Analysis on new possibility security threads in IEEE 802.1CQ

Antonio de la Oliva (UC3M, IDCC)

Outline

- Objective
- Thread Analysis in L2 wired networks
- Thread Analysis in L2 Wireless networks
- New security risks identified
- Conclusion

Objective

- SoA analysis, of the already known security risks for Wired and Wireless IEEE 802 networks, with focus on IEEE 802.1Q and IEEE 802.11 standards.
- Identification of the implications of IEEE 802.1CQ on the well known security threats
- Identification of new security threads brough by IEEE 802.1CQ operation
- Provide some recommendations

Threat analysis for Wired networks

- There are several well known threats in wired networks, which are collected in several technical documents [5][7]:
  - MAC Attacks:
    - VLAN Hopping
    - MAC Flooding (CAM Table overflow)
  - DHCP Attacks
  - ARP Attacks
  - Spoofing Attacks
  - Spanning Tree Attacks
  - Port Stealing

Threat analysis for Wired networks

- MAC Attacks
  - MAC learning table becomes full (CAM Table Full). Switch becomes a hub, forwarding all through all ports.
    - Mitigation: Port Security by limiting the number of MAC addresses allowed in one port.
      - You can put a limit to how many MAC address a port will learn
      - You can also put timers in to state how long the MAC address will be bound to that switch port
      - You might still want to do static MAC entries on ports that there should be no movement of devices
  - Relevant to IEEE 802.1CQ, although not exacerbated by it.

Threat analysis for Wired networks

- MAC Attacks
  - VLAN hopping attacks: VLAN hopping is a network attack whereby an attacking system sends out packets destined for a system on a different VLAN that cannot normally be reached by the attacker. This traffic is tagged with VLAN ID for a VLAN other than the one on which the attacking system belongs. The attacking system can also attempt to behave like a switch and negotiate trunking so that the attacker can send and receive traffic between multiple VLANs. There are two different types of VLAN hopping attacks:
    - Switch spoofing— the network attacker configures a system to spoof itself as a switch by emulating either ISL or 802.1q, and DTP signaling. This makes the attacker appear to be a switch with a trunk port and therefore a member of all VLANs.
    - Double tagging— another variation of the VLAN hopping attack involves tagging the transmitted frames with two 802.1q headers.
  - Mitigation: Disable unused ports and put them in an unused VLAN (among others)
  - Not relevant to IEEE 802.1CQ

Threat analysis for Wired networks

- DHCP Attacks
    - DHCP Starvation, a rogue client sends thousand of requests to DHCP based on spoofed MAC addresses
    - Rogue DHCP Server Attack: Rogue user impersonates the DHCP Server.
    - Mitigation:
        - Control the number of MACs per port.
        - Define a trusted port/VLAN for DHCP dialogues, switch must discard any DHCP that comes from other port.
    - Relevant to IEEE 802.1CQ but the threat is not increased by it

Threat analysis for Wired networks

- ARP Attacks
  - ARP Poisoning, a client sends ARP spoofing an IP and MAC addresses so all traffic between two machines pass through it.
  - Mitigation: Matching of MAC to IP address based on ARP inspection and IP/MAC biding table
- Spoofing Attacks
  - If MACs are used for network access an attacker can gain access to the network
  - Also can be used to take over someone’s identity already on the network
  - Only inspection of packets and matching with MAC/IP binding table helps with this attack
- Both threats are relevant to IEEE 802.1CQ, but it does not increase the threat, .1Cq can be seen as a way of mitigating them

Threat analysis for Wired networks

- Spanning Tree Attacks:
  - Spanning-Tree Protocol vulnerabilities: Another attack against switches involves intercepting traffic by attacking the Spanning-Tree Protocol. By attacking the Spanning-Tree Protocol, the network attacker hopes to spoof his or her system as the root bridge in the topology, and then the network attacker can change the topology of a network so that it appears that the attacking host is a root bridge with a higher priority. To do this, the network attacker broadcasts out Spanning-Tree Protocol Configuration/Topology Change Bridge Protocol Data Units (BPDUs) in an attempt to force spanning-tree recalculations. The attacker can then see a variety of frames forwarded from other switches to it.
  - Mitigation: Do not allow STP traffic in all ports, only in the ones not facing users.
- Not relevant to IEEE 802.1CQ

Threat analysis for Wired networks

- Port stealing:
  - The port stealing attack uses the ability of the switches to learn to bind MAC addresses to ports. When a switch receives traffic from a port with a MAC source address, it binds the port number and the MAC address. In this attack, the attacker floods the switch with forged gratuitous ARP frames with the target host's MAC address as the source address and the attacker's MAC address as the destination address. Since the target host sends frames as well, there is a race condition. If the attacker is fast enough, frames intended for the target host are sent to the attacker's switch port and not to the target host.
  - Relevant to IEEE 802.1CQ but the threat is not increased by it

Threat analysis for Wireless networks

- Wireless networks share most of the previous threats but also include new threats coming from the lack of physical boundary [3]:
  - Traffic Analysis
  - Passive Eavesdropping
  - Active Eavesdropping
  - Unauthorised Access
  - Man in the middle
  - Session High-Jacking
  - Replay
  - DoS

Threat analysis for Wireless networks

- Traffic Analysis:
  - Traffic analysis is a simple technique whereby the attacker determines the load on the communication medium by the number and size of packets being transmitted, the source and destination of the packets and the type of packets.
    - Passive Eavesdropping: In this attack the attacker passively monitors the wireless session and the payload.
    - Active Eavesdropping: The active eavesdropping technique involves the attacker injecting data into the communication to help decipher the payload.
  - The preconditions for this attack are that the attacker has access to the transmission and has access to either part of plaintext such as a destination IP address or the contents of the entire payload.
  - If meaningful MAC addresses are used, this threat may increase due to privacy recomendations

Threat analysis for Wireless networks

- Unauthorised Access:
  - Unauthorized Access is different from any of the previous attack types in that it is not directed at any individual user or set of users on the WLAN. It is directed against the network as a whole. Once an attacker has access to the network, she can then launch additional attacks or just enjoy free network use. Although free network use may not be a significant threat to many networks, access is a key step in ARP based man-in-the-middle attacks.
  - Relevant to IEEE 802.1CQ, but this thread is not increased by IEEE 802.1CQ

Threat analysis for Wireless networks

- Man in the middle:
  - A man-in-the-middle attack can be used to read private data from a session or to modify the packets thus violating the integrity of a session. This is a real-time attack, meaning that the attack occurs during a target machine's session.
  - The data may be read or the session modified as it occurs.
  - Address Resolution Protocol (ARP) attacks are a particularly dangerous subset of man-in-the-middle attacks because these attacks can be directed against targets on the wired component of the network, not just wireless clients. The attack can involve either circumventing the authorization mechanism, if it exists, or providing false credentials.
  - Needs access to the network
  - Relevant to IEEE 802.1CQ but the threat is not increased by it

Threat analysis for Wireless networks

- Session High-Jacking:
  - To successfully execute Session High Jacking the attacker must accomplish two tasks.
    - First she must masquerade as the target to the wireless network. This includes crafting the higher-level packets to maintain the session, using any persistent authentication tokens and employing any protective encryption.
    - The second task the attacker must perform is to stop the target from continuing the session. The attacker normally will use a sequence of spoofed disassociate packets to keep the target out of the session.
  - Requires access to the network
  - Not relevant to IEEE 802.1CQ

Threat analysis for Wireless networks

- Replay:
  - Replay attacks are used to gain access to the network with the authorizations of the target, but the actual session or sessions that are attacked are not altered or interfered with in anyway. This attack is not a real-time attack; the successful attacker will have access to the network sometime after the original session(s).
  - Requires access to the network
  - Not relevant to IEEE 802.1CQ

Threat analysis for Wireless networks

- Denial of Service [2][11][12]: DoS can be performed in WLAN without the need to associate
    - Probe request flood (PRF): Probe request frames are used by stations to actively scan an area in order to discover existing wireless networks; any AP receiving a probe request frame must respond with a proper probe response frame that contains information about the network, to allow the station to associate. By sending a burst of probe request frames very quickly, each with a different MAC address (MAC spoofing) to simulate the presence of a large number of scanning stations in the area, we can induce a heavy workload on the AP, resulting in a wasting of computing and memory resources which can not be used for normal operations.
    - B. Authentication Request Flood (ARF): AP response to an authentication request frame depends on the authentication settings of the network. The AP must allocate memory to keep in- formation about each new station that successfully authen- ticates. As in the previous case, by sending a burst of authentication request frames, using MAC spoofing, it should be possible to bring AP’s resources close to the saturation level.
    - C. Association request flood (ASRF): According to the protocol FSM, association request frames should not be sent by stations in unauthenticated/unassociated state, so such requests should never receive an answer by the AP. Actually we discovered that many APs respond to “illegal” association request frames by sending a disassociation or deauthentication frame. As a consequence, even a burst of association request frames is able to consume computational resources on an AP.

IEEE 802.1CQ impact on the risks

- From all the attacks analysed, all are orthogonal to IEEE 802.1CQ.
  - The operation of IEEE 802.1CQ does not make easier to perform any of these attacks.
  - Most of attacks require the attacker to be associated to the network, therefore already having a MAC address.
  - It does not seem to have any impact in IEEE 802.1AE since MACSec is used once the MAC address is allocated
- IEEE 802.1CQ can be seen as a way of mitigating these threads

New threats brought by IEEE 802.1CQ

- DoS attacks against the LAAP Server/Proxy
- MAC address exhaustion
- Difficulty to associate IP bindings to MAC addresses
- Port shutdown technique: used when not expected MAC addresses appear in the port, may require a revisit in case .1CQ is used
- New threats appearing for Man in the middle attack
- Impersonation of LAAP server

Identification of client/server

- There are situations where we need to assign a specific MAC address to a user
- We may need to have an ID for the client and mechanisms to transport it.

References

[1] Prevention of Multiple Spoofing Attacks with Dynamic MAC Address Allocation for Wireless Networks, R. Vijayakumar, K. Selvakumar, K. Kulothungan, A.Kannan, International Conference on Communication and Signal Processing,April 3-5,2014,India

[2] Access points vulnerabilities to DoS attacks in 802.11 networks, F. Ferreri and M. Bernaschi, L. Valcamonici

[3] Wireless Security Threat Taxonomy, Donald Welch, *Senior Member, IEEE,* and Scott Lathrop

[4] Using State Model Diagrams to Manage Secure Layer 2 Switches, S P Maj, D Veal, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.9, September 2010

[5] Understanding, Preventing, and Defending Against Layer 2 Attacks, Yusuf Bhaiji

[6] Design and Implementation of a Network Security Model using Static VLAN and AAA Server , Salah A. Jaro Alabady

[7] Network Security Bible, 1'st Edition, Cole E., Krutz R. and Conley J., Wiley Publishing Inc., 2005.

[8] Cisco LAN Switching Fundamentals, David Barnes, Basir Sakandar, Cisco Press, July 15, 2004

[9] LAN security: Problems and solutions for ethernet networks, R. Khoussainov and A. Patel, Computer Standards and Interfaces, 22:191–202, 2000.

[10] Securing Layer 2 in Local Area Networks, Hayriye Altunbasak1, Sven Krasser, Henry L. Owen, Jochen Grimminger, Hans-Peter Huth, and Joachim Sokol

[11] Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks, V.Gupta, S. Krishnamurthy and M. Faloutsos, In *Proceedings of 2002 MILCOM Conference*, Anaheim, CA, October 2002.

[12] The Need for an 802.11 Wireless Toolkit , M. Schiffman. *Black Hat Briefings*, July 2002