Comunicaciones Seguras

Voz/IP y Video conferencia

Rafael Bonifaz: rafael@bonifaz.ec

Voz/IP

- La información en Internet viaja como paquetes de datos
- Estos paquetes pueden ser texto, imágenes, videos o voz
- Existen protocolos para transmitir voz y video por Internet
  - Normalmente protocolos UDP
  - SIP, IAX, XMPP (Jingle)
  - Chats grupales con Mumble

Herramientas comunes de Voz/IP

- Suelen depender de servicios hipercentralizados
- La mayoría de estos servicios pertenecen a empresas miembros de PRISM
- Skype (Microsoft)
- WhatsApp (Facebook)

Software Libre y Voz/IP

- Clientes que soportan cifrado fin a fin
  - Jitsi soporta VOZ/IP, video conferencia, compartición de pantalla y cifrado
  - Ring que utiliza protocolo SIP modificado yx es p2p.
  - Tox es un **protocolo** VOIP similar a Ring
  - Mumble
  - ¿Signal?
- https://libreplanet.org/wiki/Group:Skype_Replacemen
- Software para servidores
  - Asterisk y distribuciones como Elastix
  - Mumble
  - Jitsi - meet

Jitsi

- Se requiere una cuenta en un servidor XMPP o SIP
- Soporta cifrado fin a fin a través de ZRTP
- Cliente de chat soporta OTR nativamente
- Multiplataforma
- No funciona con Tor
- http://www.jitsi.org/

Jitsi – meet

- Software para servidor
- Funciona con navegadores que soporten WRTC
- Existe implementación para probar en
  - https://meet.jit.si
- Canal cifrado con https
- Conveniente porque no hay que instalar software adicional en la máquina
- ¿Comunicación cifrada con ZRTP?
- ¿Funciona con Tor?

Ring

- Basado en el cliente SLFPhone
- Soporta el protocolo SIP
- P2P: no requiere servidor centralizado
- Usuario es un hash de la llave pública de cifrado
- Usa una versión modificada SIP que autentica los usuarios utilizando el protocolo DHT
- https://ring.cx/

Tox

- Similar a Ring, pero es un protocolo P2P
- Funciona con DHT
- Usuario es un hash de la llave pública de cifrado
- Existen varios clientes que soportan el protocolo
- Soporta Tor
- https://tox.chat/

Mumble

- Servidor de voz
- Varias personas se pueden comunicar a la vez
- Funciona con Tor
- Se puede implementar servidor propio, incluso con servicio oculto
- Cifra el canal entre cliente y servidor
- No es cifrado fin a fin