Intro. To Security Solutions For Network Devices

Uriah Pollock

Product Manager – Mentor Graphics

Agenda

- A Short Background On Cryptography
- The Building Blocks Of Security
- Security Protocols
- The Embedded Devices

Short History Of Encryption

- Always A Need To Protect Information
- One Very Early Form
  - Caesar’s Substitution Cipher

PT	A	B	C	D	E	F	G	H	I
CT	D	E	F	G	H	I	J	K	L

- Transform One Letter To Another
- In this case
  - BIG ⇔ ELJ

Short History Of Encryption

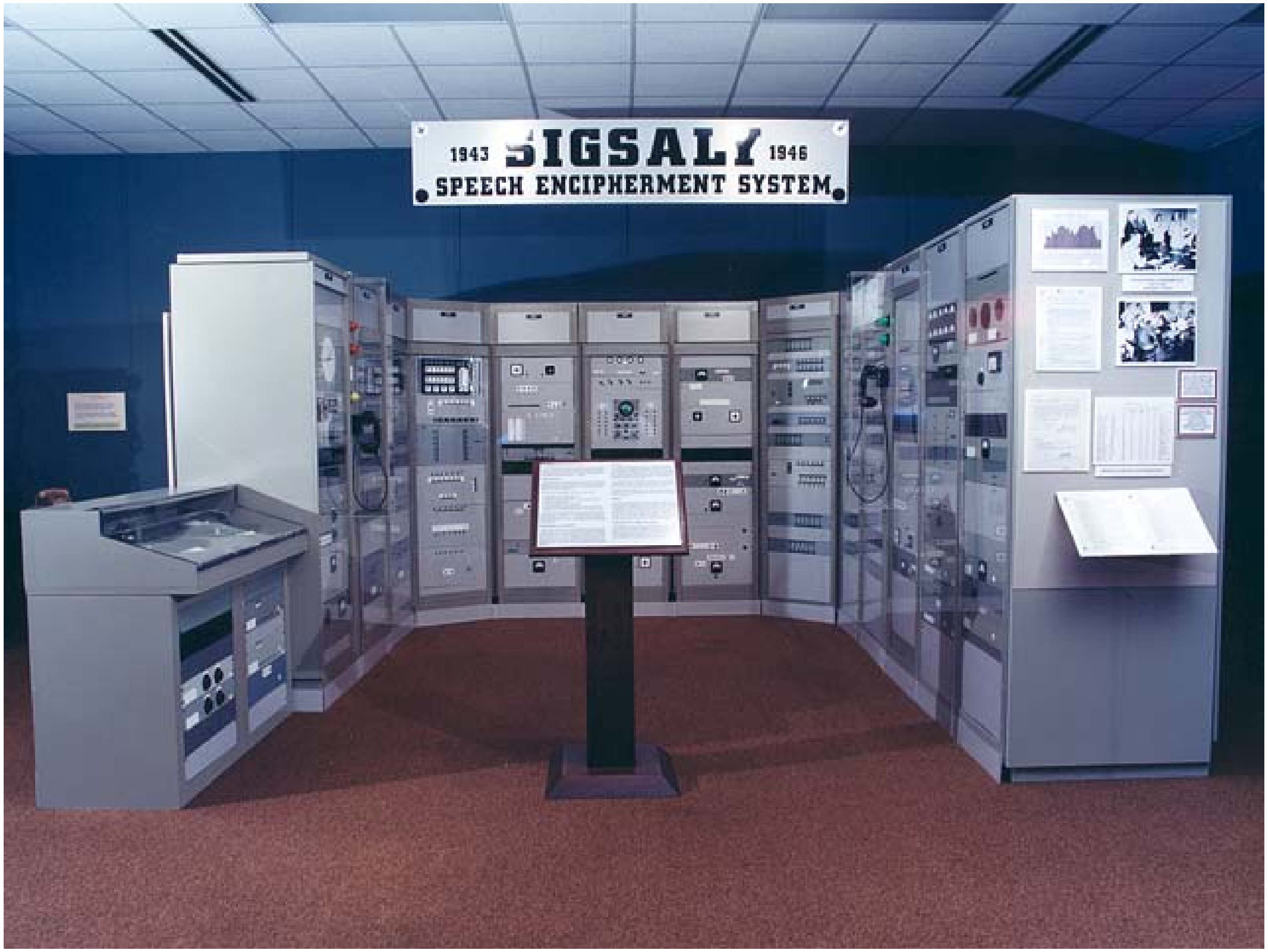
- Enigma Machine
  - Based On Caesar’s
  - Complex For Its Time
  - Sold Commercially
  - Used In World War II
  - Mechanical/Electrical System
    - Rotors
    - Keyboard
    - Lights

The Coming Of Digital Encryption

- SIGSALY
  - First Digital Encoder
  - Developed By Bell Labs
  - Used By USA and UK During World War II
  - Performed All Needed Operations
    - AD Voice Encoding
      - Vocoder
    - Encryption Of Digitally Encoded Voice
    - TX ⬄ RX Radio Signal
    - Decryption Of Digitally Encoded Voice
    - DA Voice Synthesis
- Creation Of Many New Technologies

The Coming Of Digital Encryption

- SIGSALY



Agenda

- A Short Background On Cryptography
- The Building Blocks Of Security
- Security Protocols
- The Embedded Devices

The Building Blocks Of Security

- Three Main Building Blocks
  - Symmetric Encryption Ciphers
  - Asymmetric Encryption Ciphers
  - Message Digest Algorithms
    - Hashing Algorithms

Symmetric Encryption Ciphers

- Same Key To Encrypt And Decrypt The Data
- Algorithms Such As
  - Data Encryption Standard (DES)
  - Triple DES (3DES)
  - Advanced Encryption Standard (AES)
  - Blowfish
  - And Others
- All Provide Data hiding
- Typically Fast And Small

Asymmetric Encryption Ciphers

- One Key To Encrypt Data
- Different Key To Decrypt Data
  - Public Key Cryptography
- Rivest Shamir Adleman (RSA) Algorithm
- Provides
  - Key Origin Validation
  - Authentication

Message Digest Algorithms

- One Way Hashing Algorithms
- Enables Data Integrity Authentication
  - Data Not Modified During Transmission
- Algorithms Include
  - MD4
  - MD5
  - Secure Hash 1 (SHA-1)
  - Secure Hash 256 (SHA-256)
- Use HMAC Hashing With A Key
  - Increased Security
  - Data Origin Authentication

Agenda

- A Short Background On Cryptography
- The Building Blocks Of Security
- Security Protocols
- The Embedded Devices

Security Protocols

- A Number Available
- Do They All Solve The Same Problem?
- Today I Will Cover
  - Internet Protocol Security (IPsec)
  - Layer 2 Tunneling Protocol (L2TP)
  - Secure Sockets Layer (SSL)
  - IEEE 802.1x
    - Port Based Authentication
  - IEEE 802.11i
    - WPA and WPA2
  - Secure Shell (secSH)

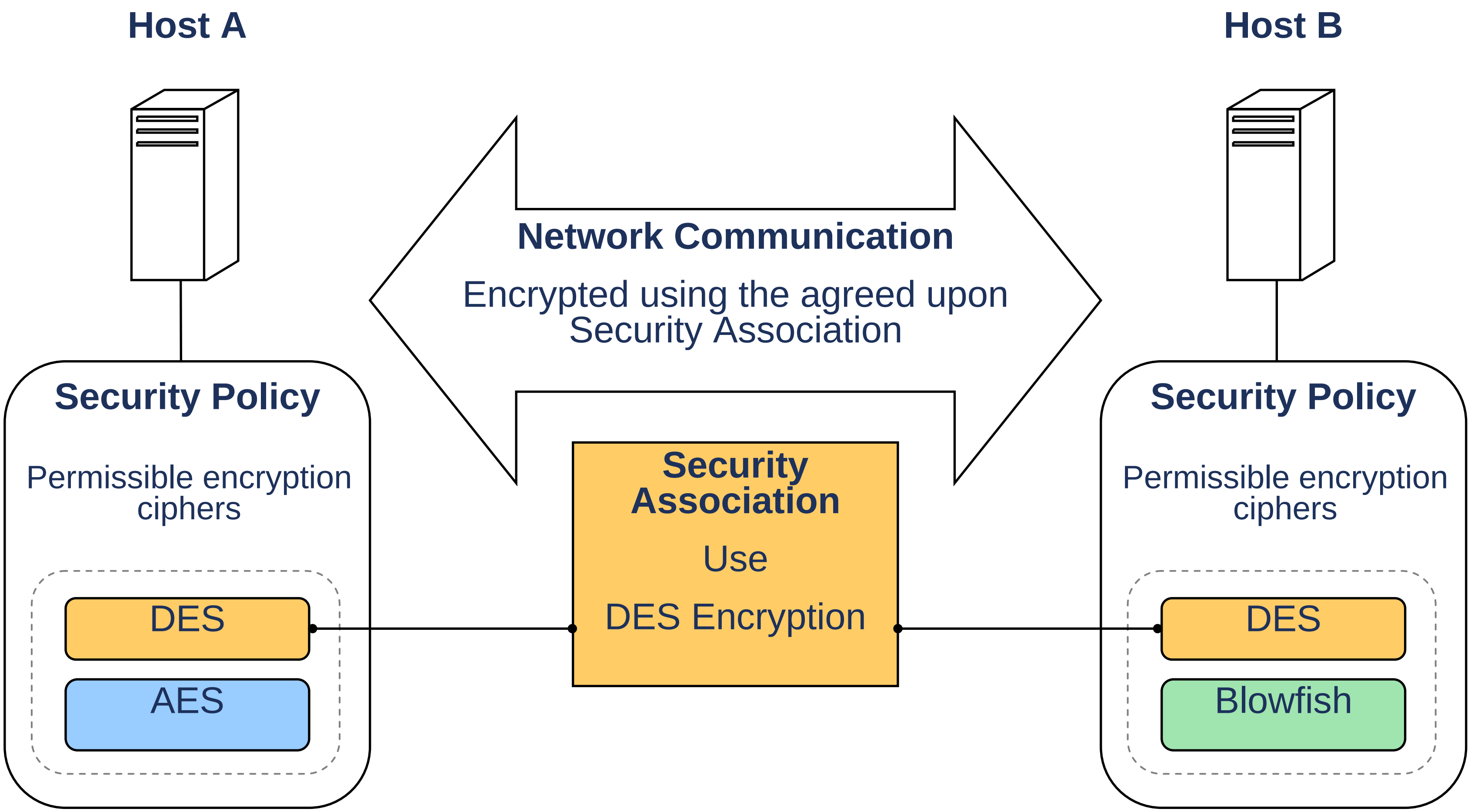
Internet Protocol Security

- Security Built In-To The Stack
- Two Main Protocols
  - Authentication Header (AH) Protocol
    - Data Is Hashed
    - Including Shared Secret
  - Encapsulating Security Payload (ESP) Protocol
    - Data Hiding
- Configuration Must Be Done
  - Which Asymmetric Cipher?
  - Which Hasing Algorithm?
  - What Shared Secret Key?

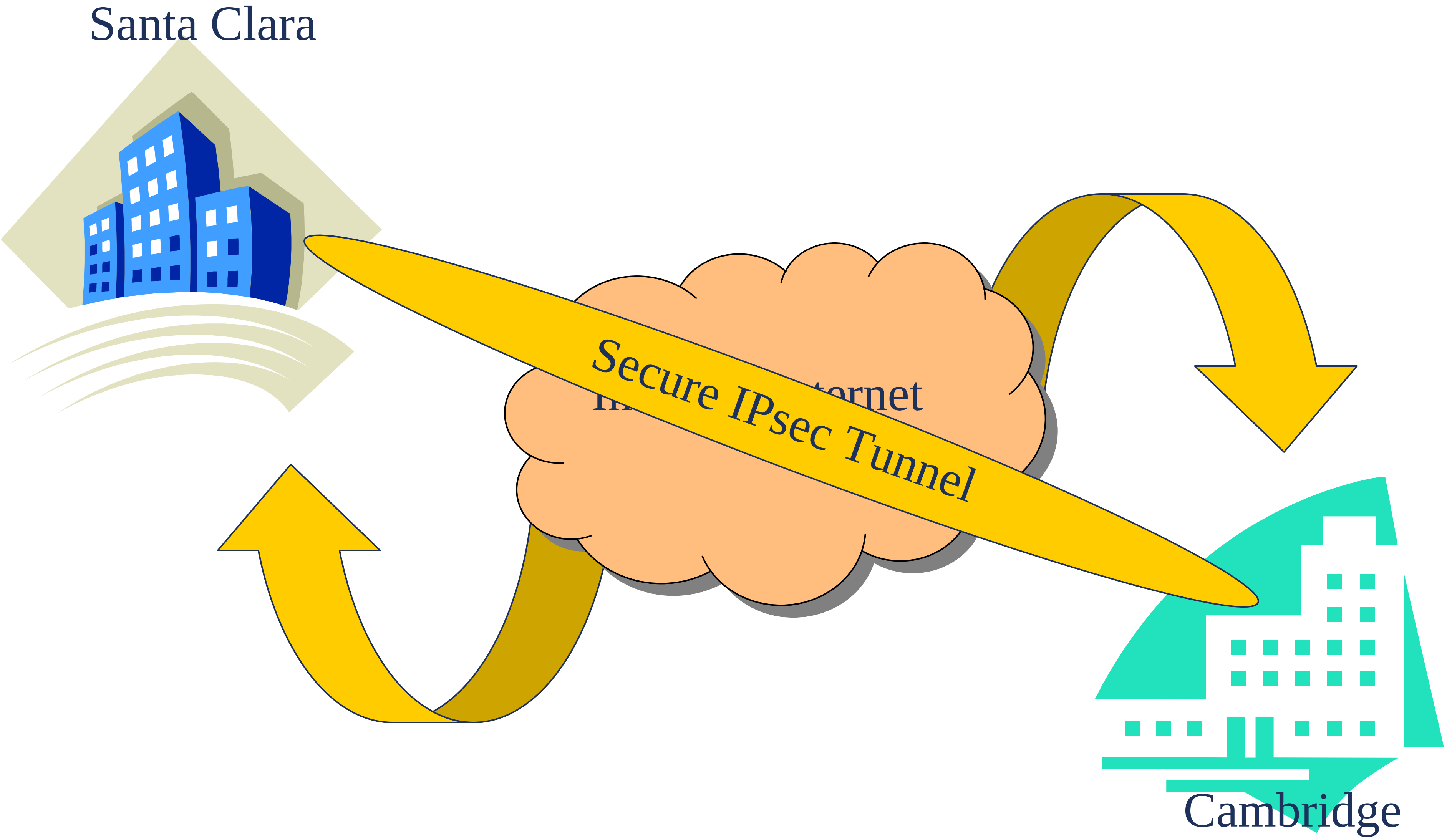
Internet Protocol Security – IKE

- Internet Key Exchange
- Automates IPsec Configuration
  - Asymmetric Encryption Cipher
  - Message Digest Algorithm
  - Shared Secret Key
- Creates Security Association
  - Both Sides In Agreement
- Periodically Renews Security Association

Internet Protocol Security



IPsec: Site-To-Site



Santa Clara

Internet

Secure IPsec Tunnel

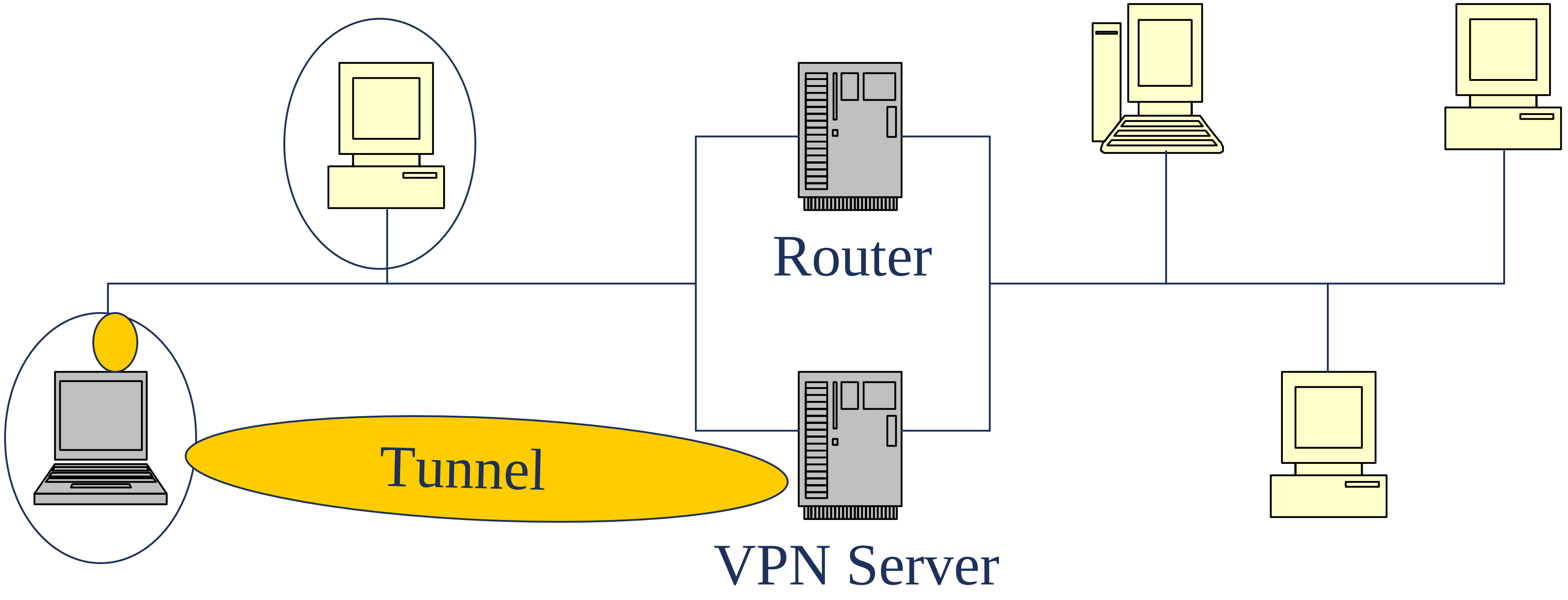
Cambridge

Layer 2 Tunneling Protocol

- Functions At Bottom Of Stack
- Provides Tunneling
- Provides Configuration
  - User Authentication
    - CHAP-MD5
    - PAP
    - MS-CHAPv1/v2
  - IP Address Assignment
  - DNS Server Assignment
- Provides No Data Hiding!
  - Use IPsec For This

Layer 2 Tunneling Protocol

- Simple Network Example Of Tunneling



Secure Sockets Layer

- Application Level Security
- Commonly Used For HTTP
- Is A General Purpose Solution
- Requires Application Modification

Port Based Network Access Control

- Defined in IEEE 802.1x
  - Based on Extensible Authentication Protocol
  - Other Variants
    - LEAP, PEAP, EAP-TLS, EAP-TTLS
- Network Ports Are Authenticated
  - Ports On A Network Switch
  - “Ports” On A Wireless Access Point
- Server Uses Authentication Mechanism
  - RADIUS
  - LDAP
  - Open Ended In 802.1x Specification

802.11 Enhanced Security

- Developed by Task Group I
  - Named IEEE 802.11i
  - Also Wi-Fi™ Protected Access 2
  - Replaces Cracked Wired Equivalent Privacy (WEP)
  - Replaces Stop-Gap WPA 1
- Built From Many Protocols
  - SSL
  - 802.1x
  - CCMP
    - With AES Encryption
- 802.11 Hardware Must Support 802.11i

Secure Shell

- Replacement For Telnet
  - Remote Machine Access
- Integrated With FTP
  - Secure FTP Log In
  - Secure FTP File Transfers
- Can Proxy Other Connections
  - Gives Security To Insecure Applications

Improving Performance

- Encryption Ciphers
  - Can Be Slow
  - Can Consume Many CPU Cycles
  - May Require Powerful CPU For Needed Performance
- Hardware Offloading Solves This
  - Algorithms Moved to Hardware
  - Speeds Algorithm
  - Speeds Security Protocol
  - Improves Entire System
- Example Part:
  - TI OMAP2420

Agenda

- A Short Background On Cryptography
- The Building Blocks Of Security
- Security Protocols
- The Embedded Devices

Securing Devices

- The Right Protocol?
- Many Networked Devices
- Mobile/Handheld Devices
- Network Infrastructure
- Medical Devices
- SOHO
- Set Top Boxes
- More

Securing Devices

- Will They Connect To A Remote VPN?
- Are They Wireless Ethernet Capable?
- Do You Need To Secure A Proprietary Protocol?
- Network Centered Equipment?

Summary Page

- Selection Of Security Solutions Available
- Each Has Appropriate Application
- Device Type/Use Guides Which To Use