Network Security - ISA 656
Voice Over IP (VoIP) Security

Angelos Stavrou

November 13, 2007

What is SIP?

- Session Initiation Protocol
- Control channel for Voice over IP
- (Other control channel protocols exist, notably H.323 and Skype's, but we'll focus on SIP)

What's a Control Channel?

- A control channel — known in the telephone world as a *signaling channel* — does call setup
- It locates the other end point, determines if it's available, asks the endpoint to alert the called party, passes back status to the caller, etc.
- Even in a pure IP world, we need a signaling channel; when connecting to the PSTN (Public Switched Telephone Network), it's essential

History of Signaling Channels

- Telephone signaling was once done "in-band" — that is, the pulses or tones were sent over the same circuit as would later be used to carry the voice traffic for that call
- "Blue boxes" — telephone fraud devices — worked by simulating some of the control tones used to set up free calls
- The solution was to move signaling to a separate, "out-of-band" data network, known today as CCIS (Common Channel Interoffice Signaling)
- Out-of-band signaling is *more* efficient; it allows easy creation of fancier services

Signaling and VoIP

- Why can't we just call a domain name or IP address?
- Many endpoints don't have stable, easily-memorized domain names
- IP addresses change frequently, especially for dial-up and hotspot users
- There are other complexities

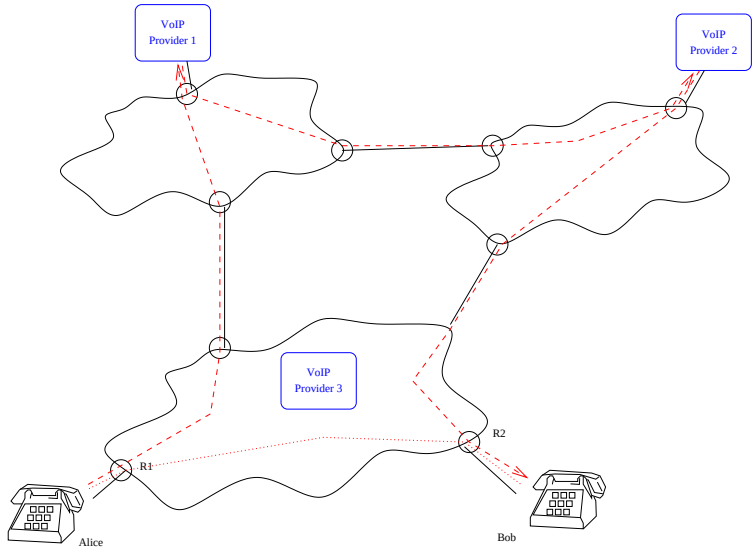
Complexity

- PSTN interconnection: very many endpoints have just a few IP addresses
- Besides, someone has to pay for the PSTN interconnection
- Firewalls
- Network address translators (NATs)
- Mapping between "phone number" and IP address
- Business arrangements between telephone companies
- Unreachable hosts
- Fancy phone features

Basic SIP Architecture

- SIP endpoints speak IP
- Ideally, the actual conversation would be end-to-end, from one SIP phone to the other
- Each node can use a SIP proxy for call setup

Simple SIP Calling



Alice Calls Bob

- Alice uses VoIP Provider 1 (VP1) as her proxy; Bob uses VoIP Provider 2 (VP2) as his
- To call Bob, Alice sends a *SIP URI* to VP1 via TCP
- VP1 determines that the URI points to VP2, so the calls setup request is relayed there via TCP
- VP2 tells Bob about the call via TCP; if he wants to, he can accept it
- Notification is sent back to Alice via VP1
- Alice establishes a direct UDP data connection to Bob for the voice traffic

Firewalls and NATs

- If Alice or Bob are behind firewalls or NATs, they may not be able to set up end-to-end data connections
- In that case, the data traffic for one or both parties will also flow through the proxy

SIP URIs

- How is a SIP URI converted to a SIP proxy address?
- What about ordinary telephone numbers?
- `tel:` URIs are used for ordinary phone numbers
- All SIP URIs are converted by means of DNS magic: NAPTR records
- (For this class, the details aren't important — the essential point is that by means of repeated, complex DNS lookups, any SIP URI is converted to an IP address)

Multiple Proxies

- Sometimes, VP1 will talk to VP3 which will route the call to VP2
- VP1 and VP2 don't know (or trust) each other; they only know VP3 (and VP4 and VP5 and . . .)
- How can they establish a trust relationship? What if money is involved? Can VP2 believe that VP1 will pay?

The Usual Questions

- What are we trying to protect?
- Against whom?

Information at Risk

- Voice content itself
- Caller and called party for each connection
- Billing information

Voice Content

- Confidentiality is the main concern
- Is VoIP easier to wiretap than traditional phone service?
- *Only* the endpoints should see that information; can be encrypted through proxies
- Relatively hard to spoof a voice in real-time, so authenticity is not a major concern

Caller/Called Party Information

- Of great interest to many parties (look at the HP case — that's the data HP was after)
- Useful even after the call (you can't intercept a call after it's over; you can look at who talked)
- Must be kept confidential — but proxies need to see it, to route the call
- Must be authentic, or the call could be misrouted maliciously

Billing Information

- Derived in part from caller/called party information
- May have other information from call routing process
- As before, must be confidential — but there's no need for other parties to see any of it
- Integrity failures can lead to billing errors, in either direction
- (Often a major privacy concern after the fact — again, consider the HP case.)

Eavesdropping on a Link

- How can someone eavesdrop on a SIP call?
- Many ways, including things like listening at a WiFi hotspot
- We'll discuss other ways later in the semester
- For now, let's just assume it's possible

Eavesdropping on a Call

- Simplest approach: listen on some link
- Which link is best for targeting a given person?
- Easiest: their access link
- What if they're mobile? Hard — they could be coming from anywhere
- Do you have the physical ability to listen on the VoIP provider's links? What if the VoIP provider is in a distant, unfriendly country?

Registration Hijacking

- An attacker can try to register with VP2 as Bob
- If the attacker succeeds, all calls destined for Bob with be routed to the attacker

Tearing Down Sessions

- Another false registration attack: tear down calls
- This is a violation of availability

Abusing the DNS

- Call routing is partially controlled by the DNS
- Is it possible to corrupt the DNS answers?
- Under certain circumstances, it's not that hard to do (more details later in the semester)
- By creating fake DNS entries, it's possible to reroute the call to go via an intercept station

Caller/Called Party Information

- Again, link eavesdropping and DNS attacks are straightforward
- The task is easier here; proxies (usually) don't move around
- VoIP providers are high-value targets, since they process many calls

Hacking the Proxies

- Is it possible to hack the VoIP proxy servers?
- Sure — why not?
- Conventional phone switches can be (and some are) hacked, but there's a big difference: the attacker can speak a much more complex protocol to a SIP switch than to a PSTN switch, which means they're more vulnerable
- It's hard to do too much damage with just a few touch-tones!
- Aside: fancier services are easier to hack, on both kinds of telephone systems

IP Addresses

- It's hard to hide IP addresses
- The legitimate recipient sees the sender's source IP address; this leaks location data
- Routing the voice traffic via a proxy can thus be a privacy feature

Billing Systems

- Similar in nature to old-style ones
- SIP billing systems are more likely to be Internet-connected
- Must use strong defenses and firewalls to protect them

Protecting SIP

- As usual, we'll use crypto to guard against eavesdropping
- The details, though, are tricky

Alice to VP1

- Alice has a trust relationship with her proxy
- Authentication is relatively easy
- Usually, TLS is used to protect the TCP session to the proxy
- Alice *must* verify VP1's certificate
- Alice can use passwords or client-side certificates to authenticate herself

Using IPsec

- IPsec is normally difficult to use to protect specific services
- However, if there is an organizational SIP gateway, it might be possible to protect all traffic from the organization to the gateway

Proxy to Proxy Traffic

- VP1 may not have a trust relationship with VP2
- How can VP1 get VP2's certificate?
- More precisely, how can VP1 validate it, if they don't share a trust anchor?
- This applies regardless of what security protocol is used (though TLS is the norm)

End-to-End Signaling Traffic

- Some signaling traffic must be secure end-to-end
- Example: Bob needs to know, authoritatively, that it's Alice who has called him
- However, the intermediate nodes need to see this
- Solution: digitally sign the data (using S/MIME), but don't encrypt it

Key Management for the Voice Call

- How do Alice and Bob get a shared key for voice traffic encryption?
- Alice uses S/MIME to send Bob an encrypted traffic key
- But — how does Alice get Bob's certificate?
- There is no general PKI for SIP users
- True end-to-end confidentiality can only happen by pre-arrangement
- (This statement is more generally true. . .)

Complex Features

- As always, complexity causes problems
- The specific issue here is complex trust patterns
- Let's look at some extra features and see how they cause trouble

Scenario: A Secretary

- Alice tries to call Carol; she reaches Bob, Carol's secretary
- Bob decides the call is worthy of Carol's attention, and wishes to transfer the call to Carol
- Bob's phone sends Alice's phone a message saying "Call Carol, you're authorized"
- Carol's phone has to verify that Bob authorized it

The First Attempt

- Bob prepares an *authenticated identity body* (AIB) with his name and the time
- He sends that to Alice along with Carol's SIP URI
- Alice presents the AIB to Carol
- What's wrong?

Oops!

- Nothing linked the AIB to this referral
- Alice can give the AIB to someone else
- At least there's a timestamp to protect against replays

Solution

- The AIB sent by Bob needs to include Alice's identity
- Carol's phone needs to check the certificate used in Alice's call setup message, to verify that it's really from Alice
- In particular, Alice's identity in the AIB must match the identity in the certificate

CallerID

- Suppose the SIP call is being relayed to the PSTN
- Where does the CallerID information come from?
- Can it be spoofed?

Phone Network Design

- The phone network was based on trust — only "real" telephone companies had phone switches
- No authentication was done on information from other switches, including CallerID
- Today, anyone can run a phone switch...

CallerID and VoIP

- Run Asterisk, an open source PBX program, on some machine
- Get a leased line to a VoIP-to-PSTN gateway company
- Configure Asterisk to send whatever information you want...
- This abuse is happening now; see `http://www.boston.com/news/globe/magazine/articles/2006/09/24/phony_identification/`

GEORGE MASON UNIVERSITY

The State of Practice

- Most vendors don't implement the fancy crypto
- VoIP is thus not as secure as it could be (but Skype does do a lot of crypto)
- Beyond that, SIP phones tend to boot themselves over the network — is that connection secure?
- NIST recommends great care in using VoIP — see `http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf`