Global Information Assurance Certification Paper

Harnessing mobile communications security: A focus on 3G

By Arman Shah bin Alias

Abstract

Players in the mobile communications industry need to put in place security measures for third-generation wireless (3G) communications to ensure the successful deployment of the network as well as the provision of services and applications as that would translate into a profitable business model for all – particularly in a cash-strapped environment with a limited market such as the one found in a developing country like Malaysia.

The paper presents an overview of the projected 3G revenue at the local, region and global levels. It highlights 3G security objectives, current 3G security features and, also, opportunities for an eco-system of players that result from the related issues. It is proposed that for all to reap benefits from 3G, a proper framework have to be established to form the basis strategic partnerships and coordinated efforts to address the security issues at infrastructure as well inter and intra-operations levels.

Introduction

The penetration rate of mobile communications is rapidly rising by the day in countries around the world. The mobile data services market is developing fast with a majority of developed markets having licensed third-generation wireless (3G) spectrum with General Packet Radio Service (GPRS) and other present mobile wireless communications – often called as 2.5G - solutions now widely deployed.

The trend is in tandem with various advances in communications technology, increasingly pervasive telecommunications infrastructure, and an evolving demography of subscriber base of which a majority is the growing youth market who are generally technologically savvy and time rich.

3G follows the first generation (1G) and the second generation (2G) in wireless communications. The 1G period began in the late 1970s and lasted through the 1980s. These systems, which featured the first true mobile phone systems known as "cellular mobile radio telephone", used analog voice signaling.

The 2G phase, whose technology is still much in use, began in the 1990s. The 2G cell phone features digital voice encoding. Today 2G technology has steadily improved with increased bandwidth, packet routing, and the introduction of multimedia.

3G refers to near-future developments in personal and business wireless technology, especially mobile communications. This phase is expected to reach maturity between the years 2003 and 2005.

3G is expected to include capabilities such as enhanced multimedia (voice, data, video, and remote control); usability on all popular modes (i.e. Mobile phones, e-mail, paging, fax, video-conferencing, and Web browsing); broad bandwidth and high speed from 2 megabits-per-second (Mbps) upwards; routing flexibility (repeater, satellite, local area network/LAN); operation at approximately 2 gigahertz (GHz) transmit and receive frequencies; roaming capability throughout Europe, Asia and North America.

While 3G is generally considered applicable mainly to mobile wireless, it is also relevant to fixed wireless and portable wireless. The ultimate 3G system might be operational from any location on, or over, the earth's surface.

This includes use in homes, businesses, government offices, medical establishments, the military, personal and commercial land vehicles, private and commercial watercraft and marine craft, private and commercial aircraft – except where passenger use restrictions apply, portable, and space stations and spacecraft.

For mobile operators, the trend represents a compelling business case with vast opportunities to be tapped into. The number of operators starting to successfully provide data services are those in Japan and South Korea, in particular, as well as O2 and Vodafone in Europe[1].

In Malaysia, where the government has awarded two companies 3G spectrum licenses to offer high-speed mobile services in the country in the latter part of 2002, the customer base for mobiles communications reached an estimated 8.2 million out of a population of some 24 million while the industry revenue hit a projected RM9.1 billion (Malaysian Ringgit) by the end of 2002[2].

With offerings of high-speed mobile services, the particular market is expected to experience a compounded annual growth rate (CAGR) of 9 percent over the period of 2002 to 2017 - reaching an estimated value of RM35 billion (Malaysian Ringgit) by the final year.

Meanwhile, on the global front, analysts are forecasting that total 3G worldwide revenues will reach US$322 billion by 2010 with cumulative revenues to hit over one trillion dollars from now to 2010. Asia Pacific alone represents the single largest total revenue opportunity with US$120 billion in 2010. By then, the projected penetration rate for 3G services in the worldwide mobile base would be some 28 per cent with the average 3G subscriber spending around US$30 per month on 3G data services[3].

3G services are made available through technologies such as Wideband Code-Division Multiple Access (WCDMA), an ITU standard. The mobile wireless technology offers much higher data speeds to mobile and portable wireless devices than commonly offered in today's market. It supports mobile/portable voice, images, data and video communications at up to 2Mbps (local area access) or 384 Kbps (wide area access). A 5 MHz-wide carrier is used, compared to 200 kHz-wide for narrowband CDMA

As 3G mobile networks roll out, the promise of video-capable bandwidth and phones, global roaming for voice and data, and rich online content has the potential to match the Internet in terms of reach and speed of acceptance. Greater bandwidth coupled with enhanced technology and improved handset futures is fast creating a new playing field for the industry. The wireless data ecosystem will see many new players.

Hence, mobile operators need to focus on the average revenue that can be derived per unit/device (ARPU). This translates into widening their business strategy to not just include voice revenue but also data revenue, introducing interactive infotainment services for the youth market, and seeking out new revenue streams through value-added services.

Although operators would be able to offer a wide variety of services, they can only act within current constraints that include handset functionality, network capacity, the determination of role to play in service provision, and the nature of relationship with content providers.

For players it is important to note that key enablers in the deployment of 3G services not only include access to content, personalized services, user convenience, data billing, payment, but also security. It is necessary that they are aware of the risks, obligations and duty of care implications and put measures in place to adopt best practice.

Concerns

While 3G promises a myriad of high-speed services for users, there are inherent dangers within. In a report in ZDNet UK[4], computer security experts in 2000 already recognized that all the connectivity and functionality within 3G would inevitably mean an increased risk of attack by mobile viruses and worms as well as malicious hackers.

The security breaches that have posed constant threat to desktop computers are migrating to the world of wireless communications where they pose a threat to mobile phones, personal digital assistants, laptop computers and other devices that capitalize on the convenience of wireless communications.

Just as Internet commerce constantly suffers from the exploitation of security vulnerabilities – with a substantial number of users reluctant to use their credit cards online, these concerns are also applicable to 3G networks.

There is also much skepticism about the viability of 3G as a safe environment. With wireless devices finding their way into corporate environments, wireless security is an increasingly growing concern. This is due to the fact that the emergence of the new devices may bring about a whole new slew of possible security breaches – there are many more possibilities for a security breach once a point of access becomes wireless and mobile.

With wireless communications, important and vital information is often placed on a mobile device that is vulnerable to theft and loss. In addition, this information is often transmitted over the unprotected airwaves.

Now, applications like mobile commerce require that this critical information be decrypted by a server somewhere in the communications chain before it is encrypted again and forwarded to a new destination. Every point in the wireless communications chain where information is decrypted represents vulnerability in the security of the system.

Thus, the network is the first place that security has to be considered. In the meantime, the growing complexity of mobile devices and the increased prevalence of interoperability software on them raises the spectre of mobile device viruses and hacking attacks.

Currently, Global System for Mobile communications (GSM) security mechanisms includes 40-bit encryption, but theoretical attacks against this and the authentication mechanisms have been demonstrated. 3G technologies will have stronger cryptographic techniques, and new authentication technologies.

The last risk is the 3G devices itself as they promise to be attractive to both petty thieves and professional criminals after corporate and financial data.

Security measures must match the nature of the application provided to ensure satisfied users. At the same time, they should be strong enough to instill a sense of trust that the transaction or download is not jeopardizing personal information, privacy and content ownership rights.

Issues

As mentioned above, there is great motivation for 3G security. After all, 3G services is a multi-billion dollar industry with millions of potential subscribers worldwide. There is also significant cost involved with some US$3 billion required to set up a network.

With the boom of handset devices and wireless technology and users demand for richer content for their mobile (such as through multimedia messaging, video conferencing, voice-over-IP, m-business), there is clearly need for security features to ensure user and data confidentiality, quality of service (QoS), billing, and protection against intruders.

In setting up a network to offer 3G services and applications, mobile operators need to observe the following 3G security objectives[5]:

- Ensure that information generated by or relating to a user is adequately protected against misuse or misappropriation
- Ensure that the resources and services provided are adequately protected against misuse or misappropriation
- Ensure that the security features standardized are compatible with worldwide availability
- Ensure that the security features are adequately standardized to ensure worldwide interoperability and roaming between different serving networks
- Ensure that the level of protection afforded to users and providers of services is better than that provided in contemporary fixed and mobile networks (including GSM)
- Ensure that the implementation of security features and mechanisms can be extended and enhanced as required by new threats and services

Thus, it is necessary to look into the security issues within 3G from various levels that are network access security, network domain security, user domain security, application domain security, and visibility and configurability of security.

With network access security, secure access to 3G services and protection against attacks on the (radio) access link is harnessed at the network level. The impact of security upon network performance includes service setup delay, end-to-end packet delay, and network load variation.

Network domain security, meanwhile, would securely exchange signaling data in the provider domain - hence, protecting against attacks on the wire line domain. User domain security looks into secure access to mobile stations while application domain security enables applications in the user and in the provider domain to securely exchange messages.

Lastly, visibility and configurability of security enable the user to inform himself whether a security feature is in operation or not, and whether the use and provision of services should depend on the security feature.

While there are issues within 3G security, there are present 3G security features[6]:

- Mutual Authentication - The mobile user and the serving network authenticate each other

- Data Integrity - Signaling messages between the mobile station and RNC (radio network controller) protected by integrity code
- Network-to-Network Security - Secure communication between serving networks. IPsec suggested.
- Wider Security Scope - Security is based within the RNC rather than the base station
- Secure IMSI (International Mobile Subscriber Identity) Usage - The usage is assigned a temporary IMSI by the serving network
- User-Mobile Station Authentication - The user and mobile station share a secret key, PIN
- Secure Services - Protect against misuse of services provided by the home network and the serving network
- Secure Applications - Provide security for applications resident on mobile station
- Fraud Detection - Mechanisms to combating fraud in roaming situations
- Flexibility - Security features can be extended and enhanced as required by new threats and services
- Visibility and Configurability - Users are notified whether security is on and what level of security is available
- Multiple Cipher and Integrity Algorithms - The user and the network negotiate and agree on cipher and integrity algorithms. At least one encryption algorithm exported on a worldwide basis (KASUMI)
- Lawful Interception - Mechanisms to provide authorized agencies certain information about subscribers
- GSM Compatibility - GSM subscribers roaming in 3G network are supported by GSM security context (vulnerable to false base station)

It needs to be emphasized that 3G security is not without its problems. Among others, all that can happen to a fixed host attached to the Internet could happen to a 3G terminal. IMSI is sent in clear text when the user is registering for the first time in the serving network. Here, trusted third party can be a solution.

Another problem is that a user can be enticed to camp on a false base station. Once the user camps on the radio channels of a false base station, the user is out of reach of the paging signals of SN (serving network). Hijacking outgoing/incoming calls in networks with disabled encryption is possible. The intruder poses as a man-in-the-middle and drops the user once the call is set-up.

Opportunities

The challenge for players in the industry now is to take hold of the security issue within 3G and create a profitable 3G business comprising of services and value. This is because 3G facilitate the landscape for new capabilities, more new applications, and more new players and, subsequently, more business risk.

This may prove quite difficult, as many mobile operators are still not developing market specific data strategies with many still not being driven by technological developments.

Adding to this, operators are not adapting quickly enough to changing market whilst saddled with old 2G internal structures, processes and approaches that would no longer be appropriate in the data environment. Furthermore, most consumers are not yet convinced about mobile data services - having been overwhelmed over WAP and initial GPRS services.

Rising to the challenge is the emergence of a new value chain that would result towards the development and management of a coherent eco-system[7] that could guarantee successful 3G services.

There are three levels to the eco-system with the base being the network provider (spectrum holder) that would provide access with GSM/GPRS/Universal Mobile Telecommunications System (UMTS) connectivity guarantee comprising coverage, uptime, speed, and dealing with loss packet and delays.

The second level is the service provider - for example, application service provider (ASP), mobile virtual network operator (MVNO), or reseller - that facilitate the platform (handset). This level provides gateway connectivity guarantees with gateway server availability, response time, throughput, authentication and authorization, as well as the security and billing gateway.

The third, or topmost level, are the content and applications providers that deal with aggregation, contents and applications. Players here guarantee user customer experience, content quality, currency and relevance, governance, content presentation and formatting, and scams control.

With the ecosystem coherent, players can go beyond stimulating market development and develop the successful business model that needs to be profitable. Proper revenue modeling is also a must at this juncture to hedge the risks. Partnership is possible along the model as risk sharing means sharing the benefit as well.

3G players must decide on the preferred position along the value chain, which will maximize value creating. In making the decision, a few points have to be considered: where the costs will reside the most; ability to leverage existing customer base and strong brand position; and impact from the unprecedented wholesale pricing.

On top of that, partnerships must be built to last and not open lust. Therefore, strategic partnerships 3G business must be on win-win spirit with long-term perspective. Factors spectrum holder or mobile network operators must consider in choosing partners include[8]:

- What value do they bring to the table
- What are the business model
- What are the revenue sources
- What are the potential returns
- What are risks involved
- What are the competitors doing
- Does it have a strategic fit
- Are we in control of customer interfaces
- Are our billing relationships strengthened

Also within the eco-system are opportunities for security solutions and service providers to play their role, as security is a necessity at every level of 3G content and service provision. After identifying their position in the chain, only then can players address the various application strata in security needs – be they low-level security needs, mid-level; or high-level for example.

Low-level security needs refer to when important or personal information is not jeopardized or when value of a transaction is fairly low. Low-level security measures must still maintain the

integrity of the information transmitted and received over wireless communications channel whilst ensuring the authenticity and non-repudiation of the transaction.

Mid-level security needs occur when the processing demands placed on a mobile device requires more complex encryption and public key infrastructure (PKI) algorithms, in conjunction with the deployment of a secure boot loader, digital rights management, filtering and anti-spamming software.

Generally, applications with high-level security needs will start with very strong encryption and PKI algorithms, and increase from there. A dedicated hardware/software security module consisting of hardware-based random number generators, hardware-protected memory where root keys can be stored, secure input/output channels, and accelerator modules to improve processing performance will be deployed at this level.

Security solutions and service providers are generally able to assist 3G players in the following areas[9]:

- Design of network interconnections from the ground with security in mind and will not compromise security for functionality
- Procedures for "hardening" network devices and servers
- Java security standards
- Standards for application level security
- The definition of high-level network security policies relevant to the players' businesses, including an information security manual
- Turning the high-level business security policies for e-commerce into strategies for implementation
- Implementing policy output onto network devices
- Regular vulnerability and penetration testing
- Implementation of intrusion detection systems

The security policies and standards developed, which can highlight potential problem areas before they become actual ones, can help provide the basis for all of the information security practices for 3G networks that are to be deployed.

The range of guidelines, standards and policies for securing network interconnections implemented will result in a robust and secure design of services over these wireless networks – providing the assurance required by 3G players and their customers. It also ensures that investment in information systems for 3G is maintained throughout its investment lifecycle.

This is important as it is foreseen that the spectrum holder or the mobile network operator will work hard in balancing usage and capacity, leading capacity utilization and differentiation in order to secure profit, which will only be possible if the network is seen as secure.

The right business model is needed in achieving the delicate balance between cost and value. This should be given the utmost priority as customers, most likely, will only recognize the service provider or mobile virtual network operator (MVNO) in their dealings and contact with 3G services.

Suggestions/Conclusion

In efforts to ensure 3G security, it is clear that players have to be aware, alert and aware of factors such as global developments and domestic developments on 3G. The new approaches to data service, technological issues as well as advances both in network and content and services are key issues to consider. They also have to be mindful of the role and value of partners in the new communications provision eco-system.

It is definitely a necessity that within the ecosystem, there are security solutions providers that are able to address the security issues at various levels discussed earlier i.e. network access security, network domain security, user domain security, application domain security, and visibility and configurability of security.

These security solutions providers have to work closely with network operators and applications, content and services providers to ensure that each block within the 3G service provided is secure in a coordinated and cohesive manner and is flexible and adequately accommodative for future additional capacity as well as applications and content expansion and technology upgrade.

In securing 3G networks, applications and services, initial parameters could perhaps be derived from deployment frameworks provided for a defined period of time by governments - especially in countries like Malaysia, where concerns about costs and success of such ventures are high. This is especially so with the potential impact of 4G over 3G where the data rates are beyond 384 Kbps.

Based on the framework, players - be it the operators or other parties in the eco-system - will be sure they touch base with various security-related elements such as the migration from 2G to 3G, 2G to 3G secure roaming and vice versa, interconnection agreements in domestic roaming, agreement on services roaming, maintaining QoS levels.

However, operators need some flexibility from government regulators to make 3G course corrections. Instead of dictating to customers, carriers should be able to respond to consumer demands.

Like in the early days of wireless voice, the enterprise and business users will be the early adopters of wireless data. These market segments are the ones with the money to invest in such applications, and they have the need to use technology to become more efficient and productive and use it to become more customer-focused.

Due to the high costs that an individual customer may have to pay for 3G services, mass-market adoption will only take place when costs are lowered to match what subscribers are willing to pay. This is closely linked to customer perception of the QoS and security of the services offered.

To fit the right security measures with individual 3G applications, 3G network operators must balance the expectation of users with the sort of multimedia experience provided by the application and the financial implications of the transaction or download. This will cause applications to fall into one of several strata that would make up the emerging marketplace.

It would certainly be beneficial for 3G telecommunications network operators and regulators in the Asian region to closely track the European market as they launch 3G services, and learn from its successes and mistakes. Being part of a global market, regional and local players do not operate in isolation. They must take caution against implementing indigenous-specific solutions as that would threaten the interoperability (nationally and internationally) between networks.

Vendors are global and develop solutions with little regard to local markets. Therefore, in terms of launch timing and the availability of network equipment that will allow infrastructure sharing, the global timetable and global standards – including those for security - must prevail.

It is also critical for 3G network operators to take into account ways to enhance the availability of mobility management, the varying services platform among the different operators, and maintaining personal profile in the roaming network.

For more secure 3G services, there is a need to extend current simulation implementation with more complicated, perhaps fully loaded, network scenario. Add video conferencing and multimedia streaming traffic. Observe variations in bit error rate and packet drop rate, among other things.

In the mean time, 3G network operators must be mindful of infrastructure sharing issues although infrastructure sharing with other operators may provide advantages in terms of capital expenditure.

Firstly, how does one maintain QoS and data integrity especially when both operators share the same infrastructure? Secondly, what about the location of new base stations. This is an issue of network control, when one telco operator has one big customer base in one area, and another operator has a big customer base in another area.

Also, what are the key considerations when players look into outsourcing of operation and maintenance of network infrastructure to equipment vendors?

Network-to-network security must be tightened. This brings into question issues such as how to establish trust between different operators as well as other players? Is IPsec a feasible solution for secure communication between networks?

End-to-end security also needs to come into place where issues like whether two mobile nodes can establish secure communication channel without relying too much on their serving network, and whether they can exchange certificates or shared secret keys.

These are but only some measures that need to be taken to harness 3G security which is imperative to ensure the successful uptake of 3G services and avoid the wastage of investment in 3G network rollout.

This is important as there are already some forward-thinking wireless operators who are now working with fourth-generation (4G) technology providers in an effort to leapfrog expensive and ineffective 3G wireless strategies.

4G is the stage of broadband mobile communications that will follow the still-burgeoning 3G that is expected to reach maturity between 2003-2005. 4G services are expected to be introduced first in Japan, as early as 2006 - four years ahead of the previous target date. The major distinction of 4G over 3G communications is increased data transmission rates, just as it is for 3G over 2G and 2.5G

A number of 4G air interfaces now being readied for beta deployments by leading wireless operators since 4G technologies offer a lower cost and/or higher performance alternative to traditional 3G systems.

4G digital IP-based high speed cellular systems are anticipated to account for 14 per cent of total mobile wireless revenues in 2007 and 50 million subscribers by year-end 2007[10]. 4G infrastructure sales are expected to reach US$5.3 billion during 2007.

4G is expected to deliver more advanced versions of the same improvements promised by 3G, such as enhanced multimedia, smooth streaming video, universal access, and portability across all types of devices. Industry insiders are reluctant to predict the direction that less-than-immediate future technology might take, but 4G enhancements are expected to include worldwide roaming capability.

Despite threats, 3G is expected to show positive results in the long run. Subscribers to WCDMA-based services are expected to reach 90 million by 2007, mainly in Japan and Europe. Towards this, it is key that 3G mobile communications security is harnessed. 3G security is a critical element in 3G strategy deployment and should be included in the planning, implementation and delivery of 3G application, content and services.

This means identifying the vulnerabilities, adopting a security strategy that takes into account all possible weaknesses, and deploying an architecture that is powerful enough to defeat today's threats yet adaptable enough to meet head-on the unimagined threats of tomorrow.

In the long run, players in the 3G eco-system will experience a number of benefits from security which includes protection from fraudulent theft of services; protection from unauthorized use of mobile devices by someone other than the owner of the device; protection from denial-of-service attacks; digital rights management protection for copyrighted content; and most importantly, competitive advantage over insecure services offered by other carriers.

For end users, the benefits include enhanced user experience through transparency, ease-of-use, and a highly secure environment. High-performance and strong encryption including on-device, disposable key generation will create a highly secure environment for electronic wallet, virtual private networks and mobile office applications.

End users would then enjoy very fast secure transactions for applications involving high data transmission rate as in content and media distribution (streaming media) and other high-end applications. This would encourage a high level of trust and data integrity to support a wide range of mobile real-time financial and content transactions over the Internet and virtual private networks.

Bibliography

Abbas, Mazlan. Examining the New Value Chain in 3G. A paper presented in *Mobiles Malaysia with Focus on WCDMA 2002.* August 12-13, 2002: Kuala Lumpur, Malaysia.

Campbell, Roy et. al. Analysis of Third Generation Mobile Security. June 28, 2002: Computer Science Department, Univeristy of Illinois at Urbana-Champaign. (http://choices.cs.uiuc.edu/MobileSec/)

Howard, Peter. 3G Security Overview. *IIR Fraud and Security Conference*. March, 2000. (http://www.isrc.rhul.ac.uk/useca/OtherPublications/IIR-overview.pdf)

Jameson, Justin. Creating a profitable 3G business: Services and value. A paper presented in *Mobiles Malaysia with Focus on WCDMA 2002.* August 12-13, 2002: Kuala Lumpur, Malaysia.

Knight, Will. 3G: Will 3G devices be secure. *ZDNet UK*. August 23, 2000. (http://news.zdnet.co.uk/story/0,,s2080988,00.html)

Kushairi, Ahmad. Work cut out for Telekom and Maxis on 3G implementation. *Computimes*. August 1, 2002: Kuala Lumpur, Malaysia.(http://www.emedia.com.my)

Mohamad, Roslan. Partnerships and Alliances - Keys to Success in 3G. A paper presented in *Mobiles Malaysia with Focus on WCDMA 2002.* August 12-13, 2002: Kuala Lumpur, Malaysia.

Narayan, Malur A. Wireless Access. A paper presented in *Mobiles Malaysia with Focus on WCDMA 2002.* August 12-13, 2002: Kuala Lumpur, Malaysia.

Ng, Adrian. Content, Content, Content - It's All About Content. A paper presented in *Mobiles Malaysia with Focus on WCDMA 2002.* August 12-13, 2002: Kuala Lumpur, Malaysia.

Walker, Michael. On the Security of 3GPP Networks.
(http://www.esat.kuleuven.ac.be/cosic/eurocrypt2000/mike_walker.pdf)

Yeap, Cindy. Telekom, Maxis unit awarded 3G service spectrums. *Business Times*. July 31, 2002: Kuala Lumpur, Malaysia.(http://www.emedia.com.my)

Zawila, Richard. WCDMA - Deployment Challenges. A paper presented in *Mobiles Malaysia with Focus on WCDMA 2002.* August 12-13, 2002: Kuala Lumpur, Malaysia.

Security in 3G Networks
(http://www.frontrunner.eu.com/services/sec-3g.asp)

Reference:

[1] Jameson, Justin. Creating a profitable 3G business: Services and value. A paper presented in *Mobiles Malaysia with Focus on WCDMA 2002.* August 12-13, 2002: Kuala Lumpur, Malaysia.

[2] Yeap, Cindy. Telekom, Maxis unit awarded 3G service spectrums. *Business Times*. July 31, 2002: Kuala Lumpur, Malaysia.(http://www.emedia.com.my)

[3] Mohamad, Roslan. Partnerships and Alliances - Keys to Success in 3G. A paper presented in *Mobiles Malaysia with Focus on WCDMA 2002.* August 12-13, 2002: Kuala Lumpur, Malaysia.

[4] Knight, Will. 3G: Will 3G devices be secure. *ZDNet UK*. August 23, 2000. (http://news.zdnet.co.uk/story/0,,s2080988,00.html)

[5] Howard, Peter. 3G Security Overview. *IIR Fraud and Security Conference*. March, 2000. (http://www.isrc.rhul.ac.uk/useca/OtherPublications/IIR-overview.pdf)

[6] Campbell, Roy et. al. Analysis of Third Generation Mobile Security. June 28, 2002: Computer Science Department, University of Illinois at Urbana-Champaign. (http://choices.cs.uiuc.edu/MobileSec/)

[7] Abbas, Mazlan. Examining the New Value Chain in 3G. A paper presented in *Mobiles Malaysia with Focus on WCDMA 2002.* August 12-13, 2002: Kuala Lumpur, Malaysia.

[8] Mohamad, Roslan. Partnerships and Alliances - Keys to Success in 3G. A paper presented in *Mobiles Malaysia with Focus on WCDMA 2002.* August 12-13, 2002: Kuala Lumpur, Malaysia.

[9] Security in 3G Networks
(http://www.frontrunner.eu.com/services/sec-3g.asp)

[10] http://www.3g.co.uk/pr/november2002/4468.htm