Media over Coaxial Alliance (MoCA): Operation and Security Posture

Andrew Hunt

Volgeneau School of Engineering,George Mason University
Fairfax, VA
ahunt5@masonlive.gmu.edu

***Abstract*— Media over Coax Alliance (MoCA) is a protocol specification to enable assured high-bandwidth connections for the high demands of voice, video, and high-speed data connections – the 'triple play.' Verizon, Cox, Comcast, and many other service providers have adopted MoCA as the de facto networking technology used to provide in-home broadband services. This paper reviews MoCA and its common implementations, assessing vulnerabilities that are presented by the protocol and its use.**

I. Introduction

MoCA is a MAC/PHY specification that allows the use of Ethernet and video protocols over coaxial wiring common to most domiciles[1]. Supported by an alliance of industry partners, it also enables the connection of the "last mile" network distribution topologies to the home via FIOS (fiber-optic), cable, or satellite delivery methods. MoCA protocols enable devices with on-board protocol support, such as DVRs and Media Center computers, to connect to the in-home network provided by the cable-modem router, e.g. an ActionTec wireless coaxial router [2]. The router serves as an uplink to bridge the incoming MoCA Wide Area Network (WAN) signal from the satellite dish, optical network terminator (ONT) or cable distribution node with the in-home MoCA LAN signals [3]. This enables the router to support the concept of 'triple play': video, voice, and data provision directly from the provider over Ethernet, wireless, and MoCA networking services within the home [4].

II. Operation

A. MoCA in the Home

MoCA acts as a direct bridging technology, converting Ethernet (802.3) data, video and satellite signals to assigned channels over the coaxial cabling [5]. The physical layer (PHY) utilizes a 50MHz-wide, orthogonal frequency division multiplex (OFDM) signalled channel, seven of which are defined between bands 875MHz and 1550 MHz [6]. The channels support large packets (>1500 bytes) and use a Reed-Solomon forward error correction algorithm to ensure packet integrity [7]. The availability of bandwidth and error correction features allow for reliable signalling between nodes, even across multiple line splitters which may introduce reflective interference to the signal transmission.

Atop the PHY, the media access control layer (MAC) provides a distributed mesh architecture via time division multiple access (TDMA), managed by a fully-scheduled access scheme. This allows up to eight nodes to reliably address one another within the coaxial bus without the need for collision negotiation. Channel and transmission negotiation is handled by an automatically selected Node Controller (NC). Reliability for the network is assured by the selection of a backup node controller that intervenes in the event of a delay from the primary NC. MAC polling from the NC every ten milliseconds ensures node registration on the network, channel availability, and priority of the transmission frames upon the entire coaxial network, allowing the implementation of Parameterized Quality of Service (pQoS) features [6][8].

Provision at speeds of at least 60 Mbps is critical for the reliable delivery of voice and video services for the high-demand, low latency requirements of high-definition entertainment [6]. Via the polling scheme used, the minimum transmission rate of the network can be guaranteed at certain rates depending upon the available bandwidth of the PHY. The following table describes how PHY bandwidth affects minimum MAC transmission rates. This indicates how a provider may use MoCA packet scheduling to calculate the delivery and prioritization of services.

Table 1: Minimum MAC Rate as a Function of PHY Rate[5]

PHY Rate (Mbps)	Minimum MAC Rate (Mbps)
≥275	139.87
250	130.78
225	119.45
200	107.74
175	95.64
150	81.98
125	68.32
100	54.65
75	39.82

As indicated above, a standard 100 Mbps Ethernet interface could be provided a minimum of 54.65 Mbps of service over the MoCA network. The Ethernet frames are encapsulated by the MoCA MAC frame transmissions using the a process defined in the MoCA specification as the Ethernet Convergence Layer (ECL) [6]. Nodes on the MoCA network must have an 802.3 ECL device (a.k.a. network bridge) either

on-board (e.g. ActionTec router, DVR, ONT) or through an interfacing device, such as a MoCA Coaxial-to-RJ45 bridge. Because MoCA encapsulates the Ethernet frame from one end of the MoCA network to the other, the bridge is invisible to the connected Ethernet device.

The MoCA specification further details categories of devices. The devices may be provided by the Operational Service Provider (OSP) or a third party vendor (non-OSP). The table below defines the categories and common device types.

Table 2: MoCA Categories and Device Descriptions[6]

MoCA Category	Function	Provided by	Example Device
Terminal	Sources or sinks content	OSP	ONT
Intermediate	Bridge user content between MoCA network and standard interfacing device (Ethernet/USB)	OSP, Non-OSP	ActionTec router, DVR, MoCA-to-Ethernet Bridge

As MoCA is designed to patch physically separated Ethernet-capable devices together, it passes all Ethernet frames over its network to other devices. This includes all Open Systems Interconnect (OSI) model layers at the encapsulated link layer and above [8, pp. 52-53]. Thus, Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Hyper Text Transfer Protocol (HTTP) and other higher-level application services are all moved transparently by the MoCA network, as if they were one Ethernet domain.

Table 3: MoCA Related to the OSI Model

OSI Layer	Origin	MoCA	Terminus
1	Fiber, RJ-45 jack, ISM Radio, USB device	Coaxial Cable	Fiber, RJ-45 jack, ISM Radio, USB device
2	Ethernet frame, Wi-Fi frame, ARP	MoCA node	Ethernet frame, Wi-Fi frame, ARP
3-6	IP datagram, TCP/UDP packet		Router, Firewall
7	HTTP, DNS, DHCP, SMTP, Skype, SIP, Video streaming		Application proxy, DNS Cache, Application server, Cloud services

MoCA specifies a feature called Link Privacy. It is a link layer encryption feature based on 56-bit DES and rotating traffic keys [9]. For the feature to work, the privacy passcode must be preconfigured before each node can register with the MoCA network.

B. MoCA for the OSP

In addition to providing Ethernet bridging to user-facing intermediate devices, providers utilize their provided routers to establish two MoCA root nodes as the base for two MoCA networks. The two roots are virtual devices that are bound to a single physical adapter and coaxial cable. As indicated in the previous section, one MoCA network and its set of related channels provides connectivity between nodes providing the local services to the user. This is configured as the MoCA Local Area Network (LAN).

The OSP typically configures a second MoCA network via the second MoCA root node and its related channels, different than the first set, to talk directly with the ONT. The ONT converts the MoCA signal back to Ethernet and forwards the frame as light back to the OSP [3]. Due to the fragility of optical cabling, flexing a fiber optic cable through a hole in the domicile's exterior wall is not a desired deployment method. Locating the ONT close to the point where the fiber optic cable comes out of its underground encasement is preferable. Thus the ONT is attached to the outside of the home in a weather-proof box [10][11]. A more robust coaxial cable is then run from the ONT to the home splitter. The main splitter is also typically located on the home's exterior as the OSP installs the home's coaxial cabling during the first installation of services to the domicile. Locating the connections and splitter at the exterior utility point of presence reduces maintenance efforts for the OSP.

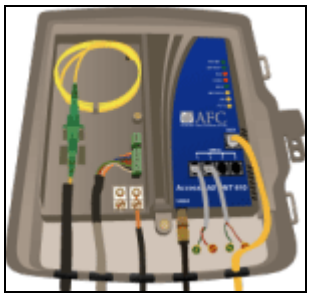

Figure 1: Diagram of Verizon FIOS Optical Network Terminator [12]

This second MoCA network carries the backhaul traffic between the router and the OSP, thus is called the MoCA Wide Area Network (WAN). Since this network provides only the uplink between two nodes – the router and the ONT – it can eliminate polling overhead and optimize MAC speed conditions to provide a higher bandwidth guarantee for the uplink.

III. Security Assessment

To assess the security of the MoCA protocol, aspects of design, deployment, and accessibility were considered. Previous work on the topic of securing Verizon's deployed architectures were consulted and equipment was procured to access the MoCA layer for testing [13][14]. The ActionTec MI424WR router used for testing supports many interfaces, including wireless, Ethernet, and MoCA.

Figure 2: ActionTec MI424WR router connections

A comparison was done on these communications form factors to scope the assessment.

A. Scope

1) Wireless

Verizon deploys its ActionTec routers with a random 8-character SSID. While the pseudo-random alphanumeric pattern is easy to recognize, it is also deployed with WPA-2 Personal (PSK) enabled. This does not preclude access via a wireless compromise, but significantly raises the level of investment for the attacker over prior WEP-only deployments used with earlier versions of the router. With many other resources available that address compromising wireless cryptographic implementations, this avenue was not pursued for this study [15].

2) Ethernet

Originally released in 1987, the commonly used 10- and 100-Base-T Ethernet protocols have had many resources devoted to penetrating, manipulating, and modifying them [16]. As a wired medium with a connectivity range of 100 meters and typically not wired outside the home, an attacker would need to get physical access to the network within the home. While not able to be attacked directly without these accesses, the MoCA layer, as a bridging protocol for Ethernet, presents situations that enable this class of attack.

3) Fiber

The fiber optic cabling from the ONT attached to the home runs underground to the local neighborhood optic hub. Without special equipment, accessing the data flowing over the cabling would be impossible. The fiber cable itself is also quite fragile, so manipulating it could break the line, leaving evidence of mishandling. Having neither the equipment or desire to damage the setup, accessing the optical cable was not considered for this assessment.

4) MoCA

OSPs typically install the domicile's coaxial cabling on the first contracting for service. To ease installation and later maintenance, these RC6-grade coaxial cables are run up to 500 feet from their termination point, typically the MoCA router or a DVR, through the household walls or attic to the exterior provider point-of-presence [17]. The cables are then hubbed with a high-frequency (>1GHz) splitter to the ONT. Coaxial cabling provides better shielding against both electromagnetic noise and the elements than standard CAT5e Ethernet cabling and connectors, which can only run to 100 feet [18]. This increases the range and reliability of the connection, reducing maintenance calls for the provider.

In the past couple of years, more venders have released products to market to take advantage of the guaranteed bandwidth and easy availability of in-home MoCA networks. To attach standard Ethernet-based devices, like many current Blu-Ray players and Media Center devices, to the MoCA network, ActionTec, NetGear and other vendors now produce MoCA-to-Ethernet bridge units. With these units mass produced and easily available through services like Amazon, access to the MoCA network has become a trivial undertaking. This access method was selected for study.

B. Situation

MoCA, as commonly deployed, provides an easy and accessible means to breach network barriers. The division between internal (LAN) and external (WAN) MoCA networks occurs within the stateful packet inspection (SPI) firewall within the ActionTec router. However, with both networks running over the same physical coaxial network and hubbed outside the home, both sides of the connection become available to an attacker that only has access to the home's exterior. This removes the constraints of physical access to the network. With commonly available components, an attacker can access and attack the in-home LAN with access only to the exterior of the home.

Even with access to both LAN and WAN networks, there is a frequency difference between the LAN and WAN channels that the attacker must determine to access one or the other. Also, most OSPs enable MoCA's data link protection feature for the MoCA WAN network between the router and the ONT. This makes attacking that portion of the traffic more difficult.

However, an attacker still has options available to them on the MoCA LAN. To enable easy compatibility, most MoCA LAN implementations do not utilize link privacy. This allows third party devices to be easily introduced to the MoCA LAN with little or no additional configuration required of the user. This provides an easily accessible, unencrypted target for the attacker to begin their reconnaissance.

C. Components

To commit the testing, several components were necessary to enable access to the MoCA LAN network. The following table describes the items required and whether they were purchased or provided by the OSP.

Table 4: MoCA Testing Components

Vendor	Model	Description	Provider
ActionTec	MI424WR	MoCA root nodes, wireless AP, Ethernet switch, router, firewall	OSP
AFC		MoCA terminator, fiber optic terminator, bridge	OSP
Tyco Electronics	LIS3777	3-way 5-1000MHZ coaxial splitter	OSP
Netgear	MCAB1001	MoCA Coax-to-	Tester

		Ethernet Adapter	
RCA	DH24SPR	2-way 5-2400 MHz coaxial splitter	Tester
RCA	VH606N	Digital RG-6 coaxial cable	Tester x2
Dell	Latitude D630	Laptop running Ubuntu 12.04	Tester
Belkin	Cat-5e patch cable	Connect the laptop to the MoCA adapter	Tester
LinkSys	E1000	Wireless router	Tester

D. Attacking the MoCA LAN

1) Penetration

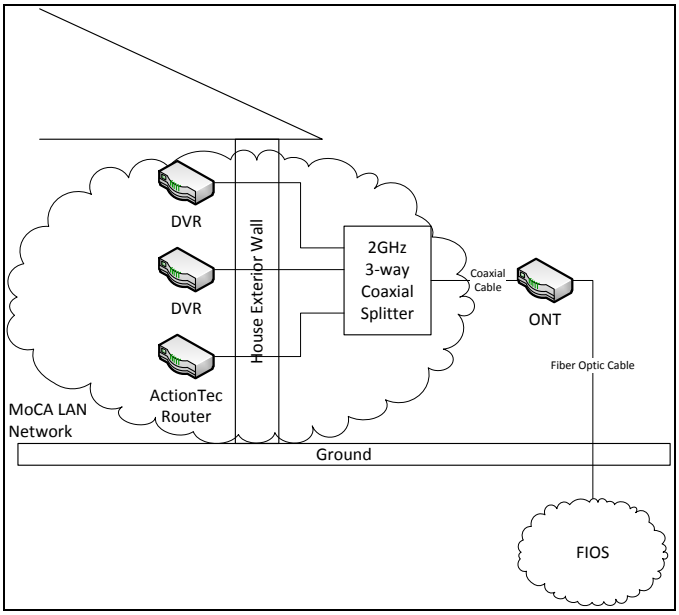

Figure 3: Diagram of MoCA LAN propagation in relation to the boundaries of the home

As indicated by Table 4, the essential MoCA infrastructure, the ONT and router, were provided by the OSP. These are connected by either a coaxial cable via the main coaxial splitter, the method preferred by the OSP, or via a CAT-5e cable run directly from the ONT to the router. Even if the direct Ethernet WAN method is employed, the MoCA LAN is still available from the external coaxial splitter as the ActionTec requires its use to provision video and data feeds to DVR units in the home. As depicted in Figure 3, this propagation of the MoCA LAN to an exterior splitter provides an easily accessible position of influence for an attacker.

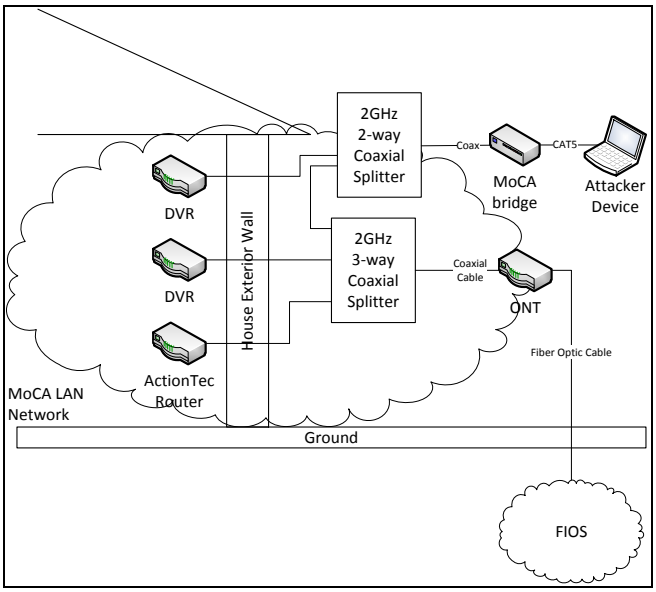

Figure 4: Diagram of MoCA LAN extension to enable attack from outside the physical boundary

To access the exterior splitter, the path to one of the connected coaxial cables must be interrupted, then reconnected through a splitter, as diagrammed in Figure 4. The other end of the splitter then connects in a new device, the MoCA-to-Ethernet adapter. This allows the extension of the MoCA LAN network and the introduction of a new Ethernet-compatible device. To accomplish the break, the original coaxial cable was disconnected from the main splitter. A new splitter, the RCA VH606N, was introduced with a short RC-6 coaxial cable. This splitter was then connected to the original coaxial cable from the home to complete the original circuit. The other side was then connected to the Netgear MCAB1001 MoCA adapter via the second RC-6 coaxial cable.

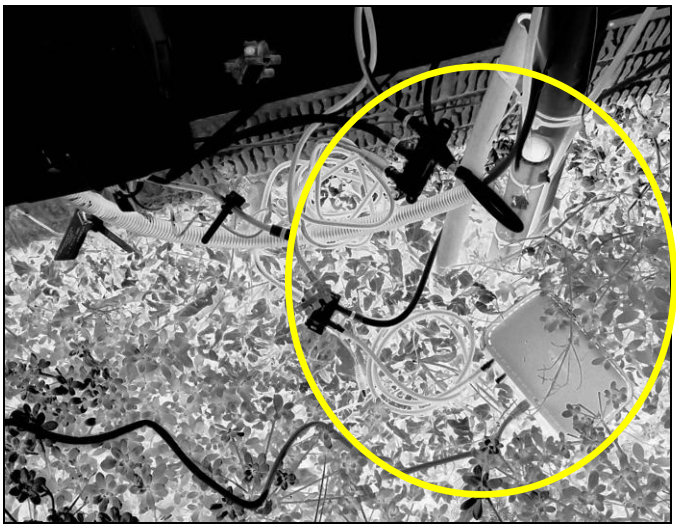

Figure 5: Color-inverted picture of components employed to split the coaxial connection and extend the MoCA LAN

As Verizon does not employ the link privacy feature of MoCA for the LAN network, the MoCA adapter integrates to the MoCA LAN without additional configuration. Figure 5 shows the successful integration of the 2-way coaxial splitter, additional RC-6 coaxial cables, and MoCA adapter to enable extension of the MoCA LAN outside the house. The picture was color-inverted to draw out the components and demonstrate the difficulty in spotting the components when viewed in natural light and color.

Having gained access to the MoCA LAN, passive packet captures yielded Ethernet broadcast traffic but no IP datagram traffic. This indicates that the MoCA LAN, when reconnected to Ethernet on the ActionTec router, is bridged to a switch. This media-sensing device prevents the delivery of link traffic to all hosts, instead delivering addressed Ethernet frames only to the port associated to the indicated MAC or IP address via the Address Resolution Protocol (ARP) table [19][8, pp. 476-482].

2) Reconnaissance

To discover more about the nodes attached to the MoCA LAN and its bridged Ethernet LAN, a more active approach was necessary to overcome the limitations established by the Ethernet switch. The following diagram depicts the normal FIOS routing operation. Data flows from MoCA LAN (DVRs), Ethernet, and Wireless devices to the same Ethernet switched router, then out over the MoCA WAN to the ONT.

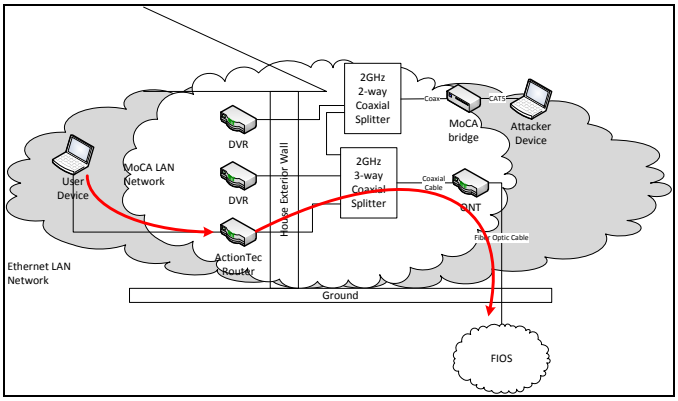

Figure 6: Normal routing operation of the standard FIOS implemenation

The switch, as an OSI layer 2 device, was subjected to an ARP poisoning attack using the Ettercap attack suite [20][21]. ARP poisoning is the injection of ARP broadcast traffic to notify all hosts on an Ethernet network that an assigned IP address on the network is associated to a MAC address [22][23]. The attack promulgated false information to the MoCA LAN's bridged Ethernet network to associate the ActionTec router's gateway IP address to the attacking laptop computer's MAC address. Once propagated, all nodes on the network communicated to the attacking laptop as the gateway. With the laptop configured to forward IP datagrams (in Ubuntu, ipv4_forward=true), a static gateway setting to the ActionTec gateway IP address, and a statically defined entry in the local ARP table for the ActionTec router, the entire network was subverted to route traffic through the attacking laptop.

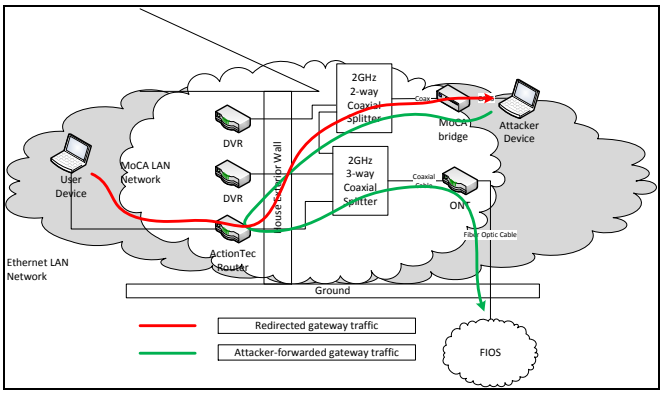

Figure 7: Diagram of the ARP-poisoned network delivering traffic to the attacking node, then forwarded through the correct route

ARP poisoning was the method of attack chosen to illustrate the weakness of running the internal MoCA LAN across a physically external hub. However, ARP poisoning is rather noisy and leaves detectable traces that can be captured by monitoring services [24]. While few of these detection tools would be running upon a typical household's LAN, the ActionTec router also proved fallible to ARP table manipulation, eventually corrupting the ARP table beyond use and rendering the ActionTec-supported LAN unroutable. While ARP poisoning provides a quick and easy method to discover assets on the LAN in a short time, there is the potential to incur a fault that will be noticed by the user.

A DHCP spoofing attack would be more stable and less noisy, but requires the attacker to wait for DHCP leases to be renewed on the network [25]. Currently there are no logging systems available to record DHCP spoofing unless a network intrusion detection system is specifically instrumented to detect rogue DHCP packets or IP collisions are detected on the network, which should not happen under a single DHCP scope. However, this method requires the attacker to invest more time in asset discovery and reliably win the race condition between the responding legitimate and rogue DHCP services.

With both access to and command of the routing within the household LAN, the attacker can efficiently collect authentication information, commit deep packet inspection, profile all machines on the network to plan further intrusion, and collect information about the user's common activities. The attacker may also come across private communications that the user engages in the privacy of their home, which may provide an opportunity for embarrassment or blackmail at a later time.

3) Exploitation

With OSI layers 2 and 3 of the local network under the attacker's control, the higher layers of the OSI stack become vulnerable to observation, redirection, interference, or

injection. The MoCA LAN bridge extended the Ethernet private LAN outside of the home, negating the firewall and network address translation (NAT) barriers established by the ActionTec router to any attacker that can walk up and plug in [8, pp. 349-352].

The attacker can take a couple of paths to exploiting discovered machines running on a network bridged to a MoCA LAN. Once a target host is identified, the attacker can engage in a direct attack, such as DNS response forgery, to redirect a target from their intended destination to the attacking host or website. This enables the attacker to engage in attacks germane to the host in question, but leave other hosts alone, which reduces the likelihood of detection. Tools like Metasploit can also aid in direct attacks, attempting to take advantage of known vulnerabilities in a profiled host's offered services to gain illicit access to the machine [26].

4) Deepening the foothold

With control of DNS and the traffic routing, the attacker can then engage in more subversive, less detectable attacks. These indirect attacks operate by injecting malicious scripts and binaries into portions of traffic streams. Because most of the stream is legitimate and the hosts are specifically targeted based on known profiles, this allows for quiet, highly likely compromise of the target machine. For example, the Browser Exploitation Framework (BeEF) could be employed to inject a malicious javascript into a web request for a common website [27][28][29]. Exploitation frameworks, such as EvilGrade, have been combined with active attack tools to produce highly effective exploitation frameworks, such as Karmetasploit [30][31].

5) Persistent pestilence

Utilizing these powerful tools, the attacker can create alternate means of access, such as reverse 'administration' tools (RATs) that call out and provide command-and-control from the attacker's points of presence. This would allow the attacker to use the MoCA LAN attack as a first step for establishment, then disengage the physical attack after establishing another foothold on the user's network. With an alternate control, the attacker can disestablish the MoCA LAN attack by simply removing the hardware. This allows for a time-limited infiltration mission to enable permanent establishment of remote control over the user's network. This method further reduces the likelihood of detection since the tell-tale equipment only remains at the site for the time necessary to gain an alternate channel. Should the alternate channel be interrupted, simply reapplying the MoCA LAN attack hardware can re-establish the aggressor's control over the home's network.

To further reduce observables, the attacker can utilize an embedded system rather than a laptop. Soekris boxes provide a compact x86 platform upon which to load the open source operating systems, libraries, and software that many attack toolkits rely on [32]. Taken further, the attacker could employ a commonly available hardware attack platform, the Pwnie [33]. Use of a generic device would reduce the amount of incriminating data available to implicate the attacker as most artifacts are common to the platform.

Another variation of the attack would be to pair the MoCA LAN access with a Wi-Fi access point. Access points are simply Ethernet bridges to the Wi-Fi transceiver. This functionality can be easily established by plugging any commonly available Wi-Fi router to the MoCA bridge adapter via one of its own LAN switch ports [34]. The attacker can then access the home's MoCA LAN from a distance, out of sight of the attacked property. This attack worked well during the assessment, however the half-duplex nature of wireless, along with the limitations of propagation distance over the air, presented performance challenges when attempting to spoof responses to the much speedier MoCA LAN.

6) Detection

Detection of a MoCA LAN attack can be difficult. As shown in Figure 8, the access points for utilities are commonly obscured. This provides ready cover for the attacker's equipment. However, the ActionTec router provides some ways to detect a tapping aggressor.

Under the Connection Configuration advanced menu, an interested user can find the Coax Connection Stats screen. This display presents a summary of all MoCA connections, including the MAC and associated IP address of each MoCA node. While this screen did display the IP address and MAC address of the MoCA bridge adapter, opening the screen is a manual process unsuitable for consistent monitoring.

An easier indicator comes from the Network Status screen. This display is easily accessible from the initial dashboard and displays all LAN-connected devices, including MoCA nodes. The MAC reported was the bridged MAC of the attacking laptop's Ethernet interface. However, the network indicator clearly states it is on the 'coax' network. This is easier to interpret, but may still be confusing to the lay user since most Blu-Ray and DVR units will appear in the same manner. This screen also requires manual access, making it unsuitable for monitoring.

The ActionTec MI424WR also provides access to its ARP table from its Advanced menu. The ARP table displayed the attacking laptop and its Ethernet MAC connected to the 'Network (Home/Office)' scope. This indicates the transparent nature of the bridging done by the router between the MoCA LAN and Ethernet LAN layers. Again, this is a manually accessed screen and unsuitable for monitoring without a web scraping agent.

The router also supports system and security logging. Disabled by default, the user can turn these options on from the Advanced menu under System Logging. A separate screen under System Monitoring displays the collected logs. While the log did record the attackers DHCP request and registered the laptop's Ethernet MAC address and IP address issued, it did not make any note of the ARP rebinding attack, duplicated IP address mappings of its routing IP, or the corruption of the router's ARP table. These logs can be forwarded to a remote syslog server, enabling a more robust monitoring scheme with the necessary services and equipment.

Figure 8: Demonstration of the obscurity of coaxial splitting outside the attacked home

Due to the lack of effective logging of the ActionTec router, alternative methods of monitoring the MoCA LAN are necessary. However, since the MoCA LAN is employed as a simple bridging layer between Ethernet nodes, known Ethernet monitoring methods work to provide monitoring capabilities to the local LAN.

Arpwatch is a tool that passively monitors ARP broadcasts for changes in the IP address allocations [19][35]. Employing this tool, the attacking ARP forgery attack and subsequent man-in-the-middle attacks were detected. At attack initiation, the Arpwatch logged 'changed Ethernet address' alerts for all of the network nodes as the attacking MAC claimed all of the known ARP assignments. Continued alerts for 'flip flop' and 'ethernet mismatch' were produced as the attack continued and the attacking laptop oscillated the ARP mappings between the true and false nodes to enable redirection. The end of the attack was notated by a final 'flip flop' that re-established the original ARP mapping of the gateway IP address to its MAC address. As the ActionTec readily releases DHCP holds after their expiry, there is some churn in the mapping of MAC address to IP address, producing false positives. However, these singular alerts do not have the propensity of an ARP poisoning attack, making Arpwatch a useful monitoring tool for a MoCA LAN hijack. While beyond the capability of most home users, this tool has been readily integrated into most major Linux distributions making installation and configuration a simple task.

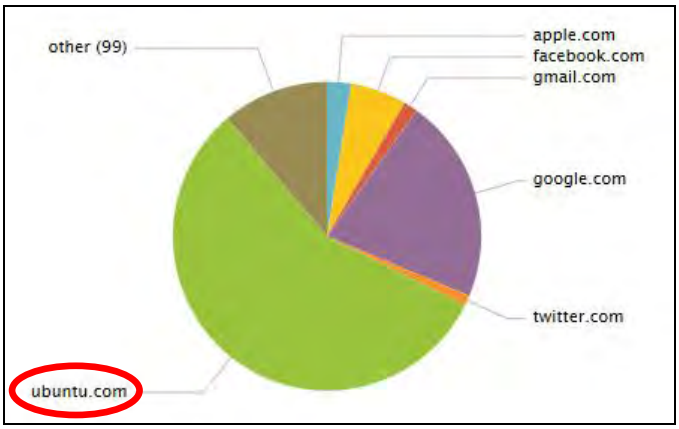

Figure 9: DNS reconnaissance techniques used to profile deviations from 'normal' baseline reveals the attacker

Logging of network services upon the home LAN is another powerful toolset to leverage against infiltration. Figure 9 demonstrates how the establishment of network services like firewalls, proxy servers, and DNS cache forwarders can provide useful data for baselining 'normal' behaviors and detecting deviations from that baseline. When properly instrumented and monitored, the attacker must make no mistakes to avoid detection. For instance, the simple act of requesting a DHCP lease could entice the attacker to automatically send their machine's background requests to the local DNS cache forwarder. In this instance, the attacker's laptop was easily distinguished from the other devices serviced by the ActionTec router as the only Ubuntu machine requesting Ubuntu.com update servers for patches. None of the legitimate nodes on the LAN ran that operating system.

7) Mitigation & Prevention

Once discovered, mitigation of the MoCA LAN compromise is as simple as removing the offending equipment and restarting the router. However, this does not preclude the possibility of an alternate installed backchannel or a recurrence should the attacker return with new equipment.

One solution would be to define static ARP tables on all machines within the internal LAN [24]. While this would preclude the ARP poisoning attack used in this testing for traffic redirection, it would be difficult to maintain, and require modifications to the access controls within OSP-provided equipment to enable the user to manipulate these system-managed components. Impractical to maintain and difficult to access every node's ARP tables without subverting existing access controls, this is not a reasonable solution.

Further, one could employ a secure ARP (s-ARP) implementation using public key infrastructure (PKI) technologies to authenticate devices at the MAC layer. This provides authenticated access from a certificate authority present upon the LAN. While a novel idea in the use of authentication techniques to definitively identify machines, it does present several drawbacks. The PKI infrastructure must be established and maintained. Additionally, s-ARP associates IP addresses with the credentials, dictating a static network design. This presents management and scalability problems

for a constantly increasing and circulating employment of consumer devices within a typical household. DHCP support is possible through a non-standard patching of the DHCP server, which the implementer then has to maintain. Implementation also requires precise time precision of all devices to a local time store, a configuration requirement many OSP-provided devices cannot adhere to. These requirements make implementation of s-ARP upon the home network impractical.

Beyond OSI layer 2, secure service implementations can help reduce the exposure to attack, or at least increase the likelihood of detection, should ARP poisoning occur. Creating a local DNS cache forwarder that implements DNSCrypt forwarding to the OpenDNS resolver service tunnels resolution traffic in a way not currently exploitable to an attacker [36][37]. Paired with firewall rules that require only that service to be allowed to communicate with OpenDNS' servers for DNS protocol, the attacker loses the ability to commit DNS rebinding attacks to redirect hosts to malicious destinations [38]. It also provides an indicator to a user monitoring firewall and DNS resolution logs when the attacker attempts to circumvent or resolve through the forced channel.

Securing all services bridged by the MoCA LAN can be daunting considering the number of services operating upon a normal machine. Consumer and OSP-provided devices frequently do not conform well to the requirements of forced network service architectures, like transparent proxy services. Thus the implementation of a completely secure network architecture is constrained.

The most straightforward way to engage the problem involves rewiring the coaxial cables to a splitter within the home that does not leave the exterior wall. This would prevent physical access to the cabling and easy addition of a splitter and MoCA bridge. However, this may prove impractical for many existing coaxial deployments and be difficult for service providers to maintain. It would also be easy to circumvent as the coaxial cable to the exterior ONT must exist in the default deployment to support the MoCA WAN, and tools for coaxial cable splicing are readily available. As both MoCA networks share the same physical bus, the MoCA LAN is still accessible through this cable.

Combining the rewiring of the main coaxial splitter within the home with an alternate physical connection from the ONT to the ActionTec router would provide a more secured WAN connection and remove access to the MoCA LAN. An Ethernet interface is available on the ONT to connect to the Ethernet WAN port on the router. Asking the OSP to configure the ONT accordingly and utilizing an armored CAT5e cable to run from the secured ONT box through the home's exterior wall would present a greater obstacle to an attacker, removing any easily-accessible access point to both the WAN and LAN connections.

IV. Future Work

Future work includes penetrating the MoCA WAN portion of the coaxial network. With access to both sides of the router NAT, reconnaissance time for LAN nodes not running through the ActionTec's Ethernet switch would become possible. Penetration of this connection may also provide layer 2 access to the upstream ISP and neighboring installations. This may present a larger array of targets to compromise for a variety of purposes.

Work would also include an assessment of defenses for both the home and service provider.

V. Conclusions

Media over Coaxial Alliance networking protocols provide many attractive features to operational service providers. Guaranteed bandwidth, quality-of-service provisioning, and a robust RF-shielded physical network help the OSP to provide reliable, easily maintained service to customers for their high-demand entertainment requirements. However, the common implementation of these broadband services , such as external wiring and splitting, extend the internal local area networks outside the home. With commonly available equipment and software tools, an attacker can take advantage of this MoCA network extension to gain influence and subvert the LAN from outside the walls of the domicile. A single network access point yields access to all hosts on the bridged Ethernet switch – MoCA, Ethernet, and wireless alike. With influence over layer 2, the attacker can then influence vulnerabilities in upper layers of the OSI service model to commit reconnaissance, targeted exploitation, and persistent footholds upon discovered devices.

Direct detection of these attacks must occur at the link layer, either via MoCA or through the bridged Ethernet LAN. Without monitoring capabilities, detection of this attack is unlikely until the failure of the router due to ARP table corruption. Indirect detection methodologies were presented, but are unlikely to be implemented by consumers of the technology.

The most direct mitigation of this class of attack is for the OSP to end the practice of wiring coaxial networks to terminate at splitters outside the home. This simple fix – wiring the coaxial network to an interior splitter – would raise the effort of the attacker, requiring them to physically damage the network infrastructure at the network terminator to gain access to it. Otherwise, the implemented network is indefensible from any attacker who walks up and takes physical control.

References

[1] "Multimedia over Coax Alliance," Wikipedia, the free encyclopedia. 22-Oct-2012. [Online]. Available: http://en.wikipedia.org/w/index.php?title=Multimedia_over_Coax_Alliance&oldid=516580035. [Accessed: 12-Nov-2012].

[2] "Actiontec MI424WR Verizon FiOS Router." [Online]. Available: http://www.actiontec.com/products/product.php?pid=189. [Accessed: 15-Nov-2012].

[3] "Verizon FiOS," Wikipedia, the free encyclopedia. 14-Nov-2012. [Online]. Available: http://en.wikipedia.org/w/index.php?title=Verizon_FiOS&oldid=519797904. [Accessed: 14-Nov-2012].

[4] S. Ovadia, "Home Networking On Coax for Video and Multimedia," 30-May-2007. [Online]. Available: http://www.ieee802.org/1/files/public/docs2007/at-sovadia-MoCA-overview-0507.pdf. [Accessed: 12-Nov-2012].

[5] "MoCA 1.1 Specification for Device RF Characteristics," Multimedia over Coax Alliance, 15-Aug-2012. [Online]. Available: http://www.mocalliance.org/marketing/specification/MoCA_Specification_for_Device_RF_Characteristics.pdf. [Accessed: 12-Nov-2012].

[6] S. Ovadia, "MoCA: ubiquitous multimedia networking in the home," "Proceedings of SPIE," presented at *Broadband Access Communication Technologies II*, 2007, vol. 6776, p. 67760C–67760C–5.

[7] J. Peltotalo, V. Roca, S. Peltotalo, and J. Lacan, "Reed-Solomon Forward Error Correction (FEC) Schemes," in *IETF Network Working Group: Request for Comments: 5510*, Tampere University of Technology, 2009. [Online]. Available: http://tools.ietf.org/html/rfc5510. [Accessed: 12-Nov-2012].

[8] J. F. Kurose and K. W. Ross, "Multiple Access Links and Protocols," in *Computer Networking: A Top-down Approach*, 6th ed. Boston: Pearson, 2013, p. 459.

[9] A. Monk, S. Palm, A. Garrett, R. Lee, and T. Leacock, "MoCA Protocols: What exactly is this MoCA thing?," in *Technology Conference and Open House*, Austin, TX, 2007. [Online]. Available: http://www.mocalliance.org/industry/presentations/2007_11_14_TechConference/docs/MoCAProtocols.pdf. [Accessed: 12-Nov-2012].

[10] "What Happens During FiOS Installation?," Verizon FIOS Support. [Online]. Available: https://www22.verizon.com/Support/Residential/Internet/fiosinternet/general+support/top+questions/questionsone/85125.htm. [Accessed: 17-Nov-2012].

[11] "FiOS Installation: The Installation Appointment," Verizon FIOS Support. [Online]. Available: https://www22.verizon.com/support/residential/internet/fiosinternet/general+support/getting+started/questionsone/98266.htm. [Accessed: 17-Nov-2012].

[12] "Verizon FIOS Optical Network Terminator Diagram." [Online]. Available: http://www.google.com/imgres?hl=en&client=firefox-a&hs=T0s&sa=X&tbo=d&rls=org.mozilla:en-US:official&biw=1218&bih=397&tbm=isch&tbnid=ZhDCCc1uR-4vmM:&imgrefurl=http://www22.verizon.com/residentialhelp/fiosinternet/general%2Bsupport/getting%2Bstarted/questionsone/85263.htm&docid=jANMuTFCrvdeDM&imgurl=http://www22.verizon.com/cs/groups/public/documents/onecmsresource/ont_150_4336.gif&w=150&h=142&ei=iOWmUNrGPILe9ASejYDoBg&zoom=1&iact=hc&vpx=12&vpy=179&dur=233&hovh=113&hovw=120&tx=97&ty=102&sig=103566994076620688022&page=1&tbnh=113&tbnw=120&start=0&ndsp=12&ved=1t:429,r:6,s:0,i:91. [Accessed: 17-Nov-2012].

[13] "Verizon FIOS Faux Paus," Notes on Security and Research, 10-Aug-2010. [Online]. Available: http://pinowudi.blogspot.com/2010/10/verizon-fios-faux-paus.html. [Accessed: 17-Nov-2012].

[14] "Securing a FIOS Network in the Home," Notes on Security and Research, 29-Aug-2011. [Online]. Available: http://pinowudi.blogspot.com/2011/08/this-article-is-in-response-to-query.html. [Accessed: 17-Nov-2012].

[15] J. Wright, "Will Hack For SUSHI." [Online]. Available: http://www.willhackforsushi.com/. [Accessed: 17-Nov-2012].

[16] "IEEE Standards for Local Area Networks: Supplements to Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications," ANSI/IEEE Std 802.3a,b,c, and e-1988, 1987. p. 0_1

[17] "Coaxial cable," Wikipedia, the free encyclopedia. 17-Nov-2012. [Online]. Available: http://en.wikipedia.org/w/index.php?title=Coaxial_cable&oldid=522004100. [Accessed: 17-Nov-2012].

[18] "Category 5 cable," Wikipedia, the free encyclopedia. 17-Nov-2012. [Online]. Available: http://en.wikipedia.org/w/index.php?title=Category_5_cable&oldid=523170116. [Accessed: 17-Nov-2012]

[19] D. Plummer, "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware," in *RFC Editor*, 1982. [Online]. Available: http://tools.ietf.org/html/rfc826. [Accessed: 12-Nov-2012].

[20] "Ettercap (computing)," Wikipedia, the free encyclopedia. 29-Oct-2012. [Online]. Available: http://en.wikipedia.org/w/index.php?title=Ettercap_(computing)&oldid=520362724. [Accessed: 12-Nov-2012].

[21] A. Ornaghi and M. Valleri, "Ettercap." [Online]. Available: http://ettercap.sourceforge.net/. [Accessed: 12-Nov-2012].

[22] "ARP spoofing," Wikipedia, the free encyclopedia. 12-Nov-2012. [Online]. Available: http://en.wikipedia.org/w/index.php?title=ARP_spoofing&oldid=522187503. [Accessed: 12-Nov-2012].

[23] S. Whalen, "An Introduction to Arp Spoofing," Apr-2001. [Online]. Available: http://dl.packetstormsecurity.net/papers/protocols/intro_to_arp_spoofing.pdf. [Accessed: 12-Nov-2012].

[24] A. Ornaghi and M. Valleri, "Man In The Middle Attacks Demos," in *BlackHat Conference USA*, Las Vegas, NV, 2003. [Online]. Available: http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-ornaghi-valleri.pdf. [Accessed: 12-Nov-2012].

[25] "10079 - ettercap DHCP spoofing MITM attack," YouTube, 2009. [Online]. Available: http://www.youtube.com/watch?v=YJAglnMegMQ&feature=youtube_gdata_player. [Accessed: 17-Nov-2012].

[26] "Penetration Testing Software | Metasploit." [Online]. Available: http://www.metasploit.com/. [Accessed: 19-Nov-2012].

[27] W. Alcorn, "BeEF - The Browser Exploitation Framework Project." [Online]. Available: http://beefproject.com/. [Accessed: 19-Nov-2012].

[28] D. Campbell and E. Duprey, "Cross Site Scripting (XSS): Exploits & Defenses," The OWASP Foundation, Denver, CO, 2007. [Online]. Available: https://www.owasp.org/images/a/ad/DC_ED_OWASP_XSS_MAY2008_v1.0.pdf. [Accessed: 19-Nov-2012].

[29] M. Vallentin and Y. Ben-David, "Persistent Browser Cache Poisoning," 2010. [Online]. Available: http://www.eecs.berkeley.edu/~yahel/papers/Browser-Cache-Poisoning.Song.Spring10.attack-project.pdf. [Accessed: 19-Nov-2012].

[30] F. Amato and F. Kirschbaum, "You STILL have pending upgrades!," in *DefCon 18*, Las Vegas, NV, 2010. [Online]. Available: https://www.defcon.org/images/defcon-18/dc-18-presentations/Amato-Kirschabum/DEFCON-18-Amato-Kirschabum-Evilgrade.pdf. [Accessed: 19-Nov-2012].

[31] V. Oezer, "The Evil Karmetasploit Upgrade," in Nullcon, Zuri, India, 2009. [Online]. Available: http://nullcon.net/nullcon2010presentation/Veysel_nullcon2010_Paper.pdf. [Accessed: 19-Nov-2012].

[32] S. Kristensen, "Soekris Engineering, Inc. | Single Board Communication Computers," Soekris Engineering, 2001. [Online]. Available: http://soekris.com/. [Accessed: 19-Nov-2012].

[33] D. Porcello, "Pwnie Express," Pwnie Express, 2012. [Online]. Available: http://pwnieexpress.com/pages/our-tech. [Accessed: 19-Nov-2012].

[34] No_Strings and DrTCP, "Using a Wireless Router as an Access Point," DSL Reports, 10-Jan-2012. [Online]. Available: http://www.dslreports.com/faq/11233. [Accessed: 19-Nov-2012].

[35] LBL Network Research Group, "Arpwatch," SecurityFocus Tools, 09-Apr-2004. [Online]. Available: http://www.securityfocus.com/tools/142. [Accessed: 12-Nov-2012].

[36] "DNSCrypt," OpenDNS. [Online]. Available: http://www.opendns.com/technology/dnscrypt/. [Accessed: 19-Nov-2012].

[37] D. J. Bernstein, T. Lange, and P. Schwabe, "The Security Impact of a New Cryptographic Library," in *Progress in Cryptology – LATINCRYPT 2012*, vol. 7533, A. Hevia and G. Neven, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 159–176.

[38] C. Jackson, A. Barth, A. Bortz, W. Shao, and D. Boneh, "Protecting browsers from DNS rebinding attacks," in *ACM Trans. Web*, vol. 3, no. 1, 2009, pp. 2:1–2:26.