Networked System Security

Data Plane Security

Panos Papadimitatos
Networked Systems Security Group
www.ee.kth.se/nss

Outline

- Problem definition
- Data plane security in wired Internet
  - IPSec
  - TCP security options
  - SCTP
- Data plane security in wireless networks
  - SSP
  - SMT
  - CASTOR

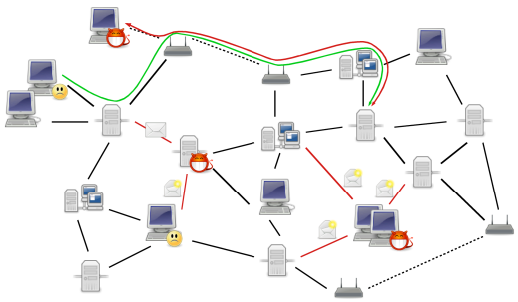
Problem definition

- In-transit data tampering
  - Routers/switches can
    - Drop data packets
    - Delay data packets
    - Modify packets
  - Adversary controls one (or more) router(s)/switch(s)
- Data forgery, injection, and replay
  - By routers/switches or end hosts
  - End hosts can take over/hijack connection/session of other hosts
  - Adversary controls one (or more) router(s)/switch(s) or end-hosts

Problem definition (cont'd)

- Attacks at different layers
  - Data link
  - Network
  - Transport
  - Application
- Focus in this lecture
  - Network and transport
  - Focii: wired and wireless networks

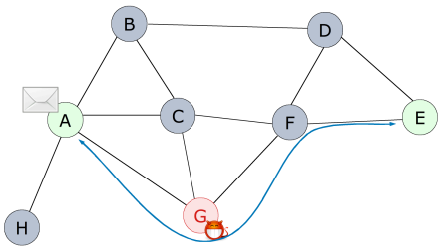
Problem definition (cont'd)



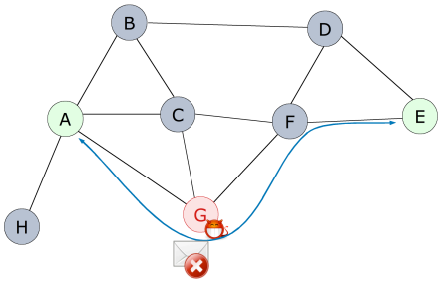
Problem definition (cont'd)

- Secure routing vs. data-plane attacks?
  - Recall: attacks against routing help the adversary become part of routes
  - Once on a route, the adversary can manipulate data at will
  - What if secure routing were fully addressed?
    - Still, data-plane attacks can be mounted
- Main difference between current Internet and emerging networks?
  - Route selection in Internet is not coupled with detection of data-plane faults (benign or malicious)
  - Emerging networks give the flexibility to design adaptive solutions

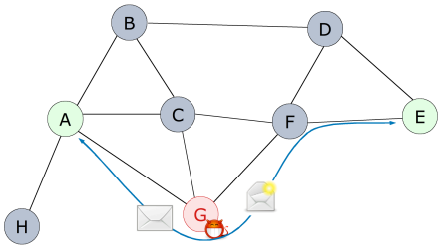
Problem definition (cont'd)



Problem definition (cont'd)



Problem definition (cont'd)



Problem definition (cont'd)

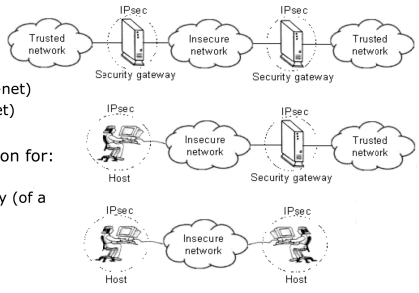
- How can an attacker be part of a route?
  - Make the route appear 'preferable' (shorter in hops, delay, or any other metric)
  - Other routing protocol-specific attacks (e.g., 'rushing')
  - Do nothing that disrupts the secure route discovery
- Consider
  - An ideal secure routing protocol, ensuring loop-free, fresh, and accurate routes against any possible attack
  - All nodes on the discovered route authenticated
- Still, the attacker can deny communication, dropping packets
- Worse even, the attacker can choose to hit when it hurts the most

IPsec: Internet Protocol Security

- Rationale: Security at the network layer
- Encrypt/authenticate IP packets
  - Authentication using Authentication Header (AH)
  - Encryption+Authentication using Encapsulating Security Payload (ESP)
  - Uncommon to use both AH and ESP for the same datagram
- Key establishment with the Internet Key Exchange (IKE) protocol/framework

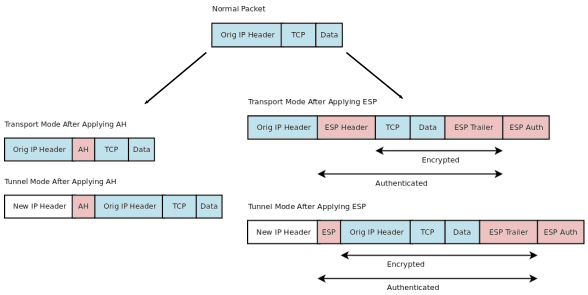
IPsec (cont'd)

- Network
  - Untrusted (Inter-net)
  - Trusted (Intra-net)
- Security Association for:
  - Two gateways
  - Host and gateway (of a trusted network)
  - Two hosts



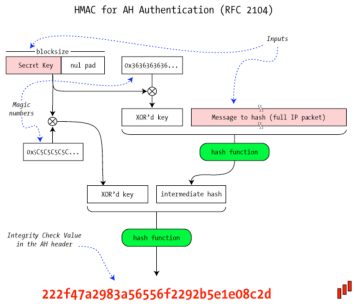
src: hsc

IPsec (cont'd)



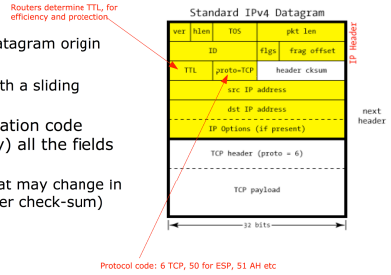
Authentication Algorithm

- Authentication Data
  - Part of the AH
- Use SHA-1
  - Recall: a check-sum alone provides no protection against intentional tampering

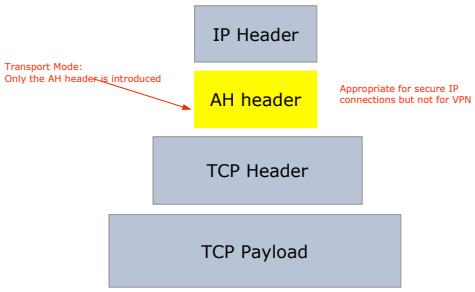


Authentication Header (AH)

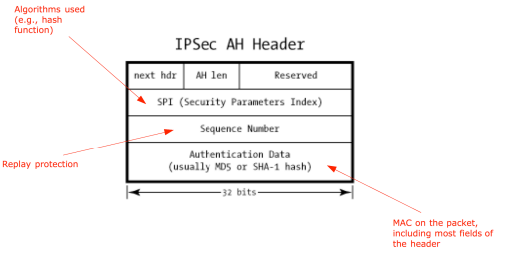
- Used to
  - Authenticate IP datagram origin
  - Ensure integrity
  - Detect replays, with a sliding window technique
- Message authentication code (MAC) over (nearly) all the fields of the IP packet
  - Excluding ones that may change in transit (TTL, header check-sum)



Transport Mode: AH



Authentication Header (AH) (cont'd)



Secure Tunneling

- Encapsulation of datagram entering the "tunnel" and decapsulation at the other end-point

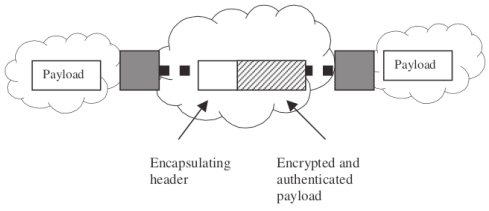
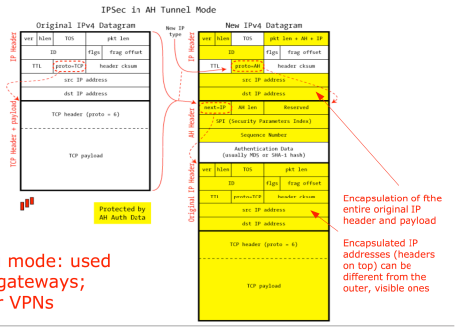


Image taken from book "Network security: current status and future directions", Christos Douligeris, Dimitrios N. Serpanos

Tunneling Mode: AH

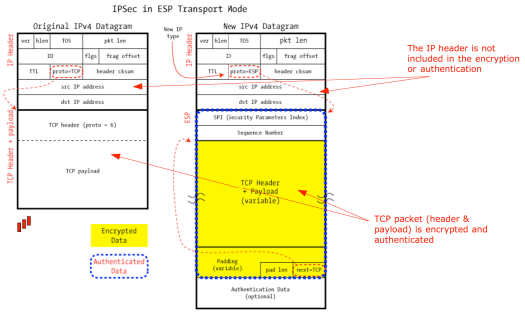


Tunneling mode: used between gateways; typical for VPNs

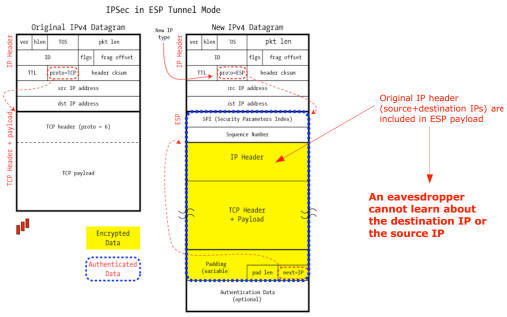
Encapsulating Security Payload (ESP)

- ESP surrounds the packet payload; it does not precede it as in AH
- Encryption algorithms include blowfish, DES, 3DES, AES
- Authentication is optional
  - Performed using hashing techniques (as in AH)
- It is possible encryption is not used; then authentication is required

Transport Mode: ESP



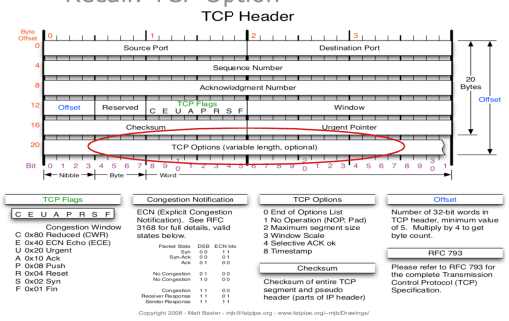
Tunnel Mode: ESP



IPsec and VPNs

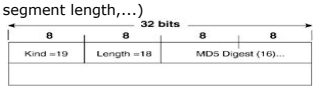
- Advantages
  - The user accessing the VPN can be authenticated
  - All user traffic can be authenticated and encrypted
  - Available key establishment framework

Recall: TCP Option



TCP-MD5

- Developed to enhance security for BGP [RFC 2385]
- New TCP option (19) for carrying an MD5 digest in a TCP segment
  - MD5 digest is 16 bytes long
  - Signature for that segment
  - Information known only to the connection end points
- Digest
  - TCP pseudo-header (src/dest IP, segment length,...)
  - TCP header excluding options
  - TCP segment data
  - Independent key/password



src: flylib

TCP Authentication Option (AO)

- New Authentication Option [RFC 5925], obsoletes TCP-MD5
- Stronger Message Integrity Codes (MICs)
- Protects against replays even for long-lived TCP connections
- IPv6 compatible
- Field
  - Kind = 29
  - Length of the option in bytes
  - KeyID indicates the master key used for generate the traffic keys
  - RnextKeyID indicates the master key of the sender (for receive data)
  - MIC is the value of e.g. SHA or other cryptographic MIC

TCP-MD5 (cont'd)

- TCP-MD5
  - Cryptographically weak (MD5)
  - No key establishment readily available (also for the TCP-AO)
- IPsec
  - Hard to use for specific applications
  - Hard to use with NAT
- TLS
  - No protection of the TCP header
    - Easy to destroy TCP sessions by packet injection

Stream Control Transmission Protocol (SCTP)

- Standard transport protocol (RCF 2960)
- Alternative to TCP and UDP
  - They lacked some needed features
  - High availability
    - Fail-over between multiple redundant networks interfaces
  - Minimum delay
    - Real-time
  - Message oriented

SCTP (cont'd)

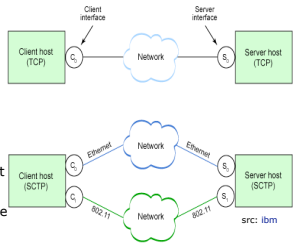
- Why SCTP?
  - Transport layer sits between IP and the application
  - Traditionally, just two choices
    - UDP: bare minimum
      - Just port numbers and optional check-sum
      - No flow control, no congestion control, no reliability or ordering
    - TCP: a package deal
      - Flow control, congestion control, byte-stream orientation
      - Total ordering and reliability

SCTP (cont'd)

- SCTP can do
  - Reliable, flow controlled, congestion controlled data exchange (TCP)
  - Unordered, unreliable data exchange (UDP)
- But also
  - Multi-homing
  - Multi-streaming
  - Message boundaries
  - Improved SYN-flood protection
  - Tunable parameters
  - A range of reliability and order (full, to partial, to none) along with congestion control

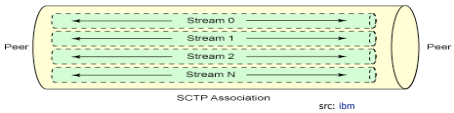
SCTP (cont'd)

- Multi-homing (improved robustness to failures)
  - TCP
    - Connections are made between <IP src, port> and <IP dest, port>
    - If a host is multi-homed you have to choose ONE IP
    - If that interface goes down, so does the connection
  - SCTP
    - List as many IP address per endpoint as you like
    - It is enough the host is still reachable through ANY of those addresses



SCTP (cont'd)

- Multi-streaming (reduced delay)
  - Partial ordering
  - Sends independent streams
    - Each ordered independently
  - A loss on one stream does not delay the delivery on other streams

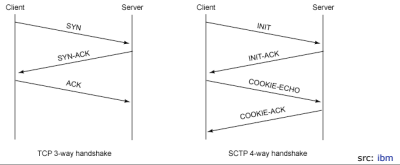


src: ibm

- Message boundaries preserved (easier coding)
  - TCP re-packetizes data, SCTP does not
    - Application protocols are easier to write

SCTP (cont'd)

- Improved SYN-flood protection (more secure)
  - Remember the TCP SYN flood?
  - SCTP uses the four way handshake
    - Connection needs to be validated



src: ibm

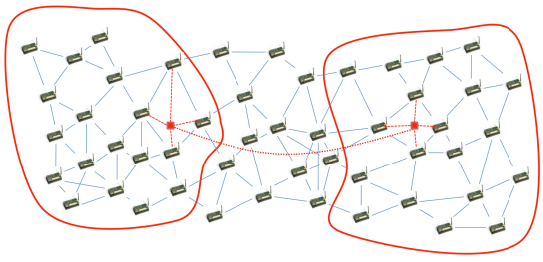
SCTP (cont'd)

- Tunable parameters (more flexibility)
  - For tuning, TCP requires *admin* privileges, kernel hacking / changes
  - SCTP parameters can be tuned on a per socket basis
- Congestion controlled unreliable/unordered data (more flexibility)
  - TCP has congestion control but cannot do unreliable/unordered delivery
  - UDP can do unreliable/unordered delivery, but not congestion control
  - SCTP
    - Always congestion-controlled
    - Range of services: from full reliability to none; full ordering to none
    - Reliable and unreliable data can be multiplexed over the same connection

Attacks Types (cont'd)

- Blackhole Attack
  - All the traffic passing through the attacking node is silently discarded (dropped)
- Grayhole Attack
  - A selected portion of the traffic passing through the node is silently discarded (dropped)
- Wormhole Attack (**more relevant to wireless networks**)
  - Tunneling of messages over alternative low-latency links to confuse the routing protocol, thereby creating sinkholes, etc
  - At the physical layer or other links
  - Distinction: Not the tunneling attack (recall: secure routing module)

Example: Wormhole Attack

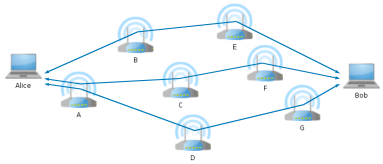


Securing Data Communication

- Goal
  - Reliable and low-delay data delivery in the presence of attackers that disrupt the data communication
- Solution
  - Detect and avoid compromised and failing routes
  - Tolerate malicious and benign faults
    - In general, hard to distinguish in highly dynamic networking environments
- Notes
  - Goal: more demanding that best-effort
  - Solution: necessitates control over routing decisions (or coordination)
    - Decoupling of routing and data (end-to-end) communication in wired networks
    - Possible in wireless ad hoc networks

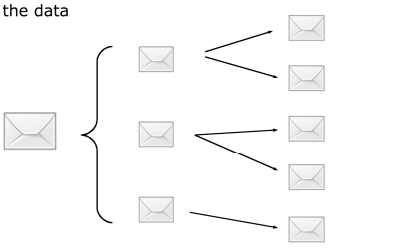
Securing Data Communication (cont'd)

- Use multiple routes



Securing Data Communication (cont'd)

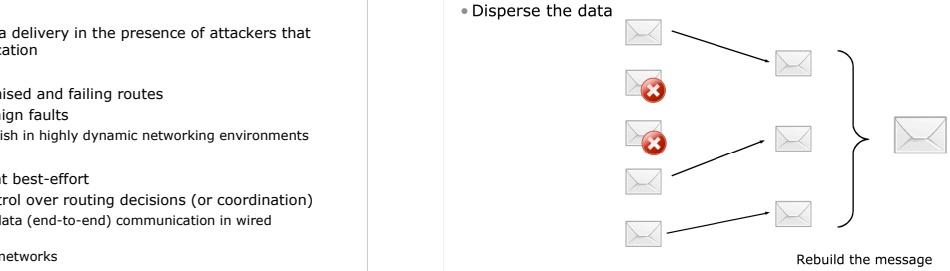
- Disperse the data



Original Message Introduce *redundancy*

Securing Data Communication (cont'd)

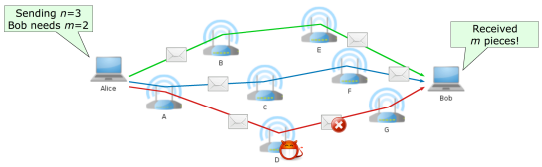
- Disperse the data



Rebuild the message

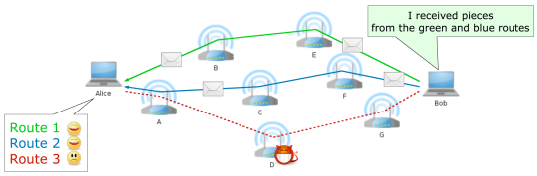
Securing Data Communication (cont'd)

- Transmit simultaneously across the routes



Securing Data Communication (cont'd)

- Bob provides a feedback for Alice



Securing Data Communication (cont'd)

- Secure Message Transmission (SMT) protocol
  - Dispersion of the transmitted data
  - Simultaneous usage of multiple node-disjoint routes
  - Data integrity and origin authentication
  - End-to-end secure and robust feedback
  - Adaptation to the network conditions
- Secure Single Path (SSP) protocol
  - Discovery and utilization of a single route
  - End–to–end security and feedback

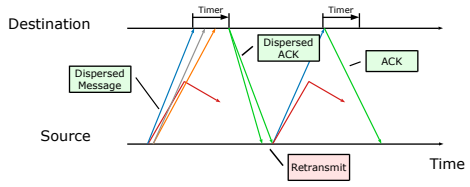
P. P. and Z.J. Haas, *"Secure Data Communication in Mobile Ad Hoc Networks"*, IEEE JSAC, 2006
P. P. and Z.J. Haas, *"Secure Message Transmission in Mobile Ad Hoc Networks"*, ACM WiSe, 2003
P. P. and Z.J. Haas, *"Secure Message Transmission in Mobile Ad Hoc Networks"*, Ad Hoc Networks, 2003

SMT Operation (cont'd)

- The Active Path Set (APS)
  - Maintain a (partial) view of the network topology
  - Construct a set of node disjoint routes (per destination)
  - Routes remain in the APS until deemed non-operational
- Multi-path operation
  - Select the APS routes to transmit a dispersed message
  - Route selection attributes
    - Path rating
    - Probability of path survival
    - Overall probability of successful message delivery
  - Assign each message piece to one of the selected routes

SMT Operation (cont'd)

- Example: Transmission of a single message



SMT Operation (cont'd)

- Secure and robust end-to-end feedback
  - Dispersed and returned over multiple routes
  - Informs on the successfully received pieces
  - Allows the correlation of successfully received pieces with data routes
  - Provides "safe" information for the adaptation of the protocol operation
- Adapt to the network conditions
  - Detect non-operational routes
  - Switch to alternate (new) routes
  - Adapt the protocol configuration
    - Number of routes
    - Transmission redundancy
    - Route selection
    - Additional route discovery

SMT Operation (cont'd)

- Path rating mechanism
  - Each route is associated to a rating $r_s \in [r_s^{thr}, r_s^{max}]$
  - Update r_s for each transmission across the route
  - For each delivered piece, r_s is increased by a constant β
  - For each lost piece, r_s is decreased by a constant α
  - The route is discarded when its rating reaches r_s^{thr}
- $$r_s(i) = \begin{cases} \max\{r_s(i-1) - \alpha, r_s^{thr}\}, & \text{if a piece is lost} \\ \min\{r_s(i-1) + \beta, r_s^{max}\}, & \text{if a piece is received} \end{cases}$$

SMT Operation (cont'd)

- Robustness to arbitrary attack patterns
  - Bounded fraction of data the adversary can drop (Bandwidth Loss (BWL)) before the compromised route is detected

    BWL ≤ β / (α – β)

  - Non-operational routes are promptly discarded
  - Route reinstatement after transient data loss

SMT Operation (cont'd)

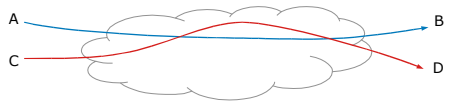
- What is the appropriate choice for α, β?
  - The attack pattern is not known in advance
  - The faster a non-operational route is discarded the better
  - Not discarding a route after a transient packet loss is preferable
  - One criterion: Min-Max Regret

CASTOR

- Continuously Adapting Secure Topology-Oblivious Routing
  - Integrated route discovery and data communication
  - Localized, autonomous routing decisions
  - Simplest security associations (as for SRP+SSP/SMT)
  - Failure agnostic operation (as for SRP+SSP/SMT)
  - Bandwidth for security: "When in the dark, broadcast (but only for a short time)"
  - Outcome: Enhanced scalability and resilience

W. Galuba, P. P., M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "*Castor: Scalable Secure Routing for Ad hoc Networks*", IEEE INFOCOM 2010

CASTOR (cont'd)



- End-to-end (EtE) and neighbor-to-neighbor (NtN) security associations
- EtE and NtN authentication only
- No routing packets, only data (PKTs) and acknowledgements (ACKs)
- In-network state updated based on PKTs and ACKs
- Crucial feature: flow isolation

Summary

- Data security
  - Integrity, authenticity, confidentiality of communication
    - Primarily; non-repudiation may be needed
  - Fault tolerance
  - Necessary even if secure routing (secure route discovery) is achieved
  - Reliable and timely and secure delivery of data
  - Flexibility to choose routes is a major plus
    - Possible in emerging, possibly flat networks
    - Hard in traditional internet