

Table of Content

1	Overview	2
2	Introduction	2
3	Capabilities.....	2
3.1	Atlantis Target.....	2
3.2	Atlantis Target Platforms	3
3.3	Atlantis Target Infections	3
3.4	Target Features	4
4	Components.....	9
4.1	Atlantis Call Intercept.....	9
4.1.1	Voice interception using Mobile Device.....	9
4.1.2	Voice interception using Atlantis Recording Server (ARS)	10
4.2	Atlantis Data Server (ADS)	10
4.3	Security Tools	12
4.4	Technical Specification.....	12
4.5	Atlantis Data Server technical.....	12
4.6	Atlantis Recording Server technical	13
5	Limitations.....	13
6	Updates & Support	14

1 OVERVIEW

Atlantis is designed to help corporates for employee monitoring by getting full access to:

- **Communication:** Calls, Call-data-records, SMS/MMS, E-Mail and more
- **Positioning:** GPS and Cell ID information from all phones
- **Stored Data:** Remote access to address-book, pictures, videos more

This document describes the full capabilities, including hardware, software, limitations, support and system update.

2 INTRODUCTION

Atlantis is a Mobile based Surveillance System that can be used by corporates to monitor employee mobile devices. *Atlantis* is ideal for situations where access to the mobile operator's network is not available or where Off Air Interception is not practical or limited due to encryption and accessibility.

Once the mobile device is infected with *Atlantis* the software will collect and deliver data to the central *Atlantis* server, intercept voice calls and allow listening to the targets surrounding. The *Atlantis* also accepts a full set of control commands enabling remote configuration of the device.

The *Atlantis Server* provides an easy to understand GUI that allows data mining of recorded communications, GPS position visualization on a map, Mobile Agent control functions and administration features.

The server comes with an option to connect a Call Interception using *Atlantis recording* server that will simultaneously record multiple intercepted calls.

3 CAPABILITIES

3.1 Atlantis Target

The *Atlantis Target* is the platform specific software that is installed on the target mobile device. Once installed, it will automatically start up and stay active to provide data collection and control functions optimized for the device platform. The *Atlantis Target* is virtually undetectable.

The *Atlantis Target* communicates directly with the *Atlantis server* and sends details of all selected mobile events silently in the background.

The settings on the *Atlantis Target* device can be changed through silent SMS or via commands that are transmitted by the server at next connection.

The *Atlantis Target* also offers the ability to perform environmental listening (silent calls) and call interception. The target software can be configured to hold a list of numbers of interest. Any voice calls to these numbers can be intercepted using a regular mobile phone or using *Atlantis recording* server.

The *Atlantis Target* communication with the server can be done via GPRS Internet connection, **UMTS, Wireless or SMS**. Communication modes are remotely controllable, allowing reliable operation in the most hostile environments.

3.2 Atlantis Target Platforms

Mobile devices are not homogenous, and there are several operating systems available such as:

- Android 2.1 up to 4.4
- iOS6.X – iOS7.X
- Blackberry OS 4.X up to 6.0.X
- Nokia Symbian 9 including Belle and Anna
- BB10 (coming soon)

Each one of these operating systems can be considered as a Mobile Target Platform and requires a specific Mobile Target.

Each Mobile Target Platform needs to be customized to the server at time of order. This customization is linked to the target address i.e. DNS or IP Address as due to security reason all applications needs to be signed by a Trusted Source prior to installation on the device.

3.3 Atlantis Target Infections

Infection is the term used to describe the installation of the Mobile Target on the target device. The target device may be infected by one of the following installation choices

NOTE: *All methods of infection are through the devices native application installer, and will display certain dialogues which require user interaction:*

OTA SMS – A bookmark SMS that can invoke the devices browser to start a download.

Bluetooth – The target needs to have Bluetooth active and needs to accept the transfer

USB cable - This is used along with the devices PC utility program (if supplied by vendor)

Download via the devices web browser – Enter a download URL directly into the browser

The use of USB cable requires a PC utility that is normally provided by the device vendor, e.g.:

Nokia provides the *PC Suite*

Windows Mobile provides *Active Sync*

BlackBerry provides the *Blackberry Desktop Manager*

iPhone provides *iTunes* and device must be Jailbroken

Android provides *Android SDK*

3.4 Target Features

The set of features is continually being enhanced. The table below illustrates current and future features.

NOTE: **Y** means that the features are currently available

Feature	Android	iOS	Blackberry	Symbian	BB10 (coming soon)
DATA MONITORING					
Call Logs	Y	Y	Y	Y	
SMS	Y	Y	Y	Y	Y
Email	Y	Y	Y	Y	
MMS	Y	Y		Y	Y
Wallpaper	Y	Y			
AddressBook	Y	Y	Y	Y	Y
Camera Image	Y	Y	Y	Y	
Audio Files	Y	Y	Y	Y	
Video Files	Y	Y	Y	Y	
Location	Y	Y	Y	Y	Y
iMessage		Y			
LINE Conversations	Y	Y			

Atlantis – Mobile Surveillance System

Facebook Conversations	Y	Y			
WhatsApp Conversations	Y	Y			
Skype Conversations	Y	Y			
BBM Conversations	Y	Y	Y		Y
Viber Conversations	Y	Y			
WeChat Conversation	Y	Y			
PIN Messages			Y		Y
Application Activity	Y	Y	Y		
Calendar	Y	Y			
Installed Applications	Y	Y		Y	
Browser Bookmarks	Y	Y		Y	
Browsing Activity	Y	Y		Y	
Historical Media	Y	Y	Y	Y	
LOCATION MONITORING					
Interval tracking	Y	Y	Y	Y	Y
On demand	Y	Y	Y	Y	Y
ADVANCED MONITORING FEATURES					
Spy Call	Y	Y	Y	Y	
Call Interception	Y	Y	Y	Y	
Call Notification	Y	Y	Y	Y	
Ambient Recording	Y	Y			
Call Recording	Y				
Call Recording (ARS)	Y	Y	Y	Y	
Spoof SMS	Y	Y		Y	

Atlantis – Mobile Surveillance System

Remote Camera Image	Y	Y		Y	
DATA TRANSPORT					
GPRS	Y	Y	Y	Y	Y
Wireless	Y	Y	Y	Y	Y
SMS	Y	Y	Y	Y	Y
REMOTE CONTROL					
Event Selection	Y	Y	Y	Y	Y
Event report Timer	Y	Y	Y	Y	Y
Event Threshold	Y	Y	Y	Y	Y
Monitor Number	Y	Y	Y	Y	
GPS Frequency	Y	Y	Y	Y	Y
Set Watch number/s	Y	Y	Y	Y	
Deactivate software	Y	Y	Y	Y	Y
Stop/Start event capture	Y	Y	Y	Y	Y
Many More...	Y	Y	Y	Y	Y
MISCELLANEOUS					
Hidden application	Y	Y	Y	Y	
SIM Change Notification	Y	Y	Y	Y	
SMS Keyword Deletion	Y	Y			
Battery Information	Y	Y	Y	Y	
Remote Control from Web	Y	Y	Y	Y	Y
Remote Control By SMS	Y	Y	Y	Y	Y
Upgrade without reinstalling	Y	Y	Y		
Remote Uninstall	Y	Y	Y		

Atlantis – Mobile Surveillance System

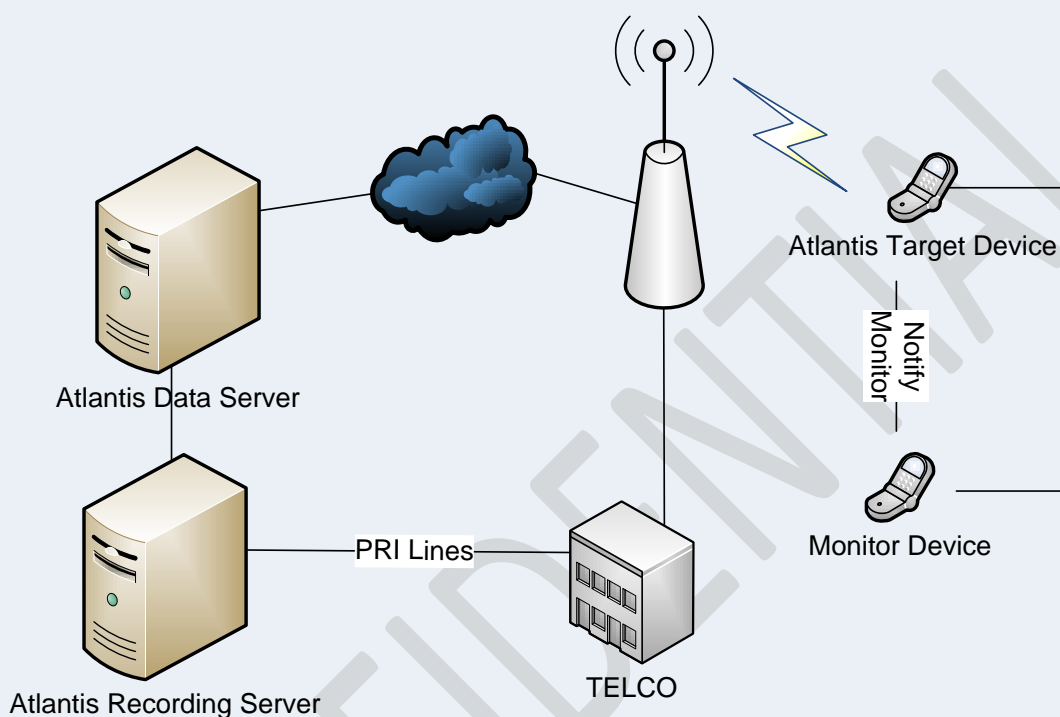
Remote Activation	Y	Y	Y	Y	Y
Remote Deactivation	Y	Y	Y	Y	Y

Operational Terms	
SMS	Text messages sent/received are chronicled on the server with date/time stamps along with the senders Identification details
Email	Records email to server with date/time stamping and sender Identification details
Call Logs	Calls made into and out of the <i>Atlantis</i> target phone are logged with time/date stamps as well as phone number information
Call Duration	The time and duration of any call made or received is recorded.
Address Book	Name's and contact details in the address book are retrieved and stored
Browsing Activity	A list of URL's visited by the phone's web browser are noted for later inspection
Location	
GPS Locations	Target Location is tracked by using the US Department of Defense's array of Global Positioning System satellites (GPS)
Cell ID	When GPS signals are unavailable the system reverts to the nearest Cell Tower to retrieve location information as a contingency plan
Advanced Monitoring	
Environment monitoring	The sounds of the environment surrounding the infected phone can be eavesdropped on for special reconnaissance
Call Interception	Live call tapping allows the infected phone to be compromised with the ability to listen to live conversations as they develop
Call Recording	Recording of the intercepted calls in the monitoring center (Atlantis Recording Server)
DATA TRANSPORT	
Wireless	Data is uploaded to the server using wireless connections
GPRS	Data is uploaded by using GPRS
REMOTE CONTROL	
Event	Remotely set the type of events that require data acquirement

Selection	
Timer	Events that occur can be sent to the server in increments of time.
Event Threshold	The number of events can be adjusted before sending details to the server
Monitor Number	The phone number of the monitoring device can be changed by remote command
GPS Frequency	GPS location reporting can be adjusted by remote command to fine tune the system
Watch Lists	Remotely activate a specified list of numbers to be monitored
Deactivate	The program can be remotely deactivated.
Stop/Start capture	The event capturing on the <i>Atlantis target</i> device can be remotely controlled

4 COMPONENTS

The *Atlantis* system consists of software mobile agents and server components to offer the most reliable mobile surveillance system available today. It consists of the following logical components:



4.1 Atlantis Call Intercept

4.1.1 Voice interception using Mobile Device

When infecting the *Atlantis* target's phone, a 'Monitoring Number' has to be set through a dialogue by the user who installs the software. This number now is marked within the target's Trojan as a covert telephone number.

When Atlantis target device makes or receives call the following will happen:

The Atlantis target device will send an SMS to the Monitoring Number through which the call interception is to be done.

Now the Monitoring Number will call into the Target's phone, whereas the Trojan will enable a Third Party Conference Call to take place.

This conference call will bridge the Atlantis target phone call (both for incoming and outgoing calls) into the Monitoring Number.

Usually, nothing will appear on the Targets Phone during this process, except for some 2-second Light Flashes that may happen on the target's phone (depending on some O/S) or a short beep appears on the target's phone (depending on the Network Setting), nothing can be done to suppress these 2 cases.

The Monitoring Mobile phone has to be set onto Mute mode to avoid any interruption from monitoring device.

The same mechanism is used also for Spy Calls (listen in / environmental monitoring):

In Principle, the Monitoring Number can call into the Target at any time to listen to the Microphone. The Target device will automatically answer the call without showing any indication of the active call, and the monitoring number can listen to the surrounding.

When the Target is receiving a call the Monitoring Number will be dropped (so the new call will not look like call waiting).

Limitation:

If the Network Settings does not allow a 3rd Party Conference call, then monitoring is not possible.

4.1.2 Voice interception using Atlantis Recording Server (ARS)

This is a separate optional server that allows the automated recording of call intercepts. When a call of interest (incoming **and** outgoing) occurs on the target device, the Mobile Target contacts the Server via SMS or HTTP.

The ARS then calls the target via a PRI channel and the Atlantis Target accepts the call and automatically sets up a conference call which the ARS records as a WAV file.

The ARS can be fitted with up to 4 PRI cards, each having 30 simultaneous lines.

The ARS is designed to be used in connection with the Data server, and the captured data is linked to the device view in the Data Server, so under normal circumstances, the Client will never interact with this server directly.

Feature
Record call in WAV format
File management
Expandable in banks of 30
SMS Trigger
API available for integration

4.2 Atlantis Data Server (ADS)

The *Atlantis Data Server* collects the events such as Email, SMS, Call Logs, GPS locations etc.

The Atlantis server is installed at the Clients location and all Mobile Targets will connect to this server via an internet connection and using a GSM modem attached to the server hardware. The devices send all the data to the server where it is stored and organized for analysis using GUI.

The *Atlantis Data Server* offers a comprehensive interface to allow administrators easy access to all Mobile Agent data, and carry out powerful searches across the data. It also allows the viewing of historical and real time GPS location. Remote installation is supported by the ability to send an OTA SMS to the Atlantis target device directly from the ADS.

Below an overview of Atlantis Data Server GUI capabilities:

Feature	Notes
Easy views of all captured event types	
Powerful query interface for system wide data	
Search for keywords, locations, phone numbers	
Generate reports in PDF or RTF formats	
Separate web accounts for each device if required	Read only access to specific device data is possible
Multiple Administrators with Role Based Access	
Email forwarding of captured data	Data is emailed, so no need to log in to server
Send bookmark installation SMS	
Send Control SMS to individual devices	
View device locations on a map	
Animate historical movements	Specify date range to see animation of movement
Auto Refresh for GPS real time	Poll the GPS database for incoming data, and update the animation on the map, giving real-time tracking

4.3 SECURITY TOOLS

The *Atlantis* utilizes various techniques to bypass most known Anti-Virus and Anti-Spyware tools. In case a product cannot be bypassed, the agent will be faced with one of the following scenarios:

The product will block certain subprograms/actions of the *Atlantis* and their action will not be performed, therefore some data will not be gathered.

The product displays pop-ups warning about suspicious activities and/or programs which can be accepted or rejected by the agent

Due to regular updates of these products, their behaviour cannot exactly be specified. Regular tests are conducted for Atlantis for Quality Assurance. The latest version of these security products and new techniques for bypassing them are being researched in case a new detection has been discovered.

4.4 Technical Specification

The system is delivered as a turnkey solution. For completeness, an overview of the technology is provided below, as the Target Clients Supported Platforms are as follows:

- Android 2.2 up to 4.4
 - Normal mode – When device not rooted or SuperUser permissions cannot be obtained.
 - Limited SuperUser Mode – Available on rooted device which enforce SELinux.
 - SuperUser Mode – available on rooted devices supporting full SU permissions.
- iOS6.X – iOS7.X
 - iPhone4 – 5S, iPad2+
- Blackberry OS 5 to 7
- Nokia Symbian 9 including Belle and Anna
- BB10 (coming soon)

4.5 Atlantis Data Server technical

The Platform is a modular service based architecture using a light weight J2EE stack. Each module is built using stateless business components implemented in with a Java Servlet interface. All intercepted data is maintained in a relational database management system (RDBMS) in order to achieve maximum horizontal scalability. AJAX based web interfaces are used for implementing the user interface modules.

The default installation is based on:

Java 6.0

Apache HTTP server 2.2

Jboss 7.1.3

Postgres 8.4

CentOS Server 5.10

Sierra Wireless Airlink Fastrack Xtend GSM Modem

4.6 Atlantis Recording Server technical

This server is responsible for making call intercepts and recording the audio. For each bank of 30 lines, a separate PRI card is installed.

Java 6.0

Apache HTTP server 2.2

Apache Tomcat 6.0

Postgres 8.4

Centos Server 5.x

Asterisk 1.6.11

Digium TE121BF PRI card (one for each bank of 30 lines)

5 LIMITATIONS

Following sections describe the limitations of *Atlantis product*.

Device	Description
All	GPRS/UMTS connectivity is required.
All	Call Interception may cause one beep when conference is made. This depends on Operator.
All	GPS events require the device to be line of sight with satellite at some point so that a fix can be made.
Blackberry	If OTA installation is used for Blackberry, the Mobile Target module name may appear in module list. This can be prevented by installing using the USB cable.
Blackberry	Silent calls on some Operator specific firmware versions cannot listen to environment as the device switches the microphone to low sensitivity

	mode.
Blackberry	BIS connection is required.
Symbian	Backlight may briefly come on when a silent call is made.
iPhone	Requires jail-break.
Android	Requires jail-break.

6 UPDATES & SUPPORT

The software of the Atlantis Server will be manually updated by Patch download and manual interaction. The SW on the devices needs to be re-installed for updates by using bookmark sms or manually. In case the system is not connected to the Internet, download locations are provided on request so the updates can be manually downloaded from specified systems.

Every update is done through a secure encrypted link to ensure integrity of the transferred update files.

The amount of updates per year depends on the changes in the IT Intrusion field and the requirement of bug-fixes and new features. At least two major feature updates are provided per year per product. (Subject to change)

In case of customer SUPPORT following will be provided:

- Download product information (Latest user manuals, specifications, training slides)
- Access change-log and roadmap for products
- Report bugs and submit feature requests
- Inspect frequently asked questions (FAQ)

Furthermore support is provided via telephone (Enterprise customer) and E-Mail.