SAND2006-6299C

An Architecture for Multi-Security Level Network Traffic

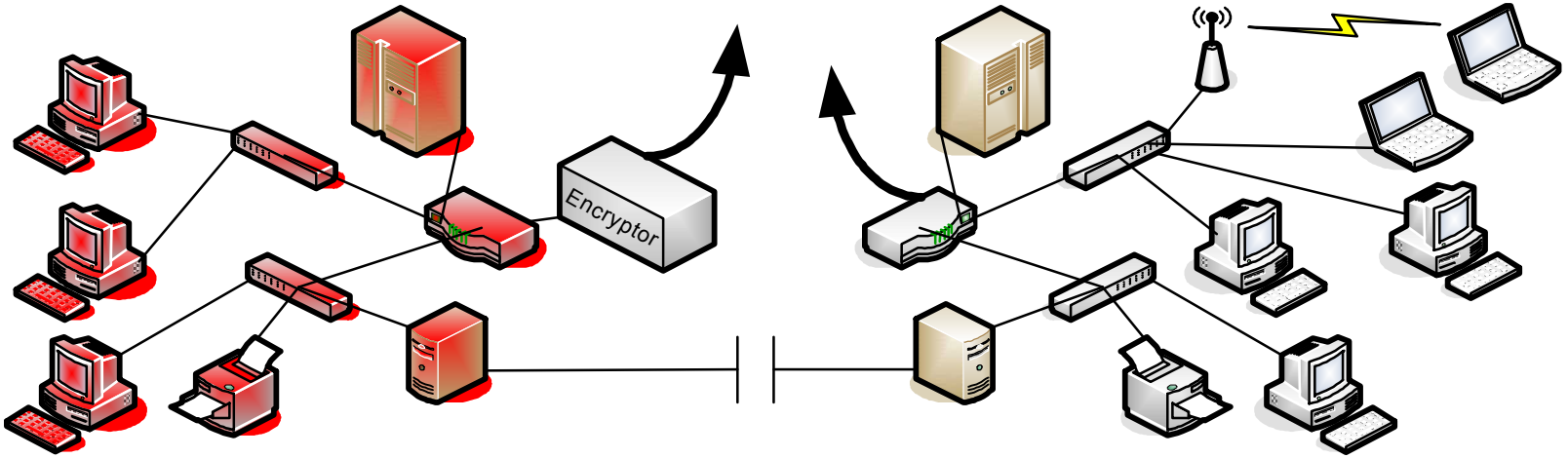
October 2006

Ed Witzke, Steve Gossage, Dallas Wiener

Sandia National Laboratories

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Traditional Model for Security Separation in Networks



Sandia National Laboratories

New Model for Security Separation in Networks

- Encryptors protecting individual systems or enclaves
  - End-to-end encryptors directly connected to end systems
  - (Relatively) Small encryptors front-ending a switch connecting several devices

Why Now?

- Interoperability
- Improved price-performance ratios
- New products

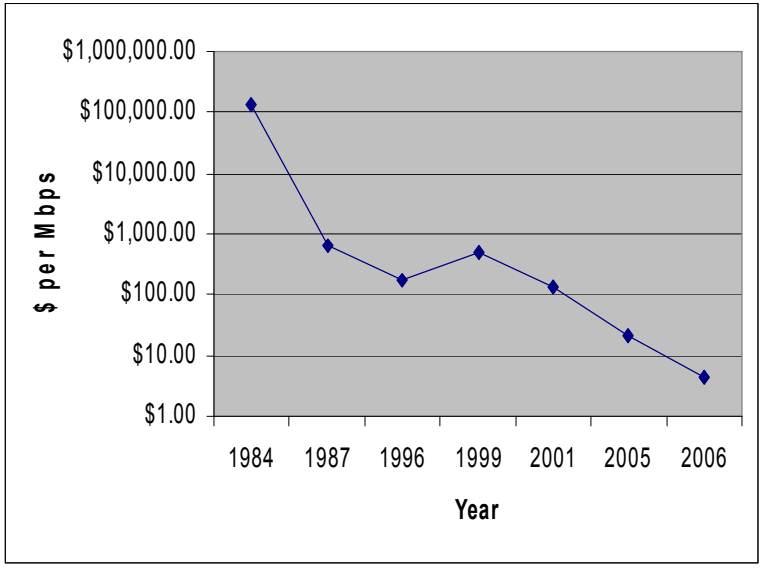
Sandia National Laboratories

Interoperability

- High Assurance Internet Protocol Encryptor (HAIPE)
  - Working group developed an interoperability specification for Type 1 encryptors
  - Enables secure IP-based applications
  - Ensures interoperability between network encryptors manufactured by different vendors
- Companies producing Type 1 HAIPE-compliant encryptors include:
  - General Dynamics C4 Systems
  - Harris Corporation
  - L3 Communications Systems

Price and Performance

- KG-84 (1984) 56 Kbps ~$8000
- KG-94 (1987) 12 Mbps ~$8000
- Taclane Classic (1999) 16 Mbps ~$8000
- Taclane E-100 (2001) 80 Mbps ~$11,000
- Taclane-Mini (2005) 100 Mbps ~$11,000
- Taclane-Gig (2005) 1 Gbps ~$23,000
- Red Eagle 245X (2006) 10 Gbps ~$45,000

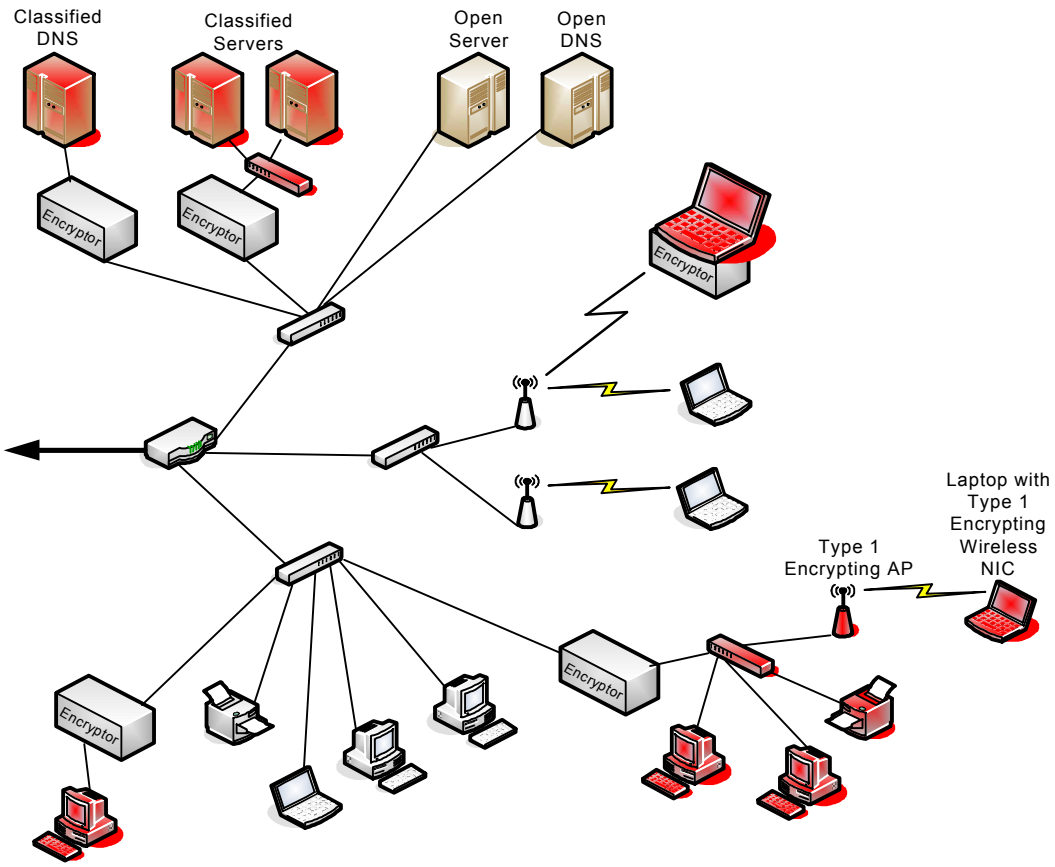


Sandia National Laboratories

New Products

- 100 Mbps end-to-end IP encryptors
- Gigabit end-to-end IP encryptors
- 10 Gigabit end-to-end IP encryptors
- End-to-end IP encryptors with interchangable transmission media modules
  - Initially 802.11 a/b/g wireless
  - Future: wired Ethernet, telephone dial-up, 802.16 WiMax
- Taclane Router
  - HAIPE network encryptor
  - Cisco routing technology

Consolidated Network Architecture



Sandia National Laboratories

Benefits

- Single network to troubleshoot and maintain
  - Short classified tail circuits
  - Less equipment
    - One set of network equipment
    - One set of communication links
- Increased flexibility and functionality
  - Easy to add secure devices in areas where only non-secure infrastructure exists

Obstacles and Issues

- Cryptographic synchronization loss
  - High level of bit integrity from the network
- Physically securing small and portable encryptors when unattended
- Configuration control
- Key management
- Troubleshooting encrypted environments
- Need-to-know separation between classified users
- DoS attack on non-secure portions of the network could affect continuity between secure nodes
- How would new encryption technology affect the enterprise

Summary

- New architecture to consolidate networks of several security levels
  - Enabled by new products, lower prices, and HAIPE specification for interoperability
  - Benifits of potential cost savings, reduction of duplication, and increased network flexibility
  - Operational and policy issues are areas for further examination and research
- Mostly conceptual at this point
  - Build testbed to start prototyping