Critical Danger:

An Introduction to Cross Site Scripting Attacks for People Who Do not Know what Cross Site Scripting Attacks Are.
Agenda

- Introduction to Browsers
- Javascript
  - Java
    - Indonesian spice trade
    - Dutch East India Company
  - Script
    - Plays, Movie and other…
- Browser Attacks Visualization
  - Text only version
VoIPhreaking

SIPhallis Unveiled

the gruggq
Agenda

- Introduction
- VoIP Abstract
- Phreaking
- VoIPhreaking
- VoIPPhishing
- Conclusion
- Q&A
Introduction

- Voice/Video over Internet Protocol (VoIP) is hot
- Grugg is hotter
  - Lots of years of security research
  - Focusing on VoIP security since forever
  - Snazzy haircut
- VoIP is a serious security threat
  - Security practices are still emerging
  - Deployment isn’t waiting for security first
VoIP Abstract Agenda

- Overview
- Functionality Realms
- Protocol Suites
- Infrastructure
VoIP Overview

- Provides a mechanism for people to communicate over networks
- Real time multimedia exchange
- In development since early 1990s
  - Bandwidth and services finally make it economically feasible
- Cost is the major driver for VoIP deployments
Functionality Realms

- **Signaling**
  - Call management
    - Setup, location, tear down, etc.

- **Media**
  - Content streams

- **PSTN integration**
  - Telephone to Internet traversal
    - Location, media conversion, signaling propagation
Protocol Suites

- **Signaling**
  - Session Initiation Protocol (SIP)
  - H.323

- **Media**
  - Real Time Protocol (RTP)
    - Transported over UDP

- **PSTN Integration**
  - Media Gateway Control Protocol (MGCP)
  - ENUM
Signaling: Session Initiation Protocol

- ASCII text protocol designed by Internet crunchies
  - Bastard child of HTTP and email
- Over a decade old
  - Design began in 1995
  - Still considered “emerging”
- Commonly used for new deployments
  - Most used VoIP protocol on the Internet
SIP Messages

- Start line
  - Request or Response
- Headers
  - Information about the message
    - Destination
    - Origin
    - Route
- Body
  - Usually media stream location information
    - Session Description Protocol
Request Messages
- Method based request system
  - INVITE, BYE, REGISTER, etc. etc.

Response Messages
- Error code + reason (smells like HTTP)
  - 404 Not Found, 403 Forbidden

Message Headers
SIP Headers

- Display information
  - To: URI
  - From: URI

- Routing information
  - Contacts: URI

- Time To Live
  - Max-Forwards

- Bad Ideas
  - Alert-Info:
Infrastructure

- **User Agents / Terminals**
  - Soft phones, Hard phones, Voice Mail, etc.
- **Proxies**
  - Entry/Exit points to a VoIP network
  - Provide authentication services
- **Location Servers**
  - Registrars, Gatekeepers
  - Map URIs to IP addresses
- **Gateways**
  - Media Gateways, Signaling Gateways
Phreaking Agenda

- History
- Techniques
- Death of Phreaking
History

- Started in the 1960’s
- Exploited in-band signaling
- Relied heavily on hardware attacks
- Famous Phreaks
  - Steve Jobs
  - Steve Wozniak
  - Cap’n Crunch
Techniques

- In band signaling @ 2600 Mhz
- Typically used for toll-fraud
- The “colour boxing era”
  - Blue boxing
  - Red boxing
Death of Phreaking

- Out of band signaling
- Aggressive prosecution of phreakers
- Improved fraud analysis complements improving technical solutions
- “I’m not dead yet… I’m feeling better…”
  - The birth of VoIPhreaking
VolPhreaking Agenda

- Motivations
- Attacks Overview
- Techniques
Motivation

- Hackers enjoy exploring new technology
- Returning to the PSTN after being expelled in the 90s
- Money.
Techniques

- Media attacks
  - Eavesdropping
  - Injection
- Signaling attacks
  - Hijacking
  - Rerouting
  - Eavesdropping
- PSTN attacks
  - MG intrusion
VoIPhishing

- Application of VoIPhreaking attacks for phishing
- Harvesting personal information
  - Account numbers and access codes
  - Personal identification data
- Wide range of possible exploitation scenarios
- Expect to see these in the news next year
  - Or not…
Techniques

- Impersonating a bank
  - Caller ID spoofing
- Hijacking
  - ENUM poisoning
  - Account theft
  - Man in the middle attacks
- Media stream manipulation
Hijacking

- ENUM Poisoning
  - ENUM database used to route VoIP calls more cheaply
  - Insert a false entry for a financial institution
- Account theft
  - Carrier level SIP Registrar mapping manipulation
  - Redirect inbound calls to an evil call server
Hijacking, cont.

- Man in the middle attacks
  - Manipulate media location
    - Send call streams to multiple locations
  - Signaling manipulation
    - Create false conference call
  - Can happen anywhere between the customer and the bank
- Media stream manipulation
  - Adding content to existing call streams
Demo

- RTP Injection
Conclusion

- New and Improved, Internet Telephony
  - Make phone calls as secure as email!
- Dialing a number doesn’t mean you’ll get that person
- What you hear on a phone call might be more than was said
Questions & Answers