## [3413ICT Network Security](file:///C:\Documents%20and%20Settings\s995689\My%20Documents\Teaching\Courses_2013\Courses_2003\6216INT_03\6216inthome.html)

### **Workshop 5A**

**Part 1 – Review the lecture, answer the following questions**

1. For network-based systems (such as online services and Internet banking), there exist security threats for which encryption alone is not an effective countermeasure. List and explain two such security threats.

Threats exist:

* + unauthorised monitoring & control of network traffic
  + IP spoofing
  + Electronic-eavesdropping
  + Packet sniffing

1. Explain why IPSec is needed in addition to other available security mechanisms?

There may be security ignorant app lications that are running. By encapsulating the data in IPSec all data being sent out becomes more secure because it is being wrapped in the transport layer with IPSec.

1. Give examples of applications of IPSec

**Secure Branch office connectivity over the Internet**: company can build a VPN over the Internet or a public WAN. Reduce the need for private networks saving costs and network management overhead.  
**Secure remote access over the Internet**: End user who is equipped with IP security protocols can make a local call to an Internet service provider and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.  
**Establishing extranet and intranet connectivity with partners**: Secure communications with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.  
**Enhancing electronic commerce security**: Some online applications are designed with security in mind. Implementing IPSEC only enhances security further.

1. What services are provided by IPSec?

Authenticate and encrypt all data at the IP level. Can provide Authentication, Confidentiality, and key management (concerned with secure exchange of keys). This is achieved by the following services: access control, connectionless integrity, data origin authentication, rejection of replayed packets, and limited traffic flow confidentiality.

1. Explain the following terms: (1) Authentication Header (AH); (2) Encapsulating Security Payload (ESP); and (3) Security Association (SA).

**Authentication Header:** provides support for data integrity and authentication of IP packets. Parties must share a secret key to use authentication headers. Based on MAC (Message authentication code).  
**Encapsulating Security Payload**: provides message content confidentiality & limited traffic flow confidentiality. Can optionally provide the same authentication services as AH.  
**Security Association**: Can implement either AH or ESP. One-way relationship between sender and receiver that affords security services to the traffic carried on it.

1. What are the basic approaches to bundling SAs?

4 different approaches to bundling SAs:  
1.AH in transport mode  
2.ESP is transport mode  
3. AH followed by ESP in transport mode (an AH SA inside an ESP SA)  
4. Any one of 1,2 or 3 inside an AH or ESP in tunnel mode

1. Why does ESP include a padding field?

ESP includes a padding field for a number of different reasons:  
1. If an encryption algorithm requires the plaintext to be a multiple of some number of bytes then the padding field is used to expand the plaintext.  
2. ESP format requires that Pad Length and Next Header fields be right aligned with 32-bit word. The cipher text must be an integer multiple of 32 bits. Padding field is used to ensure this alignment.  
3. Additional padding may be added to provide partial traffic flow confidentiality by concealing the actual length of the payload.

1. When the tunnel mode ESP is used to encrypt IPv4 and IPv6 packets show, in a diagram, what fields are encrypted and what new fields are added to the original packet.

IPV4

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| New IP hdr | ESP hdr | Orig IP hdr | TCP | Data | ESP trlr | ESP auth |

IPV6

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| New IP hdr | Ext headers | ESP headers | Orig IP hdr | Ext headers | TCP | Data | ESP trlr | ESP auth | Orig IP hdr | TCP | Data | ESP trlr | ESP auth | ESP auth |

1. What is the difference between transport mode and tunnel mode?

**Transport Mode**: Provides protection from upper layer protocols. Used for end to end communication between 2 hosts. Payload is the data after the header  
**Tunnel Mode**: Provides protection to the entire packet. After AH and ESP fields are added to the IP packet, the entire payload is added with a new outer IP header. No routers along the way are able to examine the inner IP header.

**Part 2 – Challenge Exercises**

1. In an Internet banking system using two-factor authentication, in addition to a valid account number each user is required to provide two means of evidence (i.e., two factors) to assert his/her identity to the system. The first factor is usually the password or PIN number; and the second factor can be:
2. A unique code on the user’s physical token (or an ID-card), or a code from a list (which contains a number of codes).
3. A one-time pad that the user received from the bank through a registered mobile phone.
4. Some unique information that the user owns, such as biometric data.

Compare the three types of authentication factors listed above in a), b), and c), in terms of security, system efficiency and cost. In your opinion, which type is the most secure one? Is it cost effective? Which one is the least secure one? Why? Reading the following article and confirm your analysis.