

Two attacks against VoIP

Peter Thermos 2006-04-04

"We are more secure than a regular phone line."

VoIP is here to stay. In fact many incumbent telecommunication carriers have started offering VoIP service for sometime and several new VoIP service providers have emerged. Aside from issues such as quality of service, the aspect of security, or lack thereof, is misunderstood by some of the VoIP service providers.

This purpose of this article is to discuss two of the most well known attacks that can be carried out in current VoIP deployments. The first attack demonstrates the ability to hijack a user's VoIP Subscription and subsequent communications. The second attack looks at the ability to eavesdrop in to VoIP communications. Although VoIP is implemented using various signaling protocols, this article focuses on attacks associated with the SIP (Session Initiation Protocol), an IETF standard (RFC 3261). The two attacks, among others such as DoS, have been discussed in various research papers but they haven't been acknowledged publicly as active attacks.

Industry experts believe that these attacks will become more apparent with the wider adoption and understanding of VoIP. The next section provides a brief introduction to the SIP protocol which is used to set up and tear down Internet multimedia sessions (including VoIP). The later sections of this article focus on user registration or session hijacking.

Quick introduction to SIP

The Session Initiation Protocol (IETF RFC 3261) is a widely implemented standard used in VoIP communications to setup and tear down phone calls. Figure 1 depicts (at a high level) the SIP messages that are exchanged during a phone conversation. A brief explanation will follow.

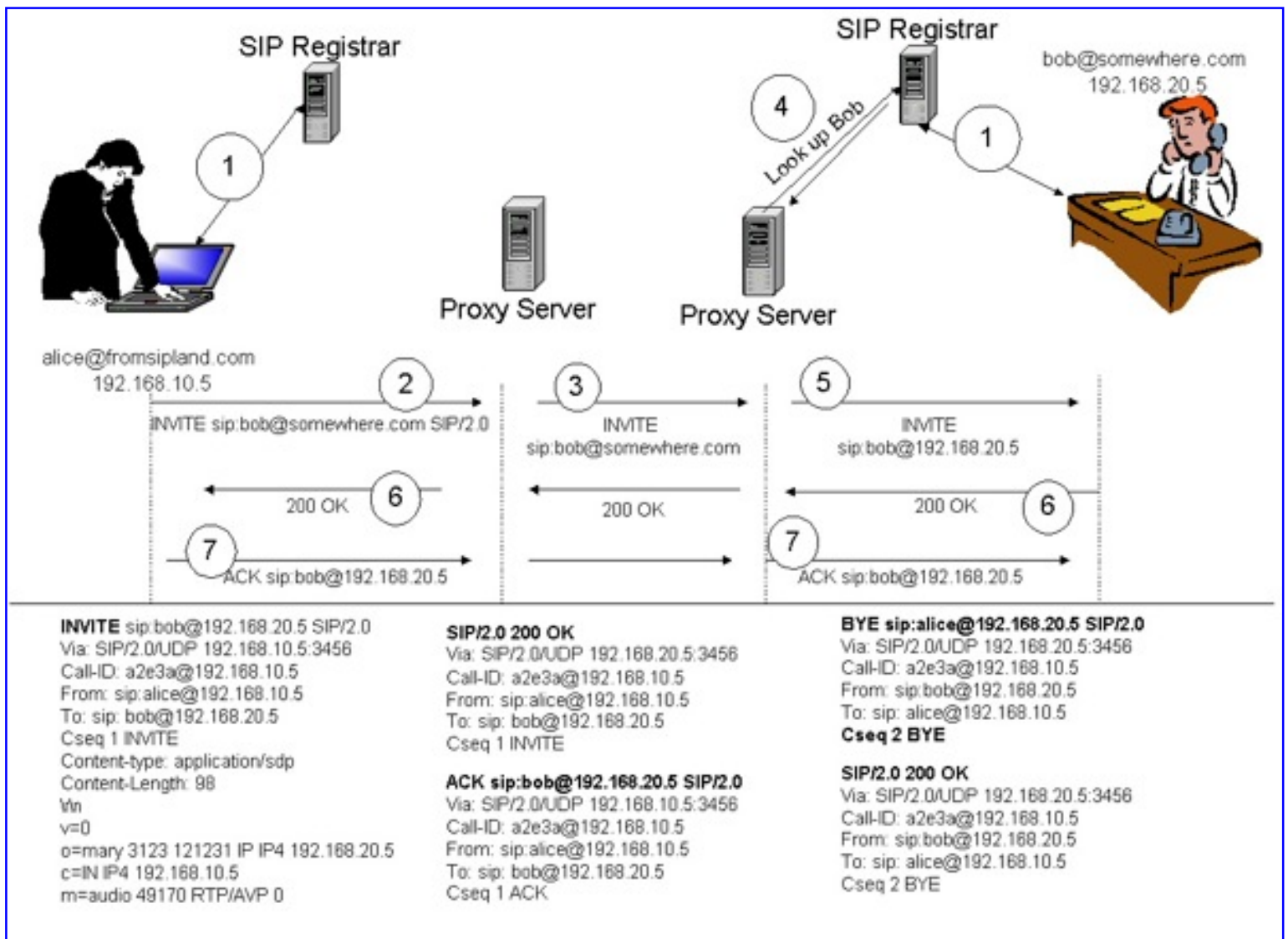


Figure 1. SIP Call Setup and tear down.

In step 1, the user's device (called a User Agent in SIP terminology) registers with the domain registrar who is responsible for maintaining a database of records of all subscribers for the respective domain. User registration in VoIP is necessary because it provides the means to locate and contact a remote party. When *Bob* wants to contact *Alice*, he will send an INVITE request to a proxy server. Proxy servers are responsible for routing SIP messages and locating subscribers. When the proxy server receives an INVITE request, it attempts to locate the called party and relay progress to the caller by performing a number of steps, such as DNS lookups and the routing of various SIP messages (provisional and informational). The step that is impacted by registration hijacking, as we will see shortly, is during the device registration in step 1 of this figure.

Registration Hijacking

Figure 2 depicts a valid registration message and response from the SIP registrar, which is used to announce a user's point of contact. This indicates that the user's device accepts calls.

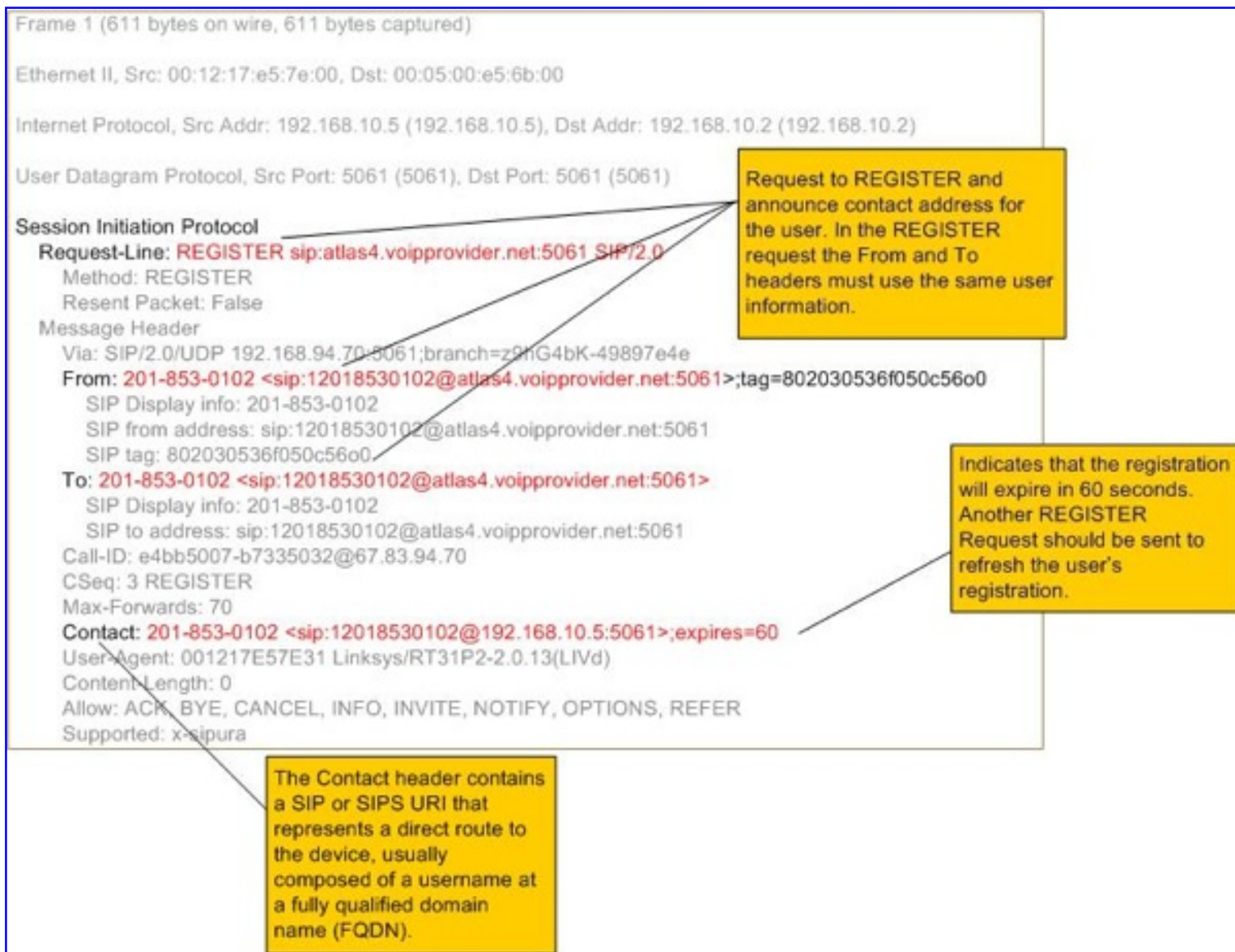


Figure 2. REGISTER Request.

The REGISTER request contains the *Contact*: header which indicates the IP address of the user's device (for either a VoIP soft or hard phone). When a proxy receives a request to process an incoming call (an INVITE), it will perform a lookup to identify where the respective user can be contacted. In this case, the user with the phone number 201-853-0102 can be reached at IP address 192.168.94.70. The proxy will forward the INVITE request to that IP address. The reader may notice that the advertised port is 5061. This port is reserved for SIPS and in this popular implementation it is actually in violation [ref 1] of RFC 3261.

The following Figure 3 displays a modified version of the REGISTER request that is sent by the attacker.

```

Frame 1 (611 bytes on wire, 611 bytes captured)

Ethernet II, Src: 00:12:17:e5:7e:00, Dst: 00:05:00:e5:6b:00

Internet Protocol, Src Addr: 192.168.1.3 (192.168.1.3), Dst Addr: 192.168.1.2 (192.168.1.2)

User Datagram Protocol, Src Port: 5061 (5061), Dst Port: 5061 (5061)

Session Initiation Protocol
Request-Line: REGISTER sip:atlas4.voipprovider.net:5061 SIP/2.0
  Method: REGISTER
  Resent Packet: False
Message Header
  Via: SIP/2.0/UDP 192.168.1.5:5061;branch=z9hG4bK-49897e4e
  From: 201-853-0102 <sip:12018530102@atlas4.voipprovider.net:5061>;tag=802030536f050c56o0
    SIP Display info: 201-853-0102
    SIP from address: sip:12018530102@atlas4.voipprovider.net:5061
    SIP tag: 802030536f050c56o0
  To: 201-853-0102 <sip:12018530102@atlas4.voipprovider.net:5061>
    SIP Display info: 201-853-0102
    SIP to address: sip:12018530102@atlas4.voipprovider.net:5061
  Call-ID: e4bb5007-b7335032@192.168.1.5
  CSeq: 3 REGISTER
  Max-Forwards: 70
  Contact: 201-853-0102 <sip:12018530102@192.168.1.3:5061>;expires=60
  User-Agent: 001217E57E31 Linksys/RT31P2-2.0.13(LIVd)
  Content-Length: 0
  Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER
  Supported: x-sipura

```



Figure 3. A modified version of the REGISTER request.

In this request, all the message headers and parameters remain the same except for the parameters in the *Contact* header. The information that has been changed in the *Contact* header is the IP address (192.168.1.3) which points to the attacker's device. The REGISTER request is sent to the SIP Registrar at 192.168.1.2. The tool that was used to generate this request is SiVuS [ref 2] which is demonstrated below in Figure 4.

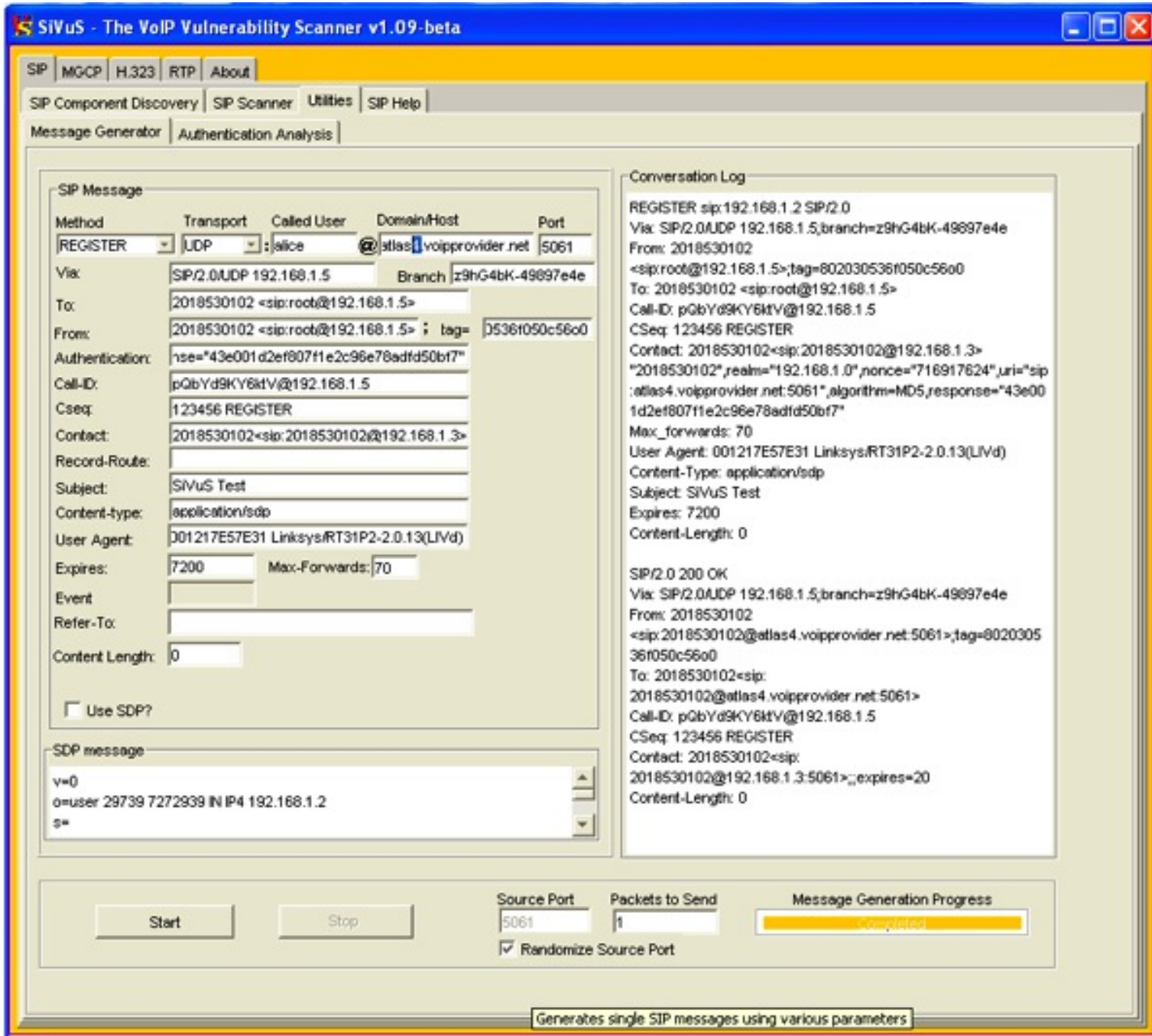


Figure 4. SIP Registration Spoofing Using SiVuS Message generator.

The hijacking attack works as follows:

1. 1. Disable the legitimate user's registration. This can be done by:
 - o performing a DoS attack against the user's device
 - o deregistering the user (another attack which is not covered here)
 - o Generating a registration race-condition in which the attacker sends repeatedly REGISTER requests in a shorter timeframe (such as every 15 seconds) in order to override the legitimate user's registration request.
2. 2. Send a REGISTER request with the attacker's IP address instead of the legitimate user's

The following Figure 5 demonstrates the attack approach.

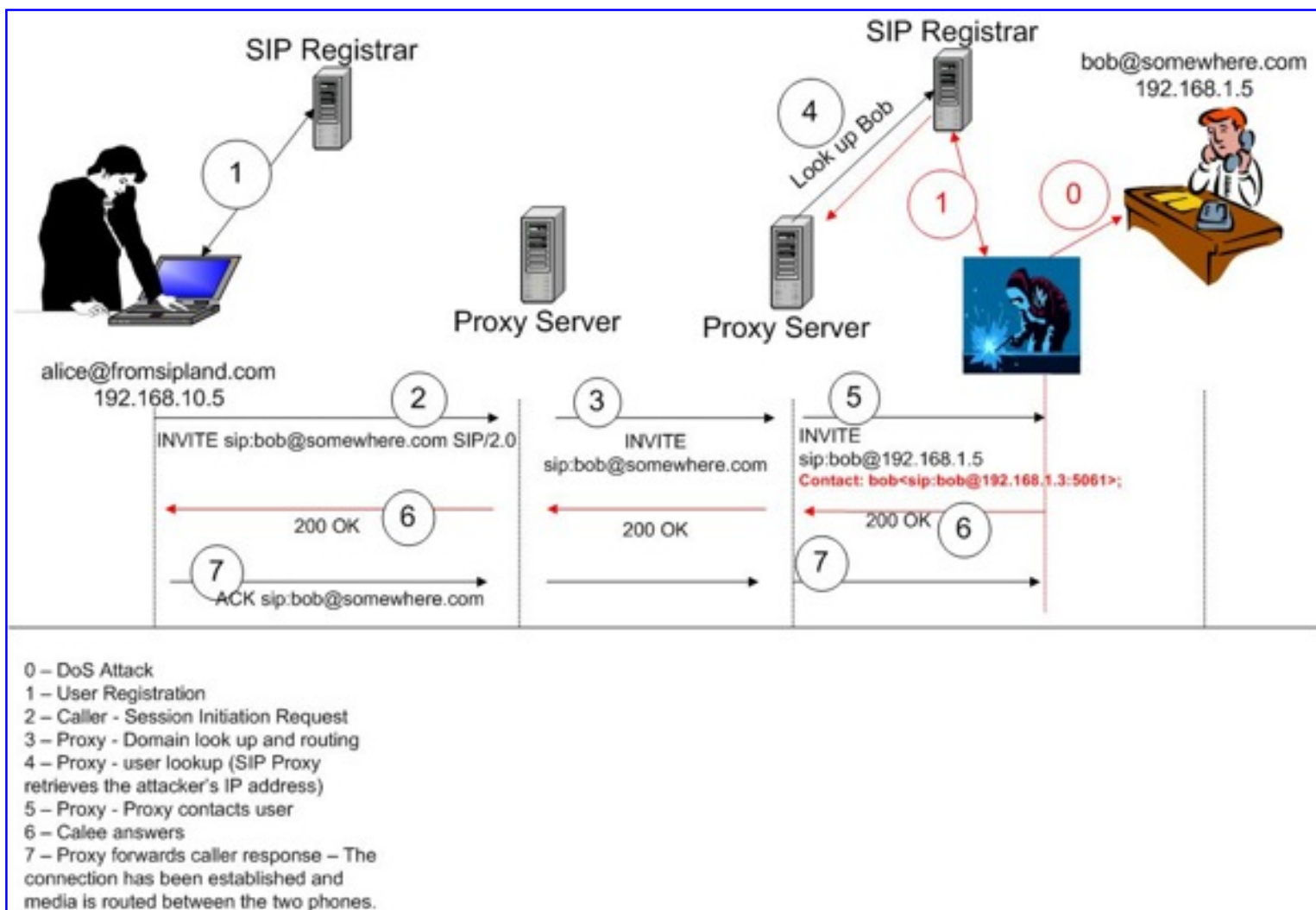


Figure 5. Overview of a registration hijack.

This attack is possible for the following reasons:

1. The signaling messages are sent in the clear, which allows an attacker to collect, modify and replay them as they wish.
2. The current implementation of the SIP Signaling messages do not support integrity of the message contents, and thus modification and replay attacks are not detected.

This attack can be successful even if the remote SIP proxy server requires authentication of user registration, because the SIP messages are transmitted in the clear and can be captured, modified and replayed. This attack can be launched against both enterprise or residential users. For example, a home network that uses a poorly configured wireless access point can be compromised by an attacker who can intercept and replay registration requests. This also includes configurations where WEP (Wired Equivalent Privacy) or WPA (Wi-Fi protected access) is used, since there are known vulnerabilities that allows an attacker to gain unauthorized access. [ref 3] As such, the attacker can perform various attacks including making fraudulent calls or redirecting communications. In an enterprise environment an attacker can divert calls to unauthorized parties. For example, calls from stockholders can be diverted to an agent that is not authorized to handle certain trade transactions for customers. In some cases this attack can also be viewed as a "feature" for employees who prefer not to be disturbed.

This attack can be suppressed by implementing SIPS (SIP over TLS) and authenticating SIP requests and responses (which can include integrity protection). In fact, the use of SIPS and the authentication of responses can suppress many associated attacks including eavesdropping and message or user impersonation.

Eavesdropping

Eavesdropping in VoIP is somewhat different from the traditional eavesdropping in data networks, but the general concept remains the same. Eavesdropping in VoIP requires intercepting the signaling and associated media streams of a conversation. The signaling messages use separate network protocols (i.e., UDP or TCP) and ports from the media itself. Media streams typically are carried over UDP using the RTP (Real Time Protocol) protocol.

Figure 6 demonstrates the steps require for a media capture using Ethereal. [ref 4]

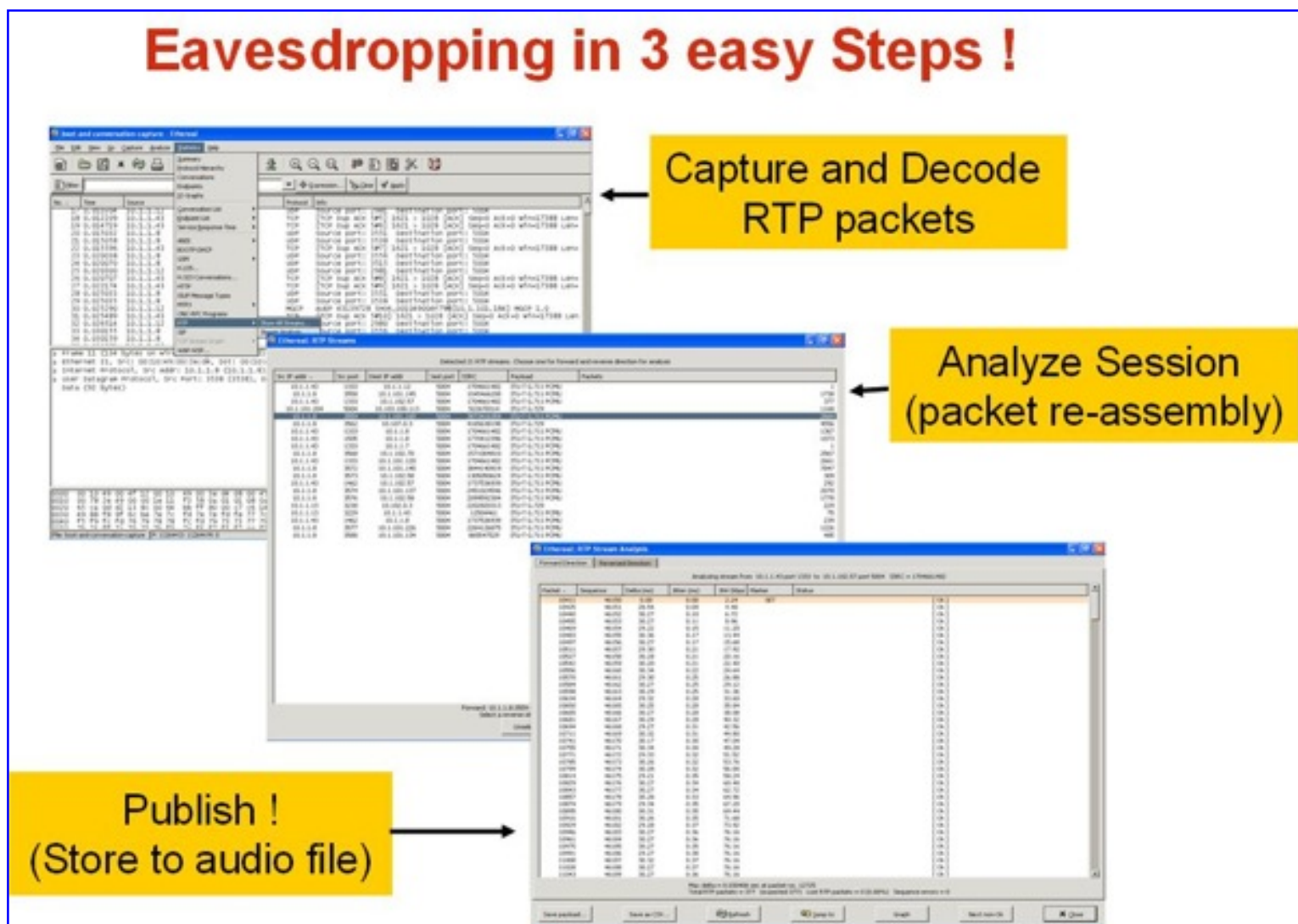


Figure 6. Steps to capture VoIP media streams using Ethereal.

The steps to capture and decode voice packets include:

- *Capture and Decode RTP packets.* Capture packets and select **Analyze -> RTP-> Show all streams** options from the ethereal interface.
- *Analyze Session.* Select a stream to analyze and reassemble.
- *Publish.* Open a file to save the audio (.au) steam that contains the captured voice.

Some may argue that the eavesdropping attack can be suppressed in IP based networks with the use of Ethernet switches which restrict broadcasting traffic to the entire network, and thus limits who can access the traffic.

This argument can be discarded when ARP spoofing is introduced as a mechanism to launch a man-in-the-middle attack. We will not cover ARP spoofing in this article since it is documented in several publications. The basic concept, however, is that an attacker broadcasts spoofed advertisements of the MAC address and thus forces subsequent IP packets to flow through the attacker's host . This thereby allows the eavesdropping of communications between two users. The following Figure 7 summarizes the ARP spoofing attack.

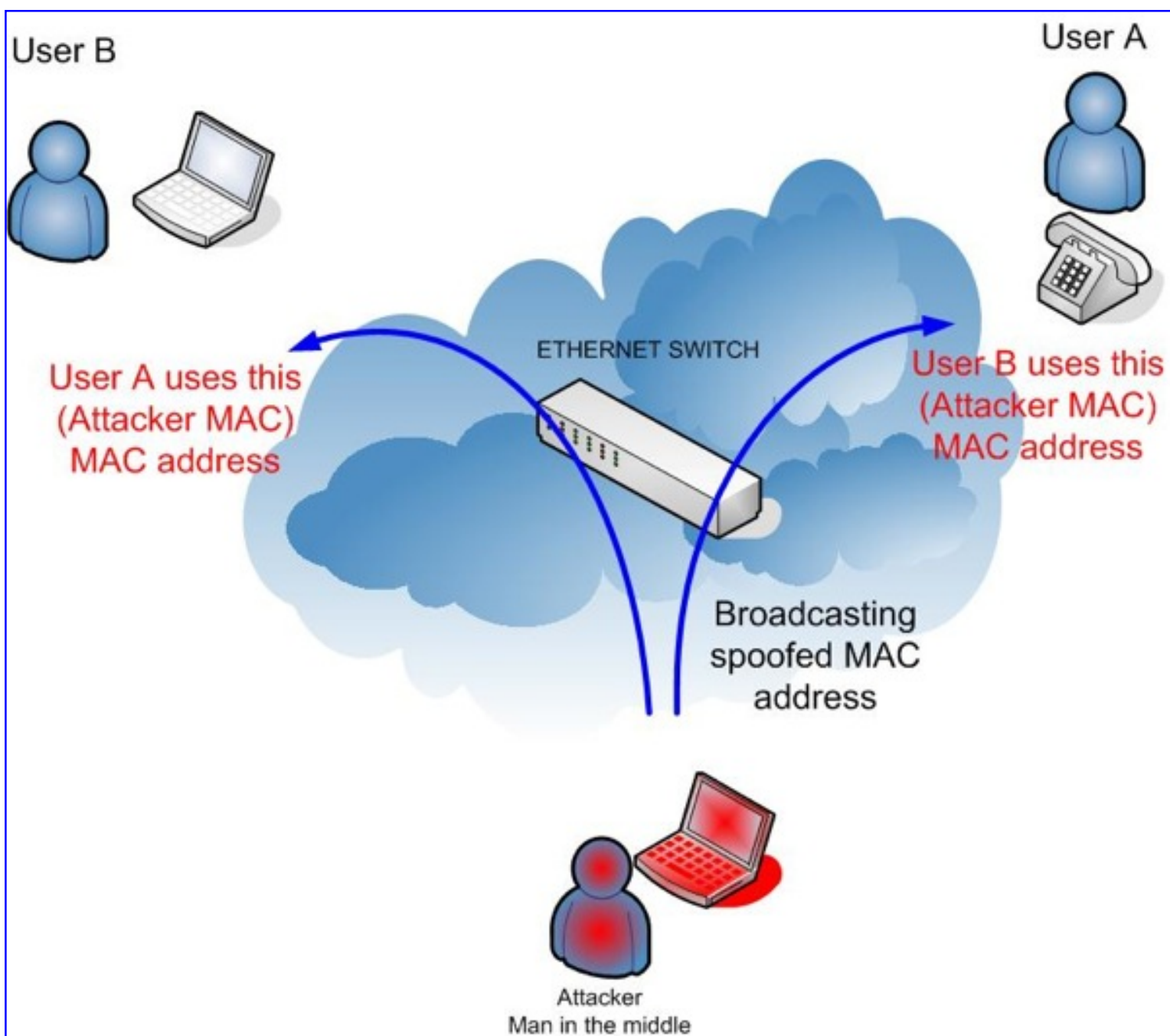


Figure 7. ARP Spoofing attack.

Using ARP spoofing, an attacker can capture, analyze and eavesdrop into VoIP communications.

The following Figure 8 demonstrates the use of the Cain tool [ref 5] which provides the ability to perform the man-in-the-middle attack and capture VoIP traffic.

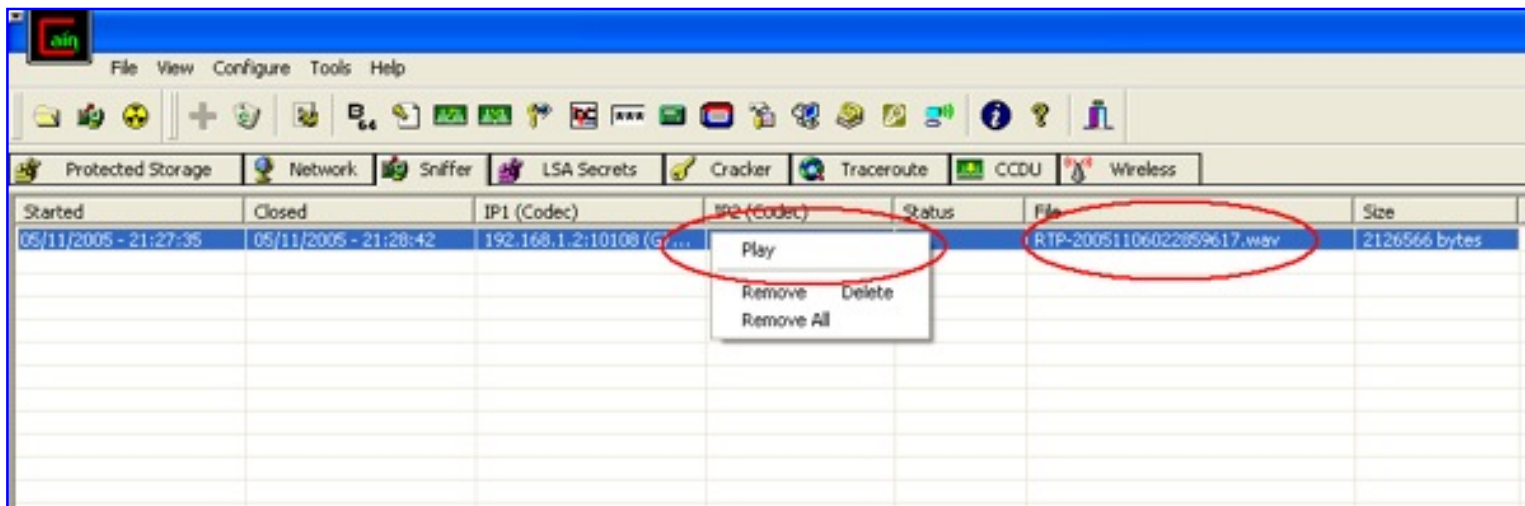


Figure 8. Using Cain to perform a man-in-the-middle attack.

Conclusion

This article outlined two of the many attacks that are currently applicable to VoIP networks. Traditionally, the average citizen maintains a level of trust with the current PSTN (Public Switch Telephone Network) or cellular networks when it comes to assumed confidentiality in phone conversations. While we know that the PSTN does not provide any encryption to protect phone conversations, we tend to feel that it is adequate. It's good enough.

But now since new access to the communications medium, such as IP based networks, is not controlled (whereas access to the PSTN is limited) and the vulnerabilities can be exploited by a larger number of attackers, the risk for realizing an attack increases dramatically. This also minimizes the level of trust. The difference is the **access** method to the network.

Of course no one argues that an attacker can not access and install a tap on a telephone pair outside your house. But that requires more visibility and there are explicit laws that prohibit eavesdropping. On the other hand, IP eavesdropping can be done from the comfort of your laptop as long as you possess the tools and expertise to carry out the attack successfully.

It is expected that the described attacks will gain popularity in the near future for personal or financial gain (such as fraud).

The investment in products and research by companies, and the proliferation of VoIP services the past three years, demonstrates that VoIP is here to stay. At the same time, it seems that security issues will become more apparent as the subscriber population increases. The IETF

has made several improvements that provide protection for the VoIP signaling and media streams. The most apparent recommendations are the use of TLS to protect SIP signaling and the SRTP (Secure Real Time Protocol) to protect the media stream. One of the problems is that vendors maintain a slow adoption and implementation rate of these protocols. Furthermore, some VoIP service providers confuse what security means in packet based communications. An example of this is found at a prominent VoIP service provider in North America who claims that, *"We are more secure than a regular phone line."* That was a response from a recent interaction between one of their millionth VoIP subscribers and the company's tier-2 tech support after providing a detail description of these issues.

References

[ref 1] See http://www.vopsecurity.org/Security_Issues_with_SOHO_VoIP_Gateways-052005.pdf for additional information.

[ref 2] SiVuS, the VoIP Vulnerability Scanner, <http://www.vopsecurity.org/html/tools.html>.

[ref 3] See "WEP: Dead Again, Part 1" <http://www.securityfocus.com/infocus/1814> and "WEP: Dead Again, Part 2" <http://www.securityfocus.com/infocus/1824>. [ref 4] Etherreal, <http://www.ethereal.com>.

[ref 5] Cain & Abel, <http://www.oxid.it/cain.html>.

[Privacy Statement](#)

Copyright 2006, SecurityFocus