GSM AND GPRS PERFORMANCE OF IPSEC DATA COMMUNICATION

Gianluigi Me, Giuseppe F. Italiano
Dipartimento di Informatica, Sistemi e Produzione,Roma,Italy

Paolo Spagnoletti
CeRSI, LUISS "Guido Carli" University,via Tommasini 1, Roma,Italy

Keywords: Mobile application, Security

Abstract: Cellular Internet services must grapple with the added security threats posed by the radio transmission, open to eavesdropping. Furthermore, the combination of always-on connectivity and an interface to the public Internet means high speed data services has to cope with the same security issues that can be found in the wired environment.Confidentiality of GSM/GPRS communications has been provided only in BS-ME/GGSN-ME by COMP128/GEA+ algorithms, whose strength is often not believed adequate for corporate/governmental requirements. Furthermore, A5/1 and A5/2 algorithms have been recently attacked with real time ciphertext only cryptanalysis by Barkan, Biham and Keller. To provide an adequate level of security, it is often argued to employ IPSec over the GSM/GPRS framework. We provide experimental evidences that IPSec is a viable solution to provide the desired level of security. In particular, the overhead generated is tolerable where high sensitive/critical communications take place. We expect that our findings could help better understanding how securing a deployed GSM/GPRS network which corporate/governmental infrastructures can rely on and what performances can be expected by using IPsec over these media.

1 INTRODUCTION

Wireless technology is widespread in today's communication networks, mainly due to its facility of deployment and management. However, many security concerns about wireless infrastructures have been raised in recent years. In particular, there has been a serious consciousness of the weaknesses of GSM and GPRS, among other wireless technologies. Important works on this area are by Barkan et al. 0, Biryukov et al. 0, Briceno et al. 0 and Ekhdal et al. 0, whose pose serious threats to GSM/GPRS, with high-cost/easy to use systems. Furthermore GSM is the most widely used cellular technology, with more than 787.5 million customers in over 191 countries.
All these facts make these two technologies highly insecure and untrustable for who has to communicate with confidentiality and suggested us to propose a secure architecture for people/corporate/government with security requirements. In this paper, we analyze the overhead introduced to secure GSM/GPRS communication. In particular, we investigate the performance of the IPSec protocol employed to secure communication over GSM/GPRS. We show with experimental results that for a wide range of parameters, the overhead introduced by the IPSec is limited. Hence, we experimentally argue that the adoption of the IPSec suite is a viable solution to secure public GPRS network infrastructure.
The remainder of the paper is organized as follows: firstly a security background, where we briefly highlight the security features and the threats to which the GSM/GPRS is subject to. Then, we detail our security architecture implementation, focusing on relevant IPSEC countermeasures to GSM/GPRS threats. Finally we develop our consideration on IPSec encryption over GSM/GPRS. In particular, we will illustrate the methodology adopted to perform the measurement and the result of our analysis, based on a wide range of experiment that have been carried out, varying different, sensitive parameters

Me G., F. Italiano G. and Spagnoletti P. (2004).
GSM AND GPRS PERFORMANCE OF IPSEC DATA COMMUNICATION .
In *Proceedings of the First International Conference on E-Business and Telecommunication Networks*, pages 3-11
DOI: 10.5220/0001384600030011
Copyright © SciTePress

of interest of the IPSec suite and the type of traffic secured.

2 GSM/GPRS STANDARD SECURITY

The Global System for Mobile Communications (GSM) (Figure 1) security was designed with three constraints in mind 0: α) Concern of granting too much security and so bringing export problems upon GSM; β) GSM did not have to be resistant to active attacks where the attacker interferes with the operation of the system, perhaps masquerading as a system entity; and γ) The trust between operators for the security operation should be minimized. The use of air interface at the transmission media allows a number of potential threats from eavesdropping. As stated by 0, it was soon apparent in the threat analysis that the weakest part of the system was the radio path, as this can be easily intercepted. In fact, there was no attempt to provide security on the fixed network part of GSM.

The General Packet Radio Service (GPRS) is a GSM-based service which provides mobile users with true packet access to data network. GPRS uses a packet-mode technique to transfer high-speed and low-speed data and signaling in an efficient manner 0. Security in GPRS is largely based on the GSM system security function. The main entities involved are the SGSN (Serving GPRS Support Node), GGSN (Gateway GPRS Support Node), AuC (Authentication Center) and HLR (Home Location Register). The HLR and AuC provide the same functionality as in GSM. The SGSN and GGSN both take care of authentication (Figure 1). The main functions related to GPRS device (MS) are authentication and encryption.

The authentication in GSM systems happens in VLR (Visitor Location Register) or HLR 0, through an Authentication Key (Ki) 0 stored in the AuC of the home PLMN (Public Land Mobile Network), using A3 (0, 0) algorithm. The operators may be free to design their own A3 algorithm.

Nearly every GSM operator in the world uses an algorithm called COMP128 for both A3 (authentication) and A8 (key generation) algorithms 0. The GPRS authentication procedure is handled in the same way as in GSM with the distinction that the procedures are executed in the SGSN. In some cases, the SGSN requests the pairs for a MS from the HLR/AuC corresponding to the IMSI of the MS. The GSM voice calls are encrypted using a family of algorithms collectively called A5. A5/0 uses no encryption. A5/1 is the "standard"-export limited encryption algorithm, while A5/2 is the "export" (weakened) algorithm. A5/3 is a new algorithm based on the UMTS/WCDMA algorithm Kasumi 0. In GPRS network the ciphering scope is different: in GSM the scope is between BTS (Base Transceiver Station) and MS, in GPRS the scope is from the SGSN to the MS. The GPRS ciphering, performed at the LLC layer, is done with a family of algorithms: GEA0 (none), GEA1 (export), GEA2 (normal strength) and GEA3 (new, and effectively the same as A5/3).

2.1 GSM/GPRS authentication algorithms vulnerabilities.

The protocol is simple, however, there are some vulnerabilities posed by its use. Namely, the TMSIs (Temporary Mobile Subscriber Identity) are generated based on the previous TMSI, therefore a missed synchronization in the TMSIs may require the IMSI to be used to set up it again, wherein the IMSI is sent in plaintext to the VLR, exposing its true identity. Also, there is no mechanism to prevent reply attacks. Once the session key Kc is compromised, by playing back the RAND, and the SRES, an intruder can impersonate the VLR since the protocol does not support network authentication.

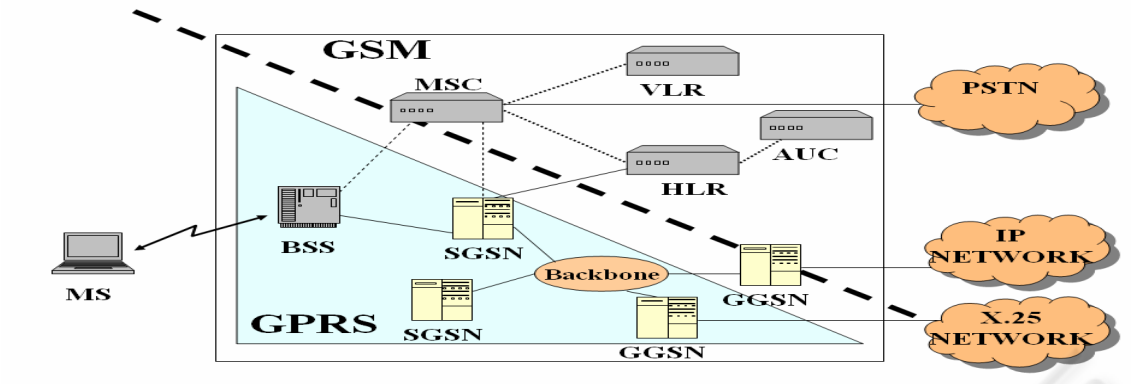

Figure 1

Furthermore,
- Wagner and Goldberg announced in April 1998 that they had cracked COMP128 who had a weakness which would allow complete knowledge of Ki if around 160000 chosen RAND-SRES pairs could be collected (chosen plaintext attack). There are active attacks that can be used to obtain these pairs.
- The quickest attack would be to steal the user's mobile phone, remove the SIM and connect it to a phone emulator that can be used to send 160 000 chosen RAND to the SIM and receive the SRES. SIM tend to have relatively slow clock speeds and it can therefore take up to 10 hours to obtain the 160000 pairs (with faster SIM, it would take 2 and a half hours).
- Retrieving the key from the SIM: the security of the whole GSM/GPRS security model is based on the secret Ki. If this key is compromised the whole account is compromised. Once the attacker is able to retrieve the Ki, he can not only listen to the subscribers calls, but also place calls billed to the original subscriber's account, because he can now impersonate the legitimate subscriber.
- Another method is to perform man in the middle attacks. Using a false BTS to send the RAND over the air interface, the rate at which pairs can be collected is slower and would take a number of days; however the attacker does not need physical possession of the SIM. After these efforts, the attacker has the Ki and can masquerade as the user and run calls on his bill, and also determine the Kc for the user's calls and therefore eavesdrop upon them 0;
- Cloning attack to A3 is further presented in 0.

The following attacks represent threats for authentication in GPRS:
- Spoofed Create PDP (Packet Data Protocol) Context Request: GTP (GPRS Tunnelling Protocol) inherently provides no authentication for the SGSNs and GGSNs themselves. This means that given the appropriate information of a subscriber, an attacker with access to the GRX (GPRS Roaming Exchange), another operator attached to the GRX, or a malicious insider can potentially create their own bogus SGSN and create a GTP tunnel to the GGSN of a subscriber. They can then pretend to be the legitimate subscriber when they are not. This can result in an operator providing illegitimate Internet access or possibly unauthorized access to the network of a corporate customer;
- Spoofed Update PDP Context Request: An attacker can use their own SGSN or a compromised SGSN to send an Update PDP Context Request to an SGSN, which is handling an existing GTP session. The attacker can then insert their own SGSN into the GTP session and hijack the data connection of the subscriber.

2.2 GSM/GPRS confidentiality algorithms vulnerabilities

The confidentiality of the GSM architecture is not completely sound. In the following we highlight a few security flows that have been published in literature. Our aim is not to discuss the GSM architecture nor its cryptographic flaws, but only showing that the native confidentiality it provides is weak, thus justifying the adoption on another independent security layer, as IPSec is. Furthermore, the security of the GSM confidentiality is based on the security through obscurity paradigm, debatable choice and usually leads, sooner or later, to system compromising 0.In the following paragraphs, we overview the main known attacks, paying the best attention to 0:
- Brute-force attack against A5. A real-time brute-force attack against the GSM security system is not feasible, since the time complexity is far too big, but with the distributed computer systems we can drastically reduce the time required;
- Divide-and-conquer attack against A5 – a divide-and-conquer attack is based on a known-plain-text

attack and can dramatically reduce the complexity (up to 2^9 – 2^14) 0;
- The only attack on an algorithm that has been confirmed to be A5/1 was that by Biryukov and Shamir, later improved by Wagner. The technique used is known as is time-memory trade off 0;
- Accessing the operator's signaling network: the airwaves between the MS and the BTS are not the only vulnerable point in the GSM system. The transmissions are encrypted only between the MS and the BTS. After the BTS, the traffic is transmitted in plain text within the operator's network. If the attacker can access the operator's signaling network, he will be able to listen to everything that is transmitted, including the actual phone call as well as the RAND, SRES and Kc;
- Real time cryptanalysis: the very new result, faced by our proposal architecture for data communication, comes from 0. The coding introduces known linear relationships between the bits to be encrypted; so even though the attacker might not know the values of particular input bits, they know that certain groups of them XOR to 0. So, taking the same groups of encrypted bits and XORing them reveals the corresponding XOR of the keystream bits. This is the fundamental problem that allows the attacks to work without any knowledge at all of what is being encrypted, which is what they mean by "ciphertext only". The important thing about the active attacks is that the attacker can confuse a mobile into doing what it wants the mobile to do. At the limit, if the attacker has intercepted the random challenge sent to a particular mobile and has recorded all the traffic, whether it is GSM voice or GPRS data, they can later send the same random challenge to the mobile and tell it to use A5/2 to communicate. When the mobile responds, they recover the key, and it's the same key that will decrypt the recorded stuff, whatever it was encrypted with.

2.3 How IPSec matches security requirements

In previous paragraphs we have shown the cryptographic vulnerabilities of GSM/GPRS. In this mobile environment we have identified the following requirements, not appropriately covered by GSM/GPRS: (Ra) Protecting sensitive information: assuring the confidentiality and integrity of communications; (Rb) Access Control and Authorization; (Rc) Upper IP layer system availability, to guarantee the best communication media DoS robusteness . Furthermore, we intend to address these specific threats considering that, in the GSM/GPRS framework, performing traffic analysis pose more concerns due to the fact that digital IP based traffic carries source and destination IP addresses in cleartext.
Furthermore, α) this system doesn't face communication parties localization tracing problem, because inherently coupled with GSM/GPRS link layer; β) DoS attacks to GSM/GPRS link layer are out of the requirements scope of this paper.
Our IPSec based architecture matches these requirements as follows:
Ra) Confidentiality of 3DES, the algorithm used in this architecture, is definitively better than A5.
Furthermore it's possible to choose the preferred encryption algorithm in the IPSec suite, e.g. AES. Integrity is performed by HMAC-MD5 (keyed hash) function.
Rb) Authentication is performed combining IPSec preshared-keys (device authentication) and One Time Password (user authentication). This further layer has been needed because preshared key authentication creates a master key that is less secure because of absence of Perfect Forward Secrecy.
Rc) This requirement is matched by using IKE (Internet Key Exchange) in main mode, not aggressive 0.

3 ARCHITECTURAL OVERVIEW

As shown in Figure 2, we used a laptop connected to a Merlin 3+1 GPRS phone (3 downlink, 1 uplink channels) through a serial PPP (point-to point) link to act as a GPRS mobile terminal. We tested this architecture in an operational environment, with an Italian mobile carrier. The firewall acts as VPN concentrator in the architecture, thus establishing an IPSec tunnel (end to end) between the mobile terminal and the firewall inside the laboratory LAN. The sniffer has been placed on a switch connected to the firewall external interface, the firewall internal interface, the authentication and the application server and the router connected by a 2 Mbps E1 with the carrier, observing all the packets exchanged between nodes of the architecture.
In the service provider's backbone network the support of GPRS is done adding two new network elements: the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN).

3.1 Security general overview

The information exchange has been shown in Figure 2. User, after providing three usual pieces of information (User Name, Password, APN) to log into mobile carrier GPRS networks, starts the IPSec tunnel setup phase with the system. An encrypted tunnel mode is adopted, where the IP information and the data are encrypted with a new IP address created and mapped to the IPSEC endpoints. This solution provides the overall highest data privacy 0.
After IPSEC device authentication and encrypted channel establishment, user authentication follows, to guarantee the identity of the person using the IPSEC node. This is because an encrypted session is established between the two devices in different locations. The user authentication mechanism gives the access to origin server application, thus preventing the attacker from accessing the system just stealing the mobile device. The system presented in this paper adopts an authentication schema based on strong two factor, token based schema, requiring two elements to verify an user identity: a physical element in user possession (a hardware keyfob) and a code that only the token owner knows (PIN code).
Furthermore, the static IP address adopted enables a greater level of security on the VPN, since the server can recognize the IP addresses of the clients. A device attempting to connect with an IP address unrecognized by the server would be denied access. NAT, economical further security level, seems a viable solution to the limited number of IP addresses available, by allowing the use of an unregistered IP addresses within the organization.

3.2 Architecture and set-up

Our architectural framework is synthetically detailed in Figure 2. It encompasses the following components:
-*Wireless mobile client*; provided with a COTS wireless mobile laptop running an application with transaction features (BITS IPSec-Telnet over GPRS capability) that provide the set up of an IPSEC ESP tunnel, strong-encrypted user authentication, host access via Telnet capabilities.
-*Firewall/Proxy*, adopting the following standards: IETF IPSec Standard, IETF IKE Standard (ISAKMP/OAKLEY) and NAT. The following services are thus available: Security Association and Key Manager, Policy Storage Service Provider, Policy Relay Service Provider, Internet Key Exchange Service Provider, and IPSec Engine. The authentication relies on the Diffie-Hellman algorithm, used with "pre-shared" keys, Diffie Hellman Group Oakley Default Group 1. The negotiation algorithm is DES-CBC with an explicit Initialization Vector 0 with authenticator HMAC-MD5-96 0;
-*Authentication server*; authenticates the users requiring to connect to the Host gateway;
-*Host gateway*, provides the results of the query to the Host, where application data resides, in a Telnet format;
For these measurements the MTU was set to 1500. When the connection is established, each end set the MSS to 1460 bytes with a window size of 16384 bytes

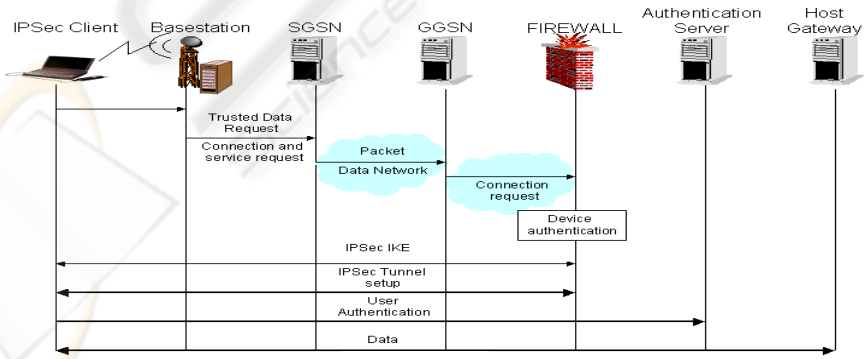

Figure 2

4 MEASUREMENTS METHODOLOGY AND SETTINGS

We analysed general statistics of the transformation made by IPSec, focusing on datagram sizes, basic step for an eavesdropper trying perform statistical cryptanalysis. The following considerations define the test environment:

- Bandwidth variation, changes of the bandwidth available for a connection throughout its lifetime, can represent a major acute problem. In fact, a number of factors may cause the connection's bandwidth variation. Change in the number or activity volume of other connections sharing the same bandwidth resource (e.g. the same time slot/s in GPRS networks), the narrowing/widening of the total bandwidth dedicated to data users (e.g. the start/end of voice calls in GPRS networks), and radio-link optimisations due to SNR changes are significant factors in bandwidth breathing. Failing to properly respond to those changes will result in the transport protocol either under utilizing the scarce wireless bandwidth or overflowing the network. A possible solution for these problems is presented in 0. Because of bandwidth variation our analysis is performed in the same low-traffic hours.
- The reliability in stationary connections is adequate, but the reliability in moving connections, with the same parameters is very poor. Therefore, the reliability of moving connections may create huge problems, if a distributed application cannot cope properly with disconnections or long pauses. This problem hardly relies on GSM/GPRS mobile operator capabilities. For this reason, presented measurements were performed with good to excellent signal coverage, since this threshold is the lowest boundary to enable the transaction, as we further investigate in next paragraph. An isolated, fixed test site was **set-up** to minimize influence from competing Internet traffic taking into account the needs of detailed measurements within lower protocol layers.

In general, in good radio signal quality environment, GPRS provides satisfactory throughput 0. The throughput and round-trip time in stationary connections were stable.

With respect of presented test environment fixed conditions, the analysis has been performed just once.

4.1 Methodology

Basing on GPRS network performance, we are interested in examining the performance of IPSEC over GPRS, evaluating performance and security strength and weaknesses of this solution, inspecting only the Ethernet traffic from two observation points located at the two sides of the firewall (encrypted and clear text).

The measurements refer to entire IP datagram length from LAN and GPRS side: in this architecture, we remark that IPSec works only on LAN IP payload, the LAN IP header is discarded and substituted with the firewall IP header. We did not perform any measurement on air link and we did not change TCP parameters (e.g. RTO, MSS, Congestion Window, SACK) during our measurements. After a general overview of traffic, we isolated traffic, keyed by state, on different channels (GPRS up/down link, LAN up/down link).

The keyed states refer to:

IKE exchange: directly inspectable by sniffing. Here, the main mode accomplish the establishment of ISAKMP SA, performed by IKE and DOI: a secure and authenticated communication channel (IKE SA) and authenticated keys used to provide confidentiality, message integrity, and message source authentication to the IKE communications between UDP exchanging packets on well-known port 500;

Device authentication: Then IPSec SA are established, and other protocol SAs can be negotiated; this phase starts on first ESP packet exchanged and we assume that finishes when the last but one ESP packet before we inspect on LAN traffic the first user authentication string. This assumption is correct as long as no Firewall - Authentication server interaction acts before the last but one ESP packet.

User authentication starts at next packet and finishes when the firewall delivers to the mobile user the ESP packets carrying the initial application form provided by the Host gateway. This form**,** triggering the application query**,** certifies that the user has been authenticated;

Transaction starts at next packet until the end;

Then we mapped this traffic segments on 4 different channels: the GPRS and LAN uplink and downlink as stated in Figure 3.

4.2 Measurements

The goal of our analysis was to compare protocol efficiency in data transfer using a telnet session encrypted with IPSEC on a GSM and a GPRS channel in terms of:

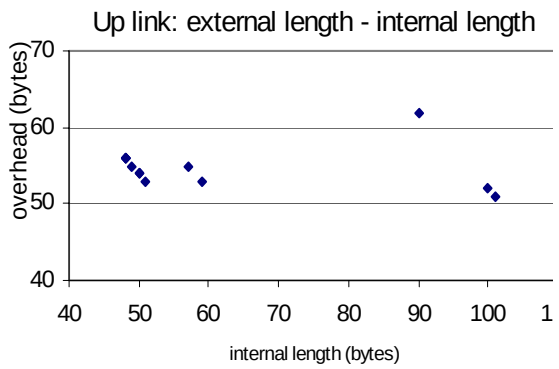

Figure 4a

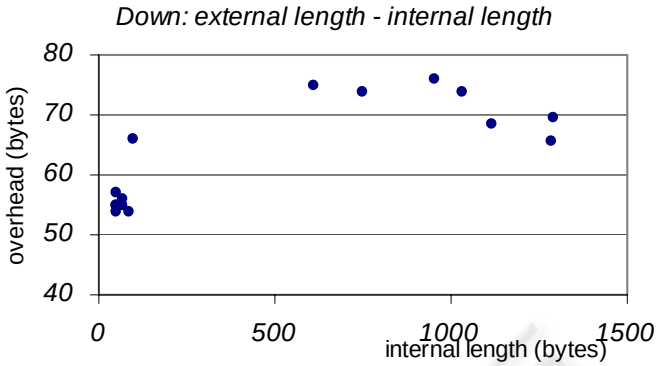

Figure 4b

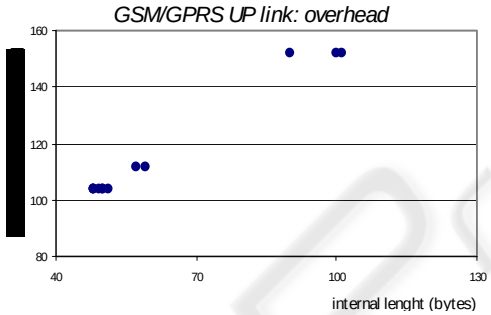

Figure 4c

- overhead and datagram fragmentation;
- time and costs.

Correspondently to all phases of session flow, IP datagram length matches in GSM/GPRS. This first straightforward result confirms the best expected forecast, due to independence of IP layer to the LLC (apart from some spurious "IKE INFORMATIONAL" datagrams). In fact, no re-transmission happened.

We made two complete connection from a MS using GSM and GPRS at the physical layer and we analysed IP datagrams exchanged between MT and External Firewall (EF) and between Internal Firewall (IF) and the Authentication Server (AS) dividing a complete transaction in three phases:

- device authentication (up-link and down-link);
- user authentication (up-link and down-link);
- telnet transaction (up-link and down-link).

The third phase was performed by executing a macro to eliminate the man latency in the editing phase of fields.

4.3 Overhead and fragmentation

The overhead analysis demonstrates that:

- the maximum length of an IP datagram in the wireless path is 608 bytes;
- the maximum length of an IP datagram in the LAN path is 1061 bytes, due to the MTU of internal network;
- the overhead change with the length of datagrams;
- the behaviour in the GSM and GPRS case is exactly the same.

During the *transaction* phase the host gateway sends clear text packets to the internal firewall which performs the encryption retransmitting the packet over the wireless path to the mobile device (LAN and wireless down link). The encrypted packets leaving the firewall present an overhead due to the application of cryptographic algorithm performed by IPSec. The inverse happens to the encrypted packets transmitted by the mobile device.

We measured the discussed overhead in the two cases: up and down link. Because of difference between the MTU of LAN and GSM/GPRS paths, the first case (up link) is more simple than the down link case. In fact, the firewall receive, from the wireless link, always datagrams smaller than 608 bytes and after the decryption, it forwards clear text datagrams to the host gateway. In this case the IPSec overhead is represented on Figure 4a where Y axis measure the overhead corresponding to the internal datagram length specified on the X axis. The overhead range is 50-62 bytes, we will discuss later about the function linking overhead and internal length. In the down link case, for the fragmented datagrams (internal length>608 bytes), we define the average overhead:

$$(\sum_{0}^{N} L - \sum_{0}^{M} l) / N$$

L= sum of fragmented datagrams length
l= sum of internal datagram length
N= number of external fragment

Figure 4b, shows how the average overhead is in the range 50-60 bytes for small datagrams (less than 608 bytes) and about 70 bytes for larger datagrams. Moreover, also in this case, there is an overhead variation for different values of internal datagram length and there are no significant differences between the GSM and the GPRS case.
To understand the relationship between overhead and datagram length we can observe from a different point of view what happens in the up link case. Figure 4c shows that the length of encrypted datagrams belongs to a discrete set of values. In particular, as the internal packet length increases, the length of external datagram assumes discrete set of increasing values. The reason of this behavior is the padding introduced by the encryption algorithm, useful to obfuscate statistical cryptanalysis.
How stated in 0, padding in an ESP packet is optional and the sender may add 0-255 bytes of padding. Padding is required when an encryption algorithm is employed that requires the plaintext to be a multiple of some number of bytes, or, irrespective of encryption algorithm requirements, to ensure that the resulting ciphertext terminates on a 4-byte boundary. Padding may be used to conceal the actual length of the payload, in support of (partial) traffic flow confidentiality. In this case, the inclusion of such additional padding has adverse bandwidth implications.

4.4 Time and costs

We have already introduced some aspect about the time analysis and the difficult in performing a valid set of tests to compare the performances of GSM and GPRS links. In fact the bandwidth variation, the signal strength and the number of users simultaneously connected, made the transmission rate of GPRS variable between 0 and the maximum rate. Moreover, the performances of interactive traffic in the particular case of the link configuration phase of PPP increase the latency slowing the first phase of a GSM connection 0. With the performed analysis we have focused only on datagram length measurement to be sure that the results are independent from the factors discussed above. Moreover also in the presented case we observed that the GPRS was faster than GSM a part a delay in the “authentication device” phase, due to an IKE informational packet present in the GPRS case. The overhead introduced by encryption afflicts costs, with respect to bytes exchanged (GPRS) and connection time (GSM) of session flow. In fact, the above measurement shows that the overhead, varying in the 50-80 bytes range for each datagram, afflicts the traffic as follows:

- up link case: datagrams, containing mainly queries data, are doubled (small packets not longer than 70 bytes);
- down link case: datagrams containing application layer responses fragments (3270 format), are increased of 7-12% (datagram longer than 600 bytes).

We argue an average increment of traffic and costs, in the GPRS case, approximately of 10%.
Further studies can take into account GPRS bandwidth variation and the relationship with IPSEC performance in term of time and cost, with different session application (e.g., FTP, HTTP) and authentication and encryption protocols.

5 CONCLUSIONS

In this paper we have showed how the IPSec suite can be effectively applied to secure GSM/GPRS communications. The level of reliability in GSM/GPRS communications that this result can induce the deployment of large scale GPRS networks, as well as the adoption of public network GPRS-based, in critical governmental/private infrastructure. In particular, we have showed the effectiveness of the IPSec, proving that the overhead generated is tolerable under a wide set of parameters. The only limitation, posed by mobile operator capabilities, relies on GPRS connection reliability while roaming.
As for further research directions, we are interested in techniques to reduce the burst overhead generated by the set up IPSec-secured GPRS communications and to further study IPSEC connection reliability while roaming in GPRS environment. Moreover, we are addressing the possibility to employ the IPSec suite to secure peer to peer, ad hoc networks.

REFERENCES

Barkan, Biham and Keller, "*Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication*", Proceedings Crypto 2003" http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2003/CS/CS-2003-05.ps.gz, 2003.

Biryukov A, Shamir A, Wagner D., “*Real time cryptanalysis of A5/1 on a PC*”, Fast Software Encryption. 7th International Workshop, FSE 2000.

Proceedings (LNCSVol.1978). Springer-Verlag. 2001, pp.1-18. Berlin, Germany

Briceno, Goldberg, Wagner, "*GSM Cloning*", http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html, 1998

Ekdahl, P. Johansson, T. *"Another attack on A5/1*", IEEE International Symposium on Information Theory - Proceedings 2001. p 160 (IEEE cat. n 01CH37252)

Brookson , GSM (and PCN) *Security and Encryption*, 1994, http://www.brookson.com/gsm/gsmdoc.htm.

M. Walker and T. Wright, *Security*. In F. Hillebrand, editor, *GSM and UMTS: The Creation of Global Mobile Communication*, pp. 385-406, John Wiley & Sons, New York, 2002.

R. J. "Bud" Bates, *GPRS*, McGraw Hill TELECOM, 2002.

Jörg Eberspächer and Hans-Jörg Vögel. *GSM switching, services and Protocols*. John Wiley and Sons, 1999.

Garg, Vijay K. *Principles and applications of GSM*. Upper Saddle River (NJ) Prentice Hall PTR, 1999

ETS 300 534. *Digital Cellular Telecommunication System (Phase 2); Security Related Network Functions*. ETSI, August 1997.

ETSI TS 100 929. *Digital Cellular Telecommunication System (Phase 2); Security related network functions.* ETSI, November 1999.

Lauri Pesonen, *GSM Interception*, http://www.dia.unisa.it/ads.dir/corsosecurity/www/CORSO-9900/a5/Netsec/netsec.html#chap1, Nov1999,

Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, Wiley, 1995

N. Doraswamy and D. Harkins, "*IPSec: The New Security Standard for the Internet, Intranets, and VPN*", PH PTR, 1999.

O. Shaham, S. Aviran, E. Simony, Y. Shapira, "*Rate Control for Advanced Wireless Networks*" , http://www.wisdom.weizmann.ac.il/~odedsh/

M.Meyer, *TCP Performance over GPRS*, In Proc. of IEEE WCNC, 1999, http://www.cs.helsinki.fi/u/gurtov/reiner/wcnc99.pdf

RFC 2406

R. Ludwig and B. Rathonyi, *Link Layer Enhancement for TCP/IP over GSM*, Proceedings of the IEEE INFOCOM '99, April, pp. 415-422.