Examination 2

200 Points

Name: Maghen Smith

Email Address: mjs0026@auburn.edu

1. Download this exam electronically from /home/www/department/csse/classes/comp6370/projects.

2. All questions are equally weighted.

3. Word-process your answers inside the exam document.

4. All references are allowed except the solutions manual to the textbook.

5. Blank spaces are not to scale.

6. Document ALL of your sources.

7. Soft Copy exam due NLT 2:00 pm CDT Thursday 21 November. Hard Copy due in my hand no later than the start of class 21 November. Late Submissions will receive a grade of zero. Turn in soft copy of exam to the exam2\_F13 turn-in directory. Outreach students need only a soft copy.

8. USE the following naming convention for your exam soft copy files: lastnameXXXX\_exam2.doc where XXXX is a four-digit pin that you select.

9. Show all work.

10. This is an individual effort exam.

11. Check your permissions and ensure what you turn-in is legible. Unreadable test files equals late equals zero.

Scoring (Instructor use only)

Q#1 \_\_\_\_\_\_\_\_ out of 10 Q#2 \_\_\_\_\_\_\_\_ out of 10

Q#3 \_\_\_\_\_\_\_\_ out of 10 Q#4 \_\_\_\_\_\_\_\_ out of 10

Q#5 \_\_\_\_\_\_\_\_ out of 10 Q#6 \_\_\_\_\_\_\_\_ out of 10

Q#7 \_\_\_\_\_\_\_\_ out of 10 Q#8 \_\_\_\_\_\_\_\_ out of 10

Q#9 \_\_\_\_\_\_\_\_ out of 10 Q#10 \_\_\_\_\_\_\_\_ out of 10

Q#11 \_\_\_\_\_\_\_\_ out of 20 Q#12 \_\_\_\_\_\_\_\_ out of 20

Q#13 \_\_\_\_\_\_\_\_ out of 20 Q#14 \_\_\_\_\_\_\_\_ out of 20

Q#15 \_\_\_\_\_\_\_\_ out of 20

**Question 1 (10 Points)** Describe in detail how symmetric keys are exchanged in IPSEC-based VPNs.

“The goal of the *Internet Key Exchange* (IKE) is for both sides to independently produce the same symmetrical key... During IKE Phase I:

The peers authenticate, either by certificates or via a pre-shared secret. (More authentication methods are available when one of the peers is a remote access client.)

A Diffie-Hellman key is created. The nature of the Diffie-Hellman protocol means that both sides can independently create the shared secret, a key which is known only to the peers.

Key material (random bits and other mathematical data) as well as an agreement on methods for IKE phase II are exchanged between the peers.

…

Figure 2‑ 1 illustrates the process that takes place during IKE phase I but does not necessarily reflect the actual order of events.” (figure 2 and source info on next page)

Diffie-hellman: “**Diffie–Hellman key exchange** (**D–H**)[nb 1] is a specific method of exchanging [cryptographic keys](http://en.wikipedia.org/wiki/Key_(cryptography)). It is one of the earliest practical examples of [key exchange](http://en.wikipedia.org/wiki/Key_exchange) implemented within the field of [cryptography](http://en.wikipedia.org/wiki/Cryptography). The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a [shared secret](http://en.wikipedia.org/wiki/Shared_secret) key over an insecure [communications](http://en.wikipedia.org/wiki/Communication) [channel](http://en.wikipedia.org/wiki/Channel_(communications))... It is also possible to use Diffie–Hellman as part of a [public key infrastructure](http://en.wikipedia.org/wiki/Public_key_infrastructure). Alice's public key is simply . To send her a message Bob chooses a random *b*, and then sends Alice (un-encrypted) together with the message encrypted with symmetric key . Only Alice can decrypt the message because only she has *a* (the private key). A preshared public key also prevents man-in-the-middle attacks.”[http://en.wikipedia.org/wiki/Diffie-Hellman\_key\_exchange#Public\_Key]

<https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13847.htm>

“The actual processes of key exchange and parameter negotiation are carried out by two protocols used by IKEv1: Internet Security Association and Key Management Protocol (ISAKMP), oakley... Oakley provides the key-exchange function between peers using the DH protocol. DH is an asynchronous protocol, meaning each peer uses its own set of keys for communications establishment and operation between peers. However, the keys are never exchanged, providing a much higher level of security than synchronous protocols... Two mandatory IKEv1 phases … must be followed by each peer before a communications tunnel can be established between them and they are ready for successful transmission: ”During phase 1 “both peers negotiate parameters (integrity and encryption algorithms, authentication methods) to set up a secure and authenticated tunnel... Its sole scope is to handle secure Phase 2 negotiations. It is called bidirectional because both peers use only one session key to secure both incoming and outgoing traffic.”Authentication must be done by either pre-shared keys or digital certificates.”

<http://books.google.com/books?id=5PJisOKJ0k8C&pg=PA14&lpg=PA14&dq=symmetric+key+exchange+VPN&source=bl&ots=EoLAeopesq&sig=4yTt_EByZkaVLqawOR6CdfXNo04&hl=en&sa=X&ei=w6R-UqPuKMrMsQTz4oDIDA&ved=0CH4Q6AEwBw#v=onepage&q=symmetric%20key%20exchange%20VPN&f=false>

**Question 2 (10 Points)** Explain in detail how the following factors affect a network security policy:

(a) Security Association

“An IPsec **security association** (SA) specifies security properties that are recognized by communicating hosts. A single SA protects data in one direction. The protection is either to a single host or to a group (multicast) address. Because most communication is either peer-to-peer or client-server, two SAs must be present to secure traffic in both directions.

The following three elements uniquely identify an IPsec SA: the security protocol (AH or ESP), the destination IP address, the [security parameter index (SPI)](http://docs.oracle.com/cd/E26502_01/html/E28990/netsecgloss-1.html#glossary-94). The SPI, an arbitrary 32-bit value, is transmitted with an AH or ESP packet. ..An integrity checksum value is used to authenticate a packet. If the authentication fails, the packet is dropped.” http://docs.oracle.com/cd/E26502\_01/html/E28990/ipsecov-5.html

(b) Transforms

“An IPSec *transform* specifies a single IPSec security protocol (either AH or ESP [or both according to http://www.cisco.com/en/US/tech/tk583/tk372/technologies\_tech\_note09186a0080094203.shtml#transform]) with its corresponding security algorithms and mode...

A *transform set* is a combination of individual IPSec transforms designed to enact a specific security policy for traffic. Transform sets combine the following IPSec factors: Mechanism for payload authentication—AH transform, Mechanism for payload encryption—ESP transform, [and] IPSec mode (transport versus tunnel)

Transform sets equal a combination of an AH transform, plus an ESP transform, plus the IPSec mode (either tunnel or transport mode).” http://www.ciscopress.com/articles/article.asp?p=25477&seqNum=3

(c) Authentication Header

“AH is used to authenticate … IP traffic, and this serves the treble purpose of **ensuring that we're really talking to who we think we are, detecting alteration of data while in transit, and (optionally) to guard against replay by attackers who capture data from the wire and attempt to re-inject that data back onto the wire at a later date.**

*Authentication* is performed by computing a cryptographic hash-based message authentication code over nearly all the fields of the IP packet (excluding those which might be modified in transit, such as TTL or the header checksum), and stores this in a newly-added AH header and sent to the other end.” http://www.unixwiz.net/techtips/iguide-ipsec.html

(d) Encapsulation Security Payload

“The encapsulation *surrounds* the payload rather than *precedes* it as with AH: ESP includes header and trailer fields to support the encryption and optional authentication. It also **provides Tunnel and Transport modes**... The IPsec RFCs don't insist upon any particular encryption algorithms, but we find DES, triple-DES, AES, and [Blowfish](http://www.schneier.com/paper-blowfish-fse.html) in common use **to shield the payload from prying eyes.** The algorithm used for a particular connection is specified by the Security Association... and this SA includes not only the algorithm, but the key used. Unlike AH, which provides a small header *before* the payload, ESP *surrounds* the payload it's protecting... In addition to encryption, ESP can also optionally provide authentication, with the same HMAC as found in AH. Unlike AH, however, this authentication is *only for the ESP header and encrypted payload*: it does not cover the full IP packet. Surprisingly, this does not substantially weaken the security of the authentication, but it does provide some important benefits.

When an outsider examines an IP packet containing ESP data, **it's essentially impossible to make any real guesses about what's inside save for the usual data found in the IP header (particularly the source and destination IP addresses). The attacker will certainly know that it's ESP data — that's also in the header — but the type of the payload is *encrypted with the payload*.**

**Even the presence or absence of Authentication Data can't be determined by looking at the packet itself (this determination is made by using the Security Parameters Index to reference the preshared set of parameters and algorithms for this connection)**... As with AH, Transport Mode encapsulates just the datagram's payload and is designed strictly for host-to-host communications. The original IP header is left in place (except for the shuffled Protocol field), and it means that — among other things — the source and destination IP addresses are unchanged.” http://www.unixwiz.net/techtips/iguide-ipsec.html

**Question 3 (10 Points)** To improve performance, browsers store web pages in a local cache on the client’s machine. Describe in detail how a hostile Java applet can exploit this information to gain more privileges than it is entitled to.

“Even if the firewall removes the <applet> tag, the JavaScript that executes when downloaded can write the <applet> tag on the downloaded Web page. The will cause the Java applet class files to execute from the user's local cache.” This “illustrates how users of the Internet Explorer (IE) can be tricked into executing any program on their machines at the behest of a remote server... The bug described here allows a Web page master to embed “short-cuts” from a Web page to a program anywhere on a user's host machine. The shortcut is a method for executing a program on a Win32 machine from the desktop. The security problem is that a computer user might hit a link on someone else's Web page (residing on a remote server), that actually causes the execution of a program that resides on the user's local machine... By combining shortcut links with client-side executable scripts such as VBScript or JavaScript, malicious commands or programs can be downloaded into the IE cache as a batch file and then executed in sequence.” http://books.google.com/books?id=y4hvPdS8HOsC&pg=SL11-PA10&lpg=SL11-PA10&dq=Even+if+the+firewall+removes+the+%3Capplet%3E+tag,+the+JavaScript+that+executes+when+downloaded+can+write+the+%3Capplet%3E+tag+on+the+downloaded+Web+page.&source=bl&ots=6owfnVn61s&sig=aWdmv1DKsgYayRqypz3vs6YjrMM&hl=en&sa=X&ei=bTaOUvqXLMHWkQfT0YHYAw&ved=0CC4Q6AEwAA#v=onepage&q=Even%20if%20the%20firewall%20removes%20the%20%3Capplet%3E%20tag%2C%20the%20JavaScript%20that%20executes%20when%20downloaded%20can%20write%20the%20%3Capplet%3E%20tag%20on%20the%20downloaded%20Web%20page.&f=false

Specific to Netscape, the applet could obtain the IP number behind the firewall.

In IE, the applet could perform a port scan and then “reports information back with URL lookup covert channel” [explained in detail below]

http://books.google.com/books?id=y4hvPdS8HOsC&pg=SL11-PA10&lpg=SL11-PA10&dq=hostile+java+applets+cache&source=bl&ots=6owenTq43r&sig=c32P2IJTMfUA6XR5HJA1G0Z-J7c&hl=en&sa=X&ei=ELF-UtzMMYnIsATn5YDQCQ&ved=0CF8Q6AEwCDgK#v=onepage&q=cache&f=false

“The Java Security Manager usually disallows port-scanning behavior, but the crackers use the well-known trick of sticking some Java code (in this case, a port scanner) in the browser's cache and later executing it through a file: URL (using frames in the usual way). This attack works because Microsoft's cache layout is transparent.This is an interesting variation on the Slash and Burn attack ... The attackers cheat a bit for demonstration purposes by having the patsy clear his or her cache, but even without this exercise, guessing the cache location (one of four possibilities) would not be all that much of a challenge... Microsoft apparently places HTML and class files in the same directory stored with their original names (remember, a Java class will only run if it is correctly named). Although MSIE can't browse cache files directly, HTML pages can reference cache files by explicit name. Thus, the file: URL, if properly constructed, can invoke the Java class.The applet stuffed in your cache is a port scanner. The port-scanning attack works because an applet is allowed to open a socket connection back to where it came from. And guess where it came from: Yep, the client machine.So a port scan is carried out by their cache-bomb applet. Unlike the Steal This IP Address problem, port scanning is very serious. Using this attack, a cracker might be able to discover things like weak sendmails listening on port 25, leaving only the problem of getting the port-scan information back to the cracker site. Accomplished crackers can simply use the URL-lookup covert channel to do this. Unfortunately, this approach is only one of many ways of sending interesting tidbits out from an applet.”[http://www.securingjava.com/chapter-five/chapter-five-13.html]

**Question 4 (10 Points)** Explain how sandboxing applies to Java security in Java 2.

“When combined with access control, code signing allows applets to step outside the security sandbox gradually. In fact, the entire meaning of sandbox becomes a bit vague. As an example of how Java code signing might work, an applet designed for use in an Intranet setting could be allowed to read and write to a particular company database as long as it was signed by the system administrator. Such a relaxation of the security model is important for developers who have complained about Java's restrictive sandbox. Writing code that works within the tight restrictions of the sandbox is a pain, and the original sandbox is very restrictive.”

http://www.securingjava.com/chapter-three/

“**The byte code verifier**: The Byte Code Verifier is the first prong of the Java security model. When a Java source program is compiled, it compiles down to platform-independent Java byte code. Java byte code is "verified" before it can run. This verification scheme is meant to ensure that the byte code, which may or may not have been created by a Java compiler, plays by the rules... On a less basic level, a built-in theorem prover is applied to each code fragment. The theorem prover helps to make sure that byte code does not forge pointers, violate access restrictions, or access objects using incorrect type information. The verification process, in concert with the security features built into the language through the compiler, helps to establish a base set of security guarantees.

**The applet class loader**: The second prong of security defense is the Java Applet Class Loader. All Java objects belong to classes. The Applet Class Loader determines when and how an applet can add classes to a running Java environment. Part of its job is to make sure that important parts of the Java run-time environment are not replaced by code that an applet tries to install. In general, a running Java environment can have many Class Loaders active, each defining its own "name space." Name spaces allow Java classes to be separated into distinct "kinds" according to where they originate. The Applet Class Loader, which is typically supplied by the browser vendor, loads all applets and the classes they reference. When an applet loads across the network, the Applet Class Loader receives the binary data and instantiates it as a new class.

**The security manager**: The third prong of the Java security model is the Java Security Manager. This part of the security model restricts the ways in which an applet can use visible interfaces. Thus the Security Manager implements a good portion of the entire security model. The Security Manager is a single module that can perform run-time checks on "dangerous" methods. Code in the Java library consults the Security Manager whenever a dangerous operation is about to be attempted. The Security Manager is given a chance to veto the operation by generating a Security Exception (the bane of Java developers everywhere). Decisions made by the Security Manager take into account which Class Loader loaded the requesting class. Built-in classes are given more privilege than classes that have been loaded over the net.

**Untrusted and banished to the sandbox** Together, the three parts of the Java security model make up the sandbox. The idea is to restrict what an applet can do and make sure it plays by the rules. The sandbox idea is appealing because it is meant to allow you to run *untrusted* code on your machine without worrying about it. That way you can surf the Web with impunity, running every Java applet you ever come across with no security problems. **Well, as long as the Java sandbox has no security holes.**”

http://www.javaworld.com/javaworld/jw-05-1997/jw-05-security.html?page=2

**Question 5 (10 points)** In lecture, a Java type confusion attack was described. Could a type confusion attack be launched in a Ruby (http://www.ruby-lang.org/en/) program? Why or why not? Explain in detail.

“Every variable in your Ruby code is (internally) a C type called

"VALUE", which is just a typedefed unsigned int pointer. This pointer

points to a larger structure (in C, RBasic and other structs based on

it, like RString), from which you can read the value's class and other

properties. (Technically, this works differently for Ruby Fixnums and

Symbols, whose values are magically encoded in the pointer value

itself.)

**So it's not possible** to have force this kind of behavior you describe

in Ruby. However... instance variables (which are

like private fields in Java) can be accessed and modified anyway with

a little magic, and private or protected methods can be with some

tricks called from the outside environment.”

<https://www.ruby-forum.com/topic/4407583>

“In Ruby, variables are type-less and dynamic...Every variable in Ruby belongs to a class built into the language (like the groups we've just talked about) - these classes are dynamically changed depending on what type of data is being stored inside the variable.”<http://www.dev-hq.net/ruby/3--variables-constants-user-input>

**Question 6 (10 Points)** In IPSEC, datagrams can be authenticated by an authentication header but also by an ESP header. Compare the two approaches. Explain in detail which one offers better protection.

“AH is used to authenticate — but not encrypt — IP traffic, and this serves the treble purpose of ensuring that we're really talking to who we think we are, detecting alteration of data while in transit, and (optionally) to guard against replay by attackers who capture data from the wire and attempt to re-inject that data back onto the wire at a later date.

*Authentication* is performed by computing a cryptographic hash-based message authentication code over nearly all the fields of the IP packet (excluding those which might be modified in transit, such as TTL or the header checksum), and stores this in a newly-added AH header and sent to the other end...AH carries an Integrity Check Value in the Authentication Data portion of the header, and it's typically (but not always) built on top of standard cryptographic hash algorithms such as MD5 or SHA-1. Rather than use a straight checksum, it uses a Hashed Message Authentication Code (HMAC) which incorporates a secret value while creating the ICV. Though an attacker can easily recompute a hash, without the secret value he won't be able to recreate the proper ICV... Adding encryption makes ESP a bit more complicated because the encapsulation *surrounds* the payload rather than *precedes* it as with AH: ESP includes header and trailer fields to support the encryption and optional authentication... Unlike AH, which provides a small header *before* the payload, ESP *surrounds* the payload it's protecting. The Security Parameters Index and Sequence Number serve the same purpose as in AH, but we find padding, the next header, and the optional Authentication Data at the end, in the ESP Trailer. In addition to encryption, ESP can also optionally provide authentication, with the same HMAC as found in AH. Unlike AH, however, this authentication is *only for the ESP header and encrypted payload*: it does not cover the full IP packet. **When an outsider examines an IP packet containing ESP data, it's essentially impossible to make any real guesses about what's inside save for the usual data found in the IP header (particularly the source and destination IP addresses). The attacker will certainly know that it's ESP data — that's also in the header — but the type of the payload is *encrypted with the payload*.Even the presence or absence of Authentication Data can't be determined by looking at the packet itself (this determination is made by using the Security Parameters Index to reference the preshared set of parameters and algorithms for this connection).**

However, it should be noted that sometimes *the envelope* provides hints that the *payload* does not. With more people sending VoIP inside ESP over the internet, the QoS taggings are in the outside header and is fairly obvious what traffic is VoIP signaling (IP precedence 3) and what is RTP traffic (IP precedence 5). It's not a sure thing, but it might be enough of a clue to matter in some circumstances... We know that ESP is the only way to provide encryption, but ESP and AH both can provide authentication: which one do we use? … The obvious solution of wrapping ESP inside of AH is technically possible, but in practice is not commonly used because of AH's limitations with respect to Network Address Translation. By using AH+ESP, this tunnel could never successfully traverse a NAT'ed device.

Instead, **ESP+Auth is used in Tunnel mode to fully encapsulate the traffic on its way across an untrusted network, protected by both encryption and authentication in the same thing. Traffic protected in this manner yields nearly no useful information to an interloper save for the fact that the two sites *are* connected by a VPN.** This information might help an attacker understand trust relationships, but *nothing* about the actual traffic itself is revealed. Even the type of encapsulated protocol — TCP, UDP, or ICMP — is hidden from outsiders. This packet-in-a-packet can actually be nested yet more levels: Host A and Host B can establish their own authenticated connection (via AH), and have this routed over the VPN. This would put an AH inner packet inside an enclosing ESP+Auth packet.”

http://www.unixwiz.net/techtips/iguide-ipsec.html

**Question 7 (10 Points)** Outline and describe in detail how Wi-Fi Protected Access version 2 (WPA2) works. Specifically address how TKIP and Michael work.

WPA2: “WPA2 uses the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol ([CCMP](http://en.wikipedia.org/wiki/CCMP)) protocol, based on the Advanced Encryption Standard (AES) algorithm for authentication and data encryption. TKIP greatly increases the difficulty of intercepting wireless traffic over WEP...

Both Personal and Enterprise modes are supported. In Personal mode, the pre-shared key is combined with the SSID to create the pairwise master key (PMK). The client and AP exchange messages using the PMK to create the pairwise transient key (PTK). In Enterprise mode, after successfully authenticating -- using one of the EAP methods -- the client and AP receive messages from the 801.1x server that both use to create the PMK. They then exchange messages to create the PTK. The PTK is then used to encrypt and decrypt messages. In both cases, Personal and Enterprise, a group temporal key (GTK) is created during the exchange between the client and AP. The GTK is used to decrypt broadcast and multi-cast messages. WPA2 also adds methods to speed the handoff as a client moves from AP to AP. The process of authenticating with an 802.1x server and generating keys takes enough time to cause a noticeable interruption of a voice over wireless call. WPA2 specifies ways in which a client can pre-authorize with neighboring APs. APs and clients can also retain keys so that a client returning to an AP can quickly resume communication.” [<http://searchnetworking.techtarget.com/tip/Wireless-security-protocols-How-WPA-and-WPA2-work>]

“**Improved data encryption:** this is done through the Temporal Key Integrity Protocol (TKIP), which includes a hashing algorithm that shuffles the keys. It also uses an integrity-checking feature to ensure that the keys have not been altered.[4] Even though “TKIP does use the RC4 stream cipher and all parties must share the same secret key,”[4] this key, called the Temporal Key (TK) must be 128 bits long, much longer than that used in WEP , which is only 40 bits long. Just like WEP , it uses an IV , but this is 48 bits long, double the size that is used in WEP. “Even if the TK is shared, all involved parties generate a different RC4 key stream.”[4] TKIP is also known as “per-packet keys,” which means that it “dynamically generates a new key for each packet created,” which prevents collisions. In fact, TKIP allows for “280 trillion possible keys that can be generated for a given data packet.”[5] … However, the most significant difference between WPA and WPA2 is WPA2’s use of the Advanced Encryption Standard (AES) instead of TKIP for data encryption. AES, as described in the 802.11i standard, is a block cipher, as opposed to RC4, used in WEP and WPA, which is a stream cipher. While a stream cipher only executes against one character at a time, a block cipher operates against an entire block of text all at once. A “substitution permutation network,” AES has a fixed block size of 128 bits[8] and three different key sizes, each used in the three different “rounds” or iterations of the algorithm. In the first iteration a 128-bit key is used to perform 9 rounds, in the second a 192-bit key performs 11 rounds, and in the third iteration a 256- bit key is used to perform 13 rounds. Because AES is a substitution cipher, “within each round bits are substituted and rearranged and then special multiplication is performed based on the new arrangement.”[5] The effectiveness of AES cannot be disputed – the time needed to break it by using a brute force attack with $1 million worth of microprocessors and a 128-bit key length is 2.20 x 1017 years. With a 192-bit key length, the time increases to 1036 years.[5] ” [<http://infotech.armstrong.edu/katz/katz/Frank_Katz_CSC2010.pdf>]

MICHAEL: “With WPA, a method known as *Michael* specifies a new algorithm that calculates an 8-byte message integrity check (MIC) using the calculation facilities available on existing wireless devices. The MIC is placed between the data portion of the IEEE 802.11 frame and the 4-byte ICV. The MIC field is encrypted together with the frame data and the ICV. Michael also provides replay protection. A new frame counter in the IEEE 802.11 frame is used to prevent replay attacks.”<http://documentation.netgear.com/wpn802/enu/202-10101-01/WPN802-09-17.html>

“Michael operates on higher-level frames passed down to the MAC. When a higher-level frame is queued for transmission, one of the first transmission steps is to compute the message integrity check (MIC) value. Micahel operates on the input shown in Figure 7-5 (a). In addition to the destination address (DA) and source address (SA), Michael adds four zero bytes before the unencrypted data. The last three bytes are reserved; the first is a priority field that is reserved for future standardization work. Michael operates on 32-bit blocks of data. Data is padded out with zeros so that it will be a multiple pf 32-bit blocks. Padding is used only for the computation of the MIC. It is not transmitted. Michael computes the MIC value by working on successive 32-bit blocks of data.

When complete, the MIC is added on to the tail of the data frame, and the data-plus-MIC is given to 802.11

http://books.google.com/books?id=9rHnRzzMHLIC&pg=PA157&lpg=PA157&dq=michael+integrity+check&source=bl&ots=3xzSL419Dr&sig=9N5c63YONGY3fx4GpjnGORXXugg&hl=en&sa=X&ei=nwKMUtqoHM3hsATHv4CICQ&ved=0CC4Q6AEwAA#v=onepage&q=michael%20integrity%20check&f=falsefor transmission. ”

**Question 8 (10 Points)** Provide a scenario where a system would most benefit from using a:

(a) Leased line – “win out in terms of security, as they are dedicated only to a specific customer’s traffic”, and expensive. “**Leased Lines are Symmetric** This can be useful if staff need to…access their work PC’s desktops from home, send large files, upload sizable files to your web sites, backup data using online services, host web sites on a server at your office, use VoIP telephony” [<http://www.webopedia.com/TERM/L/leased_line.html>, <http://www.chaffeecountyedc.com/EndUserFiles/33266.pdf>, <http://www.rcrwireless.com/mobile-backhaul/mpls-vs-vpn.html>, http://www.hso.co.uk/leased-lines/leased-line/what-is-a-leased-line-an-expert-explains/]

(b) Frame relay network

“Suppose you are working in a big company and your company has just expanded to two new locations. The main site is connected to two branch offices, named Branch 1 & Branch 2 and your boss wants these two branches can communicate with the main site. The most simple solution is to connect them directly (called a leased line). To connect to these two branches, the main site router, HeadQuarter, requires two serial interfaces which a router can provide. But what happens when the company expands to 10 branches, 50 branches? For each point-to-point line, HeadQuarter needs a separate physical serial interface (and maybe a separate CSU/DSU if it is not integrated into the WAN card). As you can imagine, it will need many routers with many interfaces and lots of rack space for the routers and CSU/DSUs. Maybe we should use another solution for this problem? Luckily, Frame Relay can do it!

By using Frame Relay we only need one serial interface at the HeadQuarter to connect to all branches. This is also true when we expand to 10 or 50 branches. Moreover, the cost is much lesser than using leased-lines.” [http://www.9tut.com/frame-relay-tutorial]

(c) ISDN

“It took so long for ISDN to be standardized that it was never fully deployed in the telecommunications networks it was intended for.” [http://www.inetdaemon.com/tutorials/telecom/isdn/]

[When ISDN was first created]“ISDN offers the speed and quality that previously was only available to people who bought expensive, point-to-point digital leased lines. Combined with its flexibility as a dial-up service, ISDN has become the service of choice for many communications applications. Popular ISDN applications include:

Internet access

Telecommuting/remote access to corporate computing

Video conferencing

Small and home office data networking... By combining your two B-channels you have access to up to 128 kbps -- more than four times as fast as a 28.8 kbps modem on a standard phone line. And ISDN's digital technology assures you the cleanest connection to the Internet so you won't be slowed down by re-transmissions because of old analog technology.”

http://public.swbell.net/ISDN/overview.html#whyisdn

**There no longer may be a good reason to use ISDN** … “The imminent demise of [**ISDN**](http://en.wikipedia.org/wiki/Integrated_Services_Digital_Network) has been talked about for some time. There now appears to be a date attached which makes it semi-sort of official. As of May 18, 2013, Verizon will no longer accept orders for new ISDN lines. They will also not make any changes to existing lines and will start charging more for the service.”[http://www.engineeringradio.us/blog/2013/03/goodbye-isdn/]

(d) VPN

“Usually, VPN users fall into a few separate categories:

**The student/worker**. This person has responsibilities to attend to, and uses a VPN provided by their school or company to access resources on their network when they're at home or traveling. In most cases, this person already has a free VPN service provided to them, so they're not exactly shopping around. Also, if they're worried about security, they can always fire up their VPN when using airport or cafe WI-Fi to ensure no one's snooping on their connection. *Photo by* [*Ed Yourdon*](http://www.flickr.com/photos/yourdon/2715599454/).P

**The downloader**. Whether they're downloading legally or illegally, this person doesn't want on some company's witch-hunt list just because they have a torrenting app installed on their computer. VPNs are the only way to stay safe when using something like BitTorrent—[everything else is just a false sense of security](http://lifehacker.com/5936938/how-do-i-torrent-safely-now-that-demonoid-is-down). Better safe than trying to defend yourself in court or paying a massive fine for something you may or may not have even done, right? **The privacy minded and security advocate**. Whether they're a in a strictly monitored environment or a completely free and open one, this person uses VPN services to keep their communications secure and encrypted and away from prying eyes whether they're at home or abroad. To them, unsecured connections mean someone's reading what you say.**The globetrotter**. This person wants to [watch the Olympics live as they happen](http://lifehacker.com/5930437/how-an-american-can-stream-the-bbcs-official-olympics-coverage-and-overcome-nbcfail), without dealing with their crummy local networks. They want to check out their favorite TV shows as they air instead of waiting for translations or re-broadcasts (or watch the versions aired in other countries,) listen to location-restricted streaming internet radio, or want to use a new web service or application that looks great but for some reason is limited to a specific country or region.” [http://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs]

**Question 9 (10 Points)**

(a). In lecture, it was stated that symmetric key cryptography was used for IPSEC because it is more efficient. Why is efficiency prioritized over security?

In Ipsec it is only prioritized over security after a secure connection has been made. “there is a catch to using asymmetric encryption. It runs about 1,000 times slower than symmetric encryption and eats up just as much processing power, straining already overburdened servers. That means asymmetric encryption is only used (by IPsec and SSL) to create an initial and secure encrypted connection to exchange a private key. Then, that key is used to create a shared secret, or session key, that is only good during the session when the two hosts are connected.”[http://searchsecurity.techtarget.com/answer/How-IPsec-and-SSL-TLS-use-symmetric-and-asymmetric-encryption]

(b). Explain in detail when you would use IPSEC Transport Mode vs. Tunneling Mode.

“Transport Mode provides a secure connection between two endpoints as it encapsulates IP's payload, while Tunnel Mode encapsulates the *entire* IP packet to provide a virtual "secure hop" between two gateways. The latter is used to form a traditional VPN, where the tunnel generally creates a secure tunnel across an untrusted Internet... *Transport Mode*, which is used to protect an end-to-end conversation between two hosts. This protection is either authentication or encryption (or both), but it is not a tunneling protocol. It has nothing to do with a traditional VPN: it's simply a secured IP connection...Tunnel Mode forms the more familiar VPN functionality, where entire IP packets are encapsulated inside another and delivered to the destination... Most implementations treat the Tunnel-mode endpoint as a virtual network interface — just like an Ethernet interface or localhost — and the traffic entering or leaving it is subject to all the ordinary routing decisions.

The reconstituted packet could be delivered to the local machine or routed elsewhere (according to the destination IP address found in the encapsulated packet), though in any case is no longer subject to the protections of IPsec. At this point, it's just a regular IP datagram.

**Though Transport mode is used strictly to secure an end-to-end connection between two computers, Tunnel mode is more typically used between gateways (routers, firewalls, or standalone VPN devices) to provide a Virtual Private Network (VPN).**”

http://www.unixwiz.net/techtips/iguide-ipsec.html

**Question 10 (10 Points)** Explain in detail how IPSEC protection provides:

(**Not looking for the definition of each term, but specifically how IPSEC provides each type of protection**)

(a) data origin authentication – AH and ESP are used. (1)

AH: “Authentication is performed by computing a cryptographic hash-based message authentication code over nearly all the fields of the IP packet (excluding those which might be modified in transit, such as TTL or the header checksum), and stores this in a newly-added AH header and sent to the other end...AH carries an Integrity Check Value in the Authentication Data portion of the header, and it's typically (but not always) built on top of standard cryptographic hash algorithms such as MD5 or SHA-1.” (2)

ESP: “ESP can also optionally provide authentication, with the same HMAC as found in AH. Unlike AH, however, this authentication is only for the ESP header and encrypted payload: it does not cover the full IP packet. Surprisingly, this does not substantially weaken the security of the authentication, but it does provide some important benefits.

When an outsider examines an IP packet containing ESP data, it's essentially impossible to make any real guesses about what's inside save for the usual data found in the IP header (particularly the source and destination IP addresses). The attacker will certainly know that it's ESP data — that's also in the header — but the type of the payload is encrypted with the payload.”(2)

(b) connectionless data integrity authentication: AH and ESP use the Hashed Message Authentication Code (1)“This service is provided by using algorithms like HMAC-MD5 or HMACSHA1.”

http://www.isoc.org/seinit/portal/index2.php?option=com\_content&do\_pdf=1&id=45

“The definition of HMAC requires a cryptographic hash function, which we denote by H, and a secret key K. We assume H to be a cryptographic hash function where data is hashed by iterating a basic compression function on blocks of data.We denote by B the byte-length of such blocks (B=64 for all the above mentioned examples of hash functions), and by L the byte-length of hash outputs (L=16 for MD5, L=20 for SHA-1). The authentication key K can be of any length up to B, the block length of the hash function. Applications that use keys longer than B bytes will first hash the key using H and then use the resultant L byte string as the actual key to HMAC. In any case the minimal recommended length for K is L bytes (as the hash output length)...

We define two fixed and different strings ipad and opad as follows

(the 'i' and 'o' are mnemonics for inner and outer):

ipad = the byte 0x36 repeated B times

opad = the byte 0x5C repeated B times.

To compute HMAC over the data `text' we perform H(K XOR opad, H(K XOR ipad, text))” http://tools.ietf.org/html/rfc2104

(c) data content confidentiality

ESP uses AES CBC mode, DES or Triple-DES (1) , <http://www.isoc.org/seinit/portal/index2.php?option=com_content&do_pdf=1&id=45>

AES CBC: “The AES algorithm is a symmetric block cipher that can encrypt and decrypt information in data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Longer key lengths provide better security at the cost of CPU performance due to the more intensive computational requirements. Cipher block chaining (CBC) is used to hide patterns of identical blocks of data within a packet. An initialization vector (an initial random number) is used as the first random block to encrypt and decrypt a block of data. Different random blocks are used in conjunction with the secret key to encrypt each successive block. This ensures that identical sets of unsecured data (plaintext) result in unique, encrypted data blocks.” <http://technet.microsoft.com/en-us/library/dd125356(v=ws.10).aspx>

DES: “There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the [key](http://searchsecurity.techtarget.com/definition/key) is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same [private key](http://searchsecurity.techtarget.com/definition/private-key).

DES applies a 56-bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds or operations.<http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard>

3DES: “Triple DES uses a "key bundle" which comprises three DES [keys](http://en.wikipedia.org/wiki/Key_(cryptography)), K1, K2 and K3, each of 56 bits (excluding [parity bits](http://en.wikipedia.org/wiki/Parity_bit)). The encryption algorithm is:

ciphertext = EK3(DK2(EK1(plaintext)))

I.e., DES encrypt with K1, DES *decrypt* with K2, then DES encrypt with K3.” http://en.wikipedia.org/wiki/Triple\_DES

(d) anti-replay protection

AH and ESP are used (1) “The anti-replay mechanism works by keeping track of the sequence numbers in packets as they arrive. Whether the mechanism is used at the receiving end depends upon a security level setting set by the receiver. When a security association has been established between a sender and a receiver, their counters are initialized at zero. The first packet sent will have a sequence number of 1, the second 2, and so on. Each time a packet is sent, the receiver verifies that the number is not that of a previously sent packet. When detection of a replayed packet occurs, the program sends an error message, discards the replayed packet, and logs the event - including in the log entry identifiers such as the date/time received, source address, destination address, and the sequence number.

”http://searchnetworking.techtarget.com/definition/anti-replay-protocol

(e) limited traffic flow confidentiality

ESP is used (1) “Traffic flow confidentiality prevents traffic analysis, ensuring that eavesdroppers cannot discover information such as the volume, frequency, or packet sizes of traffic sent between any given source and destination. Traffic flow confidentiality is available only in tunnel mode.” http://www.informit.com/library/content.aspx?b=Troubleshooting\_VPNs&seqNum=67

1. [**http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&cad=rja&ved=0CFsQFjAG&url=http%3A%2F%2Fsce.uhcl.edu%2Fyang%2Fteaching%2Fcsci5931webSecuritySpr04%2FIpSec.ppt&ei=KgaMUtaZBq22sATKyIDICQ&usg=AFQjCNFaYiHD0VeVsW5oRA6ghR5KPp9nxA&sig2=Pc-48K2rjo-sRCNS3RZXSg&bvm=bv.56643336,d.cWc**](http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&cad=rja&ved=0CFsQFjAG&url=http%3A%2F%2Fsce.uhcl.edu%2Fyang%2Fteaching%2Fcsci5931webSecuritySpr04%2FIpSec.ppt&ei=KgaMUtaZBq22sATKyIDICQ&usg=AFQjCNFaYiHD0VeVsW5oRA6ghR5KPp9nxA&sig2=Pc-48K2rjo-sRCNS3RZXSg&bvm=bv.56643336,d.cWc)

2. **http://www.unixwiz.net/techtips/iguide-ipsec.html**

**Question 11 (20 points)** Consider the CGI attack example in the lecture slides. Either write your own CGI attack script OR find a script written by someone else excluding any presented in class. Include the complete script in your answer and describe in detail what the attack script does.

“#!/usr/bin/perl

# Simple CGI script to let web users run an nmap scan from their web browser

$server = $ENV{'QUERY\_STRING'}; # using a GET request

@scan = `nmap $server`;

foreach $line (@scan) { print "$line"; }

Clearly, the 4th line - @scan = `nmap $server`; is the line of insecure code. Since $server is controlled

by our GET request, we can obviously make the server do whatever we want. If you know a bit about UNIX,

you'll know that you can execute multiple commands on a single line by separating them with a semicolon (;).As such, the string to pass to the script would be something like: www.yahoo.com;ls... Before we can actually

pass this string to the script, however, we must encode it to its hex equivalent.[www.yahoo.com](http://www.yahoo.com/);ls is GET w%77w.ya%68%6Fo.com%3B%6Cs HTTP/1.0As such, to execute our command of "ls" on our target, we could point our web browser to <http://the-server.com/cgi-bin/nmap.cgi?w%77w.ya%68%6Fo.com%3B%6Cs> and we would receive the output of the ls command

http://www.ouah.org/cgi-exploitation.txt

**Question 12 (20 points)** Explain in detail the differences between Layer 2 tunneling and Layer 3 tunneling. Provide an example of each. Include a diagram to show how each datagram/packet would be constructed for each example.

“L2TP uses packet-switched network connections to make it possible for the endpoints to be located on different machines. The user has an L2 connection to an access concentrator, which then tunnels individual PPP frames to the NAS, so that the packets can be processed separately from the location of the circuit termination. This means that the connection can terminate at a local circuit concentrator, eliminating possible long-distance charges, among other benefits. From the user's point of view, there is no difference in the operation.” <http://searchenterprisewan.techtarget.com/definition/Layer-Two-Tunneling-Protocol>

“ The following diagram depicts a typical L2TP scenario. The goal is to

tunnel PPP frames between the Remote System or LAC Client and an LNS

located at a Home LAN.

[Home LAN]

[LAC Client]----------+ |

\_\_\_\_|\_\_\_\_\_  +--[Host]

| | |

[LAC]---------| Internet |-----[LNS]-----+

| |\_\_\_\_\_\_\_\_\_\_| |

\_\_\_\_\_|\_\_\_\_\_ :

| |

| PSTN |

[Remote]--| Cloud |

[System] | | [Home LAN]

|\_\_\_\_\_\_\_\_\_\_\_| |

| \_\_\_\_\_\_\_\_\_\_\_\_\_\_ +---[Host]

| | | |

[LAC]-------| Frame Relay |---[LNS]-----+

| or ATM Cloud | |...

L2TP utilizes two types of messages, control messages and data

messages. Control messages are used in the establishment, maintenance

and clearing of tunnels and calls. Data messages are used to

encapsulate PPP frames being carried over the tunnel. Control

messages utilize a reliable Control Channel within L2TP to guarantee

delivery (see section 5.1 for details). Data messages are not

retransmitted when packet loss occurs.<http://www.ietf.org/rfc/rfc2661.txt>

“L2TP packet structure[[edit](http://en.wikipedia.org/w/index.php?title=Layer_2_Tunneling_Protocol&action=edit&section=4)]

An L2TP packet consists of  :

http://en.wikipedia.org/wiki/Layer\_2\_Tunneling\_Protocol#L2TP\_packet\_structure

“***Layer 3*** tunneling technologies generally assume that all of the configuration issues have been handled out of band, often by manual processes. For these protocols, there may be no tunnel maintenance phase. For ***Layer 2*** protocols (**PPTP** and **L2TP**), however, a tunnel must be created, maintained, and then terminated. Once the tunnel is established, tunneled data can be sent.

The **tunnel client** or **server** uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the **tunnel client** sends a payload to the **tunnel server**, the **tunnel client** first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the **tunnel server**. The **tunnel server** accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the **tunnel client** behaves similarly.” (1)

Comparison:

“***User Authentication***.   
***Layer 2*** tunneling protocols inherit the user authentication schemes of PPP.   
Many ***Layer 3*** tunneling schemes assume that the endpoints were well known (and authenticated) before the tunnel was established.   
An exception to this is IPSec **ISAKMP** negotiation, which provides **mutual** authentication of the tunnel endpoints.   
(Note that most IPSec implementations support **machine-based** certificates only, rather than user certificates. As a result, any user with access to one of the endpoint machines can use the tunnel. This potential security weakness can be eliminated when IPSec is paired with a ***Layer 2*** protocol such as L2TP.)

***Token card support.***   
Using the Extensible Authentication Protocol (**EAP**), ***Layer 2*** tunneling protocols can support a wide variety of authentication methods, including one-time passwords, cryptographic calculators, and smart cards.   
***Layer 3*** tunneling protocols can use similar methods; IPSec defines public key certificate authentication in its **ISAKMP/Oakley** negotiation.

***Dynamic address assignment.***   
***Layer 2*** tunneling supports dynamic assignment of client addresses based on the Network Control Protocol (**NCP**) negotiation mechanism.   
Generally, ***Layer 3*** tunneling schemes assume that an address has already been assigned prior to initiation of the tunnel.

***Data Compression.***   
***Layer 2*** tunneling protocols support PPP-based compression schemes.

***Data Encryption.***   
***Layer 2*** tunneling protocols support PPP-based data encryption mechanisms.   
***Layer 3*** tunneling protocols can use similar methods; IPSec defines several optional data encryption methods which are negotiated during the **ISAKMP/Oakley** exchange.

***Key Management.***   
A ***Layer 2*** protocol, relies on the initial key generated during user authentication, and then refreshes it periodically.   
IPSec, explicitly negotiates a common key during the **ISAKMP** exchange, and also refreshes it periodically.

***Multi-protocol support.***   
***Layer 2*** tunneling supports multiple payload protocols, which makes it easy for tunneling clients to access their corporate networks using IP, IPX, NetBEUI, and so forth.   
In contrast, ***Layer 3*** tunneling protocols, such as IPSec tunnel mode, typically support only target networks that use the IP protocol.”

(1) http://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio1999ttv/Figueras-Parc/Files/Protocols.html

**Question 13 (20 points)**

(a). Explain in detail how Bump-in-the-Stack (BITS) network level integration works.

“ Here IPsec is implemented "underneath" an existing implementation of an IP

protocol stack, between the native IP and the local network drivers. Source code access for the IP stack is not required in this context, making this implementation approach appropriate for use with legacy systems. This approach, when it is adopted, is usually employed in hosts.” <http://www.isoc.org/seinit/portal/index2.php?option=com_content&do_pdf=1&id=45>

“IPv6 and IPv4 networks, BIS is a translation interface between IPv4 applications and the underlying IPv6 network (i.e. the network interface driver). The host stack design is based on that of a dual-stack host, with the addition of three modules, a translator, an extension name resolver, and an address mapper... The translator rewrites outgoing IPv4 headers into IPv6 headers and incoming IPv6 headers into IPv4 headers (if applicable). It uses the header translation algorithm defined in SIIT. The extension name resolver acts as the DNS-ALG in the NAT-PT mechanism. It snoops IPv4 DNS queries and creates another query asking to resolve both ‘A’ (IPv4) and ‘AAAA’ (IPv6) records, sending the returned ‘A’ record back to the requesting IPv4 application. If only ‘AAAA’ records are returned, the resolver requests the address mapper to assign an IPv4 address corresponding to the IPv6 address. The address mapper maintains a pool of IPv4 addresses and the associations between IPv4 and IPv6 addresses. It will also assign an address when the translator receives an IPv6 packet from the network for which there is no mapping entry for the source address. Because the IPv4 addresses are never actually transmitted on the network, they do not have to be globally unique and a private address pool can be used. ”http://www.6net.org/book/deployment-guide.pdf

(b). Explain in detail what kind of complications occur from BITS duplicated functionality.

“The major issue in this implementation is duplication of effort. It requires implementing most of the features of the network layer, such as fragmentation and route tables. Duplicating functionality leads to undesired complications. It becomes more difficult to handle issues such as fragmentation, PMTU, and routing.” http://technet.microsoft.com/en-us/library/cc700826.aspx

(c) Explain in detail why it is easier for firewall vendors to integrate with BITS than with OS-level networking. “The advantage of this technique is that IPSec can be “retrofitted” to any IP device, since the IPSec functionality is separate from IP. “ http://www.tcpipguide.com/free/t\_IPSecArchitecturesandImplementationMethods-2.htm

“For companies providing solutions for VPNs and intranets, OS integrated solution has one serious drawback. On the end hosts, they have to work with the features provided by the OS vendors. This may limit their capabilities to provide advanced solutions....An advantage of BITS implementation is the capability of an implementation to provide a complete solution. Vendors providing integrated solutions such as firewalls, prefer to have their own client as the OS vendor and may not have all the features required to provide a complete solution.”

http://technet.microsoft.com/en-us/library/cc700826.aspx

**Question 14 (20 points)**

(a) Describe in detail how you defend against a bandwidth denial of service in a wired computer network attack.

“When Ethernet LANs were built using hubs instead of switches, a faulty station or broadcast storm could bring down an entire LAN. Even switched LANs can be susceptible to broadcast storms if the spanning tree protocol is not configured correctly. A DoS attack against a wired LAN must be initiated from within the facility because the intruder must physically connect to the network. However, these DoS attacks against wired LANs are rare and preventable. ” <http://www.arubanetworks.com/pdf/technology/whitepapers/wp_Burton_End_of_Ethernet.pdf>

“Most switches have some rate-limiting and [ACL](http://en.wikipedia.org/wiki/Access_control_list) capability. Some switches provide automatic and/or system-wide [rate limiting](http://en.wikipedia.org/wiki/Rate_limiting), [traffic shaping](http://en.wikipedia.org/wiki/Traffic_shaping), [delayed binding](http://en.wikipedia.org/wiki/Delayed_binding) ([TCP splicing](http://en.wikipedia.org/wiki/TCP_splicing)), [deep packet inspection](http://en.wikipedia.org/wiki/Deep_packet_inspection) and [Bogon filtering](http://en.wikipedia.org/wiki/Bogon_filtering) (bogus IP filtering) to detect and remediate denial of service attacks through automatic rate filtering and WAN Link failover and balancing” <http://en.wikipedia.org/wiki/Denial-of-service_attack>

“Victim-network mechanisms. Historically, most of the systems for combating DDoS attacks have been designed to work on the victim side, since this side suffered the greatest impact of the attack. The victim has the greatest incentive to deploy a DDoS defense system, and maybe sac- rifice some of its performance and resources for increased security... Intermediate-network mechanisms. DDoS de- fense mechanisms deployed at the intermediate network are more effective than a victim net- work mechanisms since the attack traffic can be handled easily and traced back to the attack- ers. Characteristic examples of these mecha- nisms are WATCHERS [99], traceback [65,73,68,69,74] and pushback [100]... Source network mechanisms. DDoS defense mechanisms deployed at the source network can stop attack flows before they enter the In- ternet core and before they aggregate with other attack flows.” <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.7118&rep=rep1&type=pdf>

“Hardware DoS protection solutions work by analyzing network traffic and signature-based detection of known attacks or by providing behavioral analysis of current traffic against profiles of “normal” behavior. Traffic that matches a known attack pattern or fails to resemble typical network traffic is either **automatically blocked by the device or flagged for investigation by a security analyst**. It is important to note that DoS protection appliances placed on a business’ own network are only able to protect network segments, devices and servers that are downstream from the protection appliance. ”(1)

(b) Describe in detail how you defend against a bandwidth denial of service in a wireless computer network attack. "The first category of defenses is based around a device on the customer premises. These appliances are purpose-built to deal with DoS attacks... So a new category of DoS mitigation devices has emerged to deal with these attacks. They tend to include both optimized IPS-like rules to prevent floods and other network anomalies, and simple web application firewall capabilities which we will discuss in the next post. Additionally, we see a number of anti-DoS features such as session scalability, combined with embedded IP reputation capabilities, to discard traffic from known bots without full inspection... These devices should be as close to the perimeter as possible, to get rid of the maximum amount of traffic before the attack impacts anything else. Some devices can be deployed out-of-band as well, to monitor network traffic and pinpoint attacks. Obviously monitor-and-alert mode is less useful than blocking, which helps maintain availability in real time...The first service option most organizations consider is a Content Delivery Network (CDN). These services enhance web site performance by strategically caching content. Depending on the nature of your site, a CDN might be able to dramatically reduce your ingress network traffic – if they can cache much of your static content. They also offer some security capabilities, especially for dealing with DoS attacks. The CDN acts as a proxy for your web site, so the provider can protect your site by using its own massive bandwidth to cope with DoS attacks for you. They have significant global networks, so even a fairly large volumetric attack shouldn’t look much different than a busy customer day.. Their scale enables them to cope with much larger traffic onslaughts than your much smaller pipes. Another advantage of a CDN is its ability to obscure the real IP addresses of your site, making it more difficult for attackers to target your servers. CDNs can also handle SSL termination if you allow them to store your private keys."

https://securosis.com/blog/defending-against-dos-attacks-defense-part-1-the-network

“Defending against bandwidth DoS attacks is often difficult for the target site, because the

congestion usually occurs upstream (farther in the network) from any equipment that the site

controls (e.g., a router or firewall). For an effective response, a target site typically needs to

coordinate a response with its parent ISP. If the attack traffic is easy to characterize or otherwise

“stands out”, such as a UDP packet flood against a web site, blocking at an appropriate upstream

location by the ISP is relatively straightforward. When the attack traffic is not easy to characterize,

or the necessary router resources or features are not available for filtering, ISPs resort to

blackholing. In that case, a routing entry for the target's network prefix (which may include other,

otherwise un-targeted sites) is injected into the ISP's routing protocol. That entry points effectively

causes all traffic to the target, both legitimate and attack, to be dropped by the ISP routers. In this

way, the attack traffic is dropped as soon as it enters the ISP's network, thereby avoiding link

congestion. Since legitimate traffic to the target site is also dropped, blackholing does not help

restore access to said site...Modern routers and firewalls offer some defenses against bandwidth DoS attacks, such as

terminating TCP handshakes to mitigate against SYN flood attacks and applying statistical means to

detecting network traffic anomalies. The effectiveness of such schemes varies against the different

types of attack traffic, as does their impact on router performance. Many of these features are

available on customer-premises equipment (as opposed to ISP-grade equipment), reducing their

relevance in defending against attacks that cause congestion in upstream links.”

<http://www.cs.columbia.edu/~angelos/Papers/2010/ddos.pdf>

“The most effective way to protect against the impact of DoS attacks is to stop them before they even reach a company’s network. That means partnering with the contracted ISP to block the attack at the gateway... If a clean-pipes service isn’t available from the ISP, several cloud providers offer subscription services that scrub traffic before it enters the network. These services function by **serving as an intermediary, receiving traffic bound for the network, filtering it, and passing on only legitimate connections**. Cloud-based DoS protection services are available from providers such as Imperva and VeriSign... Most notably, if a DoS attack is able to completely use up all of an organization’s Internet bandwidth, the attack will be successful, because legitimate traffic will not even be able to reach the protection appliance. For this reason, organizations should use a combination of border filtering and a clean-pipes service to present a layered defense. Organizations relying solely upon local filtering must significantly overprovision network bandwidth to ensure that the network is capable of withstanding a sustained DoS attack. Absorption, the final DoS protection strategy, attempts to prevent an attacker from using all accessible resources by making available more resources than the attacker is able to consume. This involves purchasing sufficient network bandwidth and server and device capacity to absorb significant levels of traffic over and above the typical traffic profile.”

(1)http://www.biztechmagazine.com/article/2013/02/three-elements-defense-against-denial-service-attacks

**Question 15 (20 points)** Compose an appropriate /etc/hosts.allow file for ENS machine tux184. List each entry below. Describe in detail the rules, their impact and their rationale for implementation.

Ssh : 131.204.14. : spawn /bin/echo `/bin/date` access permitted to %h>>/var/log/sshd.log \ : allow //auburn tux machines

ssh : localhost : spawn /bin/echo `/bin/date` access permitted to %h>>/var/log/sshd.log \ : allow //local host

ssh : ALL : spawn /bin/echo `/bin/date` access denied to %h>>/var/log/sshd.log \

: deny // everyone else denied and reported to log

portmap : localhost : spawn /bin/echo `/bin/date` access permitted to %h>>/var/log/sshd.log \ : allow //localhost

portmap : 131.204.14 : spawn /bin/echo `/bin/date` access permitted to %h>>/var/log/sshd.log \ : allow //au network

portmap : ALL : spawn /bin/echo `/bin/date` access denied to %h>>/var/log/sshd.log \

: deny // everyone else denied and reported to log

in.telnetd : ALL \

: spawn /bin/echo `/bin/date` from %h>>/var/log/telnet.log \

: deny //no telnet (insecure, ssh is allowed above instead) //and report to log

\* Each entry uses “spawn /bin/echo `/bin/date` access denied/permitted to %h>>/var/log/sshd.log \” to keep a log

<http://www.cyberciti.biz/faq/block-ssh-attacks-with-denyhosts/>

https://access.redhat.com/site/documentation/en-US/Red\_Hat\_Enterprise\_Linux/3/html/Reference\_Guide/s1-tcpwrappers-access.html

<http://static.closedsrc.org/articles/dn-articles/hosts_allow.html>

<http://lists.freebsd.org/pipermail/freebsd-questions/2007-January/139712.html>