SANOG 25, Kandy, Sri Lanka

Secure Your IP-PBX

- Anowar Hasan Sabir - hsujon@gmail.com
- Sumon Ahmed Sabir - sumon@fiberathome.net
- Simon Sohel Baroi - simon.baroi@fiberathome.net
- Senevi Herath - senevih@learn.ac.lk

Agenda

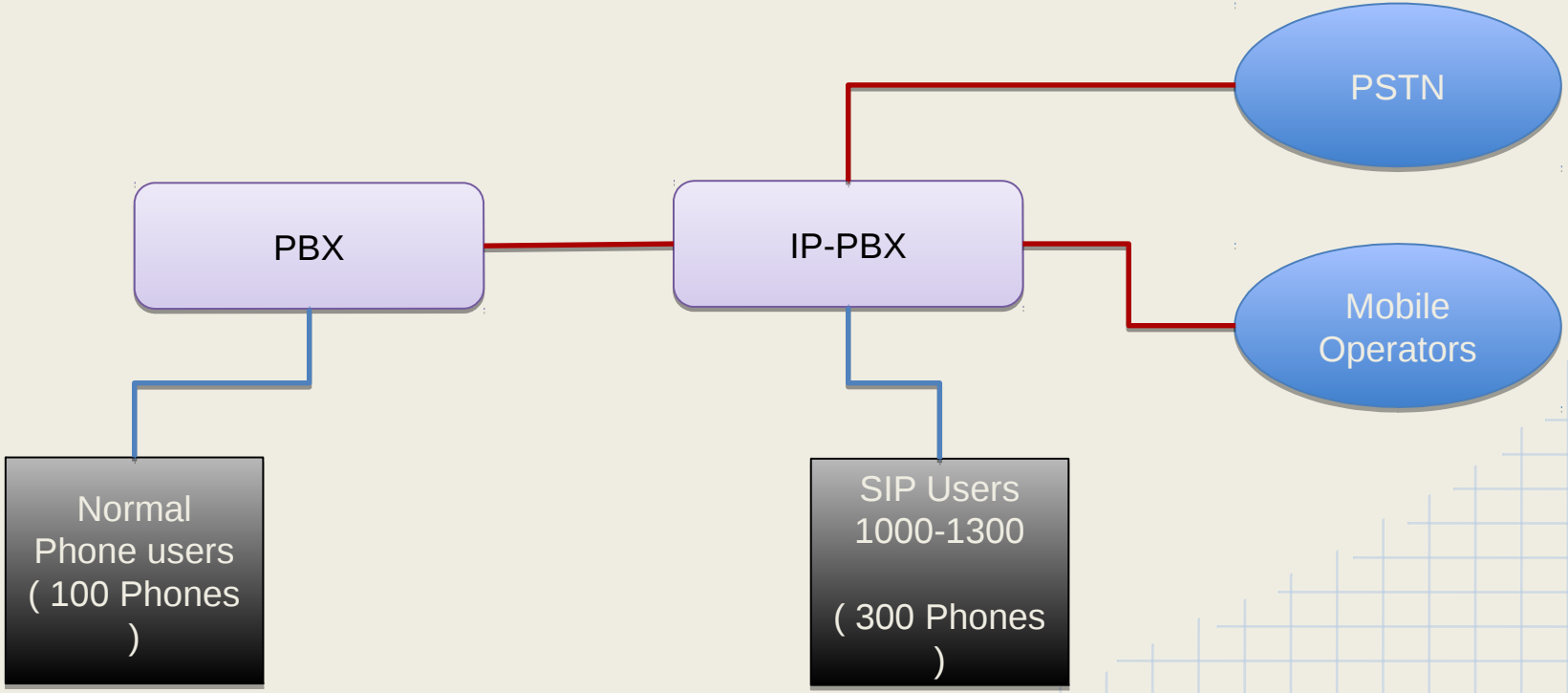
Typical Threats Overview

- Call stealing
- Compromising the server

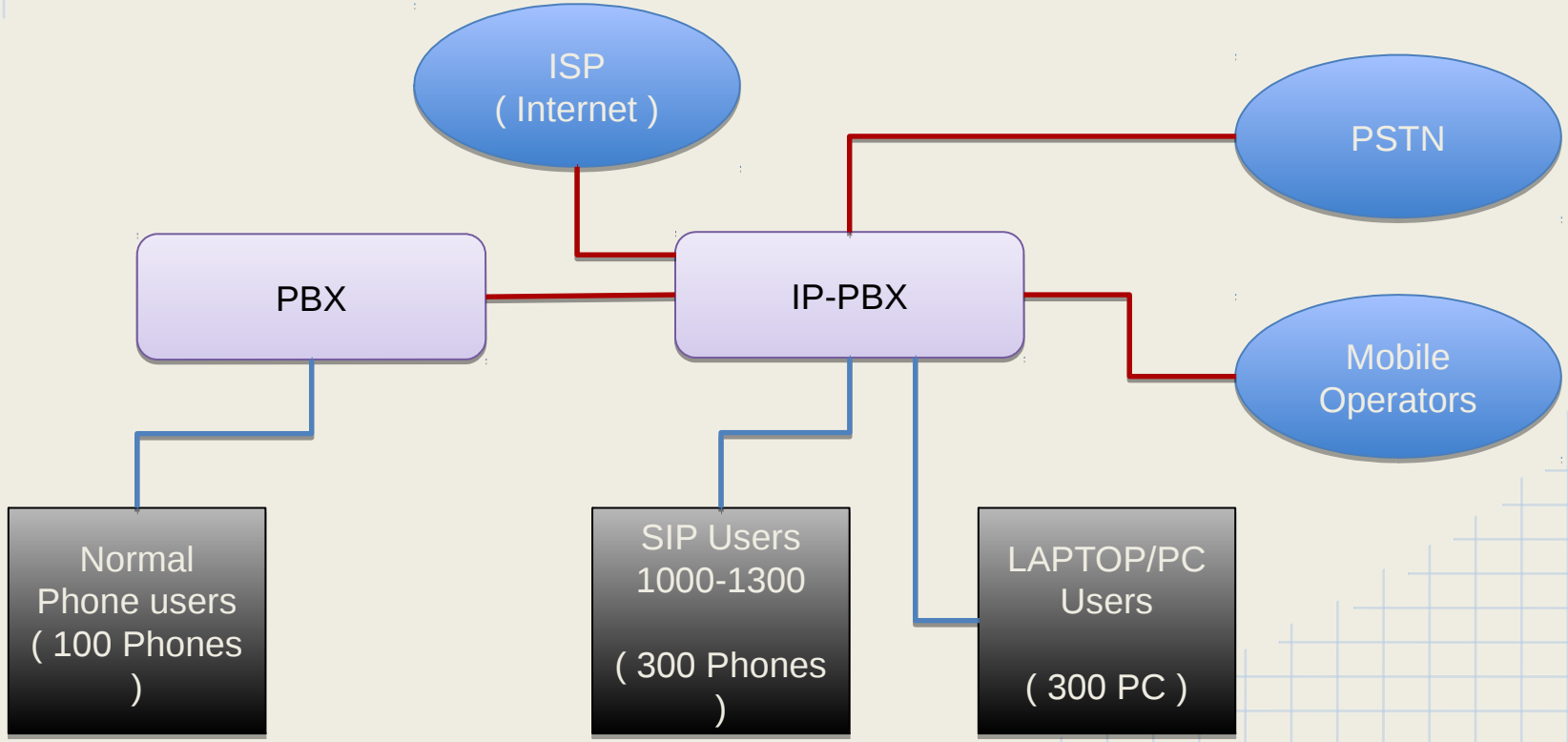
How to Protect the PBX

- SSH communication
- Separating data & voice
- HTTP communication
- Passwords

SIP Connectivity - 1



SIP Connectivity - 2



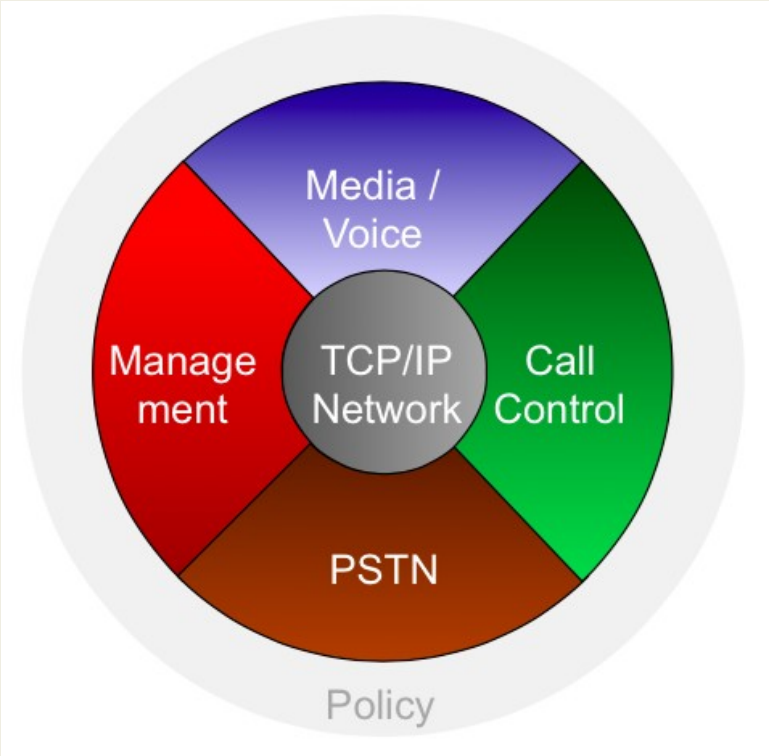
Typical Threats

Stealing of calls via:

- telephony
- VoIP trunks
- SIP
- IAX2

Compromising the Linux server via SSH/HTTP

Security Aspect of IP-PBX



Stealing Calls via Telephony or VoIP Trunks

- Disable the option of uncontrolled trunk-to- trunk calls
- DISA (Direct Inward System Access) - use long passwords and ID System.

Stealing Calls via SIP / IAX2

- Find PBX IP address and port number

Suggested tools:

- nmap (http://nmap.org/)
- svmap (http://code.google.com/p/sipvicious)

```
$ ./svmap.py 192.168.0.1/24
| SIP Device          | User Agent          | Fingerprint                    |
-------------------------------------------------------------------------
| 192.168.0.61:5060   | Asterisk PBX 1.6.2.| Asterisk / Linksys/PAP2T-3.1.|
| 192.168.0.185:5060 | Yealink SIP-T28P 2.| AVM or Speedport               |
| 192.168.0.124:5060 | Grandstream GXP2000| Grandstream phone              |
| 192.168.2.4:5060    | Yealink SIP-T26P 6.| AVM or Speedport               |
| 192.168.0.184:5060 | Yealink SIP-T22P 7.| AVM or Speedport               |
| 192.168.0.134:5060 | YATE/2.2.0          | AVM or Speedport               |
```

Stealing Calls via SIP / IAX2

- Find a PBX extension
  - svwar (http://code.google.com/p/sipvicious)
  - Attacker tries to differentiate between existing/non-existent extensions
  - SIP response to a REGISTER/INVITE/OPTION request analysis could be used for it
  - Asterisk could be configured to send an identical 401 or 407 response regardless of request rejection reason

Stealing Calls via SIP / IAX2

- Find the Password
  - svcrak (http://code.google.com/p/sipvicious)
  - When PBX is attacked there are many warning messages in the Asterisk log:

```
[Jun.. ] NOTICE[30940] chan_sip.c: Registration from '"308" failed
   for '192.168.0.192' - Wrong password
[Jun.. ] NOTICE[30940] chan_sip.c: Registration from '"308" failed
   for '192.168.0.192' - Wrong password
[Jun.. ] NOTICE[30940] chan_sip.c: Registration from '"308" failed
   for '192.168.0.192' - Wrong password
[Jun.. ] NOTICE[30940] chan_sip.c: Registration from '"308" failed
   for '192.168.0.192' - Wrong password
```

Stealing Calls via SIP / IAX2

- The PBX has been conquered
- A malicious user has registered an extension

and makes calls for free

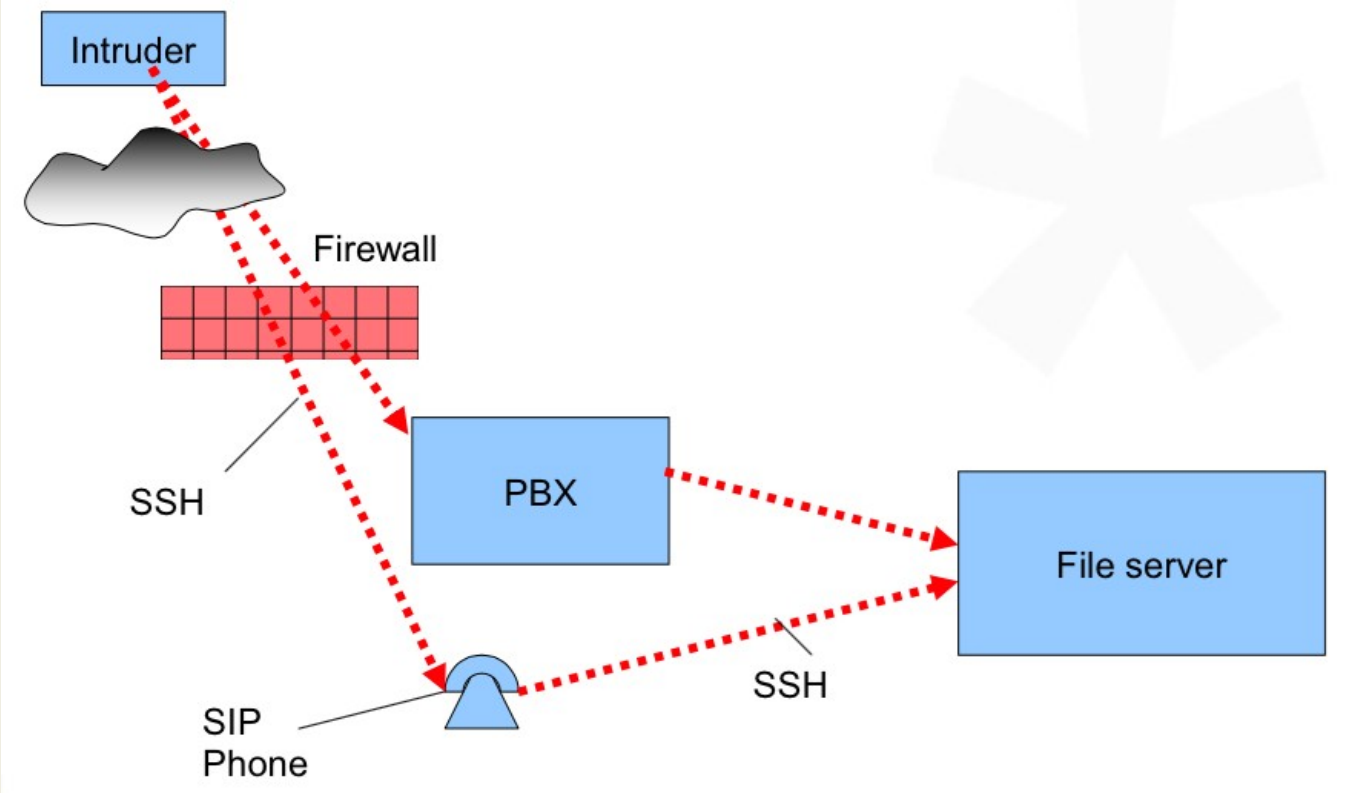
When you will be noticed :

In many cases this will be discovered only when the next telephone bill is received from PSTN or ANS .

Compromising the Linux Server

- An Asterisk server is a regular Linux machine that can also be compromised.
- Malware (viruses, trojan horses etc) may infiltrate via different Linux networking services such as SSH or HTTP.

Attack on Linux Server :



SSH Communication

 Use public/private key authentication instead of password authentication

 Create a user account and disable log in as 'root':

/etc/ssh/sshd_config

PermitRootLogin no

OR PermitRootLogin without-password

- Then it will be possible to connect to the PBX as a non-'root' user, and then become a “super-user”:

SSH Communication

- Restrict the source IP addresses that are allowed to access the server
- Don't use the default SSH port (22/tcp)
- change the listening port in the PBX SSH server configuration:
  /etc/ssh/sshd_config
  #Port 22
  Port 4245

Separating Data and VoIP Networks

- Some customers with higher security requirements separate the VoIP network from the data network
- Dedicated cabling network not required; VLAN technology may be used instead
- Helps prevent company data servers from direct access from potentially vulnerable VoIP devices

HTTP Communication

- Don't expose the PBX Web server to the Internet
- Use SSH tunneling for the PBX Web-based management interface
- Windows users can create SSH tunnels very easily using PuTTY

Passwords

- Don't use the default passwords
- Don't use simple passwords

Passwords

- Don't expose SIP and IAX2 ports unless absolutely necessary
- Use IP restriction for internal VoIP extensions

-> Allows use of weak passwords or no passwords for the internal extensions

- Use strong passwords for remote extensions

Intrusion Detection Options

- It is possible to use a network intrusion detection system
- Fail2Ban (http://www.fail2ban.org)
  -> Scans the log files and updates firewall rules to reject the IP addres
- Snort (http://www.snort.org)
  -> Powerful network intrusion prevention and detection system (IDS/IPS)

Fail2Ban Features

- Log-based brute force blocker
- Runs as daemon
  -> unlike cron-based tools, no delay before taking action
- can use iptables (/etc/hosts.deny)
- can handle more than one service
  (sshd, apache, SIP traffic etc)
- can send e-mail notifications
- can ban IPs either for a limited amount of time or permanently

Summary

Types of threats

- Call stealing
- Intrusion

Best practices

- Protecting the PBX
- Detecting attacks quickly

Thank You