2.4 INFORMATION COMMUNICATION TECHNOLOGIES – CRYPTOGRAPHY/CRYPTOANALYSIS

IoT Security Technician Skill Zone – CSSIA.ORG

2. Information Communication Technologies

2.4 Cryptography/Cryptoanalysis

1. Explain the purpose and type of cryptography used in modern communication systems.
2. Define cryptology and cryptanalysis.
3. Differentiate encryption algorithms including IPSEC, AES, GRE, IKE, MD5 and 3DES.
4. Describe the difference between cryptography and cryptanalysis.
5. Describe the use of a hashing in IoT environments and devices.
6. Describe the importance of mutual authentication in industrial control and IoT environments.

Cryptography/Cryptoanalysis

Cryptography/Cryptoanalysis can be defined as the practice and study of techniques for securing communications and stored information. Cryptography/Cryptoanalysis consists of the use of encoding and decoding algorithms. They are used to protect the confidentiality of sensitive data from adversaries and unauthorized individuals. Modern cryptography is based on mathematical operations used to scramble information with the use of keys to control the encoding and decoding of that information.

IoT security technicians must have a working knowledge of both symmetrical and asymmetrical cryptographic systems including DES, DES III, RSA, DIFFIE-Hellman and AES. They must also have working knowledge of virtual private networks (VPN's) and the protocols used to manage these networks including IPSEC, IPV6, GRE and IKE. Finally, these technicians must have knowledge of protocols used to protect data integrity.

2.4 INFORMATION COMMUNICATION TECHNOLOGIES – CRYPTOGRAPHY/CRYPTOANALYSIS

Existing Course Cross Reference

Cisco Networking Academy Courses

Cisco Security Essentials

CCNA Security

Cisco Partner Courses

Security+ (CSSIA.ORG)

IoT and ICS Security Controls (CSSIA.ORG)

ICS and SCADA Security (CSSIA.ORG)

CISSP (CSSIA.ORG)

Curriculum Resources

Videos

YouTube.com - Cryptography

YouTube.com – Cryptography IPSEC VPN Router –to-Router

YouTube.com- IPsec over a GRE Tunnel

Web Links

Configuration Management: Best Practices White Paper

Textbooks

CompTIA Security+ All-in-One Exam Guide, Fourth Edition (Exam SY0-401) 4th Edition by Conklin, White, Williams, Cothren, & Davis
ISBN-13: 978-0071841245 ISBN-10: 0071841245

CompTIA Security+: Get Certified Get Ahead: SY0-401 Study Guide by Gibson
Oct 25, 2014, ISBN-10: 1939136024 ISBN-13: 978-1939136022

Assessment Resources

Labs

Security+ Lab 19 - General Cryptography Concepts

Security+ Lab 20 - Cryptography

Lab-8.7.1.1 – Configuring a Site to Site VPN Using Cisco IOS and CCP

Lab-8.7.1.2 – Configuring a Remote Access VPN Server and Client

Lab-8.7.1.3 – Optional Configuring a Remote Access VPN Server and Client

Quizzes/Exams

CCNA Security Course Exams

Quizlet.com

Cryptography

Cryptography and Symmetric Key Algorithms