Law Enforcement Brochure

Restricted Distribution

Wireless Security
Mobile Security
Advanced Computing
Global Network Research

AGLAYA
Solutions for a Mobile Planet
ISO 9001:2008 & 14001:2004 Certified

INFORMATION WARFARE
CYBER SECURITY SOLUTIONS
SUPERCOMPUTER INSTANCES
SIGNAL INTELLIGENCE
COUNTER TERRORISM

INTRODUCTION

Aglaya (Information Security Unit) provides monitoring, defensive and offensive solutions for cyber security and advanced research.

We do not outsource our research to a third party or resell solutions of any other company. All of our development efforts are done via Internal R&D and have been thoroughly tested in simulated operational environments prior to being released.

Our research and related products fall into the following categories:

- Wireless Security
- Mobile Security
- Advance Computing
- Network Security

Aglaya offers an amalgation of hardware and software products that provide instant intelligence gathering within enemy territory and ensure national security via transparent monitoring tools.

Wireless Security provides remote monitoring of open and restricted networks.

Mobile Security provides monitoring on mobile/embedded devices.

Advance Computing division offers remote and onsite super computer facilities.

Network research unit has established virtual worldwide GSM & CDMA switches to enable covert calls in Intel and undercover operations.

Our products enable governments to manage risk, protect national infrastructure against cyber attacks, gain traction in counter-terrorist operations and intelligence gathering.

WIRELESS SECURITY DIVISION

WSD (Wireless Security Division) studies existing protocols and how their behavior changes when subjected to stress and packet insertion. Our wireless team analyzes weaknesses in global protocols and how they can assist in ensuring a safer network.

WSD works to ensure that all products yield real time results via covert or custom implementation. Using Active and passive techniques, data is gathered within seconds for instant responses.

Local Network Wifi solution: Our Wifi expertise spans the ability to monitor wireless network located within a 5 - 10 Kms radius. We can not only detect and connect but also manipulate and manage distant wifi networks irrespective of their encryption type.

The performance of our solutions for Wifi networks is instant and does not take time to collect or intercept data for analysis. Our solutions aid instant monitoring efforts by agencies and assist in time-sensitive data collection. Instant Secure-Handshake retrievals for Wifi Networks and copies of data stream ensure that evidence is never lost. Local Network data analysis is powered by super computer resources that yield instant decryption.

Portable Signal Intelligence Devices: Evidence collection is enabled for all frequencies in enemy territory without accessing large hardware or radio stations. Monitoring is enabled on a device which is portable with battery backup with the ability of instant uploads to the Monitoring post.

Frequencies can be selected or changed from the device that also has the ability to act as a normal mobile phone when the need arises. SIGINT application is hidden on device with internal modification on a Tamper detection device.

MOBILE SECURITY DIVISION

AGLAYA
Solutions for a Mobile Planet
ISO 9001:2008 & 14001:2004 Certified

The world has shifted to mobile for sharing, speaking and communicating. Our mobile security products master techniques that insure monitoring of mobile device without alerting the user.

Our research yields products that are persistant (even after device reset or format) and can work from the regular user space without detection by protection firewall or software. Mobile security division works on methods that enhance remote monitoring and work to remove legacy systems which can save lives during under cover and counter terrorist operations.

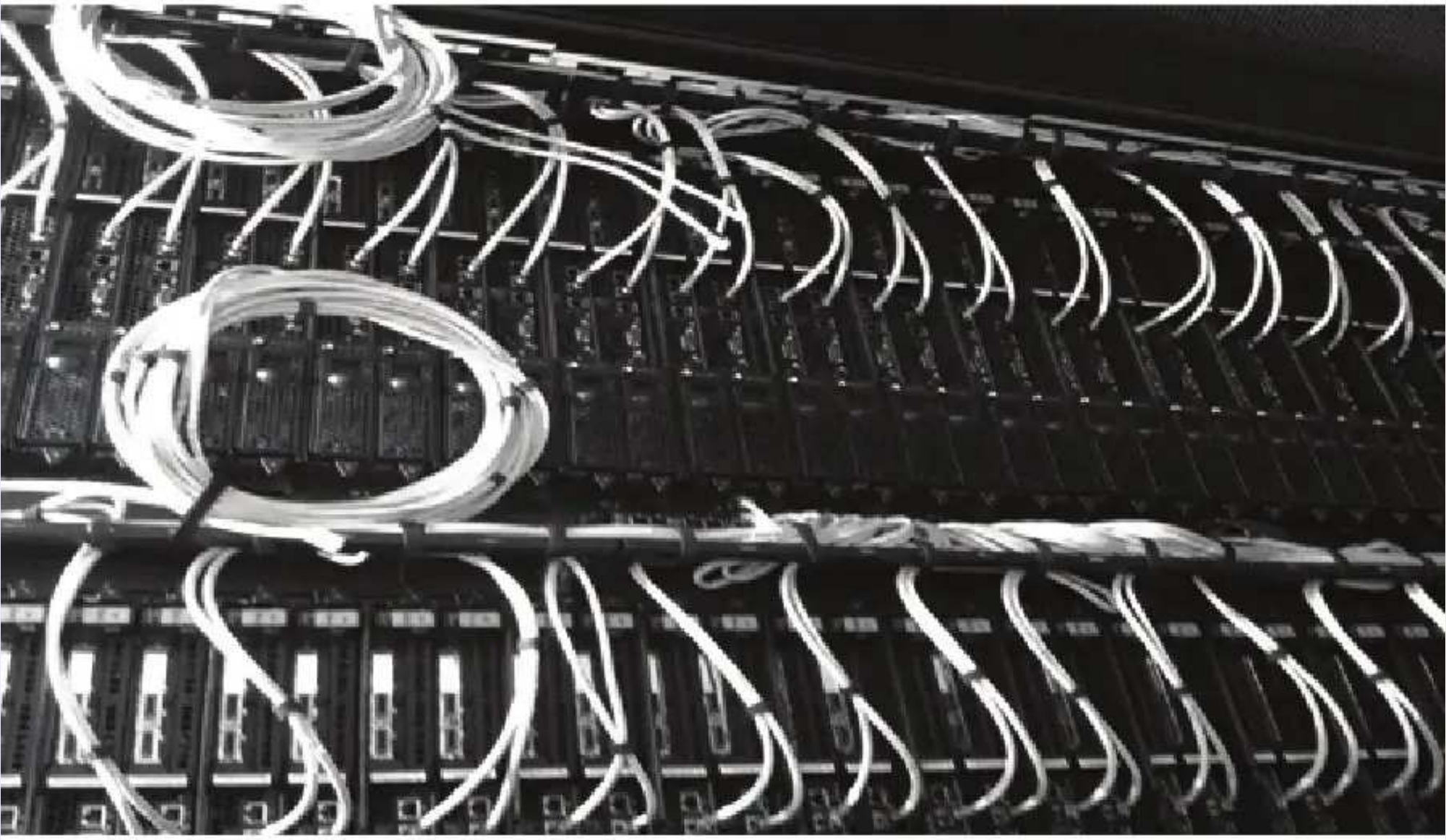
The following are real world implementations of such products:

Live operations: Installation of persistent and undetectable monitoring tools yield Room Audio, SMS communication, Location, Internet, Social media activity and web browsing. They assist in tracking locations of live targets and communications on their devices. In the event of an operation where the target's visibility has diminished, our products enable instant deactivation of the device to limit the strike capability of a target.

Undercover operations: Monitoring solutions can be used instead of live wires in uncover operatives so as to avoid detection during counter-terrorism and Intel operations. This also ensures that one or several stakeholders can be monitoring a "hot-situation" from anywhere in the world for instant response.

Encryption services: Our software solutions implement the highest level of encryption for cross communication on messaging over global networks. All encryption services have plugin space for custom or provided encryption. Base level AES 256 encryption is enabled for all products and services on RTP, UDP or HTTPS.

ADVANCE COMPUTING DIVISION



AGLAYA
Solutions for a Mobile Planet
ISO 9001:2008 & 14001:2004 Certified

Advance Computing Division provides in-house capabilities of raw computing power for defense applications and deep research into any topic relating to the Desktop, be it Windows, Mac, Linux, VxWorks, RTB and Flex OS.

Our research entails harnessing the power of parallel and super computing along with any connected, embedded or Network devices including uPnP. Super computers accept remote uploads for data processing and application tasks with multiple parallel instances of Teraflop processing power. Supercomputers can be prepared for hosting on customer premises for restricted or confidential data processing.

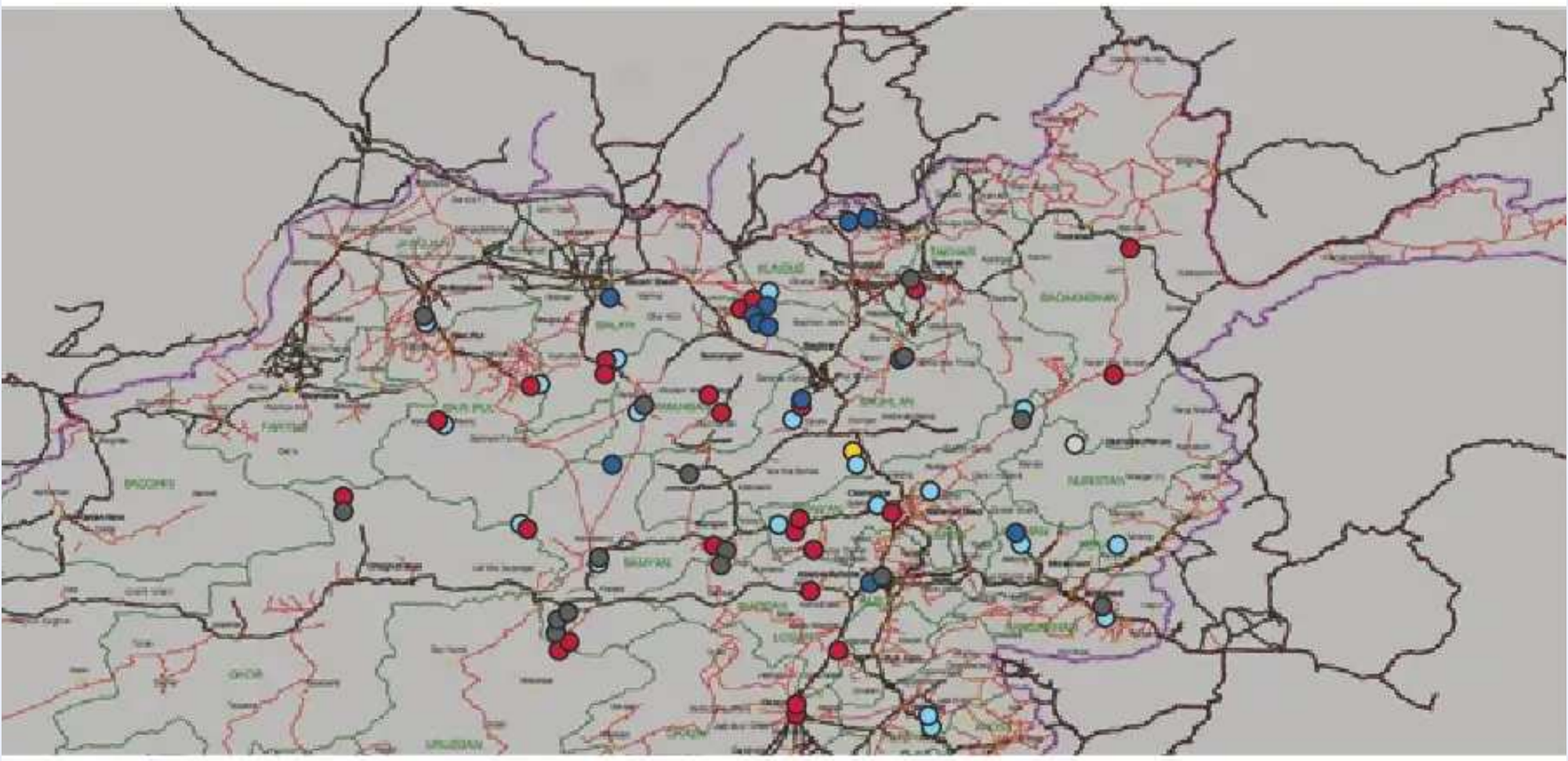
Advance Computing has two sub-divisions. The ability to access Super computing resources as instances and advanced Desktop monitoring and research solutions.

Super computing Instances: Super computer instances or rental hours provide Teraflop processing per instance for purposes of nuclear, defense or medical research. Instances can be made available for parallel processing to ensure each thread runs with the highest possible gain. Super computer also enables cracking PGP, Password protected documents, secure handshakes and wireless encryption. Application tasks need to be prepared for Super computing and have to be made available in C/C++ or Fortan.

Desktop Monitoring: Software that is embedded within PC OS to monitor target from far away. Advanced computing not only develops monitoring but also protection defensive software. Our solutions range from remote monitoring, covert access and development of protection mechanisms against Denial of service attacks, facilitate packet analysis, reply, injection and development of custom protocols for secure communications.

Communications can be forwarded to custom ports to avoid suspicion when in hostile territory.

GLOBAL NETWORKS RESEARCH DIVISION



AGLAYA
Solutions for a Mobile Planet
ISO 9001:2008 & 14001:2004 Certified

Global Networks Research Division (GNRD) works all around the globe with partners to establish a secure network for intelligence and military agencies. GNRD focuses on providing secure command and control operations that enable Telephony, Data delivery, Hosting and back end operations over an anonymous and secure network layer.

With a secure approach, access can be provided to individual networks, GSM backbone (SS7), Global Internet switch access and to multiple virtual GSM and CDMA switches that are operated by Aglaya. This existing network yields to several applications for the defense and law enforcement domain.

GNRD has the following sub-divisions:

Virtual GSM/CDMA Network switches: Existing network switches on global communication backbone enable untraceable calls with fixed interval location hopping. Physical Location can be switched during a phone call with a click. Our switches enable Data and Call access on device without a SIM Card thus ensuring that IMEI/IMSI, Cell tower or other meta data is sanitized during handshakes, Calls, SMS messaging and data transfer.

These switches enable total anonymity from Network Provider and from anyone trying to trace the location of an operative. These solutions are vital for Counter terrorism and Intel operations.

Internet Interception: Strategically placed data controller nodes throughout the Internet enable Country-wide interception or jamming. Data controllers are managed via a central command unit which can view all data flowing in and out of a country. Command center can redirect, intercept, jam or poison any protocol for a country or targeted region. The controllers do not

need to be inside the Target country.

PRODUCT CATALOG

Android Backdoor (Without rooting)

Persistent backdoor and secure exfil
Monitor Room Audio, SMS & GPS
Software remains on device after format/reset
Exfil over Telephony, Internet & SMS
Undetectable by user
Installs by entering URL in browser

Product Code: AGADILESOL8599AB35
Delivery Time: 4 Day order cycle
Price: email at lesol@aglaya.com

AGLAYA
Solutions for a Mobile Planet
ISO 9001:2008 & 14001:2004 Certified

Off-the-shelf Android (target) GSM/CDMA handset/tablet modified using persistent software implant in device ROM that collects room audio, GPS, SMS, Call list & location data. Command and data exfil is done from a Laptop & regular phone via SMS, Telephony uplink and Internet without alerting the target user.

TARGET DATA VIA SMS

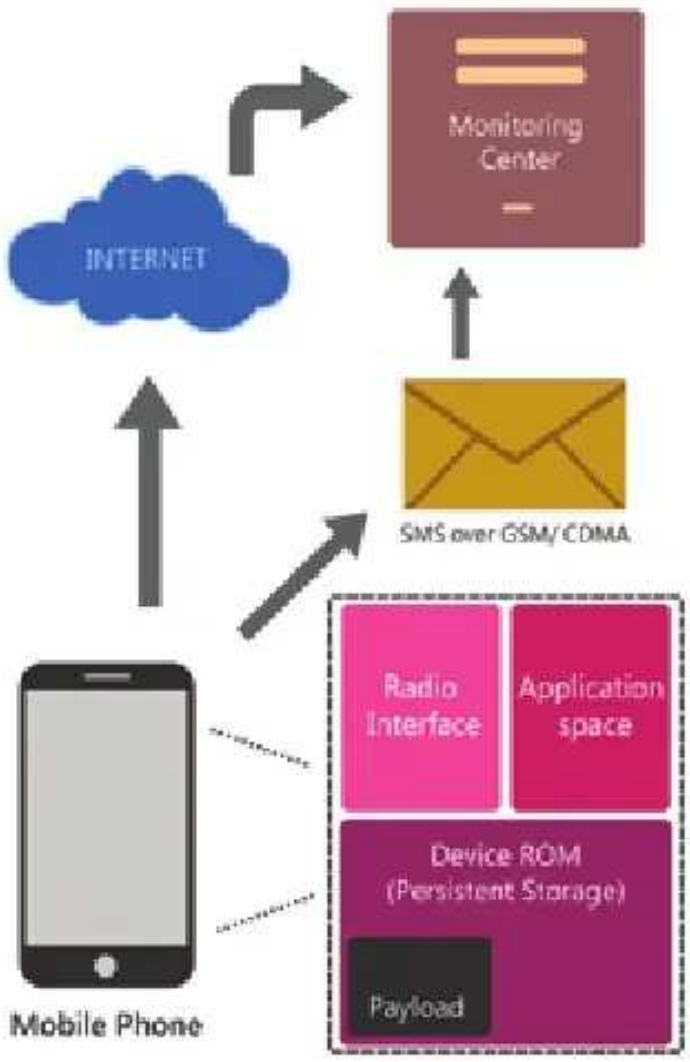
- Incoming & Outgoing call numbers
- Incoming & Outgoing SMS
- Network Detail
- Current Location Details
- Network Name, Signal & Battery strength

TARGET DATA VIA CALL UPLINK

- Room Audio collection

TARGET DATA VIA INTERNET

- Live Call recording
- GPS location
- Network Name, Signal & Battery strength
- Phone book records
- Photos stored on device



Persistent Software after deep reset/format.

HANDSET OPTIONS

All Android Phones, Tablets and Phablets. GSM, CDMA or Dual SIM.

DEPLOYMENT PROCESS

1. Enter URL on Target Device & Click "Yes" to enable backdoor .
2. Monitor from designated Laptop.

OPERATIONAL CONCEPT

- GSM/CDMA Android devices converted into Hot-Mic for the unsuspecting use without rooting.
- Converted within seconds on an unattended phone.
- Passcode required for installation.

Note: Social media monitoring such as Facebook, Skype & Viber are possible in rooted devices.

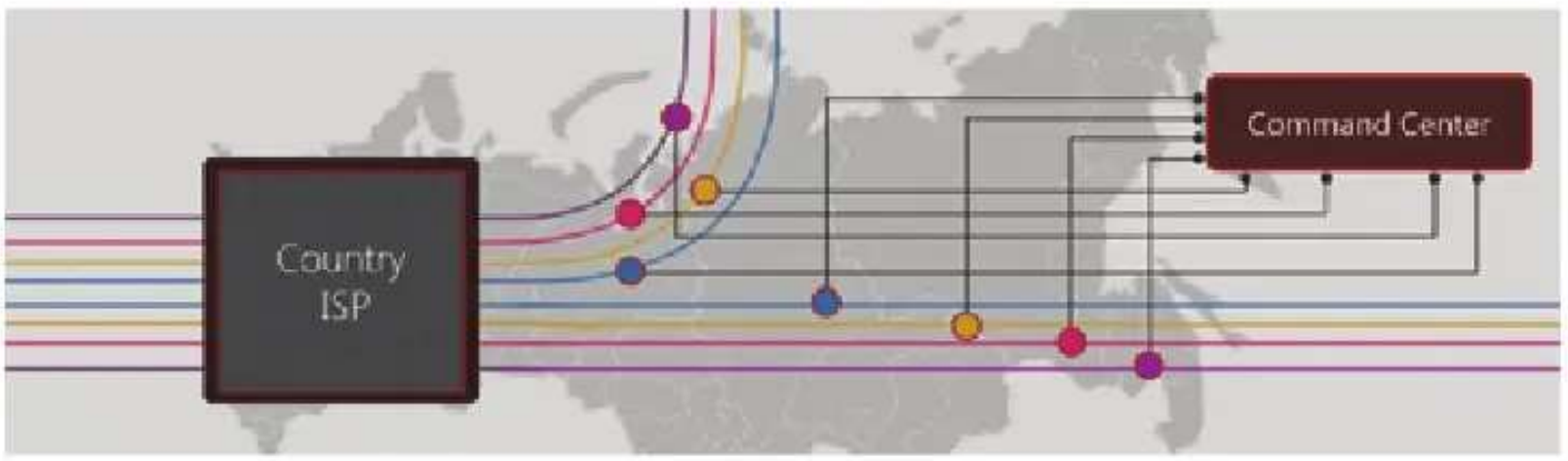
Country Internet Interception

Country Level Internet Interception
Country Wide Internet Jamming
Setup Command & Control Station
Controller nodes outside target country
Jam or monitor specific protocols or area
Undetectable by Target Country
Training option for customer team available

Product Code: AGSWIT9917ASNDJ3
Delivery Time: Custom
Price: email at lesol@aglaya.com

AGLAYA
Solutions for a Mobile Planet
ISO 9001:2008 & 14001:2004 Certified

Command center controls strategically created Data Controlling nodes for the purposes of re-directing internet (TCP/UDP) traffic. Command center can sniff Internet traffic going to a country/region, redirect or jam data streams for any amount of time. Multiple nodes need to be operational for 6 months for International Interception to avoid suspicion by Internet monitoring entities.



SYSTEM DETAILS

- Data controller units located outside target country
- 6 months uptime prior to active use
- Fully functional Internet routing systems
- 50 seat Command Center operation
- Real time data interception of all or selected protocols
- Re-route traffic to another data node
- 100 Gbp/s (min) dedicated connection required

DEPLOYMENT OPTIONS

- Turn Key setup and handover
- Turn key setup & daily operations
- Training option for teams

SYSTEM FEATURES

- Instant traffic interception and analysis
- Ability to capture all ports and sessions
- Undetectable by antivirus & traffic monitoring software
- Undetectable by target country users
- SSL Decryption available

DATA CONTROLLING NODES

- Transparent proxy plugged into Internet Backbone
- Each Node is a 10 seat operation
- Needs to be operational 24 hours
- 10 Gbp/s (min) dedicated connection required
- One node for 100,000 - 250,000 users

SETUP OPTIONS

- **TRAINING:** 4 months course for Teams of 10 to be trained in setup, interception, protocol development, hardware, reporting tools and suspicion avoidance.
- **SETUP & HANDOVER:** Ground up infrastructure setup & operations for 6 months. Training and complete handover is started within 4 months of setup.
- **DAILY OPERATIONS:** Setup, operations, reporting and activity trigger setup with full manpower support.

iOS Backdoor (Without Jailbreak)

Works on all iPhone's and iPad's
Hidden from Main Menu & running apps
Jailbreaking not required
Room Audio Collection
Remotely Jam device
Passwords of Email Accounts created in Mail App
Intercept Safari Browsing activity (HTTP & HTTPs)
Obtain Data from Third Party Apps
PIN Code Retrieval

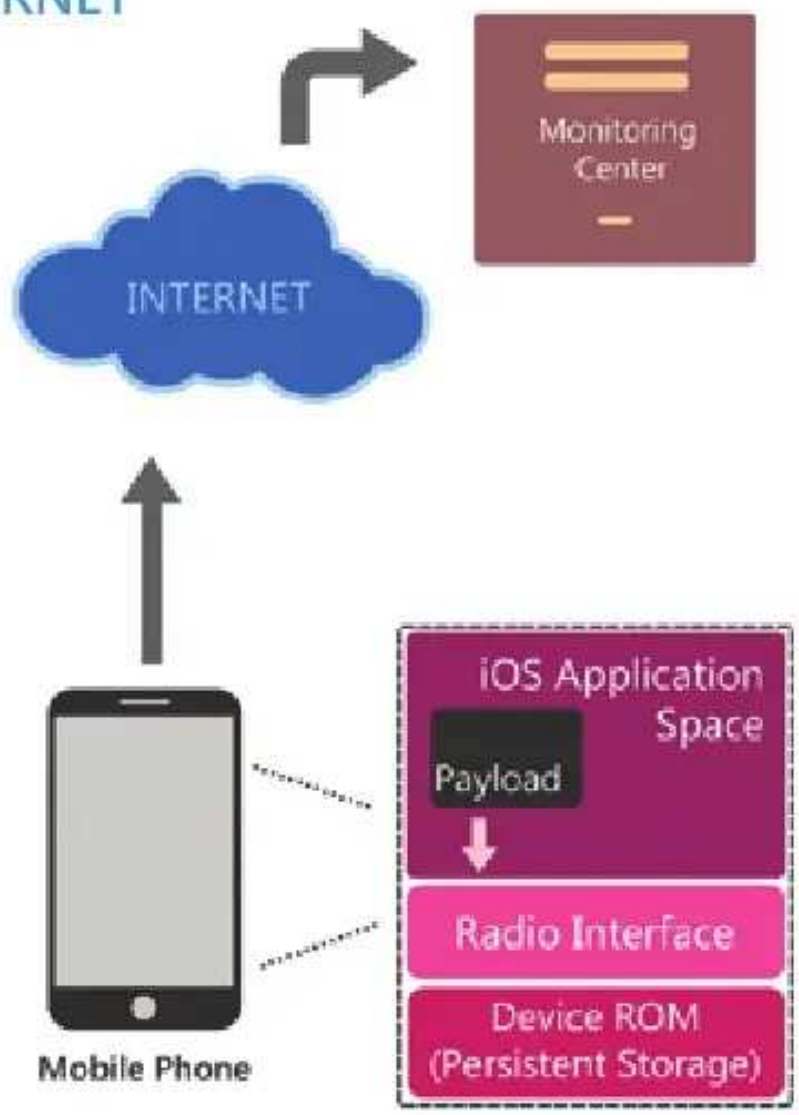
Product Code: AGPKULESOL25771231
Delivery Time: 4 Day order cycle
Price: email at lesol@aglaya.com

AGLAYA
Solutions for a Mobile Planet
ISO 9001:2008 & 14001:2004 Certified

Off-the-shelf iOS GSM/CDMA handset/tablet modified using software that collects room audio, GPS, location data, PIN, email passwords, HTTP/HTTPS browsing in Safari and third party app data such Facebook, Gmail/Yahoo and Outlook App. Command & data exfil is done via the on-device active Internet connection using a remote laptop without alerting the target user.

TARGET DATA OBTAINED VIA INTERNET

- 'Hot-mic' to collect room audio
- Network Information
- Panic Features:
  - Remotely deny phone service
  - Obtain GPS
- PIN Code of device
- Email Passwords in Mail App
- Mobile Browsing Activity
  - HTTP browsing window
  - Decrypted SSL communication
- Facebook Collection
  - Wall Activity & Contacts
  - Public and Private Group Data
  - Browsing within Facebook App
- Emails in Gmail, Yahoo & Outlook App
- Command center setup included



HANDSET OPTIONS

All iPhones, iPads & iPad Mini.

DEPLOYMENT PROCESS

1. Sideload or Enter URL on Target Device & Click "Yes" to enable backdoor on iOS Device.
2. Monitor from designated Laptop

OPERATION CONCEPT

- GSM/CDMA iOS devices converted into Hot-Mic for the unsuspecting user without Jailbreaking.
- Converted within seconds on an unattended phone.
- Passcode is required for installation.

Note: Additional Social media monitoring such as Skype & Viber are possible in Jailbroken devices.

Supercomputer Instances

Super computer instances available on rent
Cracks Wifi Encrypted handshakes, PGP & more
High speed Cracking with 30,000 Pass/sec
Ability to integrate with Nuclear, Military Research Teraflop Parallel instances

Product Code: AGSCPLESOL2NRK88300
Delivery Time: Available
Price: email at lesol@aglaya.com

AGLAYA
Solutions for a Mobile Planet
ISO 9001:2008 & 14001:2004 Certified

Supercomputer processing remotely loaned for applications in parallel time slots. Applications need to be compiled specifically for Super Computer programming and have to be written in C/C++/Fortan. These programs will be uploaded to terminal and processor output will be made available for retrieval. Computing power is made available as instances over time.

SYSTEM FEATURES

- Instances are available from 1 Teraflop (minimum) to 4.5 Teraflop (maximum)
- Memory bandwidth from 250 GB/sec to 300 GB/sec with size of 12GB
- Multiple instances can be purchased for increased load. However each instances capped at 4.5 Tflops for temperature control
- Bandwidth made available for upload might vary but are assured at a minimum of 2Mbp/s & Max of 128 Mpb/s
- Output is made available as per customer Program. No additional encryption is offered to preserve formats.
- SSL based downloads initiated for output (by default)

PASSWORD CRACKER

- The following formats do not require any changes and can be uploaded directly via terminal for cracking: Office 2003, 2007, 2010, Openoffice, PGP, PDF, iPhone & Blackberry Backup, Apple iWork
- Ability to try upto 30,000 passwords / second

APPLICATION DEVELOPMENT

- Ability to run with existing processes and can customize builds with current nuclear, aerospace, defense, and arithmetic modules.
- Data output can be posted to remote unit directly over secure channel.
- Physical access to premises is also made available for larger instance purchase.
- Customization manpower made available for larger instances.
- Can setup Super computer at customer premises as an outright purchase.

WHY CUSTOMIZATION?

Users with existing super computer resources need to note that some customization (except for password cracking) might be required. Core array configuration (CPU & GPU) might be different on our end hence, adjustments needs to be made single or double precision floating point calculations and performance.

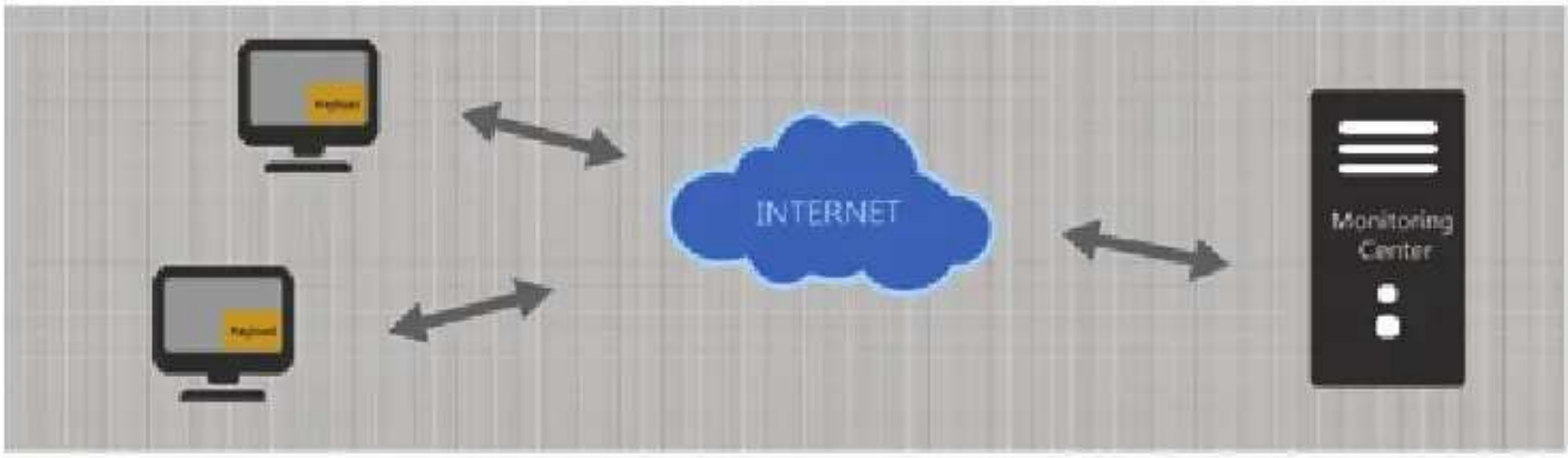
PC Monitoring

Remote PC Monitoring (Windows, Linux & MacOS)
Undetectable by Protection Software
Low overhead and footprint
Encrypted Data Transfer
Self-healing procedure incase Proxy is down
Cannot be degubbed
Multiple Command & Control Server ready
Routed over anonymous proxy(s)
Self upgrade & remote routing ready

Product Code: AGPCEXFESOL276HH88A
Delivery Time: Available
Price: email at lesol@aglaya.com

AGLAYA
Solutions for a Mobile Planet
ISO 9001:2008 & 14001:2004 Certified

Software implant for all Desktop & Server versions granting access to all features of the Operating system including connected network and devices. Data exfil is done via secure channel over UDP.



SYSTEM FEATURES

- Monitoring of Keystroke, Screenshots, passwords, emails and documents
- Command line access of logged in user
- Does not appear in registry or list of startup items
- Installs in User space and undetectable by virus scanner
- Firewall is bypassed with custom protocol implementation
- Cannot be debugged by third party application
- Not visible in list of external HTTP connections
- Ability to infect connected network, USB and PnP devices

EXFIL PROCESS

- Command and Exfil is performed on UDP channel with revolving protocol bridge
- Exfil over SSL with custom root CA 4096 bit encrypted

OVERHEAD

- Uses less than 1% overhead and does not appear in task manager
- Internet usage is kept to minimum with advanced compression

SECURITY MECHANISM

- Self healing if data is intercepted by means of advanced proxy rules
- Dynamic multi layered proxy engines insure backup incase one proxy is taken down
- Ability to route data via anonymous domains and proxy server
- Anonymous command and control servers
- Remotely change Communication protocol to avoid detection by Security Apps
- Each command can be routed over different IP/Servers

SecureSMS

Encrypted SMS Communication
SMS is sent over GSM and CDMA Networks
Third party Internet servers are not involved
AES 256 bit encryption
IV does not leave the device
Encrypted 4096 handshake
Password protected application
US DoD 5220.22-M Data Removal/Erase capability

Product Code: AGSSULESOLAS81ANA
Delivery Time: 2 day order cycle
Price: email at lesol@aglaya.com

AGLAYA
Solutions for a Mobile Planet
ISO 9001:2008 & 14001:2004 Certified

Android Handsets modified using software to enable AES 256 encrypted Peer-to-Peer SMS messages. Data is send over SMS Channel without involving transactions over Internet Servers. All normal outgoing SMS can be encrypted.

SYSTEM DETAILS

- Software solution for peer-to-peer AES 256 SMS
- Does not route SMS over Internet
- Capability to encrypt all outgoing SMS
- Data stored on device is encrypted and password protected
- Software cannot be reverse engineered even after rooting
- Data images over-written several times to ensure forensics does not yield results

ENCRYPTION FEATURES

- AES 256 IV (initializing vector) is dynamic key that is stored on device
- IV never leaves the handset, hence, unavailable to any network operator node
- Failed decryption or accidental encryption yields to damaged SMS view

SYSTEM FEATURES

- Compose a normal SMS and option to encrypt appears when sending
- Works on all International languages
- Compatible with GSM and CDMA devices

Customization is available for integration in existing systems or processes.

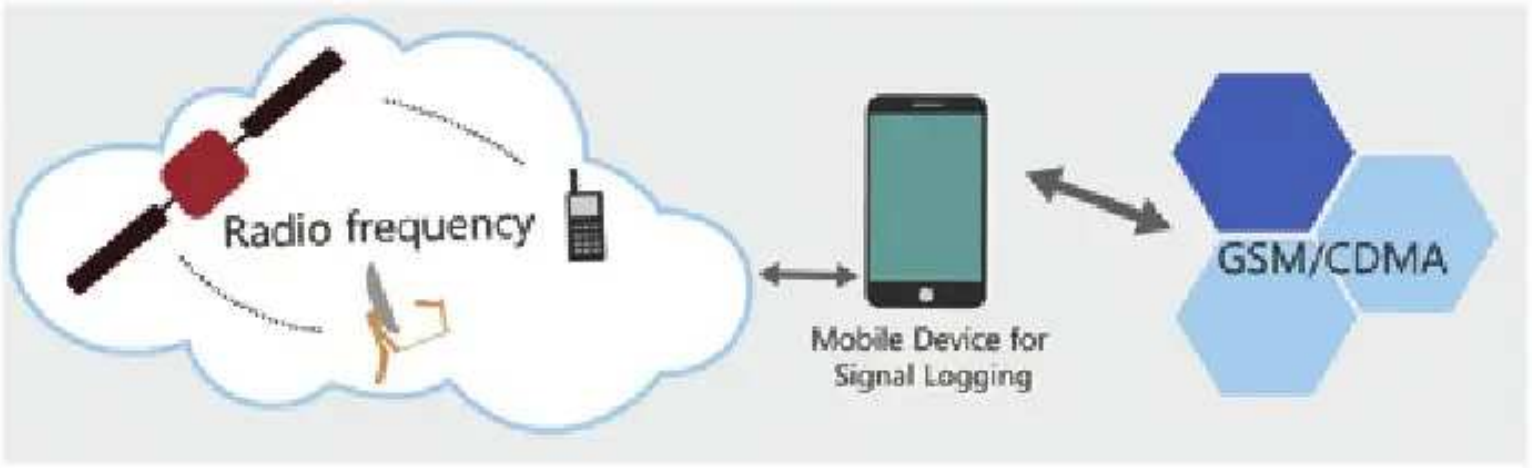
Signal Intelligence (SIGINT)

Signal Intelligence on Mobile Device
Covert Frequency logger
Application hidden on Device
Instant uploads to HQ via 3G
Undetectable in menu or Installed Apps
Operational on off-the-shelf device
Can operate as a normal Mobile Phone

Product Code: AGPKULESOL25771231
Delivery Time: 14 Day order cycle
Price: email at lesol@aglaya.com

AGLAYA
Solutions for a Mobile Planet
ISO 9001:2008 & 14001:2004 Certified

Commercial off-the-shelf GSM/CDMA handset modified to include Software Defined Software (SDR) and additional memory. The Internal SDR allows the carrying user to covertly perform network survey, record Rf spectrum or perform self-handset location in hostile environments.



SIGINT is designed to support covert operations in hostile environments. A witting user would be able to survey the local environment with the spectrum analyzer tool, select spectrum of interest of record and download the spectrum information via Bluetooth/cable to a laptop controller. SIGINT can be used alongside active interrogator, as the finishing tool when performing Find/Fix/Finish operations in unconventional environments.

Data collected from the SigInt device can also be uploaded to HQ using the on-device 3G connection. Uploads are initiated over encrypted channels.

DEVICE FEATURES

- Concealed SDR with Handset Menu Interface
- Obtain Instant copies of Data collected from SigInt device
- No supporting hardware except Mobile device is required
- Spectrum Analyzer Capability
- Ability to download recorded frequency/Data to Laptop
- Records to internal and external storage
- Integrated Antenna inside device
- Ability to record 100 Gb of data (compressed and encrypted)
- Instant upload via custom encryption to Controller server
- 3G/4G/LTE Handset Host platform
- Active interrogation capabilities

Untrackable Mobile

Mobile Phone location is untracable
Location jumps across countries on each call
Mobile Device works without SIM Card
Call is routed over Virtual Anonymous Switches
Call is stripped of IMEI/IMSI and Cell tower Info
Add multiple numbers to a handset without SIM
Numbers available from several countries
Calls are invisible to Network Provider

Wifi connection required
Tamper detection on device

Product Code: AGSCULESOLAKKA8A81
Delivery Time: 2 Week order cycle
Price: email at lesol@aglaya.com

AGLAYA
Solutions for a Mobile Planet
ISO 9001:2008 & 14001:2004 Certified

Modified Tamper-detection Mobile Phone with an "Internet only Anonymous Network" over a Wifi Connection. This shields IMEI, IMSI or Network Information such as Cell Tower Info or GPS from being transmitted over networks. Location tracking does not work since SIM card is not required for calls and signals are routed on Worldwide anonymous GSM/CDMA Switches at regular intervals and with every call. The mobile device enables user to cloak and jump their location on every call automatically.

SYSTEM DETAILS

- Tamper detection on Mobile Device
- MSISDN can be selected from a vast list of countries and states
- Random numbers are generated online & applied to software client on Handset
- Software running on handset enables call to be received on generated MSISDN
- Software enables outgoing call locations as per rule set
- Anonymous/Multiple numbers added to existing GSM/CDMA/SatPhone
- Call Routing over anonymous switched networks
- Untraceable owner, IMEI, IMSI and location information
- Route calls over different countries and locations as per purchased plan
- Call location can be switched in the middle (if available) or with initiated calls

OPERATIONS

- Setup numbers can be changed as per plan
- End to end infrastructure

can be customer owned
- Works in all countries with 3G Networks

SYSTEM FEATURES

- Multiple numbers from different countries can be added to on device.
- Ability to change/add phone numbers within 24 hours.
- Voice data is scrambled & encrypted when sent over routing network.
- Tracking Meta data such as IMEI, IMSI, Location data is stripped clean on transmitted data.
- Works over 3G/4G/LTE networks and on 3G handsets.

OPERATIONAL REQUIREMENTS

- Wifi Connection on device
- Unlimited Data or Wifi plan (preferred)
- Non-rooted/non-jailbroken device

Wifi Interceptor

Exploits WEP/WPA/WPA2
Works upto 10 Kms away
Instantly gets Encrypted handshakes
Ability to jam Wifi Networks
Can re-join network from a distance
Password cracking enabled via Super Computer
Ability to intercept all data on a Target Wifi

Range can be increased with modifications

Product Code: AGWLULESOL7738991
Delivery Time: 3 week order cycle
Price: email at lesol@aglaya.com

AGLAYA
Solutions for a Mobile Planet
ISO 9001:2008 & 14001:2004 Certified

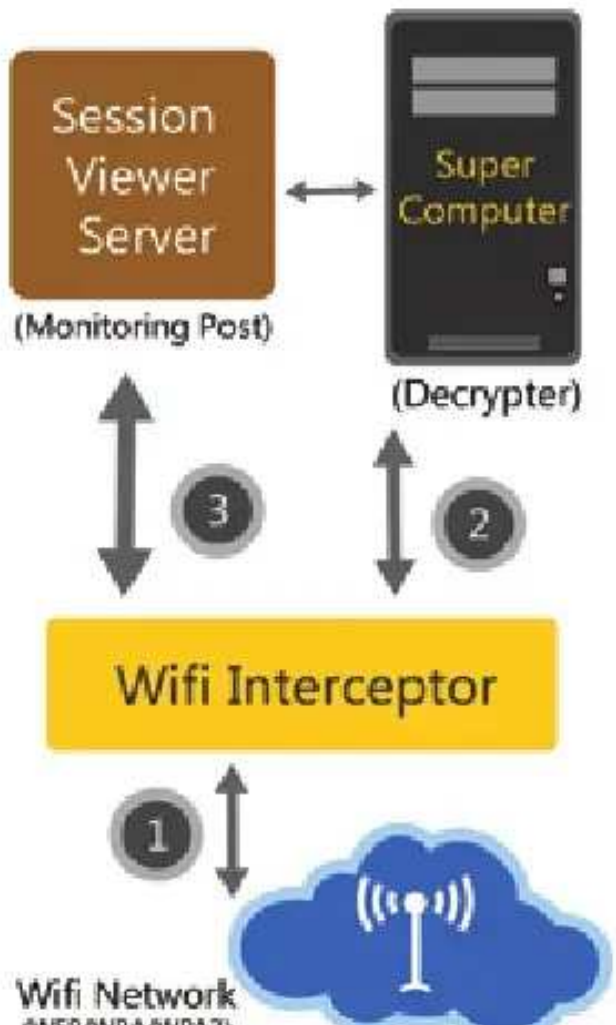
An Active 802.11 wireless exploitation tool for WEP/WPA and WPA2 Privacy types. Interceptor copies encrypted handshake within seconds from all available networks. With the retrieved key, captured data can be decrypted and (if feasible) facilitates silent delivery of the payload to the "target" machine.

SYSTEM DETAILS

- Standalone tool currently on a Raspberry Pi, Chrome book or laptop with Linux, Ubuntu or Fedora Core
- Instantly sniffs encrypted handshakes from WEP, WPA or WPA2 Type networks
- External battery of 9,000 mAH
- Encrypted handshakes are captured within 100 seconds of hardware in operational mode.

SYSTEM FEATURES

- Ability to Jam Selected Wifi Networks
- Blanket Wifi signal jamming
- Control Hardware remotely from Listening Post
- Attack is undetectable by the user
- Automatically connects Clients that may have



joined any Open Wifi Access point during their lifetime. (Such as Linksys, Netgear. Starbucks, etc)
- Decrypt intercepted Traffic at an offline or at Listening post without being near the Target Wifi Network

- Wifi Interceptor uses external antennas and can attack targets upto 5 Kms.
- Addition of Amplifiers has increased the range upto 10 Kms.
- Configuration options include: remote management capabilities, antenna, amplifiers, battery backup & processing power.

DECRYPTION CAPABILITY: Super computer assisted password cracking is available for customers on a hourly fee. For privacy concerns, separate PC/Laptop can be setup at customer site to decrypt captured Wifi handshake.

Registered Address
A2/59 Safdarjung Enclave
New Delhi 110029 India
contact@aglaya.com

Development Center
627, Udyog Vihar
Phase 5, Gurgaon
Haryana 122016 India

T: +91.11.2610.25.20
F: +91.11.2619.62.94
M: +91.98.101.20.879