An Alphabetical Version of the CyBOK's Knowledge Areas Indicative Material Version 1.1

Lata Nautiyal | University of Bristol

Awais Rashid | University of Bristol

July 2021
http://www.cybok.org

COPYRIGHT

The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at contact@cybok.org to let the project know how they are using CyBOK.

CHANGE LOG

Version date	Version number	Changes made
July 2021	1.1	Updated in line with CyBOK version 1.1
June 2020	1.0	

INTRODUCTION

This document provides an alphabetical version of the **CyBOK's knowledge areas indicative material** from the NCSC's degree certification documents. This document is aimed to be part of a set of guidelines for higher education institutions for their applications for NCSC degree certification.

The overall aim of this document is to support applicants map the content of taught degree modules onto CyBOK in order to complete the relevant tables in their certification application.

For the purposes of the NCSC certification programme each of the **CyBOK Knowledge Trees** is represented as follows:

- The nodes directly under the root node are referred to as **Topics**. Thus, for example, the Risk Management and Governance (RMG) Knowledge Area has the following Topics: **Risk Definitions, Risk Governance, Risk Assessment and Management Principles, Business Continuity: Incident Response and Recovery Planning**
- For a given Topic, Indicative Material is defined as the nodes in the **Knowledge Tree** one layer further down from the **Topic**. Thus, for example, the Indicative Material for the Risk Definitions Topic is: **Risk Assessment, Risk Management and Levels of Perceived Risk.**

It is often the case that course materials use terms from Indicative Material to describe that the course will cover. The purpose of this document is to help those applying for degree certification, as well as others, by providing an easy-to-use, alphabetical reference that maps from Indicative Material terms to **CyBOK Knowledge Areas**.

The following acronyms shown in red are used to refer to the Knowledge Areas:". The acronyms are expanded below:

Acronym	Knowledge Area
AAA	Authentication, Authorisation & Accountability
AB	Adversarial Behaviours
AC	Applied Cryptography
C	Cryptography
CI	CyBOK Introduction
CPS	Cyber-Physical Systems Security
DSS	Distributed Systems Security
F	Forensics
FMS	Formal Methods for Security
HF	Human Factors
HS	Hardware Security
LR	Law & Regulation
MAT	Malware & Attack Technology
NS	Network Security
OSV	Operating Systems & Virtualisation
PLT	Physical Layer & Telecommunications Security
POR	Privacy & Online Rights
RMG	Risk Management & Governance
SOIM	Security Operations & Incident Management
SS	Software Security
SSL	Secure Software Lifecycle
WAM	Web & Mobile Security

Note :-

This document is just a guide. We do not claim that it is complete, nor do we guarantee that the **Knowledge Areas** we refer to discuss the **Topics** or **Indicative Material** in detail, just that if they are discussed in CyBOK this is where they will most likely be found. The document should, therefore, not be treated as a definitive mechanism or a guarantee for a successful certification application. It provides a direction for applicants undertaking the mapping of their programmes to the certification requirements. Applicants are best placed to decide on the final mappings and the certification panel's decisions are based on broader criteria than those covered in this document.

INDICATIVE MATERIAL	TOPIC	CyBOK KA
A		
ACCESS CONTROL	AUTHORISATION	AAA
ACCESS/ADMISSION CONTROL AND ID MANAGEMENT	CLASSES OF VULNERABILITIES AND THREATS	DSS
ADDRESSING THE CHALLENGES	CONSUMING CRYPTOGRAPHY	AC
ADMISSION INTO EVIDENCE OF ELECTRONIC DOCUMENTS	DEMATERIALISATION OF DOCUMENTS AND ELECTRONIC TRUST SERVICES	LR
AES	SCHEMES	C
AFFILIATE PROGRAMMES	ELEMENTS OF A MALICIOUS OPERATION	AB
AGILE AND DEVOPS	ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE	SSL
AIR TRAFFIC COMMUNICATIONS NETWORKS	PHYSICAL LAYER SECURITY OF SELECTED COMMUNICATIONS TECHNOLOGIES	PLT
ALERT CORRELATION	PLAN: SECURITY INFORMATION AND EVENT MANAGEMENT	SOIM
ANALYSIS ENVIRONMENTS	MALWARE ANALYSIS	MAT
ANALYSIS TECHNIQUES	MALWARE ANALYSIS	MAT
ANOMALY DETECTION	ANALYSE: ANALYSIS METHODS	SOIM
ANOMALY DETECTION	OS HARDENING	OSV
ANTI-ANALYSIS AND EVASION TECHNIQUES	MALWARE ANALYSIS	MAT
API ATTACKS ON SECURITY HARDWARE	HARDWARE	FMS
API DESIGN	PREVENTION OF VULNERABILITIES	SS
API DESIGN FOR CRYPTOGRAPHIC LIBRARIES	CRYPTOGRAPHIC IMPLEMENTATION	AC
API VULNERABILITIES	CATEGORIES OF VULNERABILITIES	SS
APPIFICATION	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
APPLICATION LOGS: WEB SERVER LOGS AND FILES	MONITOR: DATA SOURCES	SOIM
APPLICATION STORES	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
APPLYING LAW TO CYBERSPACE AND INFORMATION TECHNOLOGIES	INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH	LR
ARCHITECTURAL PRINCIPLES	FUNDAMENTAL CONCEPTS	SOIM
ARM TRUSTZONE	HARDWARE SUPPORT FOR SOFTWARE SECURITY	HS
ARTIFACTS AND FRAGMENTS	MAIN MEMORY FORENSICS	F
ASSESSMENT CRITERIA	USABLE SECURITY	HF
ATTACK DETECTION	MALWARE DETECTION	MAT
ATTACK ON CONFIDENTIALITY, INTEGRITY, AVAILABILITY	MALICIOUS ACTIVITIES BY MALWARE	MAT
ATTACK SURFACE	ATTACKER MODEL	OSV
ATTACK TREES	MODELS	AB
ATTACK TYPES	ATTACKING P2P SYSTEMS	DSS
ATTACKER MODELS	SECURITY GOALS AND ATTACKER MODELS	NS
ATTACKS	SIDE CHANNEL ATTACKS AND FAULT ATTACKS	HS
ATTACKS AND THEIR MITIGATION	ATTACKING P2P SYSTEMS	DSS
ATTACKS ON PHYSICAL LAYER IDENTIFICATION	IDENTIFICATION	PLT
ATTRIBUTING ACTION TO A STATE UNDER INTERNATIONAL LAW	PUBLIC INTERNATIONAL LAW	LR
ATTRIBUTION	MALWARE RESPONSE	MAT
ATTRIBUTION	MODELS	AB
AUDIT-BASED TRANSPARENCY	TRANSPARENCY	POR
AUTHENTICATED ENCRYPTION (AE) SCHEMES	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
AUTHENTICATION	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
AUTHENTICATION AND IDENTIFICATION	PRIMITIVES FOR ISOLATION AND MEDIATION	OSV

INDICATIVE MATERIAL	TOPIC	CyBOK KA
AUTHENTICATION IN DISTRIBUTED SYSTEMS	AUTHENTICATION	AAA
AUTHENTICATION PROTOCOLS	STANDARD PROTOCOLS	C
AUTOMATED SOFTWARE DIVERSITY	MITIGATING EXPLOITATION	SS
B		
BASIC SECURITY DEFINITIONS	CRYPTOGRAPHIC SECURITY MODELS	C
BLIND SIGNATURES	PUBLIC-KEY SCHEMES WITH SPECIAL PROPERTIES	C
BLOCK CIPHERS	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
BLOCK DEVICE ANALYSIS	OPERATING SYSTEM ANALYSIS	F
BOARD LEVEL SECURITY	HARDWARE DESIGN PROCESS	HS
BREACH OF CONTRACT AND REMEDIES	CONTRACT	LR
BREACHES ARE COSTLY	MOTIVATIONS FOR SECURE SOFTWARE LIFECYCLE	SSL
BSIMM	ASSESS THE SECURE SOFTWARE LIFECYCLE	SSL
BUS NETWORKS	NETWORKING APPLICATIONS	NS
C		
CAPABILITIES	PRIMITIVES FOR ISOLATION AND MEDIATION	OSV
CASE STUDY: E.G., WEB BROWSERS	APPLICATION FORENSICS	F
CATALOGUE OF INTELLECTUAL PROPERTY RIGHTS	INTELLECTUAL PROPERTY	LR
CELL LEFT DELIBERATELY BLANK	THE CRYPTOGRAPHIC TRIUMVIRATE	AC
CELL LEFT DELIBERATELY BLANKS	FUTURE OF APPLIED CRYPTOGRAPHY	AC
CELLULAR NETWORKS	PHYSICAL LAYER SECURITY OF SELECTED COMMUNICATIONS TECHNOLOGIES	PLT
CENSORSHIP RESISTANCE AND FREEDOM OF SPEECH	PRIVACY TECHNOLOGIES AND DEMOCRATIC VALUES	POR
CHALLENGES OF LIVE FORENSICS	MAIN MEMORY FORENSICS	F
CHARACTERISTICS	CYBER-PHYSICAL SYSTEMS	CPS
CIRCUIT LEVEL TECHNIQUES	HARDWARE DESIGN PROCESS	HS
CIVIL LAW	INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH	LR
CLASSES OF DISRUPTIONS	COORDINATION CLASSES AND ATTACKABILITY	DSS
CLASSIFICATION OF JAMMERS	JAMMING AND JAMMING-RESILIENT COMMUNICATIONS	PLT
CLICKJACKING	CLIENT-SIDE VULNERABILITIES AND MITIGATIONS	WAM
CLIENT-SIDE STORAGE	CLIENT-SIDE VULNERABILITIES AND MITIGATIONS	WAM
CLOUD AND DATA CENTRE SECURITY	OTHER NETWORK SECURITY TOPICS	NS
CLOUD COMPUTING	ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE	SSL
CODE AND DATA INTEGRITY CHECKS	OS HARDENING	OSV
CODES OF CONDUCT	ETHICS	LR
CODING PRACTICES	PREVENTION OF VULNERABILITIES	SS
COMMON CRITERIA	ASSESS THE SECURE SOFTWARE LIFECYCLE	SSL
COMMON CRITERIA AND EMVCO	MEASURING HARDWARE SECURITY	HS
COMPLETENESS	DETECTION OF VULNERABILITIES	SS
COMPONENT VERSUS SYSTEMS PERSPECTIVES	RISK ASSESSMENT AND MANAGEMENT PRINCIPLES	RMG
COMPROMISING EMANATIONS	COMPROMISING EMANATIONS AND SENSOR SPOOFING	PLT
COMPUTATIONAL METHODS	CRYPTOGRAPHIC PROTOCOLS	FMS
CONCEPTUAL MODELS	DEFINITIONS AND CONCEPTUAL MODELS	F
CONFLICT OF LAW - CONTRACTS	CONTRACT	LR
CONFLICT OF LAW – ELECTRONIC SIGNATURES AND TRUST SERVICES	DEMATERIALISATION OF DOCUMENTS AND ELECTRONIC TRUST SERVICES	LR
CONNECTED NETWORKS AND THE INTERNET	NETWORKING APPLICATIONS	NS

INDICATIVE MATERIAL	TOPIC	CyBOK KA
CONTACT TRACING À LA DP-3T	APPLIED CRYPTOGRAPHY IN ACTION	AC
CONTRIBUTION OF SIEM TO ANALYSIS AND DETECTION	ANALYSE: ANALYSIS METHODS	SOIM
CONTROL-FLOW RESTRICTIONS	OS HARDENING	OSV
COOKIES	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
COORDINATED CLUSTERING ACROSS DISTRIBUTED RESOURCES AND SERVICES	CLASSES OF DISTRIBUTED SYSTEMS	DSS
COORDINATED SPREAD SPECTRUM TECHNIQUES	JAMMING AND JAMMING-RESILIENT COMMUNICATIONS	PLT
COORDINATION PRINCIPLES	COORDINATED RESOURCE CLUSTERING	DSS
CORE CONCEPTS	ACCESS CONTROL IN DISTRIBUTED SYSTEMS	AAA
CORE REGULATORY PRINCIPLES	DATA PROTECTION	LR
COUNTERMEASURES	SIDE CHANNEL ATTACKS AND FAULT ATTACKS	HS
COUNTERMEASURES	JAMMING AND JAMMING-RESILIENT COMMUNICATIONS	PLT
CRIMES AGAINST INFORMATION SYSTEMS	COMPUTER CRIME	LR
CRIMINAL LAW	INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH	LR
CROSS-BORDER CRIMINAL INVESTIGATION	PUBLIC INTERNATIONAL LAW	LR
CROSS-BORDER REGULATIONS	OTHER NETWORK SECURITY TOPICS	NS
CRYPTOGRAPHIC ALGORITHMS AT RTL LEVEL	HARDWARE DESIGN FOR CRYPTOGRAPHIC ALGORITHMS	HS
CRYPTOGRAPHIC DIVERSITY	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
CRYPTOGRAPHIC HASHING	CLOUD FORENSICS	F
CRYPTOGRAPHIC LIBRARIES	SOFTWARE AND LARGE SCALE SYSTEMS	FMS
CRYPTOGRAPHIC LIBRARIES	CRYPTOGRAPHIC IMPLEMENTATION	AC
CRYPTOGRAPHY AND ACCESS CONTROL	ACCESS CONTROL IN DISTRIBUTED SYSTEMS	AAA
CUSTOMERS DON’T APPLY PATCHES	MOTIVATIONS FOR SECURE SOFTWARE LIFECYCLE	SSL
CVES AND CWES	CATEGORIES OF VULNERABILITIES	SS
CYBER CONFLICT	POLICY AND POLITICAL ASPECTS	CPS
CYBER DOMAIN	DEFINITIONS AND CONCEPTUAL MODELS	F
CYBER ESPIONAGE IN PEACETIME	PUBLIC INTERNATIONAL LAW	LR
CYBER KILL CHAIN	MALICIOUS ACTIVITIES BY MALWARE	MAT
CYBER SECURITY KNOWLEDGE MANAGEMENT	KNOWLEDGE: INTELLIGENCE AND ANALYSIS	SOIM
CYBER-DEPENDENT ORGANISED CRIME	CHARACTERISATION OF ADVERSARIES	AB
CYBER-ENABLED CRIME VS CYBER-DEPENDENT CRIME	CHARACTERISATION OF ADVERSARIES	AB
CYBER-ENABLED ORGANISED CRIME	CHARACTERISATION OF ADVERSARIES	AB
CYBER-THREAT INTELLIGENCE	KNOWLEDGE: INTELLIGENCE AND ANALYSIS	SOIM
D		
DATA ACQUISITION	OPERATING SYSTEM ANALYSIS	F
DATA COLLECTION	PLAN: SECURITY INFORMATION AND EVENT MANAGEMENT	SOIM
DATA CONFIDENTIALITY	CONFIDENTIALITY	POR
DATA RECOVERY AND FILE CONTENT CARVING	OPERATING SYSTEM ANALYSIS	F
DATA SECURITY	CLASSES OF VULNERABILITIES AND THREATS	DSS
DATA SOVEREIGNTY	JURISDICTION	LR
DATA TRANSPORTATION	CLASSES OF VULNERABILITIES AND THREATS	DSS
DATABASES	RELATED AREAS	OSV
DE MINIMIS EXCEPTIONS TO CRIMES AGAINST INFORMATION SYSTEMS	COMPUTER CRIME	LR

INDICATIVE MATERIAL	TOPIC	CyBOK KA
DECENTRALISED POINT-TO-POINT INTERACTIONS ACROSS DISTRIBUTED ENTITIES WITHOUT A CENTRALISED COORDINATION SERVICE	CLASSES OF DISTRIBUTED SYSTEMS	DSS
DEFENCES	CRYPTOGRAPHIC IMPLEMENTATION	AC
DEFINITION OF CYBER SECURITY	FOUNDATIONAL CONCEPTS	CI
DEFINITIONS	DEFINITIONS AND CONCEPTUAL MODELS	F
DELAY TOLERANT NETWORKS AND AD-HOC SENSORS NETWORKS	OTHER NETWORK SECURITY TOPICS	NS
DES	SCHEMES	C
DESIGN AND FABRICATION OF SILICON INTEGRATED CIRCUITS	HARDWARE DESIGN PROCESS	HS
DESIGN CHOICES	ROLE OF OPERATING SYSTEMS	OSV
DESIGN PROCESS	HARDWARE DESIGN FOR CRYPTOGRAPHIC ALGORITHMS	HS
DETECTING ATTACKS	CROSS CUTTING SECURITY	CPS
DEVELOPMENT OF STANDARDISED CRYPTOGRAPHY	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
DEVICE CAPABILITIES AND LIMITATIONS	FITTING THE TASK TO THE HUMAN	HF
DEVICE FINGERPRINTS	IDENTIFICATION	PLT
DEVICE UNDER IDENTIFICATION	IDENTIFICATION	PLT
DIFFIE-HELLMAN KEY EXCHANGE	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
DIGITAL (FORENSIC) TRACE	DEFINITIONS AND CONCEPTUAL MODELS	F
DIGITAL SIGNATURES	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
DIMENSIONS	MALWARE TAXONOMY	MAT
DISRUPTING MALWARE OPERATIONS	MALWARE RESPONSE	MAT
DISTANCE BOUNDING PROTOCOLS	DISTANCE BOUNDING AND SECURE POSITIONING	PLT
DISTANCE MEASUREMENT TECHNIQUES	DISTANCE BOUNDING AND SECURE POSITIONING	PLT
DISTRIBUTED LOGS	ACCOUNTABILITY	AAA
DOS COUNTERMEASURES	NETWORK SECURITY TOOLS	NS
DSA	SCHEMES	C
DYNAMIC DETECTION	DETECTION OF VULNERABILITIES	SS
E		
ECOMMERCE	ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE	SSL
EFFECTS OF CONTRACT ON NON-CONTRACTING PARTIES	CONTRACT	LR
ELECTRIC POWER GRIDS	CYBER-PHYSICAL SYSTEMS DOMAINS	CPS
ELECTRONIC SIGNATURES AND IDENTITY TRUST SERVICES	DEMATERIALISATION OF DOCUMENTS AND ELECTRONIC TRUST SERVICES	LR
ELEMENTS OF RISK	RISK ASSESSMENT AND MANAGEMENT PRINCIPLES	RMG
EMPLOYEES	STAKEHOLDER ENGAGEMENT	HF
ENACTING SECURITY POLICY	RISK GOVERNANCE	RMG
ENCOURAGING SECURITY STANDARDS VIA CONTRACT	CONTRACT	LR
ENFORCEMENT – REMEDIES	INTELLECTUAL PROPERTY	LR
ENFORCEMENT AND PENALTIES	DATA PROTECTION	LR
ENFORCEMENT JURISDICTION	JURISDICTION	LR
ENFORCEMENT OF PRIVACY LAWS	PRIVACY LAWS IN GENERAL AND ELECTRONIC INTERCEPTION	LR
ENFORCING ACCESS CONTROL	AUTHORISATION	AAA
ENVIRONMENTAL CRIMINOLOGY	MODELS	AB
ERRONEOUS EXECUTION	PREVENTION OF VULNERABILITIES	SS
EVASION AND COUNTERMEASURES	MALWARE DETECTION	MAT

INDICATIVE MATERIAL	TOPIC	CyBOK KA
EVIDENCE AND PROOF	INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH	LR
F		
FACETS OF AUTHENTICATION	AUTHENTICATION	AAA
FAILURES AND INCIDENTS	FOUNDATIONAL CONCEPTS	CI
FEAR UNCERTAINTY AND DOUBT	POSITIVE SECURITY	HF
FEDERATED ACCESS CONTROL	ACCESS CONTROL IN DISTRIBUTED SYSTEMS	AAA
FEEDBACK-BASED TRANSPARENCY	TRANSPARENCY	POR
FILE INFORMATION	MAIN MEMORY FORENSICS	F
FILESYSTEM ANALYSIS	OPERATING SYSTEM ANALYSIS	F
FIPS 140-2	MEASURING HARDWARE SECURITY	HS
FIREWALLING	NETWORK SECURITY TOOLS	NS
FLOW OF CAPITAL	MODELS	AB
FOLLOW UP: POST INCIDENT ACTIVITIES	HUMAN FACTORS: INCIDENT MANAGEMENT	SOIM
FORENSIC SCIENCE	DEFINITIONS AND CONCEPTUAL MODELS	F
FORENSICS CHALLENGES	CLOUD FORENSICS	F
FORMAL VERIFICATION	OS HARDENING	OSV
FREQUENT SOFTWARE UPDATES	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
FRIENDLY JAMMING	SCHEMES FOR CONFIDENTIALITY, INTEGRITY AND ACCESS CONTROL	PLT
FROM SCHEMES TO PROTOCOLS	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
FULL-STACK VERIFICATION	SOFTWARE AND LARGE SCALE SYSTEMS	FMS
FULLY DISTRIBUTED NETWORKS: DHTS AND UNSTRUCTURED P2P NETWORKS	NETWORKING APPLICATIONS	NS
FULLY HOMOMORPHIC ENCRYPTION	PUBLIC-KEY SCHEMES WITH SPECIAL PROPERTIES	C
FUNCTIONAL ELEMENTS	ATTACKING P2P SYSTEMS	DSS
G		
GNSS SECURITY AND SPOOFING ATTACKS	PHYSICAL LAYER SECURITY OF SELECTED COMMUNICATIONS TECHNOLOGIES	PLT
GOALS	PRIVACY ENGINEERING	POR
GOALS AND TASKS	FITTING THE TASK TO THE HUMAN	HF
GOVERNANCE MODELS	RISK GOVERNANCE	RMG
GROUP SIGNATURES	PUBLIC-KEY SCHEMES WITH SPECIAL PROPERTIES	C
GRSECURITY	EMBRACING SECURITY	OSV
H		
HACKTIVISTS	CHARACTERISATION OF ADVERSARIES	AB
HANDLE: ACTUAL INCIDENT RESPONSE	HUMAN FACTORS: INCIDENT MANAGEMENT	SOIM
HARD PROBLEMS	CRYPTOGRAPHIC SECURITY MODELS	C
HARDWARE DESIGN PROCESS	HARDWARE DESIGN CYCLE	HS
HARDWARE SECURITY MODULE (HSM)	SECURE PLATFORMS	HS
HARDWARE VERIFICATION	HARDWARE	FMS
HASH FUNCTIONS	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
HIERARCHICAL P2P PROTOCOLS	DECENTRALISED P2P MODELS	DSS
HOLISTIC APPROACHES TO LEGAL RISK ANALYSIS	INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH	LR
HONEYPOTS AND HONEYNETS	KNOWLEDGE: INTELLIGENCE AND ANALYSIS	SOIM
HUMAN BIASES	FITTING THE TASK TO THE HUMAN	HF
HUMAN CAPABILITIES AND LIMITATIONS	FITTING THE TASK TO THE HUMAN	HF
HUMAN FACTORS AND RISK COMMUNICATION	RISK GOVERNANCE	RMG
HUMAN SERVICES	ELEMENTS OF A MALICIOUS OPERATION	AB

INDICATIVE MATERIAL	TOPIC	CyBOK KA
HYBRID P2P PROTOCOLS	DECENTRALISED P2P MODELS	DSS
I		
IBM 4578 SECURE COPROCESSOR	HARDWARE SUPPORT FOR SOFTWARE SECURITY	HS
IDENTIFICATION SIGNALS	IDENTIFICATION	PLT
IDENTIFYING THE ANALYSIS ENVIRONMENT	MALWARE ANALYSIS	MAT
IDENTIFYING THE PRESENCE OF MALWARE	MALWARE DETECTION	MAT
IDENTITY MANAGEMENT	AUTHENTICATION	AAA
IDENTITY-BASED ENCRYPTION	PUBLIC-KEY SCHEMES WITH SPECIAL PROPERTIES	C
IMPLEMENTATION CHALLENGES	CRYPTOGRAPHIC IMPLEMENTATION	AC
INADEQUACY OF TRADITIONAL DEVELOPMENT METHODS	MOTIVATION	FMS
INCENTIVES AND REGULATION	POLICY AND POLITICAL ASPECTS	CPS
INDUSTRIAL CONTROL SYSTEMS	CYBER-PHYSICAL SYSTEMS DOMAINS	CPS
INDUSTRY PRACTICES AND STANDARDS	POLICY AND POLITICAL ASPECTS	CPS
INDUSTRY-SPECIFIC REGULATIONS	OTHER REGULATORY MATTERS	LR
INFECTION VECTORS	ELEMENTS OF A MALICIOUS OPERATION	AB
INFORMATION FLOW	PREVENTION OF VULNERABILITIES	SS
INFORMATION FLOW CONTROL	SOFTWARE AND LARGE SCALE SYSTEMS	FMS
INFORMATION HARDENING	OS HARDENING	OSV
INFRASTRUCTURE	ELEMENTS OF A MALICIOUS OPERATION	AB
INJECTION VULNERABILITIES	SERVER-SIDE VULNERABILITIES AND MITIGATIONS	WAM
INTERACTION CONTEXT	FITTING THE TASK TO THE HUMAN	HF
INTERCEPTION BY A STATE	PRIVACY LAWS IN GENERAL AND ELECTRONIC INTERCEPTION	LR
INTERCEPTION BY PERSONS OTHER THAN STATE	PRIVACY LAWS IN GENERAL AND ELECTRONIC INTERCEPTION	LR
INTERNATIONAL NORMS	PRIVACY LAWS IN GENERAL AND ELECTRONIC INTERCEPTION	LR
INTERNATIONAL TREATMENT AND CONFLICT OF LAW	INTELLECTUAL PROPERTY	LR
INTERPERSONAL CRIMES	CHARACTERISATION OF ADVERSARIES	AB
INTRUSION DETECTION AND PREVENTION SYSTEMS	NETWORK SECURITY TOOLS	NS
INTRUSION PREVENTION SYSTEMS	EXECUTE: MITIGATION AND COUNTERMEASURES	SOIM
INVESTIGATION AND PREVENTION OF CRIME	DATA PROTECTION	LR
IOT	ROLE OF OPERATING SYSTEMS	OSV
IOT	ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE	SSL
IOT	CYBER-PHYSICAL SYSTEMS DOMAINS	CPS
ISO/IEC 27035	BUSINESS CONTINUITY: INCIDENT RESPONSE AND RECOVERY PLANNING	RMG
ISOLATION	ROLE OF OPERATING SYSTEMS	OSV
K		
KERBEROS	SCHEMES	C
KEY AGREEMENT PROTOCOLS	STANDARD PROTOCOLS	C
KEY DERIVATION	KEY MANAGEMENT	AC
KEY ESTABLISHMENT BASED ON CHANNEL RECIPROCITY	SCHEMES FOR CONFIDENTIALITY, INTEGRITY AND ACCESS CONTROL	PLT
KEY GENERATION	KEY MANAGEMENT	AC
KEY SIZES	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
KEY STORAGE	KEY MANAGEMENT	AC

INDICATIVE MATERIAL	TOPIC	CyBOK KA
KEY TRANSPORTATION	KEY MANAGEMENT	AC
KILL CHAINS	MODELS	AB
KINDS	MALWARE TAXONOMY	MAT
L		
LANGUAGE DESIGN AND TYPE SYSTEMS	PREVENTION OF VULNERABILITIES	SS
LATENT DESIGN CONDITIONS	PRINCIPLES	CI
LATENT USABILITY FAILURES IN SYSTEMS-OF-SYSTEMS	HUMAN ERROR	HF
LEGAL CONCERNS AND THE DAUBERT STANDARD	DEFINITIONS AND CONCEPTUAL MODELS	F
LEVELS OF PERCEIVED RISK	RISK DEFINITIONS	RMG
LIABILITY AND COURTS	INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH	LR
LIGHTWEIGHT SOLUTIONS	HARDWARE SUPPORT FOR SOFTWARE SECURITY	HS
LIMITATIONS	MOTIVATION	FMS
LIMITATIONS OF LIABILITY AND EXCLUSIONS OF LIABILITY	CONTRACT	LR
LIMITING PRIVILEGES	MITIGATING EXPLOITATION	SS
LINEARLY HOMOMORPHIC ENCRYPTION	PUBLIC-KEY SCHEMES WITH SPECIAL PROPERTIES	C
LOCAL AREA NETWORKS (LANS)	NETWORKING APPLICATIONS	NS
LOGICS AND SPECIFICATION LANGUAGES	FOUNDATIONS, METHODS AND TOOLS	FMS
LONG-TERM MEMORY	FITTING THE TASK TO THE HUMAN	HF
LOW-END DEVICES AND IOT	PRIMITIVES FOR ISOLATION AND MEDIATION	OSV
LOW-LEVEL CODE	SOFTWARE AND LARGE SCALE SYSTEMS	FMS
LPI AND COVERT COMMUNICATION	SCHEMES FOR CONFIDENTIALITY, INTEGRITY AND ACCESS CONTROL	PLT
M		
MACHINE LEARNING	ANALYSE: ANALYSIS METHODS	SOIM
MAKING CRYPTOGRAPHY INVISIBLE	CONSUMING CRYPTOGRAPHY	AC
MANAGING PUBLIC KEYS AND PUBLIC KEY INFRASTRUCTURE	KEY MANAGEMENT	AC
MATTERS CLASSIFIED AS SECRET BY A STATE	OTHER REGULATORY MATTERS	LR
MEDIATION	ROLE OF OPERATING SYSTEMS	OSV
MEDICAL DEVICES	CYBER-PHYSICAL SYSTEMS DOMAINS	CPS
MEMORY MANAGEMENT VULNERABILITIES	CATEGORIES OF VULNERABILITIES	SS
MEMORY PROTECTION AND ADDRESS SPACES	PRIMITIVES FOR ISOLATION AND MEDIATION	OSV
MENTAL MODELS OF CYBER RISKS AND DEFENCES	AWARENESS AND EDUCATION	HF
MENTAL MODELS OF SECURITY	USABLE SECURITY	HF
MESSAGE AUTHENTICATION CODE (MAC) SCHEMES	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
METADATA CONFIDENTIALITY	CONFIDENTIALITY	POR
MICROSOFT SDL	PRESCRIPTIVE PROCESSES	SSL
MIMO-SUPPORTED APPROACHES	SCHEMES FOR CONFIDENTIALITY, INTEGRITY AND ACCESS CONTROL	PLT
MISUSE DETECTION	ANALYSE: ANALYSIS METHODS	SOIM
MITIGATING ATTACKS	CROSS CUTTING SECURITY	CPS
MOBILE	ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE	SSL
MODERN HARDWARE EXTENSIONS FOR MEMORY PROTECTION	PRIMITIVES FOR ISOLATION AND MEDIATION	OSV

INDICATIVE MATERIAL	TOPIC	CyBOK KA
MULTICS	PRIMITIVES FOR ISOLATION AND MEDIATION	OSV
N		
NATURE OF LAW AND LEGAL ANALYSIS	INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH	LR
NCSC GUIDANCE	BUSINESS CONTINUITY: INCIDENT RESPONSE AND RECOVERY PLANNING	RMG
NEEDS OF SPECIFIC GROUPS	FITTING THE TASK TO THE HUMAN	HF
NETWORK ACCESS CONTROL	NETWORK SECURITY TOOLS	NS
NETWORK AGGREGATES: NETFLOW	MONITOR: DATA SOURCES	SOIM
NETWORK CONNECTIONS	MAIN MEMORY FORENSICS	F
NETWORK COVERT CHANNELS	OTHER NETWORK SECURITY TOPICS	NS
NETWORK INFRASTRUCTURE INFORMATION	MONITOR: DATA SOURCES	SOIM
NETWORK SECURITY MONITORING	NETWORK SECURITY TOOLS	NS
NETWORK TRAFFIC	MONITOR: DATA SOURCES	SOIM
NETWORKING INFRASTRUCTURE SECURITY	OTHER NETWORK SECURITY TOPICS	NS
NEW APPROACHES	AWARENESS AND EDUCATION	HF
NEWER PRINCIPLES	OS SECURITY PRINCIPLES	OSV
NFC	PHYSICAL LAYER SECURITY OF SELECTED COMMUNICATIONS TECHNOLOGIES	PLT
NIST PRINCIPLES	PRINCIPLES	CI
O		
OBJECTIVES	HARDWARE SUPPORT FOR SOFTWARE SECURITY	HS
OBJECTIVES OF CYBER SECURITY	FOUNDATIONAL CONCEPTS	CI
OBLIGATIONS OWED TO A CLIENT	ETHICS	LR
OBLIVIOUS TRANSFER	ADVANCED PROTOCOLS	C
ON-LINE CONTRACTS	CONTRACT	LR
ONE-TIME PAD	INFORMATION-THEORETICALLY SECURE CONSTRUCTIONS	C
OPERATING SYSTEMS	SOFTWARE AND LARGE SCALE SYSTEMS	FMS
ORIGIN-BASED POLICIES	ACCESS CONTROL IN DISTRIBUTED SYSTEMS	AAA
P		
PARTITIONING	OS HARDENING	OSV
PASSWORD BASED KEY DERIVATION	KEY MANAGEMENT	AC
PASSWORDS AND ALTERNATIVES	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
PATCHING CAN INTRODUCE VULNERABILITIES	MOTIVATIONS FOR SECURE SOFTWARE LIFECYCLE	SSL
PAX TEAM	EMBRACING SECURITY	OSV
PAYMENT METHODS	ELEMENTS OF A MALICIOUS OPERATION	AB
PAYMENT NETWORKS	OTHER NETWORK SECURITY TOPICS	NS
PEOPLE ARE NOT THE WEAKEST LINK	POSITIVE SECURITY	HF
PERMISSION DIALOG BASED ACCESS CONTROL	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
PERSONAL DATA BREACH NOTIFICATION	DATA PROTECTION	LR
PHISHING	CLIENT-SIDE VULNERABILITIES AND MITIGATIONS	WAM
PHYSICAL ACCESS AND SECURE DELETION	PRIMITIVES FOR ISOLATION AND MEDIATION	OSV
PHYSICAL ATTACKS	CLIENT-SIDE VULNERABILITIES AND MITIGATIONS	WAM
PHYSICAL LAYER ATTACKS ON SECURE DISTANCE MEASUREMENT	DISTANCE BOUNDING AND SECURE POSITIONING	PLT
PHYSICAL LAYER SECURITY	OTHER NETWORK SECURITY TOPICS	NS

INDICATIVE MATERIAL	TOPIC	CyBOK KA
PHYSICALLY UNCLONABLE FUNCTIONS (PUFS)	ENTROPY GENERATING BUILDING BLOCKS	HS
PKCS	SCHEMES	C
POLICY ANALYSIS	CONFIGURATION	FMS
POST-QUANTUM CRYPTOGRAPHY	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
POTENTIALLY UNWANTED PROGRAMS	MALWARE TAXONOMY	MAT
PRECAUTIONARY PRINCIPLE	PRINCIPLES	CI
PREPARE: INCIDENT MANAGEMENT PLANNING	HUMAN FACTORS: INCIDENT MANAGEMENT	SOIM
PRESCRIPTIVE JURISDICTION	JURISDICTION	LR
PREVENTING ATTACKS	CROSS CUTTING SECURITY	CPS
PRINCIPLES	DECENTRALISED P2P MODELS	DSS
PRIVACY AND ACCOUNTABILITY	ACCOUNTABILITY	AAA
PRIVACY EVALUATION	PRIVACY ENGINEERING	POR
PRIVACY POLICY INTERPRETABILITY	CONTROL	POR
PRIVACY POLICY NEGOTIATION	CONTROL	POR
PRIVACY SETTINGS CONFIGURATION	CONTROL	POR
PRIVACY TECHNOLOGIES AS SUPPORT TO DEMOCRATIC POLITICAL SYSTEMS	PRIVACY TECHNOLOGIES AND DEMOCRATIC VALUES	POR
PROCESS INFORMATION	MAIN MEMORY FORENSICS	F
PROPERTIES OF SYSTEMS AND THEIR EXECUTION	FOUNDATIONS, METHODS AND TOOLS	FMS
PROPERTY CHECKING	FOUNDATIONS, METHODS AND TOOLS	FMS
PROTECTED MODULE ARCHITECTURES	HARDWARE SUPPORT FOR SOFTWARE SECURITY	HS
PROTECTING DATA INTEGRITY	SCHEMES FOR CONFIDENTIALITY, INTEGRITY AND ACCESS CONTROL	PLT
PROTECTION AGAINST NATURAL EVENTS AND ACCIDENTS	CYBER-PHYSICAL SYSTEMS	CPS
PROTECTION RINGS	PRIMITIVES FOR ISOLATION AND MEDIATION	OSV
PUBLIC KEY ENCRYPTION SCHEMES AND KEY ENCAPSULATION MECHANISMS	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
PUBLIC-KEY ENCRYPTION	PUBLIC-KEY CRYPTOGRAPHY	C
PUBLIC-KEY SIGNATURES	PUBLIC-KEY CRYPTOGRAPHY	C
Q		
QUANTUM KEY DISTRIBUTION	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
R		
RACE CONDITION MITIGATIONS	PREVENTION OF VULNERABILITIES	SS
RACE CONDITION VULNERABILITIES	CATEGORIES OF VULNERABILITIES	SS
RANDOM BIT GENERATION	CRYPTOGRAPHIC IMPLEMENTATION	AC
RANDOM NUMBER GENERATION	ENTROPY GENERATING BUILDING BLOCKS	HS
REFRESHING KEYS AND FORWARD SECURITY	KEY MANAGEMENT	AC
RELIABLE AND SECURE GROUP COMMUNICATIONS	COORDINATED RESOURCE CLUSTERING	DSS
REPLICATION MANAGEMENT AND COORDINATION SCHEMA	COORDINATED RESOURCE CLUSTERING	DSS
REQUIREMENTS OF FORM AND THE THREAT OF UNENFORCEABILITY	DEMATERIALISATION OF DOCUMENTS AND ELECTRONIC TRUST SERVICES	LR
RESEARCH AND DEVELOPMENT ACTIVITIES CONDUCTED BY NON-STATE PERSONS	COMPUTER CRIME	LR
RESOURCE COORDINATION CLASS	COORDINATION CLASSES AND ATTACKABILITY	DSS
RESOURCE MANAGEMENT AND COORDINATION SERVICES	CLASSES OF VULNERABILITIES AND THREATS	DSS

INDICATIVE MATERIAL	TOPIC	CyBOK KA
RESTRICTIONS ON EXPORTING SECURITY TECHNOLOGIES	OTHER REGULATORY MATTERS	LR
REVERSE ENGINEERING	INTELLECTUAL PROPERTY	LR
RING SIGNATURES	PUBLIC-KEY SCHEMES WITH SPECIAL PROPERTIES	C
RISK ASSESSMENT	RISK DEFINITIONS	RMG
RISK ASSESSMENT AND MANAGEMENT IN CYBER PHYSICAL SYSTEMS	RISK ASSESSMENT AND MANAGEMENT PRINCIPLES	RMG
RISK ASSESSMENT AND MANAGEMENT IN CYBER-PHYSICAL SYSTEMS	RISK ASSESSMENT AND MANAGEMENT PRINCIPLES	RMG
RISK ASSESSMENT AND MANAGEMENT METHODS	RISK ASSESSMENT AND MANAGEMENT PRINCIPLES	RMG
RISK MANAGEMENT	FOUNDATIONAL CONCEPTS	CI
RISK MANAGEMENT	RISK DEFINITIONS	RMG
RISK PERCEPTION FACTORS	RISK GOVERNANCE	RMG
ROAD VEHICLES	ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE	SSL
ROBOTICS AND ADVANCED MANUFACTURING	CYBER-PHYSICAL SYSTEMS DOMAINS	CPS
ROOT OF TRUST	HARDWARE DESIGN CYCLE	HS
RSA	SCHEMES	C
RUNTIME DETECTION OF ATTACKS	MITIGATING EXPLOITATION	SS
S		
SAAS FORENSICS	CLOUD FORENSICS	F
SAFECODE	PRESCRIPTIVE PROCESSES	SSL
SALTZER AND SCHROEDER PRINCIPLES	PRINCIPLES	CI
SALTZER AND SCHROEDER’S PRINCIPLES	OS SECURITY PRINCIPLES	OSV
SAMM	ASSESS THE SECURE SOFTWARE LIFECYCLE	SSL
SANDBOXING	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
SDN AND NFV SECURITY	NETWORK SECURITY TOOLS	NS
SECRECY CAPACITY	SCHEMES FOR CONFIDENTIALITY, INTEGRITY AND ACCESS CONTROL	PLT
SECRET SHARING	INFORMATION-THEORETICALLY SECURE CONSTRUCTIONS	C
SECURE ELEMENT AND SMARTCARD	SECURE PLATFORMS	HS
SECURE MESSAGING	APPLIED CRYPTOGRAPHY IN ACTION	AC
SECURE MULTI-PARTY COMPUTATION	ADVANCED PROTOCOLS	C
SECURE POSITIONING	DISTANCE BOUNDING AND SECURE POSITIONING	PLT
SECURITY AND PRIVACY CONCERNS	CYBER-PHYSICAL SYSTEMS	CPS
SECURITY ARCHITECTURE AND LIFECYCLE	CROSS-CUTTING THEMES	CI
SECURITY AT THE APPLICATION LAYER	NETWORK PROTOCOLS AND THEIR SECURITY	NS
SECURITY AT THE INTERNET LAYER	NETWORK PROTOCOLS AND THEIR SECURITY	NS
SECURITY AT THE TRANSPORT LAYER	NETWORK PROTOCOLS AND THEIR SECURITY	NS
SECURITY CULTURE	RISK GOVERNANCE	RMG
SECURITY DOMAINS	ROLE OF OPERATING SYSTEMS	OSV
SECURITY ECONOMICS	CROSS-CUTTING THEMES	CI
SECURITY GOALS IN NETWORKED SYSTEMS	SECURITY GOALS AND ATTACKER MODELS	NS
SECURITY HYGIENE	HUMAN ERROR	HF
SECURITY METRICS	RISK ASSESSMENT AND MANAGEMENT PRINCIPLES	RMG
SECURITY MODELS	OS SECURITY PRINCIPLES	OSV
SECURITY ON LINK LAYER	NETWORK PROTOCOLS AND THEIR SECURITY	NS
SECURITY OPERATIONS AND BENCHMARKING	PLAN: SECURITY INFORMATION AND EVENT MANAGEMENT	SOIM

INDICATIVE MATERIAL	TOPIC	CyBOK KA
SELF-HELP DISFAVOURED: SOFTWARE LOCKS AND HACK-BACK	COMPUTER CRIME	LR
SENSOR COMPROMISE	COMPROMISING EMANATIONS AND SENSOR SPOOFING	PLT
SERVER-SIDE MISCONFIGURATION AND VULNERABLE COMPONENTS	SERVER-SIDE VULNERABILITIES AND MITIGATIONS	WAM
SERVICES	CLOUD FORENSICS	F
SERVICES COORDINATION CLASS	COORDINATION CLASSES AND ATTACKABILITY	DSS
SESIP	MEASURING HARDWARE SECURITY	HS
SETUP ASSUMPTIONS	CRYPTOGRAPHIC SECURITY MODELS	C
SHADOW SECURITY	HUMAN ERROR	HF
SHIELDS FROM LIABILITY	INTERNET INTERMEDIARIES	LR
SHORT-TERM MEMORY	FITTING THE TASK TO THE HUMAN	HF
SIDE CHANNEL VULNERABILITIES	CATEGORIES OF VULNERABILITIES	SS
SIDE CHANNELS	HARDWARE	FMS
SIEM PLATFORMS AND COUNTERMEASURES	EXECUTE: MITIGATION AND COUNTERMEASURES	SOIM
SIGMA PROTOCOLS	ADVANCED PROTOCOLS	C
SIGNAL ANNIHILATION AND OVERSHADOWING	JAMMING AND JAMMING-RESILIENT COMMUNICATIONS	PLT
SIMULATION OF CRYPTOGRAPHIC OPERATIONS	CRYPTOGRAPHIC SECURITY MODELS	C
SITE RELIABILITY ENGINEERING	EXECUTE: MITIGATION AND COUNTERMEASURES	SOIM
SITUATIONAL AWARENESS	KNOWLEDGE: INTELLIGENCE AND ANALYSIS	SOIM
SOAR: IMPACT AND RISK ASSESSMENT	EXECUTE: MITIGATION AND COUNTERMEASURES	SOIM
SOFTWARE DEVELOPERS	STAKEHOLDER ENGAGEMENT	HF
SOFTWARE-DEFINED NETWORKING AND NETWORK FUNCTION VIRTUALISATION	NETWORKING APPLICATIONS	NS
SOUNDNESS	DETECTION OF VULNERABILITIES	SS
SPECIALISED SERVICES	ELEMENTS OF A MALICIOUS OPERATION	AB
SPECIFICATION-BASED SYNTHESIS	CONFIGURATION	FMS
STATE ACTORS	CHARACTERISATION OF ADVERSARIES	AB
STATE CYBER OPERATIONS IN GENERAL	PUBLIC INTERNATIONAL LAW	LR
STATIC DETECTION	DETECTION OF VULNERABILITIES	SS
STOCHASTIC METHODS	CRYPTOGRAPHIC PROTOCOLS	FMS
STORAGE FORENSICS	OPERATING SYSTEM ANALYSIS	F
STRATEGIES	PRIVACY ENGINEERING	POR
STREAM CIPHERS	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
STRUCTURED OUTPUT GENERATION VULNERABILITIES	CATEGORIES OF VULNERABILITIES	SS
STRUCTURED OUTPUT GENERATIONS MITIGATIONS	PREVENTION OF VULNERABILITIES	SS
STRUCTURED P2P PROTOCOLS	DECENTRALISED P2P MODELS	DSS
SUBJECT MATTER AND REGULATORY FOCUS	DATA PROTECTION	LR
SYMBOLIC METHODS	CRYPTOGRAPHIC PROTOCOLS	FMS
SYMMETRIC ENCRYPTION AND AUTHENTICATION	SYMMETRIC CRYPTOGRAPHY	C
SYMMETRIC PRIMITIVES	SYMMETRIC CRYPTOGRAPHY	C
SYSLOG	MONITOR: DATA SOURCES	SOIM
SYSTEM AND KERNEL LOGS	MONITOR: DATA SOURCES	SOIM
SYSTEMS COORDINATION STYLES	COORDINATED RESOURCE CLUSTERING	DSS

T

INDICATIVE MATERIAL	TOPIC	CyBOK KA
TAKE-DOWN PROTECTION	INTERNET INTERMEDIARIES	LR
TECHNICAL ASPECTS	ACCOUNTABILITY	AAA
TERMS	AWARENESS AND EDUCATION	HF
TESTING AND VALIDATING INTRUSION DETECTION SYSTEMS	ANALYSE: ANALYSIS METHODS	SOIM
THE ADVERSARY	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
THE BASE-RATE FALLACY	ANALYSE: ANALYSIS METHODS	SOIM
THE CHALLENGES OF CONSUMING CRYPTOGRAPHY	CONSUMING CRYPTOGRAPHY	AC
THE ENFORCEMENT OF, AND PENALTIES FOR, CRIMES AGAINST INFORMATION SYSTEMS	COMPUTER CRIME	LR
THE KEY LIFECYCLE	KEY MANAGEMENT	AC
THE LAW OF ARMED CONFLICT	PUBLIC INTERNATIONAL LAW	LR
THE ROLE OF FORMAL SECURITY DEFINITIONS AND PROOFS	ALGORITHMS, SCHEMES AND PROTOCOLS	AC
THEORY	AUTHORISATION	AAA
THINKING FAST AND SLOW	HUMAN ERROR	HF
THREAT MODEL	HARDWARE DESIGN CYCLE	HS
THREATS TO SECURITY FOR MODERN OSS	ATTACKER MODEL	OSV
TIME	HARDWARE DESIGN PROCESS	HS
TLS	SCHEMES	C
TOUCHPOINTS	PRESCRIPTIVE PROCESSES	SSL
TOWARDS MORE SCIENTIFIC DEVELOPMENT METHODS	MOTIVATION	FMS
TRANSPORT LAYER SECURITY	APPLIED CRYPTOGRAPHY IN ACTION	AC
TRANSPORTATION SYSTEMS AND AUTONOMOUS VEHICLES	CYBER-PHYSICAL SYSTEMS DOMAINS	CPS
TROJAN CIRCUITS	HARDWARE DESIGN PROCESS	HS
TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA	PRIMITIVES FOR ISOLATION AND MEDIATION	OSV
TRUSTED COMPUTING	MOTIVATIONS FOR SECURE SOFTWARE LIFECYCLE	SSL
TRUSTED EXECUTION ENVIRONMENT	HARDWARE SUPPORT FOR SOFTWARE SECURITY	HS
TRUSTED PLATFORM MODULE (TPM)	SECURE PLATFORMS	HS
U		
UNCOORDINATED SPREAD SPECTRUM TECHNIQUES	JAMMING AND JAMMING-RESILIENT COMMUNICATIONS	PLT
UNDERGROUND ECO-SYSTEM	MALICIOUS ACTIVITIES BY MALWARE	MAT
UNDERSTANDING INTELLECTUAL PROPERTY	INTELLECTUAL PROPERTY	LR
UNIVERSAL COMPOSABILITY	CRYPTOGRAPHIC SECURITY MODELS	C
UNSTRUCTURED P2P PROTOCOLS	DECENTRALISED P2P MODELS	DSS
USER AUTHENTICATION	AUTHENTICATION	AAA
V		
VERIFICATION AND FORMAL METHODS	CROSS-CUTTING THEMES	CI
VIRTUAL MACHINES	ROLE OF OPERATING SYSTEMS	OSV
VIRTUAL MACHINES	HARDWARE SUPPORT FOR SOFTWARE SECURITY	HS
VULNERABILITIES CAN BE EXPLOITED WITHOUT BEING NOTICED	MOTIVATIONS FOR SECURE SOFTWARE LIFECYCLE	SSL
VULNERABILITY MANAGEMENT	RISK ASSESSMENT AND MANAGEMENT PRINCIPLES	RMG
VULNERABILITY TESTING	ETHICS	LR
W		

INDICATIVE MATERIAL	TOPIC	CyBOK KA
WARRANTED STATE ACTIVITY	COMPUTER CRIME	LR
WARRANTIES AND THEIR EXCLUSION	CONTRACT	LR
WEB PKI AND HTTPS	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
WEB-BASED APPLICATIONS	SOFTWARE AND LARGE SCALE SYSTEMS	FMS
WEBIFICATION	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
WIRELESS NETWORKS	NETWORKING APPLICATIONS	NS
WORKFLOWS AND VOCABULARY	FUNDAMENTAL CONCEPTS	SOIM
Z		
ZERO KNOWLEDGE	ADVANCED PROTOCOLS	C
ZERO TRUST NETWORKING	NETWORK SECURITY TOOLS	NS