Good Practices for Protection Against PBX Security Threats

While Xorcom, just like any other PBX manufacturer, is not in charge of the client's network or Internet services, we do invest a lot of effort to help prevent fraudulent intrusion into the PBX. For example, our systems include software to detect bad logins. Furthermore, we have compiled the following recommendations below to help system integrators prevent IP-PBX hacking.

1. **SSH (Secure SHell protocol)**

   a. When connecting to the PBX from the Internet, do not use SSH on the default port (22/tcp). There are two ways to set this up:

      i. Set up "port forwarding" on the router.

      ii. Change the SSH port of the PBX by altering the /etc/ssh/sshd_config file.

   b. Use SSH keys (do not type passwords). Keys are harder to crack. As a result, when connecting to a remote site, the connection is established without typing in a password. When connecting from a Windows machine using Putty, please refer to the following link: http://the.earth.li/~sgtatham/putty/0.61/htmldoc/Chapter8.html#pubkey

   c. Restrict SSH to a single IP address, which means connecting the PBX using SSH only from a specific IP address.

   d. If possible, deny root login from SSH.

2. **Web Interface**

   a. Do not expose ports 80/tcp and 443/tcp to the Internet.

   b. If you need access to the Web interface from the public Internet, set up "port forwarding" on the router, or use SSH tunneling.

3. **Passwords**

   a. Modify passwords -- NEVER use default passwords.

   b. Use strong passwords: at least eight characters long, with at least one capital letter and one symbol.

   c. Modify the shell root user login password (use the passwd command).

d. Modify the admin user password in the Elastix Web interface (System->User management->Users).

e. Modify the admin user password of unembedded FreePBX (select “Administrators” and then user 'admin').

f. If you can, type a random string. Here are some examples for generating strong passwords:

```
cat /dev/urandom| tr -dc 'a-zA-Z0-9' | fold -w 10| head -n 4
v1EFZ3T97W
FxgcU8Bkm6
Qo1Y4a7Bvl
ioZbPftWZu

cat /dev/urandom| tr -dc 'a-zA-Z0-9-_!@#$%^&*()_+{}|:<>?='|fold -w 12| head -n 4
@K%2Qk4yM7o9
RMXm+>-j0hc0
?g)+kr$VKB{U
p(yj(NgR?SW7
```

4. SIP Device Protection

a. When configuring local SIP devices try to restrict them to a specific IP address by using the extension permit field in the Elastix Web interface.

b. When configuring a remote SIP device use the secret field in the Elastix Web interface. Please use a strong enough secret.

5. Damage Control Strategy

Do not allow international or other expensive calls for all users. Select only the most common destinations. Spend time in the dial plan to specify the destinations that are really used, on a user-by-user basis.