SECURITY ADVISORY

CONTROL PLANE SECURITY BEST PRACTICES

PAPI, CPSEC, AND RISK MITIGATION

aruba
a Hewlett Packard
Enterprise company

MAY, 2016

Version 1.0

BACKGROUND

In 2003, Aruba Networks introduced one of the first scalable architectures for enterprise Wi-Fi, based on a central mobility controller and a series of distributed “thin” access points (APs). At the time, one design assumption made was that APs would be connected to dedicated wired network segments allocated only for Wi-Fi APs – in fact, the first Aruba mobility controller contained 24-port PoE line cards intended for direct attachment of APs to the controller. After a few years of experience in the marketplace, however, it became clear that the dominant deployment model had APs attaching to the same network switches and VLANs as enterprise end-user devices such as PCs and printers. This had immediate security implications for Aruba. Although Aruba’s unique centralized encryption approach meant that Wi-Fi traffic between APs and the controller was secure, the *control* traffic between APs and controllers was not so fortunate.

The original control channel between Aruba APs and controllers is called PAPI (Protocol Application Programming Interface). The PAPI protocol runs over UDP port 8211 and features a very efficient syntax for message passing. However, because of the design assumptions described in the previous paragraph, security was not the foremost concern when PAPI was designed. The protocol uses a light form of encryption, designed with obfuscation in mind rather than completely protecting confidentiality. Notably, all Aruba devices share the same encryption key, which is what allowed an Aruba AP to be taken out of the shipping box and immediately joined to a mobility controller. For integrity protection, a simple checksum based on MD5 is employed. This scheme is not resilient against an attacker.

To address the vulnerabilities of PAPI given the deployment architecture that emerged, Aruba introduced Control Plane Security (CPsec) in 2009 with ArubaOS 5.0. In 2010, CPsec was enabled by default for all new ArubaOS installations. CPsec is, at its core, PAPI running inside an IPsec ESP tunnel. The IPsec tunnel is authenticated using X.509 certificates loaded onto Aruba controllers and APs during the manufacturing process, with the private key protected by a tamper-resistant Trusted Platform Module (TPM) which is part of the hardware. Within CPsec, the PAPI protocol itself is not altered or made more secure. Instead, the system relies on IPsec to provide confidentiality, integrity protection, and anti-replay protection.

GOOGLE SECURITY TEAM INTERACTION

In January of 2016, Aruba was engaged by the Google Security Team in a discussion around the use of PAPI. During this discussion, it became clear that a number of customers are at risk today, both because of decisions that Aruba has made as well as a general unawareness on the part of customers regarding the risks of PAPI. Specifically:

- Numerous Aruba customers with controller-based AP deployments have disabled CPsec without an awareness of the risk this creates. Although Wi-Fi user data is secure (when tunnel-mode is configured), an attacker with access to the wired network may be able to disrupt the Wi-Fi network by changing radio channels, adjusting power levels, or rebooting an access point.

- Aruba's Instant product line (IAP) uses PAPI as the control protocol between IAP cluster members, and often IAP clusters are set up to allow new cluster members to join without authorization. An attacker who is able to monitor the PAPI exchange between IAP cluster members could retrieve sensitive information including administrative credentials and user passwords. An attacker who is able to inject PAPI traffic between cluster members could alter configuration.
- Aruba controllers communicate with the AirWave Management Platform *in part* using PAPI. Specifically, the AMON protocol, which is a high-speed and efficient message format for transmitting wireless statistics and measurements from a controller to AirWave, is encapsulated using PAPI. An attacker who is able to monitor this communication could learn potentially interesting information about a network. An attacker who is able to inject PAPI traffic into this communication path could cause erroneous information to be received by AirWave, which could be disruptive to network operations. The WMS Offload feature also uses PAPI between controllers and AirWave.
- Aruba controllers communicate with the Aruba Analytics and Location Engine (ALE) using the PAPI protocol. An attacker with the ability to inject traffic into this path could cause erroneous location information to be recorded by ALE.
- For controller-based deployments, some inter-controller communication protocols are encapsulated inside PAPI. Specifically:
    - Centralized licensing heartbeats in an all-master controller configuration when centralized licensing has been configured. If an IPsec tunnel has been configured between controllers as described in the user guide, these messages will be protected. By default, they will be unprotected.
    - High Availability heartbeat replies

In addition to the above, the Google Security Team pointed out a number of weaknesses in Aruba's implementation of PAPI:

- The static encryption key used by all PAPI implementations is available on AirWave Management servers. An attacker who can locate this key and has the skills to use it could inject PAPI traffic into any Aruba network if given sufficient network access.
- Validation of the HMAC-MD5 PAPI checksum was disabled in the past as a performance optimization. The checksum is still created and appended to PAPI messages, but the receiver does not validate that it is correct. Although this checksum is not a strong cryptographic message integrity check (MIC) given the static key, it does provide some protection against malformed or tampered PAPI messages and should remain enabled as a best practice.
- The method used to perform PAPI encryption, as previously explained, is not secure. A skilled attacker can discover the key by passively examining a sufficient quantity of PAPI traffic. Thus, even with a customer-configurable PAPI key, it is still possible for an

attacker with access to a PAPI communication path to learn the key, decode PAPI messages, and inject crafted PAPI messages.

- On controllers, PAPI may be blocked through firewall rules. However, IAP was listening for PAPI communication on all interfaces, including wireless interfaces, and it was not possible to disable or block this protocol listener.

UPDATES AND FUTURE PLANS

To address issues pointed out by the Google Security Team, Aruba has released a number of updates, and plans further updates in the future.

Aruba Instant

Versions 4.2.3.1 and 4.1.3.0 contain fixes for a number of PAPI issues (along with other security vulnerabilities described in a separate advisory). Version 4.2.3.1 is a patch release based on version 4.2.3.0. Version 4.1.3.0 is based on version 4.1.1.12, and contains only vulnerability-related fixes. The previously-released version 4.1.2 has been recalled; customers running that branch should migrate to 4.2.3.1. PAPI-related fixes in these versions include:

- **PAPI endpoints exposed on all interfaces (bug 134965)**

  By default, IAPs listened on all interfaces, including Wi-Fi interfaces, for PAPI messages. Previously, automatic firewall rules were added to permit PAPI, which would override any user-configured firewall rules that attempted to block PAPI. Two changes were made to this behavior:

  - In cluster mode, a new firewall configuration option has been added:

    ```
    # firewall
    (firewall)# disable-auto-topology-rules
    ```

    When this option is enabled, the automatic firewall rules that permit PAPI will not be added. This allows an administrator to configure specific firewall rules for UDP 8209/8211 to control the source of PAPI messages. Aruba recommends limiting PAPI traffic to only IP subnets where other IAP cluster members reside. See the “Best Practices” section below for a configuration example.

    Note that the above command may require CLI-based configuration, and as of this writing (May 2016) may not be supported by graphical configuration methods, including through AirWave and Aruba Central.

  - When an IAP is configured in standalone mode, automatic firewall rules will no longer be added that permit PAPI. The effect is the same as if the above “disable-auto-topology-rules” option is enabled.

- **PAPI protocol authentication bypass (bug 134971)**

A vulnerability was discovered that allowed an attacker to bypass certain PAPI authentication checks. By exploiting this vulnerability, an attacker could obtain the complete configuration of an IAP including usernames, passwords, and keys. *Fixing this vulnerability only addresses one aspect of PAPI security; the protocol still cannot be considered to be cryptographically strong.*

Future

In the near-term future, a new control protocol will be implemented for IAP clustering. This protocol will be based on DTLS, a standard security protocol used for protecting UDP-based communication. The intent is to encapsulate PAPI inside DTLS, providing it proper encryption and authentication. Through the use of DTLS, IAP clusters may be deployed on hostile networks without the risk present with the current PAPI protocol. Further details will be provided in product release notes once this feature is made available.

ArubaOS

Mobility controllers and APs running ArubaOS face much less exposure to PAPI issues than the IAP product line. CPsec is already available to secure controller-to-AP communication, and Aruba recommends that it always be enabled. To address issues related to controller-to-AirWave and controller-to-ALE communication, ArubaOS 6.5 will introduce two new features:

- **Validation of HMAC-MD5 checksum (bug 134968)**

  Beginning in ArubaOS 6.5, an option will be provided to enable enhanced PAPI security through validation of MD5 checksums. *Even with this enhancement, PAPI still cannot be considered cryptographically strong.*

- **Configurable PAPI encryption key**

  Beginning in ArubaOS 6.5, an administrator may configure a unique PAPI encryption key, rather than using a static, default key. The same key must be configured on AirWave and ALE. In a master-local environment, the master will push this key to local controllers automatically. APs will not support a configurable PAPI key; APs should use CPsec to secure their communications. *Even with this enhancement, PAPI still cannot be considered cryptographically strong.*

Future

The AMON protocol (running over PAPI), used between mobility controllers and AirWave/ALE, needs an option for strong security for cases where the intervening network is untrusted. Aruba is investigating the use of DTLS as a lightweight secure channel for these messages, and plans to introduce this as a future enhancement. Further details will be provided in product release notes once this feature is made available.

AirWave

AirWave includes a PAPI receiver, used to accept AMON feeds from Mobility Controllers. This receiver will be enhanced in the same timeframe as ArubaOS to include a configurable PAPI encryption key and an option to enable validation of HMAC-MD5 checksums. Further details will be provided in product release notes once this feature is made available.

RISK MITIGATION & CURRENT BEST PRACTICES

Aruba Instant

Without exception, IAP networks should be upgraded to a minimum of software version 4.1.3.0 or 4.2.3.1 in order to address security vulnerabilities.

Once the operating software has been updated:

- If the wired network supports port security or other features to block ARP poisoning, enables these features. This will prevent man-in-the-middle attacks against network nodes.
- If the wired network is considered hostile, consider dedicating a VLAN for Instant APs to use for management traffic.
- If the wired network is considered to be physically compromised by attackers such that an isolated VLAN will not provide any benefit, consider installing a mobility controller and converting the IAPs over to thin APs managed by the controller. Controller-managed APs are designed to be deployed into less trustworthy networks.
- It may be desirable to use firewall rules to limit PAPI communication only to local subnets. In an environment where private IP addresses are used and local subnets are not reachable from untrusted networks, this step may not be necessary.

Adding Firewall Restrictions

IAP runs a process that listens on all network interfaces for UDP 8209 and UDP 8211. For an IAP in standalone mode, it is safe to apply a firewall policy that blocks all PAPI communication. For APs in cluster mode, firewall policies should be selective so that other cluster members may still communicate over UDP 8209 and 8211. Block these ports for cluster non-members.

- For cluster-mode IAPs, enable the configuration option “firewall disable-auto-topology-rules” as described previously. This command must be performed from the command-line interface. Without this option enabled, firewall rules to permit PAPI will be automatically inserted at the beginning of the inbound firewall ruleset.
- To block PAPI on wired (“inbound”) interfaces, navigate in the WebUI to Security->Inbound Firewall. Add a rule to deny UDP 8209 and UDP 8211 from all sources. Or, for clustered IAPs, add rules to permit 8209 and 8211 from other cluster members, and then block these ports from all other sources.
- To block PAPI on wireless interfaces, edit a WLAN to bring up the WLAN configuration wizard. Navigate to the “Access” tab. If only specific protocols are permitted, a final “deny all” rule will have the effect of blocking PAPI. Otherwise, add rules to block UDP 8209 and UDP 8211.

ArubaOS

Mobility controllers and AirWave should communicate with each other over trusted management networks – a survey of Aruba’s largest customers indicates that generally, this is already the case.

Control Plane Security (CPsec) should be enabled to protect control/management messages between controllers and access points. CPsec is enabled by default for new deployments, but customers have the ability to disable it. Note that enabling CPsec has implications on how Aruba networks are managed, and migration from non-CPsec to CPsec may involve changes to procedures. Some of these include:

- APs must be authorized by MAC address by adding them to the CPsec whitelist. Alternatively, an “allow-all” configuration knob may be set for initial provisioning.
- The procedure to replace a failed controller may change, and the procedure differs depending on whether the controller is a CPsec anchor or not.

The ArubaOS User Guide has a chapter entitled “Control Plane Security” which goes through these issues in detail. Please consult the guide before enabling CPsec.

When CPsec is in use, the controller still listens for cleartext PAPI messages. A firewall rule may be used to shut down this port entirely, as long as it is not needed. Blocking PAPI with firewall rules should be done with the following caveats in mind:

- Unprovisioned APs will be unable to boot when PAPI is blocked; previously provisioned APs that are configured for CPsec will continue to function. When new APs are added to the network, temporarily remove the firewall rule blocking PAPI to allow APs to join the network, then re-enable the firewall rule. Alternatively, connect new APs directly to a “provisioning” controller, then move them to their final network location after provisioning.
- When centralized licensing is in use, PAPI is used to carry licensing messages. For standby-master controllers, or in a master-local topology, IPsec tunnels are formed between nodes and all centralized licensing communication will be protected by IPsec – blocking PAPI will have no effect. However, for “all-masters” deployments, license heartbeat messages are sent using PAPI. To protect these messages, configure site-to-site IPsec tunnels between nodes, or use firewall rules to explicitly permit PAPI communication between license servers and license clients.
- High availability features allow fast failover in the event a controller fails. Heartbeat messages are sent using IPsec tunnels, but heartbeat replies are sent in cleartext. In general, these messages do not present a security concern if intercepted. However, if HA features are in use, PAPI should not be blocked entirely. Instead, use firewall rules to selectively control where PAPI messages may be sent.

A sample site-to-site IPsec policy is found below. Note that this will enable transport mode IPsec (dst-net is the same as the peer-ip). Only IKEv1 may be used with transport mode.

```
crypto-local ipsec-map S2S-LicenseMasterVrrp 30
```

```
  set ikev1-policy 30
  peer-ip 172.17.1.100
  vlan 6
  src-net 172.17.2.2 255.255.255.255
  dst-net 172.17.1.100 255.255.255.255
  set transform-set "default-aes"
  pre-connect enable
  trusted enable
```

The following are two examples of a firewall policy that can be used to selectively permit/block PAPI:

```
ip access-list session BlockPAPI
  any any udp source 8211 dest 8211  deny
  any any any  permit
  ipv6  any any udp source 8211 dest 8211  deny
  ipv6  any any any  permit

ip access-list session BlockPAPI_With_Exception
  ipv6 host 20::1 host 20::2 udp source 8211 dest 8211  permit
  host 172.102.1.2 host 172.102.1.1 udp source 8211 dest 8211  permit
  any any udp source 8211 dest 8211  deny
  ipv6 any any udp source 8211 dest 8211  deny
  any any any  permit
  ipv6  any any any  permit
```

Once configured, these policies are applied to all active interfaces or VLANs. For example:

```
(config) #interface gigabitethernet 1/0/0
(config-if)#ip access-group BlockPAPI session
```

Or to apply to a VLAN:

```
(config) #interface gigabitethernet 1/0/0
(config-if)#ip access-group BlockPAPI session vlan 10
```

Blocking PAPI within user roles is also recommended, to prevent wireless users from sending this type of traffic. Apply this session ACL to each user role (the “authenticated” role is used as an example here):

```
ip access-list session Block_Only_PAPI
  any any udp source 8211 dest 8211  deny
  ipv6  any any udp source 8211 dest 8211  deny

user-role authenticated
  session-acl Block_Only_PAPI position 3
```

As an alternative to the above interface/user-role configuration, a *Service ACL* or *Control Plane Firewall* rule may be implemented to selectively block PAPI messages from being received on *all* interfaces – wired, wireless, and virtual. The following is an example of a Service ACL that permits PAPI from 172.102.1.2 and denies it from all other source IP addresses, including all IPv6 addresses.

```
(Hostname) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(Hostname) (config) #firewall cp
(Hostname) (config-fw-cp) #ipv4 permit host 172.102.1.2 proto 17 ports 8211 8211
(Hostname) (config-fw-cp) #ipv4 deny any proto 17 ports 8211 8211
(Hostname) (config-fw-cp) #ipv6 deny any proto 17 ports 8211 8211
```

AirWave

If the network between controllers and AirWave is untrusted, firewalls (or firewall rules configured on the AirWave server) should be used to limit communication on UDP ports 8211 so that it originates only from networks where mobility controllers are present.

FOR FURTHER ASSISTANCE

Updates to this document will be posted at http://support.arubanetworks.com under the Announcements tab. Please check back for further updates.

Main Site	http://www.arubanetworks.com/
Support Site	https://support.arubanetworks.com/
Airheads Social Forums and Knowledge Base	http://community.arubanetworks.com/
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	http://www.arubanetworks.com/support-services/contactsupport/
Software Licensing Site	https://licensing.arubanetworks.com/
End-of-life Information	http://www.arubanetworks.com/support-services/end-of-life/
Security Incident Response Team (SIRT)	http://www.arubanetworks.com/support-services/securitybulletins/
Support Email Addresses	
Americas, EMEA, and APAC	support@arubanetworks.com
Security Incident Response Team (SIRT)	sirt@arubanetworks.com