Intercepting GSM traffic

Washington D.C., Feb 2008, Black Hat Briefing
blackhatdc08@segfault.net

Abstract: This talk is about GSM security. We will explain the security, technology and protocols of a GSM network. We will further present a solution to build a GSM scanner for 900 USD. The second part of the talk reveals a practical solution to crack the GSM encryption A5/1.

0. Agenda
    a. Who we are
    b. What we do
1. GSM
    a. GSM Network
    b. Base Station, Switches and Databases
    c. Mobile Phone Technology
2. Receiving GSM signals
    a. Nokia 3310
    b. USRP / Gnu Radio
    c. Others (tsm30, omap)
3. Security in GSM
4. Cracking A5/1
5. Threats & Future

0 – Agenda

We are a group of computer security researchers. We engineered a low cost technology using off of the shelf hardware to receive and decipher GSM signals. We are the first to implement a low cost practical attack against the GSM cipher A5/1. Our goal is to raise awareness and to motivate the Mobile Industry to secure the network.

1 – GSM

GSM is the world's largest mobile phone network. It is used by over 2 billion people across more than 212 countries. GSM was designed in 1982 and became live in 1991.

A typical GSM network contains Base Stations, a Base Station Concentrator, various databases (MSC, VLR, …), switches and terminals. Various different signal protocols (including SS7) are used to transfer the information between the key elements of the network.

The air interface works on 4 main frequency bands. The range of the wireless signal can exceed 35km.

Today’s Mobile Phones (MS) are incredible powerful signal transceivers. They operate on two 32-bit CPU’s at over 350 MHz.

2 – Receiving GSM signals

Various Nokia mobile phones have been shipped by accident with maintenance functionality. These phones can be configured from a normal PC to receive any GSM data from the broadcast channel. These phones cost between $1-5 USD and are available on E-bay. Other commercial products like the Sagem trace mobile or Ericsson phones can be used as well.

The USRP is a software defined radio and can receive and transmit any kind of data between 0 and 3 GHz. We have developed a software module to receive and decode GSM signals. The USRP costs $750 USD.

There exists a wide range of commercial testing and interception equipment from resellers all around the world. Some of these products are tailored for tapping GSM conversations.

3 – Security in GSM

Only the air part of a GSM communication is encrypted. The signal is decrypted at the base station and then transmitted in clear text across the network. The encryption on the air part was broken in 1998.

The key has been artificially weakened by setting the last 10 bits to 0. On some networks the same session key is reused for multiple conversations. Some algorithms are proprietary and the GSMA denies disclosing them. The indication to the user if encryption is enabled has been removed from the mobile phones. The International Mobile Subscriber Identification (IMSI) is constantly sent in clear text over the air despite ITU recommendation that this should not happen. Location information is broadcasted to everyone.

Commercial interception equipment is available on the internet.

4 – Cracking A5/1

When a mobile phone authenticates to the base station, both possess the same symmetric key Ki and use A3/A8 to authenticate and agree upon a session key to use (Kc). Kc is then used with A5 to encrypt frames sent between the two devices. A5 is implemented as a stream cipher where a frame number is generated as an initialization vector (IV) and is used to seed A5. A5 then emits a stream of pseudo-random bytes which is XORed with the plain-text to encrypt it. The frame number and cipher-text are transmitted across and the other side can decrypt the packet by seeding A5 with the same frame number and Kc and XORing it with the cipher-text.

How does A5/1 work? A5/1 consists of 3 shift registers with majority clocking. To initialize the registers the 64-bit Kc and 22-bit frame number are first shifted into the left side of all 3 registers and XORed with the feedback. Then A5/1 is clocked using the majority clocking for 100 cycles to mix the bits. Then the next 114-bits of output from A5/1 is XORed with the plain-text to encrypt, or the cipher-text to decrypt.

Our attack requires 3-4 frames of a conversation and is fully passive. It uses a combination of the TMTO (Time-Memory Trade Off) or Rainbow Table attack and some other tricks. The key to our attack is that there are 4 frames of known plain-text so we can get 4 frames of A5/1 keystream output. This means that we can derive 204 64-bit keystream values from different offsets from within the stream. From this we can use a rainbow table to reverse it back to the internal state of A5/1. Because we have so many data points our rainbow table only has to be 1/64th of 2^{64} or 2^{58}. This still means that our rainbow table is around 120,000 times larger than the largest Lanman Rainbow Table.

One of the tricks that we use to compute such a large table is by implementing the rainbow table generation and real-time attack on FPGAs. This reduced our time drastically. On a single PC it would take roughly 33,000 years to compute the table or would take 33,000 PCs one year. With a moderate 4U cluster of 68 FPGAs we can do it in 3 months. We are also in the middle of developing new hardware to speed this up and make the attack more cost effective.

The hardware that we're currently using is the Pico E-16 in a machine that can take up to 68 E-16's. All of the cards are connected over 8x PCIe and all of the data is buffered with FIFOs on the FPGAs and bus-mastered to the host memory where it is written out to disk. The system currently has 6TB of disk storage to deal with the intermediate files and chain sorting work.

The end solution will work on 6 350GB hard drives (2TB) and 1 FPGA and is able to recover the key of a GSM conversation (voice or sms/text) under 30 min or in under a minute with 2TBs of Flash hard drives and 32 FPGAs. The speed is proportional to the hard drive access time and the number of FPGAs. For the cheap attack to work twice as fast, it would require twice the number of hard drives and twice the number of FPGAs.

Once we run our 204 data points through the rainbow tables we should have on average 3 A5/1 internal states. From this we can load them into A5/1 and reverse clock it back to after the key is mixed in. Because of the majority clocking we'll end up with multiple possible state values at that point. After we reverse all 3 internal states, we look at the possible state values and the common value will be the correct one. From that point we can clock A5/1 forward to decrypt or encrypt any frame. It is possible to derive the actual Kc key, but at this point it isn't necessary.

The tables are still computing but will be finished in March. There will probably be a commercial implementation of this attack later on this year that can be scaled to whatever time period is required for recovery.

5 – Threats & Future

GSM has to become secure.

Receiving, transmitting and cracking GSM will become cheaper and easier. It will become easier to mount an attack against the mobile network infrastructure.

We are expecting a rise in unlawful interception, data/identity theft and tracking the location of mobile phone users.