Global Information Assurance Certification Paper

Jason Kelly
GSEC Practical Version 1.4b
12/21/2002

Unified Communications Technologies

Abstract
This paper will cover the basics of unified Communications. What it is, how it works and how it is vulnerable to attack. I will begin with a short discussion on how the Unified Communications Server fits into the traditional communications networks of telephone, voice mail, fax, and Email, and the new technologies involved in making a messaging environment a communications environment. The paper will then discuss the security implications of unified communications particularly focusing on new technologies and how traditional technologies are exposed in new ways. Finally I will finish up by discussing design of a secure Unified Communications Environment.

In order to simplify this topic I will use the Avaya Unified Messenger Application Server as an example. This product integrates Microsoft Exchange and many PBXs' and Voice mail systems. Although there are products available which perform all the functions of Unified Messaging the most popular products are those which leverage existing investments in voice and data communications. In this category are also the Cisco Unity and Nortel Networks Call Pilot

Introduction
Unified Communications is the convergence of traditional forms of messaging; telephone, voice mail, fax with newer electronic communications such as email and instant messaging. A Unified Communications System will allow access to messaging applications from a variety of devices PC's, handheld wireless devices, or telephones, from both the intranet and the internet. Unified messaging will allow you to respond quickly to any type of incoming communication—whether you are onsite or remote. Email and voice mail will be available anytime anywhere using follow me / find me technologies. Short Message Service (SMS) notifications can be sent to a cell phone, hand held PC or PDA. Faxes and voicemail can be sent directly to the users desktop, voice mail, email and faxes can be retrieved from any telephone. This would allow anyone to send a message to anyone regardless of the media involved, thus allowing someone to send voice messages to a telephone from a text-messaging device, or review email from a telephone. Any device can receive notifications sent to a user. Communications between users are facilitated by location awareness or the ability of the communications system to know which device the recipient of the message is using. Two such protocols developed to support this, are session initiation protocol (SIP), and session description protocol (SDP), which were designed to work on traditional IP networks and support TCP, UDP, DNS and other internet protocols.

Unified Communications Technologies

Short Message Service (SMS)
Defines the message format transmitted and received by GSM compliant cell phones

Email
Text messages sent electronically through the public internet

Groupware
Shared email mailboxes, scheduling and collaboration tools such as Microsoft Exchange.

Voice over Internet Protocol (VoIP)
Allows voice messages to be transmitted over traditional IP networks using protocols such as SIP or H.323

Voice Mail
Voice mail is the traditional method for receiving, transmitting and forwarding voice messages. Examples of voice mail systems include the Intuity Audix and

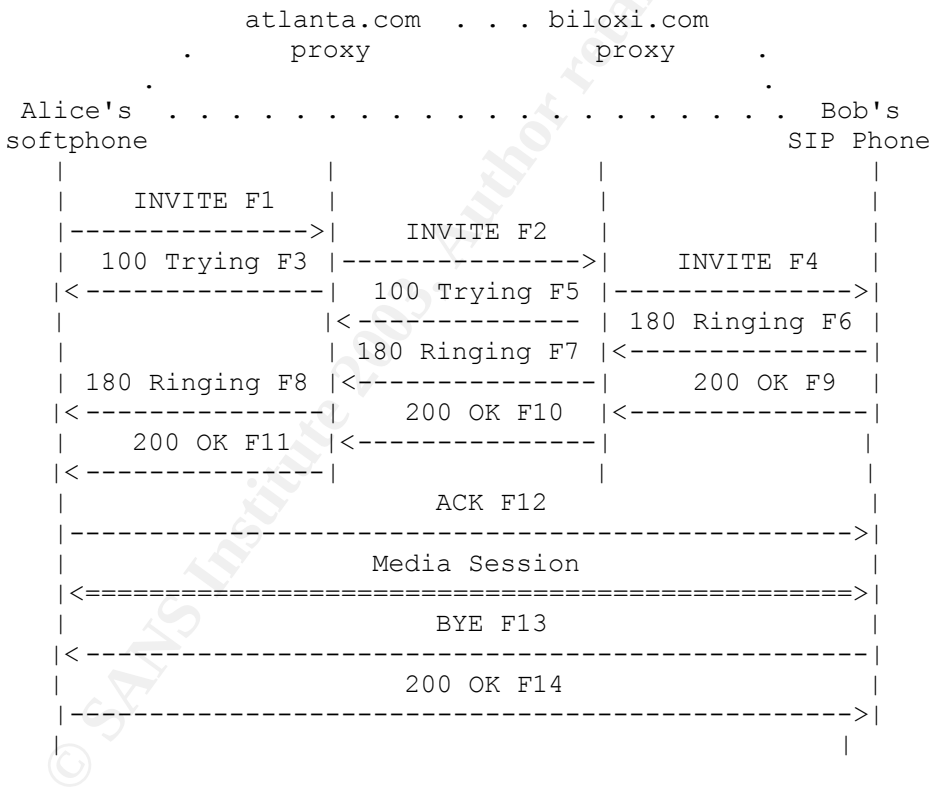
Private Branch Exchange (PBX)
Equipment installed on the customers premises to provide dial service and share a limited number of telephone numbers among a large number of users, generally refers to the privately owned circuit switch that serves as a branch of the switching equipment found at the central exchange office. This includes equipment such as Avayas' Definity, Octel, Merlin and Partner systems.

Session Description Protocol (SDP)
IETF standard protocol for many to many multimedia communications between devices, Session Description Protocol is used in conjunction with Session Initiation Protocol to facilitate the appropriate method of communication between devices.

Lightweight Directory Access Protocol (LDAP)
A set of protocols for accessing information directories, LDAP supports TCP/IP. Microsoft Exchange 2000 stores messaging information in LDAP directories.

Session Initiation Protocol (SIP)
An important part of a Unified Communications System is the Session Initiation Protocol (SIP) "an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants" (1) IETF RFC 3261. To accomplish this "SIP enables the creation of an infrastructure of network hosts (called proxy servers) to which user agents can send registrations, invitations to sessions, and other requests"(1) IETF RFC 3261. The RFC for SIP

calls for a particular series of action and response in order to initiate a call. A user initiates a call; the device sends an INVITE request containing the users address and the invitees address in the form of a Uniform Resource Indicator (URI) such as sip:joesmith@sipuri.com, to a proxy server which receives the call. The proxy performs a type of DNS lookup to determine the address of the domain of the invitee and forwards the request to a proxy server in that domain usually the invitees' registrar server. The proxy modifies the request header to include a VIA field and sends a TRYING response back to the caller. The invitees' proxy server adds another VIA field to the request header, sends a TRYING response to the caller, and forwards the packet to the invitees' device. If the invitee responds to the invitation the device sends an OK response directly to the callers' device. Once the users device is contacted it responds by sending an acknowledge signal and looking up the originating User Agent (UA) via the proxy servers on the way. Once the call is established, the two devices communicate directly with one another and there is no need for the continued use of proxies. This is referred to as the "SIP Trapezoid" (1).



SIP session setup example with SIP trapezoid
Source IETF RFC 3261 (1)

Unified Messenger Server

Such as Ayaya Unified Messenger Application Server, works in conjunction with existing Telephony, fax, voice mail and email systems such as Avayas' Definity, Intuity Audix and Microsoft Exchange to provide a single interface for managing voice mail, email and faxes. The Unified Messaging Server enables traditional

voice mail servers to store voice mail and Fax Servers to store faxes in the Microsoft Exchange Directory Store. In addition, the Unified Messenger Server utilizes Session Initiation Protocol to intelligently route calls to an end user. Messages can be retrieved from the unified messaging system using any type of device, PC using Microsoft Outlook, Mobile device through a web browser or from any telephone.

Unified Messaging Client

"is installed on a desktop PC and integrates with Microsoft Outlook to provide voice message recording and playback "(7). Microsoft Outlook provides the PC desktop interface for viewing, retrieving and sending email, voice mail and fax messages.

Vulnerabilities and Threats

The Unified Messaging Server is installed to enhance an existing messaging environment. This includes traditional groupware such as Microsoft Exchange and Voice messaging technology such as the Avaya Definity and Intuity Audix. In order to assure a secure deployment of the Unified Messenger Server it is important to understand the types of attack, which can be launched against it and against the other components of a unified messaging system. The components that are most vulnerable to attack are the web client, the groupware server, the PBX, the voice mail server and the Unified Messenger Server. The most likely types of attack include Denial of Service, Theft of Service, and Information theft.

Denial of Service can be accomplished by various means. The more traditional Denial of Service and Distributed Denial of Service attacks involve flooding the host with so many requests for service that no legitimate requests can be processed. Often the attacker will provide random fake return addresses to make this kind of attack more difficult to trace.

Theft of Service is usually a function of PBX or voice mail hacking. Theft of Service occurs when the attacker accesses the PBX and uses desirable functionality to charge long distance calls to the targets' phones, or when the attacker creates a mailbox on the targets' system to receive messages.

Information Theft occurs when an attacker accesses information to which he/she has no explicit permission. Information Theft can be accomplished by listening to a conversation in any way, hooking into a phone line sniffing packets of an Ethernet network hacking into and stealing messages from a voice mail or email server, redirecting messages to someone other than the intended recipient or simply deleting messages. This can result in anything from minor inconveniences to a major catastrophe depending on the type of information stolen and in what way.

In order to provide a secure messaging environment it is important to ensure that each component is properly secured. As Telephony, Voice Mail and Groupware

security have been discussed in detail elsewhere I will summarize those topics and move on to discuss the Unified Messaging Server in more detail.

Email / Groupware

Microsoft Exchange is an example of typical email / groupware software involved in unified messaging. As an email server, port 25 has to be left open in order to process incoming and outgoing mail requests, port 25 is a favorite of hackers and there are many potential exploits against it. The simplest method of protecting against attacks on port 25 is to place an SMTP proxy, with anti virus protection in your DMZ in order to intercept any traffic into your mail server. This serves the dual purpose of intercepting attacks on port 25 and removing virus' before they reach users mailboxes. An application level firewall will detect SMTP traffic and scan it to make sure that it conforms to the SMTP specifications. Many organizations that have traveling employees also open Port 110 for POP access to mailboxes or port 143 for IMAP. These ports should not be left open to the internet and if absolutely necessary should require secure authentication before allowing a connection and all connections should be encrypted.

Voice Mail and Telephony

The Avaya Definity PBX is a common piece of customer premise equipment, often found in conjunction with an Intuity Audix Voice mail system. Common attacks against telephony systems include theft of service, denial of service and theft of information. This is generally facilitated by the lack of awareness of potential damage, which can be done through an unsecured telephony system. The basic steps which can be taken to secure PBX and voice mail include ensuring that passwords are at least seven characters and expire after a set period. In addition, if support personnel require remote access to the system, each connection must be secured with a hardware lock and key type device so that only authorized users are able to authenticate to the system. Call forwarding should be restricted to internal extensions and local calls only, and Direct Inward System Access should be disabled.

Unified Messenger

When a device comes on line it, sends a registration request to the Unified Communications Server. Those devices not registered already can be registered manually and activated by dialing a number and entering a code. The communications ability of each device is recorded in the system so that each type of call is directed appropriately. Thus, whether one user wishes to reach another by instant messenger, email or telephone the call will always reach the appropriate device.

The Unified Communication Server acts as a gateway device between a SIP network and traditional voice and data networks and fax machines. It translates SIP URIs' into addresses on the private network such as telephone numbers or private IP addresses and vice versa. It also maintains information about users status, whether to send calls to voice mail or forward emails to a handheld device

etc. The UCS also provides a web interface for the UM client application so that mobile users can access voice, text and fax messages from any internet enabled device.

In order to secure a system, which is such a critical piece of communications infrastructure we need to understand the many ways in which service can be disrupted and information misdirected, lost or stolen. The UCS has to be exposed to the internet and to the public telephone networks. The most likely types of attack against a unified communications environment are Denial of Service, Call Hijacking and Eavesdropping, Man in the Middle type attacks. Because of the way in which SIP works there are several ways in which each can be accomplished.

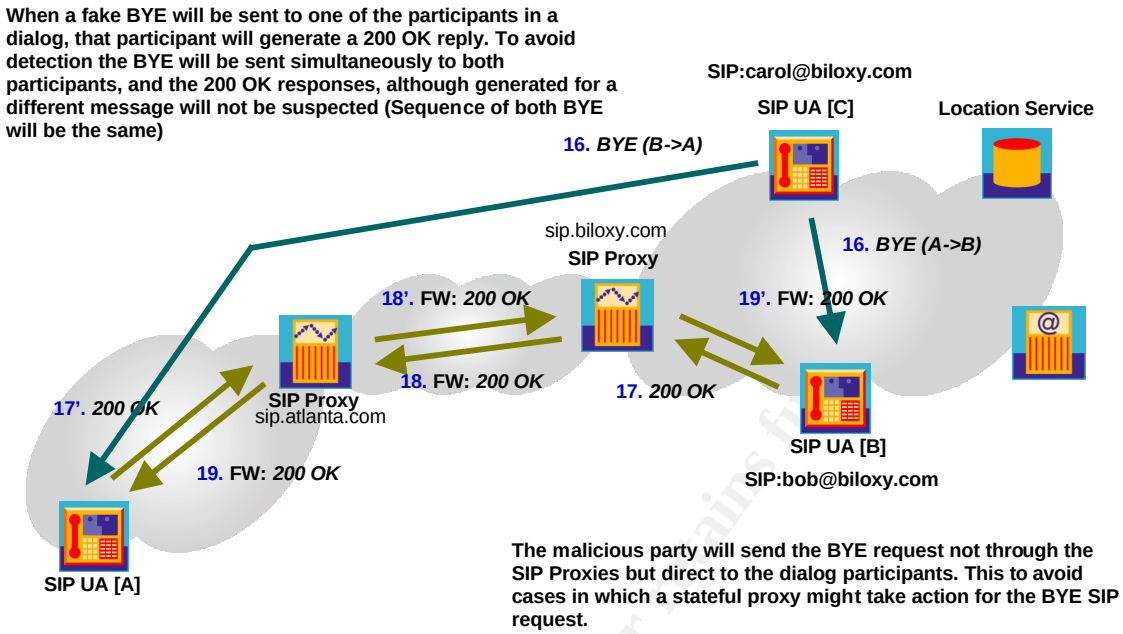
Attacks

Denial of Service

A denial of service attack can be directed against an end users device or against any of the servers involved in the process, using the SIP protocol mechanisms or more traditional Denial of Service techniques. Using SIP messages an attacker monitoring a SIP proxy server can wait for a call to arrive directed toward a specific user. Once the users' device receives the INVITE request the attacker can immediately send a CANCEL request and cause the invitees' device to generate an error and end the call. This type of attack can be very effectively used to interrupt communications; however the target will quickly realize that they are being targeted as incoming calls will be repeatedly ended. The caller will also be able to determine that the invitee is being service denied because the RFC calls for a specific error response to be sent to a cancel. In a unified communication environment the UCS which maintains the registration database for SIP contains information about alternate possible locations to send calls so if the invitee is unable to answer the call the call will be directed to a message store, voice mail, email etc.

Another type of Denial of Service which is directed against the end user is to send a BYE response to either the caller or the invitee. Although this is most effective at the moment of initiation of the call, it can be used to disrupt the call at any point. Because the RFC calls for CANCEL and BYE requests to receive a specific error response BYE denial of service attacks need to be sent simultaneously to both clients in order to avoid suspicion. This type of attack would also defeat the call going to the message store because the call is completed before it is ended, thus the UCS no longer has control of the call.

Denial of Service – BYE (to Both)



Source http://www.blackhat.com/presentations/win-usa-02/arkin-winsec02.ppt page 86 (13)

A well designed SIP device will have stateful inspection built into the protocol stack and is able to determine that the CANCEL or BYE request is not coming from the caller and should be ignored. If the SIP device is on a private network the UCS acts as a redirect server and is a stateful PROXY, this means that all communications to the end user are proxied through the UCS and as such are not vulnerable to this type of attack.

The registration server itself is a potential source of denial of service to the end user. Because the registration server can accept registrations from any device, a new registration with a "*" in the registration header supersedes any previous registration. This is also a desirable behavior, in order to enable follow me technologies a users device must be able to become the primary device as it comes on line. The UCS should be configured to require any device to authenticate before adding or updating a registration. Each device which a user will use should also be pre registered with the system and only those devices should be able to authenticate with the system.

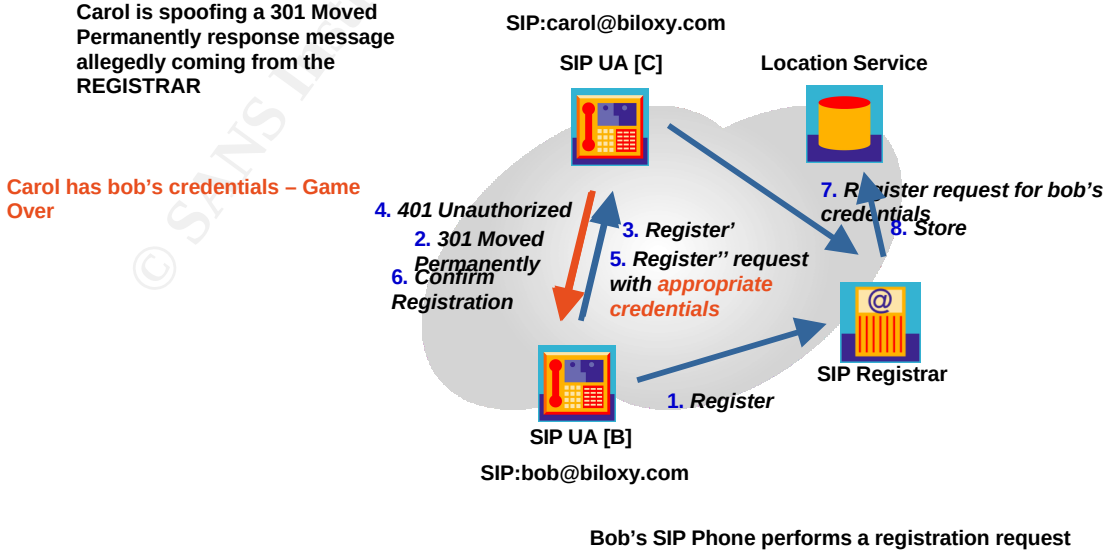
More traditional denial of service and distributed denial of service attacks are possible using desirable features of the SIP protocol. These include sending an INVITE request to a large number of SIP users simultaneously falsifying the targets address of record, causing all the devices to respond to the device simultaneously creating a denial of service situation.

Eavesdropping

According the RFC for SIP it is desirable that the user agent client be able to send re-INVITE requests to change the type of communication, so that in mid call a caller or invitee can change the communication type to include other messaging types. Because of this feature it is possible for a call to begin as a voice call and be altered mid call to include text, pictures or other multimedia. The re-INVITE could also specify a new location for the recipient of the conversation. While this behavior is desirable it is also exploitable. Once a conversation is established an attacker could send a re-INVITE to a participant in the conversation to add an additional participant in order to eavesdrop on the conversation.

In order to prevent other types of man in the middle (eavesdropping) attacks, the recommendations of the SIP working groups' security mechanisms need to be implemented on the UCS and all devices which will communicate with it. This document specifies methods of exchanging information about secure transport levels available between the client and the server. However, as these methods have not been formalized there exists the potential for a malicious entity to spoof a response from a registration server. The spoofed response could contain any legitimate response from a registration server, including authentication required, payment required, unauthorized etc. The RFC recommends that the client, upon receiving these types of responses, should not retry the request without modifying it, or sending the same request to a different server. This would result in the client sending authentication information, perhaps credit card information to the attacker. The attacker may also spoof a response such as moved permanently causing the client to send all future registration requests to a malicious registration server with all the potential consequences listed above.

Man In The Middle attack V's Registrar



Source http://www.blackhat.com/presentations/win-usa-02/arkin-winsec02.ppt page 86 (1)

Message Hijacking
There are scenarios in which it is desirable for an attacker to redirect messages to a destination other than the one intended. Times and dates for meetings, drafts of critical documents and other critical information are sent through voice mail and email. Am attacker could benefit from preventing such information from being received at all, or from sending modified versions to the intended recipient.

An attacker can accomplish this using a combination of the two attacks above. First, the UCS registration server database needs to be compromised and a mailbox needs to be defined as an address of record to send messages to. Then the victims' current device must be Service Denied. Once these two tasks are accomplished, any messages sent to the victim will default into the compromised mailbox and be retrieved by the attacker without the victim ever receiving the message.

Prevention
To prevent the exploitation of these desired features for malicious use the UCS needs to implement an authentication system. The draft IETF SIP security document (15) suggests one mechanism to accomplish this. The client device advertises the security protocols it supports, the server responds with the protocols it supports. The client then chooses the first protocol from the list with a match in the list advertised by the server, once a security protocol such as IPSEC is agreed upon the client and server can communicate securely. This is only controllable within the corporate network and to make sure that flexibility of communication is ensured devices have to be backward compatible and able to communicate with devices which are not compliant with the proposed security guidelines. This means that while the UCS can be secured within the corporate environment once communications are initiated with people outside the controlled network the call is subject to denial of service, eavesdropping, hijacking and man in the middle attacks.

In order to minimize the potential for damage, precautions can be taken; communications should be encrypted with s/mime for end-to-end body encryption of the message. This is specified in the SIP RFC as desirable and should be implemented in any UCS deployment; s/mime is also useful for authenticating the identity of the end users. This is important in preventing an attacker from sending malicious BYE requests. The UCS also needs to require authentication of any device requesting registration in order to prevent inappropriate registrations and registration server Denial of Service attacks.

At the network perimeter a SIP aware firewall should be deployed which can examine SIP headers to ensure they are compliant with the RFC, standard

techniques should be employed to protect the email and voice mail servers and gateways which are integral to the Unified Communication environment.

As with any computing solution exposed to the public internet Unified Communications Systems cannot be made 100% secure, as long as standard procedures are followed with all the involved systems then the UCS can be deployed as an integral component of corporate communications.

Conclusion

The features of a unified messaging system are highly desirable in the modern corporate environment. This means that systems such as this will be deployed ever more widely. The nature of these systems means that they contain sensitive information that will be exposed to public networks making them targets for attack. Unified Communications Systems can be deployed in a secure fashion as long as the proper precautions are taken when purchasing components, developing the software and deploying the applications.

References

1. J. Rosenberg, et. al., RFC 3261 SIP: Session Initiation Protocol, June 2002 http://www.ietf.org/rfc/rfc3261.txt
2. Weber, Chris**,** Securing Exchange 2000, Part 2, May 8, 2002, http://online.securityfocus.com/infocus/1578
3. Silbaugh, Jean, It Is Only Dialtone, September 8, 2000 http://rr.sans.org/wireless/dialtone.php
4. Waldrop, Brian L., Securing the Other System: Basic PBX Functionality and Vulnerabilities, April 24, 2001 http://rr.sans.org/telephone/PBX.php
5. English, Bill, Securing Exchange 2000 Server E-mail, March 14, 2002, http://rr.sans.org/email/sec_exchange.php
6. AVAYA, Security in Converged Networks, September 2002, http://www1.avaya.com/enterprise/whitepapers/msn1841.pdf
7. Avaya , Unified Messenger Microsoft Exchange Version, Components, http://www.avaya.com/ac/common/index.jhtml?location=M1H1005G1007F2033P3085N4601
8. AVAYA , Unified Messenger Microsoft Exchange Version, Technical Specifications, http://www.avaya.com/ac/common/index.jhtml?location=M1H1005G1007F2033P3085N4603
9. AT&T, Audix Administration, November 1993, http://support.avaya.com/edoc/docs/audix/aud8adm4.pdf
10. AVAYA, BCS Product Security Handbook, December 1997, http://support.avaya.com/elmodocs2/definity/ds9_ip600/233416_1/025600_6/025600_6.pdf

11. AVAYA, INTUITY™ AUDIX® Multimedia Messaging Server, http://www.avaya.com/ac/common/index.jhtml?location=M1H1005G1007F2027P3074N4504
12. AVAYA, Unified Messenger® -- Microsoft® Exchange version, Product Summary, http://www.avaya.com/ac/common/index.jhtml?location=M1H1005G1007F2033P3085N4596
13. Arkin, Ofir, VoIP The Next Generation of Phreaking, Version 1.1, http://www.blackhat.com/presentations/win-usa-02/arkin-winsec02.ppt
14. Schulzrinne, Port Assignments, http://www.cs.columbia.edu/sip/assignments.html
15. J. Arkko ET. Al., Security Mechanism Agreement for the Session Initiation Protocol (SIP), http://www.ietf.org/internet-drafts/draft-ietf-sip-sec-agree-05.txt