[ASRSt01] *Ralf Ackermann, Markus Schumacher, Utz Roedig, Ralf Steinmetz;* **Vulnerabilities and Security Limitations of current IP Telephony Systems;** Conference on Communications and Multimedia Security (CMS 2001), May 2001, S. 53-66.

VULNERABILITIES AND SECURITY LIMITATIONS OF CURRENT IP TELEPHONY SYSTEMS

Ralf Ackermann
Darmstadt University of Technology
Industrial Process and System Communications (KOM)
Ralf.Ackermann@KOM.tu-darmstadt.de
Markus Schumacher
Darmstadt University of Technology
IT Transfer Office (ITO)
Markus.Schumacher@ITO.tu-darmstadt.de
Utz Roedig
Darmstadt University of Technology
Industrial Process and System Communications (KOM)
Utz.Roedig@KOM.tu-darmstadt.de
Ralf Steinmetz
Darmstadt University of Technology
Industrial Process and System Communications (KOM)
German National Research Center for Information Technology (GMD IPSI)
Ralf.Steinmetz@KOM.tu-darmstadt.de

Abstract Within the traditional telephone system a certain level of quality and security has been established over the years. If we try to use IP Telephony systems as a core part of our future communication infrastructure (e.g. as classical PBX enhancement or replacement) continuous high availability, stable and error-free operation and the protection of the privacy of the spoken word are challenges, that definitely have to be met.

Since manufacturers start deploying new end systems and infrastructure components rather fast now - a critical inspection of their security features and vulnerabilities is mandatory. The critical presentation of the theoretical background of certain vulnerabilities, testing and attacking tools and the evaluation results reveals, that well-known security flaws become part of implementations in the new application area again and the security level of a number of examined solutions is rather insufficient.

Keywords: Internet Telephony, Security, Protocols, Vulnerabilities, System Evaluation

1. INTRODUCTION

IP telephony applications are considered to have a huge economic potential in the near future. The role of IP telephony can be described as a specific part of a continuously emerging scene of more general multimedia applications. Concerning signaling protocols, interfaces and implementation details, we currently face a lot of work in progress with high dynamics and multiple concurrent approaches.

Security and privacy are mandatory requirements for this application area. Unfortunately developers do not pay too much attention to these features, they are often seen as a "add-on task", following the implementation of the basic (communication) functionality.

Our paper tries to create security awareness in the field of IP telephony and addresses mainly two target groups: First, potential consumers of IP telephony solutions, who should be able to "ask the right questions" and perform checks with the supplied tools. Second, developers (protocol designers, implementors and vendors) of IP telephony equipment, that can either fix problems in their current products and (even more important) may reason about pro-active security approaches in their future designs.

From our point of view, presenting the information does not increase the risk for current IP Telephony system installations. Both customers and vendors will benefit, if security limitations are discussed *before* potential attackers start exploiting them and the installed base (with severe vulnerabilities) gets really large.

The shown vulnerabilities have not been published immediately after discovery. On the contrary, we have informed the vendors in order to enable them to work on effective solutions for final products. As stressed in [9] a skilled attacker has probably already discovered the described flaws. Then concealing of the security problems would just cause the contrary of the (perhaps initially good) intention not to spread the knowledge.

2. TERMINOLOGY AND EVALUATED SCENARIO

A system component shows a (security) vulnerability if protected in an insufficient way against abuse. Once advantage is taken of this vulnerability, the security provided for the system in question is jeopardized [9]. In order to understand the potential reasons and nature of the vulnerabilities to be shown, we will first describe the characteristics of the evaluated IP Telephony scenario.

2.1. GENERIC IP TELEPHONY SCENARIO

Figure 1 shows the parts that are typically used to build an IP Telephony scenario. It normally compromises - independent from the used protocol (H.323, SIP or others) - a signaling plane, a media transport plane and various telephony components.

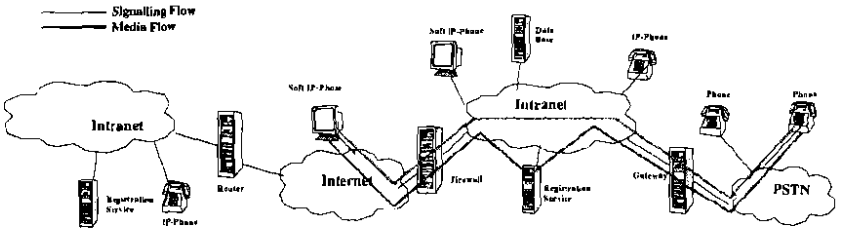

Figure 1 Generic IP Telephony Scenario

The signaling plane is used for transporting the necessary signaling information between the components. After a call setup, the media transport plane is used to carry the voice data between the components, e.g. terminals or gateways. Normally the components have to be operated remotely, so there is also a need to transport management data. This could be seen as a third plane, but this function is often considered as an addition to the signaling plane.

For a security assessment, a number of (related) facts have to be considered. First, both planes that are used, depend on the same infrastructure, the IP network. Compared to the conventional telephony in the Public Switched Telephone Network (with SS#7), where there is a certain level of isolation, this increases the risk of system misuse. In our scenario there is no physical separation between the planes.

Second, the network infrastructure is not maintained or controlled by a single authority or just a small (trusty-worth) set of providers. Signaling and media plane might be based on untrusted network parts, components and operators.

Finally the IP network, which is used by the signaling and media plane, is also used by other services and both end system and infrastructure components are often full featured computers able to fulfill many other tasks.

Based on these facts we can conclude that not only telephony related security problems (e.g. possible missing privacy of the spoken word) may occur. IP telephony systems are based on normal network and computer systems and interfere with them. The resulting security problem domain is considerably larger compared to a standard PSTN based telephony system. We will furtheron concentrate on IP Telephony specific

problems though, and will e.g. not mention the fact, that routers or other general infrastructure components are vulnerable as well.

2.2. VULNERABILITY TARGETS IN H.323

Figure 2 describes a scenario in which H.323 based components are used. It is considered to be representative for common operational areas and may slightly be adapted to individual other configurations.

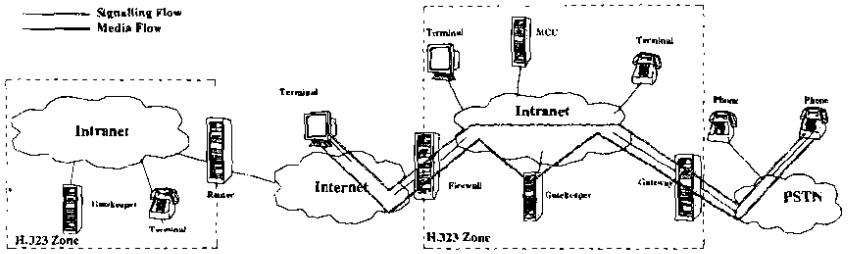

Figure 2 H.323 IP Telephony Scenario

We identify the following potential risks and derived points of attack:

- Both the signaling or media transport plane can be target of an attack. This involves integrity, confidentiality, authentication or non-repudiation of the transported data.

- Both the audio payload data but especially the signaling information exchanged between the components is sensitive to eavesdropping, jamming and even active modification. The challenges become even more evident if we consider an open environment where finding, choosing and using services and transfer points from and towards the PSTN (we can compare this to conventional "Call Routing") are subject to economic competition between various service providers.

- Compromising the identity of an end system or infra structure component leads to additional risks even when using standard and non-compromised signaling mechanisms. If a malicious user can register with a H.323 Gatekeeper (or SIP server/registrar), he can potentially gain the personality of the user whom he attacks. That involves a potential invasion of privacy (since at least incoming calls are routed to the attacker and may give him the knowledge who calls) as well as the chance of miss-using services that are charged for.

- The specific functions of the IP telephony infrastructure components might be target of an attack. For example we consider the registration service as provided by a gatekeeper.

- The components environment, hosting a specific IP telephony function can be target of an attack. This includes the management interfaces, used to configure the IP telephony function, which are also hosted by the operating system.

- Even systems and functions that are not directly involved can be attacked. For example a IP telephony enabled firewall might be weakened due to the fact that it supports IP telephony communication (and temporarily opens certain communication paths that might be used for attacks instead of regular voice conversation).

The next section gives a selection of the examined vulnerability examples which can be arranged according to our classification.

3. CASE STUDIES

In the following we present selected vulnerabilities of a H.323 based IP telephony scenario (Figure 3) that incorporates gatekeepers and gateways that form the point of (cost-rising) interaction with the PSTN world.

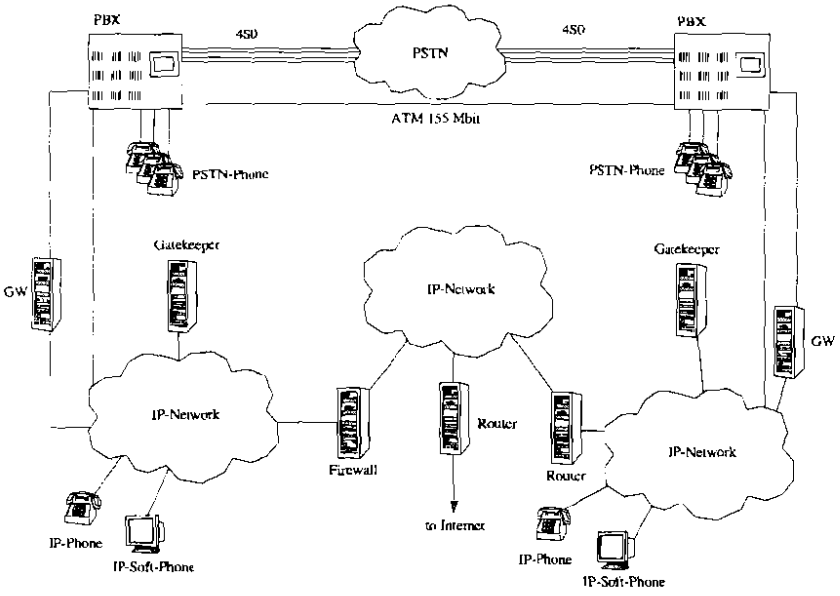

Figure 3 Evaluated Test Scenario

The conventional PBX components and their administrative IP access points (that form further potential points of attack as well) are just shown for completeness.

3.1. ATTACKING END SYSTEMS

Getting control of an end system.

IP telephony end systems will often be placed in publically accessible places (e.g. offices or even on public floors). Once an attacker gets physical access to the examined IP telephone in our scenario, he is able to reset it to its factory configuration. (In the later we show typical characteristics of the vulnerabilities or code fragments in a framed example box.)

Instructions taken from the IP telephone manual Restoring the factory settings Enter the 6-digit password: 124816 Access to the Administration menu In the as-supplied condition, the Administrators password is 123456.
Getting physical access to the telephones management

The example of providing backdoors or weak initial passwords is not a unique flaw but has been examined for multiple components from different vendors. The remote management interface (via HTTP) that the IP telephone uses is vulnerable to attacks as well. The administrator password is sent in plaintext which makes the communication vulnerable to sniffing. Additionally (due to its limited length and restricted alphabet, because it has normally to be typed in via the telephones keypad) the administration password can also be attacked with a series of automated brute-force trials.

Once initial access to the device is gained, its administrative password for both local (manual) as well as remote WWW access can be set to a value known and becomes usable for further malicious operations. The device configuration is visible to an attacker and can be used for gaining additional information about the attacked network, user identities and E.164 numbers as well as for restoring values after an attack. In our example details such as the IP phones IP address, its E.164 number and the IP address of the H.323 gatekeeper(s) that it tries to register with, can be obtained and changed. Doing so even allows an attacker to change a phones capabilities in a way, that it registers with a different gatekeeper which is under the attackers control. This gives this attacker reading and even changing access to the IP telephony signaling and may be used for getting information about communication relations (who calls whom),

enables calculated degradation or even denial of communication services (the user is unable to receive calls from or originate calls to specific other phones) or access to voice content for outgoing calls to PSTN participants if those are routed via a H.323 to PSTN gateway of the attackers choice.

Obtaining administrative access to the device can even be used for completely changing its firmware, that can be loaded from outside via the network. Though this (still, as long as no development APIs for telephone firmware are available - which might change with upcoming configurable "Java-Phones") means a very high effort for the attacker, consequences are rather severe, because a new firmware placed on the device could offer all the functionality that the original device had, while providing permanent backdoors for later attacks.

DoS-Attack using IP telephony signaling.

The end systems we evaluated (both a commercial "hard" phone and the Open Source ohphone) were unable to withstand an attack that sends unexpected or incorrect H.323 signaling PDUs. Those resulted in either a temporary unavailability or even a total system failure with the device locked up, crashing or rebooting.

In the case of a "registration attack" - that we will describe later - a malicious attacker can use a Denial of Service first, to (maybe even just temporarily) suppress the packets from the original system in order to start the de-registration / registration of another malicious end system then.

Denial-of-Service Attack using general means.

The examined IP phone uses an integrated WWW server that allows to manage the device and to query some of its settings. This WWW server and its implementation faults (though not a basic part responsible for IP telephony functions of the device) makes it vulnerable for malicious attacks. Using a URL with a sufficiently long length, the device can (depending on the length of the URL string) either be made inoperable which results in its total failure or rebooted.

```
/* uses standard TCP socket communication on port 80 (HTTP) */
...
memset(query_string, 0x1, 256);
query_string[256] =0x0;
write(sock, query_string, sizeof(query_string));
...
```

Denial of Service using the phones HTTP server

For the attack just minimal skills of the attacker, simple tools (we have performed the attack using either a standard browser, a telnet tool or a tiny test program) and low effort are required, but they result in a total loss of systems functionality and can be performed at all end systems of an installation from a remote place at the same time.

3.2. ATTACKING THE USERS PRIVACY

IP telephony applications use RTP [7] packets transmitted via the UDP protocol for carrying audio data streams. Though basic mechanisms for using symmetrically encrypted [1] audio payloads in RTP packets are described in an appropriate RTP profile [6], those are not widely used yet, due to the lack of deployed key exchange or negotiation features within the IP telephony signaling protocols. For a potential eavesdropper it is necessary to identify the data streams that form the audio connection(s). Since the ports used for that, are typically negotiated in a dynamic manner this is not a totally straight-forward task. With the public availability of IP telephony protocol stacks and an in-detail description of protocol mechanisms it becomes more easy even for non-expert attackers though. For investigation we developed and tested a tool that - after specifying the characteristics of the users we observe (depending on the kind of signaling and scenario e.g. H.323 with or without registration of symbolic names at a Gatekeeper we can e.g. specify an E.164 number we want to observe) - allows to monitor and / or record calls on the fly.

```
/* uses libpcap for packet capturing */
...
#define RTP_PAYLOAD_OFFSET 0 + 14 + 20 + 8 + 12
...
while (!finished) {
packet=(u_char *) pcap_next(pcap, &pkthdr);
...
write(audio_fd, (unsigned char *)packet+RTP_PAYLOAD_OFFSET,
rtp_payload_size);
...
}
```

Playing audio data by sniffing the (unprotected) RTP payload

Since a structured cabling with dedicated lines towards each participant instead of a shared ethernet is usually considered a basic precondition for a sufficient data throughput, low audio packet delay and loss bounds, people often argument, that the use of switches instead of hubs limits the problem of unauthorized access to the data connections. Recent

publications have shown though, how vulnerable also such configurations are to attacks. After sending faked ARP replies to a switch it starts sending data not only to the dedicated user link but also to the one of the attacker.

3.3. ATTACKING INFRASTRUCTURE COMPONENTS

Gatekeeper registration attack.

When registering an H.323 device, it establishes a mapping compromising its E.164 number and a voluntary number of additional symbolic names (so called aliases) with its IP address at the gatekeeper. This mechanism is part of the H.225 RAS (Registration, Admission and Status) signaling and allows for a comparable easy auto-configuration and portability of devices within a given local environment as well as a certain mobility.

The gatekeeper typically implements a certain policy which describes, whether just pre-configured sets of E.164 numbers/symbolic names and IP addresses are allowed to register or every potential end-system can. This is a purely administrative decision and out of the scope of the H.323 standard specification itself. In the best case, gatekeepers allow to choose which policy to use in a granular way and are pre-configured with a rather strict policy that forbids arbitrary access. For the systems we evaluated that is not the case though.

In traditional PBX systems, rights (as for instance whether a certain person is allowed to originate long distance or international calls) are usually bound to user identities. This mechanism without additional (e.g. cryptographic) protective means can be exploited by "stealing" or faking user identities. If the registration is not restricted by any means the registration mechanism can be exploited for either (miss-)using the communication services which often includes calling to external parties via IP telephony to PSTN gateways without paying for that service, for just causing costs by calling expensive external service numbers or even calling dedicated numbers that their operator has a benefit from.

```
/* uses OpenH323 for PDU generation */
/* we show the unregistration part */
/* an attacker can register then */
...
UnRegReq.m_callSignalAddress.SetSize(1);
(UnRegReq.m_callSignalAddress[0]).SetTag(
H225_TransportAddress::e_ipAddress);
H225_TransportAddress_ipAddress                    &
h225_transportaddress_ipaddress=
(UnRegReq.m_callSignalAddress[0]);
h225_transportaddress_ipaddress.m_ip[0]=ip[0];
h225_transportaddress_ipaddress.m_ip[1]=ip[1];
h225_transportaddress_ipaddress.m_ip[2]=ip[2];
h225_transportaddress_ipaddress.m_ip[3]=ip[3];
h225_transportaddress_ipaddress.m_port.SetValue(port);
...
sendto(sock, data_d, data_s, 0, (struct sockaddr*)&name, size-
of(name));
...
```

Attacking Gatekeeper Registrations

As a minimal means of protection only de-registration requests carrying the IP address of the previously registered participant could be observed while others should be disregarded or may even trigger warnings or alarms for the systems administrator. Since the (de)registration IP address is carried in the (usually unprotected) payload of an H.323 PDU, they can easily be faked. Additional checks (e.g. the test whether the PDUs source IP address corresponds to the correct entity) have either to be evaluated for their general applicability (e.g. in the case of proxying instances or additional gateway originating messages) or can be broken by using spoofing at the IP layer. (This poses some more burden at an attacker, but can and has been done.)

Only cryptographic methods such as the H.323 protocol extensions described in H.235 [2] and Annex F form a better basis for protective mechanisms. They are not implemented in the devices we evaluated though.

Denial of Service targeting the Gatekeeper.

We were able to prevent all (both commercial and Open Source) observed gatekeepers from fulfilling their regular tasks by sending them a large number of either regular (cyclic registration and de-registration of terminals) or irregular H.323 PDUs. This makes the IP Telephony service

unavailable either for a certain period or in general (if the gatekeeper is forced to crash).

It must be mentioned that for those DoS-attacks only a comparable small bandwidth is necessary (since we are attacking the signaling) and it is difficult to protect a gatekeeper (e.g. by means of a firewall) if it needs regular communication relationships with "outside" parties for its regular tasks (e.g. if outside clients are allowed to regularly call).

4. CONCLUSIONS

4.1. ASSESSMENT RESULTS

The scenarios that we described have been evaluated within our university environment and we believe them to be rather realistic, once IP phones (at the current security level) would be deployed regularly within publically accessible network segments of our campus. This deployment within just one single network (then used for both data as well as voice traffic) has been determined as on of the potential reasons for starting to use IP telephony - so scenarios planning to use two separate (then both IP networks) are considered to be not realistic.

Even if a certain level of "isolation" could potentially be obtained by using VLAN techniques this would also limit the promising chances for close computer and telephony interaction which forms the basis for new innovative services.

It should be mentioned that - differing from the situation with a conventional PBX, which compromised highly specialized equipment and is usually not available for attackers with an "average background" - IP infrastructure components such as H.323 gatekeepers or H.323 to PSTN gateways are available even as Open Source [3][4] implementations and can easily be obtained, adapted and deployed.

4.2. POTENTIAL COUNTERMEASURES

The paper intentionally concentrates on the search (based on theoretical analysis of the protocols and scenarios), description and practical exploit of vulnerabilities. We just give a short reference to potential countermeasures which can be be classified as either

- short-term and more or less just "bug-fixing" (which is definitely necessary but will not change the problem situation in general) or

- longer-term and comprehensive (which we see as a general must for the practical feasibility and success of IP Telephony solutions).

IP Telephony Specific Approach.

Both the IETF and ITU recently show more efforts to provide standards, that also cover the security aspect. For example the ITU provides some extensions to the H.323 framework, which specify how security can be added [2]. For SIP, cryptographic authentication and privacy features are defined within the base RFC already. An overview about these security related extensions to the IP telephony standards is given in [5]. As shown in this contribution, these protocol extensions are necessary to be able to solve some security problems, but do not provide a general and automatic security solution to broken system designs.

Establishing a Security Improvement Feedback-Loop.

In [8] we introduced the concept of a *Security Improvement Feedback-Loop* (SIF) which is a systematic way of understanding security weaknesses and elaborating efficient solutions. The SIF concept consists of four stages:

- Observation: security weaknesses of existing systems are observed and reflected in various forms such as mailing-lists, newsgroups, and articles.
- Information Retrieval: information is gathered from different sources. In case of electronic documents this can be done automatically. Form-based interfaces can be used to guide human users by entering information that comes from non-digital sources.
- Screening: the data is transformed according to a uniform, highly structured data scheme, as this is more suitable for further machine-based processing. It is possible to apply screening filters in order to determine the relevance of information that will be stored in vulnerability databases.
- Analysis and Utilization: as we have described in [9], appropriate data mining procedures help to identify and improve patterns that are in turn used to engineer new or to improve existing systems. For example this knowledge can be used for the elaboration of security design patterns, security guidelines or as input for security tools. Thus the security of new and existing systems will be improved as known errors should not occur again. Now the feedback-loop is closed.

The data-mining approach reveals valuable insights for security improvement. Our long term goal is to identify a set of comprehensive

security patterns for secure distributed application domains, with IP telephony just one of those.

4.3. FINAL REMARKS

The observed design flaws and potential misbehavior of IP telephony solutions are in their majority not due to limitations or shortcomings within the technology or its architectures and signaling protocols itself, but result from severe design, implementation and policy faults.

With just "basic attacking components" and without special preconditions (most attacks were performed from user space and without even physical access to the attacked network) we could show vulnerabilities that reach from the invasion of the users privacy over service misuse and fraud to the total degradation of services. Both commercial equipment as well as popular Open Source implementations (such as the OpenH323 stack, that a lot of people now start basing their future solutions on) have been shown to be vulnerable in the same way. Basically all the attacks that we theoretically planned in the first evaluation step succeeded.

The shown problems can and must be fixed by the manufacturers of the equipment and should definitely be avoided in future designs. We strongly believe that a critical view on the current situation is helpful in order to avoid potential threats to user as well as operator and vendor interests once the equipment is deployed in larger quantities.

The authors are working on improving the situation in close contact and cooperation with the component manufacturers and system integrators. Interested parties are explicitly encouraged to contact the authors for the source code and (Linux) executables for all the described checks and attacks. A number of details on the potential exploits are - due to their sensitivity - available on request only and will be publically available just after they have been fixed.

References

[1] D. Balenson. Privacy enhancement for Internet electronic mail: Part III: Algorithms, modes and identifiers. *RFC 1423*, January 1993.

[2] ITU-T. Security and Encryption for H. Series (H.323 and other H.245 based) Multimedia Terminals. ITU-T Recommendation H.235, February 1998.

[3] OpenH323 Project. OpenH323. http://www.openh323.org/.

[4] OpenH323 Project. OpenH323 Gatekeeper. http://www.opengatekeeper.org.

[5] Christoph Rensing, Utz Roedig, Ralf Ackermann, and Ralf Steinmetz. A Survey of Requirements and Standardization Efforts for IP-Telephony-Security. In M. Schumacher and R. Steinmetz, editors, *Sicherheit in Netzen und Medienströmen*, Informatik aktuell, pages 50–60. Springer Verlag, September 2000.

[6] H. Schulzrinne. RTP profile for audio and video conferences with minimal control. *RFC 1890*, January 1996.

[7] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP: A Transport Protocol for Real-Time Applications. *RFC 1889*, January 1996.

[8] Markus Schumacher, Ralf Ackermann, and Ralf Steinmetz. Towards Security at all Stages of a System's Life Cycle. In *2000 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 2000.

[9] Markus Schumacher, Christian Haul, Michael Hurler, and Alejandro Buchmann. Data-Mining in Vulnerability Databases. (90), 2000.