Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/26/2022 11:03:44 am • Time spent: 01:54

Score: 70% Passing Score: 80%

Question 1: ✔ Correct

Which of the following is an open-source hardware and software company that designs and manufactures single-board microcontrollers as well as kits to build digital devices?

- Microsoft
- Raspberry Pi
- Arduino
- Amazon

EXPLANATION

Arduino is an open-source hardware and software company. They design and manufacture single-board microcontrollers as well as kits to build digital devices.

Raspberry Pi is a common device that uses a system on a chip (SoC).

Neither Microsoft nor Amazon are an open-source hardware and software company that designs and manufactures single-board microcontrollers as well as kits to build digital devices.

REFERENCES

9.9.5 Embedded and Specialized Systems Facts

q_embed_sys_arduino_secp7.question.fex

Question 2: ✔ Correct

You manage information systems for a large co-location data center.

Networked environmental controls are used to manage the temperature within the data center. These controls use embedded smart technology that allows them to be managed over an internet connection using a mobile device app.

You are concerned about the security of these devices. What can you do to increase their security posture? (Select two.)

- [ ] Enroll each device in a mobile device management (MDM) system.
- [ ] Install anti-malware software on each device.
- [x] Install the latest firmware updates from the device manufacturer.
- [ ] Rely on the device manufacturer to maintain device security with automated firmware updates.
- [x] Verify that your network's existing security infrastructure is working properly.

EXPLANATION

Since you generally have little or no control over the embedded technology within smart environmental control devices, they are referred to as static environments. As a result, there is typically very little you can do to increase the security posture for these types of devices. For environmental controls, you may be able to perform the following, depending upon the device manufacturer:

- Install the latest firmware updates from the device manufacturer.
- Verify that your network's existing security infrastructure is working properly.

Because these devices operate in a static environment, you typically can't install third-party software on them, including anti-malware scanners or mobile device management (MDM) agents. Relying on the device manufacturer for security updates is problematic because manufacturers can be slow to take steps to protect their products against security threats. Manufacturers tend only to respond after an exploit has occurred instead of proactively defending their systems.

REFERENCES

9.9.5 Embedded and Specialized Systems Facts

q_embed_sys_facility_secp7.question.fex

Question 3: ✔ Correct

You manage the information systems for a large manufacturing firm.

Supervisory control and data acquisition (SCADA) devices are used on the manufacturing floor to manage your organization's automated factory equipment. The SCADA devices use embedded smart technology, allowing them to be managed using a mobile device app over an internet connection.

You are concerned about the security of these devices. What can you do to increase their security posture? (Select two.)

- [ ] Install a network monitoring agent on each device.
- [x] Verify that your network's existing security infrastructure is working properly.
- [ ] Enroll each device in a mobile device management system.
- [ ] Install anti-malware software on each device.
- [x] Install the latest firmware updates from the device manufacturer.

EXPLANATION

Since you generally have little or no control over the smart technology embedded within SCADA devices, they are referred to as static environments. As a result, there is typically very little you can do to increase the security posture for these types of devices. For SCADA devices, you may be able to perform the following, depending on the device manufacturer:

- Install the latest firmware updates from the device manufacturer.
- Verify that your network's existing security infrastructure is working properly.

Because these devices operate in a static environment, you typically can't install third-party software on them, including anti-malware scanners, monitoring agents, or mobile device management agents.

REFERENCES

9.9.5 Embedded and Specialized Systems Facts

q_embed_sys_manu_secp7.question.fex

Question 4: ✕ Incorrect

Which of the following serves real-time applications without buffer delays?

- ~~SCADA~~
- SoC
- FPGA
- RTOS

EXPLANATION

A real-time operating system (RTOS) is an operating system that serves real-time applications without buffer delays. They are generally used in systems that require a response within a strict time constraint.

Supervisory control and data acquisition (SCADA) devices are special computer systems that gather, analyze, and manage automated factory equipment.

A system on a chip (SoC) is an integrated circuit that includes all components of a typical computer system, including digital, analog, mixed-signal, and radio frequency functions.

A Field-Programmable Gate Array (FPGA) is an integrated circuit manufactured and then later configured by the customer.

REFERENCES

9.9.5 Embedded and Specialized Systems Facts

q_embed_sys_rtos_secp7.question.fex

Question 5: ✔ Correct

Which of the following devices are special computer systems that gather, analyze, and manage automated factory equipment?

- SoC
- MFD
- UAV
- SCADA

EXPLANATION

Supervisory control and data acquisition (SCADA) devices are special computer systems that gather, analyze, and manage automated factory equipment.

A system on a chip (SoC) is an integrated circuit that includes all components of a typical computer system, including digital, analog, mixed-signal, and radio frequency functions.

A multi-function display (MFD) is a screen surrounded by configurable buttons that can be used to display information in a variety of ways.

Unmanned Aerial Vehicles (UAVs) are used for military campaigns, search and rescue, weather monitoring, and recreation.

REFERENCES

9.9.5 Embedded and Specialized Systems Facts

q_embed_sys_scada_secp7.question.fex

Question 6: ✔ Correct

You notice that a growing number of devices, such as environmental control systems and wearable devices, are connecting to your network. These devices, known as smart devices, are sending and receiving data via wireless network connections.

Which of the following labels applies to this growing ecosystem of smart devices?

- The smartnet
- Internet of Things (IoT)
- Internet of smart devices
- Dynamic environment

EXPLANATION

These smart devices are part of a growing ecosystem known as the Internet of Things (IoT). Environments that contain these types of devices are known as static environments. A static environment is one that never changes (or changes very infrequently) and that a network administrator has very little control over. For example, a smart television in an office has embedded technology that might never be updated, which creates a security hole in the company's network.

REFERENCES

9.9.5 Embedded and Specialized Systems Facts

q_embed_sys_smart_01_secp7.question.fex

Question 7: ✔ Correct

Which Amazon device can be used to control smart devices (such as lights) throughout a home using voice commands?

- Echo
- Siri
- Home
- Cortana

EXPLANATION

Amazon Echo devices can be integrated into a user's home to control other smart devices using voice commands.

Home is Google's product line that can be integrated to control smart devices using voice commands.

Cortana is Microsoft's digital assistant.

Siri is Apple's digital assistant.

REFERENCES

9.9.5 Embedded and Specialized Systems Facts

q_embed_sys_smart_02_secp7.question.fex

Question 8: ✕ Incorrect

Which of the following do Raspberry Pi systems make use of?

- SoC
- ~~FPGA~~
- RTOS
- SCADA

EXPLANATION

A system on a chip (SoC) is an integrated circuit that includes all components of a typical computer system, including digital, analog, mixed-signal, and radio frequency functions. Raspberry Pi is a common device that uses an SoC. Because of their relatively low cost, SoCs are often used by hobbyists.

A real-time operating system (RTOS) is an operating system that serves real-time applications without buffer delays. They are generally used in systems that require a response within a strict time constraint.

Supervisory control and data acquisition (SCADA) devices are special computer systems that gather, analyze, and manage automated factory equipment.

A Field-Programmable Gate Array (FPGA) is an integrated circuit configured by the customer.

REFERENCES

9.9.5 Embedded and Specialized Systems Facts

q_embed_sys_soc_secp7.question.fex

Question 9: ✔ Correct

Which of the following lets you make phone calls over a packet-switched network?

- FPGA
- VoIP
- SCADA
- RTOS

EXPLANATION

Voice over IP (VoIP) is a protocol optimized for the transmission of voice data (telephone calls) through a packet-switched IP network. VoIP routes phone calls through an IP network, including the internet. VoIP solutions can integrate with a public-switched telephone network (PSTN) to allow VoIP customers to make and receive external calls.

A Field-Programmable Gate Array (FPGA) is an integrated circuit configured by the customer.

A real-time operating system (RTOS) is an operating system that serves real-time applications without buffer delays. They are generally used in systems that require a response within a strict time constraint.

Supervisory control and data acquisition (SCADA) devices are special computer systems that gather, analyze, and manage automated factory equipment.

REFERENCES

5.12.2 VLAN Facts

9.9.5 Embedded and Specialized Systems Facts

q_embed_sys_voip_secp7.question.fex

Question 10: ✕ Incorrect

Why do attackers prefer to conduct distributed network attacks in static environments? (Select two.)

- [x] Devices tend to employ much weaker security than traditional network devices.
- [ ] These devices are typically installed in the DMZ that resides outside of an organization's perimeter firewall.
- [x] ~~It is difficult to update the virus definitions used to protect these devices.~~
- [ ] Devices are typically more difficult to monitor than traditional network devices.
- [ ] Smart device vendors tend to proactively protect their products against security threats.

EXPLANATION

Attackers prefer static environment devices to conduct distributed network attacks for the following reasons:

- Static devices tend to employ much weaker security and are easier to exploit than traditional targets, such as desktops, notebooks, tablets, and smartphones.
- Smart device vendors tend to reactively protect their products against security threats, responding only after an exploit has occurred instead of proactively defending systems.
- Static devices are typically more difficult to monitor than traditional network devices.

Because these devices operate in a static environment, you typically can't install third-party software on them, including anti-malware scanners. Because of their relatively weak security, these devices should not be deployed in an unsecure area of a network, such as the DMZ.

REFERENCES

9.9.5 Embedded and Specialized Systems Facts

q_embed_sys_weak_secp7.question.fex