Author(s): Jahankhani, Hamid; Meal, Richard G.
Article title: Emerging Risks and Criminal Investigation of 3G “Smart Phones”
Year of publication: 2006
Citation: Jahankhani, H; Meal, R.G. (2006) ‘Emerging Risks and Criminal Investigation of 3G “Smart Phones”’ Proceedings of the AC&T, pp.35-41.
Link to published version:
http://www.uel.ac.uk/act/proceedings/documents/ACT06Proceeding.pdf

EMERGING RISKS AND CRIMINAL INVESTIGATION OF 3G "SMART PHONES"

Hamid Jahankhani*, Richard G. Meal**
*Innovative Informatics Research Group
hamid.jahankhani@uel.ac.uk
**Ex-Royal Air Force Police, currently security specialist at Echelon

Abstract: The ever increasing use of the mobile devises in particular smart phones means a new concern for security threats. Smart phone capabilities are because of Enhanced Data Rates for Global Evolution (EDGE) platform which delivers up to 7 times faster than a normal 56K Modem. The capability of 3G mobile telephone devices makes their use of value to the criminal community as a data terminal in the facilitation of organised crime or terrorism. The effective targeting of these devices from criminal and security intelligence perspectives and subsequent detailed forensic examination of the targeted device will significantly enhance the evidence available to the law enforcement community. This Paper is a technical overview of the structure and capability of the 3G networks and how the network services may be exploited by a criminal or (organised) group of criminals.

1. Introduction

Since time immemorial criminal activity has by its very nature drawn together the perpetrators of crime, who have associated together. Historically this activity led to an underclass, which in the United Kingdom was countered in Sir Robert Peels' principles of early policing. The myth that such criminals became as underclass has long since been denuded, but the very need for the police themselves to communicate to fight crime in an organised manner has been in itself a model for the criminal mind. The original London "peeler's" communicated by means of a whistle; in the centuries that followed the advent of the telephone was to provide the police of the day with a distributed network of communications posts as evidenced by the police boxes which were installed throughout the major cities in the United Kingdom during the Edwardian times. The means to communicate provides both the law enforcer and the criminal with the ability to direct resources and share information within their communities, in order to maximise their operating efficiency, flexibility and speed of response. While the means are identical the ends are clearly not, but it is therefore no surprise that the criminal elements have used communications to further their aims.

Mobile phones, like any other item of communications equipment or consumer electronics, have developed exponentially in capability with each successive model. Yet while in 2005 the handsets seem to be developing with a bias toward entertainment, it is perhaps worthy of note to consider the difference in functionality between a GSM device and a 3G device. While much of the enhanced 3G services are a product of the host network and service provider, the handsets themselves have become so sophisticated that they are data terminals in their own right with computing power that exceeds the early 8086 and 286 processor PCs.

While the functionality in itself is unlikely to draw the criminal mind into procuring a 3G handset, network launch promotions make subscription to their services most attractive. Indeed, within the youth community (where there is little brand loyalty) it is claimed, (Three, 2005) that, within the UK the fastest growth of users has been to two service providers that require no formal registration of their "pay as you go" services, thereby guaranteeing the anonymity of the initial purchaser and subsequent user(s).

The criminal now has the opportunity to obtain a largely untraceable phone (BBC, 2005).

Given the number of mobile phones within the UK and their acceptance as a means of communication within any social grouping, it is clear that their use by the criminal fraternity is a given. This, therefore provides further avenue for inquiry during the course of any criminal (or indeed intelligence) investigation. The phone is therefore likely to be a witness to crime in itself. Besides physical evidence (prints, fibres and DNA) the digital evidence contained within the phone and networks are significant.

Clearly, the weight of evidence provided by a mobile phone varies according to the type of device, protocols, network used and circumstances of use and recovery. However, in order to fully understand the nature of evidence available, particularly within the more advanced 3G arena, it is important to understand how such a system works.

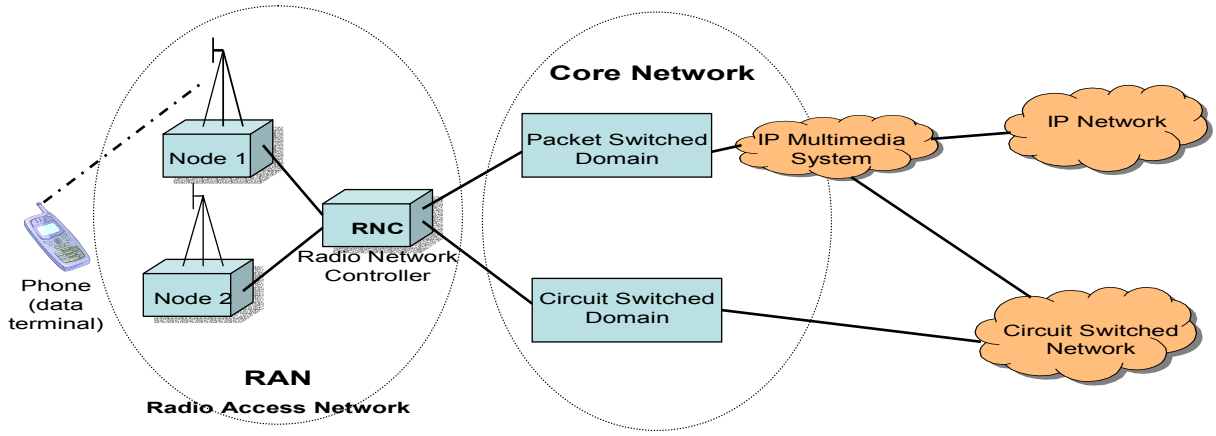
2. 3G Network Architecture

The 3G Universal Mobile Telecommunications System (UMTS) provides a significant enhancement in communications capability. As a third generation service it therefore represents the evolution of 2G GSM services and incorporates a series of significant enhancements over GSM. 3G is marketed as an integrated mobile voice and data systems with wide area (future global?) coverage in many countries. Indeed at the time of writing over 60 separate 3G UMTS networks are in operation around the world. Implemented against the 3G Partnership Project, 3GPP, specifications, (3GPP, 2005) for UTRAN (UMTS Terrestrial Radio Access Networks) radio (as opposed to the GSM GERAN radio access, which includes GPRS), 3G was formally adopted by the ITU as a standard in November 1999. 3G, service implementation was pioneered in Japan by NTT Do Co Mo who launched the first network involving WCDMA technology in 2001. However it took some 4 to 5 years to bring to market a technically robust and commercially viable service in the UK.

The 3G service overcomes the shortfalls within GSM by providing up to 2Mbit/s data at picocell and 384Kbits/s at microcell level. Compared with the 9.6Kbits/s provided under GSM, this is a significant enhancement and is achieved globally using WCDMA (wideband code division multiple access) or TDCDMA (time division/code division multiple access) to switching frames and a QPSK (quadrature phase shift keying) signal with carrier spacing of 5Mhz, (Chen, 2005). To allow future global flexible connectivity, the ITU agreed 3 end game protocols CDMA DS – direct sequence, CDMA MC – multi carrier and CDMA TD. As the dominant modes they have become de facto standards, (Kambourakis, 2005).

Though detailed in the 3GPP standards, a clearer understanding of system architecture is necessary to allow for accurate forensic analysis of 3G data. Of equal need is an understanding of the imminent and future developments within the 3G arena to

incorporate the evolution of protocols, access methods, services, broadcast, internetworking and security features. The latter are well articulated at the UMTS Forum, (UMTS, 2005). Of particular note is the implementation of the IMS (IP Multimedia System) which will allow multiple services to be carried by a single bearer medium and separates the service layer from the network layer, allowing internet-like interoperability and having the advantage of moving host networks away from the hitherto ubiquitous circuit switched arena to the packet switched domain. According to the UMTS Forum, (UMTS, 2005), this will allow for "universal, optimal, anytime, anywhere access to multimedia services".



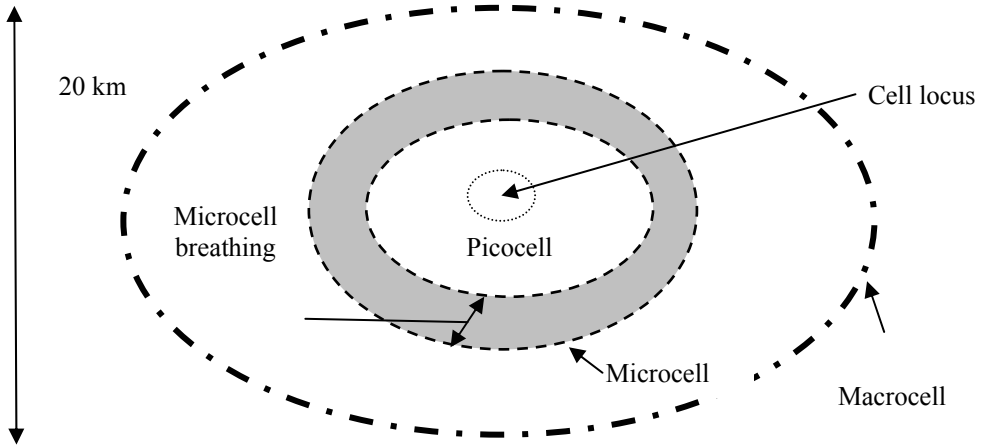
Simple 3G Network Architecture

The ITU envisages that "by the year 2020, potentially the whole population of the world could have access to advanced mobile communications" (ITU-R, 2000). Exploitation of the technology by criminal gangs or terrorist groups must therefore be considered as inevitable.

In simple terms, 3G network architecture is as shown in the Figure 2. A phone (data terminal) communicates through the RAN/UTRAN into a core network and out on the appropriate network, IP for data and voice or Circuit Switched dependant upon voice call destination. Of particular note is the 3G cell structure which differs markedly from GSM due to protocol, through-put, frequency and "load balancing" achieved through network management within adjacent cells.

The 3 basic cell structures are; Macrocells covering suburban and rural areas, Microcells covering urban areas, and Picocells covering buildings or streets.

The cell structure overlaps and interlinks as shown at Figure 3 below. Managed dynamically by autonomous management equipment it is possible to vary the cell size/footprint (known as cell breathing) and transfer subscribers from within a particular cell to an adjacent and overlapping cell to load balance and ensure a consistent level of throughput.



3G Cell Structure

In addition to the network's ability to manage the cells dynamically transferring mid call between adjacent and overlapping cells, it is also possible to transfer a subscriber to an alternate network when coverage is limited or, when the cell is at full capacity. This technique is often referred to as piggy-backing and requires complex management arrangements between service providers to ensure availability of spare capacity.

While operating within the core 3G network, the protocols in use and software/hardware interaction process provide a degree of security which significantly exceeds that provided in earlier (GSM) 2G services.

The 3GPP had already identified that there were issues relating to the confidentiality and integrity of earlier 2G protocols. Principally, that the authentication process (based on an implementation of the A3 algorithm) was inadequate; that the encryption (based on implementation of A8 and A5 algorithms) was weak; that the identification of subscribers was not well protected and the utilisation of the SIM could be hardened. These vulnerabilities were open to exploitation in such a manner that the 3GPP highlighted that GSM was vulnerable. Accordingly, the 3GPP technical specification for 3G Security outlined that although based on GSM security concepts a number of (significant) changes would be made:

- Changes to defeat a false base station attack; this would include mechanisms to improve the identification and authentication between the handset/terminal and network.
- Key lengths would be increased to allow for stronger more robust algorithms for encryption and integrity.
- Mechanisms were included to support security within and between networks.
- Security would be based within the switch rather than the base station, ergo links are protected between the base stations and switch.
- Integrity mechanisms for the terminal (handset) identity were to be built in from the start (using the IMEI).
- While not defining the authentication algorithm, guidance would be given.
- Inter network roaming would implement the higher precedence security requirements such that when a 3G handset operated through a GSM node

the smart card security from the 3G phone would be utilised.
- Provision should be made for provision of information/evidence to the law enforcement community in relation to abuse of the network, attack against the network or, use of the network in facilitation of crime.

From a law enforcement perspective these assertions are of value, since this increases the evidence threshold (balance of probability) in presenting evidence from a 3G handset and provides a mechanism for the provision of such evidence (where implemented).

2.1. Intranetwork Security

To effectively understand the value of any subscriber information extracted from the network as evidence, knowledge of the management (and security) functional elements of the network is necessary. The elements and interfaces are broken down as follows;

- Home Location Register (HLR). The HLR provides a system management control over the authorised activities of a subscriber in respect of a subscriber's profile, services registered and requested/purchased.
- Authentication Centre (AuC). The AuC manages all identification authorisation and cryptographic key management within the system.
- Mobile Switching Centre (MSC). The MSCs are the most critical component of the 3G network handling all "calls" inbound to or outbound from, the network.
- Network Interfaces. These connect all inter and intra network elements. By their very nature their distribution and roles will be logically (and physically) different, ranging from internal content server interfaces to external microwave WAN links. Usually multihoned.
- Billing Systems/Customer Care (Management) Systems. These provide extensive database records of individual subscriber details ranging from identity (where recorded), handset IMEI and USIM to billing and call record information, (Lehrer, 2004).

3. Gleaning Criminal Intelligence (Within the UK's Legislation)

Intelligence is a critical tool in fighting crime and terrorism. Accurate and timely intelligence provides knowledge which will influence the tactical and strategic planning, management and tasking of law enforcement resources in dealing with a particular target.
Historically, intelligence has been regarded as the positive results resulting from the processing of information gleaned. In practice, the gathering of intelligence is conducted in a 4 stage cyclical process; Direction, Collection, Processing and Dissemination.
Starting with the Direction or tasking (this identifies the target and scopes the requirement), this is followed by the Collection phase (where the target is monitored and information of every type gleaned), the Processing phase (when the real analysis of the information is undertaken and that output which is considered to be of value is reviewed again and then produced), finally in the Dissemination phase, the output considered relevant is passed to those persons whom may need the information.

4. Identification of Future Trends and Weaknesses in Capability and Legal Process

Research and discussion has shown that there is a gap in perception between what the law enforcement arena requires (in terms of support) and what can be provided by industry (due to cost). The rapid expansion of the high capacity networks is fraught with problems and law enforcement is already overwhelmed by the volume of equipment being handled in cases. While law enforcement looks to "grace and favour" from industry, the reality is that the 3G service providers do not have the capacity or resources to take on this role. Inevitably this will lead to a contracting out of the task to specialist companies.

Clearly the differing implementations of manufacturers' solutions within the 3G market make a "one-size fits all" approach ineffectual. While the communications protocols are matched, little else is. It is therefore critical that whatever forensic examination tools are used, that they are capable of extracting all the information from the handset regardless of the handset OS. It is therefore probable that a department will require a number of different tools or if developed, OS specific variants of the same tool.

With the rapid development of games and other content driven applications, the level of expertise in programming applications to run in J2ME, is increasing. With this increased skill and knowledge amongst programmers, it is becoming increasingly likely that for very little cost, a file/message encryption utility could be produced by the criminal fraternity; this would allow the criminals unfettered and secure text and or e-mail communication globally to the handset and they would thus attain a position of information superiority, (Houéto, 2005). Add to this the increasing processing power with each sub-generation of 3G phones, then it could be possible within an IP environment to produce full end to end encryption (rather than link or file encryption) through the infrastructure or, through use of steganographic applications, undetectable (through network) obfuscation of encrypted files. Should this become a reality, then it would pose significant problems to the law enforcement community.

Conclusions

The continuing rapid evolution of the 3G networks will bring with it a revolution in the way that the service is provided and those supporting the service will be trained and equipped. While little anecdotal evidence is available to substantiate any estimate in the volume of crime that will take place wholly or partly as a result of the outstanding and ever increasing functionality and services provided in the 3G environment. It may be worthy of note to make comparisons with the exponential rate of increase in internet related or GSM solicited crime. Nonetheless, it is believed that an industry/law enforcement representative body should be created to monitor the levels of reported and detected crime. This body should encompass the industry competitors, police and should also be supported by OFCOM and the Home Office.

References

3GPP, 2005, Specifications, http://www.3gpp.org/specs/specs.htm, 29th November 2005

BBC, 2005, Brazil considers mobile phone ban, http://news.bbc.co.uk/1/hi/business/1777516.stm, 29th November 2005

Chen M. and Hwang R., 2005, Fair and efficient packet scheduling algorithms for multiple classes of service under QoS guarantee in UMTS, Computer Communications, Volume 28, Issue 4, 16 March 2005, Pages 379-39.

Houéto F., Pierre S., 2005, networks subject to voice and video traffics, Computer Communications, Volume 28, Issue 4, Pages 393-404

ITU-R, 2000, General focus areas for research and further study for the future development of IMT-2000 and systems beyond IMT-2000, http://www.itu.int/ITU-R/study-groups/rsg8/rwp8f/docs/focus-areas.doc, 29th November 2005

Kambourakis G., Rouskas A., Gritzalis S. and Geneiatakis D., 2005, Support of subscribers' certificates in a hybrid WLAN-3G environment, Computer Networks, In Press, Corrected Proof, Available online 22 September 2005.

Lehrer M., 2005, Quality of service and performance issues in multiservice National lead markets and the design competition for 3G network applications, Journal of Business Research, Volume 57, Issue 12, Pages 1397-1401

Three, 2005, Introducing 3 a new type of company, http://www.three.co.uk/aboutus/newkind.omp, 29th November 2005

UMTS Forum, 2005, HSPA: High Speed Wireless Broadband from HSDPA to HSUPA and Beyond, http://www.umts-forum.org/, 29th November 2005