The poor state of SIP endpoint security

Kamailio World, 03.04.2014

Henning Westerholt

Head of IT Operations Access

Agenda

- Introduction
- Reasons for security issues, motivation for attackers
- Past security issues in 2013
- FritzBox security issue
- Security process and preparations

About me

- In general
  - Open Source and Linux guy since 2001
  - Seriously involved in IT since 2003
- 1&1 Telecommunication AG
  - Since beginning of 2007 as software and system developer
  - Now department lead in IT Operations, responsible for the “Access” IT systems
- Kamailio Open Source project
  - Since 2007 involved in the project
  - Developer and member of management board
  - Regularly present on different events
- Part of the much bigger team that design, build and also operate the services I’ll present in this talk

1&1 Telecommunication AG

- More than 6250 employees in the group
  - 2,656 billion € revenue in 2013
  - about 312 Million € EBIT
- Offices in several European and international locations
  - Main development and IT offices in Karlsruhe
  - VoIP development also in Bucharest
- Five datacenters with over 70.000 Servers in Europe and USA
- Own global redundant WAN with hundreds of Gbit/s external bandwith
- Second place w/r to customer base in the German DSL market
- Other products, but not focus of this talk
  - webhosting, E-Mails, Portal, Advertising
- Biggest customer growths in 2013 in the mobile area

Source: United Internet Financial Reports, Shareholder Statements, http://www.united-internet.de/

VoIP backend at 1&1

- Operated mainly with Open Source components
  - Kamailio, Asterisk, MySQL, Puppet, Debian..
- One of the biggest deployments out there
- Data
  - Over three million customers on the platform
  - More than eight Million subscribers
  - Interconnections to Telefonica, Vodafone and QSC and others
  - More then one billion minutes per Month to the PSTN
- Geographical redundant backend in a load-sharing setup
- Focus towards small businesses and home users
- Provides services for ADSL, VDSL, UMTS and LTE customer connections

Reasons for CPE security issues

- (Too) many features in one box
  - IP Routing, Firewall, Application level gateway, QoS..
  - HTTP Server, FTP Server, UPnP Server, Media Server..
  - DSL and VoIP User Agent, PBX Server, VoIP Registration Server
- Competitive Environment
  - Smaller ARPUs, smaller margins
  - Competition over price and features
  - Usually no huge interest or incentive from customer and operators to update
- Interesting target
  - Good connected to IP and phone network
  - Always on, no or little user monitoring
  - Access to user data and network traffic
  - Usually Outdated software and hardware
- Huge numbers deployed in the field

Past security issues

- Asus
  - Two security problems reported from researcher in Q3 2013 to manufacturer
  - Rollout not done in time
  - Public in February 2014
- Security bugs
  - Login to FTP server without password
  - Internal backup suite cfg files world-readable
  - Remote changes on cfg files
- Possible attacks
  - Access to all internal traffic
  - Gateway to internal network for further attacks
  - Data access on FTP server
  - Data access on internal backup server
- Still many routers online with this bug

Past security issues

- D-Link had several issues in the past year
- Security Bug in the UPnP module
  - Attack with special POST request
  - Remote OS command injection
  - On some devices also remote file execution
  - Possible attack - access to everything possible
- Security bug with User-Agent handling
  - Access with special UA without password
  - Configuration changes possible
  - Possible attack - Man in the middle over DNS or IP routing changes
- O2 router issues
- Security Bug
  - Insecure standard WLAN password
  - Possible attack – access to internal WLAN traffic

FritzBox Security issue

- FritzBox used from 1&1 and many other German providers, manufactured from AVM
- Security bug
  - Access to cfg without password
  - Remote code execution from web sites or HTML email
  - Almost all AVM products affected
- Possible attacks
  - Access to user credentials
  - Access to internal communication
  - Setup of VPN connection to internal network
- Attacks seen
  - Fraud with stolen user credentials, several hundred thousand euro damage at a “regional telecommunication provider”
  - Fraud with telephony accounts setup on local FritzBox
  - Several fraud cases also at 1&1

FritzBox Security issue development

- Extension in attack vector over time
  - First only CPEs with activated remote management
  - Later most of the CPEs
  - Later again all CPEs and also WLAN and Powerline adapters
- Increasing publicity of the issue
  - First week of February reports in IT smaller news sources
  - Second week in February reports in major IT news sources
  - Third week in February reports in the television and major newspapers
  - First week in March public exploit in news
- Increasing effort in incident response
  - Due to extensions in attack vector
  - Increasing risks due the publicity of the bug
  - Increasing customer communication requirements

FritzBox Bug Incident measures

- Security incident for tracking of all tasks inside the company
  - Coordination of internal and external communication
  - Information to management
- Publishing of updates for all affected hardware in short time from AVM
  - Update of all firmware software in a few weeks
- Rollout of updates with automatic provisioning processes
  - Monitor process closely, optimize if necessary
- Changes of password for affected services automatically or by customer information
  - Customer information expensive and not really effective
- Closely monitor fraud volume and vectors
  - fast development of counter measures
  - Work with local law enforcement
  - Proactively blocking of expensive destinations

How to prepare

- Have established incident processes involving all important company parts
  - You don’t want to work on the basic infrastructure when something bad happens
- Maintain a close relationship with your CPE vendor
  - E.g. with regular telephone conferences and technical discussion
- Ask your vendor for security evaluations including source code review
  - Most of the mentioned security bugs were in the input validation domain
  - AVM stated that four independent companies did not found the issue
- Enforce the usage of TR.69 for all of your customers
  - To enable automatic firmware rollouts and password changes
- Secure default configuration
  - External admin access disabled
  - UPnP or other media server restricted to local network
  - Random WLAN password
  - User generated password for admin access

How to prepare

- Have resources in place for preparation and executing the rollout
  - Firmware needs to be tested
  - Fast firmware rollout generates a lot of load on the systems
  - Some boxes will also break during rollout
- Think about the whole process
  - You have updated your boxed in the field, what about the ones in stock?
- Prepare your management
  - It will get expensive and block many other projects
- Prepare your customer communication
  - Work closely with the CPE vendor
  - Prepare boxes replacement policies
  - Customers will get nervous about this issue from media report and flood Hotline and also social media channels

How to prepare

- Have real-time monitoring and fraud alarming tools
  - On a weekend a lot of damage can be done
  - You want to improve your tools, not develop them during an attack
- Don’t re-use service credentials for user visible services
  - They are much harder to change
- Don’t overload your infrastructure or people with the unusual requirements
  - Databases or firmware download hosts
  - On-call services and testing resources
- Protect your backend
  - Overload protection on edge servers
  - Brute force protection on application server

Summary

- Attackers only get better over time, so expect more CPE issues in the future
- Most big security issues starts small, so try to catch the attackers early
- Learn from past attacks and think about your available processes and tools
- Choose a serious CPE vendor, establish a good relationship and stay there
- Risks from bad incident handling are usually much higher that attack risks
- Don’t panic

Thanks for your attention!

Questions?

Contact

- Henning Westerholt
  - hw@kamailio.org
- Looking for a job?
  - VoIP Backend Developer for Kamailio and Asterisk
  - System Administrator for VoIP and DSL
  - More information from me or at http://jobs.1und1.de/
- License of this slides

  http://creativecommons.org/licenses/by-nc-nd/3.0