Securing Remote PHY Infrastructure

Pawel Sowinski, Gerry White
Cisco Systems, Inc.

Abstract

The Remote PHY (R-PHY) architecture represents the next stage in the evolution of DOCSIS and video service delivery as defined in a family of specifications under development by Cable Television Laboratories (CableLabs®). Products can be expected in the near future and operators need to understand the issues with the new technology, and start planning how to deploy it.

Unlike previous versions of DOCSIS this new architecture significantly impacts the HFC access infrastructure. The CCAP PHY components migrate into R-PHY devices (RPDs) located at the edge of the IP network, which is also extended deeper into the outside plant. To enable this evolution, existing linear optical links are converted into standard Ethernet connections and the traditional fiber nodes are replaced with IP enabled R-PHY devices.

Thus the R-PHY architecture requires MSOs to deploy a large number of IP networking devices into inherently unsecure portions of the network, such as pole mounted nodes and remote cabinets. This extension of IP deeper into the plant exposes the network to a set of security threats so that the infrastructure and the RPDs must incorporate critical security measures to protect the network, the RPDs and the customer data.

The paper outlines a comprehensive approach to ensure the security of distributed IP networks in insecure locations, using R-PHY as a specific example, taking into account the unique network, protocol, and application characteristics of R-PHY systems. The authors assess the scope of security threats, propose mitigation techniques to address the identified vulnerabilities and recommend security requirements for individual network components. In particular, the paper details such procedures as the secure authentication of RPDs to prevent unauthorized access to the MSO's IP network and approaches to secure R-PHY control and data connections.

In summary, the paper demonstrates why, where, and how standards-based, distributed IP networks can be secured in a cost effective and interoperable manner using R-PHY as a specific example.

INTRODUCTION

Until recently, the conventional wisdom perceived network security as a complicated subject, which was historically understood and tackled by only well-trained and experienced experts. This view is changing in todays, post Snowden world as security awareness takes a prominent place in the global zeitgeist. Not a single week passes without news of significant cybercrimes by various perpetrators such as thieves/hackers, disgruntled employees, organized criminals, terrorist organizations, or even state-sponsored groups. New attack vectors and threats are identified every day.

A recent survey of governments, businesses, and individuals in the U.S., China, Russia, and India found that more than 88% of respondents believe that cyberspace threats are significant. While many respondents feel comfortable with online banking and shopping, more than 69% are not comfortable with sharing identity and personal data online.

This is a valid concern—the latest Internet Crime Report by the Internet Crime Complaint Center shows an increase in cybercrimes, as thieves seek out personal data and other valuable information for their own advantage or as hackers disrupt operations of businesses for various reasons.

In fact, the threat of cyberattacks has been elevated to one of the nation's most pressing security, economic and safety issues. In this year's State of the Union speech president Obama pushed Congress to bring cybersecurity legislation to fruition in order to combat emerging attacks. "No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids," Obama said in his address. "We are making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism."

As developers of equipment and operators of networks we have the responsibility to react to this rapidly changing environment and actively work to provide security for vulnerable components such as R-PHY Devices.

A lot parallels can be drawn between R-PHY devices and Internet of Things (IoT) devices. Earlier this year the Federal Trade Commission released a report on critical security and privacy issues related to IoT technology. The FTC's report proposes security guidelines for manufacturers of IoT devices. The FTC hopes that "by adopting the best practices we've laid out, businesses will be better able to provide consumers the protections they want and allow the benefits of the Internet of Things to be fully realized".

The FTC's press release outlines a number the guidelines for companies developing Internet of Things technology from which we selected four (out of total six) summary recommendations best fitting R-PHY security concerns. The FTC report recommends to:

- "Build security into devices at the outset, rather than as an afterthought in the design process;
- When a security risk is identified, consider a "defense-in-depth" strategy whereby multiple layers of security may be used to defend against a particular risk;
- Consider measures to keep unauthorized users from accessing a consumer's device, data, or personal information stored on the network;
- Monitor connected devices throughout their expected life cycle, and where feasible, provide security patches to cover known risks."

While R-PHY deployments will never reach even a small fraction of the scale of IoT, which already has over 25 billion devices, the FTC's guidelines are equally relevant to Remote PHY security.

SCOPE

The paper primarily focuses on the digital networking aspects of R-PHY system security, especially those elements that impact external network or programming interfaces of the RPDs and the MSO systems with which they interoperate.

We decided that other security concerns fall out of scope of the paper, for example, how to ensure the physical security of RPDs or how to deter R-PHY device theft. We expect that manufacturers of RPDs will individually incorporate effective elements of physical security in RPDs such as tamper proof enclosures or the ability to raise alarms if the device's access doors are open by unauthorized person.

Those features however, in most cases do not require standardization or directly impact other systems and therefore are less interesting for a discussion on the security of an IP network infrastructure built for physically insecure locations.

REMOTE PHY

Remote PHY (R-PHY) is the next stage in the evolution of DOCSIS and video service delivery. It is a modification of the current CCAP architecture in which the PHY components are moved from the CCAP platform into a separate Remote PHY Device (RPD). The RPD is connected to the CCAP Core (CCAP minus the RF PHY) by an IP network. The combination of CCAP Core and RPD provides the functional equivalent to the integrated CCAP. Essentially R-PHY takes the digital interface to the PHY component from the circuit board in the CCAP and extends it over the IP network to the RPD using pseudowire technology as shown in Figure 1 and Figure 2.

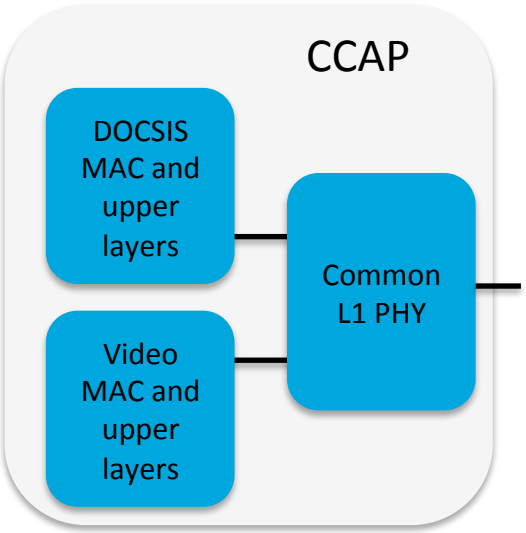

Figure 1 - Integrated CCAP

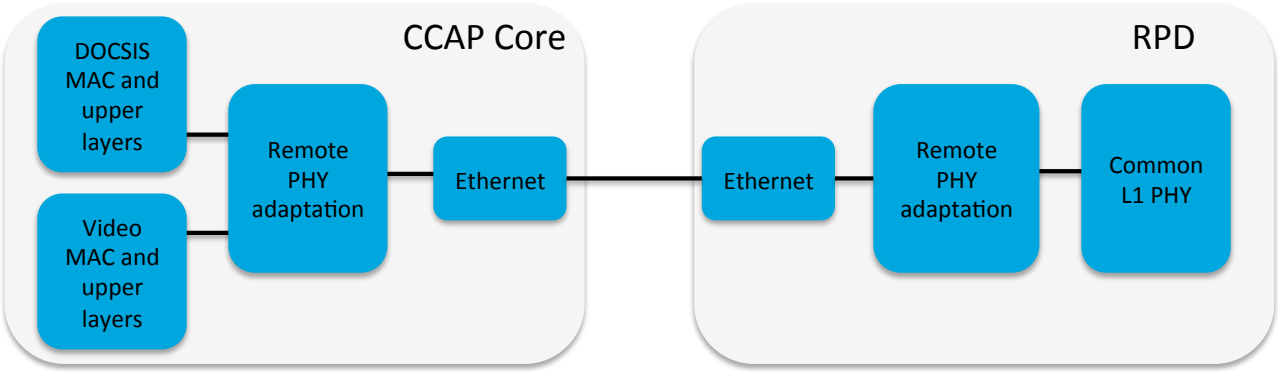

Figure 2 - CCAP with Remote PHY

This has the effect of moving the digital to RF conversion from the CCAP Core, located in the head end or hub, to the RPD located deeper in the network, such as in a fiber or optical node. Standard digital optics (e.g. Ethernet) can be used for the CCAP to RPD link in place of the analog optics previously used. RF over coax or analog fiber is used for the RPD to CM link, which is now much shorter. This extends the all digital IP network deeper into the plant providing advantages in lower cost, simpler operation and better performance. The migration of the physical layer from the CCAP to the RPD is transparent to the external DOCSIS infrastructure and CPEs so that these can be used unchanged as shown in Figure 3.

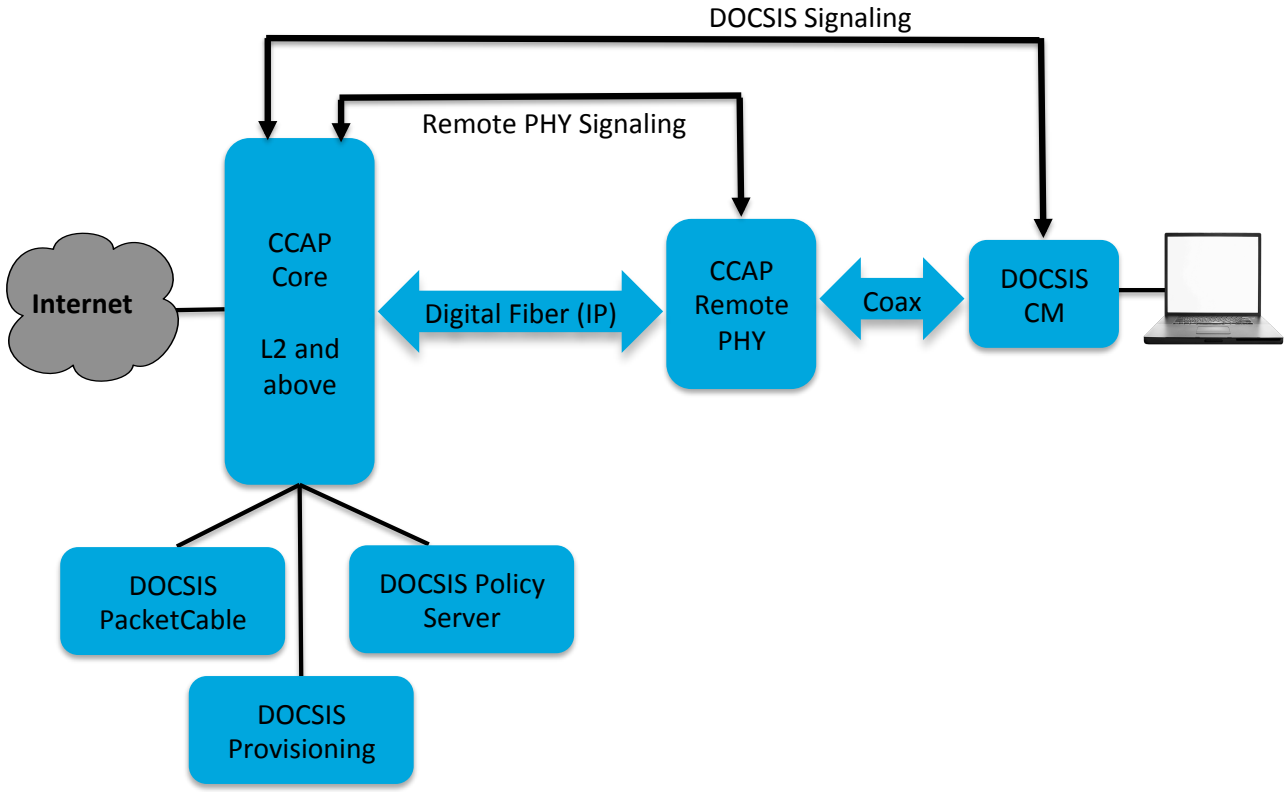

Figure 3 - RPD Deployment Environment

For a more in depth view of R-PHY please refer to [R-PHY SCTE] and [R-PHY NCTA].

R-PHY SECURITY ENVIRONMENT

In the next several years Cable Operators could potentially install hundreds of thousands of RPDs in their networks. The majority of them will be deployed as Fiber Node replacements and will be installed in inherently unsecure locations, such as pole mounted nodes and remote cabinets. The fibers which are today carrying analog HFC signals will be converted to digital use as primarily 10-gigabit Ethernet links carrying IP

data. This extension of IP deeper into the plant exposes the network to a set of security threats so that the infrastructure and the RPDs must incorporate critical security measures to protect the MSO's network, the RPDs and the customer data. Before attempting to solve this problem we will first examine how introduction of R-PHY changes the MSO's network and assess the newly introduced security threats.

As shown in Figure 4 an integrated CCAP is deployed in a head end or hub location with analog fiber / coax links to the DOCSIS CMs and video STBs. In either head end or hub deployments the CCAP is placed in a physically secure location, typically in protected network equipment buildings in a hub. Physical access to the CCAP equipment is granted only to authorized personnel. Network access to the CCAP is secured with a wide range of features including multilevel access, authorization controls and traffic control features such as source verify, access control lists and network domain isolation.

The optical node, CMs and STBs are in unsecure (from the operator's perspective) customer premises so that additional security mechanisms are required. Thus CMs must comply with the DOCSIS security specifications and video devices must comply with one of the proprietary video security schemes in use. In both cases authentication of the end device is required and traffic on the CCAP to CPE links is protected by encryption. The optical node is a physical layer optical to coax converter, is transparent to the security mechanisms used and is less susceptible to security threats. The trusted network boundary is aligned with the boundary of the HFC plant, which carries analog RF signals and inherently limits exposure to active threats. While some operators have seen isolated attempts at theft of service based on "perfect" replication of the CM hardware, such attempts are relative easy to identify and defend against.

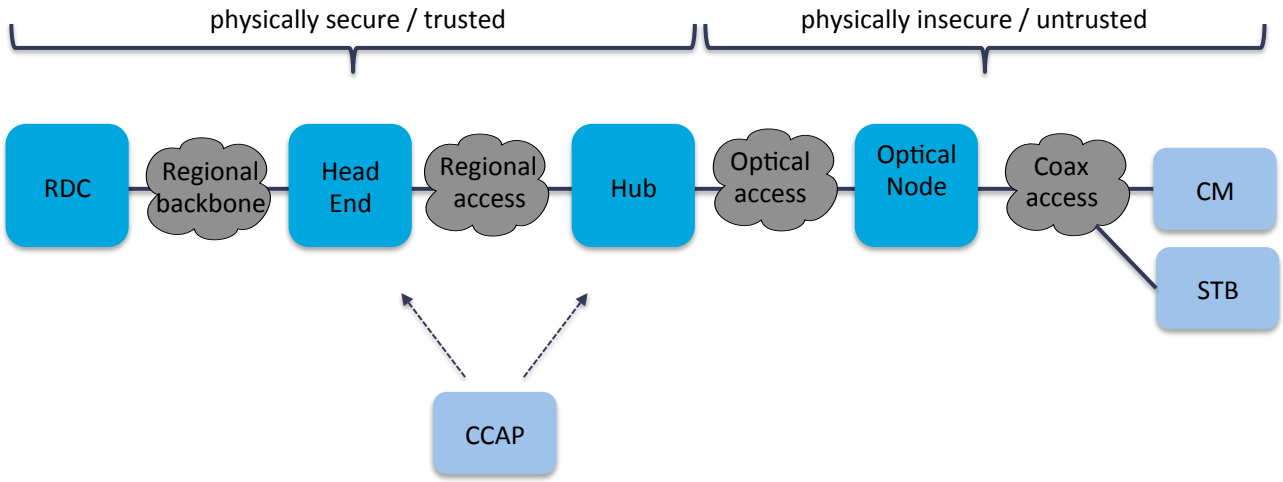

Figure 4 - CCAP Deployment Options

As shown in Figure 4 the deployment options for an R-PHY solution are more diverse. With the transition away from analog optics the CCAP Core may be deployed at a Regional Data Center (RDC) deeper in the network or in the same head end and hub

locations as an integrated CCAP. All of these are physically secure locations. An RPD may be deployed in secure head end or hub locations but may also be deployed much deeper in the network in an inherently unsecure location such as a street cabinet or a fiber node. With the deployment model when both CCAP Core and RPD are within the trusted part of the network the requirements for authentication or security between these devices can be relaxed or made optional. The combination of CCAP Core plus RPD provides the same functionality as an integrated CCAP so that the existing DOCSIS and video security to the CMs and STBs remains in place with traffic in the untrusted portion of the network encrypted as with the integrated CCAP.

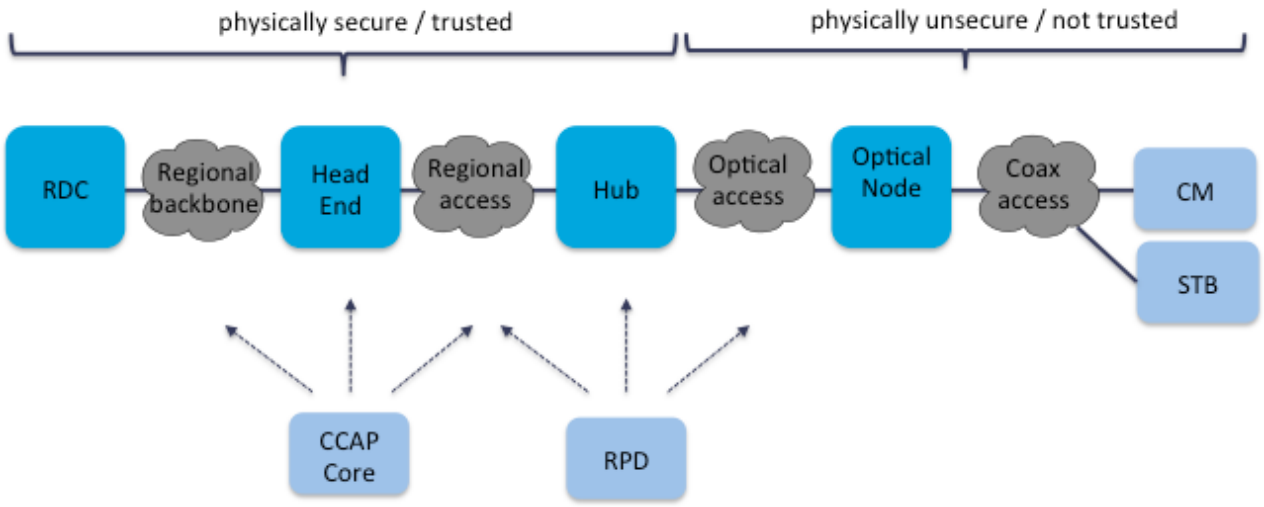

Figure 5 - R-PHY Deployment Options

When the RPD is deployed outside the physically secure domain such as in a street cabinet or optical node the security exposure is raised. The DOCSIS and video traffic is still encrypted between the CCAP core and the CMs & STBs so that it is not vulnerable to attack but the RPD represents a potential vulnerability. The RPD must be connected to the MSO IP network so that it can access not only the CCAP Core but also IP devices such as DHCP servers and network management systems. Thus the RPD requires access to the trusted network and so presents a potential point of ingress for attacks on the MSO network and services. An analysis of the threats and options for their mitigation follows.

ASSESSMENT OF SECURITY THREATS

Remote PHY equipment, in particular the RPDs, represents an attractive target for cyber attackers. RPDs become a part of the critical infrastructure through which the cable operators deliver services representing the bulk of their revenues. Assuming the success of the technology, it's conceivable that at some point the largest share of US broadband and video will be delivered with the aid of R-PHY technology. It is a distinct possibility that in a few years time an RPD will participate in the transport of internet traffic between our homes and the rest of the digital world. As mentioned earlier, attackers can easily gain physical access to RPDs because the majority of RPDs will be installed in

unsecure locations and include externally accessible Ethernet ports.

Unauthorized Network Access

In the opinion of the authors, unauthorized network access represents the most pressing security threat resulting from introduction of the R-PHY. Since the RPDs are attached to the Converged Interconnect Network (CIN), not directly to the CCAP Core, an attacker impersonating an RPD may gain access to the CIN, the MSO internal network and the devices and systems interconnected by it.

As a result of the unauthorized access to the MSO network, the attacker may be able to further exploit the vulnerabilities of the network to steal data or service, conduct cyber-espionage, eavesdrop on and tamper with customers' data or even disrupt the MSO's operations by launching Denial of Service (DoS) attacks or by other methods.

As countermeasures, the RPDs and the network they attach to must provide means for effective secure authentication and authorization of RPDs onto the MSOs network. Given the scale of RPD deployments, the processes and provisioning of these functions must be automated and minimize any configuration effort.

Customers' Data Privacy

The RPDs do not collect or maintain any subscriber data. However the customer traffic passes through the RPD. The RPD provides purely PHY layer functions; it does not perform any function that requires examination or modification at MAC or higher layers. The customer's traffic delivered via DOCSIS and video service is already effectively protected by BPI+ encryption or video encryption schemes.

Could a very sophisticated attacker posing as an RPD somehow compromise the integrity of those schemes? Conservative assessment leads to the conclusion that it is impossible to completely eliminate such a possibility. However, the authors are not aware of any documented history of significant breaches of these techniques. The threat to the integrity or privacy of encrypted customer data passing through the RPD link is low when the operators take advantage of established encryption techniques.

Theft of Service

The vulnerability towards service theft is similar to threats to Customer's Data Privacy. Because the service data is protected at a higher level and passes through the RPD opaquely, we believe that the RPD's exposure to theft of service appears to be low.

Denial of Service Attacks and Service Disruption

An RPD attaches to the MSO network through one or more high capacity links, typically 10 Gb/s Ethernet. This creates the potential for the RPD H/W platform to become a potent tool for origination of Denial of Service attacks on the operators' network. A "hijacked" RPD or a device impersonating an RPD could be used to inject a high volume of traffic into the MSO network and facilitate a DoS attack on network infrastructure e.g. DHCP, DNS servers or CCAP Cores.

Another possibility is disruption of network operation through the injection of routing or control protocol packets, for example "duplicate" IGMP joins. The countermeasures to these types of threats include securing access to the RPD itself, mandating secure software update, secure boot technology and effective network access authentication.

Other Threats

The authors believe that the outlined security threats represent the most serious risks associated with a R-PHY deployment. In the rapidly changing security environment new threats will undoubtedly emerge. While we cannot predict the future precisely we believe that the best approach is for the R-PHY architecture to adopt a defense in depth strategy, which can be upgraded over time to address emerging threats.

PROPOSED SOLUTIONS

The previous sections of the paper have described the security vulnerabilities raised by RPD deployment outside the trusted network. Fortunately security technologies and practices are available to provide a viable alternative to physical security. The nature and use of these options is discussed in depth in the paper.

As with many complex problems the simplest approach is to divide the problem into a number of components and address these one by one. In this case we have broken the problem into the following sub problems as shown in Figure 6:

1. Protecting the integrity of the trusted network by controlling access to it from the RPD
2. Requiring mutual authentication between the CCAP Core and the RPD and protecting the control plane transactions between them.
3. Protecting the data plane from the CCAP Core through the RPD to the CM
4. Protecting the software integrity of the RPD

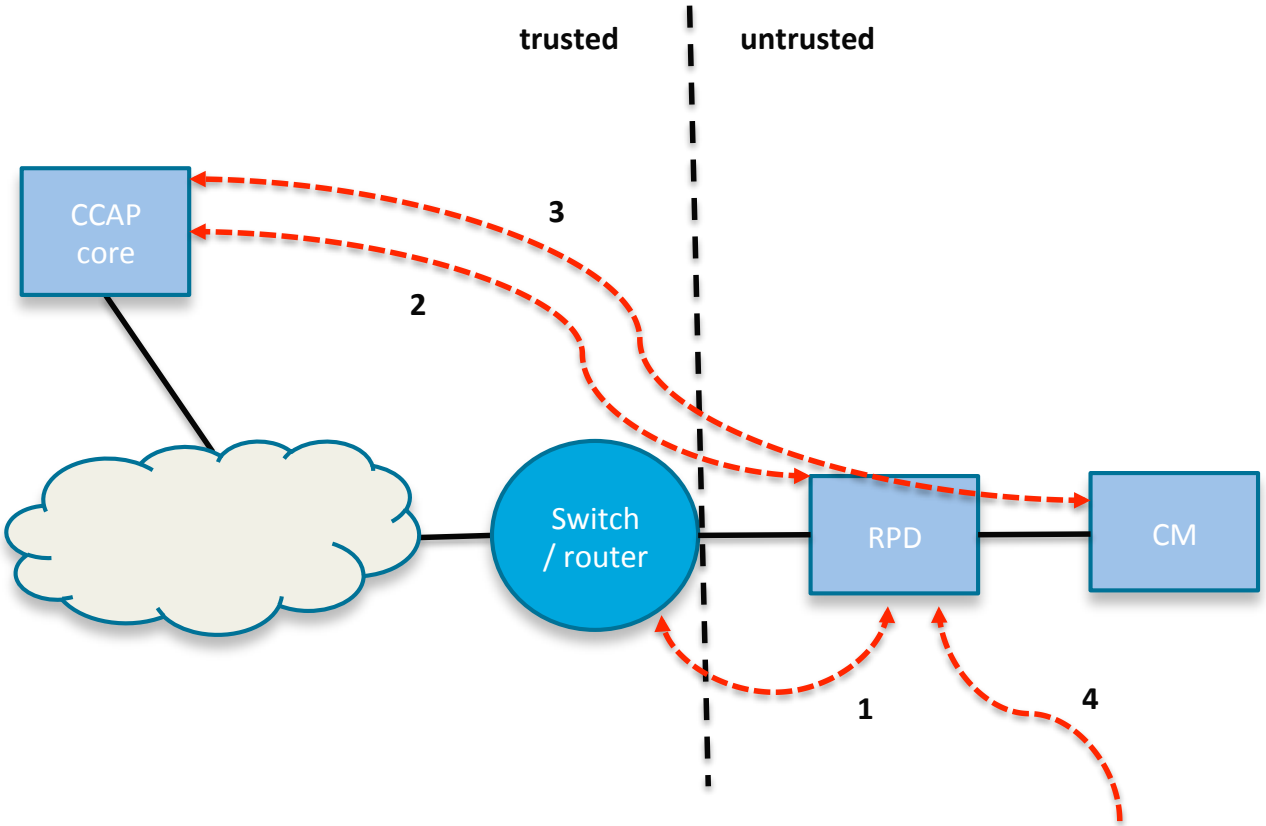

Figure 6 - Problem Set

The following sections of the paper will address these items in turn.

Protection of the Trusted Network

As mentioned earlier the RPD may be deployed in an unsecured location (refer to Figure 5) and is based on standard network technologies such as IP and Ethernet. Thus the RPD represents a point from which an attack could be launched on the MSO trusted network. In order to protect against this it is necessary to control access to the trusted network by an RPD. Fortunately similar problems have been addressed for Ethernet and WiFi networks and standard solutions developed which can be leveraged. In this case we have chosen to use the 802.1X Port Based Network Access Control standard developed by the IEEE [IEEE 802.1X] and supported by virtually all Ethernet equipment vendors .

802.1X Authentication

802.1X is a port based access mechanism used with Ethernet switches. Each port on the switch may be either fully open, fully blocked or allow a subset of packets only e.g. for device management. When the RPD is first connected to a switch port it will receive restricted or no access to the trusted network (depending on switch configuration). 802.1X messages are exchanged to identify the RPD and unblock the port if the RPD is recognized as authorized for the network.

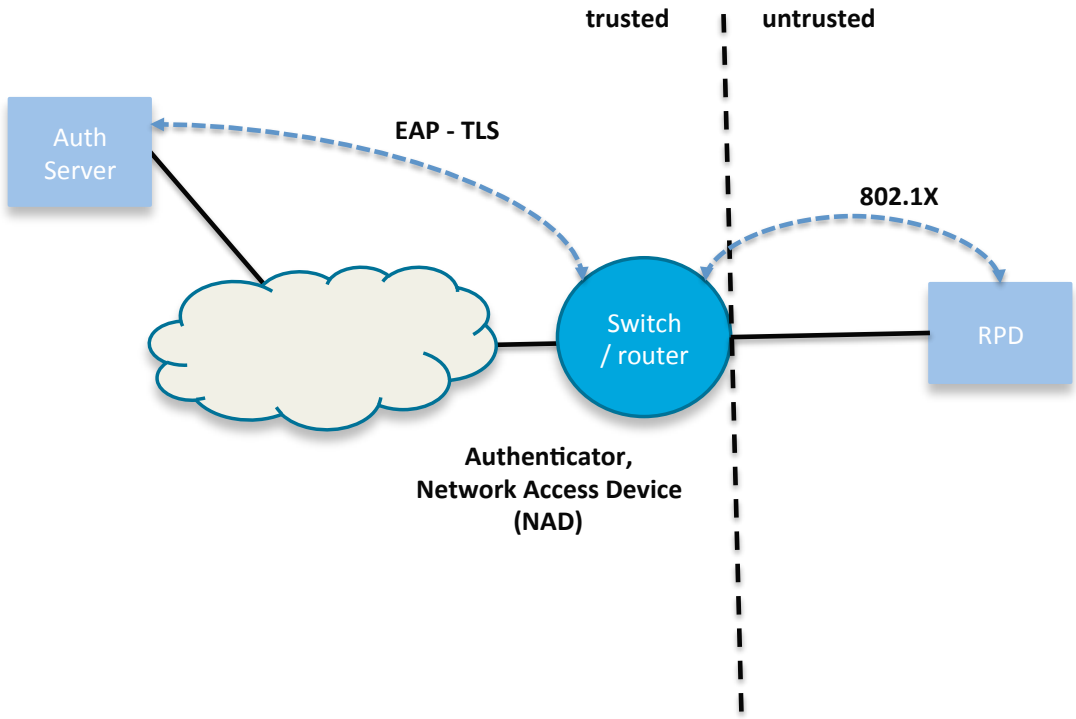

Figure 7 - 802.1X Authentication

An RPD deployment using 802.1X is shown in Figure 7.

There are three components involved in the process:

- **The Supplicant** is the device wishing to gain access to the network, in this case it is the RPD.
- **The Authenticator** is the Network Access Device (NAD), the switch or router, located at the edge of the trusted network to which the RPD must connect to in order to gain network access. The NAD itself is within the trusted domain and acts as the gatekeeper for the trusted network
- **The Authentication Server** contains the database and policy used to control access.

802.1X uses EAP, the Extensible Authentication Protocol [IETF RFC 3748], to enable authentication using a centrally administered Authentication Server. It defines EAP encapsulation over LANs (EAPOL) for communication between the supplicant (RPD) and the authenticator (NAD), which are connected directly over Ethernet. The authenticator and the authentication server exchange EAP messages over an IP network using Radius or Diameter.

Message Exchanges

The supplicant (RPD) presents credentials to the authenticator (NAD), which forwards these to the authentication server for verification. The authentication server determines the validity of the credentials and informs the NAD whether the supplicant is allowed to access the trusted network.

The message exchange used to establish authentication is shown in Figure 8.

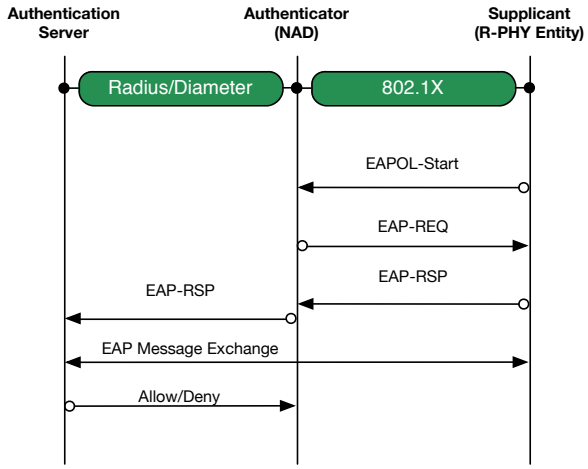

Figure 8 - 802.1X Message Exchange

The RPD informs the Authenticator of its existence using an EAPOL-start message. The authenticator generates an EAP-REQ to ask for credentials. The RPD returns these in an EAP-RSP, which is forwarded to the authentication server. The RPD and authentication server exchange EAP messages (via the authenticator) and on completion of the process the server informs the authenticator and the RPD of the result. At this point if the RPD is allowed access the Authenticator opens the switch port.

Security Credentials

In this case the credentials used are X.509 certificates issued by CableLabs, which are very similar to those used to authenticate cable modems. This enables both operators and equipment vendors to leverage existing processes for certificate deployment and validation.

MACsec

In its basic form 802.1X controls network access for a single host connected to a switch port. This is shown in Figure 9 as scenario 1. However once the port has been opened for an authenticated device it is also open for any

other devices on the same physical port. This can be problematic in some topologies such as when multiple hosts are connected via a daisy chain or through a hub as shown in scenarios 2 and 3. It is also susceptible to a device masquerading as valid by spoofing the MAC address of an authenticated system and to man in the middle attacks by inserting a rogue device between the RPD and the NAD.

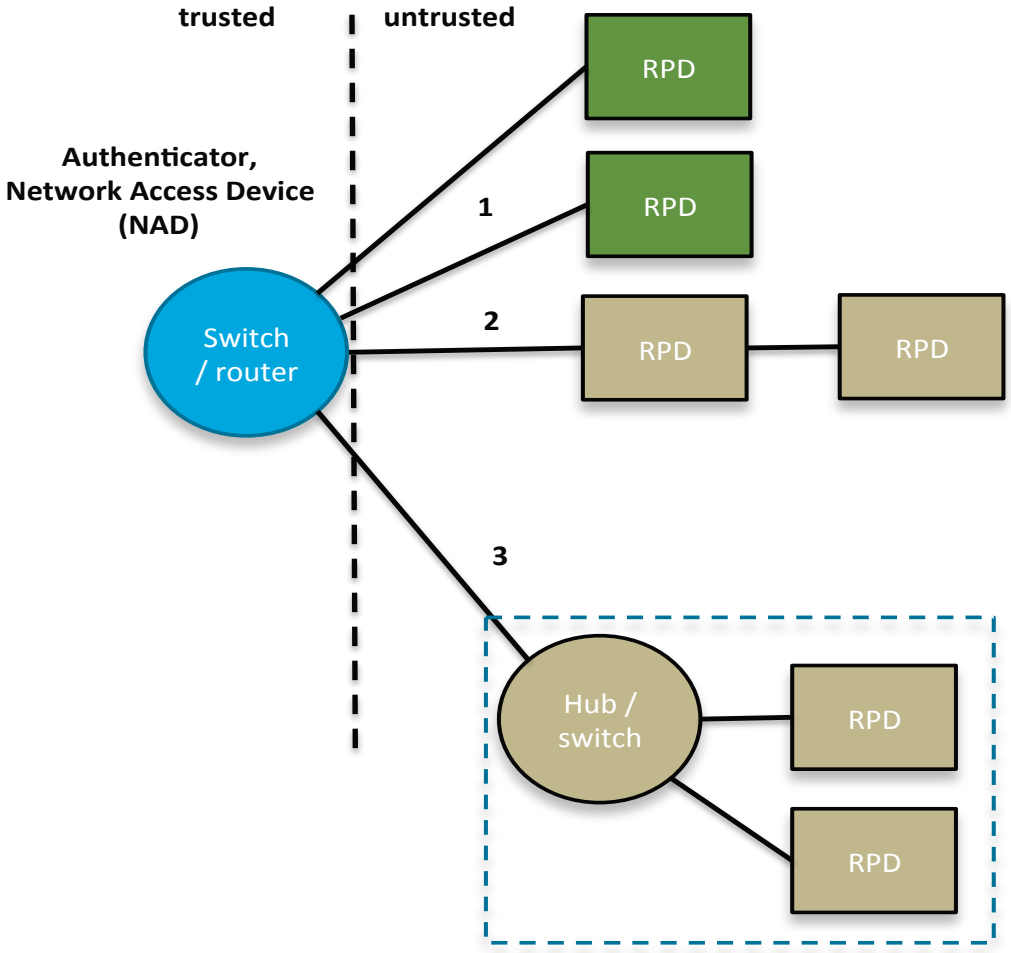

Figure 9 - RPD Deployment Topologies

To address these cases an additional mechanism, 802.1AE (MACsec) is required.

For each device connected to a physical port on the NAD MACsec defines a virtual port. A connectivity association is established between the virtual port and the MAC address of the device. Each device is authenticated via the EAP mechanism as previously described.

Security keys are derived for the connectivity association from the keying material in the EAP exchanges. Thus each connectivity association (and hence attached device) has its own encryption keys, which are used to secure messages between the NAD and the device using AES128 encryption. This enables multiple devices per physical port to be supported and prevents address spoofing or man in the middle attacks.

Mutual Authentication and Control Plane Protection

A second piece of the security architecture is mutual authentication between the CCAP Core & RPD. This is required to resolve the following risks:

- RPD could launch DOS attack on CCAP
- RPD control traffic could be hijacked to deny network access to CMs
- RPD could be replaced to enable a man in the middle attack of subscriber traffic
- A spoof CMTS could attach to the RPD for CM traffic capture

Mutual Authentication

Both the CCAP Core and the RPD are issued with X.509 certificates by Cablelabs and both have securely stored private keys. The Internet Key Exchange protocol version 2 (IKEv2) is used to facilitate mutual authentication based on these keys and certificates. IKEv2 is an IETF defined standard that is widely deployed to secure communications across the Internet. It is documented [RFC 7296] elsewhere and will not be covered in any detail in this paper.

IKEv2 provides the following important functions for the CCAP core to RPD interface as shown in Figure 10:

- Authentication of the two endpoints. The CCAP Core and the RPD exchange certificates provided from the Cablelabs certificate infrastructure. Each device (CCAP and RPD) can independently verify the authenticity of the certificate it has received from the other using standard mechanisms [ref RFC 5280]. Messages signed by the private key of each device and decoded using the public keys (from the exchanged certificates) ensure that each device is who they claim to be.
- Generation of security keys. Following the authentication exchange shared keying material is generated which is then used to secure future exchanges.
- Negotiation of a set of security profiles. Each profile defines which traffic is to be protected by the profile and the cryptographic algorithms to be used. For the RPD to CCAP interface two profiles are used.
  - For the Generic Control Plane (GCP) traffic used in general RPD configuration.
  - For the L2TPv3 control plane used for tunnel control.
- Periodic updates to security keying material as needed over time.

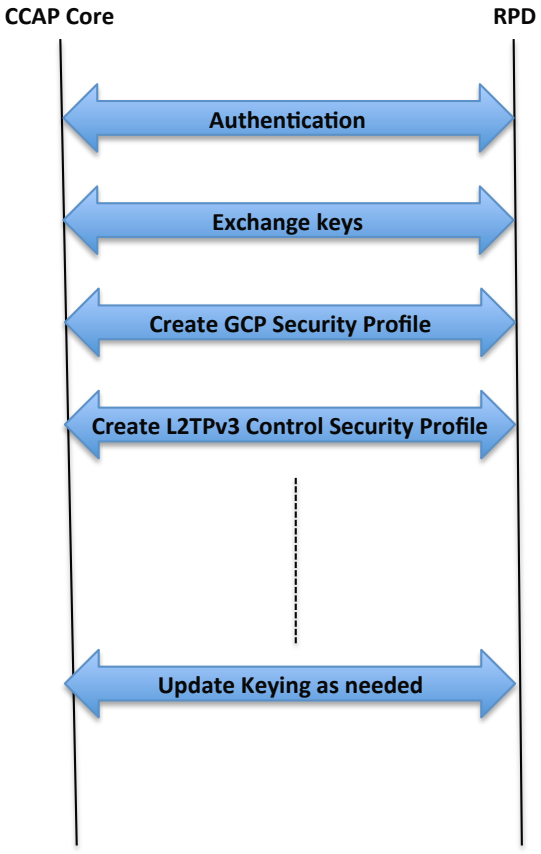

Figure 10 - IKEv2 Functions

Control Plane Protection

During the IKEv2 message exchanges the CCAP Core and RPD negotiate a security profile. This defines the traffic to be protected and the algorithms and keying material to be used. Internet Protocol Security (IPsec) is then used to secure the control plane by authenticating and or encrypting the payload. As with IKEv2 IPsec is a widely deployed Internet standard.

An operator can choose whether to select encryption and authentication or use authentication only. Authentication without encryption leaves the payload open to inspection but still prevents tampering with commands and requires fewer resources. This is shown in Figure 11.

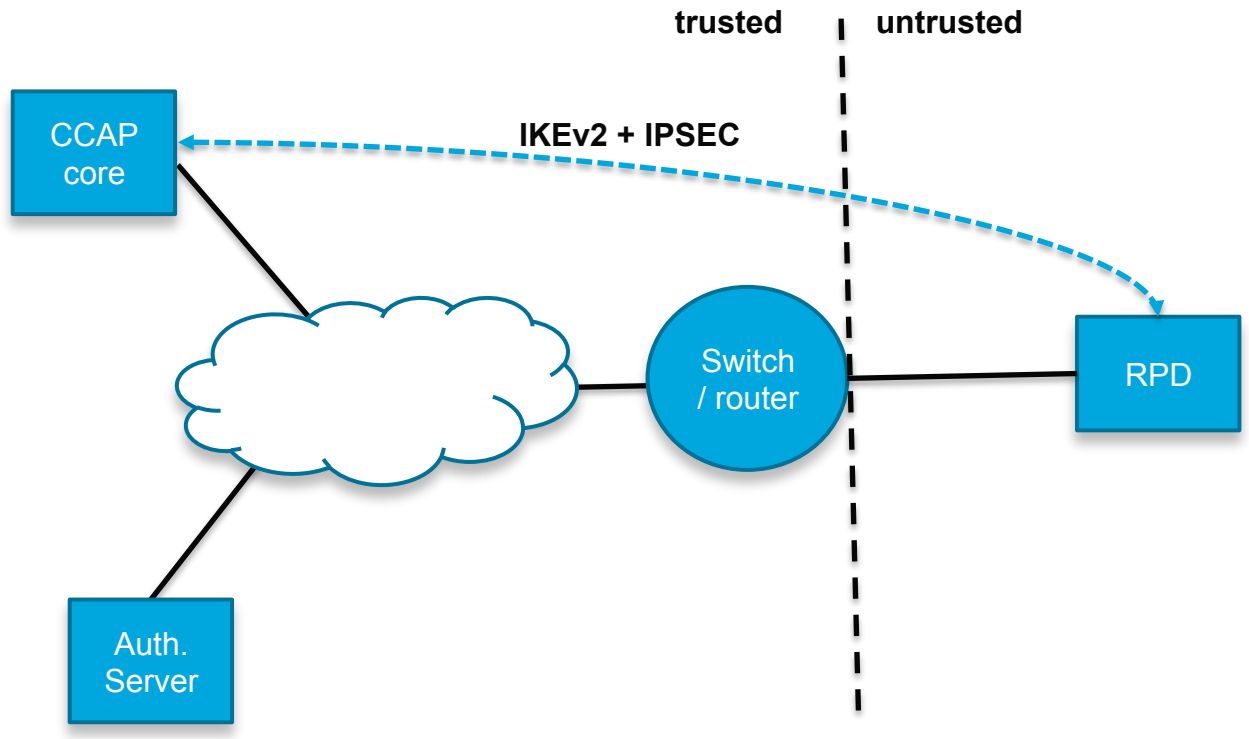

Figure 11 - Control Plane Protection

Data Plane Protection

In an R-PHY deployment the data plane traffic is carried over IP/Ethernet links between the CCAP Core and the RPD where it is converted to RF for transmission to the CM or STB. The CM and STB have always been in locations outside the operators control and the mechanisms to secure this traffic based on DOCSIS BPI and video encryption algorithms are widely deployed and well understood.

The RPD simply provides a physical layer conversion of the data plane from digital to analog with no impact on the end to end security mechanisms, which can continue to operate unchanged. This is a major advantage of the R-PHY over more complex distributed

architectures working at higher layers of the protocol stack.

Figure 12 illustrates the set of security mechanisms used to protect an RPD based network.

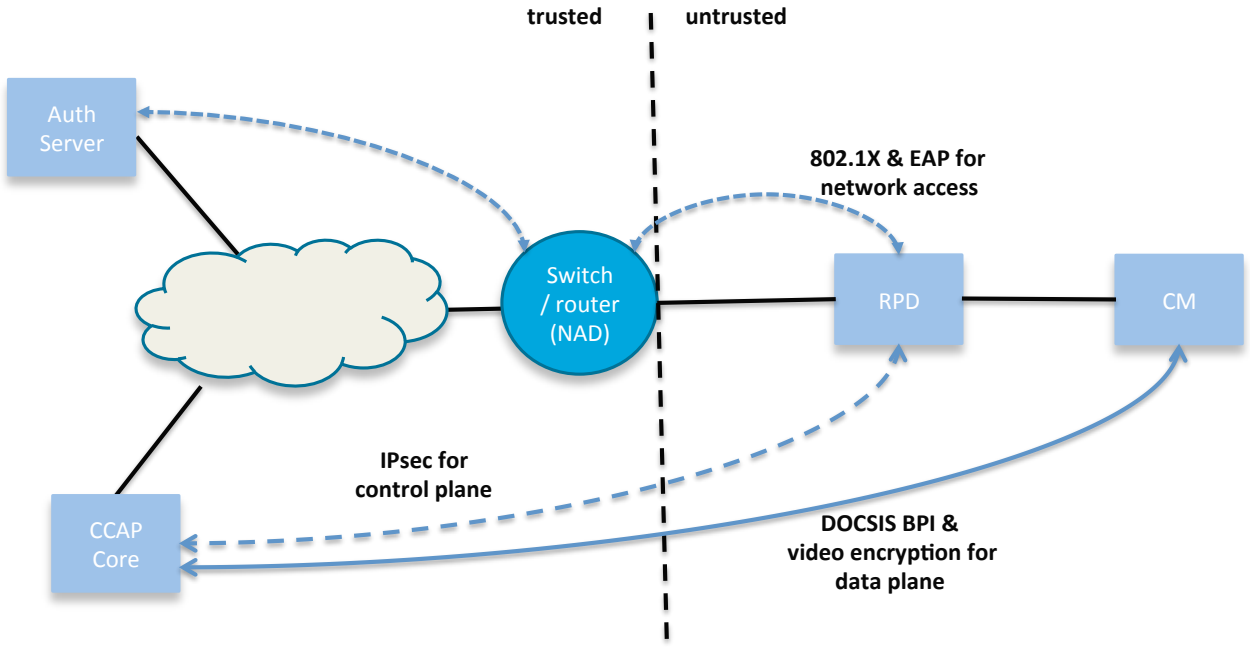

Figure 12 - RPD Based Network Security Architecture

Integrity of RPD Software

Another layer of security provides protection for the software running on the RPD from unauthorized modification. If an attacker was able to replace or modify the software running on the RPD it would open the possibility of misusing the RPD in ways the paper explained earlier.

Two functions provide the foundation for protection of the software integrity. These are Secure Software Download (SSD) and Secure Boot. Additional features augment them by limiting exposure to unauthorized modification during software execution.

Secure Software Download (SSD)

Software upgradeability is one of the most basic requirements for any computing or networking system. Cable operators need to periodically download new versions of software onto their RPDs to add new features, to fix bugs … and sometimes to address security vulnerabilities. Authenticating the source and verifying the integrity of downloaded code is fundamental to the security of R-PHY architecture.

The principles, including code signing requirements for RPD secure software download, and many implementation details have been adopted from the DOCSIS 3.1 Security Specification. Broadly speaking,

with respect to secure software download; the RPD assumes the functions of a DOCSIS Cable Modem.

It is envisioned that such an approach will allow the operators to reuse the majority of the OSS infrastructure already deployed for CM software and security certificate management to perform equivalent functions for RPDs.

To download an RPD software image securely, the RPD vendor and/or MSO will digitally sign the image using the appropriate code verification certificate (CVC) and place the image on a Software Download server.

The operator can trigger the download of the software image via parameters obtained by the RPD from the CCAP Core in the control protocol, or directly via SNMP commands.

After an RPD downloads a software image, it validates the image by verifying that the included CVC chains to the Root CA Certificate trust anchor, and by checking the image's digital signature. If this validation is successful, it installs the software image for operation.

Secure Boot and Software Execution

To complement secure software download, RPD vendors may choose to implement a set of features to further ensure that the integrity of the executed software has not been compromised. Secure Boot offers the prospect of a hardware-verified, malware-free bootstrap process that can improve the security of many system deployments.

Secure Boot technology ensures that the first code executed on a hardware platform is authentic and unmodified, establishing a root of trust in the system to build upon. This sets the foundation for establishing a full chain of trust to validate all levels of software executing on the hardware platform, including multiple phases of the boot process and the final executable image. The Secure Boot chain of trust is often attached to an immutable hardware anchor which provides secure device identity. [802.1AR-2009] describes a standard for a secure device identifier (DevID) which is a cryptographic identity bound to a device and used for assertion of the device's identity. IEEE 802.1AR compliant devices can rely on CableLabs issued RPD device certificates explained later in the paper and the executable image signing procedures of SSD.

Reliance on a secure, hardened hardware based anchor eliminates or at least raises the difficulty bar for bit-by-bit cloning of an RPD along with its identity, a scheme sometimes exploited with DOCSIS Cable Modems.

To date, multiple platforms and vendor companies have implemented secure boot techniques, including Linux, Apple, Microsoft, Cisco and MicroSemi. Secure boot implementations are generally considered proprietary as platforms and operating systems vary in requirements. RPD vendors may decide to choose different computing platforms for their RPD products. For those reasons, and because Secure Boot does not involve any external interfaces we feel that Secure Boot implementation choices should be left to individual vendors rather than be mandated by a standard specification.

Run Time Integrity and the other secure coding processes prevent many security attacks, for example Day Zero attacks. Some of the Run Time Integrity technologies that could be used in an RPD include Object Size Checking, Address Space Location Randomization, and executable space protection. We highly recommend that

vendors include these or similar mechanisms for added protection.

Security Certificates

R-PHY security protocols rely on digital certificates for establishing device identity, for authentication of key exchanges between RPD and NAD and between RPD and CCAP Core as well as in verification of the software downloaded to the RPD. Like BPI+ certificates, the R-PHY certificates are based on [X.509] standard version 3. In fact, the R-PHY digital certificates scheme mostly reuses the new Public Key Infrastructure (PKI) defined in [DOCSIS SECv3.1].

R-PHY brings two straightforward extensions to the new CableLabs PKI certificate hierarchy. The CableLabs Device CA Certificate, which in DOCSIS is used to sign Cable Modem CA Certificates, will be utilized to issue RPD Device Certificates.

A new CableLabs Service Provider CA Certificate will be created to serve as a root of trust for certificates issued to MSOs or CCAP Core vendors. The Service Provider CA will be hosted by CableLabs or an approved 3rd party which issues AAA Server Device Certificates or CCAP Core device certificates to approved manufacturers.

The hierarchy of the CableLabs PKI Certificates is shown on Figure 13.

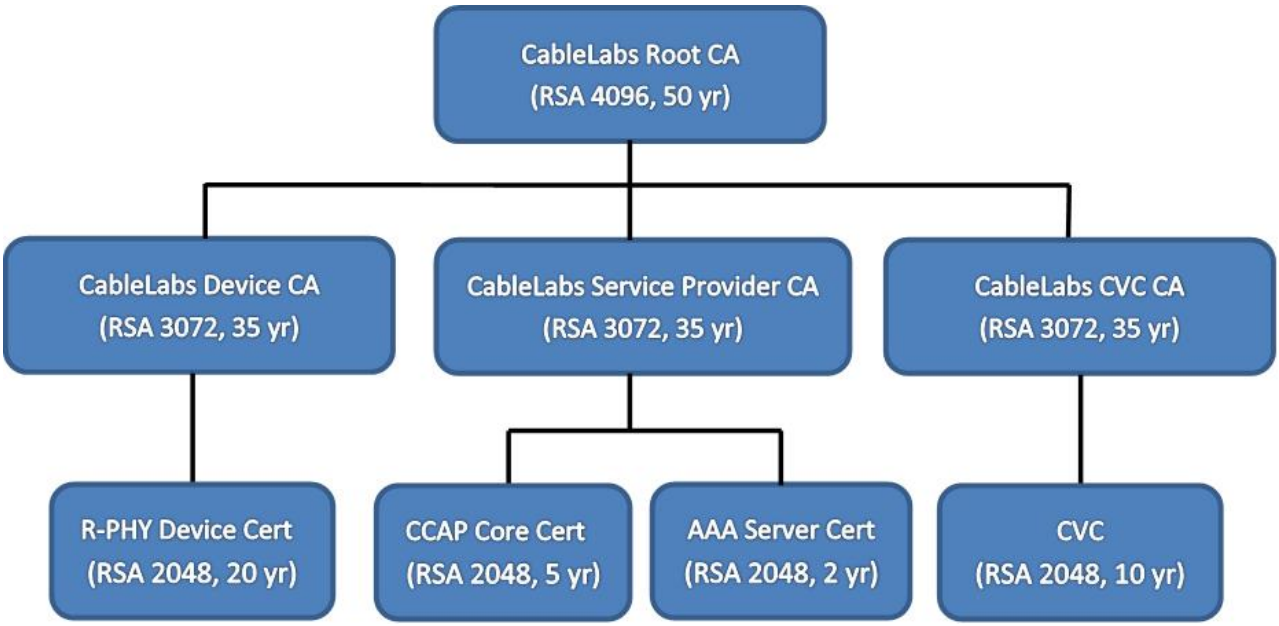

Figure 13 - CableLabs New PKI Security Certificate Hierarchy with R-PHY Extensions

The CVCs adopted to validate the RPD downloaded software images (SSD) do not require any modification to the CableLabs PKI. The CableLabs Root CA will be utilized as a trust anchor for issuing and validating CVC CAs and CVCs exactly as currently specified in [DOCSIS SECv3.1],

The reliance on the DOCSIS certificate scheme in the R-PHY environment offers a number of self-evident benefits. Not only are the involved parties familiar with the BPI+ scheme, but also the existing infrastructure and procedures can be easily extended to support R-PHY. For example, the requirements for device certificate storage and

certificate management, including the certificate revocation procedures can be directly reused.

Leveraging the well-established and verified DOCSIS methods will cut down on development time and the usual risks associated with the adoption of a new technology. The relatively straightforward expansion of the DOCSIS security certificate scheme onto the R-PHY architecture, an technology considered adjacent to DOCSIS, proves the vision of authors of the original and subsequent generations of DOCSIS Security specifications.

Secure Network Management

The R-PHY operational paradigm dictates that the RPD principally operates under the control of the CCAP Core, which provides all the interfaces to the operators' OSS systems. From the perspective of runtime operation, the distributed CCAP should have the same look and feel as integrated CCAP. This can be accomplished through a GCP connection, secured through mutual authentication as explained earlier.

In addition to runtime management from the CCAP Core, the RPD itself will also support local network management interfaces. The scope of the functionality enabled through these interfaces is limited to debug, offline HFC plant maintenance and the management of a few standalone RPD features. RPDs will support an SNMP agent and may also support other types of NM interfaces such as local or network enabled console line interface or an HTTP interface.

As in any modern networking device, these interfaces must be secured with encrypted transport, access control lists and access authentication and multi-level privilege authorization. The RPD manufactures need to follow well-known practices and principles for securing network management access to devices.

Attention needs to be devoted not only to particular network management interfaces, but also to the system a whole. The operating system or system software in an RPD can have instances where the TCP/IP or UDP stack has ports open for services or purposes not used in production devices; examples include messaging clients/servers, debug and testing ports, etc. For security purposes, these ports need to be closed when the RPD is deployed in the network. TCP and UDP ports dedicated to these purposes must be closed by default. Similar requirement are applicable to physical Ethernet ports. Finally, the RPD needs to cryptographically protect all sensitive data held in the system, including passwords and security keys.

CONCLUSION

An R-PHY architecture provides sufficient advantages to the MSO so that we can be certain it will be deployed over a significant portion of the cable infrastructure. As RPDs are deployed in locations with no physical security they could create a security vulnerability for the network. The RPD is an intelligent software enabled device based on Ethernet and IP technology and thus could provide an attractive point of entry into the network.

Security threats are increasing, general public awareness of cybercrime is at an all time high and internet security has moved beyond the technical realm to the highest levels of media and government. The paper has described some of the major threats that an R-PHY architecture could enable including unauthorized network access, breaches of customer privacy, theft of service and denial of service attacks.

Fortunately there are a number of solutions that can be applied to secure the network. The paper has described a defense in depth strategy based on proven standard approaches to resolve the problems so that:

- Access to the trusted network is protected using IEEE 802.1X and MACsec.
- The RPD and the CCAP Core are mutually authenticated using X.509 certificates using IKEv2.
- The control connection between the CCAP core and the RPD is protected with IPsec.
- The data plane traffic is protected with existing DOCSIS and video encryption.
- The software integrity of the RPD is protected using secure software download and secure boot technology.

Validating security solutions can be a very complex task but all of these mechanisms have been proven in telecommunication industry deployments and have been the subject of in depth security analysis. Thus we are confident that they provide the best options for effective R-PHY security. In addition to their security credentials they also provide a cost effective option and a fast time to market by leveraging existing standards and silicon.

We believe that using the methods described an R-PHY based architecture can be deployed while maintaining stringent levels of network security. We also believe that the outlined defensive features can evolve along with the threat environment.

The mechanisms have been described using R-PHY as the primary example but can be generally applicable to any IP device located in an insecure location whether this is an RPD, an Ethernet switch or an OLT.

Acknowledgements

The authors would like to sincerely thank the following people who provided ideas, as well as valuable insight into both DOCSIS specific and general internet security issues and protocols, which was instrumental in producing this paper: **Nancy Cam-Winget, John Chapman, Dan Hegglin, Stuart Hoggan and Brian Weis**.

Abbreviations

AAA Authentication Authorization Accounting
AES Advanced Encryption Standard
BPI Baseline Privacy Interface
BPI+ Baseline Privacy Interface Plus
CA Certificate Authority
CCAP Converged Cable Access Platform
CMTS Cable Modem Termination System
CIN Converged Interconnect Network
CM Cable Modem
CPE Customer Premises Equipment
CRC Cyclic Redundancy Check
CVC Code Verification Certificate
DevID Device Identifier
DHCP Dynamic Host Configuration Protocol
DNS Domain Name System
DOCSIS Data-Over-Cable Service Interface Specifications
DoS Denial of Service
EAP Extensible Authentication Protocol
EAPOL Extensible Authentication Protocol Over LANs
FTC Federal Trade Commission
GCP Generic Control Plane
HFC Hybrid Fiber-Coaxial
IEEE Institute of Electrical and Electronics Engineers
IETF Internet Engineering Task Force
IGMP Internet Group Management Protocol
IKEv2 Internet Key Exchange Version 2
IOT Internet Of Things
IP Internet Protocol
IPsec Internet Protocol security
L2TPv3 Layer 2 Transport Protocol version 3
LAN Local Area Network
MAC Media Access Control
MSO Multiple Systems Operator
NAD Network Access Device
OLT Optical Line Terminal
OSS Operations System Support
PHY Physical Layer
PKI Public Key Infrastructure
R-PHY Remote PHY
RPD Remote PHY Device
RDC Regional Data Center
RF Radio Frequency
RFC Request For Comments
SNMP Simple Network Management Protocol
SSD Secure Software Download
STB Set-top Box
TCP Transmission Control Protocol
UDP User Datagram Protocol

References

[R-PHY SCTE] John T. Chapman, "DOCSIS Remote PHY", SCTE Cable-Tec Expo, 2013.
[R-PHY NCTA] John T. Chapman, "Remote PHY for Converged DOCSIS, Video and OOB", NCTA Spring Technical Forum, 2014.
[R-PHY System] CableLabs, "DOCSIS Remote PHY Specification, D03", 2015
[DOCSIS SECv3.1] CableLabs, "DOCSIS 3.1 Security Specification, CM-SP-SECv3.1-I01-141023"
[IEEE 802.1AR] IEEE Std 802.1AR™-2009, Secure Device Identity
[X.509] ITU, Recommendation X.509 (10/12), 2012