with enhanced security features.

Type of threat	Media gateway controller	Proxy server	IP PBX	End-user equipment
DoS	Rate controller Authentication module	Application-level firewall (external) Rate controller Authentication module	Authentication module Application-level firewall (internal)	Authentication module Application-level firewall (internal)
Spam and phishing	Spam and phishing filter	Spam and phishing filter with ○ Presence feedback ○ User feedback ○ Call history ○ Nuisance detector	Spam and phishing filter with ○ Presence feedback ○ User feedback ○ Call history ○ Nuisance detector	Spam and phishing filter with ○ Presence feedback ○ User feedback ○ Call history ○ Nuisance detector
Eavesdropping	Encryption	Encryption	Encryption	Encryption Security features in the OS
Packet Spoofing and Masquerading	Authentication	Authentication Encryption	Authentication Encryption	Authentication Encryption
Toll fraud	Authentication	Authentication	Authentication	Authentication

5. Security issues due to PSTN-VoIP internetworking

VoIP and PSTN currently coexist despite their technical differences. Internetworking PSTN and IP networks presents a significant challenge because VoIP and PSTN use widely varying infrastructures and protocols. Interoperability issues arise because of differences in protocols, vendor implementations, the carrier used, and the services provided. These interoperability issues need to be addressed at every interconnection point of the network components.

Today, interoperation is made possible by using the signaling transport protocol (SIGTRAN) (Ong et al., 1999) – a protocol suite proposed by the Internet Engineering Task Force (IETF). This suite allows any subscriber in either network to transparently call a subscriber in another network. Unfortunately, this internetworking makes the infrastructure more vulnerable to attacks. The following are examples of two attacks:

- *Compromised signaling nodes*: Internetworking increases the possibility of signaling nodes' being compromised in the signaling system (SS7) or IP networks. The compromised node can then exploit the signaling messages to disrupt telephone services.
- *Spoofed and fabricated signaling messages*: Spoofing can be used to compromise data integrity and thus prevent the use of the technology in critical domains. When VoIP and PSTN interwork together, the traffic passing through the gateways must be screened. SS7 network's *gateway screening*, the only widely deployed security solution available today, does not check the actual content and structure of the VoIP signaling messages. The inability to interpret or properly parse messages with inappropriate content may cause a serious problem at the signaling node and thereby affect telephone services.

Most current research assumes that the PSTN network is already secure and focuses on securing the IP network. The internetworking of VoIP and PSTN, however, poses new threats to the traditional PSTN network. Thus, system administrators must take great care when plugging security gaps created by the internetworking of VoIP and PSTN.

6. Security architecture for VoIP

Sections 2–5 have discussed the vulnerabilities of a VoIP network in detail. In this section, we propose a high-level security architecture that shows the security features needed at each level in the VoIP infrastructure in order to counter security threats. It should be clear that the proposed architecture is a general solution that needs to be instantiated for different threats and network deployments.

Table 3 summarizes the security functions needed in the various network components to address each security concern. Fig. 2 gives a pictorial representation of how these components should be deployed. The components from Fig. 2 have been represented in Fig. 1 but are now enhanced with the use of information fedback from other components. Each component shown in the architecture diagram can be implemented in several ways. For example, consider the spam filter. It can use the voice spam protection algorithm by using user feedback as proposed by Dantu and Kolan (2004, 2005) and Kolan and Dantu (2009). This algorithm calculates the caller's reputation value with a Bayesian inference function, taking the caller's past history into consideration. As another example, mechanisms proposed for detecting spam e-mails (Palla and Dantu, in preparation, 2006) can be deployed in VoIP systems with some modifications. A variety of filtering techniques have been proposed to restrict spam e-mails. Most of these solutions employ content analysis. In VoIP networks, it is too late detect spam after picking up the phone; so, to counter this problem, we can base filtering on signaling header analysis. Similarly, other components will also have different implementations available from which the security administrator must choose the best one depending on the system's configuration.

The security architecture suggested in this paper requires explicit and implicit feedback from various components at different levels. Fig. 3 depicts a logical flow of information in the architecture diagram. The controllers contain the security components defined in the security architecture.

Please cite this article in press as: Dantu R et al., Issues and challenges in securing VoIP, Comput. Secur. (2009), doi:10.1016/j.cose.2009.05.003

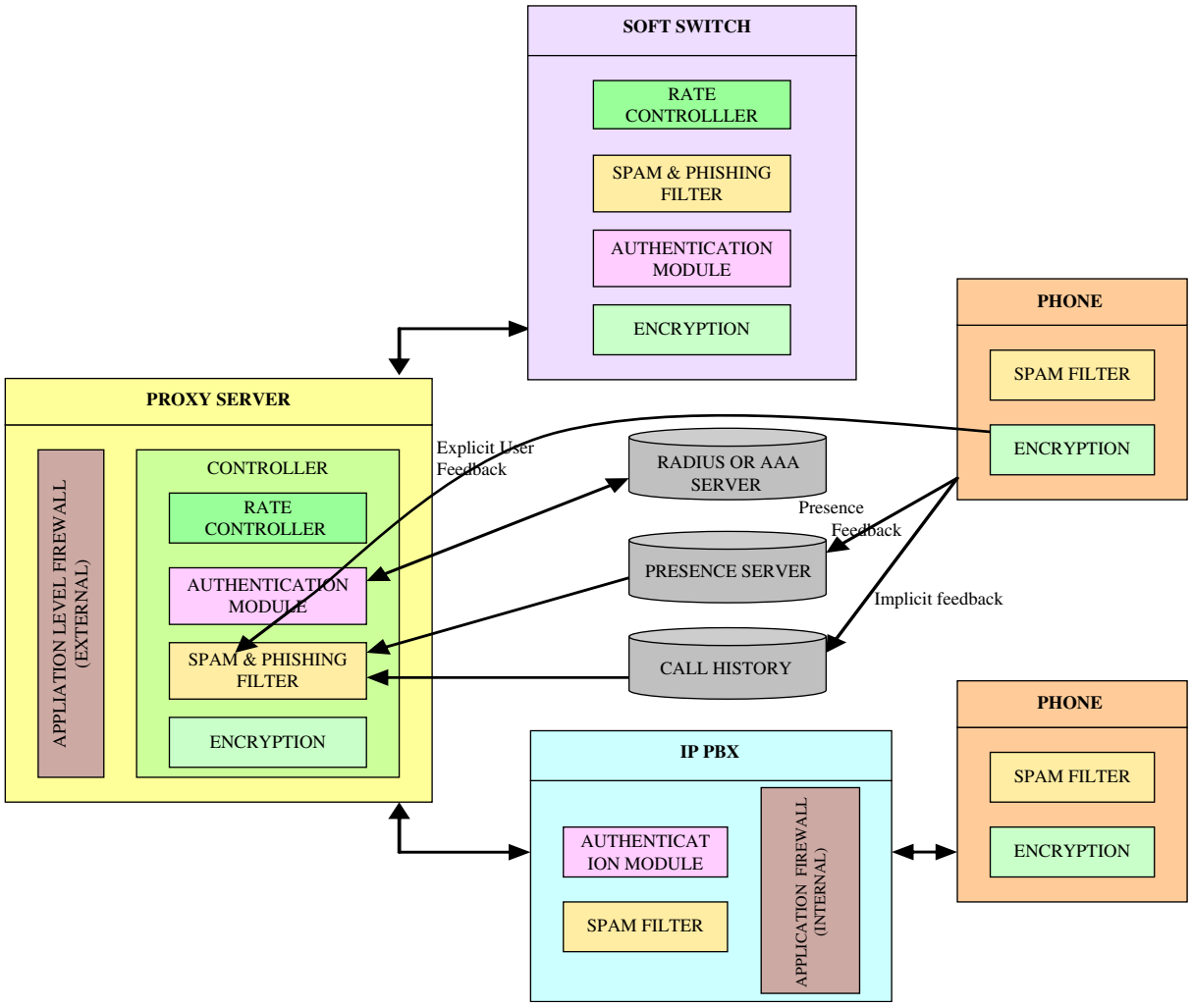

Fig. 2 – A high-level security VoIP architecture with enhanced security features.

Explicit feedback is required to train filters used in the security system. It can also be used by entities to report suspicious activities. Some examples of the use of explicit feedback are as follows:

→ Information provided by the user can flag a particular call as spam.

→ A black list (normally used to filter spam) is used as a form of explicit feedback for updating filters using formats like extensible markup language (XML).

→ When a particular IP PBX detects a phishing activity, then the PBX provides this feedback to other network components to prevent phishing activity from that source in the future.

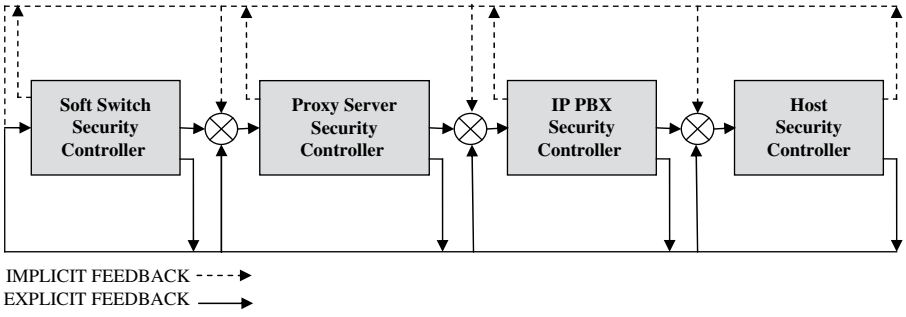

Fig. 3 – Feedback controller.

Please cite this article in press as: Dantu R et al., Issues and challenges in securing VoIP, Comput. Secur. (2009), doi:10.1016/j.cose.2009.05.003

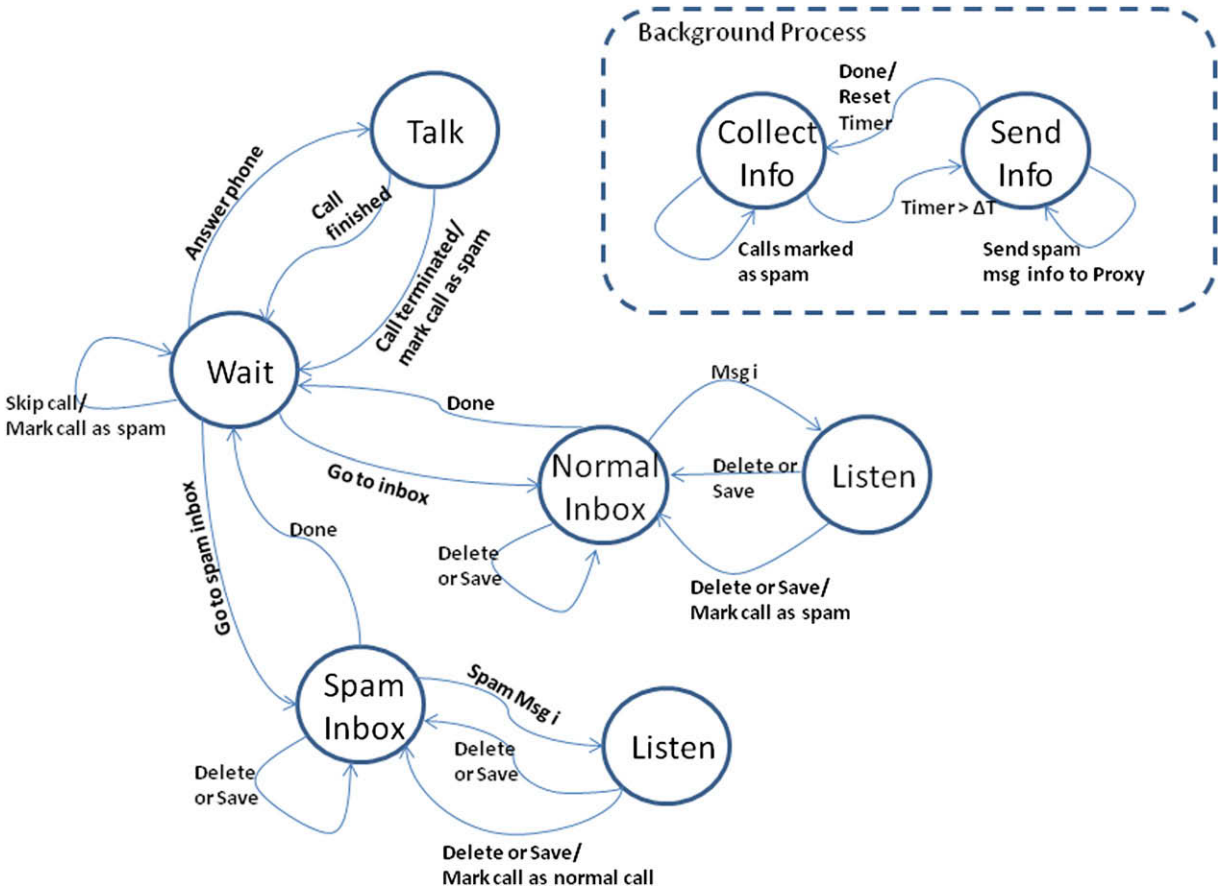

Fig. 4 – State diagram for a phone.

Implicit feedback information is derived without another entity's explicitly stating it. Some examples of the use of implicit feedback are as follows:

→ Analysis of the user's calling patterns for frequency and duration provides useful (implicit) information for improving the performance of a filter.
→ Presence information provides an important source of implicit feedback because it can be used at several levels in the security architecture to filter spam.
→ An increased call rate may implicitly signal a potential attack. If the call rate originating from a host exceeds a preset maximum, the IP PBX goes on alert status to counter possible DoS attacks.

The above examples offer only a few situations in which implicit feedback is useful. Feedback message flows, both implicit and explicit, can be used to provide a robust authentication system. The key exchange process between different entities and other authentication procedures can use this feedback system to remain updated. Protocols to exchange relevant information between controllers should be deployed as depicted in Figs. 2 and 3. Different components need access to different types of information at different levels of abstraction. For example, a firewall needs access to all messages entering or leaving the network. A firewall can supply the transaction logs useful to several other elements in the network. Thus, an efficient information-sharing protocol must guarantee that the required information is available to components in a timely manner.

Protocols for recovery: Recovery mechanisms play a key role in making VoIP systems robust. For example, consider a scenario with a "virus" in an IP phone. If this phone spreads the virus to other elements in the network, then we need mechanisms for graceful shutdown and recovery of the deceased elements in the network. These mechanisms should not affect the throughput of the legitimate calls and cannot be victims to the virus or some other attacks.

Figs. 4 and 5 exemplify how explicit feedback can be a powerful ally to improve voice spam filters performance. The end user can mark a specific call as spam and the information from the call is asynchronously sent to the proxy. As

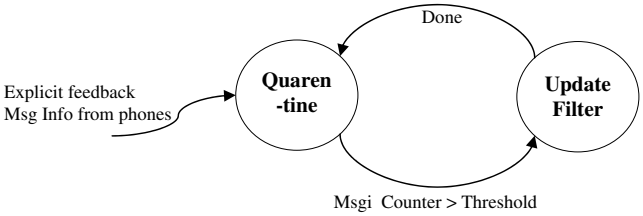

Fig. 5 – Simplified state diagram for the Proxy to handle explicit feedback from the phones.

Please cite this article in press as: Dantu R et al., Issues and challenges in securing VoIP, Comput. Secur. (2009), doi:10.1016/j.cose.2009.05.003

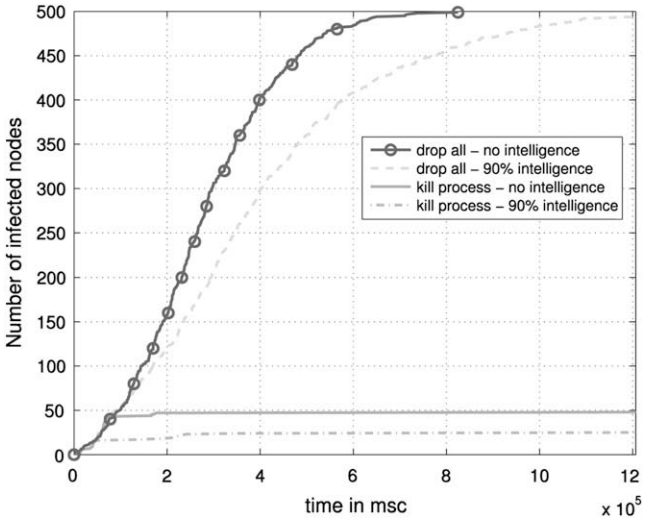

Fig. 6 – Results from the use of a PID controller at both host and FW level (Dantu et al., 2007).

seen in Fig. 4, a background process collects information of the calls marked as spam and sends such information to proxy after a pre-specified time interval; this is done to decrease the communication overhead. However, different users may perceive the call differently. That is, while a call is considered a spam for user A it could be considered normal for user B. Before updating the spam filter properties, as seen in Fig. 5, based on the received information from the phones, the proxy waits until a certain number of similar calls are flagged as spam and only after the threshold is reached the filter is updated. This approach potentially decreases the chances of false negatives. As stated before, these are just examples of how the proposed architecture can be used to improve the security level of VoIP systems; the example is not intended to be a comprehensive solution for voice spam. Another example of how a feedback based architecture can help on security issues is given by Dantu et al. (2007) where feedback from infected machines is used to update the filter and contain a spreading worm. Fig. 6 presents some results of experiments conducted on worming containment. In the figure drop all means that all suspect traffic is dropped from the queue; the level of intelligence quantifies the percentage of proper identification of malicious package; and kill process is used to terminate the process in the host node that is generating the malicious traffic. The results are a clear indication that feedback combined with existing solutions for the identification of malicious traffic provide a more efficient and comprehensive solution (Dantu et al., 2007).

7. Conclusions

This paper outlines security issues in VoIP and suggests an architecture that can assure security at different levels in the VoIP infrastructure. Apart from the isolated incidents of attacks on VoIP that we have discussed, we know of a few widespread attacks unique to VoIP systems; however, unresolved security issues could adversely affect the success of the technology. Users have become accustomed to the 99.999% reliability standard of the PSTN. Most will likely expect VoIP to meet that service level as well. A breach that compromises VoIP security would be detrimental to the public's confidence in the technology, further establishing the need for immediate efforts to secure the VoIP infrastructure. The high-level security architecture proposed can address the security concerns to make the VoIP infrastructure more secure and robust. Authors reported results on the several pieces of the architecture, and further work involves putting the pieces together.

REFERENCES

Axelsson S. Research in intrusion–detection systems. Technical Report 99-15. Dept. of Computer Engineering, Chalmers University of Technology, Sweden; Mar. 2000.

Nilanjan Banerjee, Samir Saklikar, Subir Saha. Antivamming trust enforcement in peer-to-peer VoIP Networks. In: Proceedings of the 2006 international conference on communications and mobile computing, IWCMC'06, Vancouver, Canada; July 2–3, 2006.

Baugher M, Carrara E. The use of timed efficient stream loss-tolerant authentication (TESLA) in the secure real-time transport protocol (SRTP), RFC 4383, Feb. 2006.

Baugher M, McGrew D, Naslund M, Carrara E, Norrman K. RFC 3711 – the secure real-time transport protocol (SRTP). Mar. 2004.

Blackwell Gerry. FoIP (Fraud over IP). VoIP Planet. Available at: http://www.voipplanet.com/trends/article.php/3616771; June 28, 2006.

Communications Fraud Control Association. World-wide telecom fraud survey 2006. Available at: http://www.cfca.org/Documents/fraudloss_press_release.pdf.

Celeste Biever. Move over spam, make way for 'spit.' NewScientist.com news service; Sept. 24, 2004. Available at: http://www.newscientist.com/article.ns?id=dn6445.

Ram Dantu, Prakash Kolan. Preventing voice spamming. VoIP security—challenges and solution, IEEE GLOBECOM 2004, Dallas, TX; Dec. 2004.

Dantu R, Kolan P. Detecting spam in VoIP Networks. USENIX SRUTI'05 Workshop, Cambridge, MA; July 2005, pp. 31–7.

Dantu Ram, Cangussu Joao W, Patwardhan Sudeep. IEEE TDSC – Transactions on Dependable and Secure Computing. Fast worm containment using feedback control April–June 2007; 2(4):119–36.

Dritsas S, Mallios J, Theoharidou M, Marias GF, Gritzalis D. Threat analysis of the session initiation protocol, regarding spam. In: Proceedings of the 3rd IEEE international workshop on information assurance. IEEE Press; 2007. p. 426–33.

Curtis Franklin Jr. Experts: VOIP just another way to Hack, PC Magazine; Jul 02, 2007.

Antone Gonsalves. Phishers snare victims with VoIP. TechWeb Technology News (Apr. 25, 2006). Available at: http://www.techweb.com/wire/security/186701001.

Goode B. Voice over Internet Protocol (VoIP). Proc IEEE Sept. 2002; 90:1495–517.

Gupta Prateek, Shmatikov Vitaly. Security analysis of voice-over-IP protocols. International Association for Cryptologic Research (IACR); 2006.

Gritzalis D, Mallios Y. A SIP-based SPIT management framework. Computers & Security October 2008;27(5–6):136–53.

Please cite this article in press as: Dantu R et al., Issues and challenges in securing VoIP, Comput. Secur. (2009), doi:10.1016/j.cose.2009.05.003

The Internet Engineering Task Force (IETF). http://www.ietf.org/.
Jackson Higgins Kelly. Vishing' attacks use VOIP, dark reading news analysis. Available at: http://www.darkreading.com/document.asp?doc_id=98787; July 10, 2006.
Kirk Jeremy. Worm may be spreading via Skype chat. IDG News Service. Available at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=voip&articleId=9006239&taxonomyId=81 Dec. 19, 2006.
Prakash Kolan, Ram Dantu. Socio-technical defense against voice spamming. ACM transactions on autonomous and adaptive systems (TAAS), MA; 2007.
Prakash Kolan, Ram Dantu. Nuisance of a Voice Call. ACM Transactions on Multimedia Computing, Communications and Applications (TOMCCAP); February, 2009.
Kent S, Atkinson R. RFC 2401-security architecture for the internet protocol. RFC 201. Internet Engineering Task Force Nov. 1998.
Leyden John. Cisco VoIP kit open to 'snooping attacks'. Available at: http://www.theregister.co.uk/2004/02/20/cisco_voip_kit_open/; Feb. 20, 2004.
Long Tom. Eavesdropping an IP telephony call. SANS Institute; 2002.
Marias GF, Dritsas S, Theoharidou M, Mallios J, Gritzalis D. SIP vulnerabilities and antiSPIT mechanisms assessment. In: Proceedings of the 16th IEEE international conference on computer communications and networks (ICCCN'07). IEEE Press; 2007. p. 597–604.
Edwin Mier, Randall Birdsall, Rodney Thayer. Breaking through IP Telephony. Network World Lab Alliance, May 24, 2004. Available at: http://www.nwfusion.com/reviews/2004/0524voipsecurity.html.
Robert McMillan. Georgia student arrested for hacking grades, VoIP, IDG News Service, PC World Magazine; Jul 29, 2008.
Mukherjee B. Network intrusion detection. IEEE Network 1994; 8(3):26–41.
Robert MacIntosh, Dmitri Vinokurov, Alcatel. Detection and mitigation of spam in IP telephony networks using signaling protocol analysis. In: Advances in Wired and Wireless Communication, IEEE/Sarnoff Symposium, NJ; 2005.
National Cyber-Alert System. Vulnerability Summary CVE-2005-1802, National vulnerabilities database. Last revised 10/20/2005. Available at: http://nvd.nist.gov/nvd.cfm?cvename=CVE-2005-1802.
Network computing. Security big security flaws found in Asterix PBX, IAX VoIP Client. Available at: http://www.networkcomputing.com/channels/networkinfrastructure/showArticle.jhtml?articleID=189400851; June 13, 2006.
Oulu University Secure Programming Group. PROTOS test-suite: c07-sip. Available at: http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/.
Ong L, Rytina I, Garcia M, Schwarzbauer H, Coene L, Lin H, Juhasz I, Holdrege M, Sharp C. RFC 2719: framework architecture for signaling transport. IETF Network Working Group; Oct. 1999.
Srikanth Palla, Ram Dantu. Detecting phishing in emails. In: Proceedings of MIT Spam Conference; 2006.
Srikanth Palla, Ram Dantu. Detecting Spam and phishing in emails using SMTP Paths. ACM Transactions on the Web, in preparation.
Qovia, Inc., Frederick, MD 21703.
Ryst. Sonja. The phone is the latest phishing rod. Business Week. Available at: http://www.businessweek.com/technology/content/jul2006/tc20060710_811021.htm July 11, 2006.
Rosenberg J, Schulzrinne H, Camarillo G, Johnston A, Peterson J, Sparks R, Handley M, Schooler E. SIP: Session Initiation Protocol. RFC 3261. Internet Engineering Task Force June 2002.
Rebahi Y, Sisalem D. SIP service provides and the spam problem. In: 2nd workshop on securing voice over IP, Washington, DC; June 1–2, 2005.
Richard Kuhn D, Walsh Thomas J, Fries Steffen. Security considerations for voice over IP systems. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology; 2004.
Salsano S, Veltri L, Papalilo D. SIP security issues: the SIP authentication procedure and its processing load. IEEE Network Nov./Dec. 2002;6(16):38–44.
Schulzrinne H, Casner S, Frederick R, Jacobson V. RFC 1889–RTP: a transport protocol for real-time applications. Jan. 1996.
Soupionis Y, Dritsas S, Gritzalis D. An adaptive policy-based approach to SPIT management. In: Proceedings of the 13th European symposium on research in computer security (ESORICS 2008). Springer; 2008. p. 446–60.
Teal Kelly M. VoIP network security: how a Hacker took advantage of vulnerabilities. New Telephony. Available at: http://www.businessweek.com/technology/content/jul2006/tc20060710_811021.htm June 14, 2006.
VoIP Magazine Editorial Staff. ISS finds flaws in Cisco VoIP. VoIP Magazine News. Available at: http://www.voip-magazine.com/index.php?option=com_content&task=view&id=272 July 13, 2005.
Charles Wright, Lucas Ballard, Scott Coull, Fabian Monrose, Gerald Masson. Spot me if you can: uncovering spoken phrases in encrypted VoIP conversations. In: 2008 IEEE symposium on security and privacy, May 18–22, 2008, Berkeley/Oakland, California, USA.

Dr. Ram Dantu (rdantu@unt.edu) has 20 years of experience in the networking industry where he worked for Cisco, Nortel, Alcatel, and Fujitsu, and was responsible for advanced technology products from concept to delivery. For the last five years, he has been researching prevention of DoS and spam attacks in VoIP networks. He has co-chaired three workshops in VoIP security. He is currently an assistant professor in the Department of Computer Science and Engineering at the University of North Texas (UNT). His research focus is on detecting spam, network security, and next-generation networks. He is the founding director of the Network Security Laboratory (NSL) at UNT. The objective of NSL is to study the problems and issues related to next-generation networks. Prior to UNT, he was technology director at Netrake, where he was the architect of the redundancy mechanism for VoIP firewalls. His additional experience includes as technical director in IpMobile (acquired by Cisco) where he was instrumental in the wireless/IP product concept, architecture, design, and delivery. In addition to more than 70 research papers, he has authored several RFCs related to MPLS, SS7 over IP, and routing. Due to his innovative work, Cisco and Alcatel were granted a total of twelve patents; another eight are pending.

Professor Sonia Fahmy's research interests lie in the design and evaluation of network architectures and protocols. She is currently investigating Internet tomography, network security, and wireless sensor networks. Her work is published in over 80 referred papers, including publications in IEEE/ACM Transactions on Networking, Computer Networks, IEEE INFOCOM, and IEEE ICNP. She received the National Science Foundation CAREER award in 2003, the Schlumberger foundation technical merit award in 2000 and 2001, and the OSU presidential fellowship for dissertation research in 1998. Some of the results of her work were incorporated into the ATM Forum traffic management specifications 4.0 and 4.1, and a patent has been awarded for her work on the ERICA algorithm for network

Please cite this article in press as: Dantu R et al., Issues and challenges in securing VoIP, Comput. Secur. (2009), doi:10.1016/j.cose.2009.05.003

congestion control. She has served on the organizing or technical program committees of several conferences including IEEE INFOCOM, ICNP, BroadNets, and ICDCS. She is a member of the ACM, and a senior member of the IEEE.

Prof. Henning Schulzrinne received his undergraduate degree in economics and electrical engineering from the Darmstadt University of Technology, Germany, his MSEE degree as a Fulbright scholar from the University of Cincinnati, Ohio and his Ph.D. degree from the University of Massachusetts in Amherst, Massachusetts. He was a member of technical staff at AT&T Bell Laboratories, Murray Hill and an associate department head at GMD-Fokus (Berlin), before joining the Computer Science and Electrical Engineering departments at Columbia University, New York. He is currently chair of the Department of Computer Science. He is editor of the ''IEEE/ACM Transactions on Networking'', the ''ACM Transactions on Multimedia Computing'', the ''ComSoc Surveys & Tutorials'' and the ''IEEE Internet Computing Magazine'', and a former editor of the ''IEEE Transactions on Image Processing'' and ''Journal of Communications and Networks''. He has been a member of the Board of Governors of the IEEE Communications Society and is vice chair of ACM SIGCOMM, former chair of the IEEE Communications Society Technical Committees on Computer Communications and the Internet and has been technical program chair of Global Internet, IEEE Infocom, NOSSDAV, IM, NETWORKS and IPtel and was General Chair of ACM Multimedia 2004. He serves on the Internet2 Applications, Middleware and Services Advisory Council. He also has been a member of the IAB (Internet Architecture Board). Protocols co-developed by him are now Internet standards, used by almost all Internet telephony and multimedia applications. His research interests include Internet multimedia systems, quality of service, and performance evaluation. He served as Chief Scientist for FirstHand Technologies and Chief Scientific Advisor for Ubiquity Software Corporation. He is a Fellow of the IEEE, has received the New York City Mayor's Award for Excellence in Science and Technology, the VON Pioneer Award and the TCCC service award.

Joao W. Cangussu received a B.S. degree in Computer Science from the Federal University of Mato Grosso do Sul-Brazil in 1990 and a M.S. in Computer Science from the University of Sao Paulo at Sao Carlos-Brazil in 1993. He received a Ph.D. degree in Computer Science from Purdue University in 2002. He is currently an Assistant Professor in the Department of Computer Sciences at the University of Texas at Dallas. His research interested are software process modeling and control, software testing, adaptive systems, and network security. He is a member of the IEEE and the ACM.