Security for the Internet Infrastructure

Paul A. Lambert

palamber@us.oracle.com

February 10, 1997

ORACLE®

Internet Infrastructure and Security

Security for the Internet Infrastructure

- ***Datagrams*, Messages**
- **Name Services/Directories, Routing, Time**
- **System Management**

Infrastructure for Internet Security

- **Confidentiality, Integrity, Authentication Non-repudiation, Access Control**
- ***Key Management***
- **“Public Key Infrastructure”**
- ***“Trust Management”***

ORACLE®

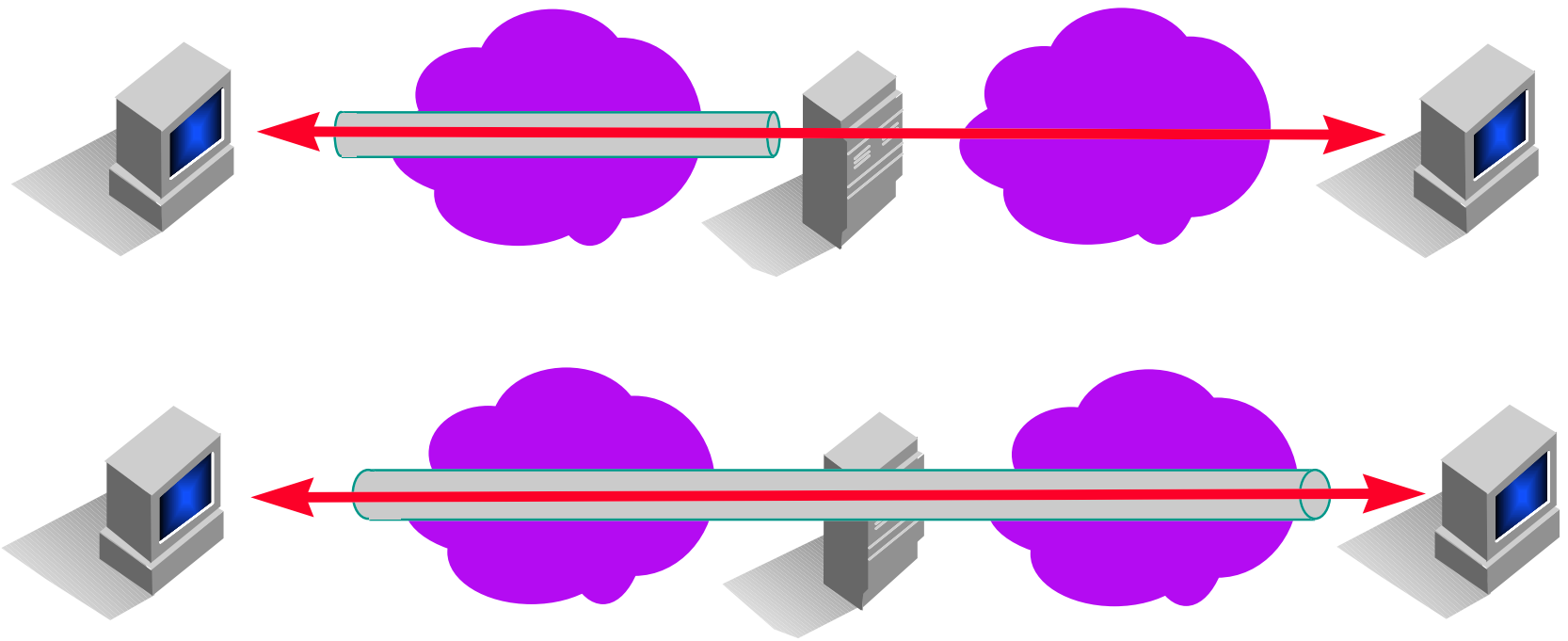
Specific Topics (this presentation)

- **IP Security (IETF IPsec)**
  - **Protects IP Datagrams**
  - **Key Management to create "Security Associations"**
- **W3C Digital Signatures (DSig)**
  - **Label Systems for Assertions**
  - **Semantic definition for Assertions**
  - **Digitally Signed Web Content**

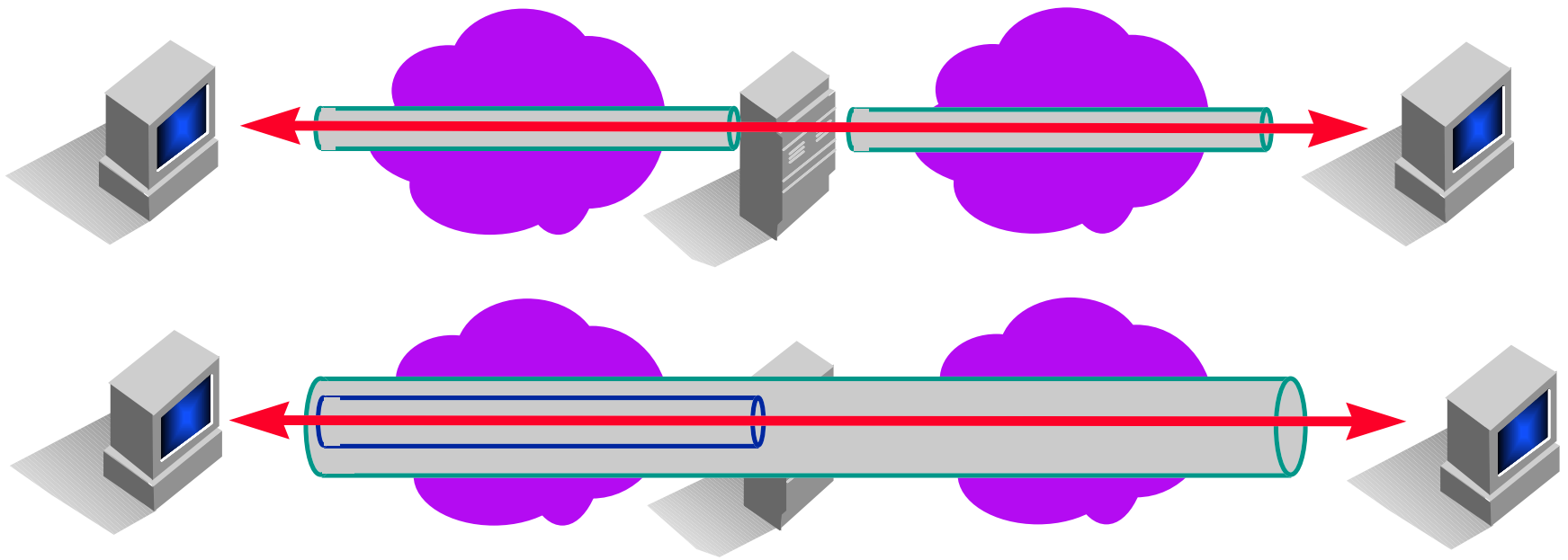
Network Security

- **Protects “Datagrams”**
  - **leaves routing information unencrypted**
- **Provides “end-to-end” security**
  - **host-to-host**
  - **host-to-router**
  - **router-to-router**
  - **host-to-Firewall**
  - **Firewall-to-Firewall**

IP Security - Secure “Pipes”



IP Security - Multiple Encapsulation



Network Layer Security - History

- **Defense Research in Network Encryption**
  - **PLI (Early 70's)**
  - **IPLI (76)**
  - **Blacker / Caneware / NES (80's)**
- **"Standards"**
  - **Secure Data Network System (86-91)**
    Published by NIST
    SP3, SP4, Key Management Protocol (KMP)
  - **Network Layer Security Protocol (ISO - early 90's)**
  - ***IPSEC (IETF - now)***

IPsec - Network Layer

- **Base Specifications**
  - **Security Architecture for the Internet Protocol (RFC 1825)**
  - **IP Encapsulating Security Payload (ESP) (RFC 1827)**
  - **IP Authentication Header (AH) (RFC 1826)**
- **Other RFCs**
  - IP Authentication using Keyed MD5 (RFC 1828)
  - The ESP DES-CBC Transform (RFC 1829)
  - HMAC-MD5 IP Authentication with Replay Prevention (RFC 2085)
  - HMAC: Keyed-Hashing for Message Authentication
  - (RFC 2104)

IPsec - Key Management

- **IPsec Base Key Management - ISAKMP/Oakley**
  - **Internet Security Association and Key Management Protocol (ISAKMP)**
  - **The resolution of ISAKMP with Oakley**
  - **Inline Keying within the ISAKMP Framework.**
  - **The Internet IP Security Domain of Interpretation for ISAKMP (31320 bytes)**
- **SKIP**
  - **SKIP Algorithm Discovery Protocol**
  - **SKIP Extensions for IP Multicast**
  - **SKIP extension for Perfect Forward Secrecy (PFS)**
  - **Simple Key-Management For Internet Protocols (SKIP)**
- **Photuris**

IP Security in the Internet

- **ISAKMP/Oakley - vendor implementations**
- **SKIP Implementations**
- **S/WAN™**
- **Swan and Linux**

ORACLE®

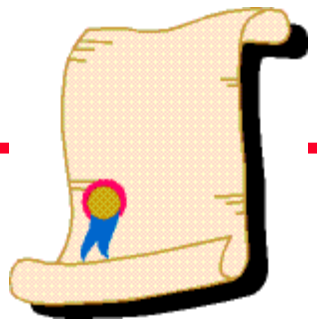
IP Security - References

- **IETF - IP Security**
  www.ietf.org
- **“Freeware” Network Encryption Plan**
  http://kpt1.tricon.net/Org/aiip/encrypt.html
- **Secure WAN Testing**
  http://www.rsa.com/rsa/SWAN/home.html
- **IP Security Background**
  http://www.cygnus.com/~gnu/netcrypt.html

ORACLE®

W3C Digital Signatures

- **Started with “code signing”**
  - **ActiveX ™ Signatures are only Binary (yes/no to submit to Microsoft policy)**
  - **Generalized to allow “assertions” on any information object**
  - **First target is Web Page labeling**
- **Built on PICS, Web Content Labeling (Platform for Internet Content Selection)**
  - **PICS Metalanguage for Rating Systems**
  - **PICS Labels or Assertions**



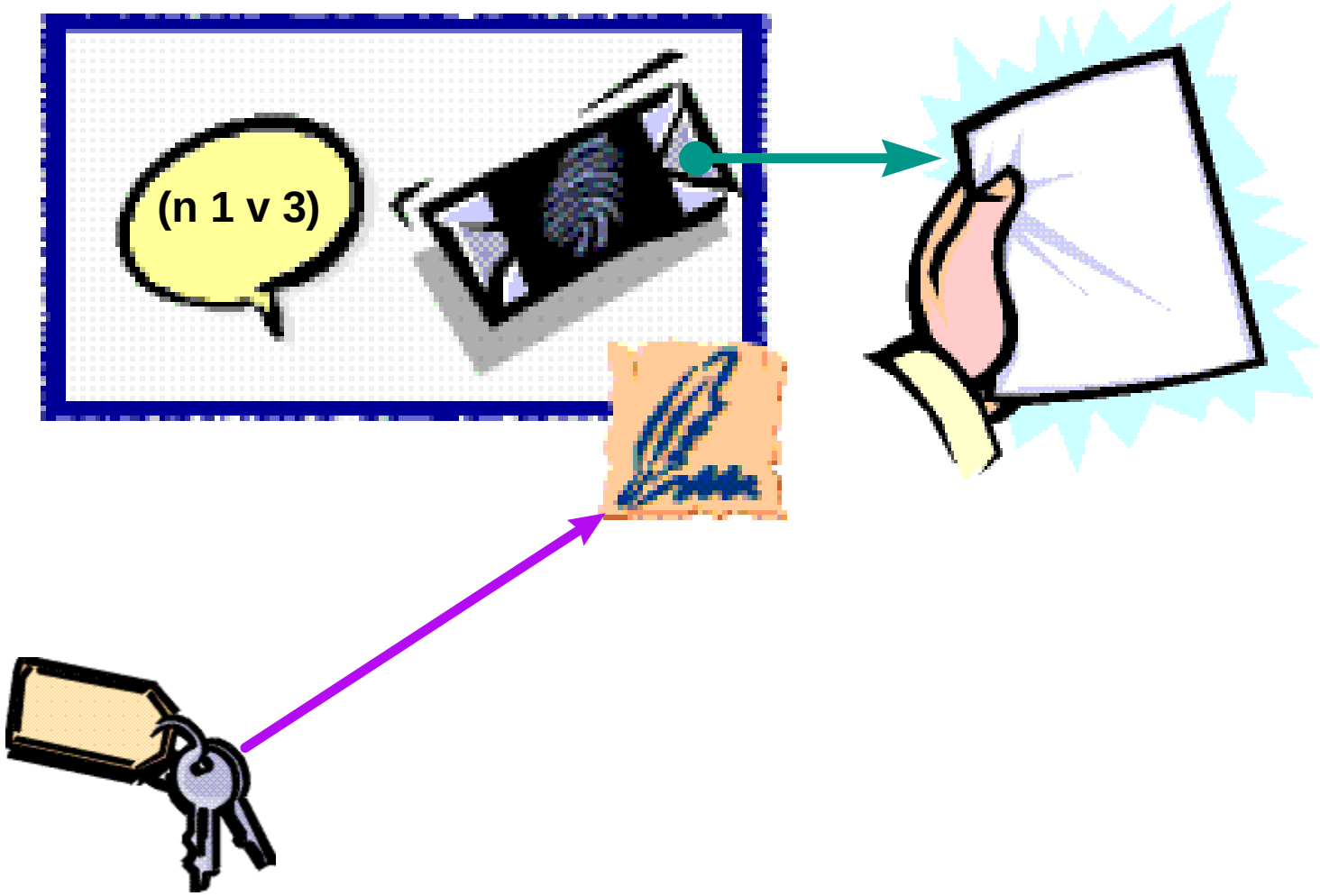
Semantics for Assertions

- **X.509**
  - **Version 3 Extensions**
- **Simple Public Key Infrastructure (SPKI)**
  - **Assertions**
- **W3C Digital Signatures (DSig)**
  - **PICS used as metalanguage for Assertions**
  - **Trust Modeling and Policy Engine**

W3C DSig

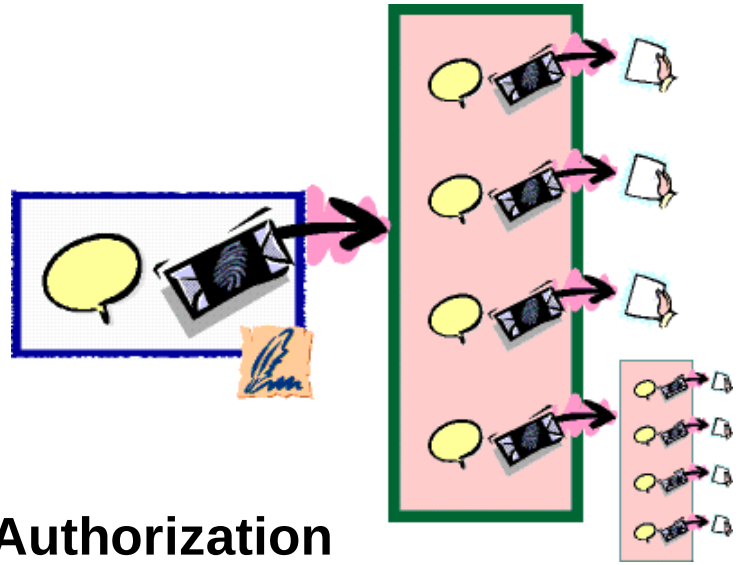
- **Metalanguage defines labels**
  - **includes human readable definitions**
  - **machine readable format**
- **Signature Block binds:**
  - **rating system**
  - **assertion (PICS label from rating system)**
  - **referent (source)**
  - **target (hash and URL)**
  - **digital signature**
- **Trust Modeling based on Assertions**

Dsig Label Example



W3C DSig

- **W3C DSig Applications**
  - **Web content rating**
  - **Active content manifests**
  - **Software Licensing**



- **Benefits:**
  - **Improved Granularity of Authorization (as compared to binary)**
  - **Flexible policy creation**
  - **Common model for trust management**
- **References - www.w3.org**

Summary

- **IP Security could provide a strong base security mechanism for the Internet (75% solution)**
- **Too many protocol specific mechanisms**
- **Trust management and assertions would support manageable security**
  - **distributed security management (Federation)**
  - **need “good” delegation**

ORACLE®

Infrastructure Security - Issues

- **“Network” Security**

  IPSEC - SSL/TLS/PCT - PPP security - SSH

- **Key Management**

  SSL - ISAKMP - SOCKS - PPP - IEEE 802.10 …

- **Certificates**

  X.509 - DNS - PGP - W3C DSig

- **Mail**

  PEM - MOSS - S/MIME ™