

Laptop Security

by: Ramanujam Narasimman , 06/23/2005

<http://www.securitydocs.com/library/3399>

Objective

To assess the current computer security issues related to Laptops and providing countermeasures to secure corporate information on these laptops.

Executive Summary

As the price of computing technology is steadily decreasing, devices like the laptops and mobile phones have become more common in use. Although these devices enhance the business functions due to their mobile access to information anytime and anywhere, they also pose a large threat as they are mobile and small. Wireless capability in these devices has also raised security concerns due to the information being transmitted over ether, which makes it hard to detect. This paper discusses about the various threats to laptops with respect to physical security, information security and wireless security domains. The threats are followed by suggested countermeasures which would help in reducing laptop security compromise. The suggestions made in this paper have been researched from various valid resources and security reports. Towards the end of this paper, we have included an example of organizational security policy for laptops used in an organization.

The paper has been written for common audiences and hence involves less of technical details. For more detailed technical information on these solutions and threats, please do refer to the List of references and bibliography available towards the end of this paper.

1. Introduction

Computers have always helped in reducing the complexity of day to day functions. The innovation of mobile computing has given the users the power and flexibility to view information on the run. Although mobile computing has been a boon in disguise, it has lead to certain critical computer security issues due to the mobility function of the computer. This report will focus on listing the current computer security threats for laptops and by providing countermeasures for the same.

2. Current computer security issues for Laptops

2.1. Physical Security

According to the computer security industry and insurance company statistics, thefts of laptops have always been a major issue. Criminals are targeting laptop systems that are expensive as it could fetch them a quick profit in the black market. Very few laptop thieves are actually interested in the information that is contained in the laptop. Most laptops contain personal and corporate information which could be sensitive. Such information can be misused if found by a malicious user. It is a common belief of senior executives in an organization to think that the information stored on their laptop is only useful for them and would not be of any interest to others. Due to this belief, most senior executives in an organization feel that it is unnecessary to protect the information stored on these laptops. (Korzeniowski, 2001).

2.2. Physical Security Countermeasures

2.2.1. Cables and hardwired locks

Securing with cables and locks specially designed for Laptops is the most cost efficient and ideal solution to safeguard any mobile devices. Kensington cables are one of the most popular brands in laptop security cables. These cables are made of aircraft grade steel and Kevlar brand fiber, thus making these cables 40% stronger than any other conventional security cables. One end of the security cable is fit into the universal security slot of the laptop and the other end is locked around any fixed furniture or item thus making a loop. These cables come with a variety of options like number locks, key locks and alarms. (Kensington, n.d.).

The downside of security cables lies in the fact that one can easily remove detachable bays like CDROM bay, PCMCIA cards, HDD bay and other removable devices from the laptop as the cable only secures the laptop from being stolen. The other disadvantage of security cables is when the laptop is locked to an object which is not fixed or is weak enough for anyone to break it. In certain cases of laptop thefts, the thief dismantled or smashed the fixed item to which the laptop was secured to. (Ryder, 2001).

2.2.2. Laptop Safes

Safes made of polycarbonate, the same material used in bullet proof windows, police riot shields and bank security screens can be used to carry and safeguard the laptops. (ESafe, n.d.). The advantage of safes over security cables is that it protects the whole laptop and its devices like CDROM bays, PCMCIA cards, HDD bays which can be easily removed in case of laptops protected by security cables. (Ryder, 2001).

2.2.3. Motion Sensor and Alarms

Even though alarms and motion sensors are annoying due to their false alarms and loud sound level, these devices are very efficient in securing laptops. Once activated these devices can be used to track missing laptops in crowded places and also due to their loud nature they help in deterring thieves. (Ryder, 2001).

TrackIT Corporation has devised a new alarm system for laptops wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop. The owner of the laptop has a key ring device which communicates with the laptop alarm device. The alarm is triggered when the distance between the laptop alarm device and the key ring device crosses the specified range. (Ryder, 2001).

Caveo has invented a security PCMCIA card which acts as a motion detector, alarm system and also has the capability to lockdown the laptop in case the laptop is moved out of the designated range. It also secures the passwords, encryption keys and prevents access to the operating system. The card has a battery which keeps it powered on even when the system is shutdown. (Caveo, n.d.).

2.2.4. Warning Labels and Stamps

Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low cost solution to laptop theft. These labels have a identification number which is stored in a universal database for verification which in turn makes the resale of stolen laptops a difficult process. (Stoptrack, n.d.).

2.2.5. Other Solutions

- Engraving the laptop with personal details.
- Keeping the laptop close to oneself wherever possible
- Carrying the laptop in different bag making it unobvious to potential thieves.
- Making the employee understand about the responsibility of the laptop and also about the sensitivity of the information contained in the laptop. (Ryder, 2001).
- Make a copy of the purchase receipt, laptop serial number and the description of the laptop.
- Installing encryption software to protect information stored on the laptop.
- Using personal firewall software to block unwanted access and intrusion.
- Anti-virus software needs to be updated regularly.
- Carrying the laptop in an unobvious bag.
- Tight office security using security guards and securing the laptop by locking it down in lockers when not in use.
- Never leave the laptop unattended until it's fitted with an anti-theft device.
- Never leave the laptop unattended in public places like the car, parking lot, conventions, conferences and the airport.
- Disable infrared ports, wireless cards and remove PCMCIA cards when not in use. (Laptop Security, n.d.).

2.3. Information Security

Information, be it corporate or private needs high security as it's the most important asset of an organization or an individual. Recently there has been an increase in laptop thefts which contained sensitive and secret information belonging to the

Australian defense and security consultant agencies. Laptops belonging to corporate bodies like Banks, Government Agencies, and Defense Authorities need to be highly secured as they might contain confidential information about any individual or the nation itself. The information stored on these laptops can be used against the organization by competitors or users with malicious intent.

2.3.1. Malicious Programs /Hackers / Social Engineering

Malicious programs can be classified into various types like Viruses, Trojans, Worms, Rootkits, Dialers, Joke, Spyware and Spam. These programs are written by malicious users to corrupt, destroy or gain access to the information stored on computers. Some Malware install backdoors on the computer to allow unauthorized access and also to send information out without the knowledge of the computer user. (Threats and Malware, n.d.).

There has been a steady increase in development of malicious programs due to lack of proper law enforcements and weak security. Information can be retrieved or damaged using these malicious programs. Apart from these programs, hackers also use social engineering skills to gather tips from users to break into their computer. (Dvorak, 2004).

2.3.2. Weak Passwords / Open Access

Passwords are like the security gates to the computer. The stronger they are the harder to break them. Choosing a weak password which is based on common names or word found in the dictionary can make the security of the computer weak. Passwords should not be less than 7 characters and should contain alphanumeric characters. Do not store passwords on the laptop drive and also do not write down any password on the laptop. Never disclose your passwords, do not use the same password for all applications and never allow applications or web browsers to store your password. (Lawrence, 2005).

2.3.3. Application security and vulnerabilities

Hackers have now started to delve into the vulnerabilities of applications to find an exploit and cause attack. Applications pose a major threat especially, if they are developed by poor project management and developing teams. Malicious users have many tools available publicly to scan for vulnerable systems and for vulnerabilities in the systems. Unpatched computers stand a higher risk of getting compromised due to open loopholes. (Symantec, 2002).

2.3.4. Unencrypted data/ Unprotected File systems

Information stored on critical laptops should not be stored as unencrypted information or in clear text. This would enable anyone who has physical access to the hard disk or has gained access to the system to read all the data stored on the laptop. Being mobile devices these need implementation of encryption due to high probability of these devices being compromised due to their mobile nature. (Ryder, 2001).

2.3.5. Removable drives / Storage Mediums / Unnecessary Ports

The removable drives like hard disk bays in laptops can be easily removed by anyone. USB ports in laptops need to be disabled whenever not in use. USB sticks can be plugged to the laptop to copy information over or pass malicious applications to the computer without the user's knowledge. USB drives are not easily traceable due to their small sizes and there is no way at present to scan the network to detect usage of USB drives. (Webster, 2005).

2.4. Information Security Countermeasures

Applications on the laptops should be frequently updated to avoid such malicious programs and unauthorized access. The owner of the laptop has to be educated towards the usage of data or applications on the laptop. (Computer Security, n.d.).

2.4.1. Password protection / Complex passwords

Passwords should be made as strong as possible and difficult to guess. Passwords should be a mix of upper case, lower case, alphanumeric characters and special symbols. Never reveal passwords to anyone under any circumstances nor do store or write the passwords anywhere it is visible to others. It is a good practice to use different passwords for different applications. The BIOS of the laptop should be locked with a password to prevent others from changing the boot sequence of the laptop. Floppy drives and other devices can be disabled using the BIOS settings. (Ryder, 2001).

2.4.2. Lock down unwanted ports / devices

Unwanted ports like USB ports, infrared ports can be password protected using device locking software. Such port locking

software would allow only the authorized user to access these ports. Unauthorized users cannot transfer information using USB drives if the USB port is locked down by the administrator. Whenever the laptop owner needs to access the ports, they have to unlock the ports via the device locking software by providing a password. (Webster, 2005). An example of such software is Device Lock from Smart Line Technologies. (Device Lock, n.d.).

2.4.3. Patches and Updates

Operating system software and other applications software needs to be updated on a regular basis to patch loopholes and other vulnerabilities which are not found during application development. All the applications on the laptop should be patched and updated from appropriate vendor's website. (CITES, 2005).

2.4.4. Anti virus software / Firewalls / Intrusion detection systems

Antivirus software and Spyware detection software needs to be installed and updated regularly on the laptop. The antivirus software can be configured to do automatic updates and scheduled scanning of the hard drive to check for possible viruses. The laptop should also be configured with personal firewall and intrusion detection systems to prevent unauthorized access and malicious scripts to the system. (CITES, 2005).

2.4.5. Encrypted File System

File systems are used by computers to read and write a file from the hard disk. It is a sign of strong security to have all the files on the hard drive in encrypted form. This protects the files from being opened or altered by unauthorized users. Encrypted file systems form a layer over the existing file system and thus encrypt all the files under it. Without the proper key or pass phrase it's a Hercules task to view these files in clear text. This kind of protection would help in preserving data integrity even when the laptop is stolen, as the thief would have to crack the encryption to view the sensitive information stored on the drive. (Ryder, 2001).

2.4.6. Other countermeasures

- Choosing a secure operating system which has been tested for quite some time and which has high security incorporated into it.
- Registering the laptop with the laptop manufacturer to track down the laptop in case of theft.
- Disabling unnecessary user accounts and renaming the administrator account.
- Disable display of the last logged in user name in the login dialog box.
- Data backup on a regular basis. (Labmice, 2003).

2.5. Wireless Security

2.5.1. Interception and Monitoring wireless traffic

Using various sniffer tools and interception software, one can intercept the information that is passed over the wireless communication links. Tools like Netstumbler (www.netstumbler.org) and Kismet (www.kismetwireless.net) can easily sniff information packets transmitted over wireless links. The attacker can masquerade his computer settings to match that of the victim's computer and access all the information passed in the wireless network. (Klaus, 2002). Interception and monitoring of wireless traffic is the initial stage of hacking technique used by attackers and is a kind of passive wireless attack. (Shimonski, 2003).

2.5.2. Packet Insertion /Hijacking attacks

Once the attacker is able to sniff the wireless traffic, it's possible for the attacker to inject false packets or commands into the existing wireless packet stream and thus compromise the wireless laptop or the wireless network that the attacker is connected to. This is known as the packet insertion or session hijacking attack. (Klaus, 2002).

2.5.3. Jamming

In this kind of attack, the attacker uses different wireless devices which run on different frequencies and thus create radio frequency interferences for any wireless network in vicinity. Due to these interfering frequencies, the victim wireless network would be jammed or frozen. (Shimonski, 2003).

2.5.4. Peer to peer attacks / Ad Hoc mode

Ad Hoc mode is used to form a peer to peer connection between two wireless devices. This is used to share files or access computers which are near each other's vicinity. When this option is turned on in a wireless enabled laptop; all shared information stored in the laptop can be accessed by any other wireless laptop within a specific range. Malicious users can transfer files or execute commands onto a victim's laptop without the knowledge of the user. By default this option is switched on in most operating system software. (Scott , 2004).

2.5.5. Man in the middle attack

The man in the middle attack has been a famous attack when it comes to wired network. Hackers have devised ways to perform the man in the middle attack for wireless networks too. In the man in the middle attack, the attacker may place a rogue access point in a legitimate wireless network, configure the rogue access point with the valid SSID of the victim's wireless network and thus gather all the sensitive information from authorized users connecting to the wireless network. Some attackers also use a laptop with two wireless network cards, where one card acts as an access point and the other wireless card forwards all the connections from the Access Point card to the legitimate access point. (Shimonski, 2003).

2.5.6. Wiphishing

Wiphishing is a new attack used by hackers to attack wireless network and wireless enabled devices. Attackers can setup access points with SSID that are used by default on most access points. This attack can be carried out on users who have their wireless adaptor enabled on their laptop and have the connection configured to automatically connect to any wireless access point in vicinity. (Mobile Pipeline , 2004).

If the wireless adaptor is left enabled on a laptop which is connected to a wired network, the attacker can compromise the wired network using the wireless adaptor of the victim's laptop. (Techtree , 2005).

2.6. Wireless Security Countermeasures

2.6.1. Enabling WEP /WPA on the wireless network

Wired Equivalent Privacy (WEP) is an encryption standard developed for wireless networks. WEP is usually turned off by default in most access points when they are shipped. WEP supports 40 bit key and 128 bit key for encryption. Even though WEP has many flaws, it's still advisable to turn WEP on as it helps in delaying the attack to the wireless network. The other more secure option to WEP is WPA (Wifi Protected Access) which can be seen as an improvement in wireless security. It uses two phases, in the first phase it keeps changing the keys and in the second phase it uses AES encryption standard. WPA also relies on encryption keys like WEP, but the only difference is that WPA keeps changing the key regularly. (Rutgers , 2003).

2.6.2. MAC address control

MAC address control feature allows access to only those wireless connections which originate from the MAC card whose MAC address is stored in the filter list. Again, this feature can be spoofed too as MAC addresses are transmitted as clear text during wireless associations and there are certain tools which allow a user to spoof their MAC address on the fly. Also this feature would suit more to a wireless environment containing a few users as its hectic task to update the MAC addresses in a dynamic environment. (Internet Security Systems , 2001 , p.6).

2.6.3. End to end encryption

This is the most recommended option where the whole conversation between wireless clients and the wireless network is in encrypted form. Technologies like SSL and SSH can be used to deploy the end to end encryption mechanism. In addition to encryption, SSL and SSH also use digital certificates which is very useful in identifying valid users. (Rutgers , 2003).

2.6.4. VPN (Virtual Private Network)

Virtual Private Networks is an alternative solution to protect the information transmitted over wireless links. VPN is also an encryption technology wherein the data that is passed between two users forming a VPN tunneling session is encrypted and cannot be sniffed. The big difference between VPN and SSL is that all the traffic that passes through a VPN tunnel is encrypted, while in SSL the encryption is only between one to one connections. VPN can be used for many to many connections. The only drawback of VPN is that all the users wishing to use VPN should have the necessary software installed on them. (Rutgers , 2003).

2.6.5. Access points evaluation

The wireless network should be regularly checked for rogue access points and also for any change in configurations details. Wireless monitoring agents can track down unauthorized access points by checking the wireless packets transmitted by them. An access point configuration policy should be set by administrators which should contain the default security settings. (Internet Security Systems , 2001 , p.7).

2.6.6. Other countermeasures

- Personal firewalls and intrusion detection systems to be installed on laptops.
- Scanning the operating system for any security misconfigurations.
- Locking down the system with limited user accounts and limited access.
- Disabling broadcast of SSID.
- Regular security audits and penetration testing should be conducted on the wireless networks.

(Internet Security Systems , 2001 , p.7,8).

3. User Education /Training

Proper implementation and maintenance of security in an enterprise lies in the hands of the users Who operate and use computing as part of their functions. Users who rely on computing needs should be educated on the need of security for the same. The policies and procedures created for the computing environment should be communicated to the users in a clear and precise manner. If the users are not reminded from time to time about the security concerns with regards to the enterprise information or enterprise in whole, they tend to ignore it.

They should be regularly updated with latest threats and information to the secure functioning of the organization. Employees should be required to understand and sign the updated computer usage and security policies every year. The key risk areas should be identified and informed to users in the organization. Also the complexity of the policies should be taken care of to make it easier for general users to understand the same. (Friedlander & Sundgren , 2004).

4. Suggested Hardware specifications

<u>Hardware Name</u>	<u>Estimated Price</u>	<u>Company</u>
Kensington cables & Locks	\$50 - \$90	www.kensington.com.au
Laptop E- Safe	\$595 - \$675	www.hide-away-safe.biz
Caveo PCMCIA Anti-Theft Alarm	\$160	www.caveo.com
Tamper Proof Labels	Unavailable	www.apro.com.au/stop.htm

5. Recommended Software List

<u>Software Name</u>	<u>Estimated Price</u>	<u>Company</u>
Norton Antivirus	\$90 - \$99	www.symantec.com.au
Norton Firewall	\$90 - \$99	www.symantec.com.au
Norton Internet Security	\$111 - \$150	www.symantec.com.au
Dragon IDS	Unavailable	www.enterasys.com
Netstumbler	Free	www.netstumbler.org
Kismet	Free	www.kismetwireless.net
Computrace	Unavailable	www.absolute.com

6. Example of Laptop Security Policy

The following security policy is an example taken from the laptop security policy statement of the University of Auckland.

6.1. Responsibility of Users

- The laptop users should agree to take responsibility for the security of the laptop and also for the information stored in the laptop.
- Users must take all the precautions and necessary steps to protect against installation of any malicious or unlicensed software.
- Comply with copyright requirements of the software or data used.
- Users should ensure that proper care is taken of the laptop.

6.2. Physical Security

- Avoid leaving the laptop unattended in public places.
- Any sensitive information displayed on the laptop screen should not be displayed in public places.
- Physically secure the laptop when it has to be left unattended for a long period in public places.
- Laptops should be carried as hand luggage while traveling.

6.3. Access Control / Authentication

- The laptop screen should be password protected if it has to be left unattended in a public place.
- A strong password should be chosen to lock down the laptop and also user should keep updating the password.

6.4. Data Protection

- All data saved on the laptop should be encrypted and classified.
- All sensitive data should be backed up on a regular basis.
- Whenever possible all sensitive information should be saved on the network servers of the organization.

6.5. Tracking / Recovery

- If the laptop is stolen or lost, it should be reported to the respective authorities and police immediately.

(Taylor , 2004).

7. Conclusion

Although there are various software and hardware mechanisms to prevent laptop theft and loss of information, the security of laptop depends on the awareness of the user possessing the laptop. If the user ignores or takes security as a minor concern, no mechanism can help prevent the theft of any a device.

8. List of references

Bajkowski, J., & Crawford, M., (2004, October 6). Highly sensitive laptops go missing, Retrieved on April 15, 2005, from <http://www.computerworld.com.au/index.php/id:260567028:relcomp:1>

Caveo. (n.d.). Caveo Anti-theft and Defcon MDP PC cards, Retrieved on April 15, 2005, from <http://www.caveo.com/products/anti-theft.htm>

CITES,(2005, January 10). Laptop Security, Retrieved on April 15, 2005, from <http://www.cites.uiuc.edu/security/scenarios/laptop.html>

Computer Security, (n.d.). Computer Security, Retrieved on April 15, 2005, from <http://www.akpei.com/RMNotes/RM129-ComputerSafety903.htm>

Device Lock, (n.d.). Device Lock, Retrieved on April 15, 2005, from <http://www.protect-me.com/dl/>

Dvorak, C.J. (2004, August 3). Why Are Virus Attacks Getting Worse? , Retrieved on April 15, 2005, from <http://www.pcmag.com/article2/0,1759,1544653,00.asp>

ESafe. (n.d.). Serious security for a serious problem, Retrieved on April 15, 2005, from <http://www.bestsecurity.com.au/laptop.html>

Friedlander,D., & Sundgren,J., (2004, January 30), Best Practices: Desktop Security, Retrieved on April 15, 2005, <http://www.microsoft.com/business/executivecircle/content/page.aspx?cID=1175&subcatID=1>

Internet Security Systems, (2001), Wireless LAN Security 802.11b and Corporate Networks, Retrieved on April 15, 2005, from http://documents.iss.net/whitepapers/wireless_LAN_security.pdf

Korzeniowski,P. (2001, February).Locking down the laptop, Retrieved on April 15, 2005, from <http://www.kensington.com/html/3980.html>

Klaus, W.C.(2002, October 6), Wireless LAN Security FAQ ,Retrieved on April 15, 2005, from [http://www.iss.net/wireless/WLAN_FAQ.php#\[2\]%20What%20are%20the%20major%20security%20risks%20to%20802.11b?](http://www.iss.net/wireless/WLAN_FAQ.php#[2]%20What%20are%20the%20major%20security%20risks%20to%20802.11b?)

Labmice,(2003, December 10). Laptop Security Guidelines, Retrieved on April 15, 2005, from <http://labmice.techtarget.com/articles/laptopsecurity.htm>

Lawrence, G. (2005, May 9).Creating Passwords, Retrieved on April 15, 2005, from http://blink.ucsd.edu/Blink/External/Topics/How_To/0,1260,13716,00.html

Laptop Security, (n.d.). Laptop Security, Retrieved on April 15, 2005, from http://www.apro.com.au/support/laptop_security.htm

Mobile Pipeline,(2005, February 4), 'WiPhishing'said to threaten Wifi users, Retrieved on April 15, 2005, from <http://informationweek.networkingpipeline.com/59301067>

Ryder, J. (2001, July 30). Laptop Security, Part One: Preventing Laptop Theft, Retrieved on April 15,2005, from <http://www.securityfocus.com/printable/infocus/1186>

Rutgers,(2003, November 3), Wireless Security Recommendations for Rutgers, Retrieved on April 15, 2005, from <http://techdir.rutgers.edu/wireless.html>

Stoptrack. (n.d.). STOPTRACK anti-theft system, Retrieved on April 15, 2005, from <http://www.apro.com.au/stop.htm>

Symantec, (2002, May 7). Is patching a priority for your enterprise?, Retrieved on April 15, 2005, from <http://www.symantec.com/symadvantage/013/patching.html>

Shimonski, J.R. (2003, February 24), Wireless Attack Primer, Retrieved on April 15, 2005, from http://www.windowsecurity.com/pages/article_p.asp?id=1133

Scott,R.(2004, July 26), Top five don'ts in wireless security, Retrieved on April 15, 2005, from http://techrepublic.com.com/5100-6264_11-5283472.html

Threats and Malware, (n.d.). Threats and Malware , Retrieved on April 15, 2005, from

http://www.virusportal.com/com/training/train_key1.shtml

Techtree,(2005, April 5), Wiphishing Threatens Laptops ,Retrieved on April 15, 2005, from <http://www.techtree.com/techtree/jsp/print.jsp?file=articleprint.jsp&storyid=66837&ion=News&subsection=Security>

Taylor,S.(2004, March 30), Laptop Security Policy Version 1.1, Retrieved on April 15, 2005, <http://www.auckland.ac.nz/security/LaptopSecurityPolicy.htm#s111>

Webster,G. (2005, March 17). Flash drives: a security risk?, Retrieved on April 15, 2005, from <http://www.newbusiness.co.uk/cgi-bin/showArticle.pl?id=2823>

9. Appendix

PCMCIA

Short for Personal Computer Memory Card International Association, and pronounced as separate letters, PCMCIA is an organization consisting of some 500 companies that has developed a standard for small, credit card-sized devices, called PC Cards.

HDD

The mechanism that reads and writes data on a hard disk.

CDROM

Short for Compact Disc-Read-Only Memory, a type of optical disk capable of storing large amounts of data

SSH

Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

SSL

Short for Secure Sockets Layer, a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection.

VPN

Short for virtual private network, a network that is constructed by using public wires to connect nodes

WPA

Short for Wi-Fi Protected Access, a Wi-Fi standard that was designed to improve upon the security features of WEP

WEP

Short for Wired Equivalent Privacy, a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard.

SSID

Short for service set identifier, a 32-character unique identifier attached to the header of packets sent over a WLAN

IDS

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Access Point

Short for Access Point, a hardware device or a computer's software that acts as a communication hub for users of a wireless

device to connect to a wired LAN.