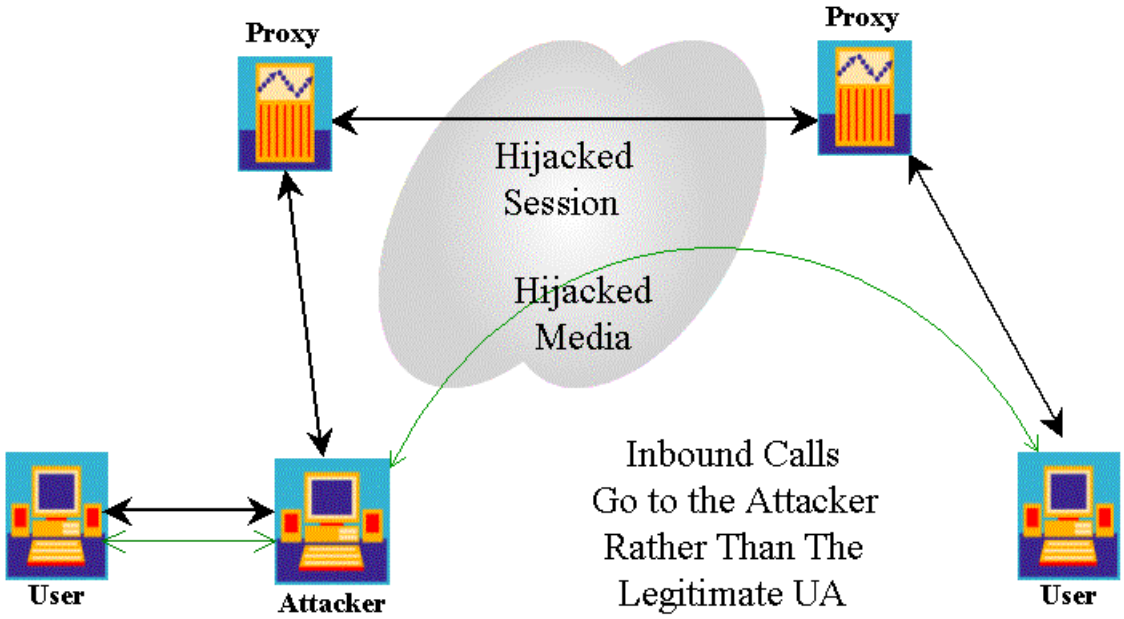
VoIP Vulnerabilities – Registration Hijacking

By Mark Collier
Chief Technology Officer
SecureLogix Corporation
mark.collier@securelogix.com

Introduction

With the deployment of Voice Over IP (VoIP)—and especially the Session Initiation Protocol (SIP)—there are a number of vulnerabilities you need to address. One such vulnerability is registration hijacking. In SIP (and other VoIP protocols), a User Agent (UA)/IP phone must register itself with a SIP proxy/registrar (or IP PBX), which allows the proxy to direct inbound calls to the UA. Registration hijacking occurs when an attacker impersonates a valid UA to a registrar and replaces the legitimate registration with its own address. This attack causes inbound calls intended for the UA to be sent to the rogue UA. The following figure illustrates registration hijacking:



Registration hijacking allows inbound calls to be hijacked and answered by an attacker, which for example, could play a spoofed voice mail prompt. Registration hijacking also allows an attacker to "get in the middle" and record signaling and audio.

Causes of Registration Hijacking

With SIP, registration is normally performed using the connection-less Universal Datagram Protocol (UDP), as opposed to the connection-oriented Transmission Control Protocol (TCP). UDP simplifies generation of spoofed packets, making attacks like registration hijacking easier.

SIP registrars are not required to authenticate the UA requesting a registration. When authentication is used, it is not strong, only involving use of a MD5 digest of the username, password, and timestamp-based nonce sent in the authentication challenge. Furthermore, passwords are often weak or "mechanically" generated, meaning that passwords are generated automatically and follow a predictable pattern. Even strong passwords can be defeated with dictionary-style attacks. Dictionary attacks are those where a list of potential passwords are used to "guess" a password needed for registration. A dictionary built with knowledge of an organization can be very effective. Quite often, knowing a single password enables breaking many other passwords.

The current SIP RFC 3261 states that "basic" authentication based upon plain-text passwords, must not be available. This form of very weak authentication was allowed by the previous SIP RFC 2543. The current SIP RFC recommends use of the Transport Layer Security (TLS), which is not yet widely implemented.

An external attacker can build a directory by scanning for your registerable UA addresses. The scanner can send various requests to your SIP proxy/registrar, and determine from the responses, which addresses are valid and registerable. Registration attempts that are external to the network should rarely be allowed, but this principle is not enforced. Max-Forwards header limits (and other techniques) could be used to detect this sort of attack, but these limits not commonly enforced.

Most registrars/proxy servers will not detect directory scanning or registration hijacking attempts. Furthermore, security products such as standard firewalls also fail to detect these types of attacks.

Effects of Registration Hijacking

Registration hijacking can result in loss of calls to a targeted UA. This may be an individual user, group of users, or a high-traffic resource, such as a media gateway, Automated Attendant (AA), Interactive Voice Response (IVR), or voice mail system. By hijacking calls to a media gateway, all outbound calls can be blocked or otherwise manipulated.

Conversely, a rogue UA acting in the middle can divert calls to a media gateway for toll fraud. A rogue UA acting in the middle can also record audio, signaling, and DTMF codes (for financial transactions).

The Mechanics of Registration Hijacking

The first step in hijacking a registration is to find registerable addresses. This is trivial for an internal attacker who knows the structure of addresses and/or has a directory. For an external attacker, it is possible to scan for registerable addresses. A "scanner," much like a traditional war dialer that searches for modems, can be built to scan for addresses. A scanner can generate several different types of requests to search for addresses, such as SIP INVITES or SIP OPTIONS, each of which returns a response that can be used to determine if an address is valid. Each approach has benefits. Using the INVITE request is less covert, because it will cause the UA to ring, but has the benefit of not requiring authentication—it isn't feasible to require authentication from every external caller. The OPTIONS request is more covert, does not cause a UA to ring, and gathers more information about the UA, but is more likely to require authentication. A scanner could generate a single request, or randomly generate a sequence of requests, and then wait for responses.

Authentication may be required during both the scanning and registration hijacking process. When authentication is used, the proxy or registrar sends an authentication challenge response. This requires one valid username/password in order to conduct the scan. A username/password can be obtained through social engineering, knowledge of the enterprises, or guessed through a dictionary-style attack. Once a single password is known, it can be used to scan addresses throughout your organization.

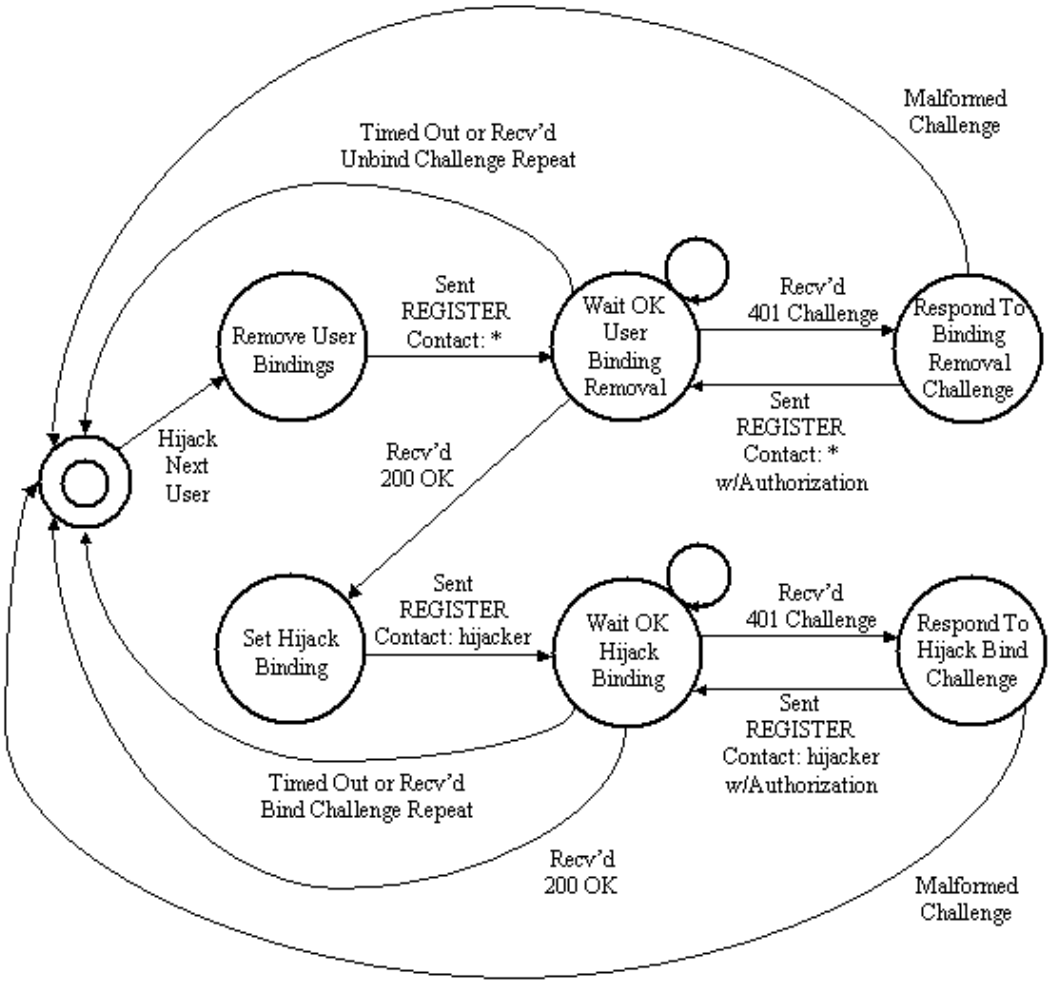
Once a target address (or addresses) has been identified, the target's registration can be hijacked. The hijacking process is outlined below:

- The hijack begins with the attacker sending a specially crafted REGISTER request to the target registrar, to unbind all existing registrations. The "Contact" header line contains the wildcard parameter (*) in conjunction with an "Expires" header line with the value 0 (zero). Together,

these lines request the Registrar to remove all bindings for the target user address specified in the "To" header line.

- It is also possible to send a REGISTER message with no Contact header lines. This informs the Registrar to respond with a list of all existing contacts. This list of contacts can then be used to send separate REGISTER requests to remove each contact individually.
- Either of these approaches work. The advantage of the second approach is that it can be repeated periodically, to verify whether the UA has re-registered. UAs periodically re-register, so for the registration hijack to continue to function, these periodic re-registrations must be removed.
- If the registrar requires authentication, it replies to the REGISTER requests with a challenge. For username/password authentication, the registrar includes a nonce in the response, which the attacker uses to calculate a MD5 digest of the username/password.
- Once all legitimate contacts have been deleted, the attacker sends a second REGISTER message containing a new Contact header line with the attacker's address. An arbitrary Expires interval is requested in the Expires header line of the second REGISTER message (for example, 1 day).
- If authentication is required, the attacker merely responds as described above.

Additional steps are present to wait for response and perform re-tries. The following diagram illustrates the process flow for registration hijacking:



Registration hijacking can also be performed by intercepting and editing REGISTER requests sent between a valid UA and registrar. This attack is possible, but is less of a concern than the attack described above.

Defenses Against Registration Hijacking

The primary defenses against registration hijacking are to use strong authentication and VoIP-optimized firewalls to detect and block attacks. At a minimum, all registrars should require MD5 digest authentication. Strong passwords must be selected. Passwords must not be "mechanically" generated (such as the extension with a prefix/suffix). These steps help to prevent dictionary-style attacks. Ideally, registrars use strong authentication, such as that provided by the TLS.

The Internet Engineering Task Force (IETF)-approved security solution is to use TLS, MD5 digest, and strong passwords.

Registrations from the external network should be disabled if possible—or at least limited to a small set of external UAs (such as teleworkers), who have a valid need to register from the external network. VoIP-optimized firewalls can be used to perform selective registration of external UAs. VoIP-optimized firewalls can also enhance security by providing the following functions:

- Detect and alert upon directory scanning attempts.
- Detect and alert upon any failed authentication attempts; specifically upon any attempts to use dictionaries to guess passwords.
- Log all REGISTER requests.
- Alert upon any unusual pattern of REGISTER requests.
- If the UAs being used do not ever use a REGISTER request to remove valid contacts, detect and block any use of this request.
- Limit REGISTER requests to an established user list.
- Filter any responses to initial REGISTER requests that immediately succeed. This ensures that only correctly configured UAs and registration servers interact.
- Act as a proxy and provide strong authentication for registrars that lack the ability to do so themselves.

Conclusions

There are a number of security issues, which are unique to VoIP. Registration hijacking is one of the more serious issues. An attacker who successfully hijacks registrations in your organization can block, record, and otherwise manipulate calls to and from your organization. This is a very real threat—which you must counter. You can defeat registration hijacking attempts by selecting a registrar that uses authentication, setting strong passwords, and using VoIP-optimized firewalls to detect and block attacks.