Wireless Security Perspectives

Cellular Networking Perspectives

Technical Editor: Les Owens, Managing Editor: David Crowe Vol. 2, No. 1 January, 2000

Recent Cryptanalysis of GSM A5/1 Algorithm: *What Does it Mean?*

> *"Human Ingenuity cannot concoct a cipher that human ingenuity cannot resolve"*
>
> - Edgar Allan Poe

This issue of *Wireless Security Perspectives* focuses on GSM and the December 1999 article titled *Real Time Cryptanalysis of the Alleged A5/1 on a PC* (preliminary draft) by Alex Biryukov and Adi Shamir. The authors describe an attack on the GSM A5/1 traffic encryption algorithm and claim that by analyzing the output of the algorithm, one can recover the cryptographic key in less than a second using an ordinary PC.

We review the GSM system and its cryptographic capabilities, provide a brief overview of the attack, discuss some of the comments that have been made about the attack, and provide our own response. Readers interested in details of the cryptanalytic attack can refer directly to the Biryukov-Shamir paper, which is available at:

www.cryptome.org/a51-bs.htm

Glossary

Some terms are defined at the end of this article. About 750 more telecommunications, wireless and internet terms can be browsed at:

www.cnp-wireless.com/glossary.html.

GSM Background

GSM, the Global System for Mobile Communications, or GSM, is a TDMA (Time Division Multiple Access) wireless system that was first developed as the next-generation digital cellular mobile communication system for CEPT (European Post Offices and Telecommunications) in Europe. In the late 1980's, GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), which published Phase I of the GSM suite of standards in 1990. By mid-1991, commercial service began. By 1993, there were 36 GSM networks in 22 countries. GSM became more than a European standard as non-European countries soon adopted the standard, including Australia, South Africa, Australia and many Asian countries. When PCS licenses were auctioned in the late 1990's, several North American companies also became signatories to the GSM MoU (Memorandum of Understanding) including Sprint Spectrum, BellSouth Mobility DCS, Omnipoint, and Pacific Bell. By 1998 in the US, there were more than 2 million subscribers in 1500 markets and GSM was operational in more than 40 states. Today, GSM is the cellular system that is used in more than 100 countries worldwide and has more than 200 million subscribers. GSM has earned its name: Global System for Mobile communications.

The functional entities that comprise the logical GSM network are illustrated in Figure 1. As shown, the GSM network is divided into three major parts: the networking subsystem, the base station sub-

About *Wireless Security Perspectives*

Price

The basic subscription price for *Wireless Security Perspectives* is $250 for one year (12 issues) for delivery within the US or Canada. International subscriptions are US$300 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees for more readers.

Current subscribers to *Cellular Networking Perspectives* receive a discounted price – only $200 for delivery within the US and Canada or $250 elsewhere.

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Month's Major Topic

WAP security.

Next Issue Due…

February 17th, 2000.

Future Topics

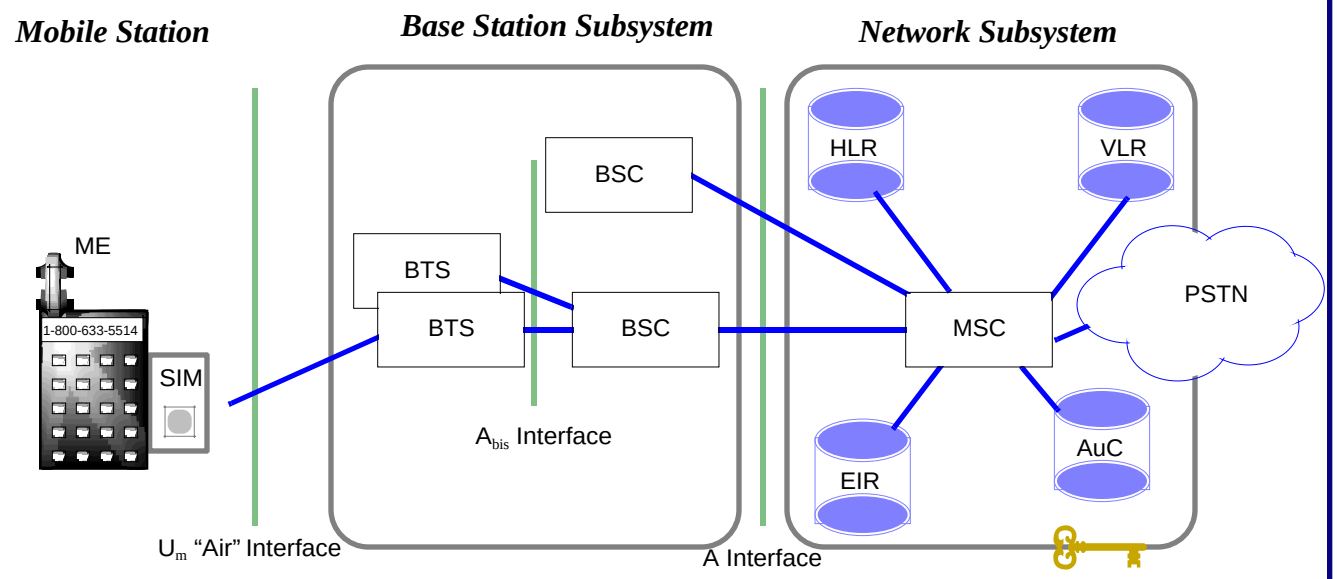
Voice over IP security • Public Keys & Wireless • Kerberos • Public Key Infrastructure • IP Security • IKE

Write to Us!

Tell us what you would like to see in future articles.

Wireless Security Perspectives is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary AB, T2N 3W1, Canada.
Contact Information: Phone: 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnpsales@cnp-wireless.com **Web:** http:/www.cnp-wireless.com/wsp.html.
Subscriptions: $200 for current *Cellular Networking Perspectives* subscribers for delivery in the USA or Canada, US$250 elsewhere. Non-subscribers pay $250/yr. for delivery in the USA or Canada, US$300/yr. elsewhere. Payment is accepted by cheque, bank transfer, American Express, MasterCard or Visa. **Delivery:** Email or 1st class mail.
Back Issues: Available individually for $20 in the US and Canada and US$25 elsewhere, or in bulk at reduced rates. **Discounts:** Educational and small business discount: 25% off any order. **Copies:** Each subscriber is licensed to make up to 10 copies of each issue or back issue. Please call for rates to allow more copies.

Figure 1: GSM Architecture



system, and the mobile station. The mobile station, which includes the mobile equipment (ME) and the subscriber identity module (SIM), is used by the subscriber. The base station subsystem, including the base transceiver station (BTS) and base station controller (BSC), controls the radio link to the mobile station. The network subsystem, including the most important mobile switching center (MSC), performs the switching of calls between the mobile and other fixed or mobile networks. Additionally, the network subsystem performs the all-important authentication of subscribers. The mobile station and the base station subsystem communicate across the 'Um interface,' also known as the air-interface. The base station subsystem communicates with the MSC across what is known as the A interface.

The architecture of GSM allows several telecommunication services. Although voice transmission is the primary service, short message service, circuit switched data at modest speeds (e.g. 9600bps) and packet switched data are either available now, or shortly in the future. Voice transmission is enhanced by supplementary services such as caller identification, call forwarding, call waiting, and conference calling.

GSM Cryptographic Algorithms and Security Services

Several cryptographic algorithms are specified in the GSM system for the delivery of security services (or features) for the system. The GSM algorithms and their associated security services are the following:

- A3: To verify or authenticate mobile subscribers to prevent phone cloning, Each operator can choose which algorithm to use as A3.
- A5: To provide traffic confidentiality (voice, fax, and data).

  Two versions of this algorithm are used. The strongest is A5/1, which was developed by the GSM Algorithm Expert Group. A5/2, developed by the ETSI SAGE group, is weaker, but is used outside Europe because of export restrictions on A5/1.
- A8: To provide for traffic encryption key-generation. Each operator can choose the algorithm that they choose to use as A8.

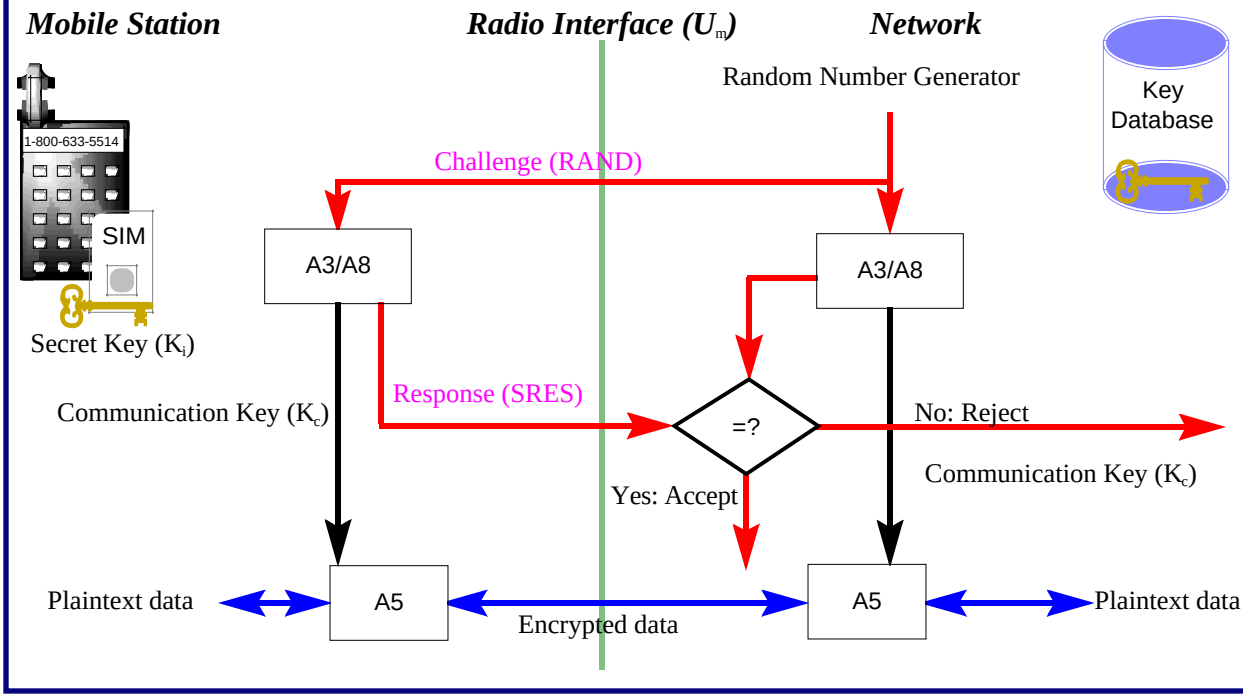
Although the algorithms are identified in the GSM specification, they are technically optional – it is up to the GSM network operator to decide whether to actually implement them, although roaming agreements are unlikely without them. Some GSM implementations support additional algorithms to provide, for example, AuC key storage encryption and confidentiality of keys during distribution from the SIM card vendor "personalization center" and the AuC.

Figure 2 below shows the placement of cryptographic algorithms A3, A5, and A8 and their associated mechanisms in the GSM system. A detailed explanation of the "challenge-response" authentication was provided in the last issue of the Wireless Security Perspectives. Refer to that issue for a review of the means used in the GSM system to prevent fraud using the A3 algorithm.

As shown in Figure 2, a secret key, K_i is stored in a user SIM card and is programmed when a wireless subscription is requested. K_i is only intended to be stored in one place in the wireless network – the authentication center (AuC). As shown in the simplified figure, this root secret provides the basis for the authentication of the mobile subscriber *and* for the encryption of the information on the radio path.

In the GSM system, data is encrypted at the transmitter (ME or BTS) in blocks of 114 bits by taking 114-bit plaintext data bursts and performing an "exclusive-OR" (modulo 2 sum) function operation with a 114-bit cipher block (key stream). Data is decrypted at the receiver in blocks of the same size using the cipher block that was created at the transmitter.

Figure 2: GSM Security Algorithms and Mechanisms



The cipher block used at both ends of the transmission path for a given transmission is generated in the base station and mobile station by either A5 cryptographic algorithm version. The A5 algorithm uses a 64-bit cipher key K_c, produced during the authentication process at time of call setup, and the 22-bit TDMA frame number (COUNT). This COUNT takes on values from 0 to 2,715,648 and has a repetition time of about 3.5 hours. The A5 algorithm produces two cipher blocks during each TDMA period, one for the forward (down) link and one for the reverse (up) link. The GSM encryption scheme is depicted in more detail in Figure 3.

Figure 3: GSM Security Encryption

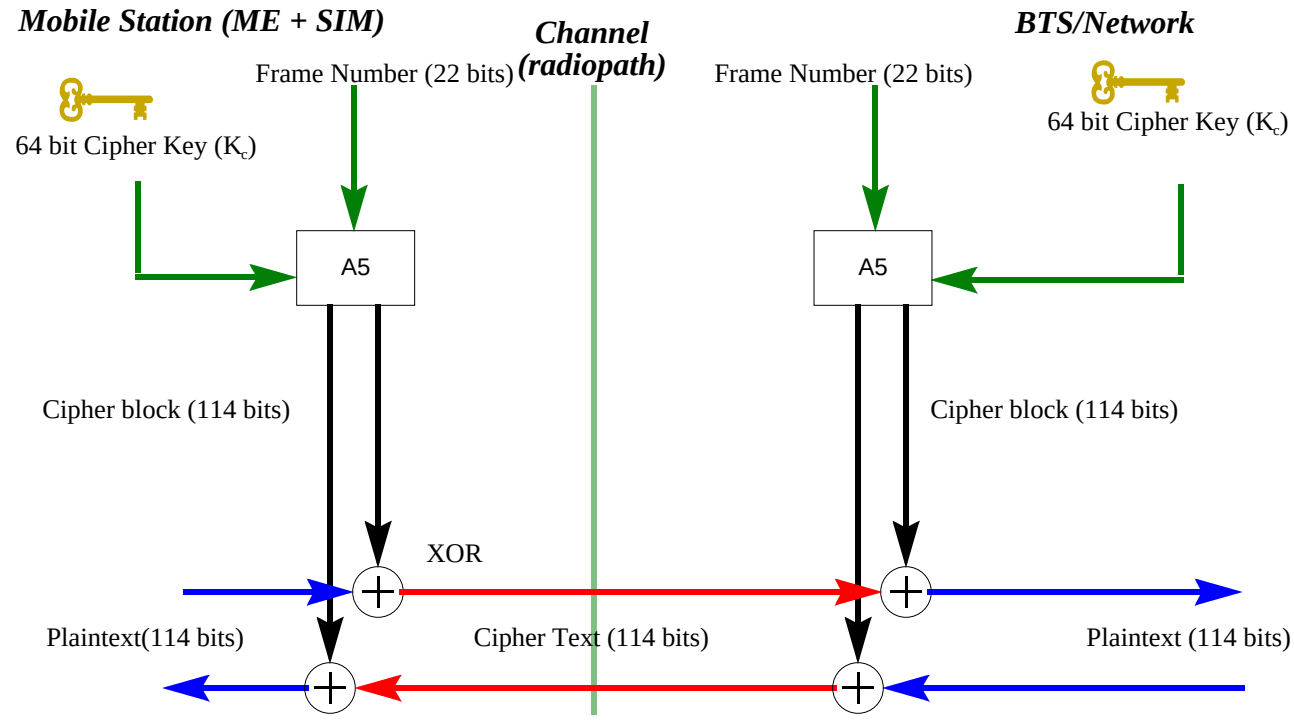
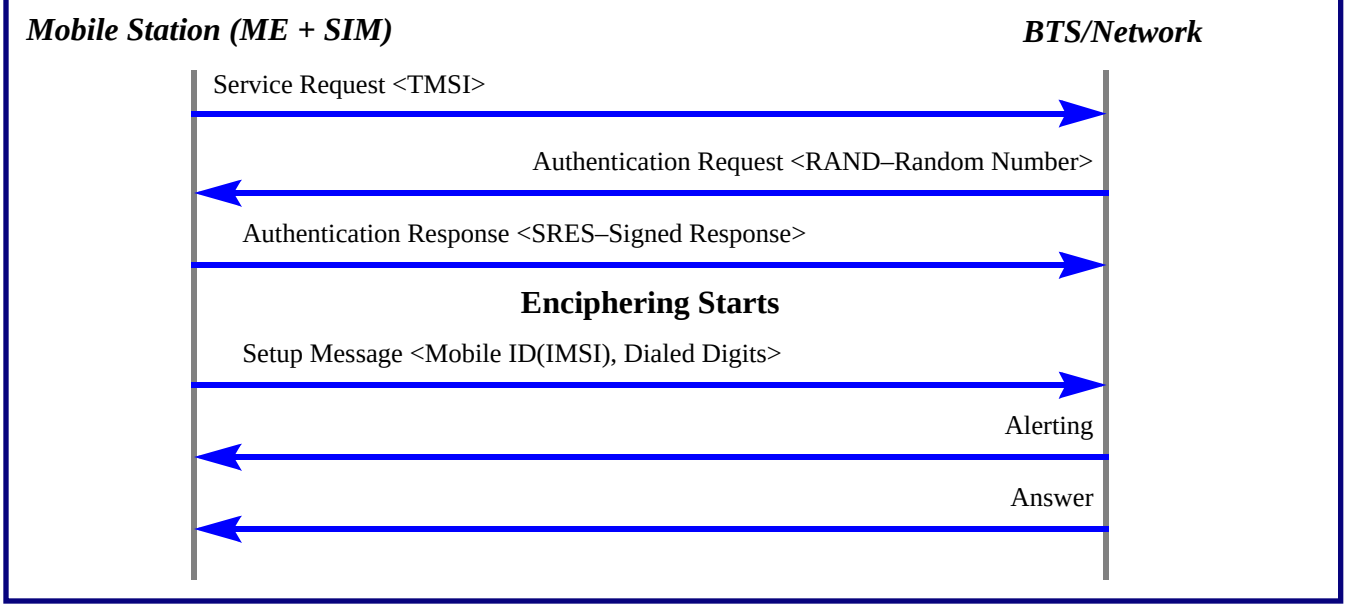


Figure 4: Authentication and Encryption Message Flow



The basic message flow between the mobile station and the GSM network is shown in Figure 4. The mobile station first provides a Service Request to the network during which the TMSI (Temporary Mobile Subscriber Identity) is provided to the network to identify in an anonymous way, the mobile station. The network authenticates the subscriber using the 'challenge-response' scheme that we have reviewed before. If authentication is successful, enciphering begins using the cryptographic key from the A8 algorithm as shown in Figure 2 above. After encryption is invoked, data passing between the subscriber's mobile station and the network is then encrypted using the A5 algorithm. It should be noted that the encryption process only occurs on the highly vulnerable radio interface (U_m) and not beyond. Only link encryption is provided and, not the perhaps more desirable end-to-end encryption. Plans are for 3G versions of GSM to support this more secure technology.

Previous Attacks on A5/1

The Biryukov-Shamir paper discusses several previous attacks on the A5/1 algorithm:

Attack 1: Briceno

This 'doesn't buy you much'. GSM operators should have no fear of this.

Attack 2: Anderson and Roe

This requires more than a month to find one key so, it too, is fairly worthless.

Attack 3: Golic

This requires about the same amount of time as Attack 2, and therefore is purely of academic interest.

Attack 4: Golic

This attack requires an enormous amount of hard disk space or an enormous amount of subscriber traffic (i.e. voice conversations) and for both of these reasons is, once again, impractical.

The Biryukov-Shamir Attack

The Biryukov-Shamir ciphertext-only cryptanalytic attack on GSM A5/1 is based on three principles related to the three short linear feedback shift registers (LFSR) that form the basis of the algorithm:

- subtle flaws in the feedback tap structure of the registers
- invertible clocking mechanism of the registers
- frequent resets

Their paper considers only the relatively narrow issue of the robustness of the A5/1 algorithm and not the practical network security of fielded GSM systems. The authors make no claims about this broader, perhaps more important, issue.

The authors claim that by analyzing the output of the A5/1 algorithm, which is used for traffic encryption in the GSM system, one can recover the cryptographic key K_c in less one second using an ordinary personal computer. The attack requires that the PC have 128 megabytes of RAM and two 73 gigabyte hard disk drives. A modern PC can certainly meet these standards. The attack also requires a data preparation process that must occur one time but may be shared among many machines in a parallel processing fashion. According to the authors of the paper, the attack had been verified with an actual implementation

GSM Chairmen and Bruce Schneier Respond

On December 16, 1999, the Chairmen of the GSM Association Security Group and the ETSI SMG10 Security Group/ 3GPP Security Group issued a statement regarding the paper by Biryukov and Shamir. They said that the paper presents an "interesting application" of the time-memory cryptanalytic technique, and that "others had studied similar attacks" on the GSM system. The GSM chairmen stated that while these kinds of attacks

are of "theoretical interest" they claimed that even this attack, like the previous attacks, is impractical, at least as an attack on GSM. They closed their correspondence, however, by stating that they are committed to "enhancing protection for GSM and ensuring that customers are offered the best protection possible".

At about the same the GSM chairmen were publishing their statement, Bruce Schneier of the recent start-up Counterpane Internet Security Inc. (www.counterpane.com) and author of a popular, encyclopedic text on modern cryptography, *Applied Cryptography*, commented on the attack. According to Schneier in his monthly e-newsletter, the *Cryptogram*, the GSM algorithms are "... robustly lousy … and result in the ability to decrypt … in real time on average computer equipment". He went on to comment that the "… algorithms were designed and analyzed by the secretive 'SAGE' group". He boldly stated, that "we don't know who the people [in SAGE] are or what their resumés look like" and noted that the analysis "is online … it's entertaining". Once again, Schneier in his typical sensationalist and pompous way said, basically – nothing.

What does this Mean?

In the Biryukov-Shamir paper, the authors provide a description of the alleged A5/1 algorithm with its three small LFSRs, discuss previous impractical attacks, and provide both a rather abstruse informal and detailed description of their attack. They did not however, discuss the practical aspects of this attack. In other words, what would one have to do to make this a meaningful threat? Should GSM carriers be concerned?

Below we attempt to list the steps that would be required to perform a meaningful attack on the GSM system using the Biryukov-Shamir cryptanalytic attack:

1. The adversary must first choose a subscriber to target.

   To do this, one must have associated the target with its TMSI. This could only be done by having monitored the target so that the publicly transmitted IMSI (International Mobile Subscriber Identity) must also be known. Because of the anonymity security feature – *security-in-depth*, this effort may not be practical or simply, not worth it. However, this step would not deter a determined eavesdropper.

2. The adversary must obtain a special (custom) radio eavesdropping device that is capable of monitoring the GSM air-interface and providing raw digital data over a data port to a PC.

   An off-the-shelf piece of test equipment almost certainly exists to perform this data capture. However, such sophisticated service monitoring equipment with the required data processing capabilities costs over ten thousand dollars. This is beyond the range of the typical phone phreaker adversary, but not beyond the reach of a determined and well-funded eavesdropper.

3. The adversary must be skilled enough with the equipment to tune to the target's radio frequency and obtain at least 120 seconds of encrypted data from a target's single target telephone conversation. The adversary must have the ability to follow or track the targeted subscriber during any kind of hand-off and mobile station movement. This requires that the attacker be determined, well-funded and sophisticated.

   With the proper equipment, capturing the necessary data is possible. However, capturing two minutes of encrypted data from the mobile subscriber is not likely for two reasons. First, many calls do not typically last more than two minutes. Second, the target is not likely to remain stationary long enough to capture the necessary data before he has moved out of range of the monitoring device.

4. Using the eavesdropping device, the adversary must store the received ciphertext on an appropriately configured PC.

   This step is easy, again, with the proper equipment. However, a PC with two hard disks with approximately 150 gigabytes of storage is not the norm today. Our eavesdropper must now be determined, well-funded, sophisticated and computer-literate.

5. The adversary must have obtained the cryptanalytic program that embodies the Shamir attack. He must then invoke the program with the 120 seconds of data and recover the key.

   If the determined, well-funded, sophisticated, computer-literate and cryptanalytically competent adversary has the properly equipped personal computer and operational cryptanalytic code, this task can be accomplished.

6. Using the recovered key, the adversary with the eavesdropping/cryptanalytic equipment can decrypt the remaining voice traffic of a single call.

   This step, again, is trivial for the determined, well-funded, sophisticated, computer-literate, cryptanalytically competent and patient adversary. But, was it worth the time and money expended?

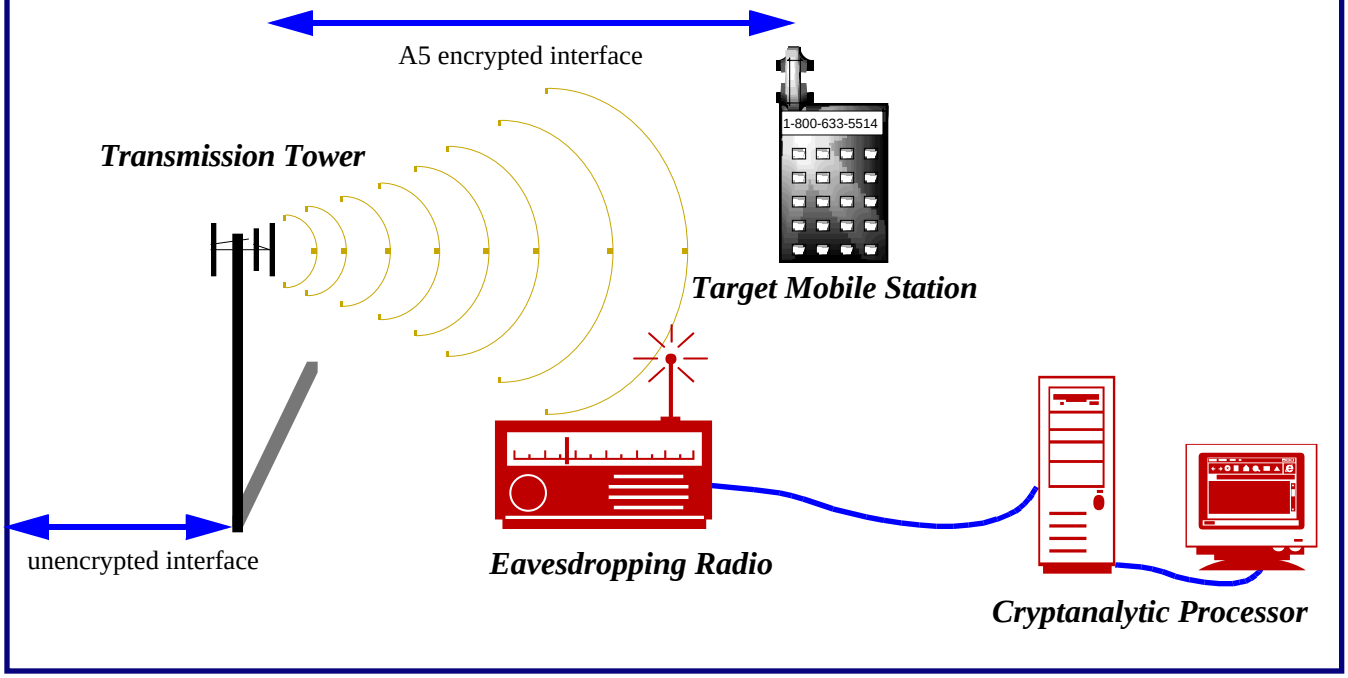
Figure 5 illustrates the equipment and approach used by the fictitious adversary described above.

Is this Attack Feasible?

While there is no question that the Biryukov-Shamir attack is theoretically possible, it would take a very sophisticated attacker with considerable resources. The adversary must capture a significant amount of GSM ciphered data (e.g. voice), and then, even after decrypting it, be able to convert it back from digitally coded voice to analog audio. This implies a considerable amount of hardware and software development. And, after all that, the decrypted message might be nothing more important than "Honey, will you bring home a l oaf of bread and gummy worms for the kids?".

If Schneier or Shamir or anyone else can show me an important message that has been decrypted in this way, I would start worrying, but until then, keep those research papers coming! It is certainly true that governments have the resources and sophistication to perform this attack,

Figure 5: Typical Equipment for GSM Cryptanalytic Attack



but then they also have other ways to eavesdrop, such as by obtaining a court order and getting access to unencrypted voice at the MSC site.

What should be done?

In this issue, we have provided an overview of the GSM system, the algorithms and the cryptanalytic attack on the GSM A5/1 algorithm. However, based on the "ifs-and-buts" from the analysis above, we believe at this point, this poses no real threat. We have to agree with the GSM chairman that this attack is of interest only from a theoretical standpoint. We believe that the attack at this time does not present any immediate danger. However, the GSM community should be vigilant and as the GSM chairmen stated, the group should constantly be looking for ways to improve the security of the GSM system and its subscribers.

List of Acronyms

A5	GSM Encryption Algorithm
AuC	Authentication Center
BSC	Base Station Controller
BTS	Base Transceiver System
EIR	Equipment Identity Register
ETSI	European Telecommunication Standards Institute
GSM	Global system for Mobile Communications
HLR	Home Location Register
IMSI	International Mobile Subscriber Identity
K_c	GSM Cipher Key
K_i	GSM Root Key
ME	Mobile Equipment
MS	Mobile Station (In GSM, ME + SIM)
MSC	Mobile Switching Center
PSTN	Public Switched Telephone Network
RAND	Random challenge number
SIM	Subscriber Identity Module ("Smart Card")
SMS	Short Message Service
SRES	Signed Response to RAND
TMSI	Temporary Mobile Subscriber Identity
VLR	Visitor Location Register
XOR	Exclusive OR (modulo 2 sum)