Spotlight

Smartphone and mobile (cell) phone security

the new security frontier

A Spotlight Paper by Bloor Research
Author : Nigel Stanley
Publish date : July 2011

The rise of the smartphone over the past few years has been a technology success story ...only now are we seeing products and services designed to improve smartphone security.

Nigel Stanley

Executive summary

If you stop and take a look at all the objects that sit within an arms length of where you are sitting the chances are that a cell phone, in all its guises, is one of the first that you see. The reality is that the cell phone is the first piece of IT that we take with us wherever and whenever we go. If we forget our cell phones we feel naked, isolated and more than a little bit worried. Whilst few would take a fully-fledged PC to bed, the cell phone has pride of place next to the bedside lamp.

From an information security perspective this poses an interesting challenge.

Quite simply, if you can compromise a cell phone then you are more or less assured that you can collect the most relevant, current and possibly damaging data possible. The breadth and depth of current cell phone technology is staggering, with new models, features and innovations delivered weekly. Whilst few would doubt the huge appeal of interactive applications, the challenge these devices give information security professionals is overwhelming. After all, we now have presidents and prime ministers touting these devices as part of their need to be in touch. No doubt this appeals to a deep-seated and basic human need to be part of something at all times.

Aside from the risk of losing emails and SMS messages, few have considered that voice data is similarly at risk from being compromised. This risk is now a reality and we need to be considering how we deal with it sooner rather than later.

The problem—have the phone, have the man

Consider these scenarios:

- Bob is attending a major trade show where the brightest and the best in his industry are negotiating deals worth millions. Bob has a meeting planned with a potential client to discuss pricing options. Eve works for a competitor. She pays a third party to install spyware on Bob's cell phone, turning it into a listening device. Eve listens into the negotiations and meets the potential client later that day with a bid that mysteriously undercuts Bobs by 1%. Eve wins the business.

- A CEO staying in a hotel room needs to take part in a conference call discussing end of year financial data, prior to a big announcement to the stock market. Fraudsters set up a fake cell phone base station and intercept the conversation, getting advanced notice on likely stock movements.

- A foreign government is keen to acquire as much hi-tech intellectual property as it can. It has targeted one company in particular that sells advanced missile systems and has information that a senior engineer from that company will be staying in a downtown hotel one weekend. Following a covert operation, it was established that the engineer used a specific handset and Bluetooth headset. This data was fed back to intercept technicians who were able to remotely monitor the engineer's conversations, having hacked the Bluetooth headset.

The reality is that those after your data will target the weakest link, and the prevalence of cell phones is making them a top target

For many people these targeted attacks would seem extreme and not something they should be bothered about. The reality is that those after your data will target the weakest link, and the prevalence of cell phones is making them a top target.

The cost to business of lost voice data

If you lose a laptop, USB stick or CD it can be fairly obvious that the data has gone missing. Voice data is very different, as a successful interception can leave no physical trace so there is little chance of realising your data has actually been intercepted until it is too late. For many, this realisation may be when they have been undercut by a competitor or see their products copied in another country. This makes the promotion of voice security more of a challenge, as a direct link to an incident is often difficult to make.

Of course this lack of detection and traceability is a real bonus for the eavesdropper. When a victim realises the loss of data the attacker is long gone, hiding their trail as they go.

> *When a victim realises the loss of data the attacker is long gone, hiding their trail as they go*

In order to understand the cost of lost voice data the Ponemon Institute [1], in collaboration with Cellcrypt [2], recently undertook a study called The Security of Voice Data [3].

The study reveals that 67% of those 75 organisations surveyed were not confident that the information passed during a cell phone conversation was adequately secured and only 14% use technologies to secure cell phone calls when travelling to sensitive areas. The cost to the organisation each time a corporate secret is revealed to competitors or their agents has been averaged at $1.3 million.

Introduction to cell phone technologies

Before attacks on cell phones can be discussed it is important that the underlying system employed by cell phone providers is understood.

There are a number of digital networks worldwide that support cell phones, of which Global System for Mobile Communications (GSM) is the most popular. GSM accounts for around 80% of worldwide networks with over 3 billion users across over 200 countries, and its ubiquity enables ease of roaming between providers for users that are travelling. cdmaOne (2G) and CDMA2000 (3G), often referred to colloquially as CDMA, are two other competing standards to GSM. Confusingly, CDMA is an acronym for code division multiple access, which is a channel access method used by these systems.

Cell phone networks have also evolved through a number of generations. 1G phones were analogue cellular networks, which were replaced by 2G networks that use digital technology. 2.5G is now the baseline standard and enables data support to be added to 2G services. 3G networks are increasing in number with an associated increase in available bandwidth and support for more enhanced services. GSM uses a technique called TDMA or Time Division Multiple Access to share a single carrier frequency between multiple users, all taking turns to use their allocated slice of the channel. This time slicing happens fast enough so that users aren't aware of sharing the channel with others.

Aside from voice traffic, cell phones have evolved to enable data transfer as an additional service. New protocols have been developed in support of this including General Packet Radio Service (GPRS), which is a packet switching protocol used across GSM networks for data transmission. Enhanced Data rates for GSM Evolution (EDGE) is a development of GPRS that provides even greater data transmission rates.

Cell phone networks typically consist of a number of elements:

- Cell phone handset which acts as a transceiver.

- Removable subscriber identity module, or SIM card. Combined with a cell phone this is referred to as the mobile station.

- The International Mobile Subscriber Identity (IMSI) is a unique number stored inside the SIM and sent to the network by the phone. To reduce the opportunities to compromise a cell phone via the air interface a Temporary Mobile Subscriber Identity (TMSI) number is assigned by the network once the original IMSI has been processed.

- The International Mobile Equipment Identity (IMEI) is a unique number used to identify a particular handset to a network, a feature that is used to "bar" stolen phones from accessing a particular network.

- Base Transceiver Station (BTS), which receives and transmits the phone signal. Importantly, it is also responsible for encrypting and decrypting call traffic with the base station controller.

- Base Station Controller (BSC) coordinates a number of base transceiver stations and manages the allocation of call channels and the important task of handing off calls between BTSs. Combined with a BTS this is referred to as the Base Station Subsystem (BSS).

- Mobile Switching Centre (MSC) is part of the network switching subsystem (NSS) and manages the routing of calls, setting up end-to-end connections, hand over requirements and account monitoring. The NSS is also responsible for managing the Home Location Register, Visitor Location Register (which are databases containing the details of authorised users of the GSM network) and the Authentication Centre that authenticates each SIM card trying to connect to the network.

Understanding GSM encryption

The design of cell phone systems originates from before direct attacks were considered. The move from an analogue to a digital system was believed to add sufficient security and network providers had historically been more concerned with tracking call fraud rather than dealing with eavesdroppers.

Early analogue cell phones were basically simple radio systems that had no in-built security features and were subsequently open for anyone to listen into with simple radio equipment. As technology advanced users quite rightly demanded better security, and in

Introduction to cell phone technologies

1987 a stream cipher called A5/1 was developed for that purpose. A5/2 was developed in 1989 as a weakened version of the cipher for export to less trusted regions of the world.

The algorithm behind A5/1 was originally kept secret, an approach that modern cryptographers quite rightly deride as foolishness. It is only by opening up algorithms to analysis and in-depth review that the security community can gain confidence in the robustness of these tools. Security by obscurity, in the case of cryptographic algorithms, is a flawed approach. Suffice to say that by 1994 the algorithm had been more or less worked out and by 1999 it had been successfully reverse engineered.

Academic hacks against A5/1 have in the past relied upon knowing some plain text—perhaps a couple of seconds of a conversation—to get to the encryption key. In reality this won't happen, as conversations would be encrypted from the start so, unless there was a flaw in the system that provided such a snapshot, this academic hack is not possible. Other hacks have relied on significant computing power, costing around $100,000, but even with such processing power the system could only decrypt around 1 SMS text message a day.

A5/1 itself is vulnerable to generic pre-computation attacks in the form of a code book attack. For ciphers with small keys code books allow decryption to take place—facilitated by the fact that a code book provides a mapping from a known plain text output to a cipher text. An A5/1 code book is 128 Petabytes and will take about 100,000 years to compute on a desktop PC. More sophisticated attacks have been shown (Karsten Nohl, Aug 2009) using rainbow tables (look up tables of plain text hashes) of about 3TB with decryption times in a matter of minutes.

A5/3 is a stronger encryption algorithm designed for use in 3G systems. This is not always implemented by service providers and a vulnerability for this was demonstrated in early 2010. In this case it took 2 hours to conduct a related key attack on A5/3 data but, as this attack relies on a large volume of plain text to be successful, it remains an academic attack at the moment.

Cell phone attacks

There are a number of ways in which cell phone voice data can be intercepted:

- Spyware can be loaded onto a phone. This in turn can activate the phone as a bugging device with full remote control available to an eavesdropper. Advanced spyware has a number of features, including voice-activated microphones to save on battery life and the ability to auto forward SMS messages and the contact list on a phone.

- GSM encryption can be hacked. A number of attacks have been demonstrated and, in theory, given suitable resources, cell phone encryption could be compromised. This is a passive attack and is undetectable as the signals are received using a specialised radio, which is both portable and easy to hide.

- Cell phone "capture". This attack exploits a couple of design weaknesses found within GSM cell phones. The first is that, whilst a cell phone needs to authenticate itself to a network, the network itself is not authenticated by the cell phone. Couple this with the design requirement for cell phones to connect to the most local base station, based on signal strength, a fake base station can be setup and all local call traffic captured. As cell phone calls are only encrypted from the phone to the base station a fake base station will be able to process calls "in the clear". This is called an active attack and, whilst it may appear complicated, a number of commercial products are available to authorised agencies and government departments. In early 2010 active attacks were demonstrated using hardware and software that can be purchased for around $1000, less than 1% of commercially available solutions [4]. The widespread availability of home base stations, such as Vodafone SureSignal, has provided a source of equipment that could be adapted for this type of intercept. In reality this attack does have limitations. As the cell phone is using a fake base station it is not registered with the cell phone network, so any incoming calls will be diverted to voice mail or receive a "cell phone unavailable" message. More sophisticated versions of this attack provide two connections—one to the compromised phone and one to the network base station. Using this man-in-the-middle approach the cell phone is able to connect to the authentic network, albeit via a fake base station that will intercept the traffic, so "normal" two-way calls can be initiated whilst the call and data flow is being monitored. 3G phones utilise mutual authentication between the phone and the network so aspects of these attacks will no longer be valid when networks are exclusively 3G and above. Until then the sharing of GSM and 3G systems in support of broader network coverage can still see 3G phones subject to compromise using this approach.

- Inside threat. Threats to information security systems often emanate from inside an organisation. These can take the form of knowledgeable insiders being bribed or bullied into supplying relevant cell phone data and can even be an employee planted by a security agency. In June 2010, a technician who worked in a Lebanese cell phone operator was arrested for being an Israeli spy and giving access to phone calls for 14 years. Because of the man's role on the technical side of the cell phone network's operations, it was assumed that the entire national network had been compromised.[5]

Preventative measures

The good news is that there are some steps you can take to help protect your phone:

- Most obviously keep your phone with you at all times, and don't be fooled into allowing someone else to use it. It can take a matter of seconds for a hacker to compromise your phone by switching out a SIM card or downloading an application. Consider using a PIN to prevent unauthorised access, but make sure you change it from the default setting and guard it as you would a banking PIN.

- Be aware of your environment when using a cell phone. Despite all the hi-tech ways in which a phone can be compromised simply eavesdropping into a conversation remains the most common way of obtaining information. Consider techniques such as hiding your lips to prevent lip reading if you are particularly concerned.

- 3G networks may provide a better level of security than 2G if they implement A5/3 encryption, but be aware that a 3G network may degrade calls to 2G in areas without you realising. Some targeted attacks will deliberately downgrade a 3G cell phone connection to an easier-to-attack 2G connection without the user realising it. Consider the country that you are calling from and

Cell phone attacks

remember that there may be different attitudes to privacy and confidentiality than in your home country. It has been reported that some countries record all phone calls as a matter of policy, so this is especially important when you know that you are dealing with sensitive commercial, political or industrial intellectual property in these areas.

- Watch out for malware. This may take the form of applications, SMS messages, service messages or email attachments in smart phones. A seemingly innocent game or applet could easily be a piece of Trojan software, carrying a phone bugging application. An unguarded Bluetooth connection can also be a route into your phone, so switch it off if you are at all concerned. A number of vendors are starting to provide anti-malware for mobile and smart phones, which may help.

- If you are concerned that your phone has been compromised turn it off and remove the battery. It is possible to have your phone examined by a forensic expert but it may be cheaper and quicker to remove your SIM card and get a new phone. Remember to back up your phone contacts to another device so that you can quickly copy them to any new phone.

- Don't leave voicemail as these systems can be targeted by interceptors. If you do need to use voicemail, ensure that your PIN is changed from the default, as voicemails can be accessed from any phone. Deleting messages after you have received them is good practice.

Voice call encryption—a Gold Standard solution?

It has been possible to scramble telephone calls since the early 1920's. Originally artificial noise was superimposed over a voice call to prevent eavesdroppers, with a suitably equipped receiver duplicating the noise on the signal enabling it to be cancelled out. Technology advanced during the Second World War, enabling secure communications in support of the war effort. The 1980's saw the availability of STU-III telephones that have been in regular use for secure communications up until the recent move to VoIP on secure government networks.

Possibly the best way of protecting your cell phone voice traffic is to have in place end-to-end encryption. This is a modern version of telephone scrambling but today's encryption technology bears no relationship to the cruder systems used in the past. Voice encryption vendors tend to take one of two routes—supplying especially designed and configured cell phones or providing software that can be downloaded onto the customer's phone of choice, assuming that it is supported. Some vendor gateway products enable calls to be routed to standard office phones and the general phone network and still remain encrypted.

The level of encryption provided by vendors is usually very high, relying on well-known and trusted algorithms that have stood the test of time and attention from mathematicians and cryptanalysts. Key sizes are normally 256-bit for call data with some systems using a 4096-bit Diffie–Hellman shared secret exchange to establish the session keys. In some systems a private key will be generated on the cell phone when the system is installed, which is then guaranteed to be unique and exist only on that device. This key value can be derived using a seed based on a random number produced by processing audio data from the cell phone microphone. An associated public key will also be created. Other systems use a new key which is generated for each call with authentication carried out by hash-based readouts.

A phone book of trusted cell phone numbers is then built along with their associated public keys. At the beginning of a phone call a unique session key is generated between the parties that only lasts as long as the call, and is then destroyed. Users will see a graphical display informing them of the status of the encrypted call, an important way of assuring them that their call is secure.

Criticism has been levelled at some cell phone encryption systems that they introduce delay, echo or some other quality of service issue. Whilst it would be expected that some delay would occur due to the encryption/decryption process a call quality similar to that found on an international landline is the norm.

In conclusion

There is no doubt that voice data is at risk. As more and more people use their smart cell phones to run their entire lives, hackers and others will focus their efforts on getting the information they need from these devices. In many respects attitudes towards cell phone data security reflect those held 20 years ago towards the humble personal computer. Back then attacks were minimal, anti-malware was yet to become established and hacking was in its infancy. Now we are in a maelstrom of attacks against the PC using sophistication and scale we previously thought impossible.

Cast one's mind forward 20 years and it boggles at the depth and breadth of attacks our cell phones will be subject to. In the meantime anyone that conducts sensitive business using a cell phone should seriously consider implementing the preventative measures discussed in this paper alongside an industry leading cell phone encryption package without delay.

Cast one's mind forward 20 years and it boggles at the depth and breadth of attacks our cell phones will be subject to

References

1. http://www.ponemon.org/index.php

2. http://www.cellcrypt.com/

3. http://www.cellcrypt.com/voice_data_study_2010.html

4. http://www.computerweekly.com/blogs/Bloor-on-IT-security/2010/04/mobile-phone-hacking-for-1000.html

5. http://www.cellular-news.com/story/44043.php

Further Information

Further information about this subject is available from
http://www.BloorResearch.com/update/2043

Bloor Research overview

Bloor Research is one of Europe's leading IT research, analysis and consultancy organisations. We explain how to bring greater Agility to corporate IT systems through the effective governance, management and leverage of Information. We have built a reputation for 'telling the right story' with independent, intelligent, well-articulated communications content and publications on all aspects of the ICT industry. We believe the objective of telling the right story is to:

- Describe the technology in context to its business value and the other systems and processes it interacts with.
- Understand how new and innovative technologies fit in with existing ICT investments.
- Look at the whole market and explain all the solutions available and how they can be more effectively evaluated.
- Filter "noise" and make it easier to find the additional information or news that supports both investment and implementation.
- Ensure all our content is available through the most appropriate channel.

Founded in 1989, we have spent over two decades distributing research and analysis to IT user and vendor organisations throughout the world via online subscriptions, tailored research services, events and consultancy projects. We are committed to turning our knowledge into business value for you.

About the author

Nigel Stanley

Practice Leader—Security

Nigel Stanley is a specialist in business technology and IT security and now heads up Bloor's IT Security practice.

IT security comprehensively covers the whole remit of protecting and defending business or organisational systems and data from unwelcome attacks or intrusions. This large area includes protection from the outer edges of the security domain such as handheld devices through to the network perimeter, inside threats and local defences. It looks at the ever-growing threats, many of them new and innovative. It includes use of firewalls, data loss prevention, data encryption, anti-malware, database protection, identity management, intrusion detection/prevention, content management/filtering and security policies and standards.

For a number of years Nigel was technical director of a leading UK Microsoft partner where he led a team of consultants and engineers providing secure business IT solutions. This included data warehouses, client server applications and intelligent web based solutions. Many of these solutions required additional security due to their sensitive nature. From 1995 until 2003 Nigel was a Microsoft regional director, an advisory role to Microsoft Corporation in Redmond, which was in recognition of his expertise in Microsoft technologies and software development tools.

Nigel had previously worked for Microsoft as a systems engineer and product manager specialising in databases and developer technologies. He was active throughout Europe as a leading expert on database design and implementation.

He has written three books on database and development technologies including Microsoft .NET. He is working on a number of business-led IT assignments and is a principal consultant with Incoming Thought Limited, a partner company to Bloor Research that specialises in security consultancy and education.

Nigel is a member of the Institution of Engineering and Technology, the British Computer Society and the Institute of Directors.

Copyright & disclaimer

Due to the nature of this material, numerous hardware and software products have been mentioned by name. In the majority, if not all, of the cases, these product names are claimed as trademarks by the companies that manufacture the products. It is not Bloor Research's intent to claim these names or trademarks as our own. Likewise, company logos, graphics or screen shots have been reproduced with the consent of the owner and are subject to that owner's copyright.

Whilst every care has been taken in the preparation of this document to ensure that the information is correct, the publishers cannot accept responsibility for any errors or omissions.

2nd Floor,
145–157 St John Street
LONDON,
EC1V 4PY, United Kingdom

Tel: +44 (0)207 043 9750
Fax: +44 (0)207 043 9748
Web: www.BloorResearch.com
email: info@BloorResearch.com