GOLDLOCK™
Gold Line Group Ltd

Gold Lock Enterprise™

White Paper

Military Grade Protection Using Gold Lock Enterprise™

White Paper

Hybrid Secure Telephone Encryption: The Best of Both Worlds

In today's global information-based economy, the ability to communicate confidential information securely is an absolute business necessity. Advances in technology have enabled instantaneous, reliable transmission of voice and data. However, secure telecommunications has remained a challenge. Until quite recently, the technology used to encode communications so that only the intended recipient can understand it – called cryptography – has lagged behind the capabilities of clever codebreakers. In the last few decades, codes based on "trapdoor" mathematical functions[1] – functions that are easy to calculate, but hard to invert – have made highly secure communications possible. Indeed, today's encryption methods are far more secure than the abilities of codebreakers to decrypt messages.

This document will present an overview of the following topics:

- Corporate espionage as it relates to mobile devices
- The history of secure phones
- Internet-based telecommunications technologies (Voice over
- Internet Protocol, or VoIP)
- Threats against secure mobile telecommunications
- Cryptographic methods used in mobile telecommunications today

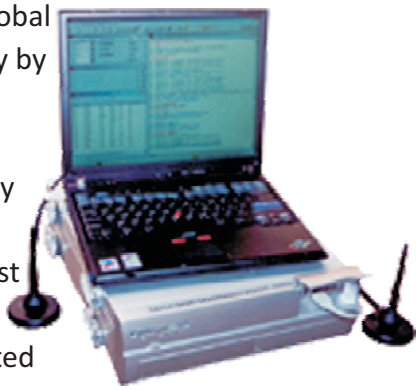
This document is not intended as a technical or mathematical treatment of cryptography, although references are provided for those interested in the subject. Instead, it discusses business requirements for secure wireless communications, and the optimal solutions that meet these requirements. A brief overview of cryptography will show that there have been two primary types of systems, referred to as asymmetric and symmetric. Each type of system has advantages and disadvantages. This paper will demonstrate that a hybrid system is the ideal implementation of wireless cryptography. Such a system combines powerful asymmetric and symmetric cryptography technologies, taking advantage of the strengths of each type.

Corporate Espionage: A Very Real Threat

Information theft is a multibillion-dollar industry, and corporate information security experts estimate that it is on the increase. According to a 2007 study sponsored by the ASIS Foundation and the Office of the National Counterintelligence Executive, "It is most likely inevitable that your organization's information assets will be targeted for compromise or infringement when doing business in a global market. If an organization's information assets are unprotected or underprotected, that organization may risk loss of control, use, or ownership of some of its intellectual property rights at some point in any business relationship. The challenge is to develop a security strategy that identifies, assesses, and addresses risks, and enables business transactions in a global market."[2]

It is most likely inevitable that your organization's information assets will be targeted for compromise or infringement when doing business in a global market.

Trends in Proprietary Information Loss, ASIS Foundation/Office of the National Counterintelligence Executive



One of the greatest security dangers for United States-based global businesses comes from an assumption that other countries play by the same rules. In fact, corrupt police and government officials often engage in or facilitate corporate espionage in developing nations. In these countries, laws against wiretaps are frequently disregarded, if they exist at all. Corporations that have development or manufacturing activities in these countries must be aware of the risks. Furthermore, the widespread availability of espionage tools makes businesses vulnerable within the United States. These tools, while they may be illegal in the United States, are easily obtained online.

Information technology professionals recognize encryption as the key weapon against espionage agents who attack corporations by attempting to intercept their mobile telecommunications. In a 2006 survey, 88% of 426 respondents, representing IT organizations worldwide, said they know that large amounts of personally identifying and other sensitive information reside on employee's mobile devices. Seventy-two percent of the respondents said that encryption is required to protect personal identifiable information.[3]

Yet less than 20% of the respondents in the survey said they had implemented encryption. When asked to identify the top three reasons why encryption, considered the primary data privacy and protection option, was not implemented, 56% of the respondents cited lack of funding; 51% said that encryption was not an executive priority; and 50% said that limited IT resources was an obstacle.

Wireless Communications Security B.V. (Before VoIP)

Voice Scrambling

One of the earliest attempts to encrypt telecommunications took place in the 1920s. The encrypting device combined a "noise" signal with the audio message before transmission. The receiver, who knew how to duplicate the "noise" signal, would use this information to remove the noise from the transmission to obtain the original message. This technique was quickly broken. A more advanced, related method called "A-3" was developed in 1939, but the Germans succeeded in deciphering messages sent using A-3.

Sigsaly

This was the first secure telephone, developed at Bell Labs in the 1940s. Not only did it successfully communicate top-secret information, including the Allied plans for the 1944 Normandy invasion – but it pioneered several important communications technologies. The disadvantage of Sigsaly was that it weighed over 50 tons and used 30kW of power. The United States government only built about a dozen of these incredibly costly units. One unit, mounted on a ship, followed General Douglas McArthur throughout his campaign in the South Pacific – the first secure mobile phone.

STU

The STU-I phone, a secure desk telephone designed for use by the United States government and its contractors, first appeared in 1970. Its successor, the STU-II, replaced the STU-I in 1975. The STU-III came out in 1987, and was one of the first applications of asymmetric cryptography, discussed below.
Little information is available regarding the STU phones because the United States government still uses them for secure government telecommunications. However, the Department of Defense is already

transitioning to VoIP phones for secure communications. Eventually, VoIP phones, which offer superior call quality and other advantages, will replace all the STU phones.

Internet-Based Mobile Communications Technologies

Internet Protocols

Before looking at security issues, we will briefly discuss the technologies used to transmit voice (audio) and data using the Internet. These technologies are referred to as VoIP (Voice over Internet Protocol). Phones with this capability are called VoIP phones; they are also known as broadband phones or internet phones.

The Internet uses several standardized communication technologies called protocols. Every communication over the Internet uses several protocols, each with a different function. The protocols that are most important in VoIP are IP, UDP, and RTP, explained below.

IP is the Internet Protocol. The most important function of IP is to append the address (IP address) of the source and destination computers to the transmitted information. In addition, IP breaks the information up into smaller pieces called datagrams, or "packets." The packets will be reassembled in the proper sequence when they reach the destination.[4]

UDP is the User Datagram Protocol. It enables connectivity within the network by transporting the diagrams from the network infrastructure and delivering them to an application, as well as the reverse process.[5]

RTP, the Real-time Transport Protocol, is used to sequence outgoing packets and reconstruct incoming packets in the correct order.[6]

Network Address Translation (NAT) and NAT Traversal

For purposes of setting up a secure connection, it is best when the parties to the communication have a direct connection and "see" each other. However, sometimes the communications are routed through a gateway. The reason for this is that because of the huge number of Internet users, we are running out of IP addresses using our current address assignment system. Until we can transition to a new assignment system, a solution to this problem has been to allow organizations with multiple users to have one public IP address (the gateway connection), then create their own private addresses within the organization. This is known as Network ddress Translation (NAT). When possible, it is generally desirable to bypass the gateway using a process called NAT traversal. NAT traversal essentially convinces the NAT gateway that the traffic is passing through it, while establishing a direct connection between the parties to the communication.[7]

Wireless Networking Technology Standards

VoIP communications between mobile devices may be transmitted using either Wi-Fi or public GSM networks. Wireless communications have evolved from their analog beginnings to digital technology, then to a broadband, high-speed technology. With each generation, data transmissions become faster and more secure.

Wi-Fi is the technology used by wireless devices that implement the IEEE 802.11 standards.[8] It works mainly over short distances, but at very high speeds. Although Wi-Fi devices have limited range, they can work anywhere in the world. They also consume power rapidly. Wi-Fi is primarily intended for data transfer, rather than voice communications.

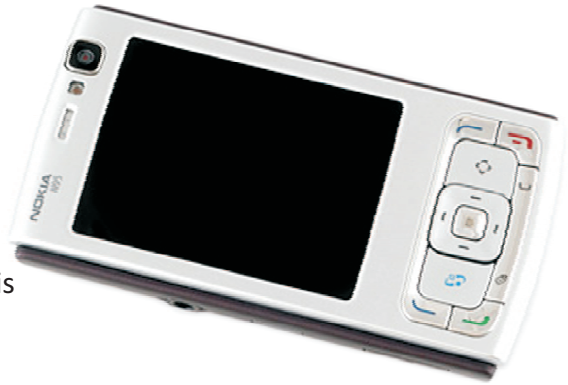
The original digital standards for mobile communications used two primary technologies for allowing multiple parties to share a single channel. The digital standards were dubbed 2G (second generation). One 2G standard, based on time division multiple access (TDMA) was known as GSM. This technology still dominates the global mobile device market.[9] TDMA is like having several people in the same room, taking turns speaking. The other significant 2G standard, IS-95 (also known as cdmaOne), used code division multiple access (CDMA), which can be compared to a roomful of people conversing in different languages.

Two major developments took place before the transition to broadband speeds that would be called 3G. The first was the addition of packet switching capabilities, or General Packet Radio Service (GPRS) to GSM.

This feature increased the speed of data transfer by a factor of 6 to 12. The second extension of GSM, Enhanced Data rates for GSM Evolution (EDGE) would effectively triple data rates. GPRS and EDGE technologies are often referred to as 2.5G and 2.75G respectively. Meanwhile, a 2.5G/3G CDMA technology, CDMA2000, was also developed.

The third-generation (3G) Universal Mobile Telecommunications System (UMTS) significantly increases both the voice and data transfer capabilities of mobile devices.[11] This technology uses wideband, or asynchronous, code division multiple access (W-CDMA) to achieve higher speeds and support more users. UMTS also closes a hole in the GSM security model by requiring mutual authentication between network and user. GSM only requires authentication by the user to the network.

The Secure Telecommunications Challenge



VoIP is already the clear successor to the public switched telephone network (PSTN). The next generation of wireless communications (4G), which will be fully IP-based and capable of transmitting data securely at between 100 Mbits/s and 1Gbit/s, is already on the horizon.[12]

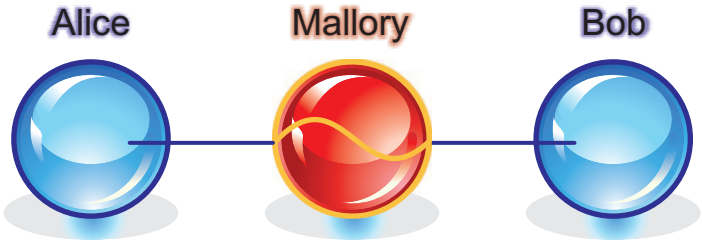
There are certainly benefits to VoIP for businesses.[13] It is already significantly cheaper, and offers more features, than PSTN. PSTN still offers better call quality, but the gap is narrowing rapidly, and the day is surely near when VoIP will provide greater clarity as well.

"While secure phones never made much impact in the PSTN market, the need for encryption for VoIP phones is obvious."

Philip Zimmerman
Creator of PGP (Pretty Good Privacy)

However, new security challenges accompany the increasing importance of VoIP in corporate communications.[14] "[V]oice over IP is about to take over all our phone calls in the next few years," Philip Zimmerman, creator of PGP (Pretty Good Privacy, a privacy software program) told VON magazine in 2007. "While historically the PSTN (Public Switched Telephone Network) calls were sent over a closed circuit between the two parties, VoIP calls are sent over the Internet, a packet switched network, which allows much greater opportunities for interception," Zimmerman said. "While secure phones never made much impact in the PSTN market, the need for encryption for VoIP phones is obvious."[15]

There are three main types of methods, or attacks, used in corporate espionage to gain unauthorized access to confidential information transmitted using VoIP.



Man in the Middle Attacks

A man-in-the-middle (MITM) attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.[16] The attacker records, and can even change, the content of the interaction. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances. "The potential for man-in-the-middle attacks with a mobile is huge," Mike Hawkes, director of mobile security at the Mobile Data Association, told Secure Computing Magazine in a 2007 interview. "The current trend among operators to move from large GSM transmitters to smaller Pico cells means that something the size of a briefcase can be a fully-functioning GSM cell, only it's monitoring all through-traffic," Hawkes explained. "GSM phones are designed to be connected to and roam seamlessly between the nearest and strongest signal, so you wouldn't notice anything wrong."[17] Before a communications channel is secured, MITM is a meaningful threat to VoIP security. However, complementary security protections, used in conjunction with public-key cryptography techniques, can thwart MITM attacks.

"The potential for man-in-the-middle attacks with a mobile is huge."

Mike Hawkes, Director of Mobile Security, Mobile Data Association

Brute Force Attacks

A brute force attack consists of trying every possible code until the attacker finds the correct code. This requires not only testing a huge number of possibilities (statistically, half the number of possible codes), but also the ability to recognize when the correct code has been guessed. Because of the size of the keys used in VoIP cryptography systems today, and the ephemeral nature of the keys, this is generally not considered a meaningful threat. However, the exponential growth rate of computer processing capabilities requires responsible designers of secure systems to provide protection that far exceeds the current security threshold. As an example, a leading cryptographer offered a prize in 1977

If A wants to send a message to B, A uses B's public key (which can be made available to anyone without compromising the security of the system) to encrypt the message. B then decrypts the message using B's private key, which only B knows.

Whitfield Diffie and Martin Hellman published the first practical method of asymmetric cryptography in 1976.[20] Their method, known as Diffie-Hellman key exchange, is still important in modern cryptography. The following year, three cryptographers at MIT developed a method based on the difficulty of factoring the product of very large prime numbers.[21] Their method, RSA, is still the most widely used method of asymmetric cryptography.

A third method, known as Elliptic Curve Cryptography (ECC) was developed in 1985 independently by Neil Miller and Victor Koblitz.[22] ECC depends on a more complex and difficult mathematical problem called the elliptical discrete logarithm problem. The practical result of this difference in complexity is that significantly smaller keys can be used with ECC to achieve the same level of security as a RSA-based system.[23] ECC is also more resistant to decryption. ECC was quickly recognized by cryptographers as possessing efficiency and security advantages over RSA, and subsequent attempts to find weaknesses in the method were unsuccessful. However, RSA was firmly established in the market for secure communications devices, and ECC has only recently gained a meaningful foothold.

Symmetric Cryptography

Symmetric cryptography uses identical or similar keys for both the encryption and decryption process. An early symmetric cipher, the Data Encryption Standard (DES), was implemented in 1977.[24] DES was controversial from the beginning because it used a relatively short key (56 bits) and was suspected of being vulnerable to a backdoor attack by the National Security Agency (NSA). By 1997, a DES key had been decrypted; by 1998, it was possible to determine a DES key using brute force methods in just two days.[25] DES is no longer considered a secure encryption standard.

In 1993, when it was already clear that the key size used by DES was insufficient, a related symmetric encryption algorithm, Blowfish, was developed. Twofish, the second generation of Blowfish, was first published in 1998, and used variable-length keys from 128 to 256 bits.[26] However, when the National Institute of Standards and Technology (NIST) announced a competition for the successor to DES that would be used to protect sensitive government information, an algorithm called Rijndael emerged victorious. Rijndael was rebranded as the Advanced Encryption Standard (AES) and is now the dominant symmetric cryptographic standard.[27]

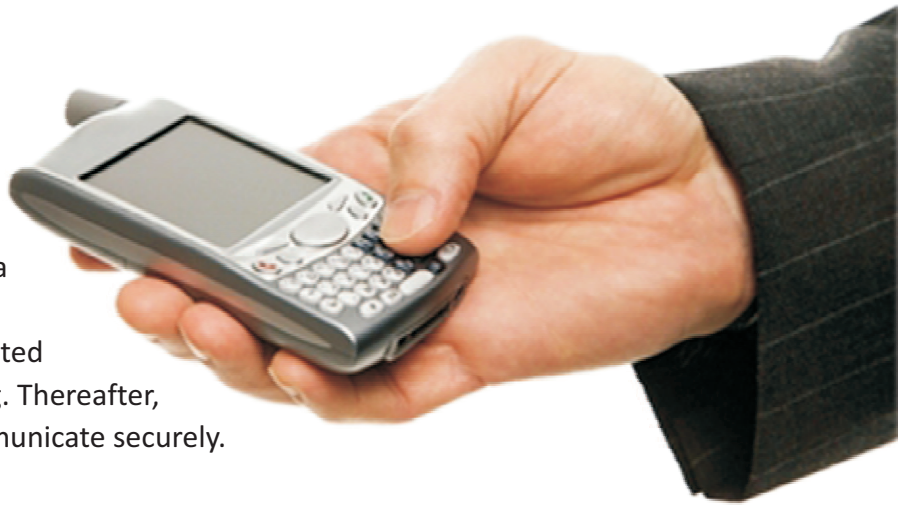
for anyone who could break his code. He estimated that it would take 40 quadrillion years to decipher the coded message. In 1993, using faster computers and improved computational methods, the code was broken.[18]

Side Channel Attacks

Side channel attacks are non-cryptographic attacks, based on information that can be retrieved from the device that is neither the text to be encrypted nor the text resulting from the encryption process.[19] Devices using encryption often have additional output and input. For example, a mobile telecommunications device produces timing information (information about the time that operations take) that is easily measureable; radiation of various sorts; power consumption statistics (that can be easily measured as well), and more. Side channel attacks make use of some or all of this information, along with other cryptanalytic techniques, to recover the key the device is using. However, a well-designed, properly implemented secure phone system will minimize the vulnerability of the device to such attacks.

Modern Cryptography: Effective Weapons against Corporate Spies

Asymmetric Cryptography



Prior to the invention of asymmetric cryptography, encrypted communications depended on the parties to the communication sharing a secret code, or key. The parties would normally exchange the key using a trusted method such as a face-to-face meeting. Thereafter, the key holders would be able to communicate securely.

Asymmetric cryptography, also known as public-key cryptography, is so called because the key used to encrypt the message is not the same as the key used to decrypt it. Each party to the communication has two keys – a public key and a private key. The keys are mathematically related, but it is computationally infeasible to derive the private key from the public key. This means that while an attacker can derive the key given unlimited time and resources, the attacker is unlikely to break the code within a finite period.

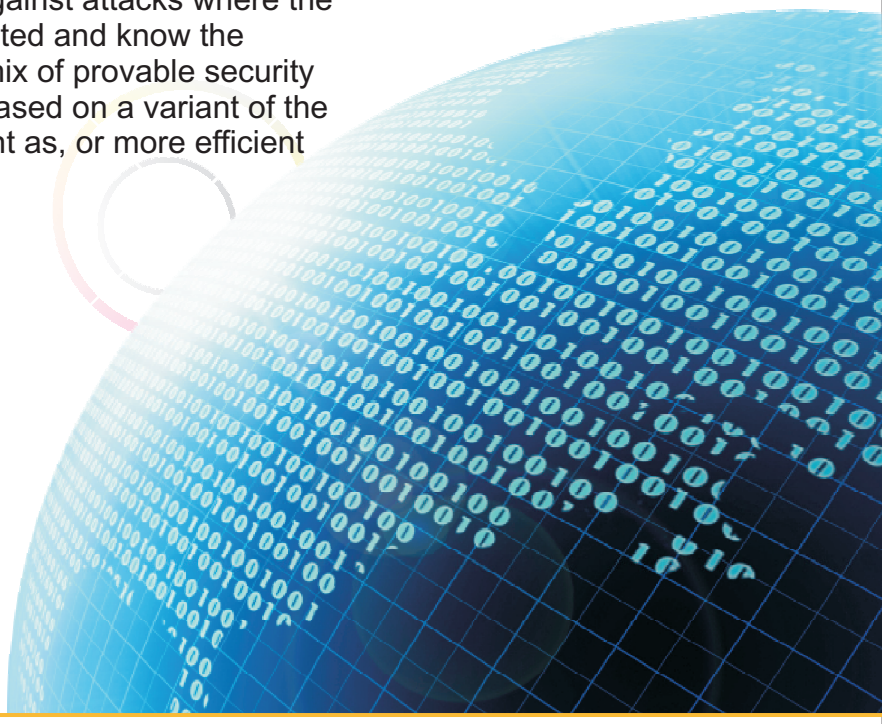
Asymmetric vs. Symmetric

The obvious advantage of asymmetric cryptography over symmetric cryptography is that the parties need not meet face to face, or rely on a possibly insecure third party (such as a postal system or Internet Service Provider) to communicate a shared key. Such meetings may be realistic when the number of parties who will need to communicate is relatively small. However, global business communications require that thousands of people be able to communicate rapidly, sometimes before a secure key exchange can be arranged.

The advantage of symmetric cryptography is in its speed. In practice, symmetric cryptographic methods are hundreds to thousands of times faster than their comparably secure asymmetric counterparts. In modern telecommunications, where very large quantities of data must be transmitted at very high bandwidth rates, computational speed is an important consideration.

Hybrid Cryptographic Technologies

The solution to the problem of secure mobile telephone communications lies in the adoption of hybrid cryptographic technologies. This enables public key exchange, a virtual necessity in the global business environment, while taking advantage of the computational efficiencies of symmetric key cryptography. One such hybrid system is the Elliptic Curve Integrated Encryption Scheme (ECIES).[28] ECIES is an implementation of Elliptic Curve Cryptography based on ECC that uses Diffie-Hellman-type key exchange and a message authentication code (MAC) for key encapsulation, coupled with a symmetric encryption scheme for data encapsulation. ECIES is designed to be semantically secure against attacks where the adversary can select text to be encrypted and know the encrypted text. It offers an attractive mix of provable security and efficiency. It was proven secure based on a variant of the Diffie-Hellman problem. It is as efficient as, or more efficient than, comparable schemes.



Gold Lock

Gold Lock Enterprise implements ECIES using ECC-256 (based on a modified Diffie-Hellman algorithm) and SHA-256 to verify key integrity, together with XOR as the data encryption technology. XOR is a symmetric-key algorithm that by itself is easily broken, but in combination with the other ECIES technologies is impervious to attack. It has the advantage of requiring limited computational resources. Each component of the Gold Lock Enterprise solution is tested and proven secure against any conceivable attack. The Israeli government (Ministry od Defense) has certified Gold Lock Enterprise™, and its manufacturer Gold Lone Group Ltd.. Gold Lock uses another hybrid encryption technology as well, namely Diffie-Hellman key exchange in combination with AES-256. The encryption scheme that Gold Lock uses at any time optimizes both security and resource utilization.

In addition to these encryption schemes, Gold Lock doesn't just select a single private key – it creates 16384 randomly generated keys each time you register your device, a process that can be repeated at any time. Gold Lock randomly chooses one key from these 16384 keys each time you initialize a call. In addition, on each call, each phone displays a randomly generated 5-digit number. This number is NEVER transmitted over the network. Voice authentication of the number confirms that there is no interceptor on the line trying to launch a man in the middle attack. Furthermore, Gold Lock offers a unique monthly subscription model. This ensures that we will always keep our technologies on top of the latest security threats and compatible with the newest phone models. We use a proprietary audio codec that compresses voice signals with the lowest latency (delay) and the highest audio quality. In addition, you don't have to worry about security issues when you roam or travel internationally. Gold Lock secures your mobile communications no matter where you are.

For more information about Gold Lock Enterprise, call our corporate headquarters at +972 8935 2335 (Israel), or visit our website: www.gold-lock.com.

References (all websites accessed 3 Mar. 2009)

[1] A. C. Yao, "Theory and Application of Trapdoor Functions," 23rd Annual Symposium on Foundations of Computer Science, pp. 80-91, 1982. <http://ufr6.univ-paris8.fr/maths/phan/secuproofs/yao82.pdf>

[2] "Trends in Proprietary Information Loss: Survey Report," ASIS International and the National Counterintelligence Executive, p. 25, Aug. 2007. <http://www.asisonline.org/newsroom/surveys/spi2.pdf>

[3] "Survey says? Consumer Data Breaches Will Get Worse," Credant Technologies, 26 Sept. 2006. <http://www.credant.com/survey-says-consumer-data-breaches-will-get-worse-stolen-unsecured-laptops-and-all-mobile-devices.html>

[4]"Protocol:IP," Protocolbase.net, 9 Dec. 2005. <http://www.protocolbase.net/protocols/protocol_IP.php>

[5]"Protocol:UDP," Protocolbase.net, 11 Mar. 2005. <http://www.protocolbase.net/protocols/protocol_UDP.php>

[6]"Protocol:RTP," Protocolbase.net, 26 Feb. 2007. <http://www.protocolbase.net/protocols/protocol_RTP.php>

[7]"NAT Traversal for VoIP and Internet Communications using STUN, TURN and ICE," Eyeball.com, <http://www.eyeball.com/technology/whitepapers/EyeballAnyfirewallWhitePaper.pdf>

[8]C. Waxer, "The 411 on Wifi VoIP Phones," VoIP News, 19 Feb. 2008. <http://www.voip-news.com/feature/wifi-voip-phones-021908/>

[9]E. Mills, "Cell phone, VoIP technologies lack security, experts say," CNET, 17 May 2008. <http://news.cnet.com/8301-10784_3-9946665-7.html>

[10]"EDGE: Introduction of high-speed data in GSM/GPRS networks," Ericsson, 2005 <http://www.ericsson.com/solutions/tems/library/tech_papers/tech_related/edge_wp_technical.pdf>

[11]N. Lewis, "VoIP Over 3G Wireless Gets Real," VoIP News, 22 Jan. 2008. <http://www.voip-news.com/feature/VoIP-Over-3G-012208/>

[12]S. Alfredsson, A. Brunstrom and M. Sternad, "Impact of 4G Wireless Link Configurations on VoIP Network Performance," IEEE International Symposium on Wireless Communication Systems, 21-24 Oct. 2008. <http://www.signal.uu.se/Publications/pdf/c0804.pdf>

[13]A. Schecter, "Mobile VoIP Means Business," ZDNet.co.uk, 03 Jan 2007. <http://resources.zdnet.co.uk/articles/comment/0,1000002985,39285315,00.htm>

[14]U.S. Dept. of Commerce/National Institute of Standards and Technology, "Security Considerations for Voice Over IP Systems," Special Publication 800-58, Jan. 2005. <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>

[15]J. Pulver, "Philip R. Zimmerman: Creator of Pretty Good Privacy," VON Magazine, pp. 14-19, Jan. 2007. <http://www.vonmag-digital.com/vonmag/200701/>

[16]A. Schonewille and B. Eenink. RP2:VoIP/SIP Man in the Middle attack Proof of Concept," University of Amsterdam, 28 June 2006.
<https://alumni.os3.nl/~talitwan/RP2/SIP_mitm.pdf>

[17]P. Love, "Mobile security: when will it become necessary?" Secure Computing Magazine, 11 April 2007.
<http://www.securecomputing.net.au/Feature/77883,mobile-security-when-will-it-become-necessary.aspx>

[18]D. Arkins, M. Graff, A.J. Lenstra, and P.C. Leyland, "The Magic Words Are Squeamish Ossifrage," Advances in Cryptology Asiacrypt '96, pp. 263-77, 1995.
<http://www.mit.edu:8001/people/warlord/rsa129.ps>

[19]H. Bar-El, "Introduction to Side Channel Attacks," Discretix.com
<http://www.discretix.com/PDF/Introduction%20to%20Side%20Channel%20Attacks.pdf>

[20]W.Diffie and M.E.Hellman, "New Directions in Cryptography," IEEE Trans. Inform. Theory, IT-22, 6, 1976, pp. 644-654.
<http://www.cs.berkeley.edu/~christos/classics/diffiehellman.pdf>

[21]R.L. Rivest, A. Shamir, and L.M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, Feb. 1978.
<http://people.csail.mit.edu/rivest/Rsapaper.pdf>

[22]"Elliptic Curve Cryptography (ECC)," Certicom, 2008.
<http://www.certicom.com/index.php/ecc>

[23]"The Case for Elliptic Curve Cryptography," National Security Agency/Central Security Service, 15 Jan. 2009.
<http://www.nsa.gov/business/programs/elliptic_curve.shtml>

[24]U.S. Dept. of Commerce/National Institute of Standards and Technology, "Data Encryption Standard (DES)," FIPS Pub. 46-3, 25 Oct. 1999
<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>

[25]"Frequently Asked Questions (FAQ) About the Electronic Frontier Foundation's 'DES Cracker' Machine," The Electronic Frontier Foundation, 16 July 1998.
<http://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html>

[26]B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Twofish: A 128-Bit Block Cipher," NIST AES Proposal, 15 June 1998.
<http://www.schneier.com/paper-twofish-paper.pdf>

[27]U.S. Dept. of Commerce/National Institute of Standards and Technology, "Announcing the Advanced Encryption Standard (AES)," FIPS Pub. 197, 26 Nov. 2001
<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

[28]V. Shoup, "A Proposal for an ISO Standard for Public Key Encryption (version. 2.1)," 20 Dec. 2001.
<http://shoup.net/papers/iso-2_1.pdf>

Gold Line Group Ltd. (Israel)
Mobile Security Division

Corporate Headquarters
Tel: +972 8935 2335
Fax: +972 8935 2335

Meginei Hagalil 5
Rehovot, 76200
Israel
Time Zone: EET = East-European time = GMT+2 Hours