Enhanced Network Forensic Solution on Wi-Fi Network by MGS

For law Enforcement Agency and Corporate IT Security Management

The operation of lawful interception or corporate IT security management on daily network communication is a regular task for both law enforcement staff and IT security officer. From such regular task, those who commit cybercrimes or harm IT security inside corporate can be found and prosecuted by clear digital evidence. The task must be carried out under the finite network infrastructure, such as wired network or telecom networks, with specific target.

Traffic interception on wired network or telecom network at this moment has been well defined by the law or de facto mandate in term of technical detail no matter how you carry out for lawful interception or corporate IT management. That's why most of operations for lawful interception and IT security management are always taken from wired network side.

Wireless network is the one dark frontier for LEA staff or CISO to probe illegal harmful cyber threats because of different data transmission pattern and secured type through the air. On the other hand, communication through wireless network is only taken in the last mile loop. Eventually all communication still goes through wired network for routing. That's why LI operation is usually taken at core service network.

The demand for LI operation on wireless network is mostly at the Wi-Fi network for tactic evidence collection in public space, such as Café shop, public square, shopping mall…etc. on drug dealers or cyber frauds. In corporate environment, disgruntled employees usually leak internal confidential to outsiders through external AP or hacker intrudes corporate network through unsecured over-spilled APs.

Wi-Fi network, after evolving for more than 30 years, provides a good and secured mean for people to access Internet through air. Especially the cost of internet access via Wi-Fi link is quite low compared to that through mobile telecom networks. That's why lots of mobile phone owners like to use Wi-Fi link for internet access whenever it is available, especially in corporate environment as BYOD or through public Wi-Fi service. So, interception on Wi-Fi network is always the major scope for tactic lawful interception and corporate IT security management.

The traffic interception on Wi-Fi network is not as simple as that on wired or telecom networks, which is usually carried out in the core service network. The first issue is the signal attenuation from radio frequency wave, i.e. the longer the distance is, the weaker the RF strength is. The second one is the background interference against RF signal, especially those with strong electromagnetic effect, such as power plant, radioactive ray, heavy quick rainfall or RF with the same frequency…etc. The third one is the secured encryption of Wi-Fi data packets by WEP, WPA or WPA2 at data link level. Those above factors always make lots of hard time for LEA staff and CISO to take LI operation.

New Enhancement of MG MFS

MGS has developed 2 different products with interception capability on Wi-Fi network before to fulfill different demands in the market. As mobile access is more and more popular at the current moment, the interception demand for both LEA and corporate IT security on Wi-Fi network is going toward the same direction. MGS provides the brand new enhanced Wi-Fi Interception product to the market – Mobile Forensic System ("MFS") enable the Network Investigation Toolkit ("NIT") in order to cover both demands.

In the new MFS, there are several significant enhance features as following:

1. Radio Frequency Wave Capture Enhancement

   The first one is the capture capability enhancement of radio frequency wave. MFS NIT provides several enhancements on RF capture:

   a. Single system with multiple wireless interfaces by external high gain antenna support – for surveillance on Wi-Fi network in small scope of public place, monitor can use NIT with 4 Wi-Fi interfaces by high gain (12dB) antenna to intercept surrounding Wi-Fi traffic. By this way, the data capture rate at specific target can reach to 95% above within 25 meter range in public square.
   b. Multiple systems at different location with backend central unit – Multiple MFSs with external high gain antenna support are deployed at different corners against the target AP for Wi-Fi packets collection. All the collected packets will be centralized in the backend MFS for data consolidation and decoding of WEP/WPA by password. By this way, the capture rate can be close to 100% within 50 meter range in public square.

   The RF capture is quite critical, because it is the first gate for data input. That's why MFS needs to required lots of R&D investment to enhance the RF capture rate.

2. Decryption on WEP, WPA password

   The second enhancement is to deal with encryption at data link level. There are WEP, WPA and WPA-2 type of protection on Wi-Fi data packets. Unless system can take off the protection, internal IP data packets will be highly encrypted. For WEP, MFS can easily take it off and expose internal IP packet; however, for WPA, an external WPA cracking system with multiple GPU support can decode WPA protection to get the key eventually and later on sent this key to NIT for decoding WPA encryption.

3. Surveillance on HTTPS Connection

   The third enhancement is for surveillance on HTTPS connection. The most common way to carry out HTTPS interception at this moment is through man-in-the-middle mechanism. By this way, MGS MFS plays the role of proxy server, takes out the original certificate for HTTPS decryption, and replaces it with self-signed one for fulfillment of the HTTPS connection at both ends.

4. Integration with Standard Lawful Interception Platform

   The fourth enhancement is for lawful interception requirement on telecom network. For telecom network, the integration of call data record (CDR) of target subscribers must be presented with reconstructed content and LI case number. The CDR information can be uploaded into MGS NIT or have Telecom Radius system sent target CDR to NIT for criminal investigation by case. NIT will correlate CDR information with reconstructed content data, and present all the information compliant with ETSI standard format.

5. Integration as Wireless Access Service Portal System

   The fifth enhancement is the integration with remote access service portal. By this way, NITcan emulate AP RAS gateway via Wi-Fi network. It is quite useful for corporate IT security staff to deploy our system for internal IT security risk monitoring.

6. Consolidated Data Life Management

   The sixth enhancement is for consolidation management of data retention and life cycle management. Data in MFS is critical and confidential for user, because it contains lots of business confidential or private data in criminal case. That's why we must take special care of the data protection during retention and life cycle management, which is part of corporate IT governance or LI Act. NIT will send internal data, which are of CDR and reconstructed content information, to the data retention management system in the backend side through FTP service periodically and either manually or automatically.

7. Target on Wi-Fi Point-to-Point Services

   The seventh enhancement is the focus on interception on Wi-Fi point-to-point communication, which is similar with that of push-talk service. These online services, such as FireChat, Serval Mesh, Wi-Fi Talking, are usually popular in the mass riot event while wireless broadband connections are overloaded and bad such as in the cases of HK umbrella movement, Indonesian and Malaysian President Election Campaign…etc. These online services are recently in the target protocol list of LEA staff in several countries.

8. Data Analysis

The eighth enhancement is the analysis on the intercepted data, especially CDR information from telecom OSS system and transaction record of online services. There are 2 steps for the data analysis in the box: one is for data scoping, and the other is for link analysis. In the data scoping stage, user can locate the intercepted data, both CDR and content, by keywords, IP address, account IDs…and other criteria into scoped data for further analysis. In the link analysis phase, user can find out the logic of facts behind telecom CDR and transaction record for relationship among account IDs from different online services. Both analyses are quite critical for LEA staff and IT security officers to find out the target suspects and associated criminal or abnormal behavior.

The above are the new enhancement in MGS NITby 2015. In the future, there are still lots of enhancement rolled out, especially on new online services and popular mobile services.

The Value Proposition of MGS NITand Service

In order to provide better service along with NIT2, MGS also provides several different levels of training programs based on customer requirement. These programs are usually delivered by qualified local instructors, senior cybercrime investigators or scholars in university. These programs are listed below:

1. **Network Packet Forensic Analysis Training (NPFAT)** - Network Packet Forensics Analysis Training is designed for operators, who uses our MFS for daily task of cybercrime investigation and IT security management. Through this training program, he or she can easily understand the data presented in MFS and use the analysis tools to find out more facts behind cybercrimes or IT security risk.
2. **Lawful Interception Training (LIT)** – it is designed for IT experts and LEA technical staff on lawful interception planning, deployment and delivery.
3. **Cyber Intelligence Training (CIT)** – It is designed for senior management staff to learn cyber intelligence deployment and delivery for national security.
4. **Cybercrime Investigation Training (CCIT)** – MGS co-works with staff of National Taiwan Central Police University and Taiwan CIB to deliver this training program of cybercrime investigation skill and theory to LEA staff from different country. The purpose is to have LEA staff fully understand how to conduct LI operation under state mandate and global standard.

Besides the above products and training programs, MGS also provides consulting service on planning of lawful interception and cyber intelligence to our partners and customer. With lots of deployment experience in different countries, MGS consultants will provide streamline lawful interception process from warrant authorization to data collection on telecom networks, and fully meet global and state mandates and regulation.

About MFS

MFS is a special Forensic Project development together with Decision Group who is located now in Taipei, Taiwan with 45 engineers in developing network forensic solutions and consulting service in network forensics division for more than 15 years.

There are several sales and service offices around the world for direct service coverage to our partners and clients in Asia, Europe, North and Latin America, African and Middle East.

All MFS product service requests will be sent to Service Department in MGS Head Quarter for ensuring high standard of customer satisfaction and Decision Group will be the back to back support over this product line worldwide.