IPSec
Internet Protocol Security

Mario Baldi

Synchrodyne Networks, Inc.

http://www.mario-baldi.net

Nota di Copyright

Overview

- Application layer security
  - Security e-mail
    - S/MIME
  - DNS security extensions
  - SSH (Secure SHell): secure telnet
- Transport layer security
  - SSL (Secure Socket Layer)
- Network layer Security
  - IPSec
    - Protection of IP, TCP, and UDP headers
    - Authentication of IP, TCP, and UDP headers

Security Objectives

- Confidentiality
  - No unauthorized access
- Integrity
  - No unauthorized modification
- Authentication
  - No source faking (spoofing)
- Non repudiation
  - No pretending not to be the source

IPsec

- A framework to address security issues
  - Standard
  - Flexible
- Based on chryptography
- Tunneling is possibly used
- Transparent to applications
  - Transparent to users

IPsec and Chryptography

- One shared pair of session keys per communicating direction
  - one for data encryption
  - one for authentication
- Shared keys must be agreed upon
- Session keys are changed regularly to increase robustness
- Key exchange
  - Manual (out-of-band)
  - Dynamic, automatic: IKE

Security Association (SA)

- Agreements that enable data exchange
- An exchange providing authentication and privacy requires a separate SA for each

An SA includes

- Session keys
- IP address of each endpoint
  - It can be a subnet prefix
- IP address of each IPSec gateway
- Expiration of session keys
  - Upon session keys expiration a new Security Association is to be created

IKE (Internet Key Exchange)

- Means to agree upon
  - Protocols
  - Algorithms
    - Encryption
      - DES
      - 3DES
      - RC5
      - Cast
    - Authentication: message digest
      - MD5
      - SHA1
  - Keys
    - Shared secret
      - Communicated off-line
    - Digital certificates

IKE (Internet Key Exchange)

- Authentication of other communicating party
  - E.g., tunnel endpoint
- Digital certificates to validate public keys
  - Including authentication of communicating party
- Key exchanges
  - Diffie-Hellman algorihm
  - Public key cryptography to sign key exchanges
    - Guarantees for identities of the two parties
  - DES (Data Encryption Standard) to encrypt keys being exchanged

IKE (Internet Key Exchange)

Combines various standards (confusing)

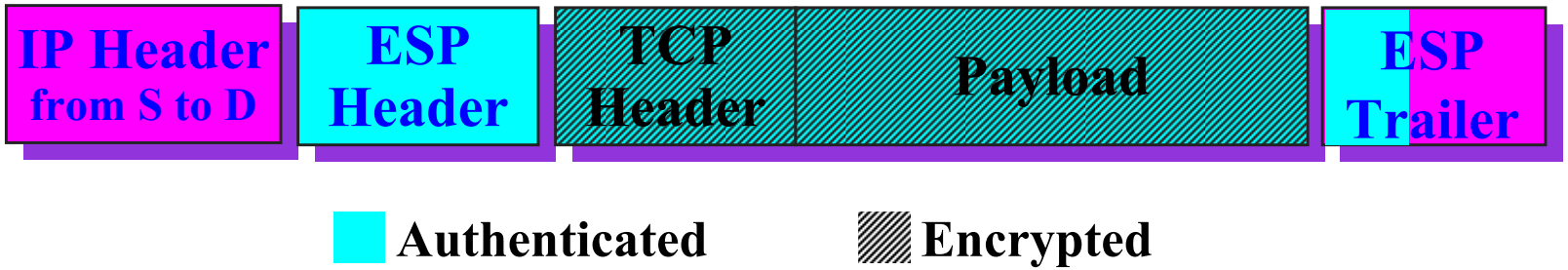
- ISAKMP: Internet Security Association and Key Management Protocol
  - Generic negotiation protocol
  - Packet format and protocol description
- DOI: Domain of Interpretation
  - IPsec specific interpretation of ISAKMP
- OAKLEY
  - Key management framework
  - Canonical key negotiation sequences
- SKEME
  - Key management framework
  - Parts used within IKE

Implementation

- Client implementation
- Gateway implementation
  - Software: on firewall or router
  - Hardware: special purpose box
- Algorithm independence

Transport Mode Encapsulation

- Host to host communications
- Information between ESP (Encapsulation Security Payload) header and trailer is encrypted
  - Security Parameter Index (SPI)
    - Pointer in SA database → encryption type
- ESP trailer: authentication
  - Message authentication code (MAC)
  - From transport (TCP/UDP) to MAC (excluded)



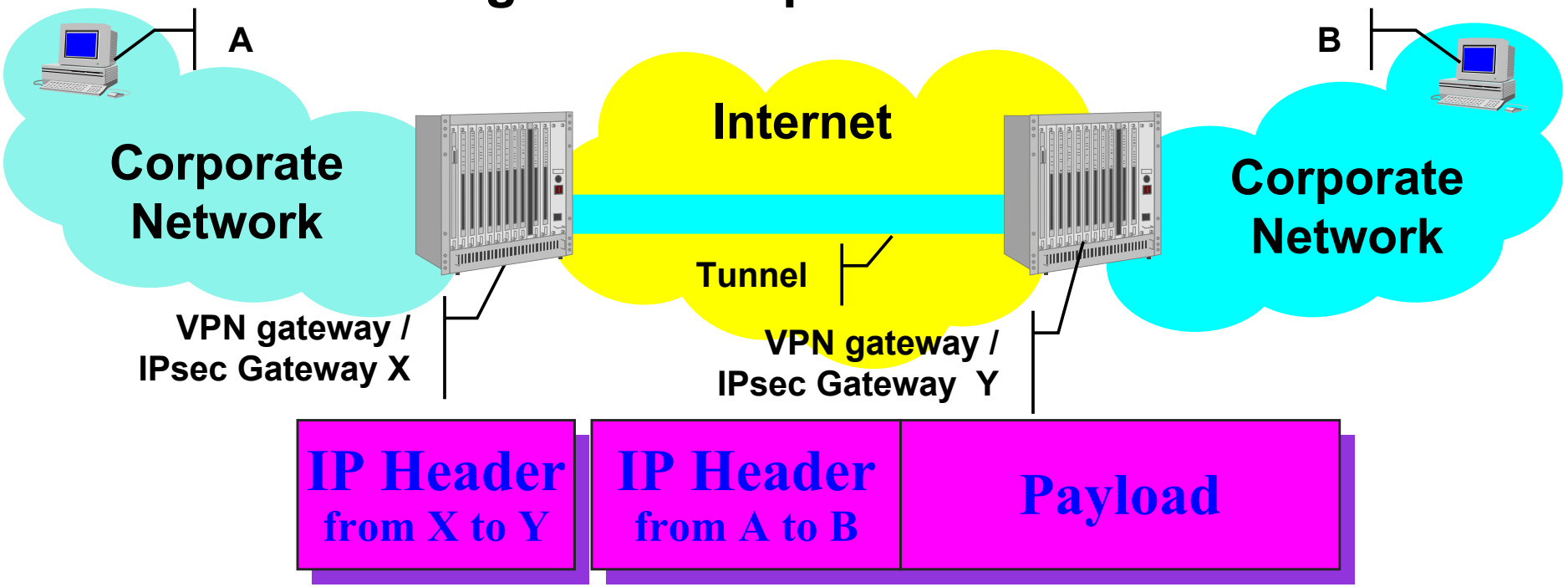
Transport Mode Encapsulation

- Authentication header
  - SPI
  - With or without ESP
  - MAC over the entire packet
    - no TTL, ToS, fragmentation information, etc.

Authenticated Encrypted

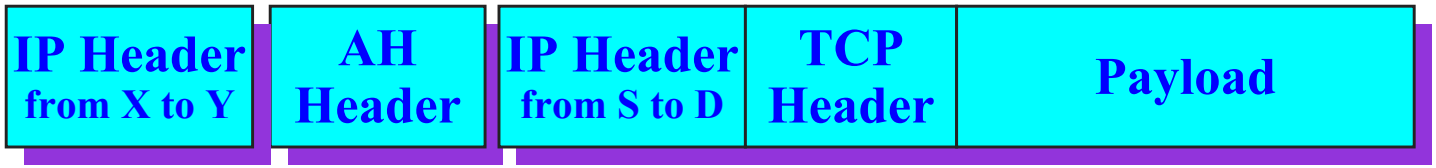
(IPsec) Tunneling

- IPsec tunneling ensures security
- Deployed in IPsec VPNs
  - A and B are enterprise addresses
    - they do not have to satisfy the public system requirements
  - Tunneling enables operation



Tunnel Mode Encapsulation

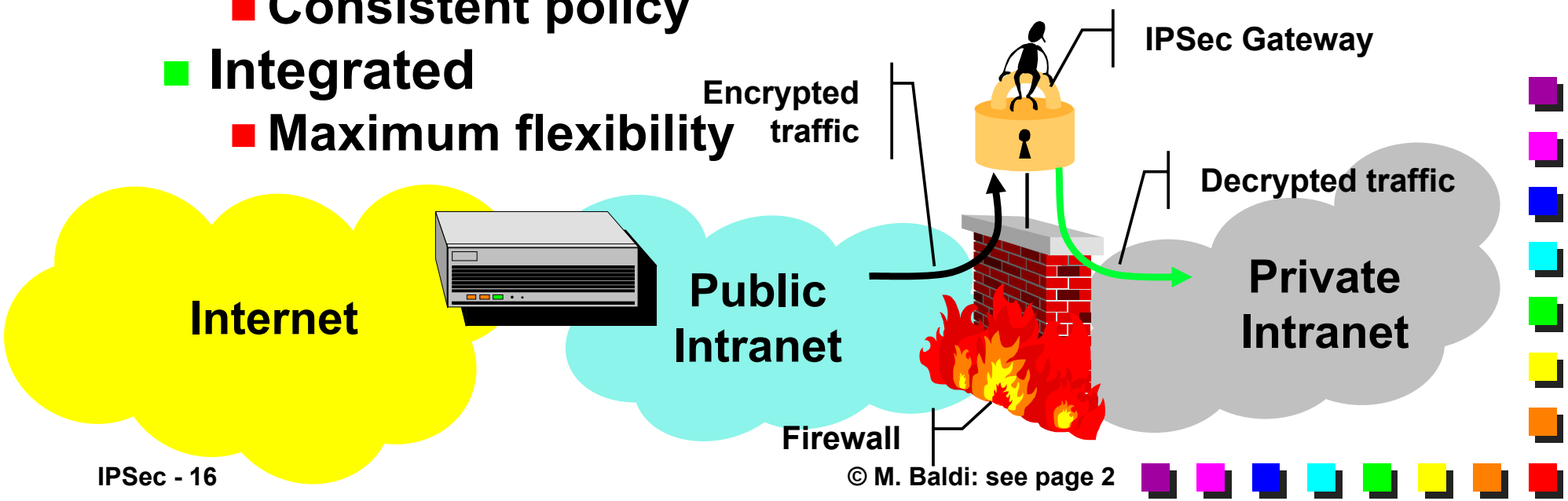
- Gateway (X) to gateway (Y) communications



Authenticated Encrypted

IPSec Gateway and Firewall

- Inside
  - No inspection of encrypted traffic
  - IPSec gateway protected by firewall
- Parallel
  - Potential uncontrolled access
- Outside
  - IPSec gateway protected by access router
  - Consistent policy
- Integrated
  - Maximum flexibility

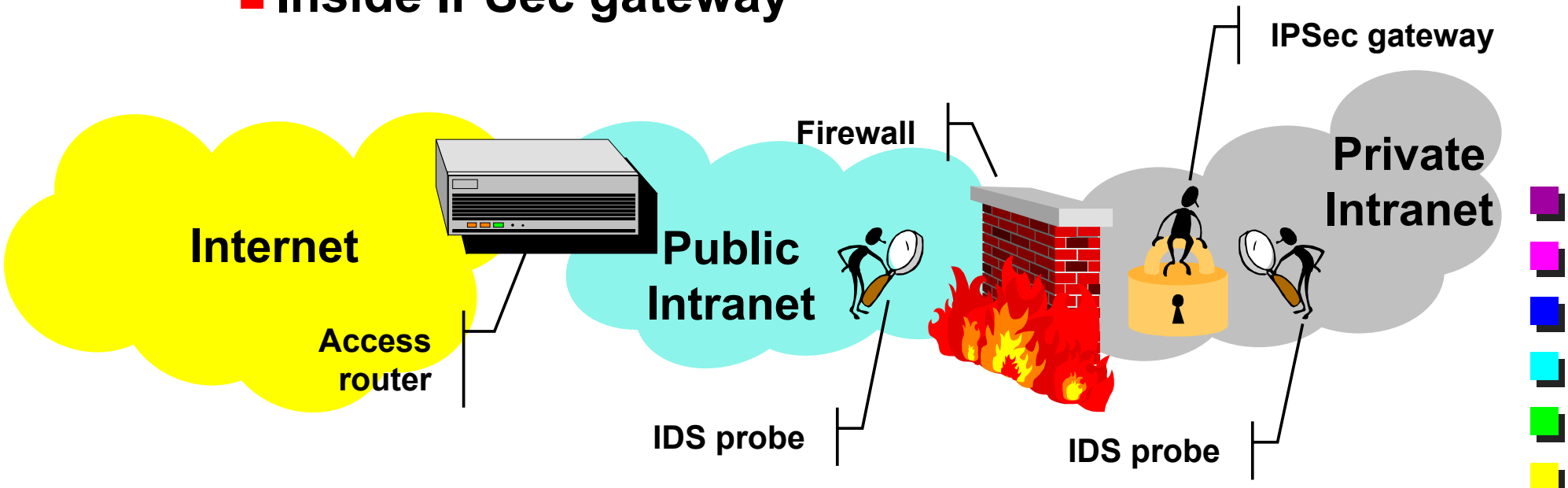


IPSec Gateway and NAT

- Authentication Header (AH)
  - IP addresses are part of AH checksum calculation → packets discarded
- Encapsulation Security Payload (ESP)
  - Port might be hidden → no address expansion
- No PAT (Port Address Translation)
- Tunnel mode
  - IP address within secure packet can be changed before entering the gateway
    - E.g., same addresses in two different VPN sites
  - Most often NAT is not needed on external packet

IPSec Gateway and IDS

- IDS is usually outside the firewall
- No control on encrypted traffic
- Multiple IDS probes
  - Outside firewall
  - Inside IPSec gateway



References

- S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol,” RFC 2401, November 1998.
- D. Harkins and D. Carrel, “The Internet Key Exchange (IKE),” RFC 2409, November 1998.
- S. Kent and R. Atkinson, “IP Encapsulating Security Payload (ESP),” RFC 2406, November 1998.
- S. Kent and R. Atkinson, “IP Authentication Header,” RFC 2402, November 1998.