METHODS TO PREVENT CONNECTED DEVICE SERVICE THEFT

INVENTORS:

STEVEN J. GOERINGER
LUIS ALBERTO CAMPOS
BRIAN A. SCRIBER
KYLE HAEFNER
MASSIMILIANO PALA

Description

Cable modems may be stolen in a variety of ways. While DOCSIS prevents unauthorized modems from accessing the network, iterations of DOCSIS before DOCSIS 4.0 do not prevent modems from accessing networks of other operators. If a given operator chooses to do so, they do not have to pay the non-recurring costs for CMs (and neither do their customers). This puts operators with more sustainable business models at a competitive disadvantage, at least in the short term.

This invention addresses this by providing a variety of mechanisms implementable in software to prevent a modem from registering, on-boarding, or connecting to a 3rd party's network. As these mechanisms are implementable in software, if a given stolen cable modem's firmware can be changed or replaced ("flashed" is the industry term), the security benefits of these mechanisms can be bypassed. However, flashing a modem is a manual process, sometimes quite intensive, this introduces costs to the 3rd party network that may be prohibitive in comparison to legitimately acquiring modems for their customers.

It should be noted that while this invention is described in terms of DOCSIS, the notions described here apply to any access network infrastructure using CPE including but not limited to LTE, 5G, optical (including point-to-point and PON), CBRS, Wi-Fi, satellite. Additionally, the same mechanisms can be applied to certain access network infrastructure components to including but not limited to access points, residential gateways, cable modems, DSL modems, LTE or 5G modems, eNB, base stations, BRAS routers, DSLAMs, CMTSs, RMDs, RPDs, OLTs, ONUs, etc...

Problem

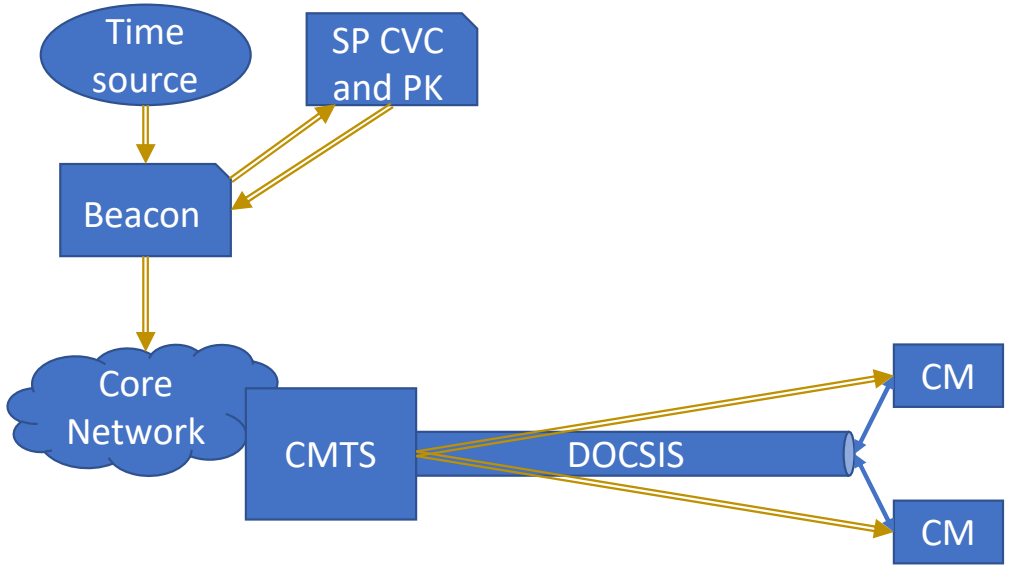
- An unauthorized cable operator can use a stolen cable modem on their network
- This can impact all versions of DOCSIS
- Goal is to prevent unauthorized use of a cable modem on a 3rd party network
  - It's relatively easy for an operator to prevent undesired modems onto their network because CMs are authenticated used PKI and other registration processes are used
  - It's relatively hard for an operator to prevent another operator from allowing modems onto that operator's network – DOCSIS iterations before D4.0 did not provide any authentication of the network
- Assumptions
  - 3rd party cable operator enabling use of stolen CMs is NOT flashing the modems
  - We cannot rely on hardware-based security controls – solution must be implemented in firmware to allow backwards compatibility (DOCSIS 3.1 through 2.0)
    - As the selected capabilities need to be backwards compatible with existing hardware limits, SIMPLE processing is essential
  - CM OEMs are able and willing to provide updated firmware to implement one or more of the controls discussed in this presentation

General idea

- Use some form of mechanism that either
  - Allows the CM to determine if it is on the authorized network (other than mutual authentication)
  - Allows the CM to determine if it has been moved
  - A combination of these methods
- The mechanisms may be utilized continuously, based on some trigger, or only at boot/restart of the CM
- If a CM determines it has been moved, possibly to another network

Beacon (Kevin Taylor, Comcast with details provided by Steve Goeringer discussed with Teco)

- A attestable broadcast/multicast packet sent from the operator to the CM to enable use
- Time correlation at the CM needs to be studies (there are DoS vectors if not done well)
- The beacon could be:
  - A signed time packet using PKI
    - One manifestation: SP CVC certificate and private key or equivalent
      - Pro – the CM can already be provisioned with a CM certificate
      - Con – increases the vulnerability of the SP CVC cert and private key
    - Alternatively: CMTS or similar element can have its own certificate and key
      - Pro -- limits exposure of SP CVC cert and key
      - Con – increases operational complexity as CMs have to have the appropriate SP beacon certificate provisioned
  - This may be at the control level in DOCSIS or a management packet at IP layer sent to the CM
- If the beacon is not received or fails attestation, the CM may either:
  - Disable connection
  - Rate limit connection
- Pro: This should be easily implemented in firmware
- Con: This may be a DoS vector if the beacon can be tampered or blocked



Device and CVC cert organization value mapping

- Firmware images should be signed
  - By the vendor to show integrity and providence
  - By the operator to authorize use of the image
- CVC validation includes an organization name check
  - organization of the vendor identified in both the device and CVC cert MUST be identical
  - Same for co-signing
- A change that once SSD requires co-signing, the co-signing requirement cannot not be disabled may prevent unauthorized use

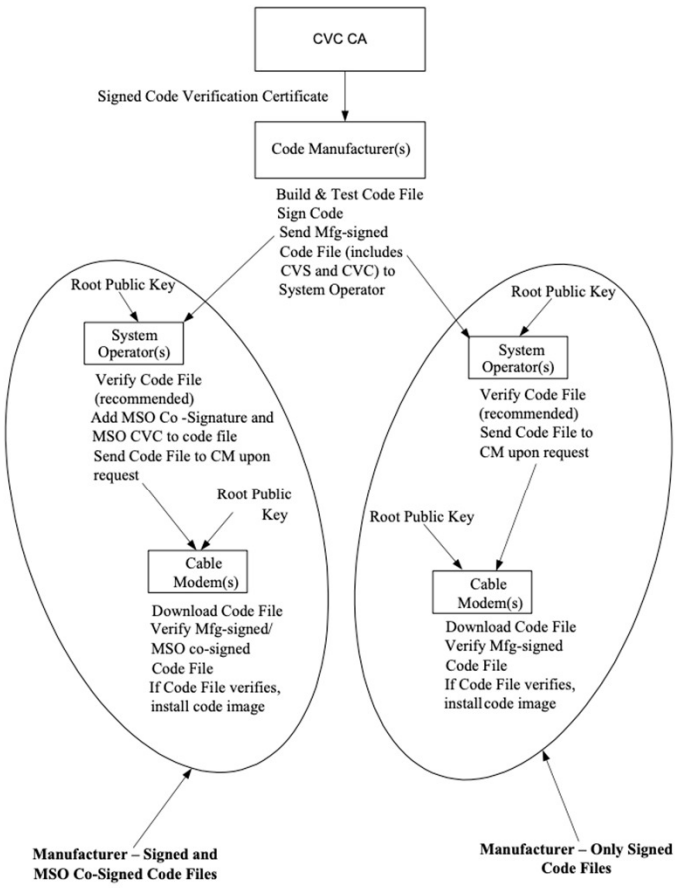
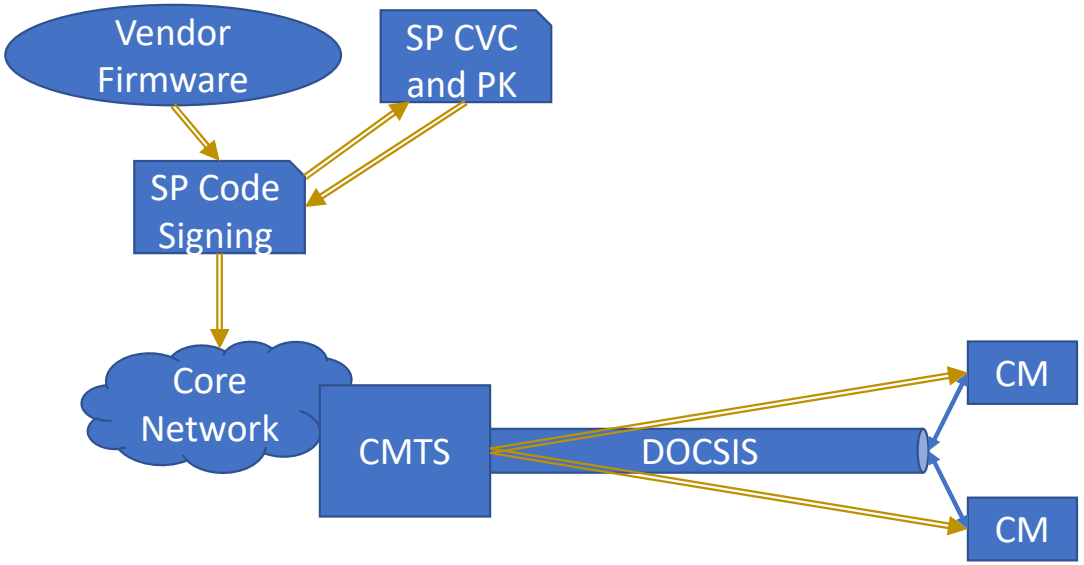


Figure 15 - Typical Code Validation Hierarchy

CVC Secure Boot (Steve Goeringer, discussed with Teco and Comcast)

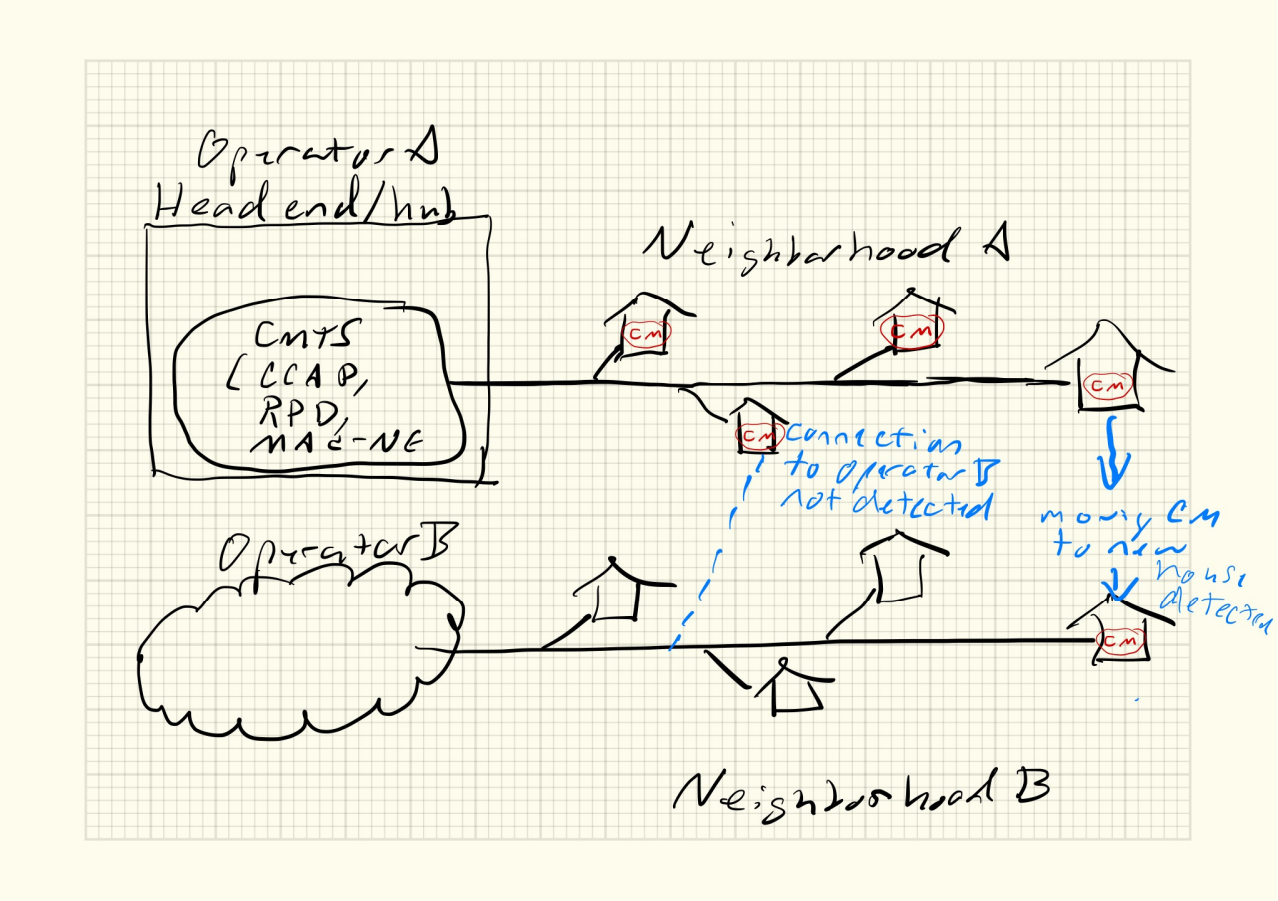
- Have service provide do CVC based code signing of firmware
- When CM boots, it should verify (chain) the firmware SP signature
- If the SP CVC verification, the CM
  - Disable connection
  - Rate limit connection
- Pro: This should be easily implemented in firmware
- Con: This may be a DoS vector if the image can be tampered
- Con: This may degrade use unintentionally if firmware image is corrupted
  - This can be addressed by requesting a new code image
- We need to do some further design work
  - How to prevent loading an unintended SP CVC cert
  - How to ensure viability for legitimate sale to secondary markets



GPS (geofencing – Kyle Haefner)

- If the CM has the ability to locate itself with GPS or WiFi, the location can be encoded and signed by the the device private key
  - This can be attested to the network
- If the CM is moved, it can be disabled, or rate limited
  - Alternatively, the modem can use the determination that it has moved as a trigger to do a higher confidence method
    - Authenticated access to a specific network address
  - Perhaps it ignores the beacon unless it notices that it moves in which case it checks the beacon
- Limitations
  - If the CM is not moved and simply connected to another network, this will not prevent theft
  - CMs may be legitimately moved by the owning operator
- A mechanism to allow authorized moving can be provided
  - A signed token from the operator using the CVC cert and key

Geofencing CM theft prevention

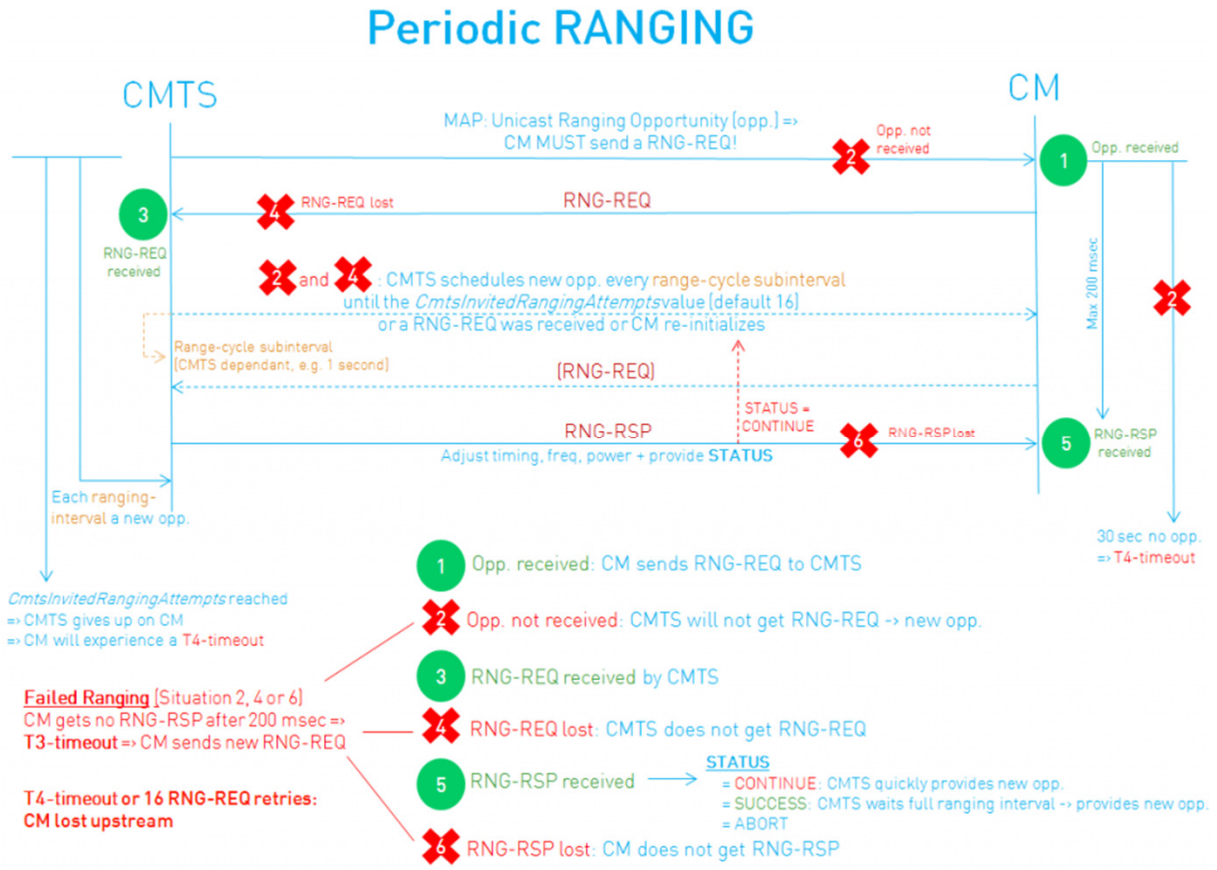


Ranging (geofencing for cable – Steve Goeringer; similar to ideas Alberto Campos is already researching)

- Most cable modems do not have any ability to locate themselves using GPS (none?)
- DOCSIS has a mechanism called ”ranging” that determines power (compensating for attenuation/loss) and timing offset that can provide benefits similar to geofencing
  - Attenuation accumulates over distance on cable systems
  - Delay is measured
- As with geofencing, if the CM detects a significant change in transmission power needs, attenuation, or timing offset, it can be disabled, or rate limited
  - Alternatively, the modem can use this determination as a trigger to do a higher confidence method
    - Authenticated access to a specific network address
  - Perhaps it ignores the beacon unless it notices that it moves in which case it checks the beacon
  - The thresholds that may indicate a CM may have moved may vary and therefore be stochastic (have some randomness in loss over time and also rate of change of loss); cloud or remote AI (ML/NN) processes may be beneficial to dynamically adjust thresholds
- A mechanism to allow authorized moving can be provided
  - A signed token from the operator using the CVC cert and key

Ranging (prior art, illustration from Excentis)

- Ranging is part of the DOCSIS specification and not a (new) claim
- Illustration source https://www.excentis.com/blog/ranging-feeling-2-bpm-docsis-heartbeat



Challenge and response (tech/homeowner)

- Leveraging existing certificates, the CM can issue a challenge to an IP address or URL (configured when the modem first initializes or comes on-line) using the co-signing CVC certificate presented during software update
  - Software updates can be signaled can are also checked every time a CM reboots
  - A method to prevent use of an update from another operator must be provided
    - Once the initial update is done, the co-signing CVC may not be changed – e.g., the co-signing CVC of a new update is compared to the previous co-signing CVC and they must match
    - Co-signing CVCs need to change over time (for example, they expire). A token signed by the co-signing CVC cert of the previous update that is checked to authorize use of a new CVC
  - This challenge protocol can be initiated by a trigger on the CM or by the technician or homeowner
- Alternatively, an ecosystem process (using a publicly routed IP address or URL) can be used that leverages the issuing CA certificate for the device, however this increases ecosystem risk as it uses the issuing CA certificate and private key

Hardware vs firmware implementation

- The options outlined should be suitable for implementation in firmware without modification of hardware
- Any security feature implemented solely in firmware can be removed if the firmware is accessible to another party
  - Exposed JTAG, SPI, or other debug ports enable flashing the system
  - Exposed management ports that allow remote exploit
  - Ability to access software update or image management functions on customer facing ports
- Hardware based or enabled solutions are far superior in terms of security; this does not seem suitable for Telecom Argentina’s