]HackingTeam[

RCS Certificates

Case Study

Contents

Important Notice

HT s.r.l. shall bear no responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any HT s.r.l. product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any HT products. Information in this document is subject to change without notice and does not represent a commitment on the part of HT s.r.l. The systems described in this document are furnished under a license agreement or non-disclosure agreement.

All information included in this document, such as text, graphics, photos, logos and images, is the exclusive property of HT s.r.l. and protected by international copyright laws. Permission is granted to view and photocopy (or print) materials from this document for personal, non-commercial use only. Any other copying, distribution, retransmission or modification of the information in this document, whether in electronic or hard copy form, without the express prior written permission of HT s.r.l., is strictly prohibited. In the event of any permitted copying, redistribution or publication of copyrighted material, no changes in, or deletion of, author attribution, trademark legend or copyright notice shall be made.

1 Overview

RCS uses a variety of certificates to let the RCS Agents gather information on each device. Certificates are mandatory and cannot be avoided for proper functioning of RCS Agents.

NOTE	Symbian aside, all the certificate are provided by HT at no additional cost for the Customer.

Certificates are organized into three categories:

1. Certificates from an existing Certification Authority (**Type 1**)
2. Certificates with no identification information (**Type 2**)
3. Self-signed certificates (**Type 3**)

Type 1 certificates bear full details about the requestor, such as company name, address, technical contacts, and administrative contacts.

Type 2 certificates are uniquely bound to the requestor but no information is directly accessible. Information about the requestor can be asked to the Certification Authority that issued the certificate; sometimes that information is available via public databases as well.

Type 3 certificates are created by the software itself or by the Customer, and are self-signed. They bear no direct information about the requestor and, *unless* the same information is used (certification authority name, location…) each time a new certificate is created, there's no way to identify them as part of an RCS installation.

On specific architectures, more than one certificate may be required.

1.1 Symbian certificate

A Symbian Developer Certificate for up to 1000 IMEIs and 17 capabilities is required to install and run the RCS Agent on Symbian devices: this is due to the highly restricted nature of Symbian platforms. Unsigned applications haven't been allowed to run in any way starting from Symbian OS 9.1.
The Customer is required to buy a *Developer Certificate* from TrustCenter.

NOTE	The procedure to request a Symbian certificate and how to use it is detailed in the RCS manuals and provided as basic training upon purchase of the Symbian Platform.

2 Visibility

Information stored into certificates may be visibile to the Target. Two levels of visibility identify how much information the Target can access:

1. Certification information is not exposed without Target's intervention, but is accessible if the Target performs specific actions, for example browses the package properties.

2. Certification information may be obtained by extracting the signed binary from the RCS Agent, then performing further analysis on it. The certificate and its information are available only upon disclosure of the RCS Agent presence.

3 Architectures

Here is a list of all the supported RCS Agent architectures with their respective requirements for certificates:

Android

Type 3 certificate required.

BlackBerry

Type 2 certificate required.

iPhone

No certificate is required.

MacOS

No certificate is required.

Symbian

Type 2 certificate required after 21/Jun/2011, *type 1* certificate required for Agents signed before 21/Jun/2011.

Windows 32-bits

No certificate is required.

Windows 64-bits

type 1 certificate is required for kernel component.

Windows Mobile

Type 1 certificate is required for dropper

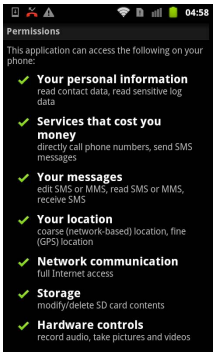
Type 3 certificate is required for Agent.

4 Analysis

Listed below is a risk analysis in case an Agent is identified, extracted and analysed.

4.1 Android

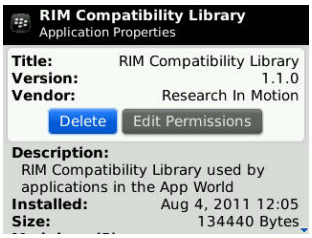
Certificate information is exposed only in case of a binary analysis of the Agent. A Type 3 certificate is currently provided by HT, thus disclosure of the Customer's identity is impossible.



4.2 BlackBerry

Certificate information is exposed only in case of a binary analysis of the Agent. T*ype 2* certificate is used, thus presenting no immediate danger of identification.

Currently the certificate is provided by HT, due to signing requirements during development process.



4.3 iOS (iPhone/iPad)

No certificate is used by the Agent on iOS platforms.

4.4 Mac OS X

No certificate is used by the Agent on OS X platforms.

4.5 Symbian

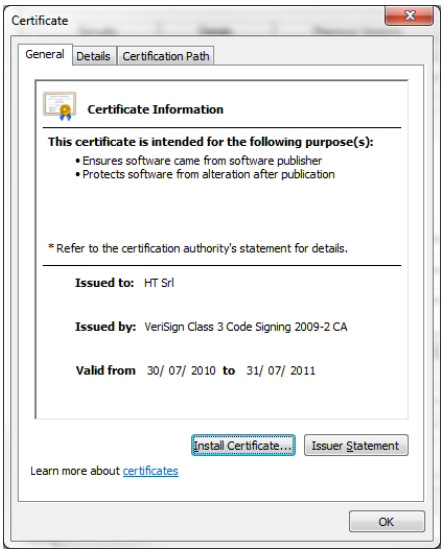
The Certificate information can be exposed by Target actions and by binary analysis of the Agent executable. *Type 2* certificate is used starting from 21st July 2011, posing no immediate risk of identification. Installations performed before 21st July 2011 uses *Type 1* certificates, thus showing identification information. Certificate is must be provided by the Customer.

4.6 Windows 32-bit

No certificate is used by the Agent on Windows 32-bit platforms.

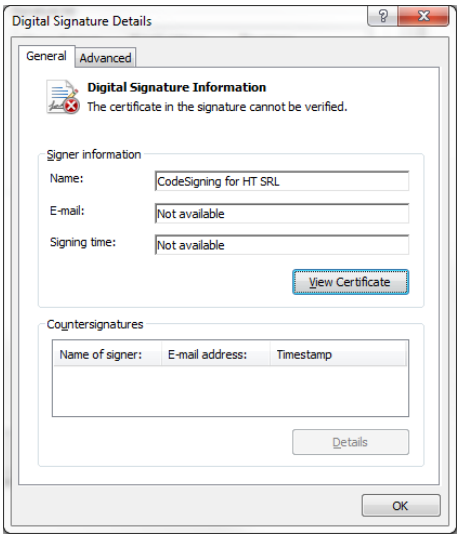
4.7 Windows 64-bit

The Certificate information can be exposed by Target actions and by binary analysis of the Agent executable. A T*ype 1* certificate containing company name and location information is used. Danger of identification is immediate if RCS or associated components are identified, extracted and analysed. Currently the certificate is provided by HT.



4.8 Windows Mobile

The Certificate information can be exposed by Target actions and by binary analysis of the Agent executable. T*ype 1* and T*ype 3* certificates are used. Danger of identification exists *only* at infection time. After this stage the component carrying *Type 1* certificate is erased from the system and only components using *Type 3* certificates are kept on the device.



5 Costs

Type 1 and T*ype 2* certificates must be acquired from Certification Authorities, the price may vary and there might be yearly subscription fees.

Android

Free.

BlackBerry

20 USD *una tantum*.

Symbian

200 USD, yearly fee.

Windows 64-bits

499 USD, yearly fee.

Windows Mobile

450 USD at subscription, 100 USD yearly fee or after signing 10 times.

]HackingTeam[

RCS Exploit Portal

Whitepaper

Important Notice

HT s.r.l. shall bear no responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any HT s.r.l. product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any HT products. Information in this document is subject to change without notice and does not represent a commitment on the part of HT s.r.l. The systems described in this document are furnished under a license agreement or non-disclosure agreement.

Document Approval

Revision	Author(s)	Release Date
1.1	Valeriano Bedeschi	6th December 2011

Table Of Contents

1 Overview

Every software application contains a discrete number of security holes (aka *vulnerabilities*) that can be *exploited* to take control of the software itself in order to install unwanted applications.

Relying on those security holes, it's possible to turn normal documents into installation vectors for RCS.

HackingTeam Exploit Portal, part of the Remote Control System platform, is a service that embeds an RCS Agents into common file formats, such as *Adobe PDF*, *Microsoft PowerPoint* and *Word documents*.

Installation of the RCS Agent is started as soon as the target opens the exploit document.

2 The Service

HackingTeam combined its expertise in offensive security and software design to build a service that make simple to prepare and use exploits as installation vectors for RCS agents.

2.1 What is an exploit?

An exploit is a piece of software that can be injected into flawed software, to take control of it.

In the layman view, exploits are seen as part of an elite hacker toolkit: some obscure piece of code usable only by those who know the most obscure hacking techniques.

That was true since the introduction of the exploit portal, which made those techniques accessible even to untrained personnel.

2.2 Why a Portal?

HackingTeam Exploit Portal is a repository of client side exploits ready to be used.
Each exploit available was selected for its effectiveness against common application software, such as web browsers and office applications.

The exploit repository resides on HackingTeam servers, and it can be easily accessed from within the RCS Console.

Each time the operator access the Exploit Portal, the Console downloads the updated exploit list that allows for the creation of documents containing an RCS Agent.

NOTE Since exploits base their effectiveness upon software flaws, the list of available exploits may change at any time, therefore supported file formats may vary frequently.

2.3 Exploit Categories

Within the Exploit Portal exploits are organized in categories: each category specifies if whether the exploit is commonly available or exclusive to the Exploit Portal, and if the security hole it uses is publicly known or secret to everyone but HackingTeam.

As an example, for exploits categorized as *public*, the vulnerability they use is known and the raw exploit code is publicly available. This means that probably the effectiveness of this kind of exploit is not at its best, but they still work and probably the vulnerable application is still in wide use.

The exploit portal uses four categories to organize the available exploits:

Category	Description
Social	This category of exploits do not rely on security holes, but on errors made by the human target in opening the document. For example, an executable file can be concealed as a PDF by relying on the fact that Windows normally hides common file extensions: the target will see the usual file icon he's used to see on real PDF files, thus making him believe that it's safe to double click on it and open the document.
Public	For this category, the software flaw is known and the exploit code is publicly available on the Internet, tough the vulnerable version of the application is considered still widely adopted by a large user base.
Private	The exploit relies on a known vulnerability, but there is no public exploit code. No technical information is available on the vulnerability, so writing an exploit is a difficult task.
Zero-day	The exploit relies on a vulnerability not even known by the vendor of the application itself, and no exploit code is available. The latest version of the software is almost always vulnerable, thus making this exploit very effective even against users that update their installed applications frequently.

This categorization permits you to have a wide selection of usable exploits, targeting different applications and file formats. Therefore, depending on the specific scenario you're confronting with, you may want to preserve private or zero-day exploits as last resorts, first using the more expendable social and public exploits.

NOTE The Exploit Portal always contain at least three zero-day level exploits.

]HackingTeam[

RCS Network Injector

Datasheet

Important Notice

Document Approval

Revision	Author(s)	Release Date
1.1	Valeriano Bedeschi	6th December 2011

Table Of Contents

1 Overview

HackingTeam's *Network Injector* (NI) installs RCS Agents over the Target's Internet connection by using a patent-pending injection technique and a proprietary streaming melting technology.

Network Injector is capable of inserting an RCS Agent into any downloaded executable file and browsed web page, without visible changes in the content.

Deployment of the Network Injector can be done inside any network: from small home WiFi networks to geographically distributed Internet Service Providers.

Multiple users can be monitored and different types of injection are available, such as injection into web pages or downloaded applications.

1.1 Deployment scenarios

The Network Injector can operate in different network scenarios, either on a LAN or an intra-switch segment. Two network links are necessary for placing the device on the target network, one for monitoring and one for injection.

NOTE In case of failure of the appliance, there is no risk of connection shortage, since the IPA is not an inline device.

1.1.1 Monitoring

The first link is used for monitoring the traffic on the tapped LAN segment, either by using a mirror port of the switch (SPAN port), a network TAP interface (transparent inline connection) or a WiFi card in monitor mode.

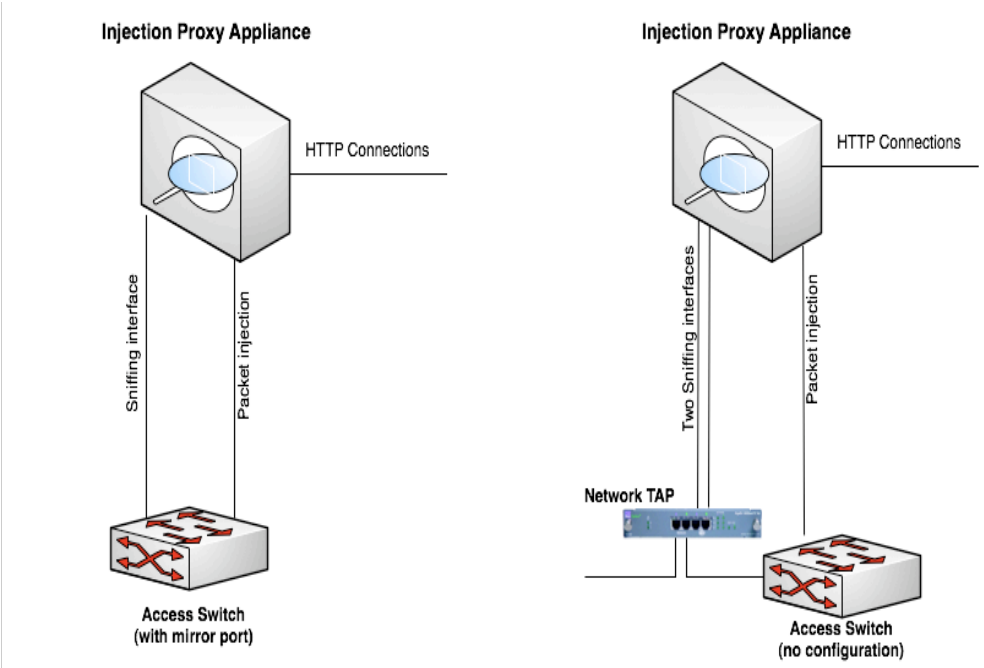


Figure 1 - Common IPA deployment scenarios

By using dedicated wire-speed network interfaces, IPA is compatible with many physical network links, and is capable of monitoring them even when running at full speed.
Connectors (GBIC) are provided for monitoring with Ethernet copper and Fiber Optic links.
NI can cope with up to 10Gbps traffic, and usually comes in two versions, with four 1Gbps ports or one 10Gbps port.

1.1.2 Packet injection

This second link is used for transparently proxying HTTP connections and crafting packets during the injection phase.

For the purpose of crafting packets, a valid IP address is required, better if on the same network under monitor.

> **NOTE** No disruptive packets are sent from the IPA.
> In the worst case, only connections related to the target under investigation may be in any way affected, dropper or modified.

Depending on the security policies present on the injection network, it may be necessary to allow some traffic on switches and routers for the IPA to work properly.

1.1.3 Management

Multiple Network Injectors can be separately managed trough the RCS Console: a different set of rules, unique to each NI, can be configured.

1.2 Deploying at the ISP

The most common scenario of deployment at the ISP is to monitor the ADSL line of subscribers under investigation.

When the Network Injector (NI) is placed on a network segment between the DSLAM concentrator and the ISP core network, any subscriber connected to the DSLAM can be monitored.

Identification of the specific subscriber can be done using one or more of the following criteria:

- RADIUS parameters
- Subscriber username
- Calling station ID
- Session ID
- NAS IP Address and NAS Physical Port
- Static IP Address
- String matching (e.g., email address, social network login)
- DHCP information

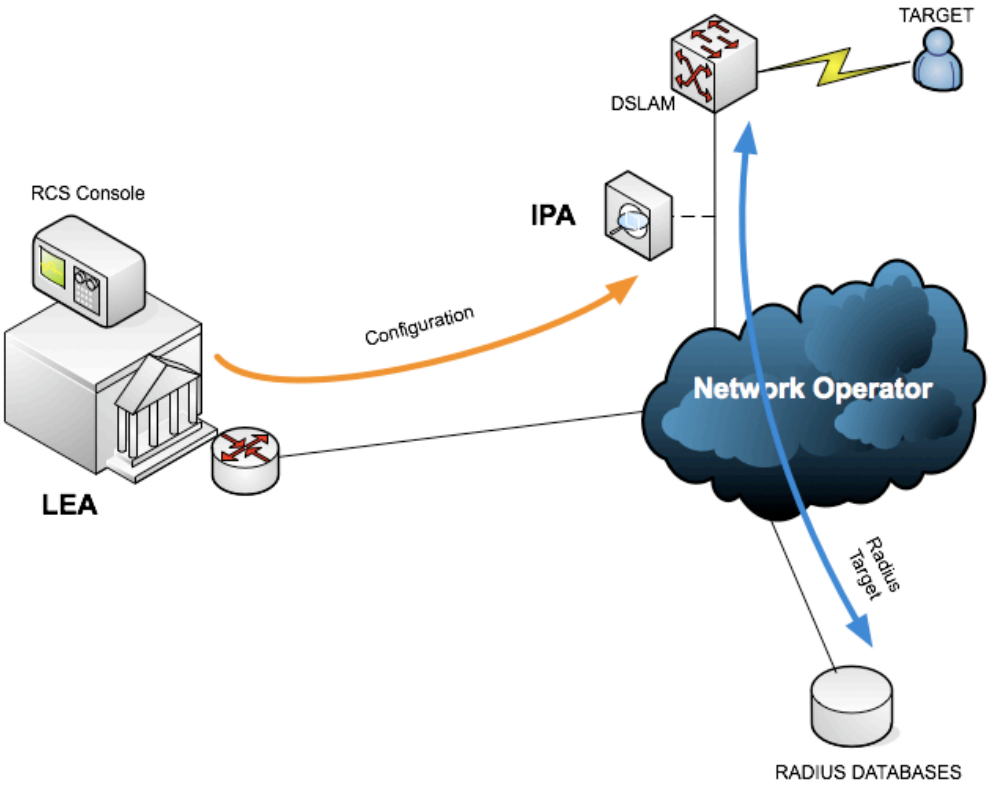


Figure 2 - ISP deployment

NOTE Installation and deployment of Network Injector on a ISP network is subject to validation by HackingTeam Engineers.

1.3 Usage in WiFi networks

If the target user is joined to a WiFi network, Network Injector must be equipped with two WiFi cards. One card is joined to the same network of the target, while the other card monitors the traffic of the same network.

2 Agent Deployment

Network Injector (NI) can embed RCS agents into different resources available on the web.

Resource	Description
Executable file	An RCS agent is embedded into any downloaded executable (e.g., setup packages, automatic software updates)
Web page	NI is able to inject special HTML code into any web page, triggering the installation of RCS agent during web browsing.
Any resource	Any resource download by the user can be replaced with an exploiting document generated by the Exploit Portal

]HackingTeam[

Remote Control System

Whitepaper

Important Notice

HT s.r.l. shall bear no responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any HT s.r.l. product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any HT products. Information in this document is subject to change without notice and does not represent a commitment on the part of HT s.r.l. The systems described in this document are furnished under a license agreement or non-disclosure agreement.

Document Approval

Revision	Author(s)	Release Date
1.1	Valeriano Bedeschi	6th December 2011

Table Of Contents

1 Overview

In modern digital communications, encryption is widely employed to protect users from eavesdropping.
Unfortunately, encryption also prevents law enforcement and intelligence agencies from being able to monitor and prevent crimes and threats to the country security.

Remote Control System (RCS) is a solution designed to evade encryption by means of an agent directly installed on the device to monitor. Evidence collection on monitored devices is stealth and transmission of collected data from the device to the RCS server is encrypted and untraceable.

RCS installations are deployed at the Customer's premises, thus guaranteeing to the Customer total control on its operations and security.

NOTE HackingTeam have no way of connecting to or receiving any information from the Customer's RCS installation.

Please refer to Figure 1 for a scheme of a standard Remote Control System installation.

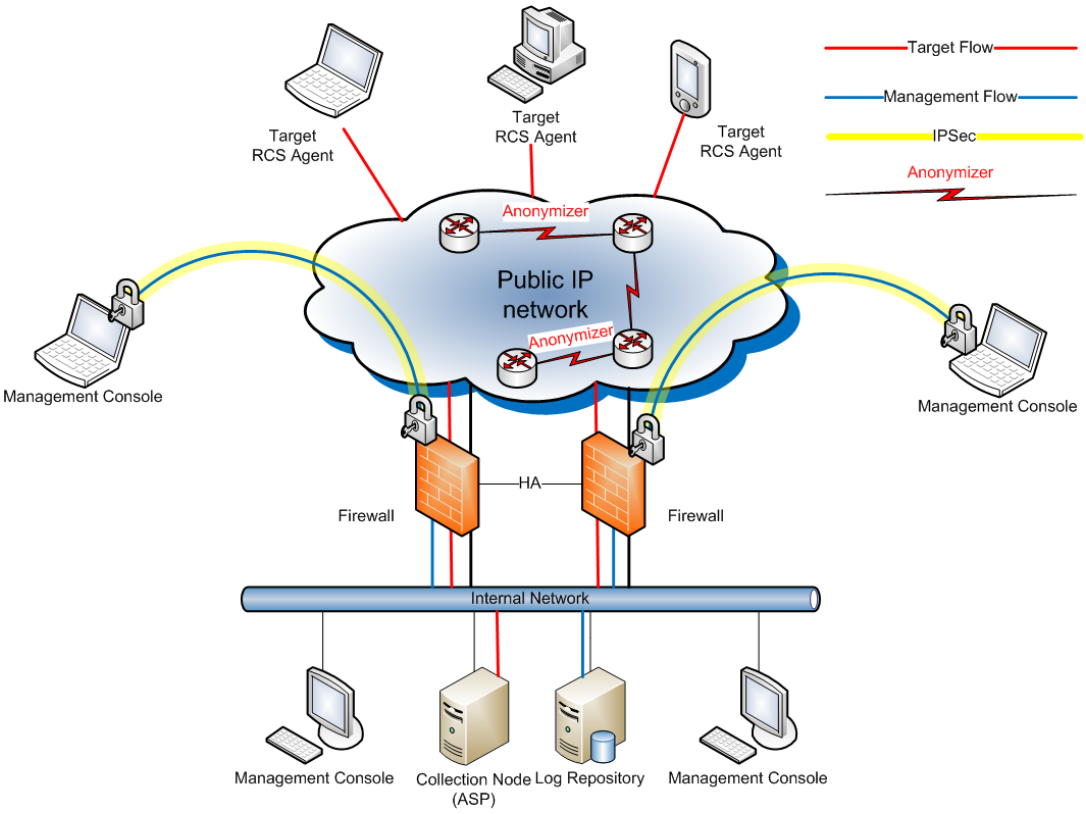


Figure 1 - Standard RCS installation

The RCS infrastructure is made of different components: one part resides at the Customer's premises, while another part is meant to be installed on the devices to be monitored.
Furthermore, some components are intended to be installed on different networks, such as Internet Service Provider's.

1.1 Naming conventions

Remote Control System's main architectural components are:

- Front End (Collection Node – ASP)
- Back End (Database – Log Repository)
- Management Console
  - Admin User
  - Tech User
  - Log Viewer User
- Target
- Anonymizer

2 Customer Side Components

2.1 Front-End

The Front-End receives connections from Agents running on intercepted devices. It acts as an isolation barrier for the Back-End, augmenting the security of the installation.

Data received by the Front-End is sent to the Back-End for decryption and processing. When new Agents configurations are available, the Front-End sends them to the interested devices.

All connections entering and leaving the Front-End are encrypted and authenticated, and can be decrypted only by the Agents. No other component is capable of decryption, thus guaranteeing total security during the Agents to Front-End communication.

A Front-End must be reachable over the Internet by a public IP address: the Agents must be able to reach the Front-End from anywhere, giving you control over the devices, anywhere they could be.

At least one Frontend is needed in order to receive data from the Agents.

Software requirements: Windows 2003 or 2008.

2.2 Back-End

The Backend server is the core of the whole infrastructure. It stores all the data collected from the Agents and handles the requests coming from the management Consoles.

All the RCS data is stored inside a standard relational database, thus extra capabilities, such as automatic backup and custom data mining can be implemented upon Customer request. The Backend can use a Storage Area Network (SAN) to enable redundancy and failure resistance.

Server sizing is dependent on the number of concurrent Targets and data retention policies.

Backend server must be installed inside the Customer's network.

Software requirements: Windows 2003 or 2008.

2.3 Management console

The RCS Console is the application used for accessing and controlling all the Remote Control System (RCS) functionalities.

Operators can be profiled to grants different level of access to the system:

- **Admin**: create users and groups, grant privileges, manage investigations, audit the system.
- **Technician**: create vectors for targets infection and configure/re-configure agents behavior.
- **Viewer**: browse evidences coming from the targets, classify and/or export them.

A single Operator can be granted more than one privilege.

Using the Alerting panel, it is possible to setup custom alerts to warn a group of Operators when evidence of interest is received.

Operators can handle all the multimedia evidences collected, such as screenshots and phone calls, from within the Console, from which they can also be exported in their native format (e.g. jpeg images, mp3 audio files) to be processed by external equipment.

The health status of each component of the system can be monitored from the Console, and the system is capable of alerting a group of Operators in case there is a problem with any component.

All the communications between the Console and the Backend are encrypted using SSL.

The Console can be installed on any pc/workstation running Windows, OS X or Linux. If the customer needs to access the data from outside its own network, a standard VPN solution can be used to permit the Console to connect to the Backend.

The Console must be able to connect to the Internet to download some information such as satellites maps for target tracking.

NOTE	A list of all the URLs that must be accessible for the Console to operate is available, in case the Customer's network is firewalled.

Software requirements: Windows, MacOS X or Linux

3 Target Side Components

3.1 RCS Agent

The RCS Agent is the software component that monitors the target computer or smartphone. Installation of the Agent is performed by means of different installation vectors.

Once installed, the Agent sends all the collected data to the Frontend, by using any of the device's Internet connections. The Agent can be configured to collect different kind of data (e.g. screenshots, phone calls) from the target device. Data are first stored, encrypted and hidden, on the device itself, until there is an Internet connection available to send them.

Operators can reconfigure the Agents behavior at any time through the Console: a new configuration is made active upon the next time the Agent connects to the frontend.

Such an asynchronous channel of communication, and the set-and-foget configuration capabilities of the Agents were specifically designed to eliminate the need for an Operator to stay in front of the Console waiting for interesting data to be collected.

RCS Agents are autonomous and can be configured to react on specific events with different actions, allowing them to adapt to different situations that may occur on the target device, even if there is no current communication between the Agent and the Frontend.

All communications between Agents and Frontends are encrypted with strong encryption algorithms and mutually authenticated, preventing any possibility of eavesdropping or leakage of information.

The Agent for Windows and Mac systems uses standard Internet connectivity through LAN or WiFi, and it's capable of connecting even in enterprise environments, where network firewalls and/or proxies are usually in place.

The Agent for smartphones can be configured to use several methods of communication (see below) such as 3G network, Wi-Fi, BlueTooth or USB connection with a laptop or desktop system.

The RCS Agent is resistant to most endpoint security technologies available on the market, such as antiviruses, personal firewalls, antispyware, antirootkits and analysis tools, as well as restoration technologies, such as DeepFreeze, commonly found in Internet Cafes.

The Agents can be controlled and configured uniformly using the RCS Console: all the differences between the various OSs are made transparent to the Operator.

Functionalities available for each platofmr may vary (please refer to the attached Compatibility List).

3.2 Agent Deployment

RCS Agent must be installed on target devices in order to monitor them, and installation can be performed either locally or remotely.

3.2.1 Local installation

When physical access to the target device is available, local installation can be very effective. Some specific local installation vectors are available, such as bootable CDs and USB storage for desktop systems, or memory card infection and USB cable connection for smartphones.

3.2.2 Remote installation

Remote installation may require some information about the target to be already available to the Operator: information like the ISP used by the target for connecting to the Internet or his e-mail address can be of great help in preparing an effective installation vector.

3.2.2.1 Melting tool

Melting inserts an Agent inside any existing executable file, such as application installers. As soon as the file is executed on the target device, RCS Agent is installed.

3.2.2.2 Exploit portal

The Exploit Portal, by making use of unwanted security holes in common applications, allows for embedding of RCS Agents into common file formats, such as *Adobe PDF*, *Microsoft PowerPoint* and *Word documents*.
Installation of the RCS Agent is started as soon as the target opens the document.

3.2.2.3 Network Injector

The *Network Injector* (NI) installs RCS Agents over the Target's Internet connection by using a patent-pending injection technique and a proprietary streaming melting technology.

Network Injector is capable of inserting an RCS Agent into any downloaded executable file and browsed web page, without visible changes in the content.

Deployment of the Network Injector can be done inside any network: from small home WiFi networks to geographically distributed Internet Service Providers.

Multiple users can be monitored and different types of injection are available, such as injection into web pages or downloaded applications.

3.2.2.4 Remote Mobile Infection

Remote Mobile Installation (RMI) is a module for the *Remote Control System* (RCS) platform designed to install RCS Agents on mobile phones.

RMI works by sending a wap-push message to the target smartphone. When the SMS is received and accepted by the user, a browser is automatically opened and the Agent installation package is downloaded from the URL embedded in the message.

The text message can be customized, thus enabling use of *social engineering* techniques to their full extent: for example, by pretending to be the telecom operator offering promotions or updates, chances of success in installation of the Agent are dramatically increased.

3.2.3 Uninstallation

Each Agent can be uninstalled remotely from the Console: uninstallation completely removes the Agent from the device.

3.2.4 Retrievable data

Evidence collected from Windows and Mac target include the following:

- Opened files (documents, images, data, etc.)
- Screen snapshots
- Web Browsing
- Mouse clicks
- Application passwords recovery (Outlook, MSN, Internet Explorer, Firefox, etc.)
- Keystrokes (any language settings)
- Clipboard
- Printed documents
- E-mails
- Location tracking (Wi-Fi info)
- Remote Audio Spy (Microphone)
- File system explorer
- Software/OS/Hardware information
- Camera Snapshots
- VOIP calls (Skype, MSN, Yahoo)
- Chat/IM (Skype, MSN, Yahoo, ICQ, etc.)
- Execute commands of operator's choice
- Upload and download files of operator's choice

Evidence collected from smartphones include the following data:

- Phone calls
- Organizer/Address book
- SMS/MMS
- E-mails
- Screen snapshots
- Location tracking (cell signal info, Wi-Fi info, GPS info if available)
- Remote audio Spy
- Camera Snapshots
- SIM Information

3.2.5 Event/Action logic

The RCS Agent is able to recognize different events happening on the target device, reacting to them with specific actions.

For example, the following combinations of events and actions can be configured to raise the chances of collecting relevant evidence and prevent the Target from becoming aware of the Agent presence on his device.

Here is a list of common examples of specific configurations that we advice to our Customers.

- When the screen saver starts, send the collected evidence to the Frontend
- When a given GPS position is reached , start the microphone recording (we suspect our target is going to have a meeting
- If battery or disk space run too low, stop recording the audio to prevent
- When receiving a phone call, take a snapshot with the front facing camera
- 30 days after installation of the Agent, uninstall the Agent itself and stop the investigation

The Operator is free to combine events to actions to fit his needs and better address each specific investigation.

3.2.6 Communication

While Agents for Windows and Mac have better chances to find a LAN or WiFi connection available anytime during the day, the Agent for smartphone may be much more limited in the availability of an Internet connection, therefore on smartphones we made available much more methods for the Agent to communicate.

GPRS/UTMS/3G+ RCS Agent is able to use any existing data connection, eventually forcing it if it's been actively disabled by the Target. If the Target doesn't have a flat rate data plan on the phone, it's possibile to configure to Agent to use a different APN, preventing any unwanted entry to appear on the Target's billing for the connections issued by the Agent.

Wi-Fi: the Agent automatically recognizes and uses any open/preconfigured wireless Access Point (e.g. hotel and home WiFi networks).

SMS: the Agent can send an SMS containing specific information such as SIM information or GPS position to a preconfigured phone number.

NOTE It's not possible to use SMS to send collected data to the Frontend.

USB: if the smartphone is connected to a desktop for charging or synchronization, the agent can use the desktop Internet connection to send the collected data.

3.2.7 OS compatibility

RCS Agents can be installed on:

- Windows XP, Vista, 7 (32/64 bit)
- MacOs X 10.6 Snow Leopard, 10.7 Lion
- Windows Mobile 6, 6.5
- iOS 3, 4 (iPhone/iPad)
- Symbian S60 3rd and 5th edition
- BlackBerry 4.5 or newer

4 Public Side

4.1 Anonymizers

Anonymizers are used to avoid exposing the real IP address of the Front End, by setting up a geographically distributed network capable of bouncing the connection between an Agent and its Frontend among different countries.

Since connections between anonymizers are fully encrypted and no data decryption is performed on them, they can be placed even in untrusted networks or countries.

Management of the Anonymizers is performed through the RCS Console, where chains of Anonymizers can be configured and changed at any time.

]HackingTeam[

RCS Remote Mobile Infection

Datasheet

Important Notice

HT s.r.l. shall bear no responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any HT s.r.l. product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any HT products. Information in this document is subject to change without notice and does not represent a commitment on the part of HT s.r.l. The systems described in this document are furnished under a license agreement or non-disclosure agreement.

All information included in this document, such as text, graphics, photos, logos and images, is the exclusive property of HT s.r.l. and protected by international copyright laws. Permission is granted to view and photocopy (or print) materials from this document for personal, non-commercial use only. Any other copying, distribution, retransmission or modification of the information in this document, whether in electronic or hard copy form, without the express prior written permission of HT s.r.l., is strictly prohibited. In the event of any permitted copying, redistribution or publication of copyrighted material, no changes in, or deletion of, author attribution, trademark legend or copyright notice shall be made.

Document Approval

Revision	Author(s)	Release Date
1.1	Valeriano Bedeschi	6th December 2011

Table Of Contents

1 Overview

Remote Mobile Installation (RMI) is a module for the *Remote Control System* (RCS) platform designed to install RCS Agents on mobile phones.

Installing RCS Agents on smartphones from remote, without any help, is not an easy task. Worse yet, if remote installation fails, installation may become a tough task: it may be impossible to have physical access to the device.

Remote Mobile Infection (RMI) makes remote installation *easy*, *repeatable* and *effective*.

RMI works by sending a wap-push message to the target smartphone. When the SMS is received and accepted by the user, a browser is automatically opened and the Agent installation package is downloaded from the URL embedded in the message.

The text message can be customized, thus enabling use of *social engineering* techniques to their full extent: for example, by pretending to be the telecom operator offering promotions or updates, chances of success in installation of the Agent are dramatically increased.

Message delivery to the mobile phone is done using common cellular protocols, such as GSM, Edge, 3G or UMTS, and is supported by the vast majority of the mobile operators all over the world.

RMI is fully integrated into the RCS Console and is therefore very easy to use: to perform an installation, you just need the mobile phone number.

1.1 Types of messages

RMI supports different methods for sending messages, each differing in the way the message is presented to the target user.

1.1.1 Update Notification

By using a dedicated GSM modem an update request can be crafted and sent to a remote mobile device.

According to mobile device security and the target platform (e.g. Blackberry, Windows Mobile), the notification message is presented to the user asking for confirmation: for installation to complete, the user must confirm.

NOTE Blackberry and Symbian phones WILL ask the user how to proceed, either to install the update or discard the message.

1.1.2 Web Redirection

By forcefully starting the web browser and redirecting to the specified website, the Agent installation is downloaded and executed.

Adding carefully chosen text, the user is tricked in accepting the message, increasing the effectiveness of the attack.

1.1.3 Service Notification

This attack opens a window containing a custom message and a URL link. Once the target accepts the message, the web browser is automatically redirected to the URL, thus starting the Agent installation.

2 FAQ

DOES RMI PERFORM A MAN-IN-THE-MIDDLE ATTACK?

No, RMI doesn't perform a MITM attack. It works by redirecting the browser toward a URL where a RCS backdoor is located.

DOES RMI ACT LIKE A FAKE BTS?

No, RMI is not an active tool like a BTS: there's no need to be close to the target device.

DOES RMI USE A FAKE APN?

No, RMI doesn't use a fake APN.

DOES RMI RELY ON ANY VULNERABILITY?

No, RMI takes advantage of wap-push messages, which are part of the GSM standard.

WHAT ARE THE BEST AND WORST CASE SCENARIO?

In the best case, the backdoor is automatically run on the target device, without any kind of user interaction. On the contrary, in the worst case the device asks for permission to execute the payload located at the specified URL, thus requiring some social engineering to trick the user into accepting the message.

WHICH PHONES SUPPORT RMI INFECTION?

RMI can be used on smartphones that run Windows Mobile, BlackBerry, Symbian or Android operating systems.

DOES RMI WORK ON ANY PROVIDER?

RMI works on every provider unless they are actively blocking wap-push messages.

]HackingTeam[

RCS Tactical Device

Datasheet

Important Notice

HT s.r.l. shall bear no responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any HT s.r.l. product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any HT products. Information in this document is subject to change without notice and does not represent a commitment on the part of HT s.r.l.
The systems described in this document are furnished under a license agreement or non-disclosure agreement.

Document Approval

Revision	Author(s)	Release Date
1.0	Valeriano Bedeschi	16th April 2012

Table Of Contents

1 Overview

HackingTeam's *Tactical Device* is a laptop computer that can be used to perform different tasks in a tactical scenario when the operator has the ability to physically be close to the target. The disk is entirely encrypted in order to guarantee security.

The Tactical Device contains software that allows the operator to infect the target with RCS Agent using the Tactical Network Injector capabilities. It also support the cracking process of the Wi-Fi encryption key and the identification of the target while the operation is in progress.

Deployment of the Tactical Device can be done inside any network: from small home Wi-Fi networks to public hotspots (airports, pubs, hotels).

The Tactical Device comes with all the equipment needed: Wi-Fi network cards, Ethernet adapters and a 3G modem to guarantee connectivity in any scenario.

Wi-Fi cards support all the standard networks (802.11a, 802.11b, 802.11g, 802.11n), and optionally provide removable antennas with RP-SMA connectors that allow the operator to use any kind of external equipment.

Additional batteries are provided for long tactical operations, besides power adapters and a hard case for carrying everything safely.

1.1 Deployment scenarios

The target infection using the Tactical Device consists in two different steps: intrusion and infection.

In the first optional step the operator has to gain access to the same network used by the target, while the second step is the identification of the target device and the injection of the RCS Agent into the network traffic using the Tactical Network Injector.

1.1.1 Wireless cracking

If the target is connected to a protected Wi-Fi network, the operator needs to know the passphrase to authenticate the Tactical Device.

If this information isn't available via different channels, the Wireless Network Intruder can be used to break the security.

Supported encryptions are Wired Equivalent Privacy (WEP-40 and WEP-104), Wi-Fi Protected Access (WPA-Personal, WPA2-Personal) and Wi-Fi Protected Setup (WPS).

1.1.2 Target identification

The identification of the target can be done in realtime during the operation.

The Tactical Network Injector monitors all the clients connected to the network and gathers

information about hostnames and visited webpages: in that way the operator can select the real target without reconfiguring the injection rules serverside.

1.1.3 Target infection

The deploy of the RCS Agent is performed using the Network Injector. The Tactical Device needs to be connected to the Internet using any kind of connection available (wired, wireless or 3G)