Attacking wifi nets with traffic injection

Entertainment, Movie

I am very much thankful to him. I benefited a lot discussing with him. I am also thankful to my parents who encouraged me and provided such amotivation, so I became able to perform this. I am also thankful to all my friends and those who helped me directly or indirectly in completion of my project. CONTENTS •Introduction •Crime Definition •Laws that have been violated •Possible Punishments (IT ACT + INTERNATIONAL LAWS) •Unlawful Losses and Gains •Working of Attacks •Description of Tools INTRODUCTION This term paper is based on " attacking wifi nets with traffic injection" also nown as packet injection which simply means the hacking of wireless networks with different techniques to send extra amount of traffic (packets, frames, duplicate copies) on a network by which a hacker can able to access the information and identity that a client is using. Some techniques are wireless network sniffing, DOS (denial of service attack), Man in the middle attack etc. Attacks on wireless LANs (WLAN's) and wireless-enabled laptops are a quick and easy way for hackers to steal data and enter the corporate network.

Many types of tools are used to perform hacking. Some of them are named as aircrack-ng, airjack etc. thts paper will later give brief information on tools used , working of tools , losses and gains with hacking etc. These type of attacks are known as INTEGRITY attacks. Wireless networks broadcast their packets using radio frequency or optical wavelengths. A modernlaptop computercan listen in. Worse, an attacker can manufacture new packets on the fly and persuade wireless stations to accept his packets as legitimate. We already know 802. 11 networks are weak.

Open networks are prone to any well-known LAN perimeter attack WEP is vulnerable. Traffic injection has changed things like •Increased DoS (denial of service) capabilities •Dramatically decreased WEP cracking achievement time •Allows traffic tampering •Allows stations attacks CRIME DEFINITION Cyber Crime –A crime where the computer is used as a tool or target. Cyber crime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cyber crime also includes traditional crimes conducted through the Internet.

For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet. Hacking – Traffic injection attacks comes under hacking. It is defined as whomever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

Hacking may also occur when a person willfully, knowingly, and without authorization or without reasonable grounds to believe that he or she has such authorization, destroys data, computer programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network. Besides the destruction of such data, hacking may also be defined to include the disclosure, use or taking of the data commits an offense against intellectual property.

This paper is a survey of wireless attack tools focusing on 802. 11 and Bluetooth. It includes attack tools for three major categories: confidentiality, integrity, and availability. Confidentiality attack tools focus on the content of the data and are best known for encryption cracking. Integrity attacks tools focus on the data in transmission and include frame insertion, man in the middle, and replay attacks. Finally, availability attack tools focus on Denial of Service (DoS) attacks. Law That Have Been Violated

The laws that have been violated are section 43, 65 and 66 of IT ACT 2000. Section 43 of IT ACT 2000, defines as If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, — (a) Accesses or secures access to such computer, computer system or computer Network; (b) Downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium; c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (d) Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programs residing in such computer, computer system or computer network; (e) Disrupts or causes disruption of any computer, computer system or computer network; (f) Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means; g) Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations

made there under; (h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, Section 65 of IT ACT 2000, defines as, Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programs, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. Section 66 of IT ACT 2000, defines as, (1) Whoever with the intent to cause or knowing that he is likely to cause rongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. (2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. POSSIBLE PUNISHMENTS (IT ACT + International laws) Cyber crime is a type of crime that not only destroys the security system of a country but also its financial system. One supporter of legislation against cyber crime, Rep.

Lamar Smith (R-Texas), stated, " Our mouse can be just as dangerous as a bullet or a bomb. " Cyber attackers should be penalized and punished severely and most cyber crimes have penalties reflecting the severity of the crime committed. Although in the past many laws against cyber crimes were insufficient, law enforcement agencies and governments have recently

proposed many innovative plans for fighting cyber crimes. Punishment Cybercrime must be dealt with very seriously because it causes a lot of damage to businesses and the actual punishment should depend on the type of fraud used.

The penalty for illegally accessing a computer system ranges from 6 months to 5 years. The penalty for the unofficial modification on a computer ranges from 5 to 10 years. Other penalties are listed below: Telecommunication service theft: The theft of telecommunication services is a very common theft and is punished with a heavy fine and imprisonment. Communications intercept crime: This is a Class-D crime which is followed by a severe punishment of 1 to 5 years of imprisonment with a fine.

Other cyber crimes like telecommunication piracy, offensive material dissemination, and other cyber frauds also belong to this category. InformationTechnologyAct-2000: According to this act, different penalties are available for different crimes. Some of the penalties are as follows: Computer source document tampering: The person who changes the source code on the website or any computer program will get a punishment up to 3 years of imprisonment or fine. Computer hacking: The individual who hacks the computer or computer devices will get an imprisonment up to 3 years or a fine.

Government protected system: An act of trying to gain access to a system which is a protected system by the government, will result in imprisonment for 10 years and a heavy fine. The introduction of such penalties have lead to a drastic reduction in the cyber crime rates as more and more criminals are becoming aware of the penalties related to them. Spreading the word

about the penalties of cyber crime can serve as a deterrent against such crime. Penalties relating to cyber crime will vary depending on the country and legislation in place. Punishments according to IT ACT 2000

The person who commits the crime shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected according to section 43 of IT ACT. The person who commits the crime shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both according to section 65 of IT ACT. Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both according to section 66 of IT ACT 2000 INTERNATIONAL LAWS In USA section 18 U. S. C. § 1030 A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and (B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; In Canada

The person who commits the crime is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction. UNLAWFUL LOSSES AND GAINS Losses due to hacking Hackers targeted major companies including Sony, RSA Security, and Citigroup, but also governmental websites and smaller

firms. Many companies could have prevented the attacks. Because of their vulnerabilities, they not only lostmoney, but also risked losing clients, prestige and market share. Multitudes of people were affected by their security breaches Recent reports showed hackers earned $12. billion in 2011, mainly by spamming, phishing, and online frauds. Some companies have made their financial losses public, while others chose not to disclose them. Here’s a top 5 of the declared losses caused by hackings from last year until present. Undeclared losses may even exceed these ones. 1. $171 million – Sony Hacked in April to June 2011, Sony is by far the most famous recent security attack. After its Playstation network was shut down by LulzSec, Sony reportedly lost almost $171 million. The hack affected 77 million accounts and is still considered the worst gaming community data breach ever.

Attackers stole valuable information: full names, logins, passwords, e-mails, home addresses, purchase history, and credit card numbers. 2. $2. 7 million – Citigroup Hacked in June 2011, Citigroup was not a difficult target for hackers. They exploited a basic online vulnerability and stole account information from 200, 000 clients. Because of the hacking, Citigroup said it lost $2. 7 million. Just a few months before the attack, the company was affected by another security breach. It started at Epsilon, an email marketing provider for 2, 500 large companies including Citigroup.

Specialists estimated that the Epsilon breach affected millions of people and produced an overall $4 billion loss. 3. $2 million – Stratfor Last Christmas wasn’t so joyful for Stratfor Global Intelligence. Anonymous members hacked the US research group and published confidential information from 4, 000

clients, threatening they could also give details about 90, 000 credit card accounts. The hackers stated that Stratfor was “ clueless...when it comes to database security”. According to the criminal complaint, the hack cost Stratfor $2 million. 4. $2 million – AT& T The US carrier was hacked last year, but said no account information was exposed.

They said they warned one million customers about the security breach. Money stolen from the hacked business accounts was used by a group related to Al Qaeda to fund terrorist attacks in Asia. According to reports, refunding costumers cost AT& T almost $2 million. 5. $1 million – Fidelity Investments, Scottrade, E*Trade, Charles Schwab The most recent declared losses were in a brokerage scam. A Russian national was charged in the US with $1. 4 million in computer and hacking crimes. $1 million was stolen from stock brokerages Fidelity Investments, Scottrade, E*Trade, and Charles Schwab.

The rest of the money was taken from fraudulent tax refunds, with the stolen identities of more than 300 people. Gains To Hackers * To use your computer: * as an Internet Relay Chat (IRC) server - hackers wouldn't want to discuss openly about their activities on their 'own' servers * as Storage for Illicit Material (ex. pirated software, piratedmusic, pornography, hacking tools etc) * as part of a DDoS Attack - where many computers are controlled by hackers in an attempt to cause resource starvation on a victim's computers or networks * To steal services and/or valuable files For thrill and excitement * To get even - maybe an IT staff who was terminated, or other parties you've 'wronged' * As a publicity stunt - an example of which was reported in 1998 by Jim Hu in MTV " hack" backfires *

Knowledge/Experiment/Ethical - some hackers probe a computer system to find its security vulnerabilities and then inform the system administrator to help improve their security * Another possible reason is that the hackers might suffer from a disease called Asperger syndrome (AS).

They are people who are very good with numbers and at focusing on a problem for a very long period of time, but are not good in social relationships. How AS can possibly be linked to hacking behavior was discussed more thoroughly by M. J. Zuckerman in his 'USA Today' article, What fuels the mind of a hacker? * Curiosity * To spy on friends, familymembers or even business rivals * Prestige - bragging rights in their social circle (particularly if they've hacked high-profile sites or systems) * Intellectual Challenge Money - although most hackers are not motivated by financial gain; many professional criminals make money by using hacking techniques either to * set up fake e-commerce sites to collect credit card details * gain entry to servers that contain credit cards details * engage in other forms of credit card fraud WORKING OF ATTACKS Before studying about how traffic injection attacks works there are some basic terms we shoud have to know WEP Wired Equivalent Privacy (WEP) is a shared-secret key encryption system used to encrypt packets transmitted between a station and an AP.

The WEP algorithm is intended to protect wirelesscommunicationfrom eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network. WEP encrypts the payload of data packets. Management and control frames are always transmitted in the clear. WEP uses the RC4 encryption algorithm. The shared-secret key is either 40 or 104

bits long. The key is chosen by the system administrator. This key must be shared among all the stations and the AP using mechanisms that are not specified in the IEEE 802. 11. FRAMES Both the station and AP radiate and gather 802. 1 frames as needed. The format of frames is illustrated below. Most of the frames contain IP packets. The other frames are for the management and control of the wireless connection. There are three classes of frames. The management frames establish and maintain communications. These are of Association request, Association response, Reassociation request, Reassociation response, Probe request, Probe response, Beacon, Announcement traffic indication message, Disassociation, Authentication, Deauthentication types. The SSID is part of several of the management frames.

Management messages are always sent in the clear, even when link encryption (WEP or WPA) is used, so the SSID is visible to anyone who can intercept these frames. Authentication Authentication is the process of proving identity of a station to another station or AP. In the open system authentication, all stations are authenticated without any checking. A station A sends an Authentication management frame that contains the identity of A, to station B. Station B replies with a frame that indicates recognition, addressed to A. In the closed network architecture, the stations must know the SSID of the AP in order to connect to the AP.

The shared key authentication uses a standard challenge and response along with a shared secret key. Traffic injection quick HOWTO •1 Insert adapter •2 Load driver and activate adapter •3 Set driver into monitor mode (real 802. 11 mode) •4 Set appropriate channel •5 Open PF PACKET/RAW socket on

interface (Linux only) •6 Use your socket and play • Still, you need a 802. 11 stack over your socket and/or good libs • and tools so you can communicate WORKING – This phase of term paper describes the working of attack by using one tool called INJECTION WIZARD

Injection Wizard is an application for injecting traffic into WEP-protected Wi-Fi networks, like aireplay-ng, but it's much more easy to use and it can work with worse conditions (for example, more interferences, weaker transmitted/received signals, more restricted access points, etc). The higher the traffic of the network, the earlier we will be able to crack a WEP key with tools like aircrack-ng, airsnort, dwepcrack, weplab, WEPAttack, WEPCrack, etc. However, injecting traffic is not easy because you must build or capture a frame that causes a response frame in any other station (that is, a wireless node).

This application carries out automatically all the needed actions to build a frame that causes a response in other station. These actions can be summarized in the following sequence of steps: 1. The application scans Wi-Fi networks and shows a list of WEP-protected networks, then it allows the user to select one of them. 2. It joins the selected network and monitors that network in order to find a data frame. 3. It tries to extract a keystream prefix from the captured frame and then it tries to extend the keystream up to 40 bytes by means of the W.

A. Arbaugh's inductive chosen plaintext attack. 4. It tries to find a host (for example, a connected computer, a network device, etc), which has an IP address belonging to a predefined range, by injecting forged ARP packets. 5. After finding an active host, it injects ARP packets targeted at that host.

Some of the benefits of this application are easiness of use (due to its graphical interface, automatic operation, etc) androbustness (detection/management of network disconnections, repetition of failed actions, etc).

Moreover, the Arbaugh's inductive attack can be performed by any Wi-Fi interface supporting injection in monitor mode, because the interface driver doesn't need any additional patch as it's usual to happen with the Bittau's fragmentation attack. Besides its higher applicability, this attack is generally more reliable than Chop-Chop attack for recovering a keystream of a given size, because it doesn't have to inject any frame larger than needed. This application is distributed under the terms of the GNU General Public License version 2 (read the license. tm file for more details) and comes with absolutely no warranty. The author assumes noresponsibilityderived from the use or the distribution of this program. The copyright of this application is owned by Fernando Pablo Romero Navarro (May 2010). Injection Wizard has made use of (with convenient modifications) the following free software applications: * scapy (version 2. 0. 1), distributed under the license: GNU GPL version 2. Copyright: Philippe Biondi, 2009 (http://www. secdev. org/projects/scapy). * python-wifi (version 0. 3. 1), distributed under the license: GNU LGPL version 2. 1.

Copyright: Roman Joost, 2004-2008 Software Requirements For the client application (graphical interface): •Any system with a recent Java virtual machine: JRE version 1. 6 or later. For the server application: * A Linux box with a recent kernel, so it should support Wireless Extensions version 22 or later (since kernel version 2. 6. 21) and the mac80211 stack for Wi-Fi

interfaces (since kernel version 2. 6. 24, it is supported by many Wi-Fi adapter drivers). * A Wi-Fi network interface driver supporting injection in monitor mode (sometimes it's required to patch the driver for supporting this feature). The iw system command, if it's not provided by your Linux distribution you can get it by installing the aircrack-ng package or by compiling the source code that can be downloaded from: http://wireless. kernel. org/download/iw. * A Python interpreter with version 2. 5, later versions might also work. Instructions 1. Uncompress the injwiz. zip file. 2. Copy the client directory on a system with a Java virtual machine accessible from the command path (for example, launch a shell, enter the client directory, execute the command: java -version and check the command outputs the JRE version number). .

Copy the server directory on a Linux box. If the client and server directories weren't copied on the same machine, you should edit the runserver. sh script (in the server directory) and replace the IP address: 127. 0. 0. 1 with the IP address of the Linux box's network interface that is attached to the same network that the client machine (i. e. the computer that hosts the clientdirectory). 4. Enter the server directory and run the script: . /runserver. sh (the Python interpreter should be accessible from the command path. You can check this by running: ython -V from the command line and verifying that the interpreter version is showed). 5. On the client machine, enter the client directory and run either the script: . /runclient. sh (for Linux or Unix-like operating systems providing a shell compatible with the Bourne shell and whose path for the executable file is: /bin/sh) orrunclient. bat (for Windows). DESCRIPTION OF TOOLS The tools used for packet injection

purposes are divided into two categories Hardware and software 1. Software Serious hackers usually use Linux-based open source penetration test tools from which to launch their attacks.

This section details some of the more popular tools that can be used to search out and hack wifi networks. •Aircrack-ng: This suite of tools includes 802. 11 WEP and WPA-PSK key cracking programs that can capture wireless packets and recover keys once enough information been captured. Aircrack-ng supports newer techniques that make WEP cracking much faster. This software has been downloaded over 20, 000 times. •Airjack: An 802. 11 packet injection tool, Airjack was originally used as a development tool to capture and inject or replay packets.

In particular, Airjack can be used to inject forged deauthentication packets, a fundamental technique used in many denial-of-service and Man-in-the-Middle attacks. Repeatedly injecting deauthentication packets into a network wreaks havoc on the connections between wireless clients and access points. •AirSnort: AirSnort is wireless LAN (CLAN) tool which recovers WEP encryption keys. AirSnort works by passively monitoring transmissions, and then computing the encryption key when enough packets have been gathered.

After that point, all data sent over the network can be decrypted into plain text using the cracked WEP key. •Cain ; amp; Able: This is a multi-purpose tool that can intercept network traffic, using information contained in those packets to crack encrypted passwords using dictionary, brute-force and cryptanalysis attack methods, record VoIP conversations, recover wireless network keys, and analyze routing protocols. Its main purpose is the

simplified recovery of passwords and credentials. This software has been downloaded over 400, 000 times. CommView for WiFi: This commercial product is designed for capturing and analyzing wifi network packets. CommView for WiFi uses a wireless adapter to capture, decode, and analyze packets sent over a single channel. It allows hackers to view the list of network connections and vital IP statistics and examine individual packets. •ElcomSoft Wireless Security Auditor: This is an all-in-one cracking solution that automatically locates wireless networks, intercepts data packets, and uses cryptanalysis techniques to crack WPA/WPA2 PSKs.

This software displays all available wireless networks, identified by channel number, AP MAC address, SSID, speed, load, and encryption parameters. While these capabilities can be found in open source tools, ElcomSoft provides a more polished product for professional use by wireless security auditors. •Ettercap: Ettercap can be used to perform man-in-the-middle attacks, sniff live connections, and filter intercepted packets on the fly. It includes many features for network and host analysis. This shareware has been downloaded nearly 800, 000 times. Firesheep: This is a plug-in to the Firefox browser that allows the hacker to capture SSL session cookies sent over any unencrypted network (like an open wifi network) and use them to possibly steal their owner’s identities. It is extremely common for websites to protect user passwords by encrypting the initial login with SSL, but then never encrypt anything else sent after login, which leaves the cookie (and the user) vulnerable to “ sidejacking.

” When a hacker uses Firesheep to grab these cookies, he may then use the SSL-authenticated session to access the user’s account. Hotspotter: Like

KARMA, Hotspotter is another wireless attack tool that mimics any access point being searched for by nearby clients, and then dupes users into connecting to it instead. •IKECrack: This is an open source IPsec VPN authentication cracking tool which uses brute force attack methods to analyze captured Internet Key Exchange (IKE) packets to find valid VPN user identity and secret key combinations. Once cracked, these credentials can be used to gain unauthorized access to an IPsec VPN. KARMA: This evil twin attack listens to nearby wireless clients to determine the name of the network they are searching for and then pretends to be that access point. Once a victim connects to a KARMA evil twin, this tool can be used to redirect web, FTP, and email requests to phone sites in order to steal logins and passwords. •Kismet: Kismet takes an intrusion detection approach to wireless security, and can be used to detect and analyze access points within radio range of the computer on which it is installed.

This software reports SSIDs (Service Set Identifiers – used to distinguish one wireless network from another) advertised by nearby access points, whether or not the access point is using WEP, and the range of IP addresses being used by connected clients. •NetStumbler: This tool turns any WiFi-enabled Windows laptop into an 802. 11 network detector. NetStumbler and dozens of similar “ war driving” programs can be used with other attack tools to find and hack into discovered wifi networks. •WireShark: WireShark is a freeware LAN analyzer that can be used to passively capture 802. 11 packets being transmitted over a wifi network.

This software has been downloaded millions of times. 2. Hardware •For hackers that prefer a turn-key package, there are also hardware wireless

hacking tools available. We've highlighted one called WiFi Pineapple. It's a simple, small, portable device that can be carried into any hotspot and used to attract any laptop trying to find a wifi access point. The Pineapple uses a technique called an Evil Twin attack. Hackers have used tools like KARMA to do the same thing for years, but with Pineapple, now you can buy a piece of hardware for only $100 that allows you to become a hacker without downloading or installing any software. Here's what their website says: " Of course all of the Internet traffic flowing through the pineapple such as e-mail, instant messages and browser sessions are easily viewed or even modified by the pineapple holder. "

REFERENCES http://www. cse. wustl. edu/~jain//cse571-07/ftp/wireless_hacking/index. html http://www. cs. wright. edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks. htm#_Toc77524642 http://www. webopedia. com/TERM/C/cyber_crime. html http://www. wi-fiplanet. com/tutorials/article. php/3568066 file:///C:/Users/jsk/Desktop/Wireless%20Hackers%20101. htm