Hacking

‘Hacking’ is a term which was originally used to describe a method for rapid software engineering, but its meaning has been perverted in recent years to become a label for someone who challenges security measures on computer systems, more often than not with some kind of malicious intent. Traditionally, a hacker was smarter than your average person and often displayed a remarkable aptitude for solving complex mathematics and logic puzzles. The challenge to the hacker was to see if they could outsmart the software engineers who put security measures in place, whether it was to just prove they could do it, or to search for evidence of the existence of UFOs in Government databases for example. Today however, the demographic for the average hacker is in his late teens to early 20’s, and not necessarily a computer or mathematic genius. Spend a few minutes on the internet with a search engine, typing in phrases like ‘hacking tools’ or ‘how to hack …’ and you’ll be presented with a plethora of websites offering community support and training on how to do it, and links to some tools that assist in the efforts. The geniuses are now creating the tools, rather than doing the hacking themselves.

Any computer system is susceptible to a hacking attempt, as long as there is some kind of interface to it. Trying to access a workmates PC by guessing their password when they leave the desk for lunch is a form of hacking just as much as someone trying to gain access to bank accounts over the internet. There is nothing we can do to stop this kind of behaviour; all we can do is protect ourselves as best we can from it. We have known for years that if you connect a PC to the internet, with no form of protection, it will be just a matter of minutes before someone around the world has detected it and started to attempt to gain access or control of it in some way. Connecting an under protected computerized telephony system to the internet is no different.

VoIP Hacking, as it has become known, is the practice of attempting to gain access and control over a computerised telephony system (IP-PBX). When successful, the potential damages caused can run into many thousands of pounds. Again, spending just a few minutes on a search engine, will return results for tools like ‘SIP Vicious’ or similar. These are tools specifically designed to attack IP-PBX systems and once they have gained access, the common scenario is that they are then programmed to dial premium rate phone numbers over the SIP channels and rack up many thousands of pounds worth of phone calls. Often, the premium rate numbers being dialled are in international destinations, and to countries where it is hard to trace or prosecute. Even if you did trace the destination number, they themselves haven’t done anything illegal. All they have done is provide some sort of premium rate telephony service. The only people that ‘benefit’ from this fraudulent activity are the owners of these premium rate services who are claiming the money from the various operators, so the cynical mind might suspect that they are also somehow behind the hacking too and are generating calls to themselves, but authorities have a hard time proving that.

There is a simpler form of VoIP Hacking too where by all the hacker needs to do is determine the username and password for the SIP account itself. Once they have the username and password from the account, they can generate the calls from anywhere in the world. The fraudulent calls wouldn’t necessarily have to come from the actual IP-PBX. This type of fraud is much like credit card cloning, but is much harder to detect. After all, a credit card can’t physically be in 2 places at once, so the

banks can detect suspicious use easily. On the other hand SIP Registrar services are designed so that several people can use the same account, from geographically separate places, so detecting this type of misuse is difficult until the damage has already been done.

Gamma has a fraud detection mechanism in place to detect suspicious activity on the account and block it, but obviously from a customer perspective, the damage has already been done. Gamma can only limit the damage, we can't stop it completely. To fully protect yourself from potential fraudulent activity on your SIP account, you must take steps also. There are several type of hack 'attack' depending on the tools being used to launch the attack, and how your IP-PBX will behave during an attack is individual to each implementation. Some symptoms of an attack in progress are but not limited to:

- Phantom Calls from a strange or unknown number.
- Difficult in making or receiving calls over the SIP trunks.
- If you use the same connection to the internet for your data services, you may notice a significant decrease in the speed of your connection.

These are symptoms of an attack. The hacker has detected that the port being used for SIP signalling (usually UDP 5060), is responding to them, and they are sending SIP traffic to the phone system. Perhaps sending many thousands of calls to it in a short period in an attempt to make it crash or exploit a bug in software that appears when the system is under heavy load. If they succeed in this part of the attack, then they may then be able to gain access to the phone system itself to program it to make unauthorized calls, or acquire the authentication details used for the SIP service being used. They may however not be able to do that, and by just sending you literally thousands of calls per minute, they are causing a nuisance and preventing real calls from getting through to you. This is called a 'Denial of Service' attack.

So what can I do to protect myself from an attack?

Simple – Use a firewall!

Most, if not all broadband routers, come with a built in firewall. You just to make sure it is properly configured from the moment you go online. If the hacker doesn't know you are there, then he can't attack you. This is all well and good for normal internet usage, but for SIP services, you have to

make ‘hole’ in the firewall to allow incoming calls, and it is this hole that the hackers will look for and target. So how can you protect yourself? The answer is you only make the ‘hole’ visible to Gamma, and no one else.

When your SIP account is built, an email detailing the IP address to be used to send your SIP traffic to is sent to you. For best practices, you should configure your firewall such that it will only allow traffic from the outside world through the SIP port (UDP 5060), when it has come from the IP address detailed. Depending on the service you have with Gamma, the IP address will be different, but you can contact the Service Desk to confirm which IP address we will be sending the traffic from (this information is in your confirmation email as well). On Gamma’s Assured Broadband service, we setup and manage the firewall for you, so you don’t need to worry about it, and as long as you stick to our best practices regarding security and port forwarding, you will remain protected.

What if it’s too late and I’m already under attack?

If you suspect someone is trying to attack you, but hasn’t yet succeeded, improve your firewall rules as mentioned above. If possible, capture a sample of the suspicious traffic using SIP logs on the IP-PBX if available, or by sampling some of the network traffic between your router/firewall and the

IP-PBX using network packet capture tool like Wireshark. This can be extremely useful in identifying the source of the traffic, which might not turn out to be a hacker at all. In either case, it will help identify the cause and Gamma can then advise on how best to proceed.

If you suspect you have already been compromised, alert Gamma immediately so we can block your outgoing traffic and limit the damage. It’s highly likely that Gamma have alerted you by detecting an unusually high spend on your account, and will have put measures in place already to limit the financial damages. On IP Authenticated SIP trunks, take measures to improve or replace your firewall to stop the attack. Speak to your ISP to get a new IP address, which will be unknown to the hacker, and make sure the toughened firewall rules are place before you start using this new address, so that they don’t then start to attack that instead. Make sure the firmware in your router/firewall and phone system is up to date as many of the exploits used by hackers are identified and patched periodically.