

Internet Protocol Security -IPSec

Chris King

March 12, 1996



INFOSEC Engineering, INC

URL: www.infoseceng.com Voice: 508-256-4494

Email: cmk@infoseceng.com

Agenda

- Evolution
- Technical Aspects
- Analysis
- References



INFOSEC Engineering, INC

URL: www.infoseceng.com Voice: 508-256-4494

Email: cmk@infoseceng.com

IPSec Evolution

- Started in November '92 as IP next generation (IPng)
 - Now referred to as IPv6
- Firewall consortium started in June of '95



IPv6 Overview

- Expanded routing and addressing capabilities
- Header format simplification
- Improved support for extensions and options
- Flow labeling capability
- Authentication and privacy capabilities

(IPSec)



INFOSEC Engineering, INC

URL: www.infoseceng.com Voice: 508-256-4494

Email: cmk@infoseceng.com

IPSec Technical Aspects

- IP Authentication Header (AH)
- IP Encapsulating Security Payload (ESP)
- Security Association (SA)
- Key management
 - Photuris
 - SKIP



IP Authentication Header (AH)

- Provides IP datagram integrity and authentication
 - Keyed MD5 (Key-Data-Key)
 - Computation performed before fragmentation and after reassembly
- Does not provide non-repudiation (symmetric algorithm) and privacy



IP Encapsulating Security Payload (ESP)

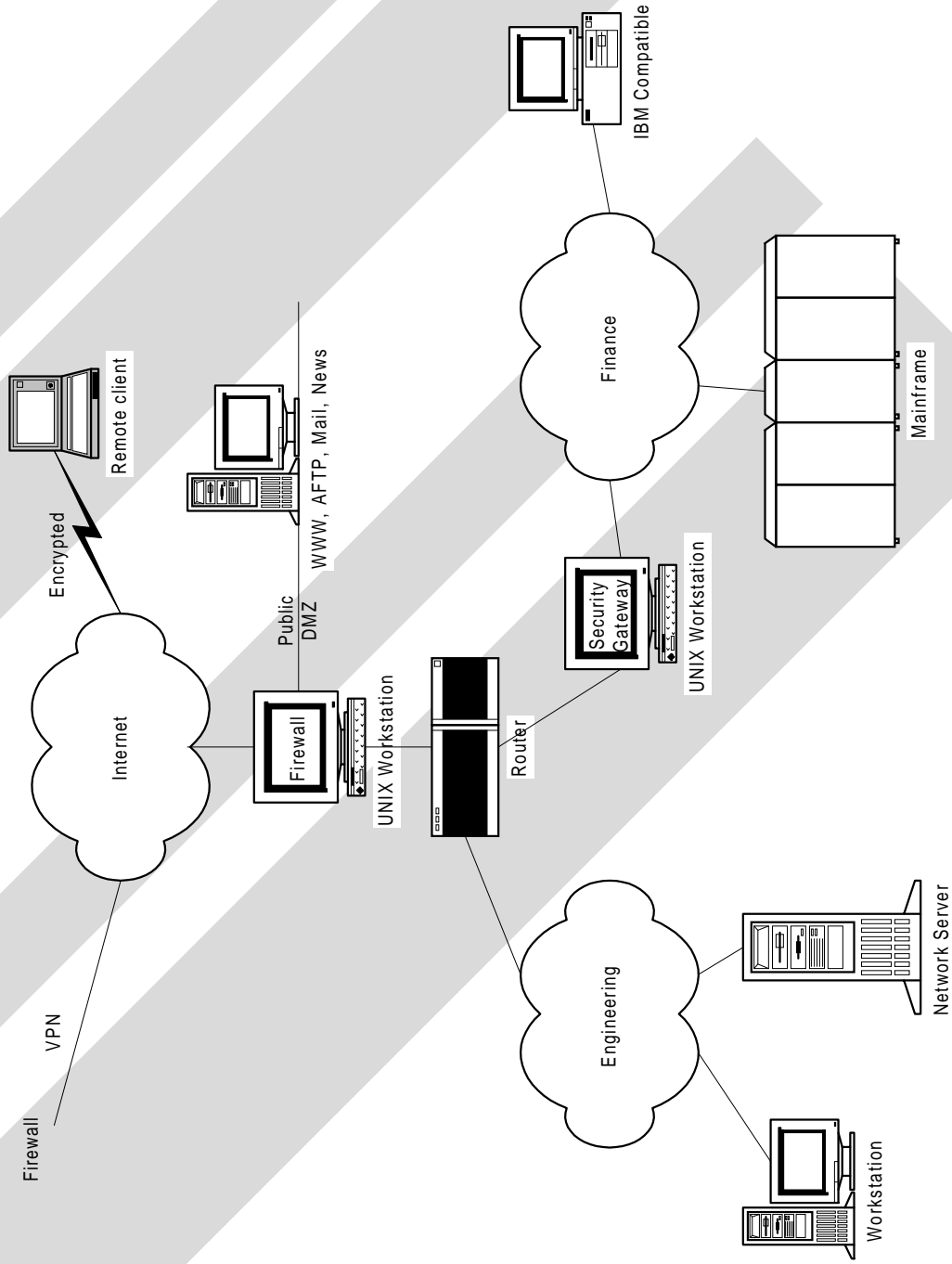
- Provides IP datagram integrity, authentication, and privacy
 - Tunnel and Transport modes
 - » Tunnel encapsulates an entire IP datagram within the ESP header
 - » Transport encapsulates an upper-layer protocol inside ESP and then prepends a cleartext IP header
 - DES Cipher Block Chaining (CBC)
 - RC2 or RC4 for international use



Security Association (SA)

- A security association defines a one way association between a sender to receiver
 - AH and ESP algorithm and mode
 - Size of cryptographic synchronization (IV)
 - AH and ESP crypto keys and lifetimes
 - Source address(es) of the security association
 - Sensitivity level
 - The destination address and Security Parameters Index (SPI) identify the SA

The Big Picture



IPSec Analysis

- Remote access will benefit if the networking software is IPSec compliant (client-VPN)
- IPSec compliant gateways must perform packet filtering on unauthenticated packet (a.k.a. Firewall)
- VPN interoperability among heterogeneous firewalls and remote clients



IPSec Analysis (Concluded)

- Internet and Intranet Firewalls will use IPsec to validate the network data used for the access control decisions (security policy update)
 - Authenticated IP headers could allow source routing
- The combination of IPSec, Firewalls and security tokens provide a complete network security solution.



IPSec Key Management

Qualcomm's Photuris

- **Scaleable to very large environments**
- **Based on Firefly**
- **Session oriented**
- **Perfect Forward Secrecy**
- **Traffic anonymity**

Sun's SKIP

- **Most suitable for small environments and established relationships**
- **Stateless**
- **No Forward Secrecy**
- **No anonymity due to certified public values (DNSSEC)**



IPSec Vendors



TIMESTEP

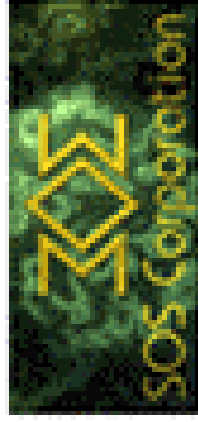
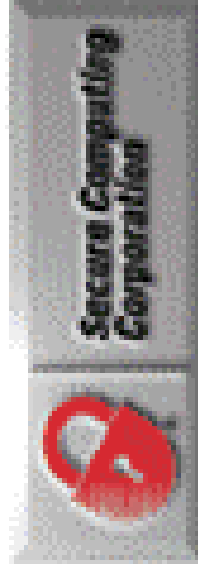


C h e c k P o i n t

Software Technologies Ltd.



M o r n i n g S t a r T e c h n o l o g i e s

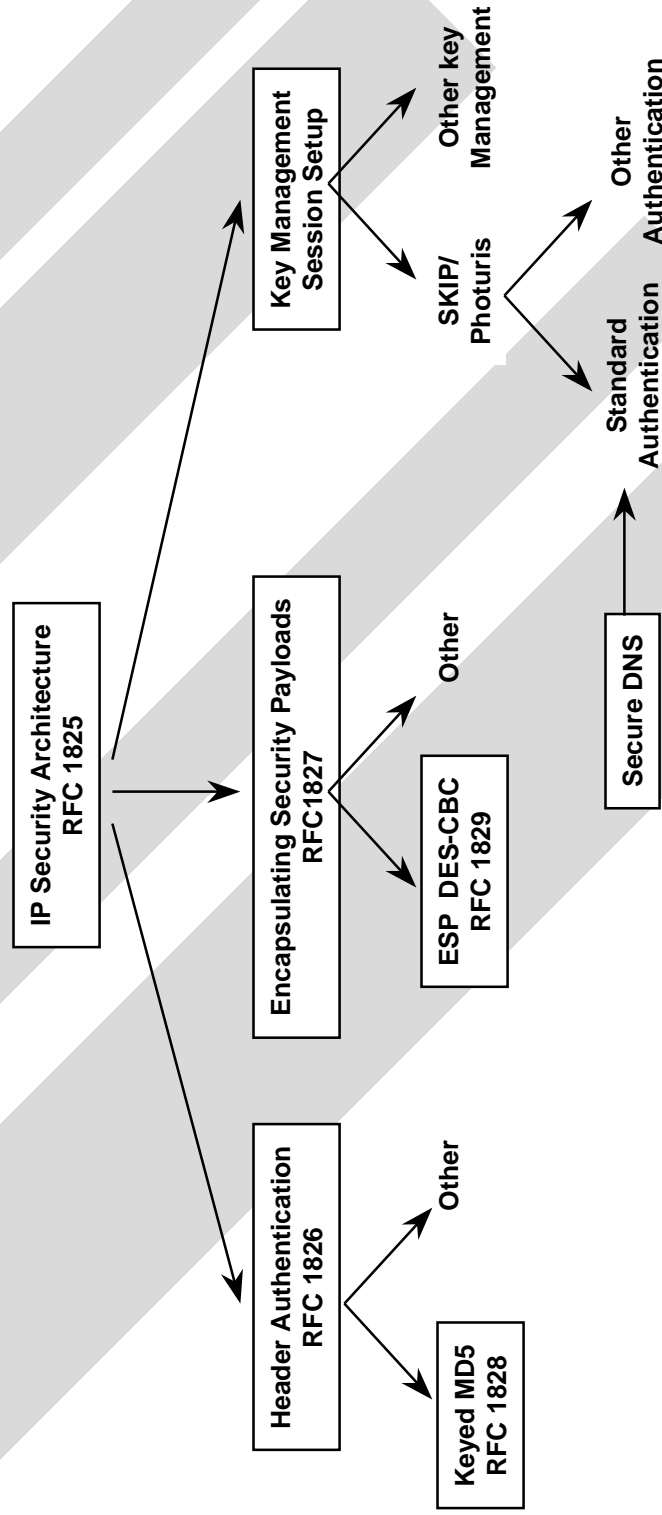


INFOSEC Engineering, INC

URL: www.infoseceng.com Voice: 508-256-4494

Email: cmk@infoseceng.com

IPSec Standard Evolution



IPv6 RFCs

- IP Version 6 Addressing Architecture (RFC 1884)
- Internet Protocol, Version 6 (IPv6) Specification (RFC 1883)
- Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) (RFC 1885)



IPv6 RFCs (Concluded)

- An Architecture for IPv6 Unicast Address Allocation (RFC 1887)
- DNS Extensions to support IP version 6 (RFC 1886)
- IPv6 Testing Address Allocation (RFC 1897)



Emerging Security Technologies for '96

- IPsec
 - Heterogeneous VPN
 - Remote client VPN
- RADIUS authentication protocol
- JAVA
- Secure Electronic Transactions (SET)



INFOSEC Engineering, INC

URL: www.infoseceng.com Voice: 508-256-4494

Email: cmk@infoseceng.com

INFOSEC Engineering Consulting Services

- Security policy generation/review
- Security audit/assessment
- Security penetration/vulnerability analysis
- Information security planning



INFOSEC Engineering, INC

URL: www.infoseceng.com Voice: 508-256-4494

Email: cmk@infoseceng.com