SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1, 2014

Workshop for Lecture 9: Network Security

QUESTION 1

TLS is a cryptographic services protocol based upon PKI and commonly used on the Internet.

(a) What port is reserved for HTTP over TLS? What is the prefix for a URL that describes a resource accessible by HTTP over TLS?

(b) TLS is designed to secure reliable end-to-end services over TCP. Briefly describe where the TLS operates in the OSI and TCP/IP protocol stacks.

(c) Briefly explain the purpose of the TLS Handshake protocol.

(d) Identify the security services provided to TLS connections by the TLS Record Protocol.

(e) How are the TLS Handshake Protocol and the TLS Record protocol connected?

(f) As part of the Handshake Protocol the client and server negotiate which 'cipher suite' to use. In what circumstances is this negotiation useful? Why can this negotiation lead to potential security weaknesses?

(a) Port 443 is reserved for HTTP over TLS. The prefix used for the URLs is HTTPS.
(b) TLS operates at the Transport Layer (OSI layer 4) The TLS Record Protocol sits above the TCP protocol.
(c) TLS Handshake Protocol: negotiates crypto parameters, establishes session key and authenticates server (and optionally authenticates the client).
(d) Security services provided are message confidentiality and message integrity
(e) The cryptographic algorithms negotiated, and the key exchanged, in the Handshake Protocol are used to protect the data transferred in the Record protocol.
(f) The cipher suite negotiation is useful when the end users support different cryptographic algorithms. A potential weakness is that an attacker may alter the protocol messages to try to make a connection employ a weaker authentication mechanism than the strongest one that both endpoints can support.

QUESTION 2

Internet Protocol security (IPSec) is a framework of open standards for Internet Protocol (IP) networks.

(a) Briefly describe three major benefits of using IPSec.

(b) Three security services that can be provided by IPSec are: message confidentiality, message integrity and traffic analysis protection. Briefly explain the mechanism used to provide each of these services.

(c) Briefly describe the three major VPN architectures supported by IPSec. Describe typical application scenarios for each of these architectures.

(a) Benefits mentioned in the lecture slides (slide 42) include:
• Is transparent to applications: Operates at layer 3 so applications are not aware

of its operation.
• Can be transparent to end users: System administrator configures IPSec; the end user is not involved.
• If applied at a firewall/router, strong security applies to all traffic crossing this boundary. Internal workstations need not be reconfigured.
(b) See slide 31
Message Confidentiality. Protect against unauthorised data disclosure. Accomplished by the use of encryption mechanisms.
Traffic Analysis Protection. A person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being ex- changed. Provided by concealing IP datagram details such as source and destination address.
Message Integrity. IPsec can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.
(c) Slides 36-41
Gateway-to-Gateway Architecture. Provides secure network communications between two networks. Establish a VPN connection between the two gateways. Network traffic is routed through the IPsec connection, protecting it appropriately. Only protects data between the two gateways. Most often used when connecting two secured networks, such as linking a branch office to headquarters over the Internet. Gateway-to-gateway VPNs often replace more costly private wide area network (WAN) circuits.
Host-to-Gateway Architecture. Commonly used to provide secure remote access. The organization deploys a VPN gateway onto its network; each remote access user then establishes a VPN connection between the local computer (host) and the VPN gateway. As with the gateway- to-gateway model, the VPN gateway may be a dedicated device or part of another network device.
Most often used when connecting hosts on unsecured networks to resources on secured net- works, such as linking travelling employees around the world to headquarters over the Internet.
Host-to-Host Architecture. Only model that provides protection for data through out its transit. Resource-intensive to implement and maintain in terms of user and host management. All user systems and servers that will participate in VPNs need to have VPN software installed and/or configured. Key establishment is often accomplished through a manual process.
Typically used for special purpose needs, such as system administrators performing remote management of a single server.

QUESTION 3
Suppose that you are responsible for designing a secure Internet banking application. You have been asked to consider basing security on one of three security mechanisms:

- HTTP Application Level Authentication
- TLS
- IPSec

Consider each of these protocols in turn to answer the following questions:
(a) Is HTTP Application Level Authentication a suitable choice? Explain your answer.
(b) Does TLS provide the required security services? What assumptions would you need to make about the client's computing environment?

(c) Does IPSec provide the required security services? What IPSec architecture would be suitable? Why is this choice not widely used in practice?

• Authentication at the HTTP Application Level is not suitable for Internet banking which requires a high level of security. It provides no confidentiality for the transmission of user data.
• TLS provides confidentiality and integrity of data which are the basic required security services. Non-repudiation is not provided since symmetric encryption is used for data integrity (rather than digital signatures). Server authentication is provided and although client authentication is possible it is often not available in practice since there is no global PKI. Therefore client authentication is often provided using a different mechanism such as a shared password.
TLS is in fact widely used to provide security for Internet banking. Probably the main threat comes from malicious software on user PCs. This is not a fault of the TLS protocol of course. Malicious software, such as trojan horses, can infect user PCs in many ways. If an operating system has such software installed then it can directly attack the implementation. For example, a 'keylogger' can record all input from the keyboard, which will include user login details, and send these to a pre-determined location.
• IPSec provides the essential services of confidentiality and data integrity, but like TLS does not provide non-repudiation. The additional service of traffic analysis protection is not likely to be particularly useful for Internet banking (unless you really care that an attacker knows when you are communicating with your bank).
While a host-to-gateway architecture could be used (with the client PC connecting to a bank gate- way) this would not be appropriate on its own since user transactions would then be in the clear in the bank network. Therefore a host-to-host architecture would be most appropriate.
While there are some potential problems with using IPSec in IP V4 networks and across firewalls, it seems that the main reason that IPSec is not widely used in this context is historical. Most Internet bank users have browsers with TLS (SSL) installed. IPSec is a newer protocol suite. Possibly IPSec may become more popular in Internet banking applications in the future.

QUESTION 4
A firewall is a component or set of components that restricts access between a protected network and other sets of networks, and is often used to protect an organization's networks from the Internet.
(a) Briefly describe the operational characteristics of:
- A simple packet filter;
- A stateful packet filter;
- An application proxy gateway.

(b) Briefly discuss the strengths and weaknesses of deploying:
- A packet filter;
- An application proxy gateway.

(a) Operational characteristics:
• A packet filter examines each packet that attempts to pass through the filter. Each packet is examined independently of other packets that may be part of the

same connection Packet filters examine each packet's headers and make decisions based on attributes such as:
– Source or destination IP addresses – Source or destination port numbers – Protocol (UDP, TCP or ICMP) – ICMP message type
– And which interface the packet arrived on
• Stateful packet filters take account of the current state of a connection. Stateful packet filters are more 'intelligent' than simple packet filters. Stateful packet filters are able to recognise if a particular packet is part of an established connection by 'remembering' recent traffic history. This makes the definition of filtering rules easier to accomplish and therefore potentially more secure.
• Application level gateway (ALG) acts as a relay of application level traffic and is also known as an application proxy because the firewall needs to act on behalf of the client. ALG are usually configured to support only specific applications or specific features of an application. Each application is supported by a specific gateway.
(b) Strengths and weaknesses: • Packet filter strengths:
– Low overhead and high throughput
– Supports almost any application • Packet filter weaknesses:
– Do not usually interpret application layer data/commands – may allow insecure operations to occur – Allows direct connection between hosts inside & outside firewall
2
– Non-stateful packet filters only: less secure and more difficult to write complex rules • Application proxy gateway strengths:
– Easy logging and audit of all incoming traffic
– Provides potential for best security through control of application layer data/commands • Application proxy gateway weaknesses:
– May require some time for vendor to write new gateways for new applications – Requires one more additional connection (including processing resources) for each new connection – Slower than packet filters

QUESTION 5
The type of firewall that is most appropriate for protecting a network depends on the organization itself and the size of the network. Some factors to consider are the cost, the ease of use and the level of security available if the product is used correctly. Use your web browser to find information on commercial firewall products, and see if you can find products that you think are suitable in the following cases:
(a) A home user with a single PC.
(b) A small organization such as a local accounting business with less than 10 employees.

(a) Home user with single PC could use software firewall on PC (free or cheap product, lots to choose from): • Firewall built in to O/S, such as Windows XP (free) • PCTools Firewall Plus (free) • Trend Micro PC cillin • McAfee Personal Firewall • Checkpoint Zone Alarm (about $50) • For free software downloads, make sure it is from a reputable site (check the certificate!)
(b) Small organisation - local accounting business - looks after financial information, so legal obligations to protect information. Need to protect network rather than individual PC, so business needs justify the expense of hardware firewall. cost can be from $hundreds to $thousands.
• Software: Checkpoint Zone Alarm Pro • Hardware: D-Link DFL-800 Net defender

(around $1000) Cisco Linksys router

QUESTION 6

Malicious software is one of the major threats to modern computer system security.

(a) Briefly describe the following types of malware:

a. Spyware
b. Botnets
c. Phishing
d. Rootkits

(b) What is the difference between Resident and Non-Resident viruses?

(c) The Melissa virus was one of the first macro viruses that became very wide spread at the time of its inception. Read the following historical description of this virus at the following link https://www.cert.org/historical/advisories/CA-1999-04.cfm. Briefly describe how this virus worked and why it was so successful in its aims.

(a) See slides 86, 88 and 89.

Spyware

Spyware is software that aids in gathering information about a person without their knowledge and send that information without the owner's consent, or knowledge. Spyware is mostly used for the purposes such as; tracking and storing users' movements on the web; serving up pop-up ads to internet users.

Botnets

Botnets are a network of infected machines. A botnet does the bidding of its master.

Some botnets might have a few hundred or a couple thousand computers, but others have tens and even hundreds of thousands of hosts at their disposal. Criminals use botnets to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud.

Phishing

Phishing is sending an email to a user falsely claiming to be legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. Phishing email may direct the user to visit a website where they are asked to update personal information, such as a password, or credit card.

Rootkits

A rootkit is a type of software designed to hide the fact that an operating system has been compromised. Rootkits allow viruses and malware to "hide in plain sight" by disguising as necessary files that your antivirus software will overlook.

(b) What is the difference between Resident and Non-Resident viruses?

In order to replicate itself, a virus must be permitted to execute code and write to memory. Nonresident viruses immediately search for other hosts that can be infected, infect those targets, and finally transfer control to the application program they infected. Resident viruses do not search for hosts when they are started. Instead, a resident virus loads itself into memory on execution and transfers control to the host program. The virus stays active in the background and infects new hosts when those files are accessed by other programs or the operating system itself.

(c) The Melissa macro virus propagates in the form of an email message containing an infected Word document as an attachment. Users who open an infected document in Word97 or Word2000 with macros enabled will infect the

Normal.dot template causing any documents referencing this template to be infected with this macro virus. If the infected document is opened by another user, the document, including the macro virus, will propagate. Note that this could cause the user's document to be propagated instead of the original document, and thereby leak sensitive information. Indirectly, this virus could cause a denial of service on mail servers. Many large sites have reported performance problems with their mail servers as a result of the propagation of this virus.