SiETEC
INTEGRATED BUSINESS COMMUNICATIONS

AUCKLAND | WELLINGTON | CHRISTCHURCH | DUNEDIN

Telephone System Security Guide

Introduction

Toll fraud and Hacking is a multi-dollar business in the USA and the UK and has now arrived in New Zealand. Hackers use various methods to access a PABX, which may be done for many reasons but primarily for obtaining free calls. This inevitably results in very large telephone bills for the hacked company.

What is hacking?

When telephone system hacking began, it was achieved by people who used PC's to break into the voice mail system. Hackers used mailboxes to spread Information, conduct drug sales, post stolen credit numbers or simply to record nasty greetings for callers. Now however hackers use telephone systems to obtain outgoing trunks, they then sell this 'access' to a community of people for dialling expensive international calls. If the incoming trunks are Free-phone numbers the fraudsters enjoy the benefit of completely free calls, with the hacked company paying the bill for both ends of the call.

- Why has hacking now become a problem in New Zealand?
- Hacking has become a serious problem in New Zealand for the following reasons
- The sophistication of telephone systems now available to companies in New Zealand
- Wide use of maintenance modems on telephone systems
- Sophisticated voice mail systems
- Widespread use of the internet which is used for posting hacking information
- Widespread use of modems in New Zealand which has resulted in cheap and user friendly modems being available on the market
- The huge demand for free international calls as overseas nations develop their telephone networks and business requirements
- Customers either ignoring or not being aware of the hacking problem thereby leaving their telephone systems open to fraud
- The widespread use of the free-phone numbers 0500 and 0800
- Direct Inward System Access (DISA).

By far the greatest current problem in New Zealand for PABX owners is toll fraud, a service that has millions of potential "customers".

What can be done to prevent the PABX from being hacked?

Hacker activity may not be completely avoidable but steps can be made to reduce the risks. The principle aim of telephone security is to deter hackers from taking control of a customer's telephone system.

Fraudsters seeking free calls will move on to other PABX's if it takes too long to break into a system.

However, hackers with a personal or political grudge against a company will spend a considerable amount of time in hacking the targeted telephone system, in order to achieve their required objective. This may be:

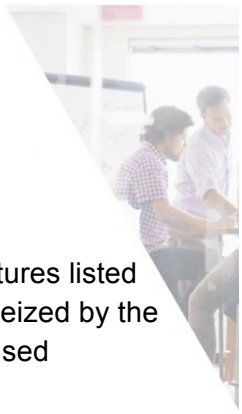
- To obtain free calls
- Crash the telephone system
- Leave abusive messages on the voice mail system.

So the chief objective must be to reduce the risks that expose a telephone system to being successfully hacked.

Risk factors

The principle factors that attract a hacker to a telephone system are:

- Free-phone numbers connected to the telephone system
- Modem access to the telephone system
- Voice mail systems
- Systems with a large amount of trunks/DDI trunks
- Direct Inward System Access (DISA)
- Network ports open to the internet



Once the hacker as ascertained that the targeted telephone system has one or more of the features listed above and there are inadequate counter security measures on the telephone system it will be seized by the hacker. Once seized the systems are reconfigured for fraudulent use. Systems are often not used immediately as the fraudster has to inform their "Customers" of the "toll free access number".

Hacking counter measures

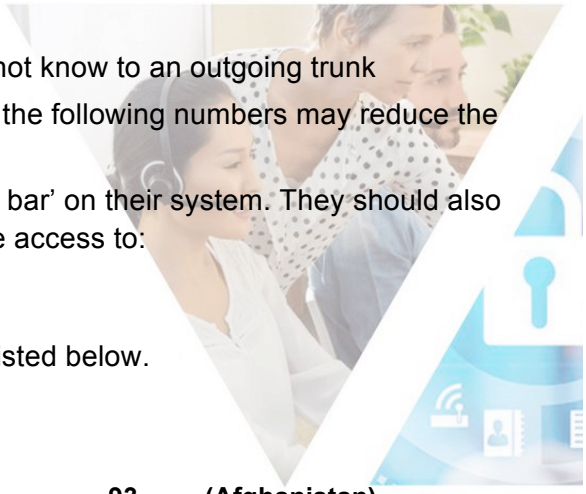
The primary method of preventing fraudulent access to the telephone system is for the customer to educate their staff with regard to telephone security.

Implementing all, or at least some, of the following simple steps can reduce the susceptibility of a system to being hacked.

Customer level measures passwords/codes

- Use random numbers for PINs, which should utilise the maximum number of permissible digits
- Ensure system passwords are not left as default, particularly system administration passwords
- Cancel passwords and security codes of departing employees
- Change passwords and security codes as often as possible
- Do not divulge passwords/codes over the phone

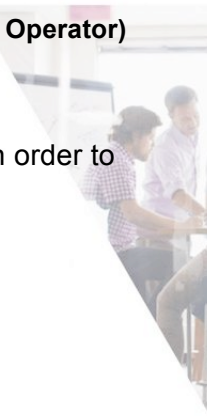
Trunk access



- Educate everyone about not connecting anyone they do not know to an outgoing trunk
- Ensure effective call barring has been carried out barring the following numbers may reduce the possibility of the system being used for fraudulent calls
- The customer should consider ‘call allow’ rather than ‘call bar’ on their system. They should also bar access to countries that they do not require telephone access to:
- Do not allow Voice Mail Systems to have trunk access.

Note: No call barring plan should be limited in respect to the codes listed below.

7	**(CIS - former USSR)**	**38**	**(Slovenia)**	**93**	**(Afghanistan)**
234	**(Nigeria)**	**86**	**(China)**	**96**	**(Middle East)**
1809	**(Jamaica)**	**91**	**(India)**	**0170**	**(International Operator)**
		92	**(Pakistan)**		



However hackers are now even routing their calls via “safe” destinations such as the UK & USA in order to still reach their “pay per minute” services by circumventing these country-specific toll-bars.

System information

Guard information on the telephone system:

- Network service providers’ authorization codes should be kept in a secure location
- Do not write authorization codes in notebooks
- Keep all System Manuals in a secure location and do not write information that may be useful to hackers in these manuals. Cabinets used to store system manuals must be kept locked
- Customers and engineers should dispose of sensitive information securely and not leave information useful to hackers in waste bins.

Equipment room access

Access to the telephone system should be restricted as much as possible. Customers should ask for identification before allowing access to the telephone system. Engineers should record all site visit details in the site logbook.

Monitoring the telephone system

Fraudulent calls and Hacking attempts can be detected if the Call logging Information is reviewed on a daily basis. Immediate correct action should be taken and the Network Service Provider should be informed as soon as possible.

Control Phreak from Callista Group is one product specifically designed to provide real-time protection and management.

Engineering level measures

- Engineers must be security conscious at all times when dealing with a customer's PABX.
- Change the default passwords/Passcodes to new codes when an installation is completed, particularly the engineering Passcodes.
- Destroy any customer code that has been written down before leaving site
- Configure systems in accordance with the equipment security guidance information
- DO NOT enable features on the telephone system that allows ‘Dial Through’
- Unless the customer requests this feature
- Disable any feature on the system which allows or facilitates ‘Dial Through’ applications, unless specifically requested otherwise by the customer
- Advise and configure any PIN digits used by the customer to be the maximum number of permitted digits. These PIN numbers must not include the customer’s STD number or be related to extension numbers
- Hackers are adept at finding the numbers of maintenance modems. If a maintenance modem is used, the allocated extension number should be different for each site.
- Maintenance modems should ideally be configured as dial back modems so that they ring back to the service centre. Under no circumstances should the customer be told the passcode for the maintenance modem
- Keep all documentation up to date, accurate and secure. If a telephone system has been successfully hacked and the perpetrator is found and prosecuted, documents such as site visit log books and configuration manual may be required as evidence in court
- DO NOT leave spare configured Mail box numbers and only configure the minimum amount of spare extension numbers. Ideally there should be no spare extension numbers or mailboxes on the system at all.
- Educate the customer to ask for security pass from engineers requesting access to the switch room. Make sure that the customer is aware of who should be allowed entry to the equipment room and what their security passes would look like.

Maintaining the currency of your Operating Systems and Anti-Virus protection mechanisms

Server and PC operating systems always contain flaws but these get discovered over time and their manufacturers release updates that address those issues. However, if you do not update your Operating Systems then historical vulnerabilities will remain and once hackers come across your business they will mercilessly exploit them, all.

More esoterically but just as importantly you also need to maintain the currency of such parts of your OS as the NTP service. NTP is the Network Time Protocol, it is a relatively obscure protocol that runs over port 123 UDP and is used to sync time between machines on a network. It is not a service that is upgraded often, leaving it vulnerable to reflection attacks.

Attackers take advantage of the monlist command to send a small forged packet that requests a large amount of data be sent to the target IP Address in what is termed an NTP reflection attack.

NTP reflection is a kind of Denial of Service attack and as a DDoS tool monlist enables a small query to redirect megabytes worth of traffic – bringing down the target server or service.

The easiest way to eliminate the threat is to update to NTP version 4.2.7, which removes the monlist command entirely. If upgrading is not an option then you can start the NTP daemon with no query enabled in the NTP conf file. This will disable access to mode 6 and 7 query packets (which includes monlist).

The combined effect of carrying out these countermeasures will reduce the likelihood of a telephone system being hacked.

Not sure? Need help?
Get in contact with Sietec's service-desk
0800-800-989 or service@sietec.co.nz