

An Avyidian presentation



VOIP Security

Challenges and incidents in contemporary telecommunications

Your next 45 minutes

VOIP Security Lecture. We'll keep it short and to the point...

- Introduction
- Where VOIP is taking us (*well, according to me anyway*)
- Quick overview of common VOIP threats
- VOIP challenges and incidents for related to ...
 - ... National and Homeland Security
 - ... Incumbents and VOIP providers
 - ... End Users

Introduction

How I got to know VOIP

- So, one day an information security professional invests into a VOIP technology company...
- What did I learn:
 - SIP is the most insecure modern protocol ever invented
 - VOIP start-ups require a lot of money
 - VOIP is definitely not ready to be a front-end technology (*yet*)
 - Oh, and investment rounds mess up your business



Where VOIP is taking us

Or at least, my honest opinion

- VOIP as a front-end technology is dead. Why? Hear me out:
 - VOIP is currently only useful on fixed lines, while mobile applications are cumbersome, frustrating and simply not mature enough for a large audience (*do you really need examples??*)
 - Fixed-Mobile convergence is being experimented with by smaller companies, such as Fring, Talkster, Nimbuzz, Truphone, Cherry, ... (*successful experimental companies have SS7, Wi-Fi and SIP switching; others are just goofing around...*)
 - Cell phone manufacturers (Nokia, etc.) are cutting back on SIP functionalities using *obscurity* practices to limit the loss for the incumbents (their largest stakeholders)
 - Current incumbents are ready (don't be fooled), it's just sound financial, acquisition and risk management strategy that prevents "them" from blowing the smaller companies out of the water...



Where VOIP is taking us

Or at least, my honest opinion

- OK, what will happen next then ?
 - The experimental wave, where smaller players live in the illusion of going for a profitable breakthrough by experimenting with technology to reduce the cost of mobile calls while trying to support FMC features. Incumbents sit back and enjoy the show. This is where business models are conceived.
 - The maturing wave, where alliances will be forged with profitable players that have established wholesale contracts with incumbents and carriers. These alliances are a forebode for future acquisitions. Similar business models are prepared by incumbents. I call this the *proof of concept* period.
 - The go to market wave, where incumbents offer triple and quadruple play services to their audience, winning back customers through acquisitions and unbeatable cost-savings, while employing stable technologies such as femtocell and back-end VOIP services to offer better quality than pure VOIP players, which will then be a dying breed.



Quick overview of common VOIP risks

A taxonomy of risks

- Privacy risks (confidentiality):
 - Eavesdropping on conversations, using hacker tools such as *vomit* (Cisco phones mainly), *Oreka* or *VoIPong*. Or simply go commercial using *Vonalink SoloRecord*, *Zoom CallREC*, etc.
 - Call behavior analysis, by extracting SIP and RTP headers and map your victims' calling patterns. Yes, a simple *tshark* or *tcpdump* will do...
 - Extract DTMF tones, in order to obtain PIN codes or other authentication tokens one simply can run a sniffed session through *DTMF Encoder* or other open source decoder tools



Quick overview of common VOIP risks

A taxonomy of risks

- Availability risks (oh, in VOIP terms this is called 'loss'):
 - Loss or degradation of conversations due to bandwidth or processing depletion attacks (yes, disruption of services) using DNS spoofing or simple UDP flooders. Can also be induced by RTP, INVITE (and the "INVITE of Death") and IAX flooders, application buffer overflows or ARP spoofing attacks.
 - Call teardown situations, where the injection of SIP packets introduce a rogue "SIP BYE" packet and tears down the call session.



Quick overview of common VOIP risks

A taxonomy of risks

- Health and safety risks (yes, VOIP can kill):
 - Imagine you don't have connectivity and your toddler has a lethal seizure ? Is VOIP FMC looking hot now ? Well, does it ? Talk to the parents of Elijah Luck.
 - Administrative, legally and technically looped implementation of E911 services is making victims. So, are we saying "You can make calls to whoever you want, but don't call 911 when you're in trouble" ? Yes, we do...



Quick overview of common VOIP risks

A taxonomy of risks

- Theft of services, when someone goes about stealing minutes from your account to make free phone calls and you end up paying for them...
- Unwanted contact, where insertion of rogue packets can lead to unwanted content and contacts; such as SPIT (“*SPAM over IP Telephony*”) and more.
- Impersonation and manipulation
 - Called ID Spoofing
 - Fax manipulation (attention: T.30/T.38 manipulation is very hard to do)
 - Caller Hijacking



VOIP challenges and risks

For National and Homeland security

- What VoIP components are at risk:
 - End-User equipment (e.g. IP-Phones, mobile phones running SIP applications)
 - IP network equipment (e.g. routers, switches, etc.)
 - RTP and SIP routing and switching equipment
 - Billing databases and invoicing systems



VOIP challenges and risks

For National and Homeland security

- **National Security and Lawful interception challenges:**

- Asian and Middle East VOIP policies are restrictive and block VoIP traffic, but is this 100% effective ?
- CALEA and ETSI standards include “packet mode telecommunication”, but how to put in practice ?
- Economic protectionism for national telecommunication industry disguised under “anti terrorist acts” ?

Some first hand illustrations and incidents:

- UAE, Dubai’s VoIP policy over the past few years and the occasional VoIP incidents upsetting residents;
- GIS’s policy against VoIP (and Skype) by Russian Union of Industrialists and Entrepreneurs
- TruPhone bypasses roaming due to local SS7 number detection



VOIP challenges and risks

For Incumbents and VOIP Providers

- **Internet Telephony Service Providers:**

- Additional costs for Lawful Interception compliance to government regulations and policy
- Revenue assurance has become an additional hurdle, due to potential SQL injection attacks in SIP packets that might affect billing systems
- Financial consequences of customer hacks are paid by ... ?
- First ever real-life case (2006): VoIP fraud is a new (but serious) phenomenon
http://www.usdoj.gov/usao/nj/publicaffairs/NJ_Press/files/pdffiles/moore-complaint.pdf

Some first hand illustrations and incidents:

- Transfer (XFER) issues on Asterisk aren’t billed
- The legal-commercial trade-off for incumbents in times of crisis
- A financial case of by Canadian SIP termination fraudsters onTraff-x (5 mio EUR)



VOIP challenges and risks

For End Users

- Financial losses:
 - Customer has his account hacked (easy to guess password: “201”) and used to make long-distance phone calls for one month, amounting up to 75.000 EUR
 - IP Phone hacked to call Liechtenstein and Sierra Leone up to 207.000 USD in October 2008 (Canada)
- Disruption and hacking:
 - Accounting firm with 27 employees (Brussels) was hacked and voicemails were screened for over six months
 - SQL injection into SIP traffic bypass CDR-parsing and invoicing for two months in a row, up to 38.000 EUR
 - EU investment bank had a trojan-incident with modified VoIPong source code to monitor and send calls in MP3



VOIP challenges and risks

For End Users

- Safety or the Elijah Luck case (U.S.)
- Injection attacks:
 - Using RTP Insertsound 3.0, obnoxious sounds uploaded into phone conversation between father and daughter (ok, so this might be considered *fun*, she did get a whole lot to explain about her “extracurricular activities”)
 - Voicemail bombing using spam messages
 - Personal experiences on DTMF replay attacks on Phone Bank systems
- Caller ID Spoofing:
 - Personal experiences with social engineering attacks (mostly successful!)
 - The 112 experiment. The “Hello, this is your bank” experiment. The “Hello, this is your girlfriend’s lover using her cell-phone”



VOIP challenges and risks

In general

- So... Honestly ?
 - Actually, few incidents happen and VOIP incidents are currently rather limited to theoretical risks
 - Blown out of proportion ? It's a chicken-and-egg situation...
- Currently, low visibility, but what's around the corner ?
 - Governments on VOIP (FOD Foreign Affairs, etc.)
 - Your hospital on VOIP infrastructure (AZ Groeninge, UZ Leuven, etc.)
 - Your financial institution on VOIP (KBC, etc.)
 - ...



An Avyidian presentation



VOIP Security
Challenges and incidents in contemporary
telecommunications