The Cyber Security Landscape for Screening Equipment

Information security and security screening technologies

Edam Colón
Cybersecurity Specialist
Information Assurance and Cybersecurity Division

Why do we care about Cybersecurity?

We don’t, we REALLY care about Cybersecurity!

- Information Technology enhances Operational Technology’s availability and integrity
- Current cybersecurity of screening solutions?
- Analogy… would you buy a laptop in this condition?
- Have you asked your security team if they would be willing to connect your screening solution to the corporate network?

We like to believe that our environments are secured and could easily detect a compromise before it affects us:

- Operation Aurora – Google source code compromise
- Stuxnet – Isolated environment, PLC rootkits
- Target Hack – Third party vendor / supply chain attack

Hot topic – airport security

North America Gov
Massive (400+ sites) asset replacement (US), Centralised Admin (CA)

US Gov
NIST RMF;
NIST SP 800-53

Vendors
Still struggling to demonstrate cyber security expertise

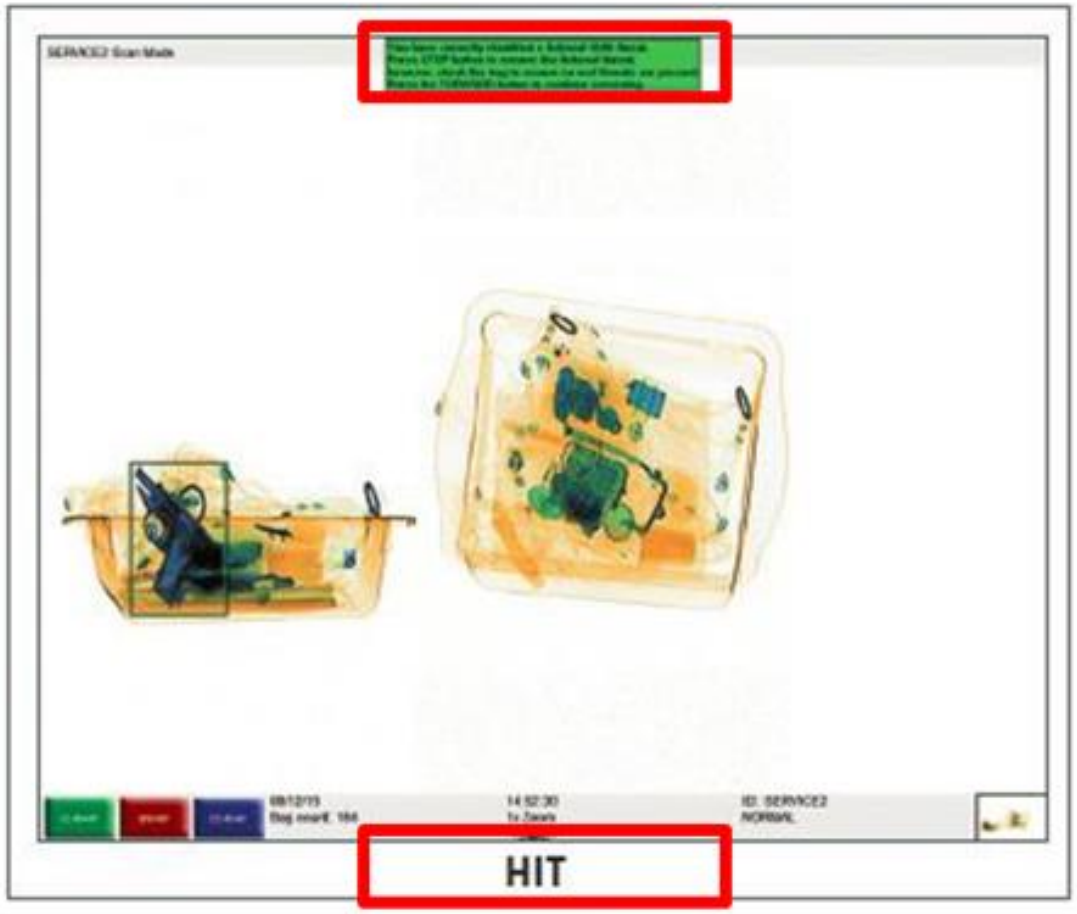
UK Gov
Functional requirements from DfT/CAA; advice on Cyber from DfT/NCSC; CAA now aware of challenges

Heathrow
Automation, T5+/T3; Security Programme,
Asset Replacement; Expansion

ICAO/EU
Regulations on cyber security – 4Q2019

ACI/European Airports
All facing same challenges

What's the worst that could happen?



Source: http://blackhat.com/docs/us-14/materials/us-14-Rios-Pulling-Back-The-Curtain-On-Airport-Security.pdf

Status of Cyber Security across Screening environment

- The vendors provide very good hardware
  - Detection algorithms are often developed in partnership with academia and niche players
- International collaboration
  - Partners such as the TSA and CATSA shared knowledge and expertise

- Long lifetime/traditional IT security practices are difficult to implement
  - Implementation/Configuration/Operation is OT – not IT
  - Patching/testing may be impractical
  - Multiple versions/ages in operation
  - 'Blackbox' solutions potential to increase cyber security threat landscape
- Inter-vendor cooperation a challenge; who is responsible when integration is needed?
- Impending EU Regulations (“NIS-like”)
- Lack of awareness from regulators
- Vendor commitments on software capabilities
- Responding to government mandates, regulation, legislative changes

- Manufacturers demonstrate poor cyber-security culture and practices – examples include:
  - Default passwords; vulnerable operating systems; lack of encryption; poor configuration; risky behaviour/lack of awareness
  - Hardware and software, lack of upgrade paths,'unnecesary' capability
- No quality score of ECAC compliance available to purchases of equipment
- Interoperability between vendors, data standards and Open Architecture
- Reputational awareness

Key requirements

Commitment from vendors to meet

1. Cybersecurity culture - adopt a culture of “cybersecurity by design” for Security Equipment – demonstrable
2. Access Control - implement adequate access control and account management practices
3. Access Control - enable multi-level access to equipment resources and ability to restrict users to required access level
4. Password Control - implement and provide capability for airport operator to change system level passwords
5. Identification and Authentication - ensure unique identification of individuals, activity, or access to Security Equipment
6. Audit and Accountability - ensure capabilities to audit events, conduct analysis and reporting, and monitor for appropriate information disclosure
7. Protected Sensitive Screening Algorithms - must ensure adequate system protections to protect screening algorithms from compromise, modification, rendering the equipment inoperable and provide immediate alerting when algorithms have been accessed
8. Physical and Environment Protections - ensure physical security measures prohibit unauthorized access to Security Equipment (e.g. ensure USB ports are covered, access to ports, cables, and other peripherals are protected from unauthorised use)
9. Configuration Management - employ automated measures to maintain baseline configurations and ensure system protections are employed to protect these from compromise, modification, rendering the equipment inoperable and provide an immediate alerting when baseline configurations have been accessed, and/or modified

Key requirements

Commitment from vendors to meet

10. Systems and Communications Protections - ensure system adequately manages any internal and external interfaces, encrypts ingress and egress traffic with cybersecurity industry standard technology
11. System and Information Integrity - address/implement methods to update Security Equipment affected by software flaws including potential vulnerabilities resulting from those flaws
12. Security Scanning - security assessment tools run on devices to ensure appropriate configuration, patch levels, and that there are no Indicators of Compromise (IOC) present that may impact screening process system integrity
13. Supported Systems - ensure full Security Equipment hardware, software, and operating system support to remediate any identified vulnerabilities with the Security Equipment or supporting systems (Patching)
14. Data at Rest Encryption - ensure all data at rest on Security Equipment fully utilises approved encryption method to ensure integrity
15. Supply Chain Management - provide a comprehensive list of all software and hardware (Bill of Materials) that comprise Security Equipment offering
16. Threat update - demonstrate ability to update equipment design and capabilities to align with changing cyber intelligence and threat reporting
17. Personnel Security - all maintenance personnel (local or remote) must be vetted by local or country authority including appropriate background checks

Key technical areas

Operating Systems

- The primary tool used to test operating systems is a vulnerability scanner. The vulnerability scanner will remotely connect to each target asset operating system and review items such as configuration settings, registry entries, patch levels, and user accounts.
  - Vulnerability scanning is a non-intrusive testing method.

Web Applications

- Web applications and services are tested using a variety of testing tools. These tools look for vulnerabilities such as SQL injection, cross-site scripting, privilege escalation, and default configurations.
  - Automated web application testing is considered to be **highly intrusive** and will inject, delete and modify data.

Databases

- All database instances are reviewed by database scanners. The database scanner will make a remote connection to each database instance to evaluate items such as user accounts, inappropriate privileges, missing patches, and weak passwords.
  - Database scanners are considered a non-intrusive testing tool.

Network Devices

- Network devices include devices such as switches, routers, and firewalls. Different tools can be used to audit these devices for weak configuration settings, use of insecure services, and other security issues.
  - Network evaluation tools are a non-intrusive testing tool.

Questions to Consider

- How will you **detect and validate the integrity** of your software and data?
- How will you maintain a regular schedule for **standard security patching** and **emergency patches**?
- How will the system **protect its data**, both at rest, in transit and in use?
- How will you, as the vendor, **vet maintenance personnel** that is working on the equipment at the airports (either physically or virtually)?
- How will you ensure the **integrity** of these systems when maintenance personnel use their diagnostic equipment (e.g., laptops, testers, USBs)?
- What else are you connecting to this system?

Thank you for your attention

Any questions?