Scheme Of Evaluation
Internal Assessment Test 2 – March.2019

Sub:	Cryptography,Network Security & Cyber law							**Code:**	15CS61
Date:	15/ 04 / 2019	Duration:	90mins	Max Marks:	50	**Sem:**	VI	**Branch:**	ISE

Note: Answer Any Five Questions

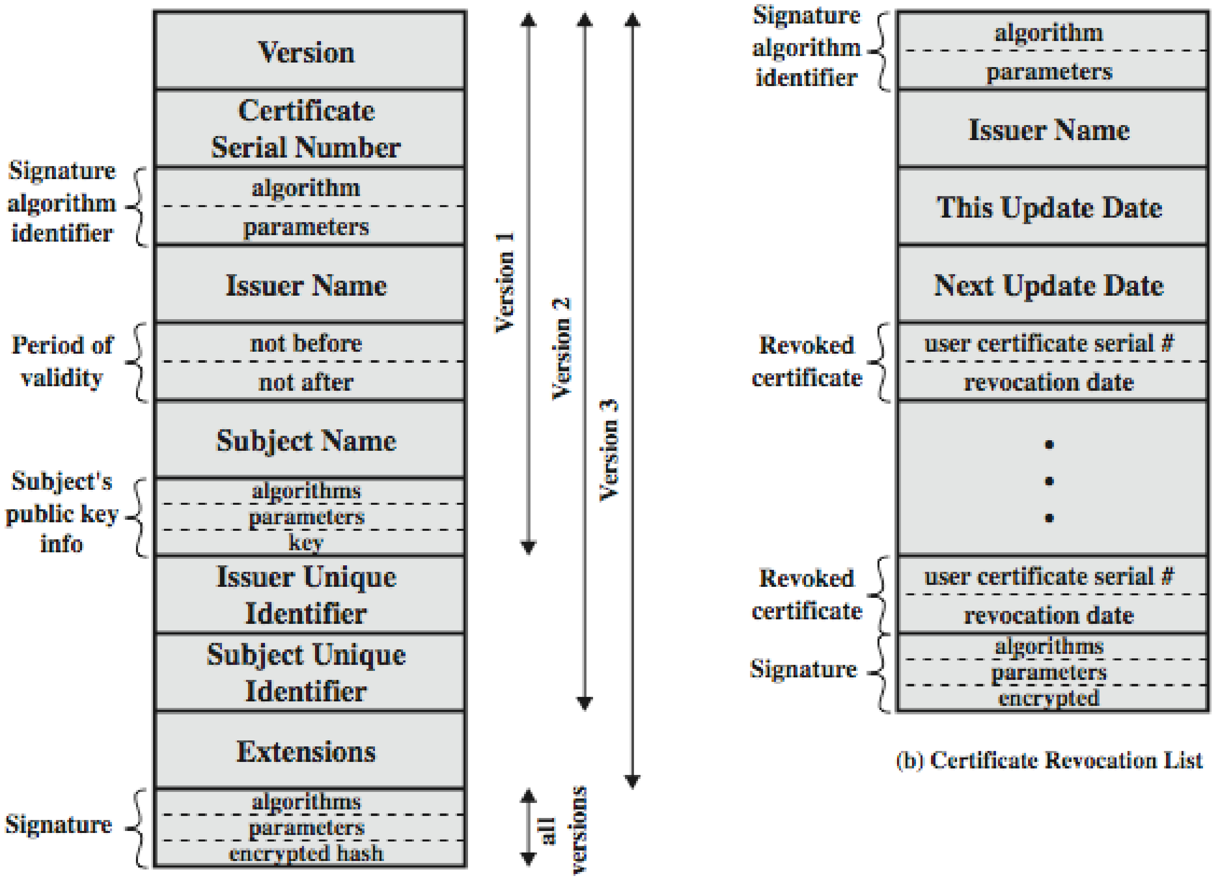
Question #		**Description**	**Marks Distribution**		**Max Marks**
1	a)	**Label X.509 certificate.** • Certificate	5M	5M	10 M
	b)	**Draw final version of Needham Schroeder protocol.** • Protocol communication	5M	5M	
2	a)	**Describe in brief about biometrics and error measures** • Biometrics • Error measures	5M 5M	10M	10 M
3	a)	**Summarize the phases of Internet Key Exchange protocol.** • Phase 1 • Phase 2	5M 5M	10M	10 M
4	a)	**Discuss cyber regulations appellate tribunal.** • Regulations	7M	7M	10 M
	b)	**Quote the penalties and adjudication specified by cyber law** • Penalties & adjudication	3M	3M	
5	a)	**Show how security is provided in transport layer.** • Handshake protocol • Record layer protocol	5M 5M	10 M	10 M
6	a)	**Explain in detail about Kerberos.** • Diagram	5M	7M	10 M

		• Dialogue	2M		
	b)	**List the duties of subscribers specified by cyber law.** • Duties	3M	3M	
7	a)	**Compare and contrast one-way authentication and mutual authentication in detail.** • One-way authentication • Mutual authentication	5M 5M	10M	10 M
8	a)	**Whether physical characteristics can be used as an authentication mechanism. If yes justify your answer.** • Yes/No • Justification	1M 9M	10M	10 M

Answers

1. A. Label X.509 certificate.

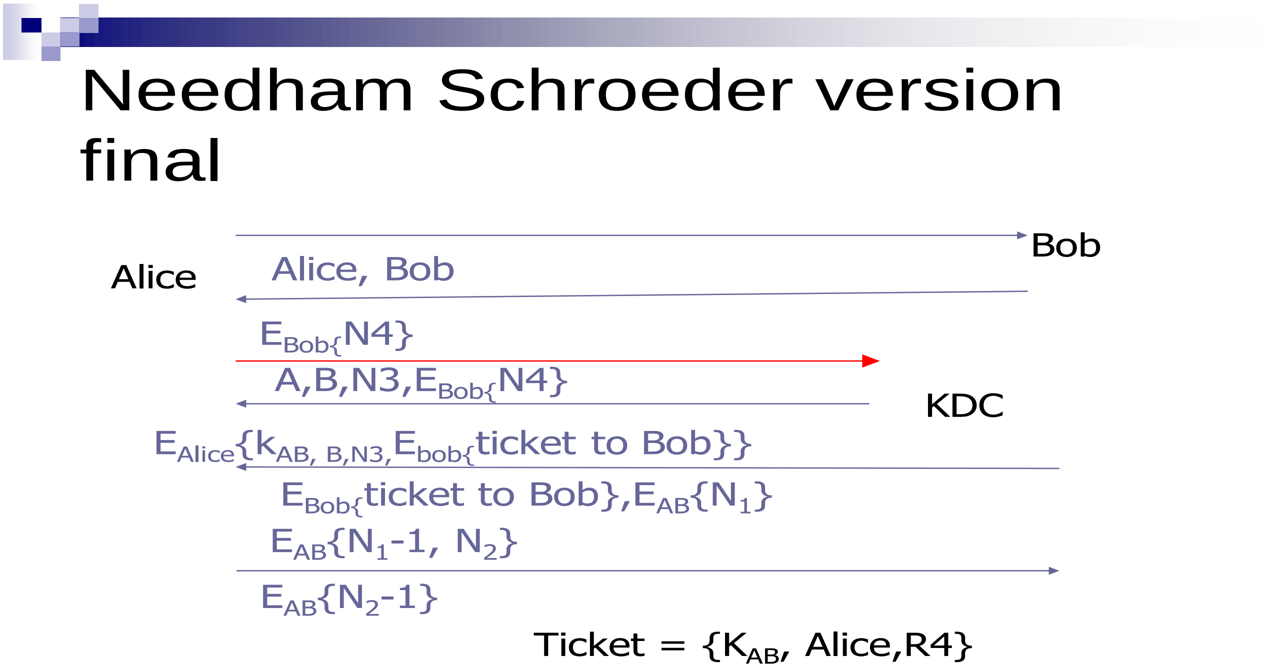
- part of CCITT X.500 directory service standards
  - distributed servers maintaining user info database
- defines framework for authentication services
  - directory may store public-key certificates
  - with public key of user signed by certification authority
- also defines authentication protocols
- uses public-key crypto & digital signatures
  - algorithms not standardised, but RSA recommended
- X.509 certificates are widely used
  - have 3 versions



(a) X.509 Certificate

(b) Certificate Revocation List

b. Draw final version of Needham Schroeder protocol.



Needham Schroeder version final

Alice

Bob

Alice, Bob

$E_{Bob\{}N4\}$

A,B,N3,$E_{Bob\{}N4\}$

KDC

$E_{Alice}\{k_{AB,\ B,N3,}E_{bob\{}$ticket to Bob$\}\}$

$E_{Bob\{}$ticket to Bob$\}$,$E_{AB}\{N_1\}$

$E_{AB}\{N_1$-1, $N_2\}$

$E_{AB}\{N_2$-1$\}$

Ticket = $\{K_{AB,}$ Alice,R4$\}$

2. A . Describe in brief about biometrics and error measures

Biometrics(5)

Is the technical term for body measurements and calculations. It refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.

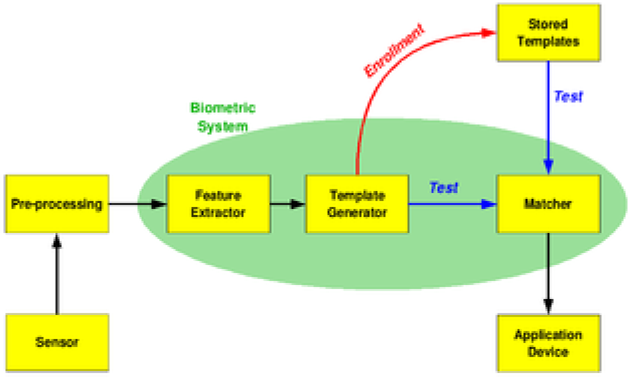
Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.

More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information

Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Jain et al. (1999) identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication.

- Universality means that every person using a system should possess the trait.
- Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.
- Permanence relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm.
- Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.
- Performance relates to the accuracy, speed, and robustness of technology used.
- Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.
- Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute.

Proper biometric use is very application dependent. Certain biometrics will be better than others based on the required levels of convenience and security.[8] No single biometric will meet all the requirements of every possible application.



The block diagram illustrates the two basic modes of a biometric system. First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person. In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using the same identity".

Second, in identification mode the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

The first time an individual uses a biometric system is called enrollment. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the filesize and to protect the identity of the enrollee.

During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area). Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements. In selecting a particular biometric, factors to consider include, performance, social acceptability, ease of circumvention and/or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence. Selection of a biometric based on user requirements considers sensor and device availability, computational time and reliability, cost, sensor size and power consumption.

Error Measures (5)

- False match rate (FMR, also called FAR = False Accept Rate): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs that are incorrectly accepted. In case of similarity scale, if the person is an imposter in reality, but the matching score is higher than the threshold, then he is treated as genuine. This increases the FMR, which thus also depends upon the threshold value.[9]
- False non-match rate (FNMR, also called FRR = False Reject Rate): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs that are incorrectly rejected.

- Receiver operating characteristic or relative operating characteristic (ROC): The ROC plot is a visual characterization of the trade-off between the FMR and the FNMR. In general, the matching algorithm performs a decision based on a threshold that determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matches but more false accepts. Conversely, a higher threshold will reduce the FMR but increase the FNMR. A common variation is the Detection error trade-off (DET), which is obtained using normal deviation scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).
- Equal error rate or crossover error rate (EER or CER): the rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is the most accurate.
- Failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.
- Failure to capture rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
- Template capacity: the maximum number of sets of data that can be stored in the system.

3. Explain the phases of Internet Key Exchange protocol.

IKE Phase 1

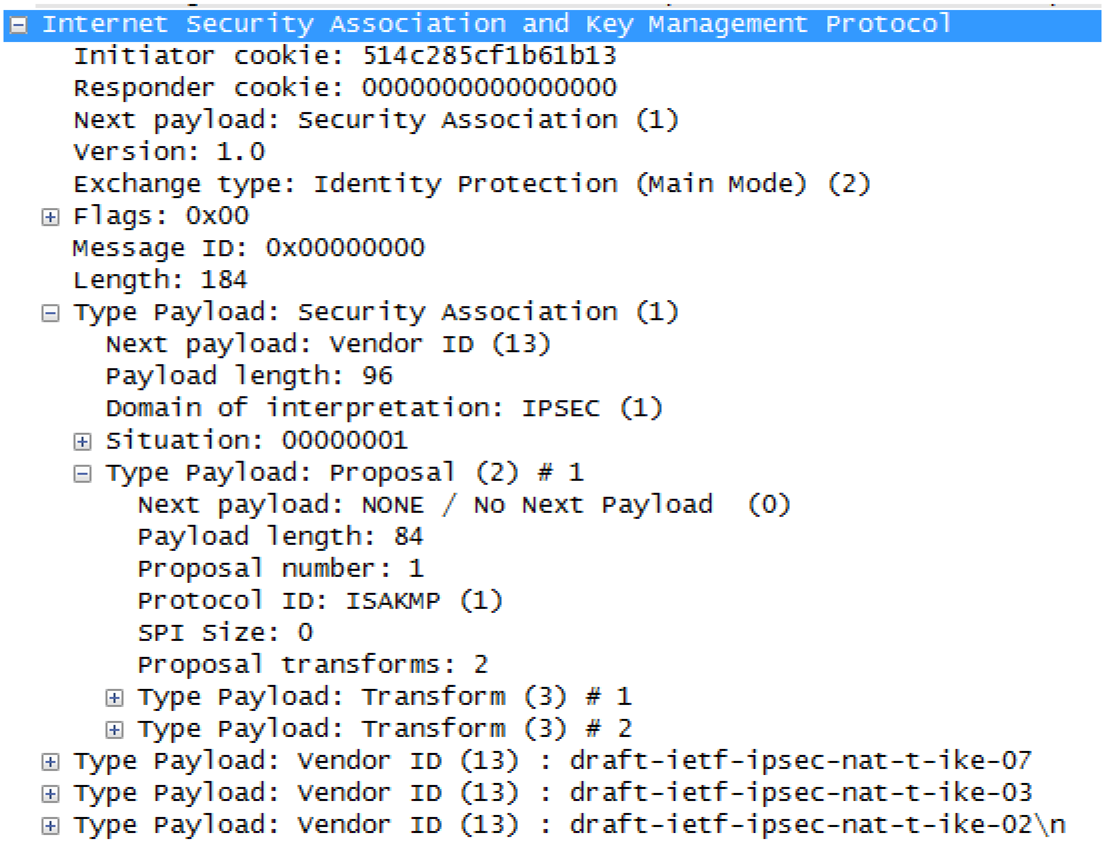
IKE Phase 1 works in one of two modes, main mode or aggressive mode now of course both of these modes operate differently and we will cover both of these modes.

Main Mode:

IKE Phase 1 operating in main mode works with both parties exchanging a total of 6 packets, that’s right 6 packets is all it takes to complete phase 1.

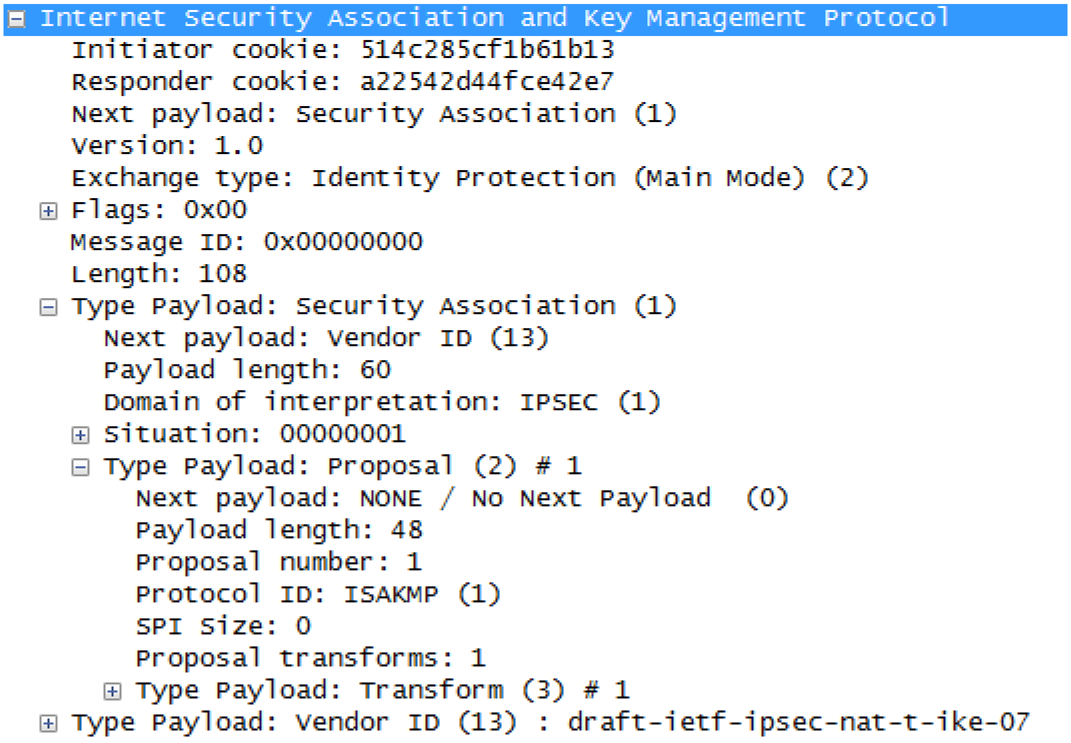
1. The first packet is sent from the initiator of the IPSec tunnel to its remote endpoint, this packet contains the ISAKMP policy
2. The second packet is sent from the remote endpoint back to the initiator, this packet will be the exact same information matching the ISAKMP policy sent by the initiator.
3. The third packet is sent from the initiator to the remote endpoint, this packet contains the Key Exchange payload and the Nonce payload, the purpose of this packet is generate the information for the DH secret key
4. This fourth packet as you would expect comes from the remote endpoint back to initiator and contains the remote endpoints Key Exchange and Nonce payload.
5. The fifth packet is from the initiator back to the remote endpoint with identity and hash payloads, the identity payload has the device’s IP Address in, and the hash payload is a combination of keys (including a PSK, if PSK authentication is used)

6. The sixth packet from the remote endpoint to the initiator contains the corresponding hash payloads to verify the exchange.



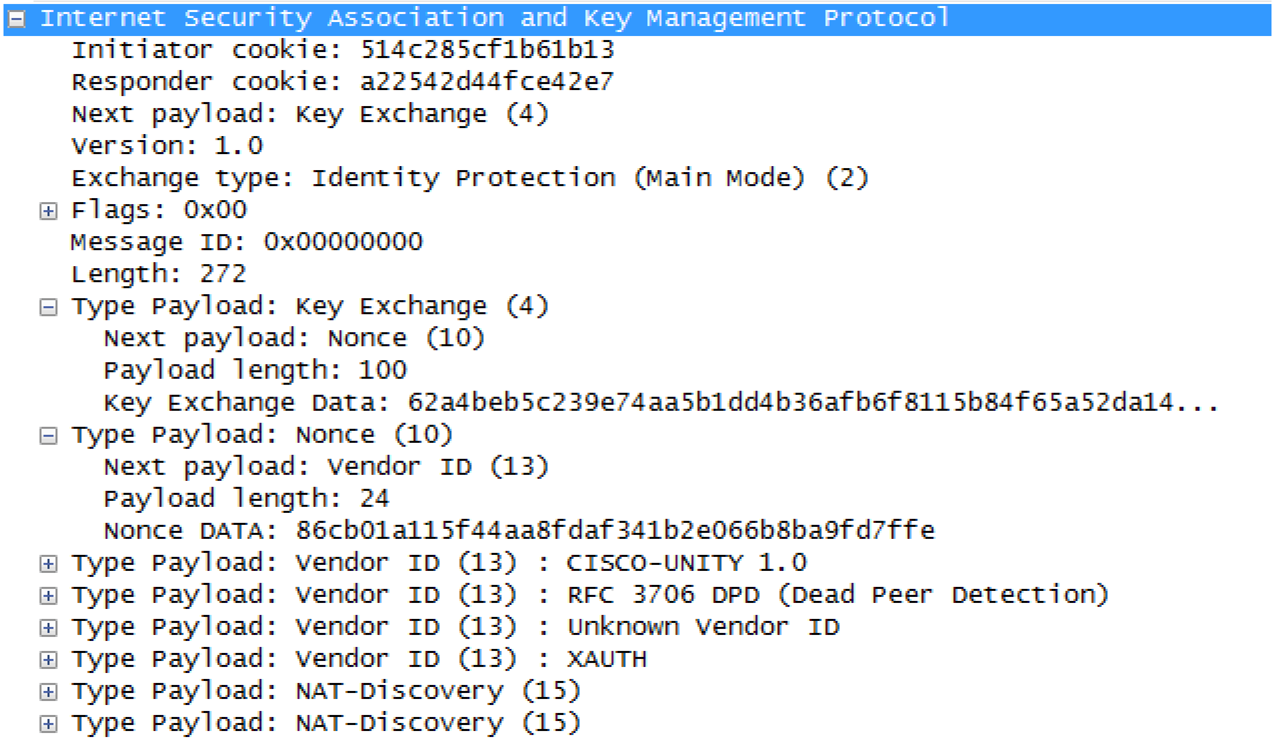
```
⊟ Internet Security Association and Key Management Protocol
    Initiator cookie: 514c285cf1b61b13
    Responder cookie: 0000000000000000
    Next payload: Security Association (1)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  ⊞ Flags: 0x00
    Message ID: 0x00000000
    Length: 184
  ⊟ Type Payload: Security Association (1)
      Next payload: Vendor ID (13)
      Payload length: 96
      Domain of interpretation: IPSEC (1)
    ⊞ Situation: 00000001
    ⊟ Type Payload: Proposal (2) # 1
        Next payload: NONE / No Next Payload  (0)
        Payload length: 84
        Proposal number: 1
        Protocol ID: ISAKMP (1)
        SPI Size: 0
        Proposal transforms: 2
      ⊞ Type Payload: Transform (3) # 1
      ⊞ Type Payload: Transform (3) # 2
  ⊞ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-07
  ⊞ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-03
  ⊞ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02\n
```

First packet in the IKE Phase 1



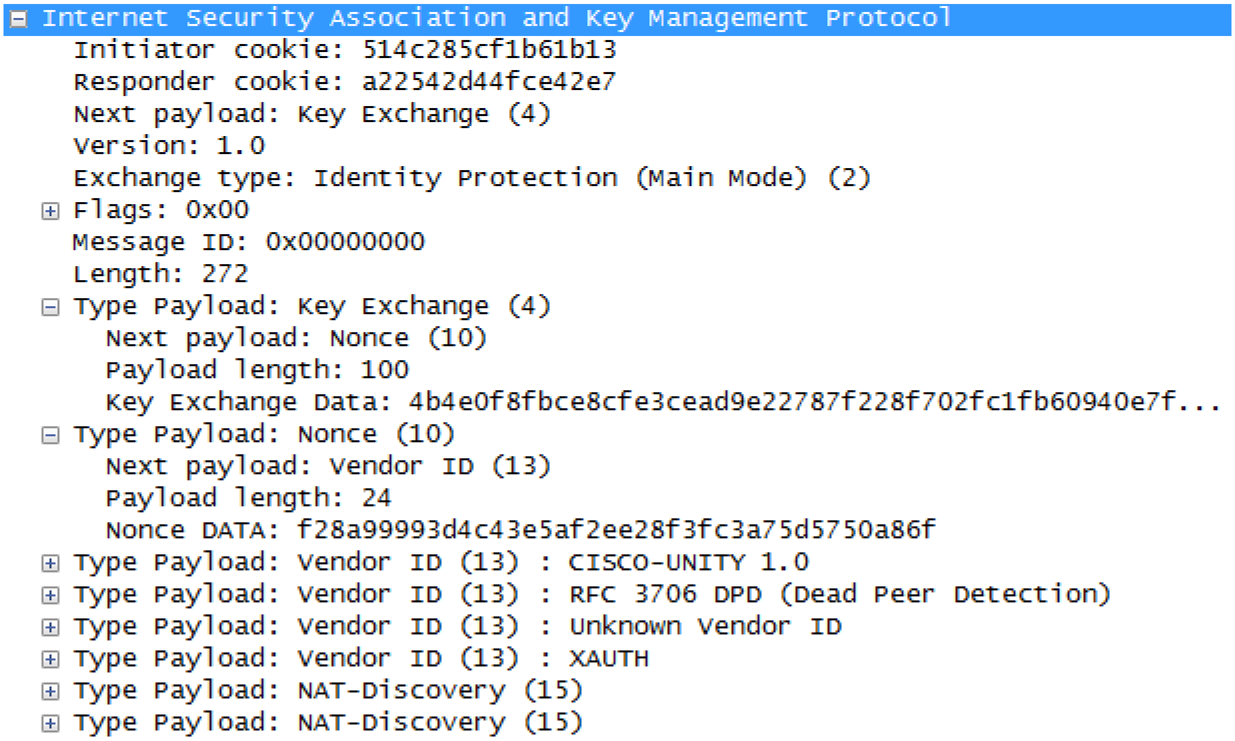
```
⊟ Internet Security Association and Key Management Protocol
    Initiator cookie: 514c285cf1b61b13
    Responder cookie: a22542d44fce42e7
    Next payload: Security Association (1)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  ⊞ Flags: 0x00
    Message ID: 0x00000000
    Length: 108
  ⊟ Type Payload: Security Association (1)
      Next payload: Vendor ID (13)
      Payload length: 60
      Domain of interpretation: IPSEC (1)
    ⊞ Situation: 00000001
    ⊟ Type Payload: Proposal (2) # 1
        Next payload: NONE / No Next Payload  (0)
        Payload length: 48
        Proposal number: 1
        Protocol ID: ISAKMP (1)
        SPI Size: 0
        Proposal transforms: 1
      ⊞ Type Payload: Transform (3) # 1
  ⊞ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-07
```

Second packet of the IKE Phase 1 process



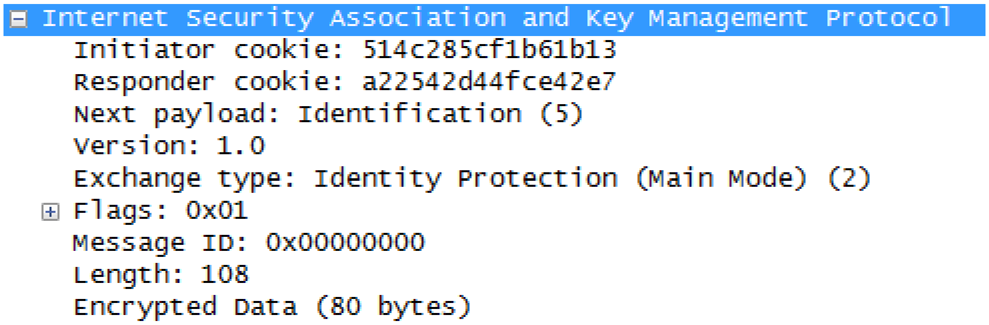
```
⊟ Internet Security Association and Key Management Protocol
    Initiator cookie: 514c285cf1b61b13
    Responder cookie: a22542d44fce42e7
    Next payload: Key Exchange (4)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  ⊞ Flags: 0x00
    Message ID: 0x00000000
    Length: 272
  ⊟ Type Payload: Key Exchange (4)
      Next payload: Nonce (10)
      Payload length: 100
      Key Exchange Data: 62a4beb5c239e74aa5b1dd4b36afb6f8115b84f65a52da14...
  ⊟ Type Payload: Nonce (10)
      Next payload: Vendor ID (13)
      Payload length: 24
      Nonce DATA: 86cb01a115f44aa8fdaf341b2e066b8ba9fd7ffe
  ⊞ Type Payload: Vendor ID (13) : CISCO-UNITY 1.0
  ⊞ Type Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
  ⊞ Type Payload: Vendor ID (13) : Unknown Vendor ID
  ⊞ Type Payload: Vendor ID (13) : XAUTH
  ⊞ Type Payload: NAT-Discovery (15)
  ⊞ Type Payload: NAT-Discovery (15)
```

Third packet in IKE Phase 1



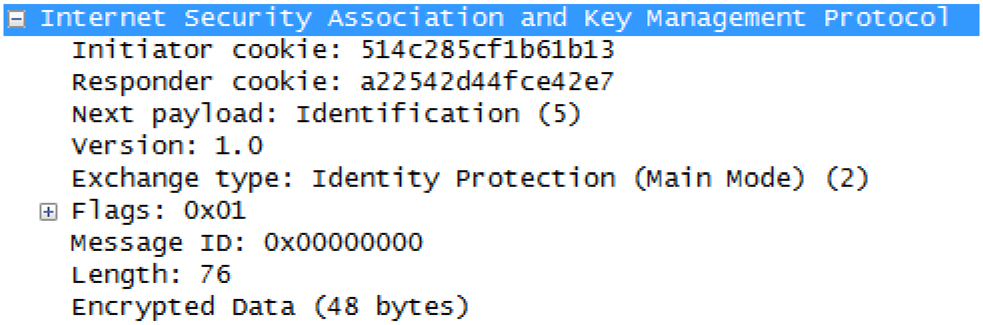
```
⊟ Internet Security Association and Key Management Protocol
    Initiator cookie: 514c285cf1b61b13
    Responder cookie: a22542d44fce42e7
    Next payload: Key Exchange (4)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  ⊞ Flags: 0x00
    Message ID: 0x00000000
    Length: 272
  ⊟ Type Payload: Key Exchange (4)
      Next payload: Nonce (10)
      Payload length: 100
      Key Exchange Data: 4b4e0f8fbce8cfe3cead9e22787f228f702fc1fb60940e7f...
  ⊟ Type Payload: Nonce (10)
      Next payload: Vendor ID (13)
      Payload length: 24
      Nonce DATA: f28a99993d4c43e5af2ee28f3fc3a75d5750a86f
  ⊞ Type Payload: Vendor ID (13) : CISCO-UNITY 1.0
  ⊞ Type Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
  ⊞ Type Payload: Vendor ID (13) : Unknown Vendor ID
  ⊞ Type Payload: Vendor ID (13) : XAUTH
  ⊞ Type Payload: NAT-Discovery (15)
  ⊞ Type Payload: NAT-Discovery (15)
```

Fourth packet in the IKE Phase 1 process



```
⊟ Internet Security Association and Key Management Protocol
    Initiator cookie: 514c285cf1b61b13
    Responder cookie: a22542d44fce42e7
    Next payload: Identification (5)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  ⊞ Flags: 0x01
    Message ID: 0x00000000
    Length: 108
    Encrypted Data (80 bytes)
```

Fifth packet in the IKE Phase 1 process



```
⊟ Internet Security Association and Key Management Protocol
    Initiator cookie: 514c285cf1b61b13
    Responder cookie: a22542d44fce42e7
    Next payload: Identification (5)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  ⊞ Flags: 0x01
    Message ID: 0x00000000
    Length: 76
    Encrypted Data (48 bytes)
```

Sixth and final packet in IKE Phase 1

Aggressive Mode:

IKE Phase 1 operating in aggressive mode only exchanges 3 packets compared to the 6 packets used in main mode. One downside in aggressive is the fact it not as secure as main mode.

1. The first packet from the initiator contains enough information for the remote endpoint to generate its DH secret, so this one packet is equivalent to the first four packets in main mode.
2. The second packet from the remote endpoint back to the initiator contains its DH secret
3. The third packet from the initiator includes identity and hash payloads. After the remote endpoint receives this packet it simply calculates its hash payload and verifies it matches, if it matches then phase one is established.

IKE Phase 2

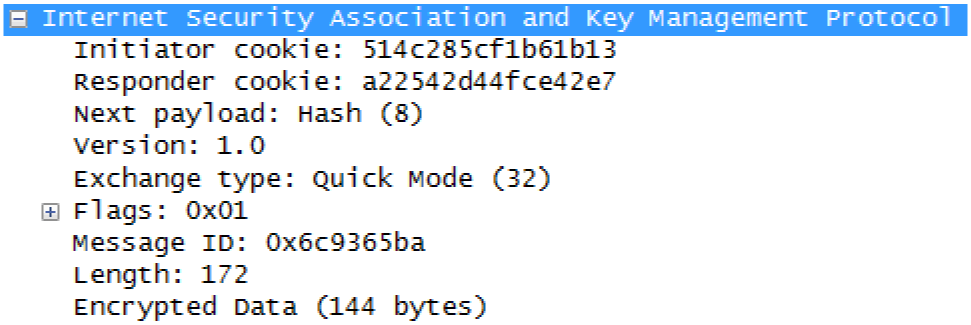
Now let's look at IKE Phase 2, IKE Phase 2 occurs after phase 1 and is also known as *quick mode* and this process is only 3 packets.

- Perfect Forward Secrecy PFS, if PFS is configured on both endpoints the will generate a new DH key for phase 2/quick mode.

1. Contained in this first packet from the initiator to the remote device are some of the hashes/keys negotiated from phase 1, along with some IPSec parameters IE: Encapsulation (ESP or AH), HMAC, DH-group, and the mode (tunnel or transport)
2. The second packet contains the remote endpoint's response with matching IPSec parameters.
3. The last packet is sent to the remote device to verify the other device is still there and is an active peer.

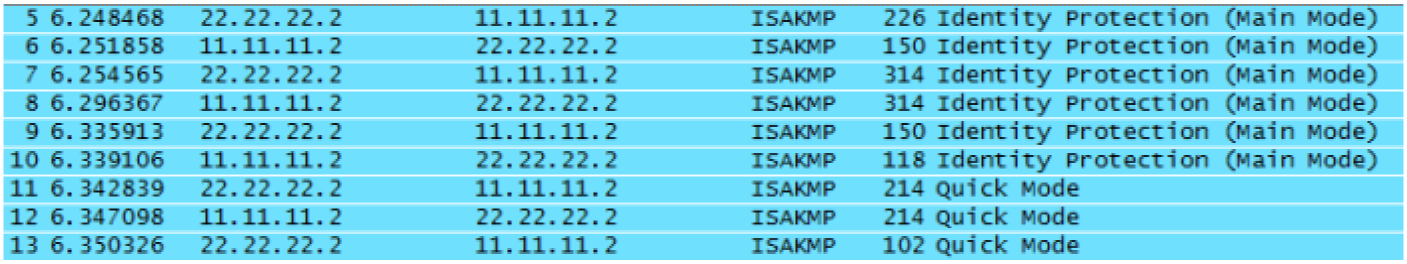
That last packet concludes the forming an IPSec tunnel and the phase 1/2 process.

- Note: These 3 quick mode packets are encrypted



```
⊟ Internet Security Association and Key Management Protocol
    Initiator cookie: 514c285cf1b61b13
    Responder cookie: a22542d44fce42e7
    Next payload: Hash (8)
    Version: 1.0
    Exchange type: Quick Mode (32)
  ⊞ Flags: 0x01
    Message ID: 0x6c9365ba
    Length: 172
    Encrypted Data (144 bytes)
```

Quick Mode packets with encrypted payload.



```
 5 6.248468   22.22.22.2        11.11.11.2        ISAKMP    226 Identity Protection (Main Mode)
 6 6.251858   11.11.11.2        22.22.22.2        ISAKMP    150 Identity Protection (Main Mode)
 7 6.254565   22.22.22.2        11.11.11.2        ISAKMP    314 Identity Protection (Main Mode)
 8 6.296367   11.11.11.2        22.22.22.2        ISAKMP    314 Identity Protection (Main Mode)
 9 6.335913   22.22.22.2        11.11.11.2        ISAKMP    150 Identity Protection (Main Mode)
10 6.339106   11.11.11.2        22.22.22.2        ISAKMP    118 Identity Protection (Main Mode)
11 6.342839   22.22.22.2        11.11.11.2        ISAKMP    214 Quick Mode
12 6.347098   11.11.11.2        22.22.22.2        ISAKMP    214 Quick Mode
13 6.350326   22.22.22.2        11.11.11.2        ISAKMP    102 Quick Mode
```

4. A. Discuss cyber regulations appellate tribunal.

The Cyber Regulations Appellate Tribunal

48. Establishment of Cyber Appellate Tribunal.

- The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.
- The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

49. Composition of Cyber Appellate Tribunal.

A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Residing Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.

50. Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal.

A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he -

- is, or has been. or is qualified to be, a Judge of a High Court, or
- is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

51. Term of office

The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

52. Salary, allowances and other terms and conditions of service of Presiding Officer.

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of. the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed:

Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment.

53. Filling up of vacancies.

If, for reason other than temporary absence, any vacancy occurs in the office n the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of. the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed:

Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment.

54. Resignation and removal.

The Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

Provided that the said Presiding Officer shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

The Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding Officer.

55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings.

No order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

56. Staff of the Cyber Appellate Tribunal.

- The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit
- The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.
- The salaries, allowances and other conditions of service of the officers and employees or' the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

4.b. Quote the penalties and adjudication specified by cyber law.

PENALTIES AND ADJUDICATION

43. Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network -

- accesses or secures access to such computer, computer system or computer network.

The Gazette of India Extraordinary

- downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium.
- i ntroduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.
- damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network.
- disrupts or causes disruption of any computer, computer system or computer network
- denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means.
- provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder.
- charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network.

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation : For the purposes of this section-

- "computer contaminant" means any set of computer instructions that are designed-
  - to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network, or

    - by any means to usurp the normal operation of the computer, computer system, or computer network.
- "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network.
- "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, daia or instruction is executed or some other event takes place in that computer resource.
- "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

44. Penalty for failure to furnish information return, etc.

If any person who is required under this Act or any rules or regulations made thereunder to-

- furnish any document, return or report to the Controller or ?he Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure.
- file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues.

The Gazette of India Extraordinary

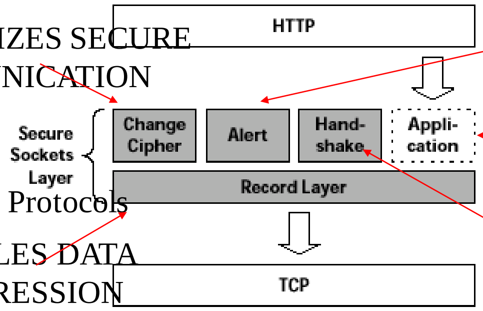
- maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

5. Show how security is provided in transport layer.

Introduction

- SSL (Secure Socket Layer) was standardized by IETF in 1999 and called as TLS(Transport Layer Security)
- Principal means of securing communications between an internet client & a server.

SSL (Secure Sockets Layer)



INITIALIZES SECURE COMMUNICATION

ERROR HANDLIN

HANDLES COMMU
WITH THE APPLIC

Protocols

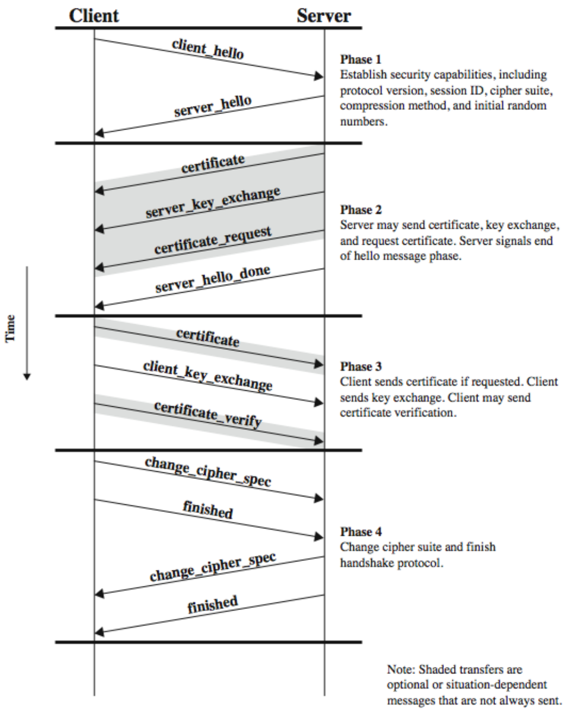
INITIALIZES COM
BETWEEN CLIENT

HANDLES DATA COMPRESSION

SSL is comprised of 2 main protocols

- The handshake protocol: is used to negotiate the set of algorithms to be used for securing the communication link.
- The record layer protocol: providing authentication, integrity checking & encryption

SSL Handshake Protocol



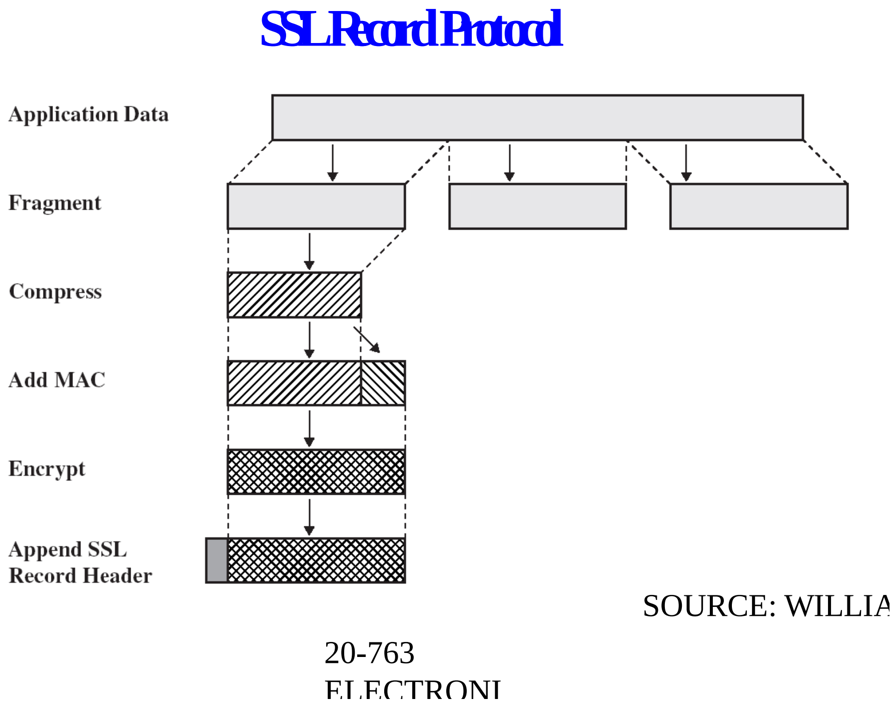
Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4
Change cipher suite and finish handshake protocol.

Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

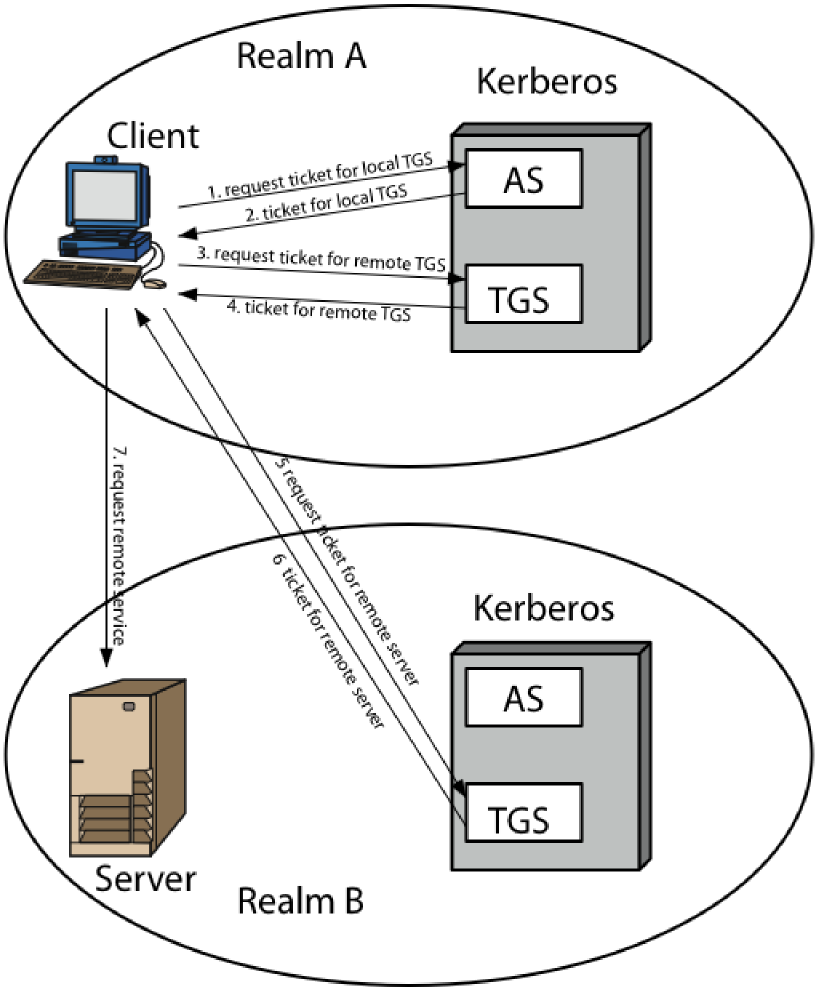


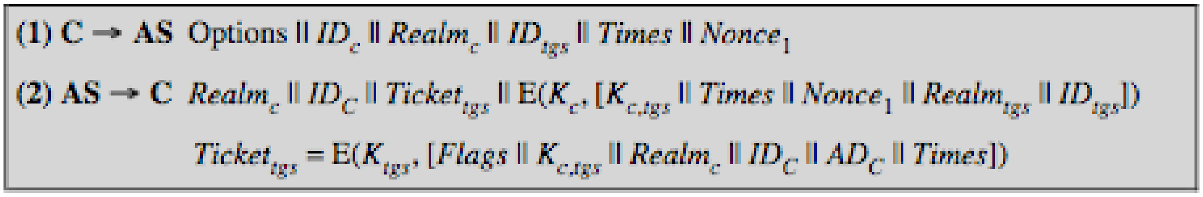
SSL Record Protocol

SOURCE: WILLIA

20-763
ELECTRONI

6. a. Explain in detail about Kerberos.


Realm A
Kerberos
Client
AS
TGS
1. request ticket for local TGS
2. ticket for local TGS
3. request ticket for remote TGS
4. ticket for remote TGS
5 request ticket for remote server
6 ticket for remote server
7. request remote service
Kerberos
AS
TGS
Server
Realm B

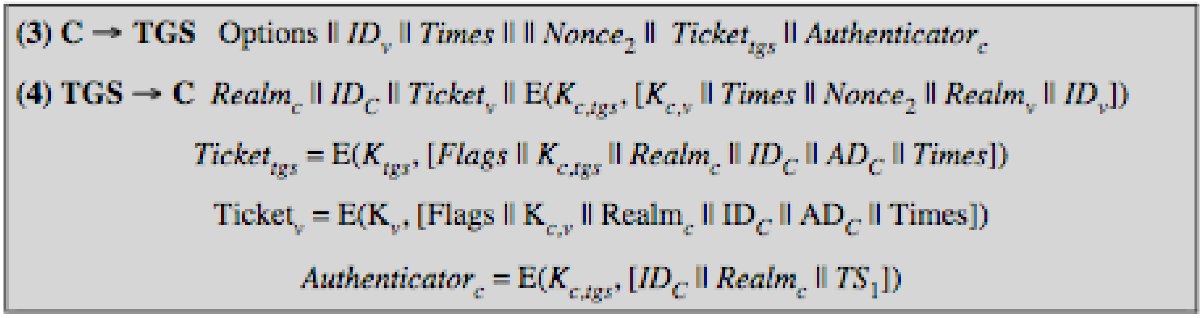


(1) C → AS Options $\| ID_c \| Realm_c \| ID_{tgs} \| Times \| Nonce_1$

(2) AS → C $Realm_c \| ID_C \| Ticket_{tgs} \| E(K_c, [K_{c,tgs} \| Times \| Nonce_1 \| Realm_{tgs} \| ID_{tgs}])$

$$Ticket_{tgs} = E(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$$

(a) Authentication Service Exchange to obtain ticket-granting ticket



(3) C → TGS Options $\| ID_v \| Times \| \| Nonce_2 \| \ Ticket_{tgs} \| Authenticator_c$

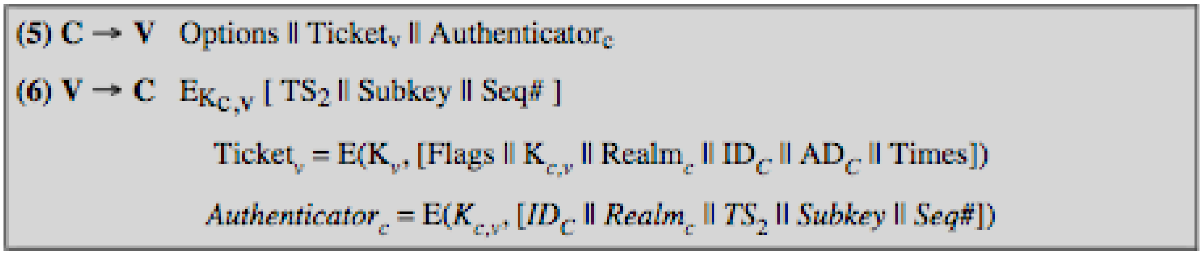
(4) TGS → C $Realm_c \| ID_C \| Ticket_v \| E(K_{c,tgs}, [K_{c,v} \| Times \| Nonce_2 \| Realm_v \| ID_v])$

$$Ticket_{tgs} = E(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$$

$$\mathrm{Ticket}_v = \mathrm{E}(\mathrm{K}_v, [\mathrm{Flags} \| \mathrm{K}_{c,v} \| \mathrm{Realm}_c \| \mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{Times}])$$

$$Authenticator_c = E(K_{c,tgs}, [ID_C \| Realm_c \| TS_1])$$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket



(5) C → V Options $\| \mathrm{Ticket}_v \| \mathrm{Authenticator}_c$

(6) V → C $\mathrm{E}_{K_{c,v}}\ [\ \mathrm{TS}_2 \| \mathrm{Subkey} \| \mathrm{Seq\#}\ ]$

$$\mathrm{Ticket}_v = \mathrm{E}(\mathrm{K}_v, [\mathrm{Flags} \| \mathrm{K}_{c,v} \| \mathrm{Realm}_c \| \mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{Times}])$$

$$Authenticator_c = E(K_{c,v}, [ID_C \| Realm_c \| TS_2 \| Subkey \| Seq\#])$$

(c) Client/Server Authentication Exchange to obtain service

b. List the duties of subscribers specified by cyber law.

DUTIES OF SUBSCRIBERS

40. Generating key pair.

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.

41. Acceptance of Digital Signature Certificate.

- A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate-
  - to one or more persons.
  - in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.
- By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that-

- the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same.
- all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true.
- all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

42. Control of private key.

- Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.
- If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by .the regulations.

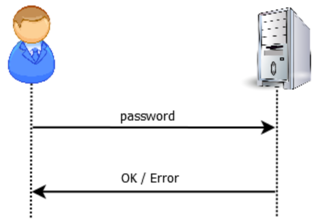
  Explanation.- For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

6. Compare and contrast one-way authentication and mutual authentication in detail.

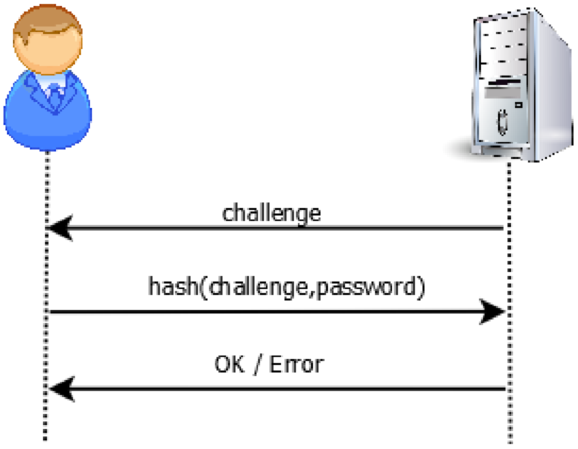
One way authentication

- In client-server communication, the client authenticates itself to the server
- The server may or may not be authenticated to the client

Password-based authentication Communicating Password Can be hacked



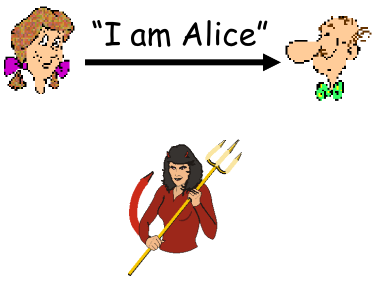
communicating hash of password –replay attack



Challenge-response Authentication

Goal: Bob wants Alice to “prove” her identity to him

Protocol ap1.0: Alice says “I am Alice”



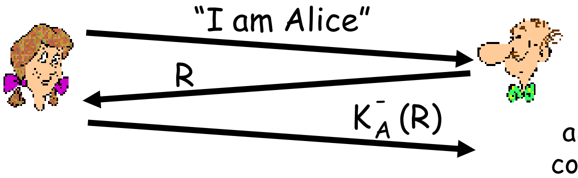
Failure scenario??

Authentication: ap5.0

ap4.0 doesn’t protect against server database reading

- can we authenticate using public key techniques?

ap5.0: use nonce, public key cryptography



“I am Alice”

R

$K_A^-(R)$

Bob computes

$K_A^+(K_A^-(R)) = R$

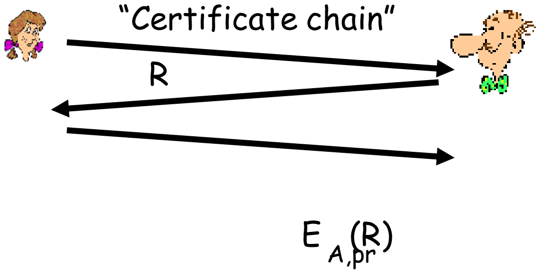
and knows only Alice could have the private key, that encrypted R such that

$K_A^+(K_A^-(R)) = R$

Challenge -response

- The client will send the A to convey its identity
- Server will send challenge(encrypted nounce)
- Client will decrypt the nounce to prove his identity

Certificate based authentication

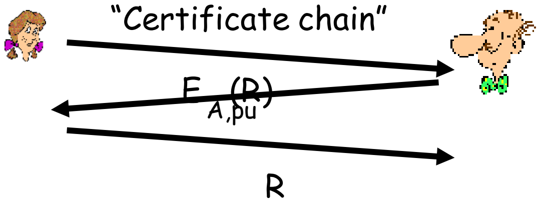


"Certificate chain"

R

$E_{A,pr}(R)$

Certificate based authentication



"Certificate chain"

$E_{A,pu}(R)$

R

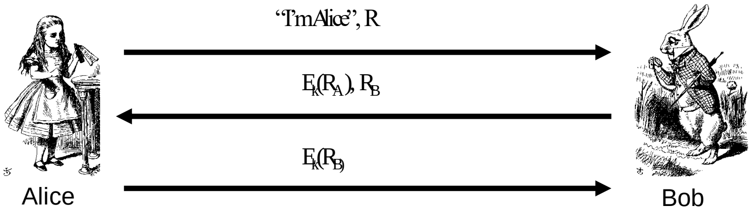
- A client need not share a secret with the server but may have a public key certificate.
- A. A sends her certificate in msg 1. B performs certain checks such as on the validity period & name of principal.
- He also verifies the signature of the CA on the certificate.
- He then sends his challenge a nounce R.

- A responds by encrypting the challenge with her private key
- When B receives E A.pr(R) he decrypts it with A’s public key & compares it with the nounce he transmitted in Msg 2.
- If they match, he concludes that A has used the private key corresponding to the public key in her certificate.

Mutual authentication

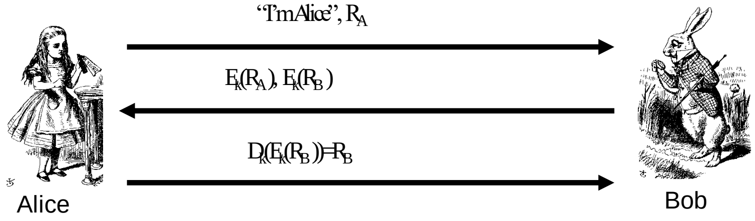
- Both communicating parties have to authenticate themselves to each other.
- Types
- Shared secret key authentication
- Asymmetric key based authentication

Mutual Authentication?



- **Flawed protocol**
- What’s wrong with this picture?
- “Alice” could be Trudy (or anybody else)!

Symmetric Key Mutual Authentication



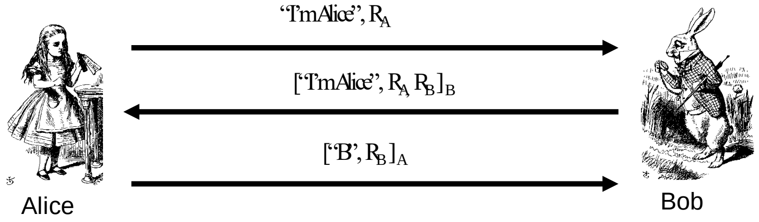
“I’m Alice”, R_A

$E_K(R_A), E_K(R_B)$

$D_K(E_K(R_B))=R_B$

- Do these “insignificant” changes help?
- Yes!

Asymmetric key based Authentication

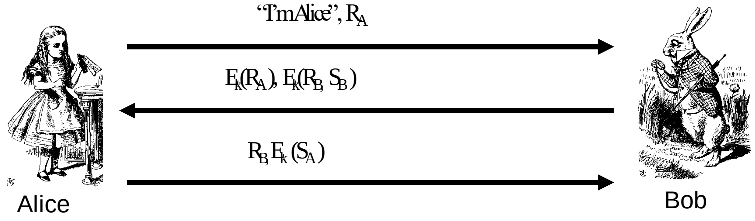


“I’m Alice”, R_A

[“I’m Alice”, R_A, R_B $]_B$

[“B’, R_B $]_A$

Using secret Key cryptography



“I’mAlice”, R_A

$E_k(R_A)$, $E_k(R_{B,}\ S_B)$

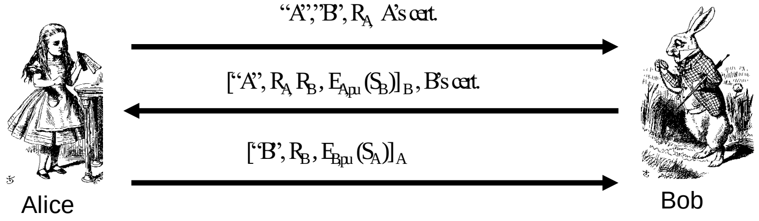
$R_{B,}E_k\ (S_A)$

Alice

Bob

- Session key= $S_{A\,xor}\,S_B$

Using public Key cryptography



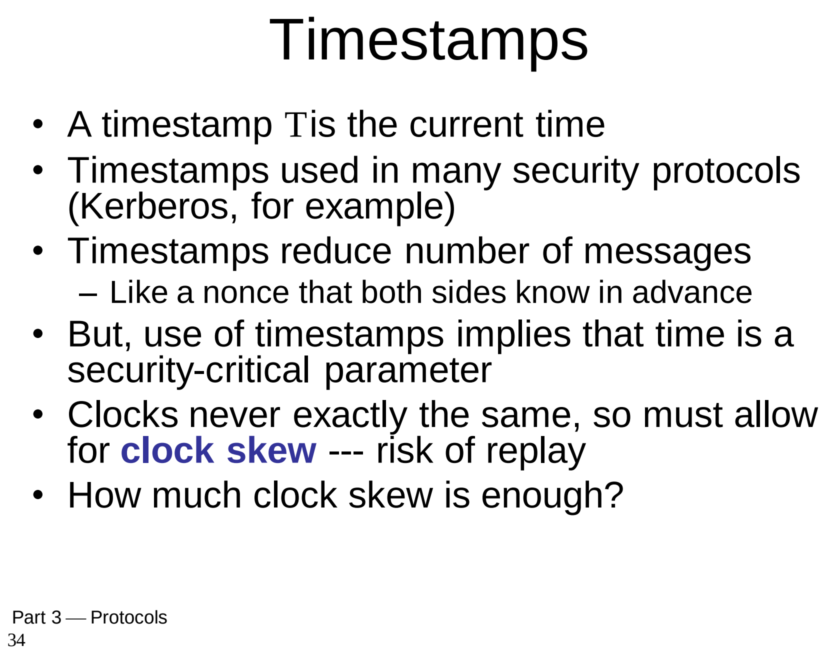
“A”,”B”, $R_{A,}$ A’s cert.

[“A”, $R_{A,}$ R_B , $E_{A,pu}$ $(S_B)]_B$, B’s cert.

[“B”, R_B , $E_{B,pu}$ $(S_A)]_A$

Alice

Bob



Timestamps

- A timestamp Tis the current time
- Timestamps used in many security protocols (Kerberos, for example)
- Timestamps reduce number of messages
  - Like a nonce that both sides know in advance
- But, use of timestamps implies that time is a security-critical parameter
- Clocks never exactly the same, so must allow for **clock skew** --- risk of replay
- How much clock skew is enough?

Part 3 — Protocols
34

8. Whether physical characteristics can be used as an authentication mechanism. If yes justify your answer.

Yes, physical characteristics can be used as an authentication mechanism.

Biometrics(5)

Is the technical term for body measurements and calculations. It refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.

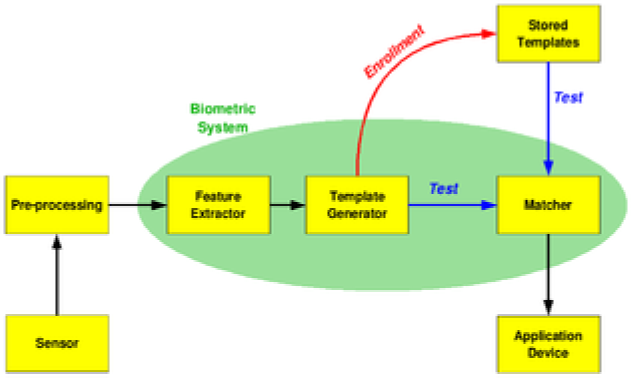
Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.

More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information

Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Jain et al. (1999) identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication.

- Universality means that every person using a system should possess the trait.
- Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.
- Permanence relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm.
- Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.
- Performance relates to the accuracy, speed, and robustness of technology used.
- Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.
- Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute.

Proper biometric use is very application dependent. Certain biometrics will be better than others based on the required levels of convenience and security.[8] No single biometric will meet all the requirements of every possible application.



The block diagram illustrates the two basic modes of a biometric system. First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person. In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using the same identity".

Second, in identification mode the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

The first time an individual uses a biometric system is called enrollment. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the filesize and to protect the identity of the enrollee.

During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area). Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements. In selecting a particular biometric, factors to consider include, performance, social acceptability, ease of circumvention and/or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence. Selection of a biometric based on user requirements considers sensor and device availability, computational time and reliability, cost, sensor size and power consumption.