Security Issues with the Military Use of Cellular Technology

Brad Long, Director of Engineering, IFONE, Inc.

Executive Summary

IFONE provides securable private cellular networks. It presents this paper to military users in order to increase awareness of the technical risks of commercial cellular use in hostile areas. New mandates and their related technologies allow the location of cellular telephones to be identified within as few as 50 meters. While this offers the user a great advantage when calling 911 or accessing location based services, the external knowledge of a user's location is a decided liability for military or security force applications.

One misconception about these services is that they are call related. In fact the network knows where the user is at all times whether he is making a call or not. The only way to prevent the network from knowing the cell phone location, is to turn it off.

Much effort has been put into applying technology to securing the mobile channel. While this is very good at preventing conversations from being overheard, the knowledge of who you are, when you called, who you called, and the length of the conversation, is still known by the network.

Against a sophisticated enemy, cell phones present a risk. Media reports have touted the collection of intelligence and evidence against terror groups on the basis of cell phone tracking. This sword cuts just as easily the other way.

It is only a matter of time before the exposure is exploited. Public cell phones should be handled as carefully as munitions

Background

The trend in wireless communications over the last two decades has been undeniable. The rise in popularity of cell phones may be seen by some as a sign of affluence in our society, or achievement of technology by others, but this is insufficient explanation for the explosion in the market place. Indeed cell phones are actually more popular in developing economies, where people must allocate a far greater portion of their income or wealth toward service subscriptions than in western countries.

The explanation for the skew of resources towards communications can only be explained in terms of economics. Wireless communications, and the mobility that this affords, simply makes the individual more effective and efficient. By some estimates this increase efficiency can be as much as two to three times on average.

It is no longer reasonable to believe that in our society, we can perform properly without appropriate communications. This is a time where researching the existing body of knowledge is expected to take minutes, not months. Decisions are to be implemented instantly. Availability and access to people resources is demanded, and skills and knowledge cannot be delineated and separated by locality.

Availability of communications affects how we organize ourselves to the task. This is seen in changing job descriptions and role responsibilities all designed around taking maximum advantage of the new capabilities available to leaders. While two decades ago a desk job meant you would be likely to answer your office telephone anytime of the day, we now have many meetings, and work outside far more often than ever before.

It would simply be too burdensome to do without these modern advantages.

Increase in effectiveness has real bottom line value to industry and commercial ventures that drive the adoption of this technology, both at the individual and organizational level. It is no surprise that since non-commercial ventures also allocate resources, and generally have a need to maximize the use of resources (no one has unlimited funds) they would also wish the benefits of wireless mobility communications.

It is important to appreciate however, that as with any technology, it only does what it was designed to do. Issues not under the attention of the original designers, are likely to become liabilities of the technology. Engineers do tend to be very good at anticipating the possible shortcomings (and designing good defenses) when the technology is used as they anticipate. When a technology is applied to a different problem than that which it was designed, more serious liabilities may be discovered.

This paper discusses the special circumstances of the military and its need for communications.

Military Communications

The military clearly can benefit from increased efficiency to the task that good mobile communications would afford them. The military circumstances are different from their commercial counterparts in two important ways:

- Military is subject to overt threats that are not subject to restriction protocols
- Failures of a technology to perform can exact a cost in terms of loss of life

A commercial entity can rely on laws to protect itself from the actions of an adversary, and appeal to the legal system for satisfaction. This extra measure means that commercial communications need only a moderate amount of security about them. The restrictions on a military adversary are far less; in fact, there are almost none. Indeed, great recognition is given to those who visit this kind of compromise upon an enemy and their exploits are widely celebrated.

It is also very rare that a technology security failure would result in anything more that a quantifiable economic or financial loss in the commercial sector. The military on the either hand has both a financial exposure as well as the potential to have people hurt or killed. The relative value of this varies from nation to nation and culture to culture, but in the west, we tend to put this extremely high. The value of life is so high that many millions of dollars are sometimes spent to only slightly reduce the risk to only a few lives. We view this as an indicator of our civility, and admired by this author. It is important to point out that this is not a universal value amongst adversaries.

Many other important issues arise when comparing military to commercial needs. For the most part these vary widely but vary by degree. I am hard pressed to come up with many scenarios in one domain, which would not have an approximate analogy in the other. The risk and cost do vary widely.

Intelligence

I don't pretend to be an expert in this area. It is important here for me to identify some of the ways in which information is valuable to an adversary, and the kinds of information that is available to be compromised.

The classic code is what is what first comes to mind when you talk about intelligence. When you overhear the command to "attack at dawn", it enables the opponent to organize defences against the plan. This type of intelligence is protected by strong ciphers that keep information to the persons intended, and away from all others. Most compromises of this type of information do not happen because of cracking the cipher as best selling novels would have you believe. Most compromises occur by intercepting the message before encryption of after decryption, or by compromising/intercepting the keys.

On the other hand, if you are sufficiently aware of the adversary's situation, the fact that a message was sent can often be far more useful than the message content.

Similarly the 'envelope details' such as who sent the message and to whom it was sent are extremely useful in intelligence efforts.

The nature of the message cipher text can also be an indicator. If the message is short, then it is unlikely to contain a great deal of new data (it can be references to pre-prepared sets of data). If it is long, then it is likely to be either a complex message, or a ruse.

The number of messages sent on secure channels, or the balance between secured and unsecured communications, are all useful when interpreted in the appropriate context.

Further the actions that are taken by a person after they receive a message are indicators of the content of a message (just ask Martha Stewart about this one)

Clearly it is a benefit if a communications system could:

- Protect the message content
- Protect the message address
- Protect the senders identity
- Hide the message volume
- Hide the fact that message even was sent

Further, it needs to be noted that mis-information is also a weapon of war. A fully featured communications system should protect against false messages entering the message stream.

Finally, it would almost have gone without mention that the methods a communications technology uses should not compromise any non-communications intelligence gathering protections in place.

Security

At the outset it must be clearly understood that the primary focus of GSM security is to protect the network from users. Further, it assumes that the intent of any compromise will be economic motivation. Almost no thought has been given to protecting the user beyond a few simple features developed for marketing reasons. The network is hence subject to compromise at many points that are areas of concern when employing the technology in other applications.

GSM provides three main features in the area of security:

- Anonymity
- Authentication
- Privacy

Authentication was the first form of security in the network. Original laws required that an unalterable ESN be recorded in cell phones to identify the phones and prevent fraud in the network. Violators however felt no compulsion to adhere to the law and the result was massive ‘cloning’ of telephones in the late 80’s and billions of dollars in fraud.

Authentication protects the network from that cloning fraud.

Privacy came to the network as a result of some very bad press. High profile incidence of people’s personal business becoming exposed in tabloid and other newspapers lead to a distrust of cellular technology for the purpose of conducting private affairs. Therefore the industry had to respond with appropriate features.

Anonymity is something of an anomaly in the suite of security feature in that it solves a problem that had few high profile failures in the past (that we are aware of). The exposure to the user is real enough, but it may be intended to protect the operator against the collection and sale of data to marketing companies.

In all these cases it is important to note that the security designed into the network is there to protect the network operator from a hostile environment. Any protections afforded the user are in place only for marketing reasons, and none of these protect the user from hostile acts.

Over the years I have seen many approaches where the network has been hostile toward the user. The strategy has generally been to try to capture roamers away from the competition and charge mega-bucks for service in an unregulated environment. If an operator had even more malicious intent, the tools and techniques are well established.

Compromising the User

Understanding how the technology works is important in understanding its shortcomings. In most cases compromise can be achieved with either a mobile in test mode (most mobiles can be configured to do this with information available on the web) or a base station simulator, easily available on eBay for less than the price of a single rocket

Who am I really?

> Authentication is strong. Unfortunately too many systems do not validate user to user information. The number displayed on you telephone as the calling number actually comes from the users equipment in all but the most basic of telephone services. This can allow a single piece of equipment to serve many different telephone lines, but also exposes the network to misrepresentation by the user.
>
> The network almost never checks that the originating number offered is appropriate or part of the available numbers for that station. If you wish to be known as the president, simply put the Whitehouse number into the calling number field of the setup message and that what appears in the network records (including the caller id)

Want to know the user? Just ask the mobile phone.

> Mobile identity is protected from observation by TMSI (anonymity). If the adversary is able to transmit a signal however, a mobile can lock on to it and will happily present its real address when prompted

How private is the conversation?

> It is as good as locking it in a safe. Unfortunately even the manufactures of safes rate their robustness in terms of the time it will take a professional to crack “the code.” It is the same with the over the air cipher text of the conversation. Given enough time and processing power it can be decoded. The hope is that the message will not be useful in the timeframe that it could be decoded.
>
> However, just like a bank, the majority of times they are compromised, it turns out to be an “inside job.” This is similar to the exposure of a user’s conversation. Only the over the air portion is protected and it is encoded/decoded by the base station. It is likely easier to put a microphone in the area of the user, or even easier, monitor at the network equipment where the voice is plaintext format.

Location, location, location.

It has been argued that the map has been a more important development in warfare, than was the gun. Knowing where you are, or even better, knowing where you enemy is. And all the terrain and circumstance in between has often allowed a lesser opponent to prevail.

The network is able to deliver calls to the user half way around the world, because the network knows where the user is. In the original analog technology this knowledge was limited to the nearest base station and it coverage areas.

The migration to digital technology and its exacting standards require the mobiles to transmit at a very specific time reference relative to the base station. This requires the mobile to adjust its transmit time based on how far it is from the base station due to limitations of the speed of light. As a result distance is known by the network as well as the mobile, and anyone able to see the commands between.

This is also the basis for the UTDA (uplink time difference of arrival) which is used to identify the location of the mobile for location based services and E911. The main point is that it requires no changes to the technology, only that the measurements be made and calculations performed to achieve this service.

Scenarios

The following describes some scenarios by which an adversary might exploit the weakness of cell phone technology to gain advantage. These are obvious ways to anyone familiar with the technology. To a soldier with a sharp mind however, there will no doubt be many more creative and non-obvious ways to exploit this technology

- Military users are evident by their frequent presence at bases.
- Military users tracked to off base locations can be used to launch attacks
- Military users moving toward fixed points can be used to detonate devices
- Location of high value targets can be identified
- Advance notice of visiting VIPs can be exposed by cross-correlation data that would identify their advance teams.

If you have questions or concerns regarding this paper, please contact iFONE:

IFONE, Inc.,
3648 St. Gaudens Rd
Miami, Florida 33133
305-567-0432
305-567-0966 FAX