November 2009 System Assessment and Validation for Emergency Responders (SAVER)

Homeland Security
Science and Technology

TechNote

Wireless Network Analyzers for Investigative Applications

Wireless networks, or Wi-Fi, have become more common as a growing number of people use these networks to access the Internet and share electronic information from Wi-Fi enabled devices, such as computers and smart phones. As a result, Wi-Fi is often used in the planning and execution of illegal activities. Wireless network analyzers, however, enable law enforcement officers with the proper warrants to investigate and collect forensic evidence to counter illegal activities. This forensic evidence can include pictures, videos, personal communications, and/or data files.

Wireless network analyzers use computer software and hardware to detect, locate, monitor, and/or capture information passed over Wi-Fi. Wireless network analyzers can be off-the-shelf laptops equipped with Wi-Fi network analyzer software or may be custom-built network analyzers. Wireless network analyzers are also known as network sniffers, packet analyzers, network sniffing tools, and wireless sniffers.

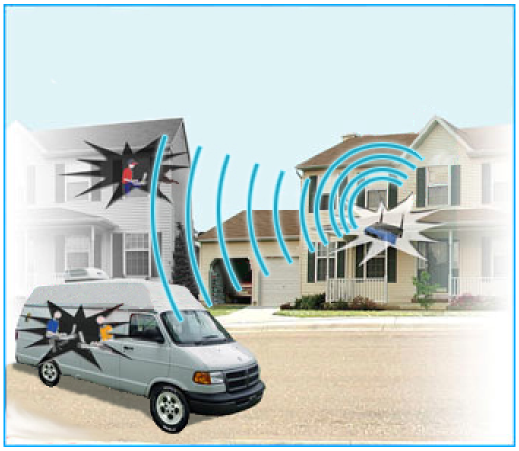

Figure 1. Accessing Wi-Fi Networks from a Nearby Vehicle and Home

Wi-Fi

Wi-Fi provides for short range communication between Wi-Fi enabled devices, such as computers, cameras, personal digital assistants (PDAs), and cell phones. Wi-Fi enabled devices detect and connect to available wireless networks to exchange data. Wi-Fi can operate on 14 different channels on both the 2.5 and 5 gigahertz radio spectrums, allowing for multiple networks to operate within close proximity without interfering with each other. Wi-Fi signals travel about 120 feet in typical residential or office environments and about 300 feet outdoors. Wi-Fi signal strength drops as the distance from the wireless access point increases. A wireless network analyzer designed to detect or monitor Wi-Fi signals must be relatively close to the Wi-Fi access point.

Cybercrimes

Wi-Fi is attractive to criminals for a number of reasons, including remote access, vulnerability, and anonymity. Since Wi-Fi operates using radio waves, a criminal can access a network that is in a home by parking in the

U.S. Department of Homeland Security

SAVER

System Assessment and Validation for Emergency Responders

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions.

Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercial equipment and systems and provides those results along with other relevant equipment information to the emergency response community in an operationally useful form. SAVER provides information on equipment that falls within the categories listed in the DHS Authorized Equipment List (AEL).

The SAVER Program is supported by a network of technical agents who perform assessment and validation activities. Further, SAVER focuses primarily on two main questions for the emergency responder community: “What equipment is available?” and “How does it perform?”

For more information on this and other technologies, contact the SAVER Program Support Office.

RKB/SAVER Telephone: 877-336-2752
E-mail: SAVER@dhs.gov
Web site: https://www.rkb.us/saver

This SAVER TechNote was prepared by the Space and Naval Warfare Systems Center Atlantic for the SAVER Program.

SPAWAR Systems Center ATLANTIC

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by the United States Government. Neither the United States Government nor any of its employees make any warranty, expressed or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose for any specific commercial product, process, or service referenced herein.

street in front of the home. Criminals can even hide Wi-Fi enabled devices in neighboring homes or structures, avoiding capture of evidence by normal searches.

Wi-Fi is designed to provide quick and easy access to wireless networks; even with the use of encryption, it remains relatively easy for a knowledgeable criminal to hijack a connection or listen in, possibly with their own network analyzer. This ability to compromise a connection, along with the remote accessibility of Wi-Fi, exposes a wealth of information that can be used to commit identity theft or fraud.

Wi-Fi's design for ease of use also provides an extra layer of anonymity to users. Usually, an Internet crime can be traced to an origination point using IP addresses, unique identifiers for each connection point to the Internet. Wi-Fi, however, only assigns an IP address to the source, and each user is assigned a temporary identifier while connected to the network instead of an IP address. This makes tracking a user much more difficult.

Wi-Fi Network Analyzers

Some wireless network analyzers are standard, off-the-shelf laptops equipped with wireless network analyzer software. Other network analyzers are built specifically to analyze Wi-Fi communications and are more capable devices than a laptop with software. Depending on design, a specific wireless network analyzer may have any or all of a broad range of capabilities, including:

- Detecting the strength of the Wi-Fi signal and, depending on conditions, approximate distance from the source of the transmission.
- Triangulation and location of active Wi-Fi devices.
- Determining the media access control (MAC) address of the communicating device, a unique identifier assigned by the manufacturer. The MAC address enables investigators to determine if a specific Wi-Fi enabled device is active on a network.
- Identifying whether Wi-Fi communication is open or encrypted (protected), and, if encrypted, the protocol used—wired equivalent privacy (WEP) or Wi-Fi protected access (WPA, WPA2).
- Global Positioning System (GPS) date, time, and location stamping of captured data.
- Passive data collection, allowing monitoring of Wi-Fi network traffic without broadcasting a signal that could alert a suspect that monitoring is taking place.
- Remote operation capability, which allows investigators to control the analyzer safely from a distance without alerting a suspect.

Capturing enough data on an encrypted wireless network can allow for the encryption to be cracked. WEP encryption is considered relatively weak and can be decoded automatically by an analyzer designed to do so. WPA and WPA2 encryption provide stronger protection, but can sometimes be broken by computer forensic experts if a sufficient amount of data is captured. Once decrypted, data can be manipulated with network traffic analysis software to detect patterns and reconstruct applications used. For example, an Internet chat session could be reassembled or investigators could reconstruct part or all of the Web pages a suspect has viewed.

Extended investigations and efforts to capture and decrypt data for use in court may require extensive data storage capabilities. Some analyzers can capture simultaneous transmissions on all 14 Wi-Fi channels.

Since Wi-Fi enabled devices may be hidden or located on neighboring properties, some wireless network analyzers can locate active devices on a wireless network and determine their positions using triangulation.

Investigations

Wireless network analyzers can be powerful investigative tools, especially in surveillance situations. While many of the functions of a network analyzer may not require a search warrant, capturing data with a network analyzer can violate wiretapping laws if done without a warrant. Since laws on wiretapping vary by state and municipality, users should check and validate their standard operating procedures when using wireless network analyzers.

Resources

The following Web sites can provide additional information on wireless network analyzers and their uses.

The Electronic Crime Partnership Initiative
http://ecpi-us.org/index.html

Wireless Evidence, What are We Missing?
http://www.jus.state.nc.us/NCJA/jg_wireless%20evidence.pdf