Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Internet in the Palm of Your Hand

3G is positioned to radically transform the Internet paradigm from a static, PC-centric model into a mobile Internet. Imagine commuting home from work on a train while conducting a broadband videoconference on a handset no larger than today's cellular telephone. Scenarios as this are what have the telecommunications industry and governments energized. Of course, there are issues yet to be addressed with the imminent rollout of 3G. Will there be a global standard? Who will control the airwave spectrums necessary for 3G?...

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.

watchfire

The Internet in the Palm of Your Hand

Ronald M. Buchanan

27 August 2001

Introduction

3G is positioned to radically transform the Internet paradigm from a static, PC-centric model into a mobile Internet. Imagine commuting home from work on a train while conducting a broadband videoconference on a handset no larger than today's cellular telephone. Scenarios as this are what have the telecommunications industry and governments energized. Of course, there are issues yet to be addressed with the imminent rollout of 3G. Will there be a global standard? Who will control the airwave spectrums necessary for 3G? When will it arrive? And, finally, what are the security concerns? To better understand where we are headed tomorrow; let's take a look to see has what has brought us to the brink of 3G.

The mobile communications industry has evolved in three stages: analogue, digital and, finally, multimedia. Each of these stages is expressed as a "generation" with analogue being the first generation and multimedia being the third generation.

1G

Description:

We all remember first generation telecommunications, 1G. 1G mobile telephones are little more than FM radios operating in the 824 – 829 MHz range. In North America, 1G is governed by the Advance Mobile Phone System (AMPS) standard. 1G is able to share frequencies using a technique called Frequency Division Multiple Access (FDMA) which creates multiple frequencies. AMPS allows 45 different channels per cell and requires a lot of bandwidth.

Security Issues:

One of the primary security concerns for analogue phones is that the signals are unencrypted and can be easily intercepted. Although analogue phones are still being utilized in the US and the technology has improved somewhat, the logical evolution was to go digital.

2G

Description:

More memorable than 1G, second generation telecommunications (2G), is the circuit switched[1], digital technology most commonly used in today's digital mobile telephones.

[1] Circuit Switching: A type of communications in which a dedicated channel (or circuit) is established for the duration of a transmission. The most ubiquitous circuit-switching network is the telephone system, which links together wire segments to create a single unbroken line for each telephone call.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

(Motorola)

Being digital, the user's voice is sampled then converted into 1's and 0's and transmitted via a wireless network to another 2G handset or to a traditional telephone where it is converted back to sound waves. Improved features of 2G from 1G include: digital phone calls, voice mail, and receiving simple email messages. With 2G, roaming is possible throughout 159 countries.

Being digital, telecommunications providers are able to manipulate the signal in ways unimaginable with first-generation phone systems. Unfortunately, this set the stage for varied standards to be introduced by competing providers. FDMA, the technique utilized to divide analogue 1G spectrum into channels was combined with Time Division Multiple Access (TDMA), which divided each channel into three to ten time slices, to be shared by several phones. Other systems used Code Division Multiple Access (CDMA), also referred to as spread spectrum, which didn't use fixed frequency channels at all, but broadcast the radio signals over several frequencies simultaneously. Originally a European standard before arriving in America, Global System for Mobile Communication (GSM) is another second-generation standard. GSM operates in the 800-900 MHz frequency range.

Security Issues:

2G was designed with security in mind. The responsibility for security rests with the home environment operator. Authentication is not required when roaming and is not exposed over the air. Some GSM security concerns center around the fact that nearly everyone believes that 2G is secure. Also, the base station to mobile connection is encrypted with a 40 bit key to make the signal appear as random noise, however, the algorithms are getting old.

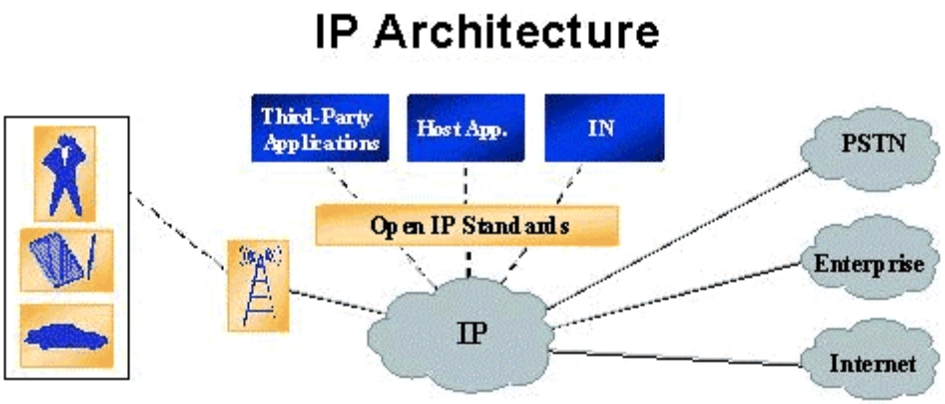
2.5G

Description:

2.5G or General Packet Radio Service (GPRS) can be looked at as GSM service for Internet access. 2.5G supports higher speed data (171kbits/s) and sustains a permanent data connection.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

GPRS is intended for limited browsing, email, card transactions, etc. GPRS is an Internet Protocol packet switched[2] layer on top of the circuit switched GSM service.



(Motorola)

This creates a permanent connection to the Internet. Users are charged by the bit rather than time. This can prove costly unless dealing with file transfers. GPRS is good for the operator as well as the user since it makes use of existing equipment investment in earlier standards. GPRS makes efficient use of its spectrum and exploits spared capacity though a session is lost if a call is dropped.

Security Issues:

GPRS, another step closer to realizing a mobile Internet, also suffers from many of the vulnerabilities common to the Internet today. Any service that is used over the Internet: File Transfer Protocol (FTP), web browsing, chat, email, telnet, will be available over the mobile network. Additionally, Internet Protocol mixes customer data with internal management data. In some networks, encryption is effectively on 40bit. Finally, GPRS is vulnerable to denial of service (DOS) attacks by its customers.

2.75G

Description:

Enhance Data Rates for Global Evolution (EDGE) is GPRS on steroids; or in this case, GPRS with a service touting a new modulation scheme. Operating in the 800/900/1800/1900 frequency bands, EDGE allows data transmission rates up to 473 kbits/s. The big draw of EDGE is that it allows 3G services without purchasing an expensive 3G license. Many companies in the United States are considering EDGE as an alternative to 3G because the hardware is backward compatible saving infrastructure costs associated with upgrading the base stations.

[2] Packet Switched: Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Security Issues:

Security concerns are the same for EDGE as GPRS as it is IP based.

3G

Description:

3G, also known as IMT-2000 (International Mobile Telecommunication 2000), is the new generation of wireless communication; a mobile Internet. Its development is based on the initiative of the International Telecommunication Union (ITU)[3]. Since most 3G systems evolved from different, incompatible 2G systems like CDMA, GSM, and TDMA, the IMT-2000 standard is seen as providing compatibility and interoperability of different systems in 3G.

3G is broadband and packet-based. It can be used to transmit text, Voice over IP, video, and multimedia at data rates up to 2Mbps in a fixed or stationary wireless environment and 384kbps in a mobile environment. Moreover, 3G offers a consistent set of services to mobile users no matter where they are located around the world assuming the frequencies utilized in the various countries are the same. 3G is more spectrally efficient than GSM and its wider bandwidth, 5MHz, results in better reception.

3G is different depending where you are in the world. In Europe, 3G is UMTS: wideband CDMA focused on Frequency Division Duplex (FDD) with some Time Division Duplex (TDD). In Japan, 3G is Wideband CDMA with only FDD. In the United States, 3G is either EDGE (Enhanced Data Rates for GSM Evolution) or 3G is Wideband CDMA but called CDMA-2000.

3G is due to be launched at the end of 2001 in many markets. Countries around the world have been auctioning their spectrum to telecommunications providers and receiving premium prices; often billions of dollars from companies striving to get an early foothold in the eagerly anticipated 3G market. The internationally agreed upon spectrum for 3G is the1,755 - 2,200-MHz range. Unfortunately, the United States has already allocated much of that spectrum, 1,755 1,850 MHz, to government agencies: "Within the United States, this band is allocated exclusively to the federal government, particularly for defense purposes, such as space systems, mobile tactical communications, and combat training." (GAO, p. 7) The reason for the debate over such a limited amount of bandwidth is the spectrum under 3 MHz carries signals further, faster, and with greater reliability. The Government Accounting Office (GAO), in a report regarding the impending US auction of the 1,755 – 1,850 spectrum, recommended the government delay the auction pending further study of the situation. That recommendation does not bode well for US telecommunications company's quest to compete in the international in the 3G market.

[3] The International Telecommunication Union (ITU) is a United Nations specialized agency. The federal government considers the ITU the principal competent and appropriate international organization for the purpose of formulating international treaties and understandings regarding certain telecommunications matters.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Security Issues:

Being a node on an always-on IP network, many are concerned about the security implications associated with 3G. "They [3G devices] will definitely be targeted," says chief researcher at Symantec's European computer security labs, Eric Chien. "The question is to what extent." (Knight, p. 1).

3G will see two security improvements:

- The cryptography used will be strengthened with the introduction of 128bit keys. This increase is important. Cryptographic experts at the Weisemann Institute in Israel claimed in December to have developed a technique allowing a standard PC to listen in to GSM networks and figure out the 40bit key used to encrypt voice signals. Increasing the length of the key to 128bits would make this virtually impossible even with vastly increased computer power.
- Mutual authentication will be introduced using cryptographic keys to establish the identity of both user and base station over a connection. The signalling system providing authentication for users passing between different networks will also be protected using a public key cryptographic system (Knight, p.1).

Methods manufacturers are looking at to address security include 3G handsets with their own Java Virtual Machine with built-in security enhancements. The operating systems will utilize server side applications to decrease the chance of interference. Of course, someone can still simply steal the handset and access the content at a later date. Hardware manufacturers are exploring removable SIM (Subscriber Identity Module) cards called USIM (User Services Identity Module). Additionally, manufacturers are considering biometric devices like voice recognition to enhance the physical security of the handset and its contents. As a device with a permanent connection to the Internet, the location of the user can be tracked. This possibility holds good prospects in relation to personal safety but negative prospects regarding privacy issues. Another inevitable security consideration is the seamless integration of other wireless products into the 3G system. One such product is Bluetooth.

Compatible Technologies

Bluethooth

Bluetooth replaces cables between devices (2.4 GHz radio) and has data rates up to 720 kbits/s. Ad hoc networks of up to 8 devices can be created and is being marketed to the public in increasing amounts. It is projected that 1.4 million appliances will be Bluetooth enabled by 2005. Examples of such devices include: computers, keyboard, printers, stereos, TV's, games, domestic appliances, fixed telephones, and mobile phones. The marriage of 2.5G - 3G and Bluetooth will be ubiquitous. Whether walking into an office building or and airport terminal, Bluetooth enabled devices will be soliciting responses from, or pushing data to, other wireless devices. Due to this relationship, 3G systems may inherit Bluetooth vulnerabilities by association. Bluethooth enabled devices have unique addresses that allow monitoring and its authentication and encryption are designed for small networks; not the large, often ad hoc,

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

networks that will likely be encountered on a daily basis. Potential for other exploits are on the data side, too.

WAP/WML

The worldwide standard for providing Internet communications on digital mobile phones, personal digital assistants (PDA's), and other wireless terminal is the Wireless Application Protocol (WAP). WAP is defined by participants in the WAP forum (www.wapforum.org). WAP is designed for efficient, secure use of bandwidth, slow connection speeds, small screens, and client computational power. WAP is similar to Hypertext Transfer Protocol (HTTP) as Wireless Markup Language plays a similar role to Hypertext Markup Language (HTML). WML is designed for micro-browsers; as you would find on the handset of a telephone.

4G

Description:

While 3G is yet to become a reality in most parts of the world, Japan is already studying the possibilities of 4G (fourth generation telecommunications). Japan's mobile broadband standard i-mode is one of the international 3G frontrunners. 4G is not anticipated to be the evolutionary step that was 3G. 4G will be an enhancement to the throughput and services the public will already receive through their 3G provider.

Conclusion

Third generation telecommunications is poised to change way we live. What we used to take for granted from a desktop personal computer we will soon come to expect from a handset smaller than the digital phones we carry today. There are plans already on the drawing board for fourth generation telecommunications (4G). 4G, much like today's PC market, will not be the evolutionary step 3G was but an enhancement to the existing technology. The transfer rates will be faster and the services will be enhanced. Of course, before anyone gets too excited thinking about 4G, there are still many hurdles for 3G to surmount before it becomes a publicly purchased and trusted system. The United States needs to decide if it is going to stick with EDGE or make the complete commitment to 3G. The security issues facing 3G are no different than the computer community has face before. The difference is that the designers and manufacturers of the standards and hardware have the opportunity to design and construct the 3G system with security in theforefront.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References:

United States Government Accounting Office, Defense Spectrum Management: More Analysis Needed to Support Spectrum Use Decisions for the 1755 – 1850 MHz Band. August 2001
http://www.gao.gov

Nathan J. Muller, Bluetooth Demystified. McGraw-Hill Telecom. 326 – 336
http://www.privateline.com/Bluetooth/Relation.pdf

Knight, Will, "3G: Will 3G Devices be Secure?". Zdnet, 23 August, 2000.
http://news.zdnet.co.uk/story/0,,s2080988,00.html

Buckingham, Simon, "3GSM: The Future of Comunications". GSM World, 20 June, 2001
http://www.gsmworld.com/technology/3g_intro.html#3

Zeichick, Alan, "3G Wireless Explained". Red Herring, 01 September, 2000
http://www.redherring.com/index.asp?layout=story&channel=70000007&doc_id=1010013701

Gutzman, Alexis D., "The Who, What and Why of WAP". Ecommerce-guide.com, 26 May, 2000
http://ecommerce.internet.com/news/insights/ectech/article/0,,10378_381271,00.html

Motorola, "Wireless Internet Network Communications Architecture". International Engineering Consortium.
http://www.iec.org/online/tutorials/winternet/index.html

© SANS Institute 2001, Author retains full rights

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**