**Unit-4: Network Security**

Session -1 Authentication applications Date: 19.08.2013 period: 03

Video : why Kerberos: [**http://www.youtube.com/watch?v=8xdBULP1aqQ**](http://www.youtube.com/watch?v=8xdBULP1aqQ)

**Content: presentation slides: http://www.cisa.umbc.edu/courses/cmsc/487/spring07/slides/ch14.ppt**

Crossword puzzle: 

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|   |   | 1 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   | 2 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   | 3 |   |   |   |   |   |   |   |   |
| 4 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 5 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 6 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 7 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 8 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 9 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |

 |

|  |  |
| --- | --- |
| ACROSS 2. who prove clients identity4. The encryption used by current Kerberos5. authenticate user to server and server to user6. one of the threat7. its a random number, used to seal request and response8. Tickets are dispensed by the  | DOWN 1. replay attack3. -------------provides a single client with access to a single server |

 |  |

 |

Unspoken words:

Secure, Reliable, Transparent, Scalable

Animated video: http://www.youtube.com/watch?v=7-LjpO2nTJo

**Session -2 Kerberos Date: 22.08.2013 period: 04**

Activity: Show and tell (Kerberos realm and multiple kerberi)

Content : presentation slides (http://www.cisa.umbc.edu/courses/cmsc/487/spring07/slides/ch14.ppt)

****

****

* Question and answer:
* What problem was Kerberos designed to address?
* Kerberos is designed to provide authentication of user identity in a networked computing environment
* What are three threats associated with user authentication over a network or Internet?
* *Unauthorized access*
* *Disclosure of information*
* *Denial of service*
* List three approaches to secure user authentication in a distributed environment.
	+ allows users access to services distributed through network
	+ without needing to trust all workstations
	+ rather all trust a central authentication server
* What four requirements were defined for Kerberos?
	+ secure
	+ reliable
	+ transparent
	+ scalable
* What is a realm?
	+ typically a single administrative domain

Session -3 X.509 Authentication service Date: 24.08.2013 period: 07

* Presentation – X.509 authentication service, Certificate revocation and authentication procedures

(http://www.cisa.umbc.edu/courses/cmsc/487/spring07/slides/ch14.ppt)

Conclusion: Puzzle (crossword)



**Session -4 Electronic mail security** Date: 04.09.2013 period: 02

* Content : Pretty Good Privacy – Presentation (**www.cs.uky.edu/~singhal/CS485-Au07/ch15.ppt)**
* Question and answer
* Remember by Keyword
* *Ks* =session key used in symmetric encryption scheme
* *PRa* =private key of user A, used in public-key encryption scheme
* *PUa* =public key of user A, used in public-key encryption scheme
* EP = public-key encryption
* DP = public-key decryption
* EC = symmetric encryption
* DC = symmetric decryption
* H = hash function
* || = concatenation
* Z = compression using ZIP algorithm
* R64 = conversion to radix 64 ASCII format
* Quiz

**1.What are the five principal services provided by PGP?**

Authentication, confidentiality, compression, e-mail compatibility, and

Segmentation

**2.What is R64 conversion?**

R64 converts a raw 8-bit binary stream to a stream of printable ASCII characters.

Each group of three octets of binary data is mapped into four ASCII characters.

**3.Why is the segmentation and reassembly function in PGP needed?**

E-mail facilities often are restricted to a maximum message length

**5.How does PGP use the concept of trust?**

PGP includes a facility for assigning a level of trust to individual signers and to keys**.**

* Snake and Ladder

 **Some of the Sample questions are:**

1. Name the 4 types of the keys used in PGP?
2. List out the 3 requirements identified with respect to key.
3. Why Session key is generated?
4. How many bits are given as input to the random number generator?
5. Why Key Identifiers are used?
6. List out the Public/ Private Key pairs owned by the owner.
7. What does the User ID typically refers to?
8. Differentiate Key ID with user ID.
9. Why key ID is used?
10. Why **radix64 is used?**

**Answers to the questions:**

1. One-time session symmetric keys
2. Public keys
3. Private keys
4. Passphrase based symmetric keys

 1. A means of generating unpredictable session keys is needed

 2. some means is needed for identifying particular keys.

 3. Each PGP entity must maintain a file of its own public/private key pairs as well

 as a file of public keys of correspondents.

1. for the purpose of encryption and decrypting the message
2. 128
3. It is possible to have more than one public/private key pair per user.

Each one therefore needs an ID of some kind.

* + Timestamp
	+ Key ID.
	+ Public Key.
	+ Private key.
	+ User ID.
1. user’s e-mail address
2. Key ID is -The least significant 64 bits of the public key for this entry and User ID –s – User’s eMail Address.
3. A key ID is also used for the PGP digital signature
4. radix64 which maps 6 bits of a binary data into and 8 bit ASCII character

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 100 |  |  |  |  |  |  |  |  |  |
| 99 | 98 | 97 | 96 | 95 | 94 | 93 | 92 | 91 | 90 |
| 80 | 81 | 82 | 83 | 84 | 85 | **86** | 87 | 88 | 89 |
| 61 | **62** | **63** | 64 | 65 | 66 | 67 | 68 | **69** | 70 |
| 60 | 59 | 58 | 57 | 56 | 55 | 54 | 53 | 52 | 51 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| 40 | 39 | 38 | 37 | 36 | 35 | 34 | 33 | 32 | 31 |
| 21 | 22 | 23 | 24 | **25** | 26 | 27 | 28 | 29 | 30 |
| 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

**Session -5 Electronic mail security** Date: 04.09.2013 period: 04

* Presentation –PGP Mail Security (**www.cs.uky.edu/~singhal/CS485-Au07/ch15.ppt)**

 Conclusion: questions and answer



**Session -6 S/MIME** Date: 05.09.2013 period: 04

* Presentation –S/MIME Mail Security (**www.cs.uky.edu/~singhal/CS485-Au07/ch15.ppt)**

Recall by keywords

* MIME Version
* Content-type
* Content transfer encoding
* Content ID
* Content description
* Snake and ladder

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 100 |  |  |  |  |  |  |  |  |  |
| 99 | 98 | 97 | 96 | 95 | 94 | 93 | 92 | 91 | 90 |
| 80 | 81 | 82 | 83 | 84 | 85 | **86** | 87 | 88 | 89 |
| 61 | **62** | **63** | 64 | 65 | 66 | 67 | 68 | **69** | 70 |
| 60 | 59 | 58 | 57 | 56 | 55 | 54 | 53 | 52 | 51 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| 40 | 39 | 38 | 37 | 36 | 35 | 34 | 33 | 32 | 31 |
| 21 | 22 | 23 | 24 | **25** | 26 | 27 | 28 | 29 | 30 |
| 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

1. Unformatted text; may be ASCII or ISO 8859 - **Plain text**
2. Provides greater format flexibility.- **Enriched text**
3. The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message. - **Mixed multipart**
4. Differs from Mixed only in that no order is defined for delivering the parts to the receiver **Parallel multipart**
5. Similar to Mixed, but the default type/subtype of each part is message/rfc822.- **Digest multipart**
6. The body is itself an encapsulated message that conforms to RFC 822.- **rfc822 message**
7. Used to allow fragmentation of large mail items, in a way that is transparent to the Recipient - **parallel message**
8. General binary data consisting of 8-bit bytes -**octet stream application**
* Recall by keyword
* Enveloped data
* Signed data
* Clear-signed data
* Signed and enveloped data

**Questions and answers:**

1. What are the functions of SMIME?

 enveloped data, signed data, clear signed data, signed and enveloped data.

1. Differentiate enveloped data with signed data?

 **Enveloped data:** This consists of encrypted content of any type and encrypted-content

encryption keys for one or more recipients.

 **Signed data:** A digital signature is formed by taking the message digest of the content to be signed and then

encrypting that with the private key of the signer. The content plus signature are then encoded using base64 encoding.

 A signed data message can only be viewed by a recipient with S/MIME capability.

1. What is clear signing?

With clear signing recipients without S/MIME capability can view the message content, although they cannot verify the signature.

Session -7 IP Security Date: 10.09.2013 Period: 01

* Presentation (**www.cisa.umbc.edu/courses/cmsc/487/spring07/slides/ch16.ppt)**
* Recall by keyword
* Architecture
* Encapsulating Security Payload (ESP)
* Authentication Header (AH)
* Encryption Algorithm.
* Authentication Algorithm
* Key Management
* Domain of Interpretation (DOI)
* Quiz

1.Give examples of applications of IPSec.

* Secure branch office connectivity over the Internet
* Secure remote access over the Internet
* Establishing extranet and intranet connectivity with partners
* Enhancing electronic commerce security

2.What services are provided by IPSec?

* Access control
* Connectionless integrity
* Data origin authentication
* Rejection of replayed packets (a form of partial sequence integrity)
* Confidentiality (encryption)
* Limited traffic flow confidentiality

3.How IPSec helps in routing applications

* Routing protocols such as OSPF should be run on top of security associations between routers that are defined by IPSec.

 4.Name the 7 documents.

* Architecture
* Encapsulating Security Payload (ESP)
* Authentication Header (AH)
* Encryption Algorithm
* Authentication Algorithm
* Key Management
* Domain of Interpretation (DOI)

5.List out the parameters of security association

* Security Parameters Index (SPI)
* IP Destination Address
* Security Protocol Identifier

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

* Tunnel mode provides protection to the entire IP packet
* Transport mode provides protection primarily for upper-layer protocols.

**Session -8 Web security** Date: 11.09.2013 Period: 02

* Presentation (**www.cisa.umbc.edu/courses/cmsc/487/spring07/slides/ch17.ppt**)
* Remember by keywords
* Oakley Key Determination Protocol
* Internet Security Association and Key Management Protocol (ISAKMP
* Digital signatures
* Public-key encryption
* Symmetric-key encryption
* Initiator Cookie (64 bits)
* Responder Cookie (64 bits)
* Next Payload (8 bits)
* Major Version (4 bits)
* Minor Version (4 bits)
* Exchange Type (8 bits)
* Flags (8 bits)
* Message ID (32 bits)
* Length (32 bits)
* **Video clipping**
* <http://www.youtube.com/watch?v=GUkVyQZBaqU&feature=related>
* Brainstorming
	+ integrity
	+ confidentiality
	+ denial of service
	+ authentication
* Question and answer

1.What protocols comprise SSL?

SSL handshake protocol; SSL change cipher spec protocol; SSL alert protocol; SSL record protocol

2.What is the difference between an SSL connection and an SSL session?

**Connection:** A connection is a transport that provides a suitable type of service.

**Session:** An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol.

3.List the parameters that define an SSL session state.

**Session identifier** , **Peer certificate** , **Compression method, Master secret**

4.List the parameters that define an SSL session connection.

**Server and client random** , **Server write MAC secret, Client write MAC secret, Server write key, Client write key, Initialization vectors, Sequence numbers**

5.What services are provided by the SSL Record Protocol?

**Confidentiality, Message Integrity**

6.What steps are involved in the SSL Record Protocol transmission

Fragmentation; compression; add MAC; encrypt; append SSL record header