Technical Committee and Assessors Panel

CREST Wireless Syllabus

Issued by	CREST Technical Committee and Assessors Panel
Document Reference	Wireless-Syl
Version Number	0.4
Status	Release
Issue Date	1/4/2012
Review Date	16/4/2013

Table of Contents

1 Introduction 4
2 Certification Examination Structure 4
3 Syllabus Structure 4
Appendix A: Computer Networking Fundamentals (Core Skill) 5
Appendix B: Virtualisation Technologies 9
Appendix C: Platform Security 10
Appendix D: Identification and Access Management 13
Appendix E: Cryptography 14
Appendix F: Applications 15
Appendix G: Governance 16
Appendix H: Security Methodologies 18
Appendix I: Security Vulnerabilities & Prevention Techniques 20

Version History

Version	Date	Authors	Status
0.1	3/2/2012	Technical Committee and Assessors Panel	Internal Draft
0.2	11/3/2012	Technical Committee and Assessors Panel	Internal Draft
0.3	1/4/2012	Technical Committee and Assessors Panel	Internal Release
0.4	16/4/2012	Technical Committee and Assessors Panel	Updated

Document Review

Reviewer	Position
Chair	Technical Committee / Assessors Panel
Chair	CREST Board

1 Introduction

The technical syllabus identifies at a high level the technical skills and knowledge that CREST expects candidates to possess for the Wireless Certification Examination.

- **CREST Certified Wireless Specialist (CCWS)**
- The (CCWS) Examination tests candidates' knowledge and expertise in a common set of core skills and knowledge for penetration testers performing wireless security reviews; success will confer the qualification (CCWS) to a an existing CREST Certified Consultant who has previously passed one of the CREST CCT level examinations.

2 Certification Examination Structure

CREST Certified Wireless Specialist (CCWS)

The examination structure is as follows

Multiple Choice Exam – 90 minutes (90 marks)

Practical Exam – 120 minutes (120 minutes)

Candidates are required to meet or exceed the 60% pass mark in both sections independently in order to pass the exam overall.

3 Syllabus Structure

The syllabus is divided into ten knowledge groups (Appendices A to I below) , each of which is subdivided into specific skill areas.

For each skill area, CREST has indicated where and how the area will be assessed and in which component (Written Multiple Choice or Practical).

Within the tables, the following acronyms apply:

CCWS	CESG Certified Wireless Specialist
MC	Written Multiple Choice
P	Practical

Appendix A: RF Concepts

ID	Area	Details	How Examined
			CCWS
A1	Radio Bands	Awareness of the different radio frequency bands and their allocations for use: • LF • HF • VHF • UHF • SHF • ISM	MC
A2	Propagation	Awareness of the characteristics of radio signals at various bands and frequencies and in particular an understanding of limitations of range at higher frequencies.	MC
A3	Bandwidth and Modulation	Understanding the concept of available bandwidth over a radio link and the types of modulation that can be used to carry both analogue and digital signals.	MC
A4	Safety	Awareness of the common safety issues associated with radio use and in particular those from high power transmitters.	MC
A5	Availability	Understanding of the fundamental restrictions of any broadcast media when considering availability requirements. Understanding the implications of shared / uncontrolled bands such as the ISM bands. Understanding the implications and uses of signal jammers.	MC
A6	Security Concepts	Understanding of the fundamental restrictions of any broadcast media when considering security requirements. Understanding of basic security technologies such as channel hopping and the implications these have for security testers.	MC P
A7	Tempest	Understanding the basic concepts of compromising emanations (Tempest) and common countermeasures.	MC

Appendix B: Legal Issues

ID	Area	Details	How Examined
			CCWS
B1	Interception	Understanding of the key legal issues related to authorised and unauthorised interception of radio signals.	MC
B2	Transmission	Understanding of the key legal issues related to authorised and unauthorised transmission of radio signals.	MC
B3	Airwave	Awareness of the spectrum used by blue light services within the UK for TETRA radio services.	MC
B4	Jamming	Understanding of the key legal issues related to the use of signal jamming equipment including the effects on location based services such as GPS.	MC

Appendix C: Cryptography

ID	Area	Details	How Examined
			CCWS
C1	Public Key Infrastructure (PKI)	An understanding of the concepts behind PKI solutions including certification generation, handling, recovery, non-repudiation, revocation and hierarchical chains of trust. An understanding of the concepts behind PKI solutions commonly implemented in wireless networking solutions.	MC P
C2	Storage Encryption	An understanding of the concepts behind storage encryption including the advantages and weakness of common solutions. Knowledge of common products that can be used to meet this requirement is also required. An understanding of the need to protect locally stored data and configuration files that may provide access to wireless networking solutions.	MC
C3	Virtual Private Networks	An awareness of the varying VPN types that could be encountered during a a wireless audit project: • Point to Point • Roaming remote user • Virtual Circuits / Tagging • IPSEC • PPTP • L2TP • SSL/TLS	MC
C4	Encryption and Hashing Algorithms	Awareness of common, publically available encryption algorithms and their common uses. Awareness of common, publically available hashing algorithms and their common uses.	MC

Appendix D: Bluetooth

ID	Area	Details	How Examined
			CCWS
D1	Technical Description	Understanding the existence and use of protocol and the capabilities offered by the protocol.	MC P
D2	Common Vulnerabilities	Understanding the history of the protocol and any inherent design vulnerabilities as well as an awareness of known public issues. This will include issues from poor product implementation (eg buffer overflows, weak encryption) as well as poor user/admin implementation (weak passwords).	MC P
D3	Common Uses	Awareness of common uses of the protocol and an understanding of how these may impose physical or logical restrictions on the level of security available.	MC P

Appendix E: RFID

ID	Skill	Details	How Examined
			CCWS
E1	Technical Description	Understanding the existence and use of protocol and the capabilities offered by the protocol.	MC P
E2	Common Vulnerabilities	Understanding the history of the protocol and any inherent design vulnerabilities as well as an awareness of known public issues. This will include issues from poor product implementation (eg buffer overflows, weak encryption) as well as poor user/admin implementation (weak passwords).	MC P
E3	Common Uses	Awareness of common uses of the protocol and an understanding of how these may impose physical or logical restrictions on the level of security available.	MC P

Appendix F: 802.11 Networking

ID	Skill	Details	How Examined
			CCWS
F1	Technical Description	Understanding the existence and use of protocol and the capabilities offered by the protocol.	MC P
F2	Common Vulnerabilities	Understanding the history of the protocol and any inherent design vulnerabilities as well as an awareness of known public issues. This will include issues from poor product implementation (eg buffer overflows, weak encryption) as well as poor user/admin implementation (weak passwords).	MC P
F3	Common Uses	Awareness of common uses of the protocol and an understanding of how these may impose physical or logical restrictions on the level of security available.	MC P

Appendix G: Wireless Technologies

ID	Skill	Details	How Examined
			CCWS
G1	Zigbee	Understanding the existence and use of protocol and the capabilities offered by the protocol. Awareness of common implementations and vulnerabilities.	MC
G2	Microwave	Understanding the existence and use of protocol and the capabilities offered by the protocol. Awareness of common implementations and vulnerabilities.	MC
G3	Optical	Understanding the existence and use of protocol and the capabilities offered by the protocol. Awareness of common implementations and vulnerabilities.	MC
G4	GSM	Understanding the existence and use of protocol and the capabilities offered by the protocol. Awareness of common implementations and vulnerabilities.	MC
G5	GPRS/EDGE	Understanding the existence and use of protocol and the capabilities offered by the protocol. Awareness of common implementations and vulnerabilities.	MC
G6	3G/HSPA	Understanding the existence and use of protocol and the capabilities offered by the protocol. Awareness of common implementations and vulnerabilities.	MC
G7	TETRA	Understanding the existence and use of protocol and the capabilities offered by the protocol. Awareness of common implementations and vulnerabilities.	MC

Appendix H: RF Hardware

ID	Skill	Details	How Examined
			CCWS
H1	Transmitters	Understanding the existence and role in a radio communications system. Awareness of common implementations and potential vulnerabilities.	MC
H2	Receivers	Understanding the existence and role in a radio communications system. Awareness of common implementations and potential vulnerabilities.	MC
H3	Antenna	Understanding the existence and role in a radio communications system. Awareness of common implementations and potential vulnerabilities.	MC
H4	Cabling	Understanding the existence and role in a radio communications system. Awareness of common implementations and potential vulnerabilities.	MC
H5	Amplifiers	Understanding the existence and role in a radio communications system. Awareness of common implementations and potential vulnerabilities.	MC
H6	Software Radio	Understanding the existence and uses of a software based radio communications system. Awareness of common implementations and potential limitations.	MC
H7	Test Equipment	Understanding the existence and uses of RF test equipment and an awareness of common implementations and potential limitations.	MC