Seminar on Network Security and Related Research Issues

Dr. Haitham S Cruickshank
http://www.ee.surrey.ac.uk/Personal/H.Cruickshank/
Q: Why do everybody agree that network security is very important, but not many providers are welling to implement it?

Answer: Not understood very well and too complex to implement effectively.
Seminar outline

- Introduction to security basics
- Examples of security systems in communication network
- Overview to IPSec and secure multicast
- Impact of using IPSec on middle entities such as Performance Enhancing Proxies (PEPs)
- Security issues in challenged networks such as Delay Tolerant Networks (DTN)
Existing security technologies

Data Communications

Application layer
Transport layer
Network Layer
Link layer
Physical layer

Application specific security

SSL/TLS
IPsec
ATM/DVB

Application layer
Transport layer
Network Layer
Link layer
Physical layer
Different facets of security

- **Authentication**: validate authentic identity.
- **Authorization**: access control.
- **Integrity**: protection from unauthorized change.
- **Confidentiality or Privacy**: keep information private such that only authorized users can understand it.
- **Availability**: outsider cannot block legitimate access.
- **Non-repudiation**: supply undeniable evidence to prove the message transmission and network access.
Security attacks

- **Passive attacks**: eavesdropping on transmission or monitor and analyze the network traffic.
- **Active attacks**: modification of information, interruption of information transmission and fabrication of messages:
  - Denial-of-service (DoS)
  - Masquerade
  - Man-in-the-middle
  - Replay
Security systems - two categories

❖ Secret-key algorithm:
  – Symmetric: same secret-key is used for both encryption and decryption
  – DES: Data Encryption Standard
  – AES: Advanced Encryption Standard

❖ Public-key algorithm:
  – Asymmetric: different keys are used for encryption and decryption
  – RSA (Rivest, Shamir and Adleman)
Secret-key system: encryption and decryption

plaintext

Encryption Algorithm

Ciphertext

Decryption Algorithm

plaintext
Secret-key system example – Data Encryption Standard (DES)

64 bit plaintext

Initial Transposition

Iteration 1

Iteration 2

Iteration 16

32 bit swap

Inverse transposition

64 bit ciphertext

56 bit key

56 bit ciphertext

32 bit swap

L (i-1)

R (i-1)

L (i-1) + F[R(i-1,K(i)]

32 bit ciphertext

32 bit ciphertext

32 bit

L (i)

R (i)

Secret-key system example

– Data Encryption Standard (DES)
### Other secret-key algorithms

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Author</th>
<th>Key length</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blowfish</td>
<td>Bruce Schneier</td>
<td>1–448 bits</td>
<td>Old and slow</td>
</tr>
<tr>
<td>DES</td>
<td>IBM</td>
<td>56 bits</td>
<td>Too weak to use now</td>
</tr>
<tr>
<td>IDEA</td>
<td>Massey and Xuejia</td>
<td>128 bits</td>
<td>Good, but patented</td>
</tr>
<tr>
<td>RC4</td>
<td>Ronald Rivest</td>
<td>1–2048 bits</td>
<td>Caution: some keys are weak</td>
</tr>
<tr>
<td>RC5</td>
<td>Ronald Rivest</td>
<td>128–256 bits</td>
<td>Good, but patented</td>
</tr>
<tr>
<td>Rijndael</td>
<td>Daemen and Rijmen</td>
<td>128–256 bits</td>
<td>Best choice</td>
</tr>
<tr>
<td>Serpent</td>
<td>Anderson, Biham, Knudsen</td>
<td>128–256 bits</td>
<td>Very strong</td>
</tr>
<tr>
<td>Triple DES</td>
<td>IBM</td>
<td>168 bits</td>
<td>Second best choice</td>
</tr>
<tr>
<td>Twofish</td>
<td>Bruce Schneier</td>
<td>128–256 bits</td>
<td>Very strong; widely used</td>
</tr>
</tbody>
</table>
Message authentication

- A methodology to assure data integrity and to authenticate the data origin.
- **One-way hash function:**
  - A one-way hash function takes an arbitrarily long input message and produces a fixed-length, pseudorandom output called a hash
  - Knowing a hash, it is computationally difficult to find the message that produced that hash
  - It is almost impossible to find different messages that will generate the same hash
- **Message Authentication Code (MAC).**
Message authentication code (MAC)

Hashed MAC (HMAC)

Ipad = repeated 36 in Hex
Opad = repeated 5c in Hex
Public-key system

- **Public key:**
  - Publicly available to anyone

- **Private key:**
  - Only users themselves know their own private keys
Public-key system example – RSA (Rivest, Shamir and Adleman)

Two large prime numbers p and q are chosen 'at random' and multiplied together to form a modulus n

\[ n = p \times q \]

Since it is not possible to factorise large numbers - the modulus can be published without disclosing p and q.

A pair of keys, e = encryption key, d = decryption key, are found by solving the following equation

\[ e \times d \mod (p-1)(q-1) = 1 \]

A message M may then be enciphered with the encryption key e by raising M to the power e modulo n

\[ \text{Ciphertext } C = M^e \mod n \]

This message may be recovered by raising the ciphertext C to the power d modulo n

\[ \text{Message } M = C^d \mod n \]

Simple example
Choose p = 3, q = 11, then n = 33
now (p-1)(q-1) = 20
so e.d mod 20 = 1
choose d = 7 then e = 3
if M = 5 (the message)

\[ C = 5^3 \mod 33 = 26, \quad \text{Encryption} \]
\[ M = 26^7 \mod 33 = 5 \quad \text{Decryption} \]
Integrity and authentication by public-key
Digital signature concept

- Combines a hash with Public-key authentication
Digital certificates

• Certificates bind a public key to a named entity
• Relies on the trust of the certificate authority
• A possible certificate and its signed hash, may look like this:

```
I hereby certify that the public key
19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A
belongs to
  Robert John Smith
  12345 University Avenue
  Berkeley, CA 94702
  Birthday: July 4, 1958
  Email: bob@superdupernet.com
```

SHA-1 hash of the above certificate signed with the CA’s private key
Public-Key Infrastructures (PKI)

RA: Regional Authority
CA: Certification Authority
Diffie-Hellman key exchange protocol - 1

- Diffie-Hellman key exchange protocol allows senders and recipients such as Alice and Bob to exchange a shared secret-key.
- Alice and Bob have to agree on two large prime numbers: n and g where (n - 1) / 2 is prime as well. These numbers can be public, so either of them can pick n and g and tell the other openly.
- Now Alice picks a large number (say 512-bits) x and keep it secret. Similarly, Bob picks a large prime number y.
- Alice initiates the key exchange protocol by sending message M1:
  - M1 = (n, g, gx mod n)
Diffie-Hellman key exchange protocol - 2

- Bob responds by sending message M2:
  - \( M_2 = (g^y \mod n) \)

- Now Alice can calculate the shared secret-key \( K \):
  - \( k = (g^y \mod n) \times \mod n = g^{yx} \mod n = g^{xy} \mod n \)

- Also Bob can calculate the same secret-key \( k \):
  - \( k = (g^x \mod n) \times \mod n = g^{xy} \mod n \)

- The main weakness of Diffie-Hellman protocol is that neither Alice nor Bob can authenticate the origin of messages \( M_2 \) and \( M_1 \) respectively. One solution is to add Alice’s digital signature to message \( M_1 \) and Bob’s digital signature to \( M_2 \).
Examples of Security Systems in Communication Network
The scrambling/descrambling function aims to make the service incomprehensible to unauthorised users:

- Descrambling can be achieved by any receiver having an appropriate descrambler and holding a secret Control Word (CW).

The CW is encrypted with a service key and sent inside a dedicated message (DVB tables) called Entitlement Control Messages (ECMs).

The service key is encrypted with the smart card key and sent inside a dedicated message called Entitlement Management Messages (EMMs).
DVB conditional access - encryption

Conditional Access (CA) system

- Mux
- Smart card processing system
- Subscriber Authorization System (SAS)
- Control Word (CW) generator
- Encryption
- Encryption
- Encryption

- Scrambled & modulated DVB stream to satellite

- Video PES
- Audio PES
- Data PES
- EMM
- ECM
- EMM
- EMM
- EMM
- EMM
- EMM

- Billing & Customer service
- Subscriber Management System (SMS)

- Subscriber
DVB conditional access - descrambling

Satellite input

Tuner

DVB descrambler (uses Control Word (CW))

CW

Demultiplex ECM & EMM

ECM session key / CW

EMM service key

Demultiplexer

ECM decryption algorithm

Smart Card key

EMM decryption algorithm

Smart card

MPEG-2 decoder

Descrambled programme data (Video/audio/text)
Mobile networks - GSM security system

Mobile Station
- Secret Key (K_i) (128-bit)
- SIM

Radio Interface
- Challenge (RAND) (128-bit)
- A8 Algo.
- A3 Algo.
- Response (SRES) (32-bit)
- COUNT (22 bits)
- K_c

Wireless Network
- Random Number Generator (128-bit)
- A3 Algo.
- COUNT (22 bits)
- SRES
- A8 Algo.
- K_c

Encrypted Data (114-bit)
- A5 Algo.
- Plain text

Plain text
Mobile networks - 3G: authentication vector

\[ \text{AUTN} := \text{SQN} \oplus \text{AK} \mathbin{||} \text{AMF} \mathbin{||} \text{MAC} \]

\[ \text{AV} := \text{RAND} \mathbin{||} \text{XRES} \mathbin{||} \text{CK} \mathbin{||} \text{IK} \mathbin{||} \text{AUTN} \]
Mobile networks - 3G: authentication process

RAND

f5: anonymity key generator

SQN □ AK

AMF

MAC

AUTN

f1: MAC algorithm

f2: authentication algo.

f3: cipher key generator

f4: integrity key generator

SQN

XMAC

RES

CK

IK

Send Sync Failure & Abort

Send Reject & Abort

Send Response to VLR

Master Key (K) (128-bit)

MS: Mobile Station

HE: Home Environment

S_{HE} > S_{MS} = ?

S_{HE} ≤ S_{MS}

RES

Send Response to VLR
Network layer security (IPSec)
Internet security - introduction

Internet security is difficult because:
- the internet spans a very wide area across political and organisational boundaries
- it involves how and when communicating parties (such as users, computer, services and network) can trust each other, as well as understanding the network hardware and protocols

Mechanics for Internet security:
- access control using firewalls
- IPSec
- Application layer security
Internet security protocol layers

- Applications
  - Email
  - Higher-level net protocols
    - TCP/IP
  - Data link
  - Physical

- e-commerce protocols
  - S/MIME, PGP

- SSL, TLS, SSH
  - Kerberos
  - IPSEC

- Hardware link encryption

- Internet

- Applications
  - Email
  - Higher-level net protocols
    - TCP/IP
  - Data link
  - Physical
IPSec overview

- **IPSec** provides a set of security services for traffic at the IP layer, in IPv4 and IPv6, through the use of IP Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols.

- **Important IPsec databases:**
  - Security Policy Database (SPD): Defined the protection offered by IPsec: PROTECTed using IPsec security services, DISCARDed, or allowed to BYPASS
  - Security Association Database (SAD): Which encryption and integrity keys are associated with each IP packet

- **Two modes of operations:**
  - **Transport mode:** End-to-end principle is observed
  - **Tunnel mode**
Family of IPSec protocols

IP Security Architecture RFC 4301

- Authentication Header (AH) RFC 4302
  - HMAC-MD5-96 RFC 2403
    - HMAC-RIPEMD-160-96 RFC 2857
  - HMAC-SHA-1-96 RFC 2404
  - DES-CBC (with explicit IV) RFC 2405
- Encapsulating Security Payload (ESP) RFC 4303
  - NULL Encryption Algorithm RFC 2410
  - CBC-mode Cipher Algorithm RFC 2451
- IPsec ISAKMP DOI RFC 2407
  - ISAKMP RFC 2408
  - Internet Key Exchange RFC 4306
  - OAKLEY RFC 2412
# IPSec: Authentication Header (AH)

**IPv4**

<table>
<thead>
<tr>
<th>Original IP header</th>
<th>AH</th>
<th>TCP</th>
<th>Data</th>
</tr>
</thead>
</table>

Transport mode: coverage of authentication (except for mutable fields)

**IPv6**

<table>
<thead>
<tr>
<th>Original IP header</th>
<th>Hop-by-hop extensions</th>
<th>AH</th>
<th>End-to-end extensions</th>
<th>TCP</th>
<th>Data</th>
</tr>
</thead>
</table>

IPv4 and IPv6: coverage of authentication (except for mutable fields)

**Tunnel mode**

<table>
<thead>
<tr>
<th>Encapsulating IP header</th>
<th>AH</th>
<th>Original + ext IP header fields</th>
<th>TCP</th>
<th>Data</th>
</tr>
</thead>
</table>

coverage of authentication (except for mutable fields)
# IPSec: Encapsulated Security Payload (ESP)

### IPv4

<table>
<thead>
<tr>
<th>Original IP header</th>
<th>SPI</th>
<th>Seq Nr.</th>
<th>TCP</th>
<th>Data</th>
<th>Padding</th>
<th>Auth Data</th>
</tr>
</thead>
</table>

- **Coverage of Confidentiality**
- **Coverage of Authentication**

### Transport mode:

### IPv6

<table>
<thead>
<tr>
<th>Original IP header</th>
<th>Hop-by-hop extensions</th>
<th>SPI</th>
<th>Seq Nr.</th>
<th>End-to-end extensions</th>
<th>TCP</th>
<th>Data</th>
<th>Padding</th>
<th>Auth Data</th>
</tr>
</thead>
</table>

- **Coverage of Confidentiality**
- **Coverage of Authentication**

### Tunnel mode: IPv4 and IPv6

<table>
<thead>
<tr>
<th>New IP header</th>
<th>New extensions</th>
<th>SPI</th>
<th>Seq Nr.</th>
<th>Original IP header</th>
<th>TCP</th>
<th>Data</th>
<th>Padding</th>
<th>Auth Data</th>
</tr>
</thead>
</table>

- **Coverage of Confidentiality**
- **Coverage of Authentication**
IPSec applications

- End-to-end security
- VPN (virtual private network) with IPsec (Satellite example)
- End-to-end with VPN security
- Secured remote access
Limitations of IPSec - problems with middle entities

- **IPSec in transport mode** encrypts all data above IP layer. **IPSec in tunnel mode** encrypts all data including the original IP layer. However it conflicts with:
  - **Satellite bandwidth acceleration**: Performance Enhancing proxies (PEPs) need to inspect TCP and HTTP header.
  - **Traffic Analysis**: Service provider might require monitoring of their network traffic for management and QoS purposes.
  - **Traffic Engineering**: Flow classification is essential in supporting a variety of classes of service and QoS.
## Secure Sockets Layer (SSL)

<table>
<thead>
<tr>
<th>Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application (HTTP)</td>
</tr>
<tr>
<td>Security (SSL)</td>
</tr>
<tr>
<td>Transport (TCP)</td>
</tr>
<tr>
<td>Network (IP)</td>
</tr>
<tr>
<td>Data link (PPP)</td>
</tr>
<tr>
<td>Physical (modem, ADSL, cable TV)</td>
</tr>
</tbody>
</table>
SSL - Connection establishment

1. SSL version, Preferences, $R_A$
2. SSL version, Choices, $R_B$
3. X.509 certificate chain
4. Server done
5. $E_B$ (Premaster key)
6. Change cipher
7. Finished
8. Change cipher
9. Finished
SSL – Data transmission

Message from browser

Fragmentation

Part 1

Compression

Part 2

MAC added

Message authentication code

Encryption

Header added
Example multicast applications

- Digital TV
- Satellite mobile (military/civil)
- 3G mobile
- Wide Area Internet Multicast
Secure group communications

- The IPSEC standards and its related technologies, are aimed mainly at unicast transmissions between one sender and one receiver:
  - Securing multicast is a difficult issue because it involves group communications

- MSEC is an IETF Working Group focusing on standardizing building blocks and protocols for secure group communications and multicast.

- In addition, there is a Research Group called GSEC which is an IRTF (Internet Research Task Force) group formed to discuss research issues related to multicast security.
Factors affecting secure multicast

• **Applications**: One-to-many and many-to-Many

• **Group dynamics**: Size and behaviour

• **Trust model**: Security policies and key management

• **Critical issues**:  
  - Secure group management  
  - Key distribution for large groups
Secure Multicast architecture - Centralised

- Multicast security policies
- Group key management
- Multicast data handling

Diagram:
- Policy server
- Group Controller/Key Server
- Receiver
- Sender

Flow of information:
- Policy server to Group Controller/Key Server
- Group Controller/Key Server to Receiver
- Receiver to Sender
- Sender to Group Controller/Key Server
Secure Multicast architecture - Distributed

Policy server

Group Controller/Key Server

Receiver

Sender

Policy server

Group Controller/Key Server

Receiver

Multicast security policies

Group key management

Multicast data handling
Group key management protocols

- **Group Secure Association Key Management Protocol (GSAKMP):**
  - It includes mechanisms for group policy dissemination, group key dissemination, and group rekey operation

- **Multimedia Internet KEYing (MIKEY):**
  - The MIKEY protocol is used for peer-to-peer, simple one-to-many, and small-size (interactive) groups, and is intended for use in real-time applications. One of the main multimedia scenarios is the conversational multimedia scenario, where users may interact and communicate in real-time

- **Group Domain of Interpretation (GDOI):**
  - GDOI (RFC 3547) is an ISAKMP Domain of Interpretation (DOI) for group key management to support secure group communications. It proposes new exchanges according to the ISAKMP and IKE standard
GSAKMP message sequence

- **Group Controller (GC)**
- **Group Member (GM)**

**Group establishment** (once per GM)
- Request to join
- Key download
- Notification (acknowledgement)

**Group maintenance** (repeat as necessary)
- Server rekey

**Group removal**
- Group removal / destruction
Key distribution:
Logical Key Hierarchy (LKH) - 1

- RFC 2627 defines the Logical key hierarchy (LKH) as a mechanism for improving the scalability of multicast key management.
- LKH provides the following two features:
  - Secure removal of a compromised user from the multicast group.
  - Key transmission efficiency.
Key distribution: Logical Key Hierarchy (LKH) - 2

Key hierarchy

(a)
LKH – Tree (user 4 joins)
LKH – Tree (group rekey)

Key hierarchy

Group members

Group key

Rekey

Unchanged

Unchanged
LKH – Tree (removal of member 4)

Key hierarchy

Group members

Group key

Rekey

Unchanged

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Screen capture for LKH

RFC 2627 rekey messages
16 users = 7
2048 users = 21
131072 users = 33

Rekey messages = $2\log_2^{N} - 1$
16 users = $2^4$
2048 users = $2^{11}$
131072 users = $2^{17}$
1 million users = $2^{20}$
Performance Enhancing proxies (PEPs)
ETSI - BSM Architecture

- The Broadband Satellite Multimedia (BSM) architecture divides the protocol stack into 2 parts:
  - Satellite Independent (SI) upper layers
  - Satellite Dependent (SD) lower layers

- The upper layers contain a set of common IP interworking functions:
  - Define Satellite Independent Adaptation Functions (SIAF)
  - Common ways of handling Quality of Service (QoS); Addressing; Multicast and Security etc.

- **Satellite Independent Service Access Point (SI-SAP)** defined as a common interface between the upper and lower layers.

- The lower layers contain the satellite specific functions:
  - The lower layers are closely tied to the payload capability of the satellite
BSM Protocol Stack

IPv4 and IPv6

- IP Routing
- IP Route Determination

IP Packet Forwarding

- IP QoS Management
- IP Security

SIAF

- BSM Address Resolution
- BSM Routing Adaptation
- BSM Connection CTRL

- SDAF
- Satellite Data Unit Switching

- SI-U-SAP
- SI-C-SAP
- SI-M-SAP

Satellite Link Control (SLC)

Satellite Medium Access Control (SMAC)

Satellite Physical (SPHY)
Performance Enhancing Proxies (PEPs) types and layering

- **Transport Layer PEPs (T-PEP):** T-PEPs interact with TCP. Such an implementation is sometimes called TCP Performance Enhancing Proxy (TCP PEP). The term TCP spoofing is sometimes used synonymously for TCP PEP functionality.

- **Application layer PEPs (A-PEP):** Application layer PEPs operate above the transport layer. An example of application layer proxy is a Web cache. A-PEPs can be implemented to improve the HTTP performance over wireless links.
T-PEP and A-PEP mechanisms

- **TCP ACK Spacing**: In environments where ACKs tend to bunch together, ACK spacing is used to smooth out the flow of TCP acknowledgments traversing a link.

- **Local TCP Acknowledgements**: In some PEP implementations, TCP data segments received by the PEP are locally acknowledged by the PEP.

- **Local TCP Retransmissions**: A TCP PEP may locally retransmit data segments lost on the path between the TCP PEP and the receiving end system.

- **Browser Cache Leveraging**: Caching some web pages not residing in browser cache, improving efficiency.

- **HTTP pre-fetching**: Intercepting requested Web pages, identifying Web objects referred to by the Web pages, downloading these objects in anticipation of the next user requests.
Security issues in PEPs

- Security can be applied in application, transport (SSL), IP (IPSec) or link layers:
  - However, security must allow T-PEP access to the transport protocol headers and A-PEPs access to application layer contents (e.g., web pages).

- This implies that IPSec and SSL can be applied in limited cases.

- Satellite link layer security can be applied transparently to T-PEPs and A-PEPs.
Successful T-PEP (not A-PEP) with end-to-end SSL
Successful T-PEP and A-PEP with IPSec - 1
Successful T-PEP and A-PEP with IPSec - 2
Successful PEPs with link layer security
Limitations of IPSec - problems with middle entities - revisited

- **IPSec in transport mode** encrypts all data above IP layer. **IPSec in tunnel mode** encrypts all data including the original IP layer. However it conflicts with:
  - Satellite bandwidth acceleration: Performance Enhancing proxies (PEPs) need to inspect TCP and HTTP header.
  - Traffic Analysis: Service provider might require monitoring of their network traffic for management and QoS purposes.
  - Traffic Engineering: Flow classification is essential in supporting a variety of classes of service and QoS.

- **A solution Multi Layer IPSec (ML-IPSec)**: divides the IP datagram into several zones and apply different protection schemes to each zone.
Multi Layer IPSec (ML-IPSec) - design

<table>
<thead>
<tr>
<th>IP HEADER</th>
<th>TCP/UDP HEADER</th>
<th>TCP/UDP DATA</th>
<th>ESP HEADER</th>
<th>TCP/UDP HEADER</th>
<th>TCP/UDP DATA</th>
<th>ESP TRAILER 1</th>
<th>ESP TRAILER 2</th>
<th>ESP AUTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone 1</td>
<td>Zone 2</td>
<td>Encrypted</td>
<td>Zone 1 (k1)</td>
<td>Zone 2 (k2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ML-IPSec: zone map
Interworking between ML-IPSEC and LKH

Key hierarchy

Users

Group key K1
(for transport layer header)

Group key K2
(for transport layer data)
Delay/Disruption Tolerant Networks (DTN) - security
Delay/Disruption Tolerant Networking (DTN - Introduction)

- DTN is an overlay network architecture which runs on top of heterogeneous networks.
- It provides good services in high delay/disruption environments. It originated within the Inter Planetary research community.
- It has three main components:
Example DTN scenario: UN monitoring in disaster and conflict areas
DTN security issues

- Current security protocols such as IPSec and TLS (or SSL) do not perform well in high delay/disruption conditions because of the following assumptions:
  - end-to-end connectivity is always present
  - low link delays
  - low error rate on link channels
DTN Security Architecture

- DTN security architecture provides hop-by-hop authentication and end-to-endish authentication, integrity, and confidentiality.

- It has several blocks (headers) to provide these security services.
  - Bundle Authentication Block (BAB): hop-by-hop authentication & integrity
  - Payload Integrity Block (PIB): end-to-endish authentication and integrity
  - Payload Confidentiality Block (PCB): end-to-endish confidentiality
Internetworking of heterogeneous networks using DTN Gateways
DTN security: Hop-by-Hop authentication

- Pre-Shared Key (Public or Symmetric)
- Security Zone 1
- Security Zone 2
- Security Zone 3

BN1

BN2

BN3

BN4

Stack

Bundle Primary Block

Bundle Authentication Block 1

Bundle Payload

Stack

Bundle Primary Block

Bundle Authentication Block 1

Bundle Payload

Stack

Bundle Primary Block

Bundle Authentication Block 3

Bundle Payload

Stack

Remove BAB 1 to verify integrity & authenticate
Append BAB 2 for authentication & integrity

Remove BAB 3 to verify integrity & authenticate

Append BAB for Authentication & Integrity
DTN security: End-to-End authentication and integrity
DTN security: End-to-End confidentiality
Open research issues in DTN security

- Lightweight key management
- Lightweight AAA-like architecture for authentication/authorisation
- Resilience to Denial of Service (DoS) attacks
- Providing anonymity to end users for some services/applications
### Summary - security layers comparison

<table>
<thead>
<tr>
<th>Major advantages</th>
<th>Link layer</th>
<th>Network layer</th>
<th>Transport layer</th>
<th>Application layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete control of the link security</td>
<td>IPSec is the best solution for Internet security</td>
<td>Widely used for securing TCP connections</td>
<td>Can satisfy applications requirement very well</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Major disadvantages</th>
<th>Link layer</th>
<th>Network layer</th>
<th>Transport layer</th>
<th>Application layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only the one link hop is secure</td>
<td>IPSec works only for IP networks</td>
<td>No security for UDP and multicast</td>
<td>No transparency, where applications need modification to fit security</td>
<td></td>
</tr>
</tbody>
</table>
## Summary - security services at various protocol layers

<table>
<thead>
<tr>
<th></th>
<th>Link layer</th>
<th>IP Network layer</th>
<th>Transport layer</th>
<th>Application layer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Terminal authentication</strong></td>
<td>Yes</td>
<td>Yes (IP address)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Host authentication</strong></td>
<td>No</td>
<td>Yes (IP address)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>User authentication</strong></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Link privacy</strong></td>
<td>Yes</td>
<td>Yes (IPSec IP tunnel)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>End to end privacy</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Link data integrity</strong></td>
<td>Yes</td>
<td>Yes (IPSec IP tunnel)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>End to end data integrity</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>