
Secure real-time audio/video communication – H.350, Encryption & Gatekeeper/Proxy – using H.323 (...and a bit SIP)

Tutorial/workshop session

- Introduction Gatekeeper/Proxy + Firewalls, Security concepts -

**19th APAN Meeting
Bangkok, Thailand
January 2005**

Outline

- The H.323 firewall problem (...and problems with firewalls in general)
- GnuGK
 - What is it?
 - Why you should use it?
 - The proxy
 - Authentication (? Egon's part)
 - H.350 & H.235
- Firewalls & GnuGK – A security concept?!

The H.323 firewall problem

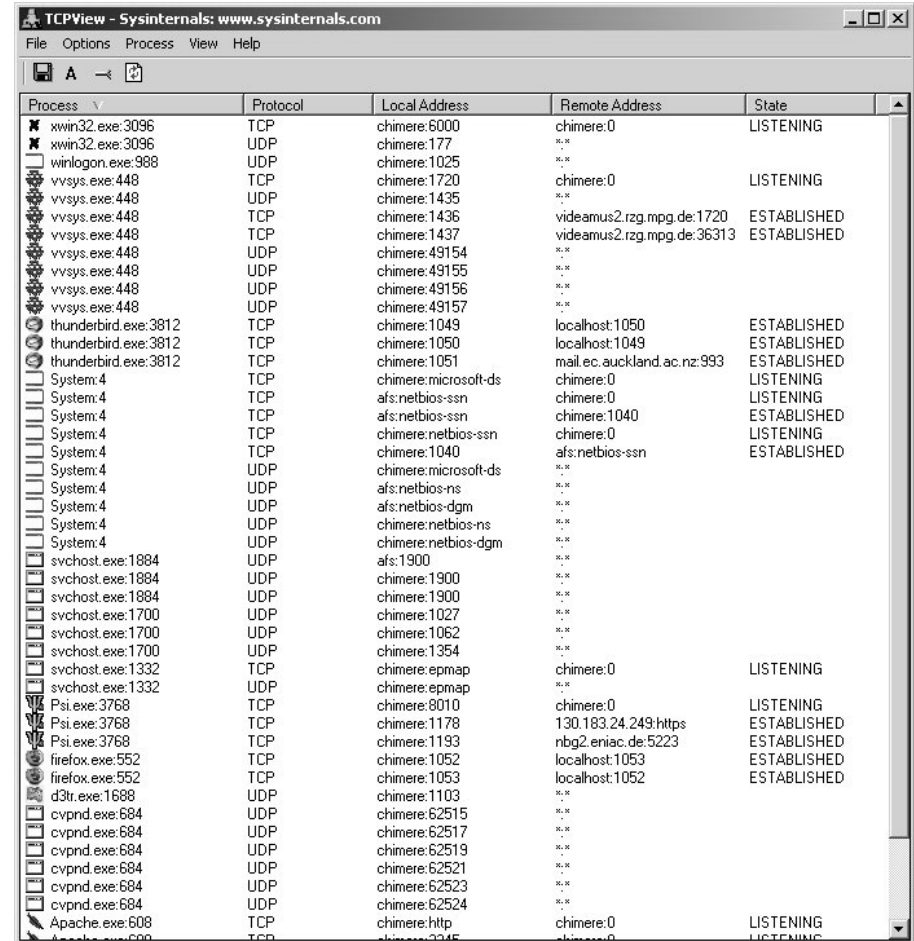
- H.323 uses a few fixed ports, such as 1718, 1719 tcp
- Other communication ports are DYNAMICALLY negotiated during the setup process
 - Used port range: 2^{10} to 2^{16} (1024 – 65535) udp
 - 4 to 8 ports used per call
 - This dynamic negotiation is the problem aka. H.323-Firewall problem

How do you open ports if you don't know them?

- Complexity of the media streams can cause problems as well
 - many different sub-protocols are used for several different data/control channels ? today more or less just a minor glitch

The H.323 firewall problem (cont')

- The screenshot on the right hand side shows a Viavideo in call
 - 3 TCP streams
 - Control channels (H.225, H.245)
 - 1 fixed port: 1720
 - 2 dyn. ports: 1436, 1437
 - 5 UDP streams
 - 1 Control channel
 - 4 data channel (a/v)
 - all ports dynamically
 - 1435
 - 49154 to 49157

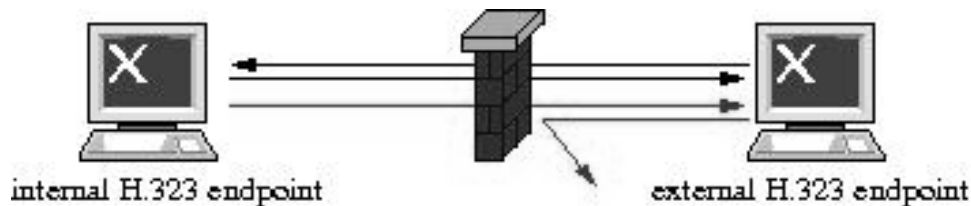


The screenshot shows the TCPView application window with a table of active network connections. The table has columns for Process, Protocol, Local Address, Remote Address, and State. The connections are as follows:

| Process | Protocol | Local Address | Remote Address | State |
|----------------------|----------|----------------------|----------------------------|-------------|
| xwin32.exe:3096 | TCP | chimere:6000 | chimere:0 | LISTENING |
| xwin32.exe:3096 | UDP | chimere:177 | ... | ... |
| winlogon.exe:988 | UDP | chimere:1025 | ... | ... |
| vvsys.exe:448 | TCP | chimere:1720 | chimere:0 | LISTENING |
| vvsys.exe:448 | UDP | chimere:1435 | ... | ... |
| vvsys.exe:448 | TCP | chimere:1436 | videamus2.rzg.mpg.de:1720 | ESTABLISHED |
| vvsys.exe:448 | TCP | chimere:1437 | videamus2.rzg.mpg.de:36313 | ESTABLISHED |
| vvsys.exe:448 | UDP | chimere:49154 | ... | ... |
| vvsys.exe:448 | UDP | chimere:49155 | ... | ... |
| vvsys.exe:448 | UDP | chimere:49156 | ... | ... |
| vvsys.exe:448 | UDP | chimere:49157 | ... | ... |
| thunderbird.exe:3812 | TCP | chimere:1049 | localhost:1050 | ESTABLISHED |
| thunderbird.exe:3812 | TCP | chimere:1050 | localhost:1049 | ESTABLISHED |
| thunderbird.exe:3812 | TCP | chimere:1051 | mail.ec.auckland.ac.nz:993 | ESTABLISHED |
| System:4 | TCP | chimere:microsoft-ds | chimere:0 | LISTENING |
| System:4 | TCP | afs:netbios-ssn | chimere:0 | LISTENING |
| System:4 | TCP | afs:netbios-ssn | chimere:1040 | ESTABLISHED |
| System:4 | TCP | chimere:netbios-ssn | chimere:0 | LISTENING |
| System:4 | TCP | chimere:1040 | afs:netbios-ssn | ESTABLISHED |
| System:4 | UDP | chimere:microsoft-ds | ... | ... |
| System:4 | UDP | afs:netbios-ns | ... | ... |
| System:4 | UDP | afs:netbios-dgm | ... | ... |
| System:4 | UDP | chimere:netbios-ns | ... | ... |
| System:4 | UDP | chimere:netbios-dgm | ... | ... |
| svchost.exe:1884 | UDP | afs:1900 | ... | ... |
| svchost.exe:1884 | UDP | chimere:1900 | ... | ... |
| svchost.exe:1884 | UDP | chimere:1900 | ... | ... |
| svchost.exe:1700 | UDP | chimere:1027 | ... | ... |
| svchost.exe:1700 | UDP | chimere:1062 | ... | ... |
| svchost.exe:1700 | UDP | chimere:1354 | ... | ... |
| svchost.exe:1332 | TCP | chimere:epmap | chimere:0 | LISTENING |
| svchost.exe:1332 | UDP | chimere:epmap | ... | ... |
| Psi.exe:3768 | TCP | chimere:8010 | chimere:0 | LISTENING |
| Psi.exe:3768 | TCP | chimere:1178 | 130.183.24.249:https | ESTABLISHED |
| Psi.exe:3768 | TCP | chimere:1193 | rbg2.eniac.de:5223 | ESTABLISHED |
| firefox.exe:552 | TCP | chimere:1052 | localhost:1053 | ESTABLISHED |
| firefox.exe:552 | TCP | chimere:1053 | localhost:1052 | ESTABLISHED |
| d3tr.exe:1688 | UDP | chimere:1103 | ... | ... |
| cvpnd.exe:684 | UDP | chimere:62515 | ... | ... |
| cvpnd.exe:684 | UDP | chimere:62517 | ... | ... |
| cvpnd.exe:684 | UDP | chimere:62519 | ... | ... |
| cvpnd.exe:684 | UDP | chimere:62521 | ... | ... |
| cvpnd.exe:684 | UDP | chimere:62523 | ... | ... |
| cvpnd.exe:684 | UDP | chimere:62524 | ... | ... |
| Apache.exe:608 | TCP | chimere:http | chimere:0 | LISTENING |
| Apache.exe:608 | TCP | chimere:80 | chimere:0 | LISTENING |

The H.323 firewall problem (cont')

- The big picture or what happens if...
 - often the setup (tcp) will go through the firewall (black lines)
 - audio/video can be send from inside ? outside, but not vice versa
 - external H.323 endpoint gets audio and video
 - internal H.323 endpoint gets a black screen ☹



The H.323 firewall problem (cont')

- Is there a way to solve this problem?
 - Don't use H.323 ☹
 - “OpenFirewalling” ☹
 - Open the firewall for all H.323 endpoints
 - Wait until some one rewrote the standard ☹
 - Use GnuGK 😊

GnuGK

- What is it?
 - A fully functional Gatekeeper
 - Available for free
 - Supports H.323 V.4 (depending on underlying libraries)
 - Besides the standard features each Gatekeeper has, such as Bandwidth control, Address translation, Admission control, Zone management, and Call control signaling, GnuGK comes with a wide range of authentication methods and a full-feature media proxy

GnuGK

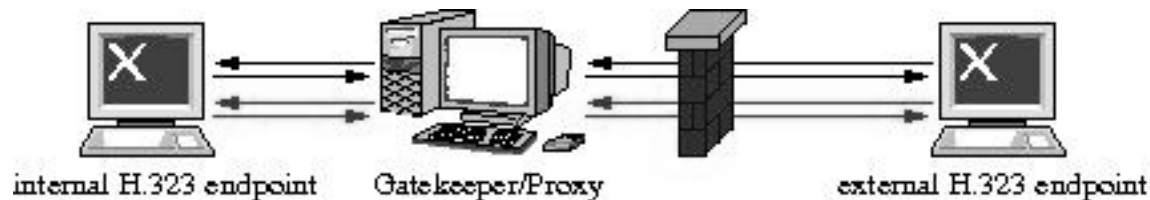
- Why should you use it?
 - Its free 😊
 - It runs on a variety of OS, like Unix/Linux, Windows and Macs
 - Precompiled binaries are available for several platforms
 - Some features are not (yet) available on Windows
 - Media Proxy (? this solves the H.323-firewall problem)
 - Several endpoint authentication methods
 - New services can be applied by interacting with other tools
 - billing, etc.

GnuGK

- The proxy
 - Proxy is used to bypass firewalls
 - Only gk/proxy IP address is allowed to bypass the firewall by opening the port ranges only for this system, and not for all clients
 - Proxy transports ('proxies') all control/media streams (tcp/udp)
 - Data/Stream flow
 - Endpoint ? Proxy ? Endpoint: for signaling streams (tcp)
 - Endpoint ? Proxy ? Endpoint: for media streams (udp)
 - Endpoints don't know that proxy is a proxy; they assume proxy is the endpoint

GnuGK

- The proxy (cont')
 - external H.323 endpoint 'talks' to the gatekeeper/proxy, who then forwards the streams to the internal H.323 endpoint, and vice versa
 - only the IP of the gatekeeper/proxy is allowed to bypass the firewall
 - both endpoints get audio/video



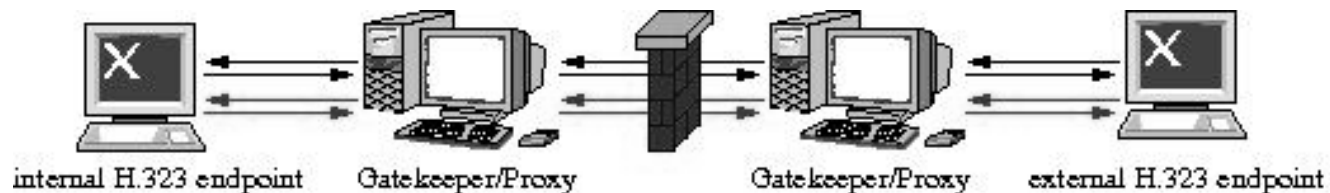
GnuGK

- Is it secure?
 - All systems who have internet connection can be hacked, highjacked, etc. NO SYSTEM IS 100% SECURE
 - Apart from that, yes it is, because
 - Videoconferencingsystems and/or IP-Phones are still protected by the firewall, and they are only allowed to talk to the IP of the gatekeeper/proxy
 - Gatekeeper/Proxy should be located in DMZ
 - An example: H.323 system using this scheme were not affected by the H.323 vulnerability reported early 2004
 - Is it possible to get it even more secure?

YES

GnuGK

- ...add some more security
 - Add a second gatekeeper; one in the internal network, the other one in the external network, and open the firewall, that only the two IP addresses are allowed to talk to each other ? other traffic is blocked



GnuGK

- Some extra features
 - Proxy can be fully/partially switched off
 - if deactivated, GnuGK just works as a standard gatekeeper
 - Proxy can be partially switched off, e.g. for internal communication
 - Proxy can handle different media streams such as
 - Videocodecs
 - H.261, H.263, H.263+, H.264,...
 - Audiocodecs
 - G.728, G.711, G.722, Siren,...
 - Data streams
 - T.120, People+Content (Polycom), Duovideo (Tandberg), H.239
 - AES/DES encryption
 - Can handle some 'exotic' clients
 - H.323-VRVS gateway, FVC server

GnuGK

- Some extra features
 - Support for NATed endpoints/private networks
 - Load balancing via alternate GKs
 - Call Queueing (using 3rd party software)
 - Call forwarding
 - H.235
 - ToS bit forwarding
 - Accounting/Billing (File, mySQL, Radius,...)
 - Call limitation fr prefixes, IPs, subnets, etc.
 - Several authentication schemes
 -

...ok, lets use it