Architecture of XMPP Proxy for Server-To-Server Connections

Juha Järvinen, Aleksi Marttinen, Marko Luoma, Markus Peuhkuri and Jukka Manner

Department of Communications and Networking, Aalto University
Finland

- This year the 100-year-old Finnish Maiden, birthday 6.12.2017
  - #Finland100

- 5 521 571 inhabitants (13.11.2017)
  - 338424 km²
  - Density: 16/km²

- 168000 lakes

- Waiting for snow
  - In Finnish about 40 words for snow
Aalto University

- Aalto University is a multidisciplinary university, where science and art meet technology and business
- Helsinki University of Technology 1849-2011
- Campus area next to Helsinki, Espoo, Otaniemi
- 17 563 students
- Aalto.fi
- This Saturday Aalto Campus is getting own Metro station ”Aalto University”
Architecture of XMPP Proxy for Server-To-Server Connections

- Driving factor was build up a proxy service for each service
  - A security aspect to secure own services in Internet
  - Proxies enable interoperability between different security domains acting as Information Exchange Gateways (IEGs).
  - Different proxys and mechanisms for HTTP(S), SMTP etc.
The Extensible Messaging and Presence Protocol (XMPP)

- Quite many organization use XMPP protocol in instant Messaging
  - Message, Presence information, files, Voice

- The XMPP Standards Foundation develops extensions to the protocol in the XEP series
  - 4 core RFCs
  - Currently there are approximately 170 extensions, XEPs, for the XMPP
    - Different XMPP server and client software exploit XEPs solely for their own interests.

- The XMPP uses a client-server architecture – clients do not talk directly to one another, i.e. the XMPP model is decentralized. There are different methods for both client-to-server (c2s) and server-to-server (s2s) connections.
  - All the messages are sent in an XML message structure, called stanza.

- Very heavy link between DNS and XMPP, SRV records
XMPP Proxy

- For c2s connections there are available open-source proxy implementations
  - IMSpector
- Several of those proxies act as connection managers by joining client connections to improve the scalability of the XMPP server
- The Bidirectional-streams Over Synchronous HTTP (BOSH) technique can be utilized in client proxies. BOSH is designed for asynchronous XMPP communication between a client and server using HTTP
XMPP Proxy for s2s

- Transform ‘signal’ to another format
  - Internet Relay Chat (IRC), HTTP
  - Losing information?
- Building XMPP server to act a proxy from scratch
  - XEPs?
  - Maintaining?
- Idea: Using cluster mode of certain (vibrant) XMPP server communities
Openfire & Hazelcast clustering

- Init testing, what happens
- Problems if initiation begins from Client A
  - connecting to XMPP2 and not participates in Multi-User Chat (MUC)
- Everything ok if vice versa
- Something has to be done to XMPP2 server
- Cluster link: not normal s2s traffic (stanzas)
- IP & TCP connections break
What done?

- Modified code in routing a file in XMPP2
- Finding out Node ID of XMPP1
- Forward all the sessions to XMPP1
Results

- Acting as proxy
- No extra delay
- IP & TCP connections
Pros & Cons

- TCP connection breaks
  - only the content of messages is forwarded
  - not the XMPP stanza structure.
  - attacks targeting the XMPP stanza structure are blocked automatically.
  - At the cluster link we are able to implement DPI functionalities, for example, virus scanning
  - IEG, Security domains

- The only drawback of this architecture is the dependency of the software used in the XMPP server – the proxy server software version has to be the same across all nodes.
- In such a case, one single vulnerability can give an attacker complete access to an internal network.
Thank You!