VoIP Security at the Enterprise Edge

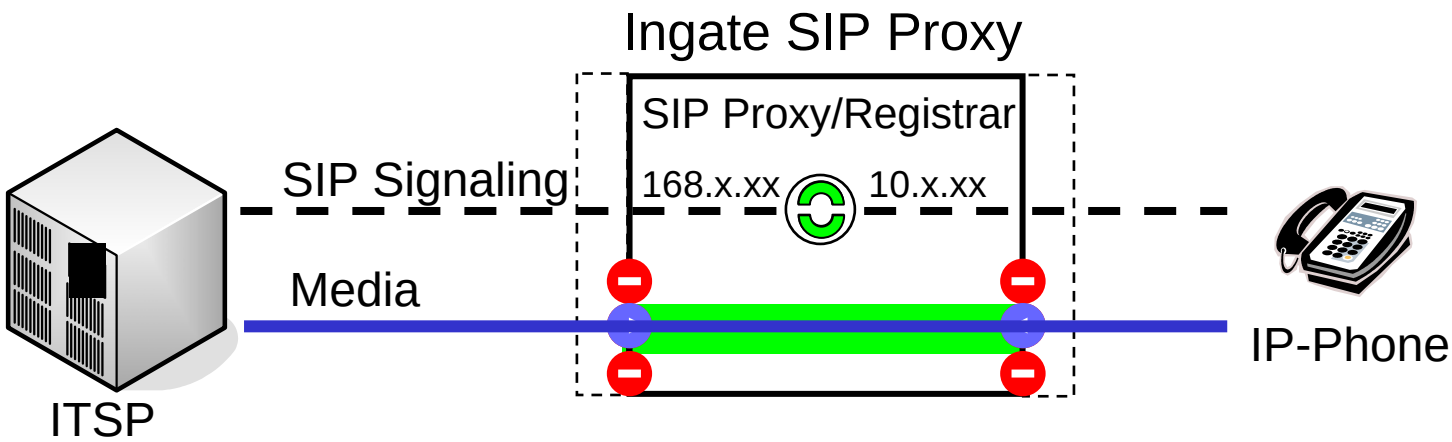
Janne Magnusson, Ingate Systems
mail/sip: janne@ingate.com

VoIP – just another IP application

- VoIP is very similar to e-mail
  - Unencrypted VoIP is just as easy to eavesdrop as unencrypted e-mail (or anything else you do via the network)
- Respect the fact that a new major application are added to our IP networks
  - A new attempting target for hackers with unproven implementations
  - A application with different user expectations
- Good old IP network engineering is the fundament for good VoIP security and reliability
  - Well managed IP network (switches etc)
  - Replace default passwords
  - Disable unused services
  - Well configured firewalls
  - Update software

inGate

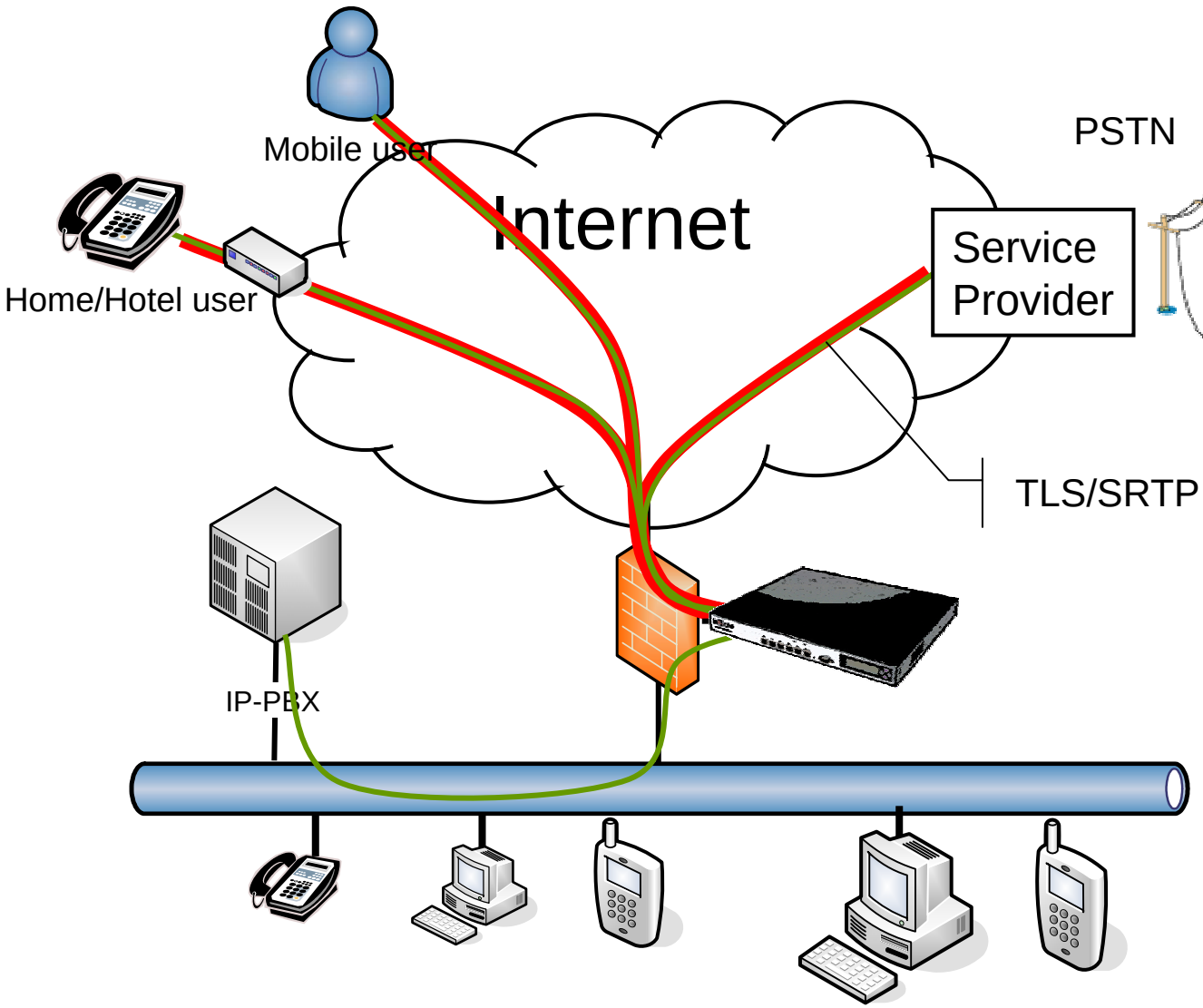
The function of a full featured SIP Proxy



1. Check the SIP signaling, packet inspection
   - Full flexibility to handle future threats
2. Rewrite for the different address spaces
3. Forward the signaling to the correct SIP proxy or client
4. Open ports (UDP/TCP) in the firewall for the media
   - Only for the duration of the call
   - Only between the exact endpoints
5. Media flows through the ports
6. Close ports after the call

inGate

Integrity and Confidentiality on Internet



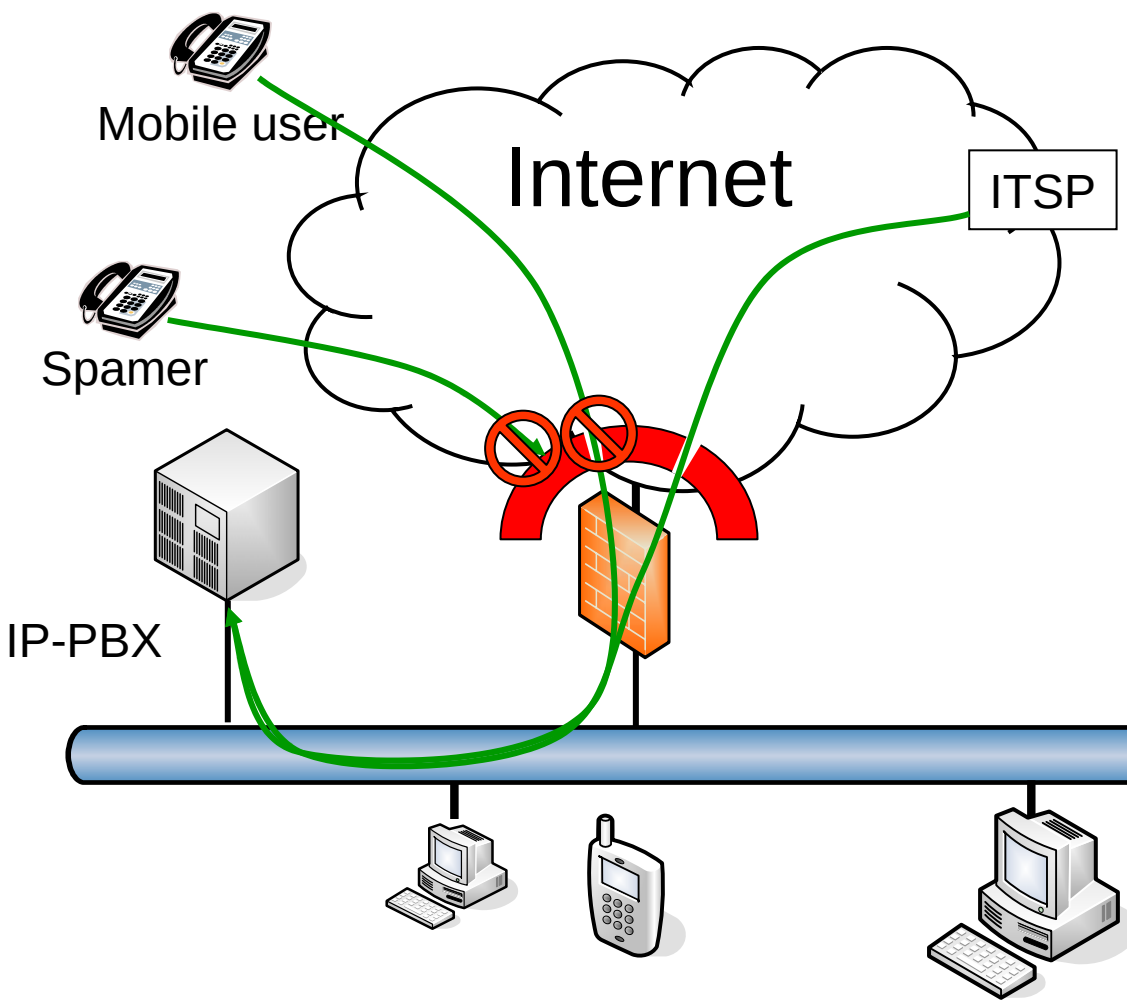
User authentication (HTTP Digest)
– Used

SIP Signaling encryption (TLS)
– Not widely used

RTP Media encryption (SRTP)
– Not widely used

inGate

SPIT, DoS – Filter, IDS/IPS



Dynamically allow authenticated users

Block non authenticated users

Monitor traffic and block end-points with a un-normal behavior

inGate

Common flaws in today's installations

- Connecting the PBX directly to Internet
  - Is the PBX built as a firewall with security as the top priority in all aspects?
  - What happens to the internal phone system during a DoS attack?
- SIP ALGs lack necessary functionality (traditional Firewall with SIP support)
  - Not enough features to handle common phone scenarios like transfers and conferences
  - Cannot do security features like authentication, encryption et.c.
  - Some ALGs allow media from any source IP/port and forwards it into the internal phone
- A Proxy or B2BUA solution is the only sufficient alternative!

inGate

Summary

Problem	Solution
Authentication	- Digest
Integrity/ Confidentiality	- Good network engineering - Encrypted Signaling (TLS) - Encrypted Media (SRTP) - Well managed software
Availability (DoS etc.)	- Good network engineering - Tight SIP firewall configuration - IDS/IPS traffic monitoring

inGate

Thanks

Questions?

mail/sip: janne@ingate.com

inGate