GSMK CryptoPhone® Baseband Firewall
Technical Briefing

Preface

The GSMK CryptoPhone® Baseband Firewall (BBFW for short) in GSMK CryptoPhone secure mobile phones from the 500 Series onwards has been designed to provide protection against attempts to exploit the baseband processor (BP) over the air, and alert the user to network conditions that are indicative of a likely attempt to use active intercept techniques commonly known as "IMSI catcher attacks".

The BBFW consists of a series of heuristics and detection functions[1] that can be separated into two distinct parts:

- BP behavior anomaly detection
- Network anomaly detection

In this document, the warnings and alerts generated by both functional parts of the BBFW as well as the respective technical and tactical rationale for the selection of detection methods will be outlined. The BBFW also logs a number of events that are not indications of a hostile situation but that provide context for other events to either skew the classification towards "normal behavior" or "suspicious event".

1. General classification of events & reboots

In the graph display of the BBFW, the time sequence of events on the air interface is shown in different colors: The color white represents normal events, green represents non-suspicious events, yellow represents possible suspicious events, red represents suspicious events. You can go to the log-list for the desired period of time by long-pressing in the respective area of the graph (cf. Figure 1).

Events on the air interface are aggregated into a "network confidence" bar graph (cf. Figure 2) that provides an intuitive representation of the aggregate risk of the network situation and the likelihood that the BP has been exploited. The sensitivity configuration of the BBFW is tuned towards "trigger happy", meaning that it errs on the side of caution in respect to warnings and alerts. Depending on the network operator configuration, the number of false positive events can be higher or lower.

[1] Please note that most of the functionality described in this manual is covered by various U.S. and European patents held by GSMK, including US20140004829.

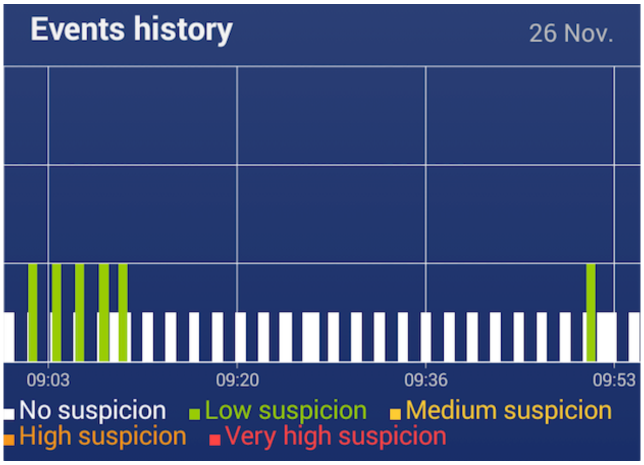

Figure 1 - BBFW Chart

Figure 2 - BBFW Bar Graph

The BBFW evaluates the density and severity of suspicious events over time. Once a certain level of suspicious events per hour (default: 8 events per hour, this is user configurable) has been reached, the BP will be reset to get rid of any potential RAM resident exploit code[2].

Statistics on the number of events in each category are displayed in the BBFW screen. Network anomalies are considered "persistent events" since they reflect a condition of the network situation.

2. Baseband processor behavior anomaly detection

2.1. Introduction

Exploitation of the BP over the air has become a growing concern due to the fact that recent security research has shown that the firmware of all currently used BPs contains a substantial number of bugs that can be exploited by various means, also over the air. If an attacker can gain access to the BP to the extent of being able to execute code on the BP of a secure phone, then he can circumvent or bypass a number of security functions, including access to the phone's application processor (AP) memory, which may contain valuable secrets like clear text or encryption keys.

BP firmware is proprietary and is commonly not available in source code for security analysis and bug fixing. In addition, a BP firmware image contains critical functionality for radio communication with the mobile network that is subject to regulations and certifications. This means that even if it were technically possible to audit and fix bugs for a specific BP image, it would most likely need to be re-certified if the fix touches part of the software stack that is communicating with

[2] Research by GSMK has shown that in the presence of the security measures taken on the GSMK CryptoPhone 500 series, it is very difficult for a BP exploit to become flash-resident and survive a BP reboot.

the mobile network. Re-certification is a time-consuming and expensive process, which is one of the reasons why the BP manufacturers have a relatively slow cycle of security updates. An exploitable bug that is reported to a BP manufacturer first needs to go into their internal bug fixing cycle, and then the fix needs to make it into the next release of the BP firmware. This release is then handed over to the phone manufacturer that applies its own configuration and parameterization and decides based on its own economic criteria when to release a new BP firmware image for a certain phone. Frequently only updates that provide better data throughput or longer battery life are pushed out for phones that already have been released. Security fixes make it out more often by accident in maintenance releases for "user relevant" bugs then in specific security fix releases. The fixing process can take many months, and usually only the next phone model in the pipeline receives a "fresh" BP firmware image. Users of older phones are frequently stranded with security bugs that are never fixed during the service lifetime of their device.

This situation created the need for a software component on the GSMK CryptoPhone 500 that through external observation of the BP behavior looks for indications of a successful BP exploitation.

2.2. Correlation between AP intentions and BP activity

One primary set of heuristics is the analysis of the correlation between network usage caused by applications running on the AP and resulting network usage as observed on the BP. The rationale is that one common modus operandi for an attacker who got exploit code running on the BP is to exfiltrate data, or to cause the BP to work as a room bug. These malicious functions cause BP activity that is not motivated by applications running on the AP requesting network activity.

The inherent challenge of this correlation heuristic is of course to distinguish between autonomous (not AP-related) network activity of an exploited BP and legitimate traffic caused by normal BP-internal functions like e.g. AGPS updates that are not directly visible to the AP. The rules that govern the BP - AP correlation are the following:

a) When there is BP data activity, there also should be OS data activity. Rationale: if the BP would have been exploited, then the attacker would likely try to exfiltrate data to the outside world

b) When there is BP phone activity, within some interval there also should be OS phone activity or SMS activity, or within 1s data activity.
Rationale: The BP setting up a traffic channel for voice or SMS without corresponding AP activity is suspicious and a possible sign of BP exploitation (SMS are sometimes delivered via data, depending on network configuration).

c) When there is BP control channel or SMS activity, within a short period there also should be AP data activity / SMS activity.
Rationale: BP activity should be reflected on the AP side in order to be non-suspicious (incoming SMS, kept alive data contexts)

d) Check that BP data activity ended at the same time when AP data activity ends.
Rationale: A clever attacker with the capability to execute code on the BP could wait for legitimate data usage and exfiltrate data either directly afterwards or at the same time[3].

e) Check that BB phone activity ended at the same time when AP phone activity ended.
Rationale: An attacker could keep an existing voice channel open even while the AP-side app thinks it has been closed, using the phone as a room-bug.

f) If an incoming call is off hook, then the user must have answered it.
Rationale: The BP should never accept an incoming voice call without user interaction. If that happens, there is a very high likelihood of a successful attack against the BP.

It is of critical importance to understand that the analysis of BP behavior in correlation to the AP is a statistical function. Individual warnings of suspicious events do not necessarily indicate a successful BP exploit, or the presence of an IMSI-catcher. A high number of these events under otherwise normal network conditions would however be a strong indication that something is wrong. From tests and user experience under attack conditions it is known that a common technique – the opening of a traffic channel without content transmission – is frequently used to facilitate further attacks. When a malicious base station is in the area, which will likely trigger persistent events regarding encryption etc., also non-correlation between AP and BP activity very often happens. It should be noted, however, that under sub-optimal network conditions (like the combination of legitimate roaming and bad network), there can be a high frequency of warnings that are just artifacts of the network situation.

In the following, the suspicious log messages and their meaning are explained:

- BB data activity detected without OS data activity (a data context has been established without AP intention)
- BB phone activity detected without OS phone activity (a phone call is ongoing without AP intention)
- incoming call is in progress but the user has not answered (a traffic channel has been set up for a call by the BP, but user has not picked up on AP)
- BB phone activity ended much later than OS phone activity ended (a data transmission initiated by the AP took much longer to complete on the BP then the corresponding AP activity)

[3] This rule has shown to cause a relatively high number of false positive events in the real world, and might be discarded or modified in future BBFW versions.

The list below contains the events that are logged because they provide context for the classification of other events. Since for technical reasons, the timing correlation between detection of BP activity and AP activity is not in all cases immediate, the suspicious events are only logged after a certain time during which no "relieving" event happened. A typical example would be a sequence where a negative "BB data activity detected without OS data activity" event is logged, followed a second later by a "BB data activity initiated by OS" event that provides the "justification" or explanation for the previous event. In this case no suspicious event is logged as long as the positive event happens within a pre-configured timeframe (typically 5 seconds).

- BB data activity ended because OS data activity ended
- BB phone activity ended because OS phone activity ended
- Phone (AP) control activity related to phone call termination
- BB control phone activity ended
- BB activity was started again shortly after it has stopped
- BB data activity related to OS data connection termination
- BB data activity stopped and started again shortly
- BB data activity initiated by OS
- BB phone activity initiated by OS
- BB control channel activity caused by sending / receiving SMS
- Phone (AP) activity related to data connection initiation
- Phone (AP) control activity related to data connection termination
- Periodic 2G / 3G location update
- User answered the call

3. Network anomaly detection

3.1. Introduction

A prerequisite for a successful over-the-air attack against the BP is the ability of the attacker to establish radio communications with the BP[4]. In order to do this, the attacker needs to either gain control over a base station belonging to a legitimate network operator's network (which is non-trivial in practice in most mobile networks in the western world), or force the victim's phone onto a base station under the control of the attacker (the latter having become easy and cheap due to the proliferation of the necessary technology).

There are various techniques for luring a victim's phone onto a malicious base station, and there are various methods to detect these techniques. Not all detection

[4] There are other means to attack the BP via manipulated firmware upgrades etc. that are out of scope for this technical briefing, and that are covered by different protection mechanisms part of all GSMK CryptoPhone products.

methods could be implemented in the BBFW as some of them would cause very high battery drain, or make the phone unfit for normal usage. Due to these technical constraints, the BBFW's network anomaly detection functionality is aimed primarily at detecting the most common and cheapest effective attack methods[5].

3.2. Events and warnings

The BBFW logs events that are indicative of the presence of a rogue base station as "persistent events" because they are not going away quickly. "No ciphering" and "operator change" events always cause a popup box with a warning or request to the user to provide his opinion on the event in question (typically requesting whether the user is in an expected roaming situation, in which a change of the network operator can be considered normal behavior).

A typical sequence of events that indicates the presence of an IMSI-Catcher is:

a) Network force-down from 3G to 2G
b) Current cell has no neighboring cells
c) Connection is not encrypted

In some cases a "value C1 is too large" warning might occur in addition. What has happened in such a case is that an attacker who wants to force all phones in the vicinity onto his malicious base station jammed the 3G bands while simultaneously providing his malicious 2G cell as an alternative. In order to ensure that the victims' phones camp onto his malicious cell and not onto one that the regular official cellular network provides, the attacker may make his own cell more attractive to the phones by manipulating the C1 value upwards (which causes a phone to use this cell even if it does not have the highest receiving power value). In order to prevent the victims' phones from leaving the attacker's malicious cell again, this cell does not publish a neighbor-cell-list that normally provides a list of alternative cells a phone can use. There are circumstances where each individual event can happen sometimes in isolated cases in badly configured networks, but the specific sequence of these events is a clear indicator that an IMSI-Catcher is in the vicinity.

Below is the list of events and warnings with explanations of their meaning:

- *Active connection without ciphering detected* (Warning box pops up): The "no encryption" warning is relevant to the user even in those cases that are just normal network malfunctions. Without GSM A5 encryption on the air activated, it becomes rather trivial even for a not very sophisticated attacker to listen in passively on cellular communications.

[5] For a system designed for comprehensive in-depth mobile network security monitoring based on stationary sensors aimed at detecting and localizing all types of rogue base stations, please inquire about the "GSMK Overwatch" system.

- *No neighboring cells detected*: The cell the phone is currently camping on does not advertise neighbor cells. This can sometimes happen in bad network conditions or on misconfigured networks. Without a neighbor cell list, it is hard for the phone to leave this cell.

- *Value C1 is too large*: The value C1 (in conjunction with C2, which for technical reasons cannot be retrieved from the CP500's BP) is used to model the "attractiveness" of a cell. Attackers frequently use unusually high values that are not found on regular cellular networks.

- *Location update (T3212) timer value is suspiciously small*: The location update timer (T3121) describes the interval after which the mobile station will perform a location update. Normally, the value is between two and 16 hours. If it is very small, then this can be an indication of an ongoing attack, as several attack techniques use the parameter to manipulate the mobile station's behavior.

- *Network operator change* (Warning box with requestor pops up): Under normal network conditions, and if there is no international or local roaming, the network operator does not change. There are a number of attack techniques that use fake roaming to lure the phone onto a malicious base station or that use SS7-based tricks to get access to the encryption keys needed for passive interception which use fake roaming cells. The user can manually acknowledge the roaming request if he is in a legitimate roaming situation, in which case the warning is cleared.

- *Network mode change (2G/3G)*: This event happens frequently during normal phone use, so it is only logged to provide context to the events listed above in order to allow better situational awareness. While this event is normal and harmless without any of the events above happening at the same time, in conjunction with one or multiple of the warnings listed above it becomes an important data point to detect an IMSI-Catcher-type attack.

Just as with the BP-AP behavior correlation, there are a number of positive events that provide context to a potential negative event that can cancel out the necessity of a warning. These events are:

- Location update timer now has normal value
- BB data activity due to WiFi connectivity status change
- Ciphering got re-enabled after being disabled
- Detected neighbor cells
- C1 value is now normal
- USSD activity
- Location area changed

If you plan to use the BBFW specifically to detect IMSI-Catchers in a specific geographic area, then it is strongly recommended to focus on the "active connection without ciphering detected" in combination with "no neighbor cells detected" events, especially when a 3G towards 2G network change has happened before them. Other warnings may pop up triggered by specific attack techniques, but not necessarily so. To weed out false positives it is recommended to have a second unit at a different location with a SIM card from the same operator (and, if possible, SIM cards bought at the same store at the same time) and compare the results. If the "no ciphering" warning is displayed simultaneously on both (spatially separated) locations it is likely a network problem (specifically, the network operator's home location register (HLR) having problems with handing out the encryption keys to the base stations due to some error or maintenance). Moving around a suspected IMSI-Catcher's location and verifying whether the warnings can be associated with a specific area is also a good technique to try.

About GSMK

GSMK Gesellschaft für Sichere Mobile Kommunikation mbH, headquartered in Berlin, Germany, is the technology leader in mobile voice encryption, secure messaging, and mobile device security. Established in 2003, the company develops, produces and markets voice and message encryption systems and mobile device security products for clients from the private and governmental sector. Its clients include military, police and public service clients as well as international organizations, mobile network operators, and enterprise customers from the banking, insurance, automotive, energy and raw materials industries. GSMK CryptoPhone® products are based on client-verifiable source code employing strong cryptographic algorithms that give customers an unprecedented level of security in mobile communications. GSMK was the first and still is the only company to offer commercial smartphones with defense-grade encryption strength, comprehensive 360-degree mobile device security, and client-verifiable source code. Today, GSMK can look back at satisfied clients in over 50 countries worldwide.