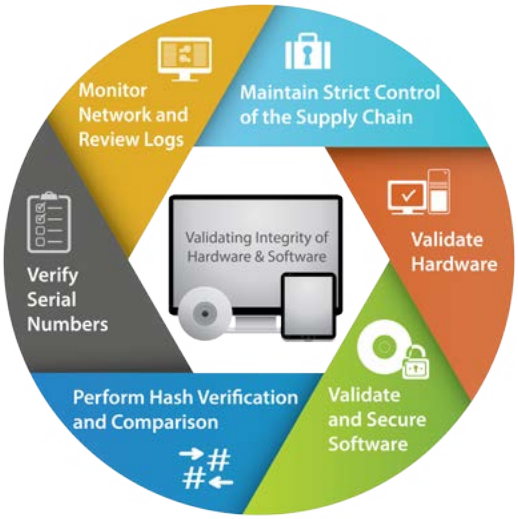
Validate Integrity of Hardware and Software

June 2016

Threat of Counterfeit Network Infrastructure Devices

Grey market devices are network infrastructure devices acquired through unofficial channels. These devices can cause a loss of intellectual property and damage to reputation. Counterfeit hardware and software have appeared across many industries. They are often introduced into the supply chain through non-reputable re-sellers. Unknowingly using grey market devices can significantly compromise your network by introducing vulnerabilities such as logic bombs, backdoors, and altered security functions. It is important to confirm the integrity of devices and software throughout the entire supply chain.



Maintain Strict Control of the Supply Chain

Having robust supply chain management processes can reduce the risk of introducing grey market devices:

- Purchase only from manufacturer-authorized resellers.
- Obtain an original copy of the invoice.
- Verify that all serial numbers match throughout the supply chain.
- Train network owners and administrators how to detect grey market devices.
- Require resellers to implement a supply chain integrity check to validate hardware and software authenticity.

Validate Hardware

- Visually inspect hardware devices for anomalies on the chassis and cards to check for tampering.
- Check the packaging for any skewed or missing logos as well as missing serial numbers, model numbers, or holograms.
- Serial numbers on the hardware and boxes should match.
- Examine hardware for missing circuit board labels or discoloration. Circuit board chips should be in the appropriate location for the device.

Verify Serial Numbers

Collect serial numbers and compare using vendor management tools. Once the serial number of the device has been collected, complete a counterfeit assessment to determine if the serial numbers are consistent with the vendor's. Check with the vendor to see which tools are available. Examples include:

- SolarWinds®[1]: Kiwi CatTools: Use the "Report.Version" table component to pull serial numbers from the device.
- CiscoWorks®[2]: Validate the Cisco Internetwork Operating System® (Cisco IOS®) on network devices to determine whether the device has been tampered with. To view the Cisco IOS® information, issue the "show version", "show inventory", and "show hardware" commands to retrieve the serial number.
- Brocade®[3]: Use the "chassisshow" command to retrieve serial numbers.

If an automated tool is not available, a script can be used to retrieve serial numbers.

---

[1] SolarWinds® is a registered trademark of SolarWinds Worldwide

[2] Cisco IOS® is a registered trademark of Cisco Systems, Inc.

[3] Brocade® is a registered trademark of Communications Systems, Inc.

Validate Integrity of Hardware and Software

Validate and Secure Software

Hash software and compare to the vendor database to determine whether it has been altered. Additional mitigations to prevent grey market software from being introduced onto a network include:

- Download software, patches, and upgrades from validated sources. Software provided by the vendor should be digitally signed by the vendor.
- Protect network information data by encrypting both stored configurations and network management communications.
- Maintain secure configurations offline and at an offsite location.

Perform Hash Verification and Comparison

Hash comparison is a method that can be used to verify network device software integrity. Check with the vendor to identify the appropriate integrity validation process and methodology. There are several types of hashes that must be compared with the hash of a known, trusted operating system image from the vendor in order to achieve the highest level of confidence. All of these hashes should be identical. If any of the hashes do not match, the source of the concern should be further examined. An example of a robust hash-based verification processes is:

- Acquire the known trusted operating image from the vendor.
- Calculate the online hash. Remotely log into the device with proper credentials and use the built-in functionality of the network device's operating system to compute the hash.
- Derive the offline hash. Copy the operating system image directly from the network device to a trusted system and use the built-in functionality to compute the hash.
- Compare computed hashes to the trusted known good hashes.

Monitor Network and Review Logs

If a device is suspected of not meeting the quality standards and assessments, it is best not to immediately disconnect or cause a denial of service. This can make it challenging to obtain an authenticated image. Keep in mind, a false positive hash can occur which would create a hash that does not match the vendor hash.

- Monitor all ports through passive sensors. Data that is concentrated on network packets sent to and from the device should be collected and logged.
- Check logs for unauthorized logins, unauthorized reboots, misconfiguration of settings, and operating system anomalies. This information can then be used by incident response teams for evaluation and can accelerate analysis to isolate the problem.
- If there are discrepancies in the logs, the network device can be removed and replaced if necessary.
- Continuously monitor and verify network configurations on a regular basis in order to determine if the security compromise extends beyond the device.

Detection and prevention of grey market and counterfeit devices can be improved by incorporating requirement assessments and technical reviews into the acquisition process. Training network owners and administrators will increase awareness of grey market devices. A knowledgeable and cooperative effort will maximize the detection and prevention capabilities for the network.

Contact Information

Industry Inquiries:

Business Affairs Office
410-854-6091
email: bao@nsa.gov

Client Requirements and General Information Assurance Inquiries:

IAD Client Contact Center
410-854-4200
email: IAD_CCC@nsa.gov