Welcome to the RSA Security Web Seminar Series

October 3, 2001
1pm Eastern
10am Pacific
6pm GMT

Securing the Network of the Future

Presented by RSA Security's

Kim Getgen, Product Marketing Manager
Benjamin Lail, Senior Systems Engineer
Nino Marino, Technical Manager

RSA SECURITY

Agenda

- Introduction
- What applications will drive broadband?
- Securing the next-generation network:
  - Security vulnerabilities
  - Development challenges
  - Standards
- Case Study: CableLabs PacketCable
- What solutions are available?
- Q&A

RSA SECURITY

Market Overview

RSA SECURITY

Market Opportunities and Issues

Broadband and wireless consumer devices

- **Manufacturers and system operators have new business opportunities**
  - New devices to manufacture and sell
  - High-speed internet connection services – wired and wireless
  - New transactional services for operators (cable and wireless)
  - New "content" to deliver to users: Voice over-IP and Video on Demand
  - Secure code updates to hardware
- **…that bring new risks**
  - Service theft
  - Liability through privacy breeches
  - Malevolent code introduced causes network or subscriber damage
- **Requiring that security is serious for both broadband cable and wireless consumer devices**

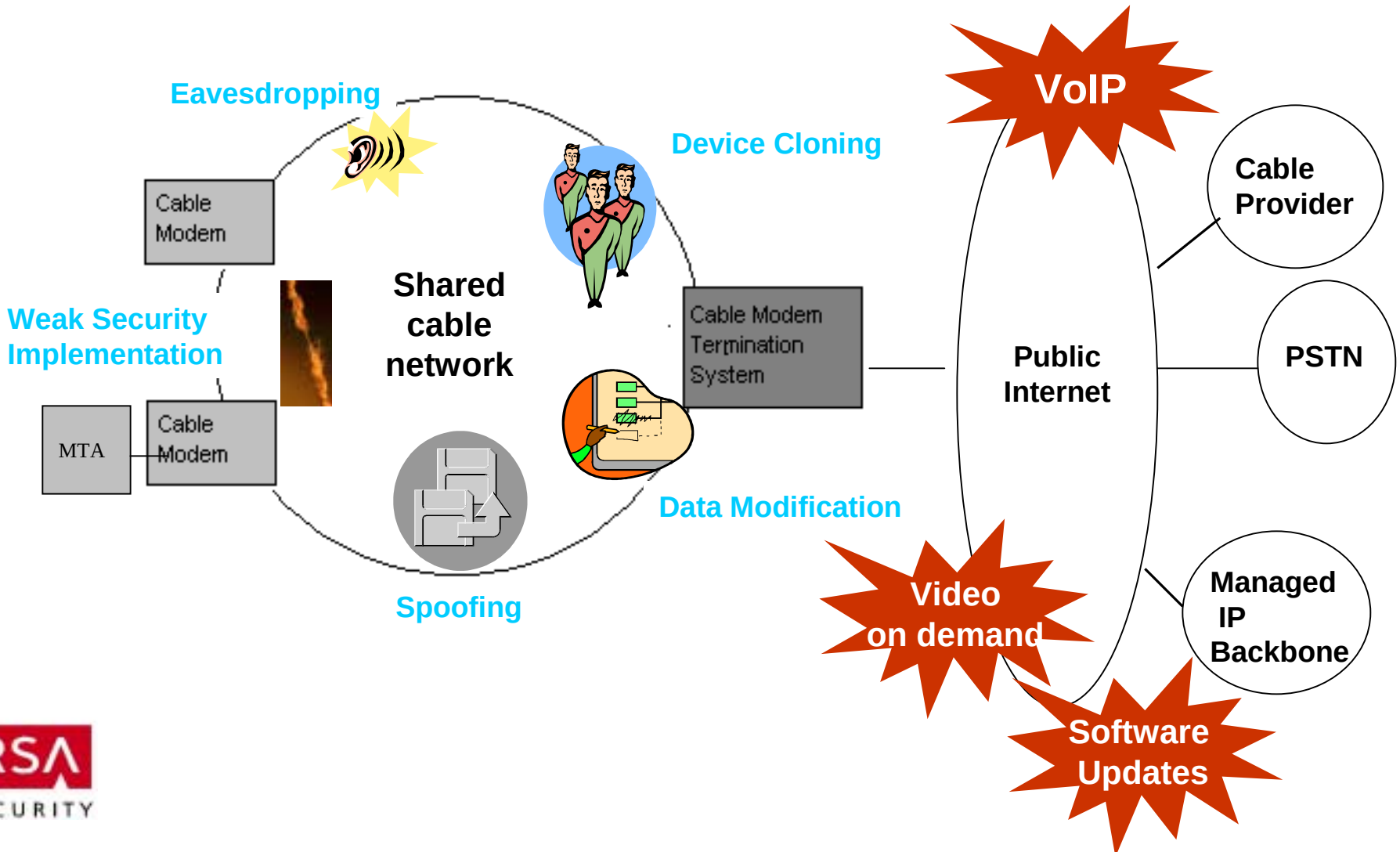
RSA SECURITY

New Consumer Devices that Require Security

- **New consumer devices:**
  - Wireless phones and PDAs
  - Set-top boxes
  - VoIP phones connected to MTAs
  - Gaming devices
  - Networked appliances
  - Residential Gateways
  - Securing Wireless Networks in the home
- **Infrastructure**
  - Switching and routing infrastructure equipment that merges voice, video and data networks
  - Security now being required at the network level:
    - IPSec implementations are increasing
    - IPv6 will push the adoption of IPSec
    - 802.11 standards in wireless

RSA SECURITY

Security Essential to Deployment of New Applications



RSA SECURITY

Securing the Network of the Future

RSA SECURITY

Security Vulnerabilities on Public Networks

Common security vulnerabilities that exist on public networks:

- ✓ **Eavesdropping**
- ✓ **Device cloning/impersonation**
- ✓ **Denial-of-Service (DoS)**
- ✓ **Data modification**
- ✓ **Replay attacks**
- ✓ **Spoofing**
- ✓ **Protocol or application security weaknesses**

Note: Many of these may result in *theft of service*.

RSA SECURITY

Groups Most Affected by Threats

Groups:

- **End-Users (Consumers)**
- **Service Providers**
- **Device Manufacturers**

Note: Each group has their own concerns and responsibilities.

RSA SECURITY

End-Users

- **Concerns:**
  - **Protect personal and/or customer information**
  - **Protect online accounts**
  - ***Should not* be concerned with security of underlying network infrastructure**
- **Responsibilities:**
  - **Education and security awareness**
  - **Use of personal firewall, anti-virus, SSL-enable browser, and desktop encryption**

RSA SECURITY

Service Providers

- **Concerns:**
  - **Protect user and provider data in the access, distribution, and backbone networks**
  - **Reduce or eliminate theft of service**
  - ***Should not* be concerned with securing data outside the network (e.g. cable modem or CPE)**
- **Responsibilities:**
  - **Securely implement underlying network infrastructure**
  - **Maintain performance and availability of services**
  - **Choose interoperable (certified?) network components**
  - **Implement proposed security standards closely**

RSA SECURITY

Device Manufacturers

- **Concerns:**
  - **Limit cost of production – maintain price point/increase profit**
  - **Correctly implement standards within devices**
  - **Maintain high level of device performance (balance cost and security)**
- **Responsibilities:**
  - **Develop products that conform to security standards**
  - **Certify devices when appropriate**

RSA SECURITY

Current Challenges

- **Service providers and manufacturers face a number of challenges in securing broadband services and devices.**
- **Transparency to end-users and ease-of-use is paramount – security cannot hinder usage**
- **Other areas of concern:**
  - **Network operation and performance**
  - **Embedded device limitations**
  - **Standards development, acceptance, and deployment**

RSA SECURITY

Network Operation Challenges

- **Implement multiple protocols: signaling, QoS, billing, and security**
- **Maintain appropriate performance (QoS) levels:**
  - **Bandwidth**
  - **Latency**
  - **Jitter**
  - **Packet loss**
  - **Availability**
- **Protect services that cross multiple network boundaries, architectures, and providers**
- **Field equipment upgrades**

RSA SECURITY

Embedded Device Challenges

- **Maintain profit margin (e.g. balancing cost vs. value-added functionality)**
- **Limited processing power - hardware or software?**
- **Limited memory**
  - **Flash memory - code footprint**
  - **RAM - runtime memory**
- **Physical protection of credentials**
- **Choice of security implementation: build or buy?**

RSA SECURITY

Standards Challenges

- **Choosing security appropriate for the environment (e.g. link layer vs. end-to-end security, associated performance)**
- **Competing standards – maintaining vendor neutrality**
- **Nonexistent implementation of security components**
- **Lack of test environment to validate standard**

RSA SECURITY

Case Study:
Securing the Cable Industry

RSA
SECURITY

Cable Television Laboratories

- **Consortium of *multiple systems operators (MSOs)***
- **Develop standards to promote the advancement and interoperability of cable services**
- **Proposed standards for securing:**
  - **Interactive set-top services - OpenCable Copy Protection System**
  - **Cable data services - DOCSIS BPI+**
  - **IP telephony - PacketCable Security**

RSA SECURITY

What is PacketCable?

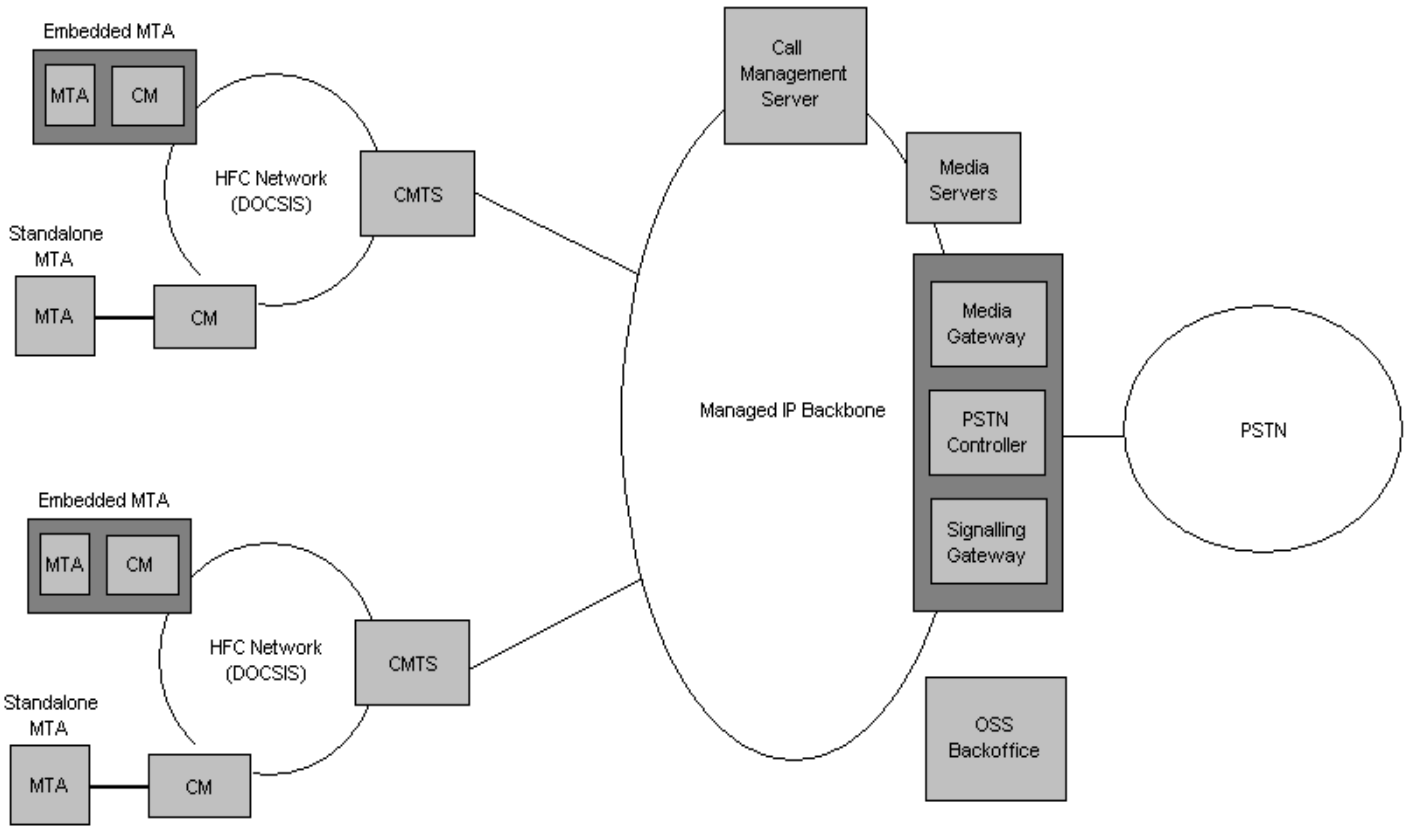
*"PacketCable is a set of **protocols** and associated element **functional requirements** developed to provide the capability to deliver **Quality-of-Service (QoS) enhanced secure communications services** using **packetized data** transmission technology to a **consumer's home** over the **cable television** hybrid fiber coax (HFC) data **network**."*

"While the initial service offerings in the PacketCable product line are anticipated to be Packet Voice and Packet Video, the long-term project vision encompasses a large family of packet-based services."

- CableLabs

RSA SECURITY

PacketCable Network Infrastructure



Application
Presentation
Session
Transport
Network
Data Link
Physical

RSA SECURITY

PacketCable Security in Detail

- **Eavesdropping:**
  - **Uses IPSec for traffic encryption (3DES, RC5, CAST, IDEA, Blowfish transforms)**
  - **Real-Time Protocol (RTP) messages secured using AES (MTA-to-MTA traffic)**
- **Device Cloning and Impersonation:**
  - **RSA key pair embedded within MTA in write-once memory – identification and key exchange between MTA and numerous other PacketCable devices**
  - **X.509 certificate installed during manufacturing**
  - ***Limited* use of digital signatures**

RSA SECURITY

PacketCable Security in Detail

- **Eavesdropping:**
  - Uses IPSec for traffic encryption (3DES, RC5, CAST, IDEA, Blowfish transforms)
  - Real-Time Protocol (RTP) messages secured using AES (MTA-to-MTA traffic)
- **Device Cloning and Impersonation:**
  - RSA key pair embedded within MTA in write-once memory – identification and key exchange between MTA and numerous other PacketCable devices
  - X.509 certificate installed during manufacturing
  - Some use of digital signatures

RSA SECURITY

PacketCable Security in Detail (2)

- **Data Insertion/Modification:**
  - IPSec provides varying degrees of integrity for *all* data packets
  - HMAC SHA1 and HMAC MD5 algorithms
- **Spoofing:**
  - Certificate-based authentication combined with encrypted (IPSec) communication
  - Relies on DOCSIS 1.1 authentication as well to bind to MAC address
- **Message Replay – IPSec anti-replay service**

RSA SECURITY

PacketCable's Use of IPSec

IPSec provides:

- **Encryption:**
  - ✓ **Transport and Tunnel modes - PacketCable uses *only* Transport mode**
  - ✓ **PacketCable uses only Encapsulating Security Payload (ESP) – no Authentication Header (AH)**
- **Message Integrity – IPSec ESP mode incorporates HMAC functionality**
- **Authentication/Key Management:**
  - ✓ **RSA key pairs/X.509v3 digital certificates or pre-shared keys**
  - ✓ **Internet Key Exchange (IKE)**
  - ✓ **Kerberos (PKINIT and KINK)**
  - ✓ **Inter-domain authentication provided by PKCROSS**
- **Routable for end-to-end security**

RSA SECURITY

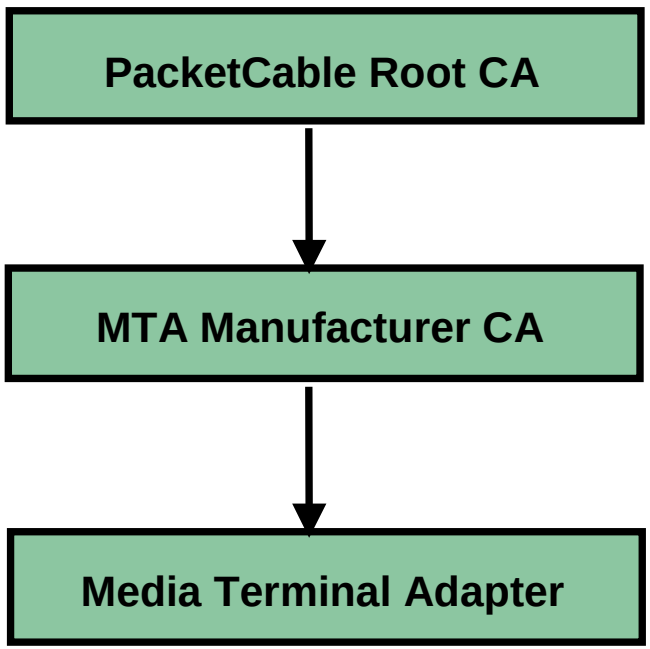
PacketCable and Public Key Infrastructure (PKI)

- **PKI and Digital Certificates provide:**
  - **Device authentication = reduced service theft**
  - **Simplified key management**
  - **Centralized trust for MSOs**
  - **Secure software upgrades**
- **PKI provides mechanism for developing trust between various communication devices (a trust domain)**

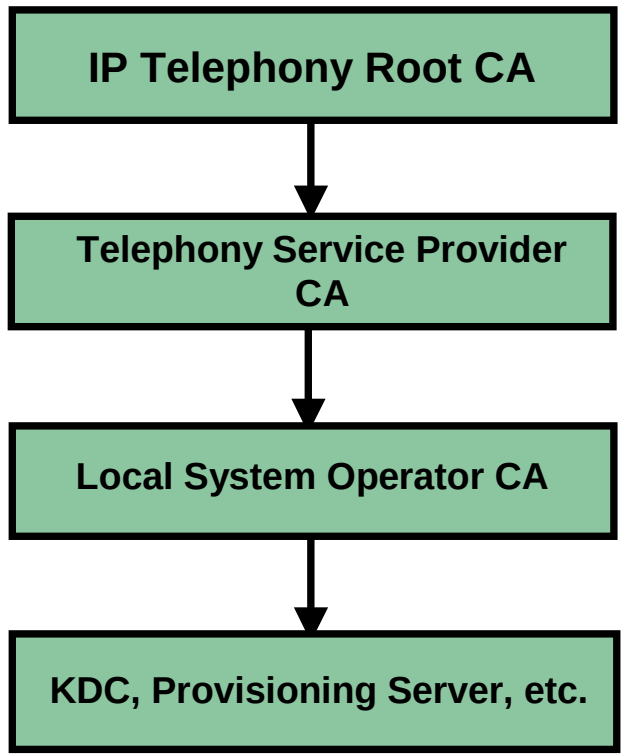
RSA SECURITY

PacketCable PKI Hierarchies

MTA Device PKI Hierarchy

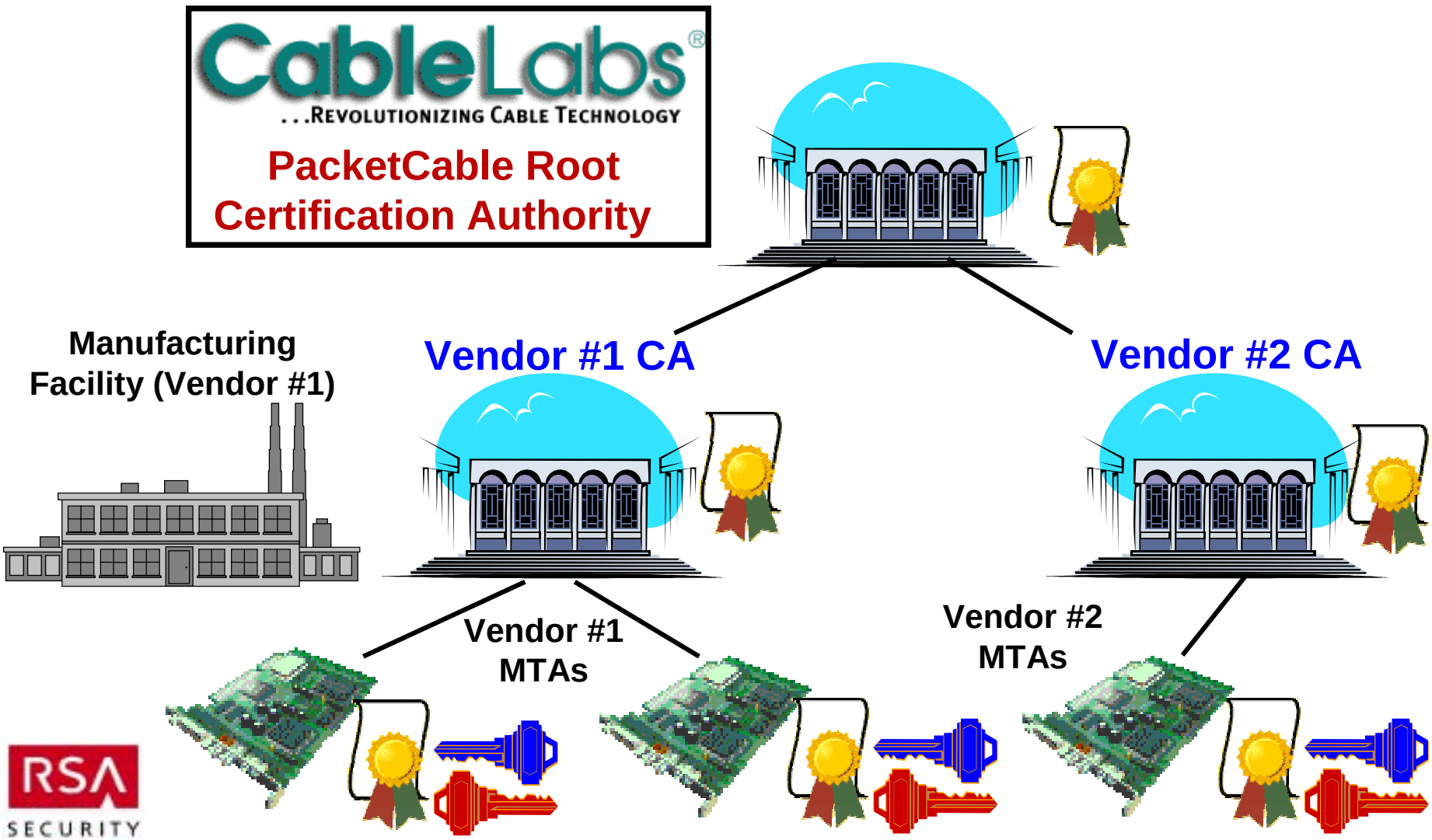


Telephony PKI Hierarchy



RSA SECURITY

PacketCable Manufacturing CAs



Signed Software Upgrades

- **PacketCable currently specifies MTAs embedded within cable modems (no standalone MTAs)**
- **Embedded MTAs utilize signed software upgrade functionality built into DOCSIS 1.1**
- **Standalone MTAs must implement software upgrade signature verification**

RSA SECURITY

Signed Software Upgrades (2)

- **PKCS#7 formatted software upgrades distributed by manufacturer**
- **Code is digitally signed by manufacturer and optionally by MSO**
- **MTA must verify signatures before installing software upgrade**
- **Requires an additional PKI hierarchy for Code Verification Certificates (CVCs):**
  - **PacketCable Root CA issues Manufacturer and MSO CVCs (one level hierarchy)**

RSA SECURITY

PacketCable Security Design Considerations and Challenges

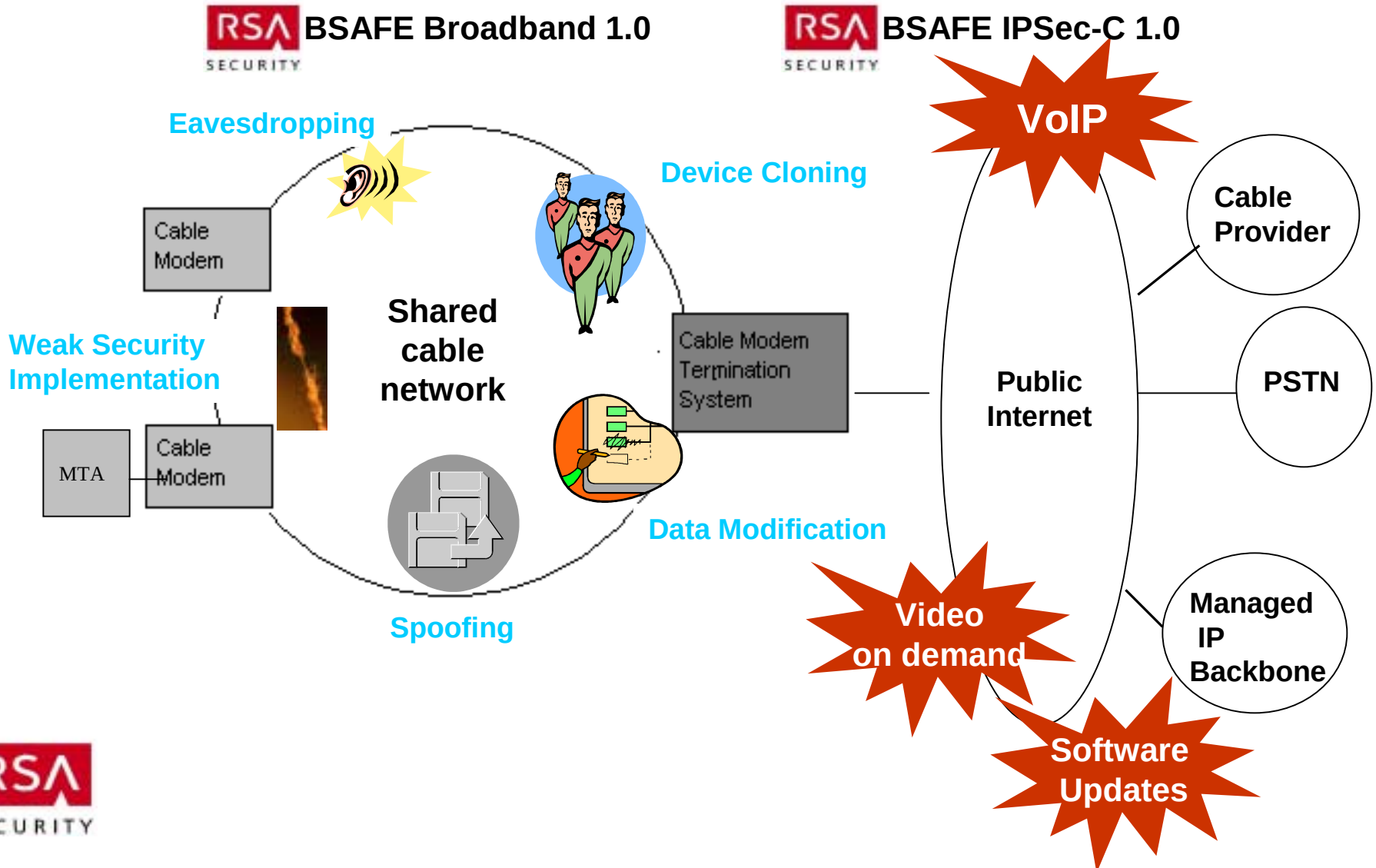
- **Many traffic encryption algorithms to choose from:**
  - **3DES is a standard, but relatively slow**
  - **RC5 is *fast* and *highly secure***
- **New form of IPSec key management:**
  - **Kerberos PKINIT and KINK**
  - **Many manufacturers lack a Kerberos test environment**
- **Must secure communications across multiple cable provider networks (more than one Kerberos domain)**
- **Must secure communication with telephony providers (disparate network architectures)**

RSA SECURITY

What Solutions are Available?

RSA SECURITY

Security Essential to Deployment of New Applications



RSA Security Products for Broadband Security

Modem, Chipset and Consumer Electronic Manufacturers

RSA BSAFE® Broadband SDK

- Currently Available
- Announcing in Europe
- Reduces risk and allows rapid compliance with DOCSIS
- Part of complete manufacturing solution

Carrier Class Gateway and Consumer Electronic Manufacturers

RSA BSAFE® IPSEC-C

- Currently available
- Tested and interoperable implementation of protocol
- One-stop shop for complete standard support
- PacketCable and VoIP opportunities today

RSA SECURITY

RSA BSAFE Broadband Features

- All crypto and certificate handling features in DOCSIS 1.0 and 1.1 specification
  - Unwrap PKCS#7 signed secure code updates
  - Verify multiple signatures attached in PKCS#7 messages
  - Parse and verify ASN.1 DER encoded X.509 certs
- Optimized cryptography for ARM and MIPS processors
  - RSA encrypt/decrypt
  - RSA with SHA-1
  - DES, AES
  - MD5
  - Diffie-Helman
- Plug & play support for VxWorks/ARM
- Compact code size

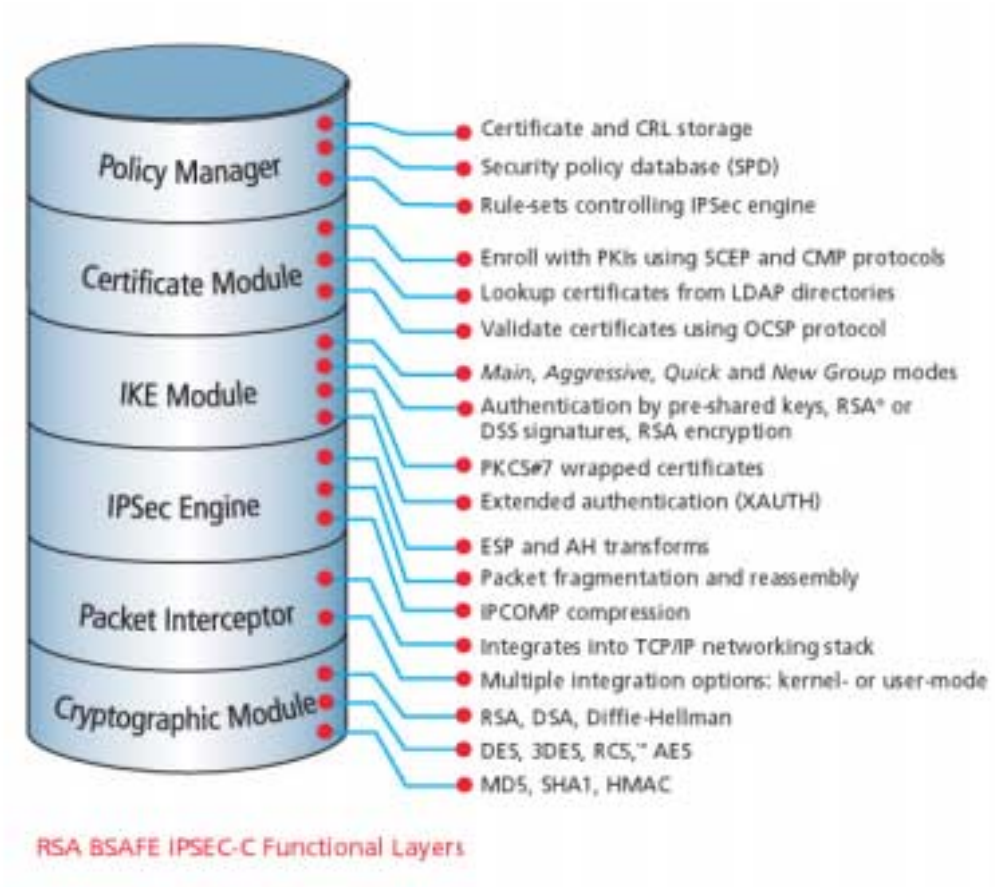
RSA SECURITY

Key Benefits of RSA BSAFE Broadband-C

- **Enables innovation while reducing risk**
  - Memory management features allows manufacturers to focus differentiating product rather than security
- **Eases and facilitates compliance with DOCSIS security standards**
  - Reduces risk, eases compliance and accelerates time to market
- **Optimizes performance and accelerates testing cycles**
  - Manufacturers using RSA Broadband 1.0 can benefit from a 10x performance enhancement
  - Performance optimizations accelerating testing at production facility
- **Trusted by CableLabs**
  - Manufacturers can now embed two decades of security experience optimized to their unique manufacturing environment

RSA SECURITY

RSA BSAFE IPSEC-C Features



RSA BSAFE IPSEC-C Functional Layers

- **Policy Manager**
  - Certificate & CRL storage, rules-set IPSec engine
- **Digital certificate support:**
  - SCEP, OCSP, CMP and LDAP protocols
- **IKE Module**
  - Authentication by RSA, pre-shared keys or DSS signature
- **IPSec Engine**
  - ESP and AH, Packet fragmentation and reassembly
- **Cryptographic Module:**
  - RSA, DSA, Diffe-Hellman, DES, 3DES, RC5, AES, SHA1, HMAC

RSA SECURITY

Key Benefits of RSA BSAFE IPSEC-C SDK

- **Simplified development**
  - **Tested and complete implementation of IPSec protocol suite**
  - **Proven quality, reliability and interoperability**
- **The industry's leading, high-performing encryption algorithms**
- **Worldwide developer support and documentation**

RSA SECURITY

RSA Security Broadband Solution

The only “one stop shop” for broadband security:

- **RSA BSAFE SDKs**
- **PKCS#7 signing tool for manufacturers to sign software downloads**
- **Broadband Certificate Authority designed to allow manufacturers to build-in trust at the point of manufacture**
- **Interoperable APIs to support third party CA services**
- **Professional Services to customize the solution**

RSA SECURITY

Software Downloads and White Papers

- **Free Software Downloads:**
  - RSA BSAFE Broadband SDK:
    http://www.rsasecurity.com/go/bbwebcast
  - RSA BSAFE IPSEC-C SDK:
    http://www.rsasecurity.com/go/bbwebcast
  - Sygate Personal Firewall SDK:
    http://www.sygate.com/partners/rsa_spf.htm
- **White Papers**
  - A Guide to Securing Cable Broadband Networks Part I: DOCSIS Security

    http://www.rsasecurity.com/products/bsafe/whitepapers/CBB1_WP_0601.pdf
  - A Guide to Securing Cable Broadband Networks Part II: PacketCable Security

    http://www.rsasecurity.com/products/bsafe/whitepapers/CBB2_WP_0601.pdf

RSA SECURITY

For more information…

- CableLabs - http://www.cablelabs.com
- RSA Security's Developer Solutions

  http://www.rsasecurity.com/solutions/developers/cablenetworks/index.html
- Cable Data News: http://www.cabledatacomnews.com

To play back a recording of today's event, or to download the slides, go to:

http://www.rsasecurity.com/events/webcast/archive.html

To complete the post-webcast survey, go to:

http://www.rsasecurity.com/go/webcast/100301/

RSA SECURITY

Thank You for Participating in Today's Webcast

The Most Trusted Name in e-Security™

www.rsasecurity.com