An Alphabetical Version of the CyBOK's Knowledge Areas Indicative Material Issue 1.0

Lata Nautiyal | University of Bristol

Awais Rashid | University of Bristol



COPYRIGHT

© Crown Copyright, The National Cyber Security Centre 2020. This information is licensed under the Open Government Licence v3.0. To view this licence, visit:

http://www.nationalarchives.gov.uk/doc/open-government-licence/ OCL

When you use this information under the Open Government Licence, you should include the following attribution: CyBOK © Crown Copyright, The National Cyber Security Centre 2018, licensed under the Open Government Licence: http://www.nationalarchives.gov.uk/doc/open-government-licence/.

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.



INTRODUCTION

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

The ultimate purpose of this document is to support applicants in mapping the contents of particular course modules or teaching units on to the NCSC certification requirements with a specific aim to complete Table 3.3 in the NCSC certification application.

For the purposes of the NCSC certified master's programme each of the **CyBOK Knowledge Trees** is represented as follows:

- The nodes directly under the root node are referred to a Topic. 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 Topics 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 what 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**.



For the sake of brevity, the following acronyms are used to refer to the Knowledge Areas: Knowledge areas are shown in red. The acronyms are expanded below:

Acronym	Knowledge Area
AAA	Authentication, Authorisation & Accountability
AB	Adversarial Behaviours
С	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. 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.



ACCESS/ADMISSION CONTROL AND ID MANAGEMENT ADMISSION INTO EVIDENCE OF ELEC- TRONIC DOCUMENTS AES SCHEMES SCHEMES SCHEMES AFFILIATE PROGRAMMES ALIEMATO FOR ANALICIOUS OPERATION AGILE AND DEVODPS ARI TRAFFIC COMMUNICATIONS NET- WORKS ALERT CORRELATION PLAN: SECURITY INFORMATION AND EVENT MANAGE- MENT ANALYSIS ENVIRONMENTS ANALYSIS ENVIRONMENTS ANALYSIS ENVIRONMENTS ANALYSIS ENVIRONMENTS ANALYSIS TECHNOLOGIES ANOMALY DETECTION ANALYSE ANALYSIS METHODS ANALYSE ANALYSIS METHODS ANALYSE ANALYSIS METHODS OSI ANALYSES AND EVASION TECH- NIQUES API DESIGN API VULNERABILITIES API VULNERABILITIES API VULNERABILITIES APPICATION GATEWAY APPILCATION ACTER SECURITY ON THE VULNERABILITIES APPICATION GATEWAY APPILCATION LAYER SECURITY APPILCATION TO SELECTED MALWARE ANALYSIS METHODS OSI ANALYSE ANALYSIS APPICATION GATEWAY APPILCATION GATEWAY APPILCATION GATEWAY APPILCATION GATEWAY APPILCATION TORRES FUNDAMENTAL CONCEPTS AND APPROACHES WAN APPILCATION TORRES FUNDAMENTAL CONCEPTS AND APPROACHES WAN APPILCATION TECHNOLOGIES APPROXIMATE ANALYSIS ARTIFACT ANALYSIS ARTIFACT ANALYSIS ARTIFACT ANALYSIS ARTIFACT ANALYSIS APPICATION TORRES FUNDAMENTAL CONCEPTS AND APPROACHES WAN ANALYSE ANALYSIS ARTIFACT OR ANALYSIS	ACCESS CONTROL ACCESS/ADMISSION CONTROL AND ID MANAGEMENT ADMISSION INTO EVIDENCE OF ELEC- TRONIC DOCUMENTS AES AFFILIATE PROGRAMMES AGILE AND DEVOPS	CLASSES OF VULNERABILITIES AND THREATS DEMATERIALISATION OF DOCUMENTS AND ELECTRONIC TRUST SERVICE SCHEMES ELEMENTS OF A MALICIOUS OPERATION ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE PHYSICAL LAYER SECURITY OF SELECTED COMMUNICATIONS TECHNOLOGIES PLAN: SECURITY INFORMATION AND EVENT MANAGE-	AAA DSS LR C AB SSL PLT
ACCESS/ADMISSION CONTROL AND ID MANAGEMENT MANAGEMENT ADMISSION INTO EVIDENCE OF ELEC- TRONIC DOCUMENTS AND ELEC- TRONIC DOCUMENTS AES SCHEMES SCHEMES SCHEMES SCHEMES AFFILIATE PROGRAMMES AEILAND DEVOPS ARI TRAFFIC COMMUNICATIONS NET- WORKS ANALYSIS ENVIRONMENTS ANALYSIS ENVIRONMENTS ANALYSIS ENVIRONMENTS ANALYSIS ENVIRONMENTS ANALYSIS TECHNIQUES 2 ANALYSE ANALYSIS METHODS ANOMALY DETECTION OS HARDENING APPLICATION LAYER SECURITY OF SELECTED COMMUNI- CATIONS TECHNIQUES 2 MALWARE ANALYSIS MAY ANALYSIS TECHNIQUES 2 MALWARE ANALYSIS MAY ANOMALY DETECTION OS HARDENING	ACCESS/ADMISSION CONTROL AND ID MANAGEMENT ADMISSION INTO EVIDENCE OF ELECTRONIC DOCUMENTS AES AFFILIATE PROGRAMMES AGILE AND DEVOPS	CLASSES OF VULNERABILITIES AND THREATS DEMATERIALISATION OF DOCUMENTS AND ELECTRONIC TRUST SERVICE SCHEMES ELEMENTS OF A MALICIOUS OPERATION ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE PHYSICAL LAYER SECURITY OF SELECTED COMMUNICATIONS TECHNOLOGIES PLAN: SECURITY INFORMATION AND EVENT MANAGE-	DSS LR C AB SSL
MANAGEMENT ADMISSION INTO EVIDENCE OF ELECTRONIC DOCUMENTS AND ELECTRONIC DOCUMENTS AES SCHEMS SCHEMS SCHEMS SCHEMS AGILE AND DEVOPS ADAPTATIONS OF SEQUEE SOFTWARE LIFECYCLE SSIAR TRAFFIC COMMUNICATIONS NET-PHYSICAL LAYER SECURITY OF SELECTED COMMUNI-WORKS ALERT CORRELATION PLAN: SECURITY INFORMATION AND EVENT MANAGE-MENT ANALYSIS ENVIRONMENTS MALWARE ANALYSIS ANALYSIS STECHNIQUES 2 MALWARE ANALYSIS METHODS SOIN ANDMALY DETECTION ANALYSIS AND EVASION TECH-NIQUES APPLICATION OF VULNERABILITIES APPLICATION AND EVENT MANAGE-SPECIAL AND APPLICATION AND APPROXIMATE AND APPLICATION APPLICATION AND APPLICATION AND APPLICATION AND APPLICATION AND APPLICATION	MANAGEMENT ADMISSION INTO EVIDENCE OF ELECTRONIC DOCUMENTS AES AFFILIATE PROGRAMMES AGILE AND DEVOPS	DEMATERIALISATION OF DOCUMENTS AND ELECTRONIC TRUST SERVICE SCHEMES ELEMENTS OF A MALICIOUS OPERATION ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE PHYSICAL LAYER SECURITY OF SELECTED COMMUNICATIONS TECHNOLOGIES PLAN: SECURITY INFORMATION AND EVENT MANAGE-	LR C AB SSL
TRONIC DOCUMENTS AES SCHEMES SCHEMES AFFILIATE PROGRAMMES ELEMENTS OF A MALICIOUS OPERATION AGULE AND DEVOPS ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE SS AIR TRAFFIC COMMUNICATIONS NET WORKS ALERT CORRELATION PLAN: SECURITY INFORMATION AND EVENT MANAGE- MENT ANALYSIS ENVIRONMENTS ANALYSIS ENVIRONMENTS ANALYSIS EVENTRONIMENTS ANALYSIS TECHNIQUES 2 MALWARE ANALYSIS ANDMALY DETECTION ANALYSIS TECHNIQUES 2 MALWARE ANALYSIS ANDMALY DETECTION ANALYSIS AND EVASION TECH- NIQUES API DESIGN PREVENTION OF VULNERABILITIES APIPICATION OF ATTACKS APPLICATION LAYER SECURITY APPLICATION LAYER SECURITY APPLICATION LAYER SECURITY APPLICATION LAYER SECURITY APPLICATION TECHNOLOGIES APPLICATION TORES FUNDAMENTAL CONCEPTS AND APPROACHES WAM APPLICATION TECHNOLOGIES APPLICATION TORES FUNDAMENTAL CONCEPTS AND APPROACHES WAM APPLICATION TECHNOLOGIES APPLICATION TOREN ARM TRUSTSZONE HARDWARE SUPPORT FOR SOFTWARE SECURITY HARDW	TRONIC DOCUMENTS AES AFFILIATE PROGRAMMES AGILE AND DEVOPS	TRONIC TRUST SERVICE SCHEMES ELEMENTS OF A MALICIOUS OPERATION ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE PHYSICAL LAYER SECURITY OF SELECTED COMMUNI- CATIONS TECHNOLOGIES PLAN: SECURITY INFORMATION AND EVENT MANAGE-	C AB SSL
AFFILIATE PROGRAMMES AFFILIATE PROGRAMMES AGILE AND DEVOPS ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE SISTAMATER COMMUNICATIONS NET- PRYSICAL LAYER SECURITY OF SELECTED COMMUNI- WORKS ALERT CORRELATION PLANS SECURITY INFORMATION AND EVENT MANAGE- WORKS ALERT CORRELATION PLANS SECURITY INFORMATION AND EVENT MANAGE- MANALYSIS ENVIRONMENTS MALWARE ANALYSIS ANALYSIS ENVIRONMENTS ANALYSIS ENVIRONMENTS ANALYSIS ENVIRONMENTS ANALYSIS ENVIRONMENTS ANALYSIS ENVIRONMENTS ANALYSIS ANALYSIS METHODS SOIM ANTI-ANALYSIS AND EVASION TECH- NIQUES API DESIGN PREVENTION OF VULNERABILITIES CATEGORIES OF VULNERABILITIES SISTAMATI-ANALYSIS APPLICATION AND EVENT MANAGE- APPLICATION LAYER SECURITY INTERNET ARCHITECTURE APPLICATION LAYER SECURITY INTERNET ARCHITECTURE APPLICATION STORES APPLICATION STORES APPLICATION STORES APPLICATION STORES APPLICATION FOR THE CYBERSPACE AND INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH ILL INT	AFFILIATE PROGRAMMES AGILE AND DEVOPS	ELEMENTS OF A MALICIOUS OPERATION ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE PHYSICAL LAYER SECURITY OF SELECTED COMMUNI- CATIONS TECHNOLOGIES PLAN: SECURITY INFORMATION AND EVENT MANAGE-	AB SSL
AGILE AND DEVOPS ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE SSI AIR TRAFFIC COMMUNICATIONS NET. PHYSICAL LAYER SECURITY OF SELECTED COMMUNI- WORKS ALERT CORRELATION PLAN: SECURITY INFORMATION AND EVENT MANAGE- MENT ANALYSIS ENVIRONMENTS MALWARE ANALYSIS ANALYSIS TECHNIQUES 2 MALWARE ANALYSIS ANALYSIS TECHNIQUES 2 MALWARE ANALYSIS ANALYSIS TECHNIQUES 2 MALWARE ANALYSIS MATHANALYSIS AND EVASION TECH- NIQUES API DESIGN API PULIVERABILITIES API EVENTION OF VULNERABILITIES API PULIVERABILITIES API FUNDAMENTAL CONCEPTS AND APPROACHES AND FILES APPLICATION LOGS: WEB SERVER LOGS AND FILES APPLICATION STORES APPLICATION TECHNOLOGIES APPLICATION TECHNOLOGIES APPLYING FOR THE CYBERSPACE AND INFORMATION TECHNOLOGIES APPROXIMATE ANALYSIS ARM TRUSTZONE APPROXIMATE ANALYSIS ARM TRUSTZONE APPROXIMATE ANALYSIS ARM TRUSTZONE ARTIFACTS AND FRAGMENTS ASSESSMENT CRITERIA ATTACK DETECTION ATTACK ON CONFIDENTIALITY, IN- TEGRITY AVAILABILITY, IN- TEGRITY AVAILABILITY, IN- TEGRITY AVAILABILITY, IN- TEGRITY AVAILABILITY, IN- TEGRITY AVAILABILITY ATTACK ON CONFIDENTIALITY, IN- TEGRITY AVAILABILITY ATTACK SUFFACE ATTACK TREES MODELS ATTACK TREES MACHITECTION ALTHERITION ALTHERITION MALWARE RESPONSE MACHITECTION ALUTHERT TO AND IDENTIFICATION ALUTHER TRUSTA	AGILE AND DEVOPS	ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE PHYSICAL LAYER SECURITY OF SELECTED COMMUNI- CATIONS TECHNOLOGIES PLAN: SECURITY INFORMATION AND EVENT MANAGE-	SSL
AIR TRAFFIC COMMUNICATIONS NET- WORKS CATIONS TECHNOLOGIES ALERT CORRELATION PLAN: SECURITY OF SELECTED COMMUNI- CATIONS TECHNOLOGIES ANALYSIS ENVIRONMENTS MALWARE ANALYSIS ANALYSIS ENVIRONMENTS MALWARE ANALYSIS APPLICATION OF VULNERABILITIES SI APPLICATION CATEWAY APPLICATION CATEWAY APPLICATION CATEWAY APPLICATION CATEWAY APPLICATION CATEWAY APPLICATION ALYER SECURITY INTERNET ARCHITECTURE NI APPLICATION STORES APPLICATION STORES APPLICATION STORES APPLICATION STORES APPLICATION THE CYBERSPACE AND INFORMATION TECHNOLOGIES APPLICATION THE CYBERSPACE AND INFORMATION TECHNOLOGIES APPROXIMATE ANALYSIS ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS AND APPROACHES WAN APPLICATION THE CYBERSPACE AND INFORMATION TECHNOLOGIES ARM TRUSTZONE HARDWARE SUPPORT FOR SOFTWARE SECURITY HARDWARE RESPONSE MALWARE ARCHITECTURE MALWARE RESPONSE MALWARE ARCHITECTURE MALWARE RESPONSE MALWARE ARCHITECTURE MALWARE ARCHITEC		PHYSICAL LAYER SECURITY OF SELECTED COMMUNI- CATIONS TECHNOLOGIES PLAN: SECURITY INFORMATION AND EVENT MANAGE-	
ALERT CORRELATION PLAN: SECURITY INFORMATION AND EVENT MANAGE. ANALYSIS ENVIRONMENTS MALWARE ANALYSIS MANALYSIS TECHNIQUES 2 MALWARE ANALYSIS MANALY DETECTION ANDMALY DETECTION ANDMALY DETECTION ANDMALY DETECTION OS HARDENING ANTI-ANALYSIS AND EVASION TECH- NIQUES API DESIGN PREVENTION OF VULNERABILITIES SEAPPIFICATION APPLICATION ACTEWAY APPLICATION LOGS: WEB SERVER LOGS AND FILES APPLICATION STORES FUNDAMENTAL CONCEPTS AND APPROACHES APPLICATION TECH- NICOURD STORES APPLICATION TECH- NICOURD STORES FUNDAMENTAL CONCEPTS AND APPROACHES WARA APPLICATION LOGS: WEB SERVER LOGS AND FILES APPLICATION LOGS: WEB SERVER LOGS AND FILES APPLYING FOR THE CYBERSPACE AND INFORMATION TECHNOLOGIES APPLYING FOR THE CYBERSPACE AND INFORMATION TECHNOLOGIES ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS AND APPROACHES WARA APPLYING FOR THE CYBERSPACE AND INFORMATION TECHNOLOGIES ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS AND APPROACHES WARA APPROXIMATE ANALYSIS ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS SOIN ARM TRUSTZONE HARDWARE SUPPORT FOR SOFTWARE SECURITY HARDWARE SUPPORT FOR SOFTWARE ATTACK TORS ATTACK SUPFACE ATTACK TORS ATTACK SUPFACE A		CATIONS TECHNOLOGIES PLAN: SECURITY INFORMATION AND EVENT MANAGE-	PLT
ANALYSIS ENVIRONMENTS MALWARE ANALYSIS MATAMALYSIS TECHNIQUES 2 MALWARE ANALYSIS METHODS SOIM ANOMALY DETECTION ANALYSE: ANALYSIS METHODS SOIM ANOMALY DETECTION OF HARDENING OS HARDENING SERVICE OF VULNERABILITIES SERVICE SERV			
ANALYSIS TECHNIQUES 2 ANAUMAIX DETECTION ANALYSE ANALYSIS METHODS SOIN ANOMALY DETECTION ANAUTSE ANALYSIS METHODS SOIN ANOMALY DETECTION ANAUTSE ANALYSIS METHODS SOIN ANOMALY DETECTION OS HARDENING OS HARDENING OS HARDENING OS HARDENING ANTI-IANLAYSIS AND EVASION TECH- NIQUES API DESIGN PREVENTION OF VULNERABILITIES SISTEMALYSIS MAY APILOCATION GATEWAY NETWORK DEFENCE TOOLS APPICATION GATEWAY NETWORK DEFENCE TOOLS APPLICATION LOGS: WEB SERVER LOGS MONITOR: DATA SOURCES SOIN APPLICATION STORES FUNDAMENTAL CONCEPTS AND APPROACHES WAAN APPLICATION STORES FUNDAMENTAL CONCEPTS AND APPROACHES WAAN APPLICATION TO RESEMANCE AND INFORMATION TECHNOLOGIES APPLYING FOR THE CYBERSPACE AND INFORMATION TECHNOLOGIES APPROXIMATE ANALYSIS ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS AND APPROACHES WAAN APPROXIMATE ANALYSIS ARTIFACT ANALYSIS ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS SOIN ARM TRUSTZONE HARDWARE SUPPORT FOR SOFTWARE SECURITY HIS ARTIFACTS AND FRAGMENTS MAIN MEMORY FORENSICS INFORMATION ATTACK ON CONFIDENTIALITY, IN- TEGRITY, AVAILABILITY ATTACK ON CONFIDENTIALITY, IN- TEGRITY, AVAILABILITY ATTACK SURFACE ATTACK RYPES ATTACKER MODELS ATTACKING PLEY SYSTEMS DIST ATTACKER MODELS ATTACKING PLEY SYSTEMS DIST ATTACKER MODELS ATTACKING PLEY SYSTEMS DIST ATTACKING NO PHYSICAL LAYER IDENTI- FICATION ATTRIBUTION AUWARE RESPONSE MAA ATTRIBUTION AUWARE RESPONSE MAA ATTRIBUTION AUGHSTANDARDENCY TRANSPARENCY POIL AUTHENTICATION AND IDENTIFICA- PRIMITIVES FOR ISOLATION AND MEDIATION AUTHENTICATION AND IDENTIFICA- PRIMITIVES FOR ISOLATION AND MEDIATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION AND IDENTIFICA- BUNDAMENTAL CONCEPTS AND APPROACHES WAAN AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION AND IDENTIF	ALERT CORRELATION	MENT	SOIM
ANOMALY DETECTION ANALYSE: ANALYSIS METHODS OSI ANOMALY DETECTION OS HARDENING OSI ANTI-ANALYSIS AND EVASION TECH- INQUES API DESIGN PREVENTION OF VULNERABILITIES SEAP APPLICATION FUNDAMENTAL CONCEPTS AND APPOACHES API PULNERABILITIES CATEGORIES OF VULNERABILITIES SEAP APPLICATION GATEWAY NETWORK DEFENCE TOOLS APPLICATION LAYER SECURITY INTERNET ARCHITECTURE NO APPLICATION LAYER SECURITY INTERNET ARCHITECTURE APPLICATION STORES APPLICATION STORES APPLICATION STORES APPLICATION FECHNOLOGIES APPLICATION TECHNOLOGIES APPLICATION TECHNOLOGIES APPROXIMATE ANALYSIS ARCHITECTURAL PRINCIPLES APPLICATION TECHNOLOGIES APPROXIMATE ANALYSIS ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS AND APPROACHES ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS SOIN ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS SOIN ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS SOIN ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS SOIN ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS SOIN ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS SOIN ARTIFACTS AND FRAGMENTS MAIN MEMORY FORENSICS INTERVIPCE ATTACK DETECTION MALWARE DETECTION MALWARE DETECTION MALWARE DETECTION MALWARE DETECTION MALYARE DETECTION MALY	ANALYSIS ENVIRONMENTS	MALWARE ANALYSIS	MAT
ANOMALY DETECTION OS HARDENING OST ANTI-ANALYSIS AND EVASION TECH-MIQUES API DESIGN PREVENTION OF VULNERABILITIES SI API PULNERABILITIES CATEGORIES OF VULNERABILITIES SI API PULNERABILITIES CATEGORIES OF VULNERABILITIES SI API VULNERABILITIES CATEGORIES OF VULNERABILITIES SI APPLICATION GATEWAY NETWORK DEFENCE TOOLS NA APPLICATION LAYER SECURITY INTERNET ARCHITECTURE NA APPLICATION LOGS: WEB SERVER LOGS MONITOR: DATA SOURCES SOIN AND FILES PUNDAMENTAL CONCEPTS AND APPROACHES WAAN AND FILES FUNDAMENTAL CONCEPTS AND APPROACHES WAAN AND FILES FUNDAMENTAL CONCEPTS AND APPROACHES WAAN APPLICATION STORES FUNDAMENTAL CONCEPTS AND APPROACHES WAAN APPLICATION TECHNOLOGIES APPLICATION TECHNOLOGIES APPLICATION TECHNOLOGIES APPLICATION TECHNOLOGIES APPLICATION TECHNOLOGIES APPLICATION TECHNOLOGIES ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS AND APPROACHES WAAN APPROXIMATE ANALYSIS ARTIFACT ANALYSIS ARTIFACT ANALYSIS ARTIFACT ANALYSIS ARTIFACT ANALYSIS ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS SOIN ARM TRUSTZONE HARDWARE SUPPORT FOR SOFTWARE SECURITY HE ANALYSIS AND FRAGMENTS MAIN MEMORY FORENSICS IN ATTACK DETECTION MALWARE DETECTION MALTACK SURFACE ATTACK SURFACE ATTACKER MODEL OSS ATTACKER MODELS ATTACK SURFACE ATTACKING P2P SYSTEMS DESTATACK SURFACE ATTACKING P2P SYSTEMS DESTATACK SON PHYSICAL LAYER IDENTIFICATION ATTACK SON PHYSICAL LAYER IDENTIFICATION ATTACKING P2P SYSTEMS DESTATACKER MODELS ATTACK SON PHYSICAL LAYER IDENTIFICATION ATTACKING P2P SYSTEMS DESTATACKER MODELS ATTACK SON PHYSICAL LAYER IDENTIFICATION ATTACKING P2P SYSTEMS DESTATACKER MODELS ATTACK SON PHYSICAL LAYER IDENTIFICATION ATTACKING P2P SYSTEMS DESTATACKER MODELS ATTACK SON PHYSICAL LAYER IDENTIFICATION ATTACKING P2P SYSTEMS DESTATACKER MODELS ATTACK SON PHYSICAL LAYER IDENTIFICATION ATTACKING P2P SYSTEMS DESTATACKER MODELS ATTACKED PARKS PARENCY POTO ATTACKS ON PHYSICAL LAYER IDENTIFICATION FUNDAMENTAL CONCEPTS AND APPROACHES WAAN AUT	ANALYSIS TECHNIQUES 2	MALWARE ANALYSIS	MAT
ANTI-ANALYSIS AND EVASION TECH- NIQUES APPLOSIGN PREVENTION OF VULNERABILITIES SI APPLICATION FUNDAMENTAL CONCEPTS AND APPROACHES MAN APPLICATION GATEWAY APPLICATION LOGS: WEB SERVERLOGS APPLICATION LOGS: WEB SERVERLOGS APPLICATION STORES APPLICATION STORES APPLICATION TO THE CYBERSPACE AND INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH INFORMATION TECHNOLOGIES APPLICATION TO THE CYBERSPACE AND INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH INFORMATION TECHNOLOGIES ARM TRUSTZONE ARM TRUSTZONE HARDWARE SUPPORT FOR SOFTWARE SECURITY HATTACK DETECTION MALWARE DETECTION MALWARE DETECTION MALWARE ANALYSIS ARTIFACT ANALYSIS INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH LEGAL R	ANOMALY DETECTION	ANALYSE: ANALYSIS METHODS	SOIM
API DESIGN PREVENTION OF VULNERABILITIES SIAPIPECESION PREVENTION OF VULNERABILITIES SIAPIPECATION PROVINERABILITIES SIAPIPECATION FUNDAMENTAL CONCEPTS AND APPROACHES WAN APPLICATION GATEWAY NETWORK DEFENCE TOOLS NAPPLICATION LAYER SECURITY INTERNET ARCHITECTURE NAPPLICATION LAYER SECURITY INTERNET ARCHITECTURE NAPPLICATION LAYER SECURITY INTERNET ARCHITECTURE NAPPLICATION LOGS: WEB SERVER LOGS MONITOR: DATA SOURCES SOIN AND FILES AND FILES FUNDAMENTAL CONCEPTS AND APPROACHES WAN APPLICATION STORES FUNDAMENTAL CONCEPTS AND APPROACHES WAN APPLYING FOR THE CYBERSPACE AND INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH LINFORMATION TECHNOLOGIES APPROXIMATE ANALYSIS ARTIFACT ANALYSIS ARTIFACT ANALYSIS ARTIFACT ANALYSIS ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS SOIN ARM TRUSTONE HARDWARE SUPPORT FOR SOFTWARE SECURITY HARDWARE SUPPORT FOR SOFTWARE SECURITY HARDWARE SUPPORT FOR SOFTWARE SECURITY HARDWARE SECURITY SECURITY SECURITY HARDWARE SEC	ANOMALY DETECTION	OS HARDENING	osv
API VILINERABILITIES APPIFICATION FUNDAMENTAL CONCEPTS AND APPROACHES WAM APPLICATION GATEWAY APPLICATION LOGS: WEB SERVER LOGS AND FILES APPLICATION STORES APPLICATION STORES APPLICATION STORES APPLICATION STORES APPLICATION ECHNOLOGIES APPLICATION STORES APPLICATION STORES APPLICATION FOR THE CYBERSPACE AND INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH		MALWARE ANALYSIS	MAT
APPIFICATION FUNDAMENTAL CONCEPTS AND APPROACHES APPLICATION GATEWAY APPLICATION LAYER SECURITY INTERNET ARCHITECTURE MAPPLICATION LOGS: WEB SERVER LOGS AND FILES APPLICATION STORES APPLICATION TECHNOLOGIES APPLICATION TECHNOLOGIES APPROXIMATE ANALYSIS ARCHITECTURAL PRINCIPLES APPROXIMATE ANALYSIS ARCHITECTURAL PRINCIPLES ARM TRUSTZONE ARM TRUSTZONE ARTIFACTS AND FRAGMENTS ASSESSMENT CRITERIA USABLE SECURITY HIS ATTACK DETECTION MALWARE DETECTION MALWARE DETECTION MALWARE DETECTION MALWARE DETECTION MALYSIS ATTACK SURFACE ATTACK SURFACE ATTACK SURFACE ATTACK FREES MODELS ATTACK TREES ATTACK TYPES ATTACKER MODELS ATTACK TREES ATTACKER MODELS ATTACK TREES ATTACKER MODELS ATTACK SURFACE ATTACK SURFACE ATTACKER MODELS ATTACK SURFACE ATTACKER MODELS ATTACK SURFACE ATTACKER MODELS	API DESIGN	PREVENTION OF VULNERABILITIES	SS
APPLICATION GATEWAY APPLICATION LAYER SECURITY INTERNET ARCHITECTURE APPLICATION LOGS: WEB SERVER LOGS AND FILES APPLICATION STORES FUNDAMENTAL CONCEPTS AND APPROACHES APPLICATION STORES FUNDAMENTAL CONCEPTS AND APPROACHES APPLING FOR THE CYBERSPACE AND INFORMATION TECHNOLOGIES APPLYING FOR THE CYBERSPACE AND INFORMATION TECHNOLOGIES APPLICATION THE CYBERSPACE AND APPROACHES APPLICATION TO THE CYBERSPACE AND APPROACHES APPLICATION AND APPLICATION TO A STATE UN- DER INTERNATIONAL LAW ATTRIBUTION AND IDENTIFICA- TORMATION AND IDENTIFICA- TON AUTHENTICATION AND MEDIATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION AND DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION AND MEDIATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATI	API VULNERABILITIES	CATEGORIES OF VULNERABILITIES	SS
APPLICATION LAYER SECURITY INTERNET ARCHITECTURE NA APPLICATION LOGS: WEB SERVER LOGS MONITOR: DATA SOURCES AND FILES APPLICATION STORES FUNDAMENTAL CONCEPTS AND APPROACHES WAN AND FILES APPLICATION STORES FUNDAMENTAL CONCEPTS AND APPROACHES APPLYING FOR THE CYBERSPACE AND INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH INTRODUC	APPIFICATION	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
APPLICATION LOGS: WEB SERVER LOGS AND FILES APPLICATION STORES APPLICATION STORES APPLYING FOR THE CYBERSPACE AND INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH INFORMATION TECHNOLOGIES APPROXIMATE ANALYSIS ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS AND APPROACHES APPROXIMATE ANALYSIS ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS ARM TRUSTZONE HARDWARE SUPPORT FOR SOFTWARE SECURITY HE ARTIFACTS AND FRAGMENTS MAIN MEMORY FORENSICS INTRODUCTORY ASSESSMENT CRITERIA USABLE SECURITY HAITACK DETECTION MALWARE DETECTION MALWARE DETECTION MALWARE DETECTION MATTACK ON CONFIDENTIALITY, IN- MALICIOUS ACTIVITIES BY MALWARE MATTACK SURFACE ATTACK REES MODELS ATTACK TREES MODELS ATTACKER MODELS ATTACKER MODELS ATTACKER MODELS ATTACKER MODELS ATTACKER MODELS ATTACKS AND THEIR MITIGATION ATTACKS AND THEIR MITIGATION ATTACKS ON PHYSICAL LAYER IDENTI- FICATION ATTARIBUTING ACTION TO A STATE UN- DER INTERNATIONAL LAW ATTRIBUTION ATTRIBUTION ATTRIBUTION ATTRIBUTION ATTRIBUTION MALWARE RESPONSE MAA AUDIT-BASED TRANSPARENCY TRANSPARENCY POR AUTHENTICATION AND IDENTIFICA- TION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS-	APPLICATION GATEWAY	NETWORK DEFENCE TOOLS	NS
AND FILES APPLICATION STORES ARTIFACT ANALYSIS AR	APPLICATION LAYER SECURITY	INTERNET ARCHITECTURE	NS
APPLYING FOR THE CYBERSPACE AND INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH INFORMATION TECHNOLOGIES APPROXIMATE ANALYSIS ARTIFACT ANALYSIS SOIM ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS SOIM ARM TRUSTZONE HARDWARE SUPPORT FOR SOFTWARE SECURITY HIS ARTIFACTS AND FRAGMENTS MAIN MEMORY FORENSICS INTRODUCTORY PRINCIPLES BY MAIN MEMORY FORENSICS INTRODUCTORY PRINCIPLES BY MAIN MEMORY FOR SOFTWARE SECURITY HIS ASSESSMENT CRITERIA USABLE SECURITY HIS ATTACK ON CONFIDENTIALITY, INMALICIOUS ACTIVITIES BY MALWARE MATTACK ON CONFIDENTIALITY, INMALICIOUS ACTIVITIES BY MALWARE MATTACK SURFACE ATTACKER MODEL OSTATACK RESES MODELS ATTACK TREES MODELS ATTACK TREES MODELS MODELS ATTACK TYPES ATTACKING P2P SYSTEMS DSS ATTACKER MODELS MODELLING AND ABSTRACTION FIMS ATTACKS ON PHYSICAL LAYER IDENTIFICATION ATTACKING P2P SYSTEMS DSS ATTACKS ON PHYSICAL LAYER IDENTIFICATION PLEICATION PLEICATION PLEICATION PLEICATION MODELS ATTRIBUTION ATTRIBUTION AND ASTATE UNDER INTERNATIONAL LAW ATTRIBUTION MODELS ATTRIBUTION MODELS ATTRIBUTION MALWARE RESPONSE MATTRIBUTION MALWARE RESPONSE MATTRIBUTION MALWARE RESPONSE MATTRIBUTION AND IDENTIFICATION FUNDAMENTAL CONCEPTS AND APPROACHES WAN AUTHENTICATION AND IDENTIFICATION PUNDAMENTAL CONCEPTS AND APPROACHES WAN AUTHENTICATION AND IDENTIFICATION PUNDAMENTAL CONCEPTS AND APPROACHES WAN AUTHENTICATION AND IDENTIFICATION PUNDAMENTAL CONCEPTS AND APPROACHES WAN AUTHENTICATION IN DISTRIBUTED SYS-AUTHENTICATION		MONITOR: DATA SOURCES	SOIM
INFORMATION TECHNOLOGIES APPROXIMATE ANALYSIS APPROXIMATE ANALYSIS ARCHITECTURAL PRINCIPLES FUNDAMENTAL CONCEPTS SOIN ARM TRUSTZONE HARDWARE SUPPORT FOR SOFTWARE SECURITY HE ARTIFACTS AND FRAGMENTS MAIN MEMORY FORENSICS I ASSESSMENT CRITERIA USABLE SECURITY HI ATTACK DETECTION MALWARE DETECTION MALWARE DETECTION MALYON CONFIDENTIALITY, IN- TEGRITY, AVAILABILITY ATTACK ON CONFIDENTIALITY, IN- TEGRITY, AVAILABILITY ATTACK SURFACE ATTACKER MODEL ATTACK TREES MODELS ATTACK TREES ATTACKING P2P SYSTEMS ATTACKER MODELS ATTACKS AND THEIR MITIGATION ATTACKS ON PHYSICAL LAYER IDENTI- FICATION ATTRIBUTING ACTION TO A STATE UNDER INTERNATIONAL LAW ATTRIBUTION ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION MODELS ATTRIBUTION ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION MODELS ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION ATTRIBUTION MALWARE RESPONSE MAA AUDITERNATIONAL LAW AUTHENTICATION FUNDAMENTAL CONCEPTS AND APPROACHES WAN AUTHENTICATION AND IDENTIFICA- TION AUTHENTICATION AND IDENTIFICA- TION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AND MEDIATION AND MEDIATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICAT	APPLICATION STORES	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
ARCHITECTURAL PRINCIPLES ARTHOUGH HARDWARE SUPPORT FOR SOFTWARE SECURITY ARTIFACTS AND FRAGMENTS ASSESSMENT CRITERIA ATTACK DETECTION ATTACK ON CONFIDENTIALITY, INMALICIOUS ACTIVITIES BY MALWARE ATTACK SURFACE ATTACK SURFACE ATTACK TREES ATTACK TYPES ATTACKS MODELS ATTACKS ATTA		INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH	LR
ARM TRUSTZONE ARTIFACTS AND FRAGMENTS MAIN MEMORY FORENSICS ASSESSMENT CRITERIA USABLE SECURITY HI ATTACK DETECTION MALWARE DETECTION MALWARE DETECTION MALWARE DETECTION MALWARE ATTACK ON CONFIDENTIALITY, IN- TEGRITY, AVAILABILITY ATTACK SURFACE ATTACK RODEL ATTACK TREES MODELS ATTACK TREES MODELS ATTACKER MODELS ATTACKER MODELS ATTACKS MODELS ATTACKS SIDE CHANNEL ATTACKS AND FAULT ATTACKS HIS ATTACKS ON PHYSICAL LAYER IDENTI- FICATION ATTRIBUTION ATTRIBUTION ATTRIBUTION MODELS ATTR	APPROXIMATE ANALYSIS	ARTIFACT ANALYSIS	F
ARTIFACTS AND FRAGMENTS ASSESSMENT CRITERIA ATTACK DETECTION MALWARE DETECTION MALWARE DETECTION MALWARE DETECTION MALTACK ON CONFIDENTIALITY, IN- ATTACK ON CONFIDENTIALITY, IN- ATTACK ON CONFIDENTIALITY, IN- ATTACK SURFACE ATTACKER MODEL ATTACK TREES ATTACK TREES ATTACK TYPES ATTACKING P2P SYSTEMS ATTACKER MODELS ATTACKS AND FAULT ATTACKS ATTACKS ATTACKS ATTACKS AND FAULT ATTACKS ATTACKS AND FAULT ATTA	ARCHITECTURAL PRINCIPLES	FUNDAMENTAL CONCEPTS	SOIM
ASSESSMENT CRITERIA ASSESSMENT CRITERIA ATTACK DETECTION MALWARE DETECTION MALWARE DETECTION MALICIOUS ACTIVITIES BY MALWARE MATTACK ON CONFIDENTIALITY, IN- MALICIOUS ACTIVITIES BY MALWARE MATTACK SURFACE ATTACKE MODEL ATTACK TREES ATTACK TYPES ATTACKING P2P SYSTEMS ATTACKER MODELS ATTACKS ATTACKS ATTACKS AND ABSTRACTION FMS ATTACKS ATTACKS AND THEIR MITIGATION ATTACKS ON PHYSICAL LAYER IDENTI- FICATION ATTRIBUTING ACTION TO A STATE UN- DER INTERNATIONAL LAW ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION MODELS ATTRIBUTION MODELS ATTRIBUTION MODELS ATTRIBUTION MALWARE RESPONSE AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION AND IDENTIFICA- TION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AND AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUT	ARM TRUSTZONE	HARDWARE SUPPORT FOR SOFTWARE SECURITY	HS
ATTACK DETECTION ATTACK ON CONFIDENTIALITY, IN- ATTACK ON CONFIDENTIALITY, IN- ATTACK ON CONFIDENTIALITY, IN- ATTACK SURFACE ATTACK SURFACE ATTACKER MODEL ATTACK TREES ATTACK TYPES ATTACKING P2P SYSTEMS ATTACKER MODELS ATTACKER MODELS ATTACKER MODELS ATTACKS ATTACKS SIDE CHANNEL ATTACKS AND FAULT ATTACKS HS ATTACKS ON PHYSICAL LAYER IDENTI- FICATION ATTRIBUTING ACTION TO A STATE UN- DER INTERNATIONAL LAW ATTRIBUTION ATTRIBUTION MODELS ATTACKS ON DELS ATTACKS ON DELS ATTACKS ON BATTACKS ON BATTACKS ON BATTACKS ON BATTACKS AUTHENTICATION ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION MALWARE RESPONSE MATTACKS ON BATTACKS ON B	ARTIFACTS AND FRAGMENTS	MAIN MEMORY FORENSICS	F
ATTACK ON CONFIDENTIALITY, IN- TEGRITY, AVAILABILITY ATTACK SURFACE ATTACKER MODEL ATTACK TREES ATTACK TYPES ATTACKING P2P SYSTEMS ATTACKER MODELS ATTACKS SIDE CHANNEL ATTACKS AND FAULT ATTACKS HIS ATTACKS AND THEIR MITIGATION ATTACKING P2P SYSTEMS DSS ATTACKS ON PHYSICAL LAYER IDENTI- FICATION ATTRIBUTING ACTION TO A STATE UN- DER INTERNATIONAL LAW ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION MODELS ATTRIBUTION MALWARE RESPONSE MATACKS AND APPROACHES WAN AUTHENTICATION AND IDENTIFICA- TION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AAAA AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION AAAA AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AAAAA AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	ASSESSMENT CRITERIA	USABLE SECURITY	HF
TEGRITY, AVAILABILITY ATTACK SURFACE ATTACKER MODELS ATTACK TREES MODELS ATTACKING P2P SYSTEMS ATTACKER MODELS ATTACKER MODELS ATTACKER MODELS ATTACKER MODELS ATTACKER MODELS ATTACKS MODELLING AND ABSTRACTION FMS ATTACKS ATTACKS SIDE CHANNEL ATTACKS AND FAULT ATTACKS HS ATTACKS AND THEIR MITIGATION ATTACKS ON PHYSICAL LAYER IDENTI- FICATION ATTRIBUTING ACTION TO A STATE UN- DER INTERNATIONAL LAW ATTRIBUTION MODELS ATTRIBUTION MODELS ATTRIBUTION MALWARE RESPONSE MATACKS AND APPROACHES MATACKS ON PHYSICAL CONCEPTS AND APPROACHES MATACKS ON PHYSICAL CONCEPTS AND MACHORITHM AND MEDIATION AUTHENTICATION AND IDENTIFICA- PRIMITIVES FOR ISOLATION AND MEDIATION OSTATACTOR OF STATE AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AAAA AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AAAA AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AAAA AUTHENTICATION AAAA AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AAAA A	ATTACK DETECTION	MALWARE DETECTION	MAT
ATTACK TREES ATTACK TYPES ATTACKING P2P SYSTEMS DSS ATTACKER MODELS ATTACKER MODELS ATTACKS ATTACKS ATTACKS SIDE CHANNEL ATTACKS AND FAULT ATTACKS ATTACKS AND THEIR MITIGATION ATTACKS ON PHYSICAL LAYER IDENTI- FICATION ATTRIBUTING ACTION TO A STATE UN- DER INTERNATIONAL LAW ATTRIBUTION ATTRIBUTION ATTRIBUTION ATTRIBUTION ATTRIBUTION ATTRIBUTION ATTRIBUTION ATTRIBUTION AUDIT-BASED TRANSPARENCY AUDIT-BASED TRANSPARENCY AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION AND IDENTIFICA- PRIMITIVES FOR ISOLATION AND MEDIATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS-	•	MALICIOUS ACTIVITIES BY MALWARE	MAT
ATTACK TYPES ATTACKING P2P SYSTEMS DS3 ATTACKER MODELS ATTACKER MODELS ATTACKS SIDE CHANNEL ATTACKS AND FAULT ATTACKS ATTACKS AND THEIR MITIGATION ATTACKS ON PHYSICAL LAYER IDENTI- FICATION ATTRIBUTING ACTION TO A STATE UN- DER INTERNATIONAL LAW ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION MALWARE RESPONSE AUDIT-BASED TRANSPARENCY AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENT	ATTACK SURFACE	ATTACKER MODEL	osv
ATTACKER MODELS ATTACKS ATTACKS ATTACKS ATTACKS AND THEIR MITIGATION ATTACKING P2P SYSTEMS DSS ATTACKS ON PHYSICAL LAYER IDENTI- FICATION ATTRIBUTING ACTION TO A STATE UN- DER INTERNATIONAL LAW ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION MODELS ATTRIBUTION MALWARE RESPONSE AUDIT-BASED TRANSPARENCY AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION AND IDENTIFICA- TION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICA	ATTACK TREES	MODELS	AB
ATTACKS SIDE CHANNEL ATTACKS AND FAULT ATTACKS ATTACKS AND THEIR MITIGATION ATTACKING P2P SYSTEMS DSS ATTACKS ON PHYSICAL LAYER IDENTI- FICATION ATTRIBUTING ACTION TO A STATE UN- DER INTERNATIONAL LAW ATTRIBUTION MODELS ATTRIBUTION MALWARE RESPONSE AUDIT-BASED TRANSPARENCY AUTHENTICATION AUTHENTICATION AND IDENTIFICA- TION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATIO	ATTACK TYPES	ATTACKING P2P SYSTEMS	DSS
ATTACKS AND THEIR MITIGATION ATTACKING P2P SYSTEMS ATTACKS ON PHYSICAL LAYER IDENTIFICATION ATTRIBUTING ACTION TO A STATE UNDER INTERNATIONAL LAW ATTRIBUTION ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION MALWARE RESPONSE AUDIT-BASED TRANSPARENCY AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION	ATTACKER MODELS	MODELLING AND ABSTRACTION	FMS
ATTACKS ON PHYSICAL LAYER IDENTI- FICATION ATTRIBUTING ACTION TO A STATE UN- DER INTERNATIONAL LAW ATTRIBUTION MODELS ATTRIBUTION MALWARE RESPONSE AUDIT-BASED TRANSPARENCY AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION AUTHENTICATION AAA AUTHENTICATION AAA AUTHENTICATION AAA AAA AAA AUTHENTICATION AAA AAA AAA AUTHENTICATION AAA AAA AAA AAA AUTHENTICATION AAA AAA AAA AAA AAA ACTION ACTION AAA ACTION ACTIO	ATTACKS	SIDE CHANNEL ATTACKS AND FAULT ATTACKS	HS
FICATION ATTRIBUTING ACTION TO A STATE UNDER INTERNATIONAL LAW DER INTERNATIONAL LAW ATTRIBUTION ATTRIBUTION MODELS ATTRIBUTION MALWARE RESPONSE AUDIT-BASED TRANSPARENCY AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AAAA AAAA AAAA AAAA AAAA AAAA ACTION	ATTACKS AND THEIR MITIGATION	ATTACKING P2P SYSTEMS	DSS
DER INTERNATIONAL LAW ATTRIBUTION MODELS ATTRIBUTION MALWARE RESPONSE MATAINSPARENCY AUDIT-BASED TRANSPARENCY TRANSPARENCY AUTHENTICATION FUNDAMENTAL CONCEPTS AND APPROACHES WAN AUTHENTICATION AND IDENTIFICA- PRIMITIVES FOR ISOLATION AND MEDIATION OST TION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AAA		IDENTIFICATION	PLT
ATTRIBUTION MALWARE RESPONSE MACTOR AUDIT-BASED TRANSPARENCY TRANSPARENCY PORT AUTHENTICATION FUNDAMENTAL CONCEPTS AND APPROACHES WAN AUTHENTICATION AND IDENTIFICA-PRIMITIVES FOR ISOLATION AND MEDIATION OST TION AUTHENTICATION IN DISTRIBUTED SYS-AUTHENTICATION AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		PUBLIC INTERNATIONAL LAW	LR
AUDIT-BASED TRANSPARENCY TRANSPARENCY TRANSPARENCY AUTHENTICATION AND IDENTIFICA- PRIMITIVES FOR ISOLATION AND MEDIATION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AAA AAA AUTHENTICATION AAA AAA AAA AAA AAA AAA AAA	ATTRIBUTION	MODELS	AB
AUTHENTICATION FUNDAMENTAL CONCEPTS AND APPROACHES AUTHENTICATION AND IDENTIFICA- PRIMITIVES FOR ISOLATION AND MEDIATION OSV TION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AAA	ATTRIBUTION	MALWARE RESPONSE	MAT
AUTHENTICATION AND IDENTIFICA- PRIMITIVES FOR ISOLATION AND MEDIATION OSI AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AAA	AUDIT-BASED TRANSPARENCY	TRANSPARENCY	POR
TION AUTHENTICATION IN DISTRIBUTED SYS- AUTHENTICATION AAA	AUTHENTICATION	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
7.6 7.1 <u>-</u> 1.7 7.6 7.1 6.7 7.6 7.1 6.7 7.6 7.1 6.7 7.6 7.1 6.7 7.6 7.1 6.7 7.6 7.1 6.7 7.6 7.1 6.7 7.6 7.1 6.7 7.6 7.1 6.7 7.1		PRIMITIVES FOR ISOLATION AND MEDIATION	osv
TEMO	AUTHENTICATION IN DISTRIBUTED SYSTEMS	AUTHENTICATION	AAA



INDICATIVE MATERIAL	TOPIC	CyBOK KA
AUTOMATED SOFTWARE DIVERSITY	MITIGATING EXPLOITATION	SS
В		
BASIC SECURITY DEFINITIONS	CRYPTOGRAPHIC SECURITY MODELS	С
BLIND SIGNATURES	PUBLIC-KEY SCHEMES WITH SPECIAL PROPERTIES	С
BLOCK DEVICE ANALYSIS	OPERATING SYSTEM ANALYSIS	F
BLOCK-LEVEL ANALYSIS	ARTIFACT 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
С		
CAPABILITIES	PRIMITIVES FOR ISOLATION AND MEDIATION	osv
CASE STUDY: E.G., WEB BROWSERS	APPLICATION FORENSICS	F
CATALOGUE OF INTELLECTUAL PROP- ERTY RIGHT	INTELLECTUAL PROPERTY	LR
CELLULAR NETWORKS	PHYSICAL LAYER SECURITY OF SELECTED COMMUNI- CATIONS TECHNOLOGIES	PLT
CENSORSHIP RESISTANCE AND FREE- DOM OF SPEECH	PRIVACY TECHNOLOGIES AND DEMOCRATIC VALUES	POR
CHALLENGES OF LIVE FORENSICS	MAIN MEMORY FORENSICS	F
CHARACTERISTICS	CYBER-PHYSICAL SYSTEMS	CPS
CIRCUIT LEVEL GATEWAY	NETWORK DEFENCE TOOLS	NS
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 COMMUNICA- TIONS	PLT
CLICKJACKING	CLIENT-SIDE VULNERABILITIES AND MITIGATION	WAM
CLIENT-SIDE STORAGE	CLIENT-SIDE VULNERABILITIES AND MITIGATION	WAM
CLOUD COMPUTING	ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE	SSL
CLOUD-NATIVE ARTIFACTS	ARTIFACT ANALYSIS	F
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
COMMON NETWORK ATTACKS	NETWORK PROTOCOLS AND VULNERABILITY	NS
COMPLETENESS	DETECTION OF VULNERABILITIES	SS
COMPONENT VERSUS SYSTEM PER- SPECTIVES	RISK ASSESSMENT AND MANAGEMENT PRINCIPLES	RMG
COMPROMISING EMANATIONS	COMPROMISING EMANATIONS AND SENSOR SPOOF-ING	PLT
CONCEPTUAL MODELS	DEFINITION AND CONCEPTUAL MODELS	F
CONFLICT OF LAW - ELECTRONIC SIGNATURE AND TRUST SERVICE	DEMATERIALISATION OF DOCUMENTS AND ELEC- TRONIC TRUST SERVICE	LR
CONFLICTS OF LAW-CONTRACTS	CONTRACT	LR
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 SER- VICES	CLASSES OF DISTRIBUTED SYSTEMS	DSS



INDICATIVE MATERIAL	TOPIC	CyBOK K
COORDINATED SPREAD SPECTRUM TECHNIQUES	JAMMING AND JAMMING-RESILIENT COMMUNICA- TIONS	PĽ
COORDINATION PRINCIPLES	COORDINATED RESOURCE CLUSTERING	DS
CORE CONCEPTS	ACCESS CONTROL IN DISTRIBUTED SYSTEMS	AA
CORE REGULATORY PRINCIPLES	DATA PROTECTION	LI
COUNTERMEASURES	SIDE CHANNEL ATTACKS AND FAULT ATTACKS	H
COUNTERMEASURES	JAMMING AND JAMMING-RESILIENT COMMUNICA- TIONS	PĽ
CRIME AGAINST INFORMATION SYS- TEM	COMPUTER CRIME	Ц
CRIMINAL LAW	INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH	LI
CROSS-BORDER CRIMINAL INVESTIGA- TION	PUBLIC INTERNATIONAL LAW	Ц
CRYPTOGRAPHIC ALGORITHMS AT RTL LEVEL	HARDWARE DESIGN FOR CRYPTOGRAPHIC ALGO- RITHMS	H
CRYPTOGRAPHIC HASHING	ARTIFACT ANALYSIS	1
CRYPTOGRAPHY AND ACCESS CONTROL	ACCESS CONTROL IN DISTRIBUTED SYSTEMS	AA
CUSTOMERS DON'T APPLY PATCHES	MOTIVATIONS FOR SECURE SOFTWARE LIFECYCLE	SS
CVES AND CWES	CATEGORIES OF VULNERABILITIES	S
CYBER CONFLICT	POLICY AND POLITICAL ASPECTS	CPS
CYBER DOMAIN	DEFINITION AND CONCEPTUAL MODELS	I
CYBER ESPIONAGE IN PEACETIME	PUBLIC INTERNATIONAL LAW	LI
CYBER KILL CHAIN	MALICIOUS ACTIVITIES BY MALWARE	MA
CYBER SECURITY KNOWLEDGE MAN- AGEMENT	KNOWLEDGE: INTELLIGENCE AND ANALYSIS	SOIN
CYBER-DEPENDENT ORGANISED CRIME	CHARACTERISATION OF ADVERSARIES	Al
CYBER-ENABLED CRIME VS CYBER- DEPENDENT CRIME	CHARACTERISATION OF ADVERSARIES	Al
CYBER-ENABLED ORGANISED CRIME	CHARACTERISATION OF ADVERSARIES	Al
CYBER-THREAT INTELLIGENCE	KNOWLEDGE: INTELLIGENCE AND ANALYSIS	SOIN
D		
DATA ACQUISITION	OPERATING SYSTEM ANALYSIS	
DATA COLLECTION	PLAN: SECURITY INFORMATION AND EVENT MANAGE- MENT	SOIN
DATA CONFIDENTIALITY	CONFIDENTIALITY	PO
DATA RECOVERY AND FILE CONTENT CARVING	OPERATING SYSTEM ANALYSIS	
DATA SECURITY	CLASSES OF VULNERABILITIES AND THREATS	DS
DATA SOVEREIGNTY	JURISDICTION	LI
DATA TRANSPORTATION	CLASSES OF VULNERABILITIES AND THREATS	DS
DATABASES	RELATED AREAS	OS
DE MINIMIS EXCEPTIONS TO CRIME AGAINST INFORMATION SYSTEM	COMPUTER CRIME	LI
DECENTRALISED POINT-TO-POINT IN- TERACTIONS ACROSS DISTRIBUTED EN- TITIES WITHOUT A CENTRALISED COOR- DINATION SERVICE	CLASSES OF DISTRIBUTED SYSTEMS	DS
DEFINITIONS	DEFINITION AND CONCEPTUAL MODELS	
DEFINITION OF CYBER SECURITY	FOUNDATIONAL CONCEPTS	C
DES	SCHEMES	(
DESIGN AND FABRICATION OF SILICON INTEGRATED CIRCUITS	HARDWARE DESIGN PROCESS	H
DESIGN CHOICES	ROLE OF OPERATING SYSTEMS	081
DESIGN PROCESS	HARDWARE DESIGN FOR CRYPTOGRAPHIC ALGO- RITHMS	H



INDICATIVE MATERIAL	TOPIC	CyBOK KA
DETECTING ATTACKS	CROSS CUTTING SECURITY	CPS
DEVICE CAPABILITIES AND LIMITA- TIONS	FITTING THE TASK TO THE HUMAN	HF
DEVICE FINGERPRINTS	IDENTIFICATION	PLT
DEVICE UNDER IDENTIFICATION	IDENTIFICATION	PLT
DIGITAL (FORENSIC) TRACE	DEFINITION AND CONCEPTUAL MODELS	F
DIMENSIONS	MALWARE TAXONOMY	MAT
DISRUPTING MALWARE OPERATIONS	MALWARE RESPONSE	MAT
DISTANCE BOUNDING PROTOCOLS	DISTANCE BOUNDING AND SECURE POSITIONING	PLT
DISTANCE MEASUREMENT TECH- NIQUES	DISTANCE BOUNDING AND SECURE POSITIONING	PLT
DISTRIBUTED LOGS	ACCOUNTABILITY	AAA
DOLEV-YAO ADVERSARIAL MODEL	NETWORK PROTOCOLS AND VULNERABILITY	NS
DSA	SCHEMES	С
DYNAMIC DETECTION	DETECTION OF VULNERABILITIES	SS
E		001
E-COMMERCE	ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE	SSL
EFFECTS OF CONTRACTS AND NON- CONTRACTING PARTIES	CONTRACT	LR
ELECTRIC POWER GRIDS	CYBER-PHYSICAL SYSTEMS DOMAINS	CPS
ELECTRONIC SIGNATURE AND IDEN- TITY TRUST SERVICE	DEMATERIALISATION OF DOCUMENTS AND ELEC- TRONIC TRUST SERVICE	LR
ELEMENTS OF RISK	RISK ASSESSMENT AND MANAGEMENT PRINCIPLES	RMG
EMBRACING SECURITY	RELATED AREAS	OSV
EMPLOYEES	STAKEHOLDER ENGAGEMENT	HF
ENACTING SECURITY POLICY	RISK GOVERNANCE	RMG
ENCOURAGING SECURITY STANDARDS VIA CONTRACT	CONTRACT	LR
ENFORCEMENT AND PENALTIES	DATA PROTECTION	LR
ENFORCEMENT JURISDICTION	JURISDICTION	LR
ENFORCEMENT OF PRIVACY LAWS	PRIVACY LAW IN GENERAL AND ELECTRONIC INTER- CEPTION	LR
ENFORCEMENT-REMEDIES	INTELLECTUAL PROPERTY	LR
ENFORCING ACCESS CONTROL	AUTHORISATION	AAA
ENVIRONMENTAL CRIMINOLOGY	MODELS	AB
EQUIVALENCE-BASED	ANALYSIS AND VERIFICATION	FMS
ERRONEOUS EXECUTION	PREVENTION OF VULNERABILITIES	SS
EVASION AND COUNTERMEASURES	MALWARE DETECTION	MAT
EVIDENCE AND PROOF	INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH	LR
FACETS OF AUTHENTICATION	AUTHENTICATION	AAA
FACETS OF AUTHENTICATION		CI
FAILURES AND INCIDENTS FEAR UNCERTAINTY AND DOUBT	FOUNDATIONAL CONCEPTS 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
FLOW OF CAPITAL	MODELS	AB
FOLLOW UP: POST INCIDENT ACTIVITIES	HUMAN FACTORS: INCIDENT MANAGEMENT	SOIM
FORENSIC SCIENCE	DEFINITION AND CONCEPTUAL MODELS	F
I ONLINGIO GOILINGE		



INDICATIVE MATERIAL	TOPIC	СуВОК КА
FORMAL VERIFICATION	OS HARDENING	osv
FREAK SSL/TLS VULNERABILITY	REAL-WORLD EXAMPLES	FMS
FREQUENT SOFTWARE UPDATES	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
FRIENDLY JAMMING	SCHEMES FOR CONFIDENTIALITY, INTEGRITY AND ACCESS CONTROL	PLT
FULLY HOMOMORPHIC ENCRYPTION FUNCTIONAL ELEMENTS	PUBLIC-KEY SCHEMES WITH SPECIAL PROPERTIES ATTACKING P2P SYSTEMS	C DSS
G		
GAME-BASED	ANALYSIS AND VERIFICATION	FMS
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 MODEL	RISK GOVERNANCE	RMG
GROUP SIGNATURES	PUBLIC-KEY SCHEMES WITH SPECIAL PROPERTIES	С
GRSECURITY	EMBRACING SECURITY	OSV
H		
HACKTIVISTS	CHARACTERISATION OF ADVERSARIES	AB
HANDLE: ACTUAL INCIDENT RESPONSE	HUMAN FACTORS: INCIDENT MANAGEMENT	SOIM
HARD PROBLEMS	CRYPTOGRAPHIC SECURITY MODELS	С
HARDWARE DESIGN PROCESS	HARDWARE DESIGN CYCLE	HS
HARDWARE SECURITY MODULE (HSM)	SECURE PLATFORMS	HS
HIERARCHICAL P2P PROTOCOLS	DECENTRALISED P2P MODELS	DSS
HOLISTIC APPROACH 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 LIMITA- TIONS	FITTING THE TASK TO THE HUMAN	HF
HUMAN FACTOR AND RISK COMMUNI- CATION	RISK GOVERNANCE	RMG
HUMAN SERVICES	ELEMENTS OF A MALICIOUS OPERATION	AB
HYBRID P2P PROTOCOLS	DECENTRALISED P2P MODELS	DSS
1		
IBM 4578 SECURE CO-PROCESSOR	HARDWARE SUPPORT FOR SOFTWARE SECURITY	HS
IDENTIFICATION SIGNALS	IDENTIFICATION	PLT
IDENTIFYING THE ANALYSIS ENVIRON- MENT	MALWARE ANALYSIS	MAT
IDENTIFYING THE PRESENCE OF MAL- WARE	MALWARE DETECTION	MAT
IDENTITY MANAGEMENT	AUTHENTICATION	AAA
IDENTITY-BASED ENCRYPTION	PUBLIC-KEY SCHEMES WITH SPECIAL PROPERTIES	С
INCENTIVES AND REGULATION	POLICY AND POLITICAL ASPECTS	CPS
INDUSTRIAL CONTROL SYSTEMS	CYBER-PHYSICAL SYSTEMS DOMAINS	CPS
INDUSTRY PRACTICES AND STAN- DARDS	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 HARDENING	OS HARDENING	OSV
INFRASTRUCTURE	ELEMENTS OF A MALICIOUS OPERATION	AB
INJECTION VULNERABILITIES	SERVER-SIDE VULNERABILITIES AND MITIGATIONS	WAM



INDICATIVE MATERIAL	TOPIC	CyBOK K
INTERACTION CONTEXT	FITTING THE TASK TO THE HUMAN	F
INTERCEPTION BY A STATE	PRIVACY LAW IN GENERAL AND ELECTRONIC INTER- CEPTION	ı
INTERCEPTION BY PERSON OTHER THAN STATE	PRIVACY LAW IN GENERAL AND ELECTRONIC INTER- CEPTION	l
INTERNATIONAL NORMS	PRIVACY LAW IN GENERAL AND ELECTRONIC INTER- CEPTION	l
INTERNATIONAL TREATMENTS AND CONFLICT OF LAW	INTELLECTUAL PROPERTY	l
INTERNET OF THINGS	CYBER-PHYSICAL SYSTEMS DOMAINS	CF
INTERNET OF THINGS SECURITY	ADVANCED NETWORK SECURITY TOPICS	N
INTERPERSONAL CRIMES	CHARACTERISATION OF ADVERSARIES	Į.
INTRUSION DETECTION SYSTEMS	NETWORK DEFENCE TOOLS	1
INTRUSION PREVENTION SYSTEMS	EXECUTE: MITIGATION AND COUNTERMEASURES	SOI
INTRUSION PREVENTION SYSTEMS	NETWORK DEFENCE TOOLS	1
INVESTIGATION AND PREVENTION OF CRIME	DATA PROTECTION	l
IOT	ROLE OF OPERATING SYSTEMS	08
IOT	ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE	S
ISO/IEC 27034	BUSINESS CONTINUITY: INCIDENT RESPONSE AND RECOVERY PLANNING	RM
ISOLATION	ROLE OF OPERATING SYSTEMS	0
K		
KERBEROS	SCHEMES	
KEY AGREEMENT PROTOCOLS	STANDARD PROTOCOLS	
KEY ESTABLISHMENT BASED ON CHAN- NEL RECIPROCITY	SCHEMES FOR CONFIDENTIALITY, INTEGRITY AND ACCESS CONTROL	Р
KILL CHAINS	MODELS	
KINDS	MALWARE TAXONOMY	M
L		
LANGUAGE DESIGN AND TYPE SYS- TEMS	PREVENTION OF VULNERABILITIES	•
LATENT DESIGN CONDITIONS	PRINCIPLES	
LATENT USABILITY FAILURES IN SYSTEMS-OF-SYSTEMS	HUMAN ERROR	ı
LEGAL CONCERNS AND THE DAUBERT STANDARD	DEFINITION AND CONCEPTUAL MODELS	
LEVELS OF PERCEIVED RISK	RISK DEFINITION	RM
LIABILITY AND COURTS	INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH	ı
LIGHTWEIGHT SOLUTIONS	HARDWARE SUPPORT FOR SOFTWARE SECURITY	H
LIMITATION OF LIABILITY AND EXCLU- SIONS OF LIABILITY	CONTRACT	I
LIMITING PRIVILEGES	MITIGATING EXPLOITATION	,
LINEARLY HOMOMORPHIC ENCRYP- TION	PUBLIC-KEY SCHEMES WITH SPECIAL PROPERTIES	
LINK LAYER SECURITY	INTERNET ARCHITECTURE	1
LONG TERM MEMORY	FITTING THE TASK TO THE HUMAN	ı
LOW-END DEVICES AND IOT	PRIMITIVES FOR ISOLATION AND MEDIATION	05
LPI AND COVERT COMMUNICATION	SCHEMES FOR CONFIDENTIALITY, INTEGRITY AND ACCESS CONTROL	P
M		
M MACHINE LEARNING	ANALYSE: ANALYSIS METHODS	SOI



INDICATIVE MATERIAL	TOPIC	СуВОК К
MEDIATION	ROLE OF OPERATING SYSTEMS	os
MEDICAL DEVICES	CYBER-PHYSICAL SYSTEMS DOMAINS	СР
MEMORY MANAGEMENT VULNERABILI- TIES	CATEGORIES OF VULNERABILITIES	S
MEMORY PROTECTION AND ADDRESS SPACES	PRIMITIVES FOR ISOLATION AND MEDIATION	os
MENTAL MODEL OF CYBER RISK AND DEFENCES	AWARENESS AND EDUCATION	Н
MENTAL MODELS OF SECURITY	USABLE SECURITY	Н
METADATA CONFIDENTIALITY	CONFIDENTIALITY	PO
MICROSOFT SDL	PRESCRIPTIVE PROCESSES	SS
MIMO-SUPPORTED APPROACHES	SCHEMES FOR CONFIDENTIALITY, INTEGRITY AND ACCESS CONTROL	PL
MISUSE DETECTION	ANALYSE: ANALYSIS METHODS	SOII
MITIGATING ATTACKS	CROSS CUTTING SECURITY	СР
MOBILE	ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE	SS
MODEL-CHECKING TOOLS	TOOLS	FM
MODERN HARDWARE EXTENSIONS FOR MEMORY PROTECTION	PRIMITIVES FOR ISOLATION AND MEDIATION	os
MULTICS	PRIMITIVES FOR ISOLATION AND MEDIATION	os
N		
NATURE OF LAW AND LEGAL ANALYSIS	INTRODUCTORY PRINCIPLES OF LEGAL RESEARCH	L
NCSC GUIDANCE	BUSINESS CONTINUITY : INCIDENT RESPONSE AND RE- COVERY PLANNING	RM
NEEDS OF SPECIFIC GROUP	FITTING THE TASK TO THE HUMAN	Н
NETWORK AGGREGATES: NETFLOW	MONITOR: DATA SOURCES	SOII
NETWORK ARCHITECTURE DESIGN	NETWORK DEFENCE TOOLS	N
NETWORK CONNECTIONS	MAIN MEMORY FORENSICS	001
NETWORK INFRASTRUCTURE INFOR- MATION	MONITOR: DATA SOURCES	SOII
NETWORK LAYER SECURITY	INTERNET ARCHITECTURE	N
NETWORK TRAFFIC	MONITOR: DATA SOURCES	SOII
NEW APPROACHES	AWARENESS AND EDUCATION	Н
NEWER PRINCIPLES	OS SECURITY PRINCIPLES	08
NFC	PHYSICAL LAYER SECURITY OF SELECTED COMMUNI- CATIONS TECHNOLOGIES	Pl
NIST PRINCIPLES	PRINCIPLES	•
OBJECTIVES	HARDWARE SUPPORT FOR SOFTWARE SECURITY	н
OBJECTIVES OBJECTIVES OF CYBER SECURITY	FOUNDATIONAL CONCEPTS	
OBLIGATIONS OWED TO A CLIENT	ETHICS	Ľ
OBLIVIOUS TRANSFER	ADVANCED PROTOCOLS	_
ONE-TIME PAD	INFORMATION-THEORETICALLY SECURE CONSTRUC- TIONS	
ON-LINE CONTRACTS	CONTRACT	L
ORIGIN-BASED POLICIES	ACCESS CONTROL IN DISTRIBUTED SYSTEMS	AA
OTHER REAL-WORLD EXAMPLES	REAL-WORLD EXAMPLES	FM
P		
PACKET FILTERS	NETWORK DEFENCE TOOLS	N
PARTITIONING	OS HARDENING	os
PASSWORDS AND ALTERNATIVES	FUNDAMENTAL CONCEPTS AND APPROACHES	WA
PATCHING CAN INTRODUCE VULNERA- BILITIES	MOTIVATIONS FOR SECURE SOFTWARE LIFECYCLE	SS



INDICATIVE MATERIAL	TOPIC	СуВОК К
PAX TEAM	EMBRACING SECURITY	os
PAYMENT METHODS	ELEMENTS OF A MALICIOUS OPERATION	A
PEOPLE ARE NOT THE WEAKEST LINK	POSITIVE SECURITY	Н
PERMISSION DIALOG BASED ACCESS CONTROL	FUNDAMENTAL CONCEPTS AND APPROACHES	WAI
PERSONAL DATA BREACH NOTIFICA- TION	DATA PROTECTION	L
PHISHING	CLIENT-SIDE VULNERABILITIES AND MITIGATION'S	WA
PHYSICAL ACCESS AND SECURE DELE- TION	PRIMITIVES FOR ISOLATION AND MEDIATION	OS
PHYSICAL ATTACKS	CLIENT-SIDE VULNERABILITIES AND MITIGATION'S	WA
PHYSICAL LAYER ATTACKS ON SECURE DISTANCE MEASUREMENT	DISTANCE BOUNDING AND SECURE POSITIONING	Pl
PHYSICALLY UNCLONABLE FUNCTIONS (PUFS)	ENTROPY GENERATING BUILDING BLOCKS	Н
PKCS	SCHEMES	
POTENTIALLY UNWANTED PROGRAMS	MALWARE TAXONOMY	MA
PRECAUTIONARY PRINCIPLE	PRINCIPLES	(
PREPARE: INCIDENT MANAGEMENT PLANNING	HUMAN FACTORS: INCIDENT MANAGEMENT	SOII
PRESCRIPTIVE JURISDICTION	JURISDICTION	L
PREVENTING ATTACKS	CROSS CUTTING SECURITY	СР
PRINCIPLES	DECENTRALISED P2P MODELS	DS
PRIVACY AND ACCOUNTABILITY	ACCOUNTABILITY	AA
PRIVACY EVALUATION	PRIVACY ENGINEERING	PO
PRIVACY POLICY AS SUPPORT TO DEMOCRATIC POLITICAL SYSTEM	PRIVACY TECHNOLOGIES AND DEMOCRATIC VALUES	PO
PRIVACY POLICY INTERPRETABILITY	CONTROL	PO
PRIVACY POLICY NEGOTIATION	CONTROL	PO
PRIVACY SETTING CONFIGURATION	CONTROL	PO
PROCESS INFORMATION	MAIN MEMORY FORENSICS	
PROTECTED MODULE ARCHITECTURES	HARDWARE SUPPORT FOR SOFTWARE SECURITY	Н
PROTECTING DATA INTEGRITY	SCHEMES FOR CONFIDENTIALITY, INTEGRITY AND ACCESS CONTROL	Pl
PROTECTION AGAINST NATURAL EVENTS AND ACCIDENTS	CYBER-PHYSICAL SYSTEMS	СР
PROTECTION RINGS	PRIMITIVES FOR ISOLATION AND MEDIATION	OS
PUBLIC-KEY ENCRYPTION	PUBLIC-KEY CRYPTOGRAPHY	
PUBLIC-KEY SIGNATURES	PUBLIC-KEY CRYPTOGRAPHY	
R	DDEVENTION OF VIII NEDADII ITIEO	s
RACE CONDITION MITIGATION'S	PREVENTION OF VULNERABILITIES	s S
RACE CONDITION VULNERABILITIES	CATEGORIES OF VULNERABILITIES	S H
RANDOM NUMBER GENERATION REFINEMENT-BASED	ENTROPY GENERATING BUILDING BLOCKS ANALYSIS AND VERIFICATION	FM
REFINEMENT-BASED RELIABLE AND SECURE GROUP COM- MUNICATIONS	COORDINATED RESOURCE CLUSTERING	DS
REPLICATIONS REPLICATION MANAGEMENT AND CO- ORDINATION SCHEMA	COORDINATED RESOURCE CLUSTERING	DS
REQUIREMENTS OF FORM AND THE THREATS OF UNENFORCEABILITY	DEMATERIALISATION OF DOCUMENTS AND ELEC- TRONIC TRUST SERVICE	L
RESEARCH AND DEVELOPMENT ACTIV- ITIES CONDUCTED BY NON-STATE PER- SONS	COMPUTER CRIME	L
RESOURCE COORDINATION CLASS	COORDINATION CLASSES AND ATTACKABILITY	DS
RESOURCE MANAGEMENT AND COOR- DINATION SERVICES	CLASSES OF VULNERABILITIES AND THREATS	DS



INDICATIVE MATERIAL	TOPIC	CyBOK KA
RESTRICTIONS ON EXPORTING SECU- RITY TECHNOLOGIES	OTHER REGULATORY MATTERS	LR
REVERSE ENGINEERING	INTELLECTUAL PROPERTY	LR
RING SIGNATURES	PUBLIC-KEY SCHEMES WITH SPECIAL PROPERTIES	С
RISK ASSESSMENT AND MANAGEMENT METHODS	RISK ASSESSMENT AND MANAGEMENT PRINCIPLES	RMG
RISK ASSESSMENT AND MANAGEMENT METHODS IN CYBER PHYSICAL SYS- TEM	RISK ASSESSMENT AND MANAGEMENT PRINCIPLES	RMG
RISK ASSESSMENT	RISK DEFINITION	RMG
RISK MANAGEMENT	RISK DEFINITION	RMG
RISK MANAGEMENT	FOUNDATIONAL CONCEPTS	CI
RISK PERCEPTION FACTOR	RISK GOVERNANCE	RMG
ROAD VEHICLES	ADAPTATIONS OF SECURE SOFTWARE LIFECYCLE	SSL
ROBOTICS AND ADVANCED MANUFAC- TURING	CYBER-PHYSICAL SYSTEMS DOMAINS	CPS
ROOT OF TRUST	HARDWARE DESIGN CYCLE	HS
RSA	SCHEMES	С
RSN	WIRELESS LAN SECURITY	NS
RUN-TIME DETECTION OF ATTACKS	MITIGATING EXPLOITATION	SS
S		
SAAS FORENSICS	CLOUD FORENSICS	F
SAFE CODE	PRESCRIPTIVE PROCESSES	SSL
SALTZER AND SCHROEDER PRINCIPLES	OS SECURITY PRINCIPLES	OSV
SALTZER AND SCHROEDER PRINCIPLES	PRINCIPLES	CI
SAMM	ASSESS THE SECURE SOFTWARE LIFECYCLE	SSL
SANDBOXING	FUNDAMENTAL CONCEPTS AND APPROACHES	WAM
SECRECY CAPACITY	SCHEMES FOR CONFIDENTIALITY, INTEGRITY AND ACCESS CONTROL	PLT
SECRET SHARING	INFORMATION-THEORETICALLY SECURE CONSTRUCTIONS	С
SECURE ELEMENT AND SMARTCARD	SECURE PLATFORMS	HS
SECURE MULTI-PARTY COMPUTATION	ADVANCED PROTOCOLS	С
SECURE POSITIONING	DISTANCE BOUNDING AND SECURE POSITIONING	PLT
SECURITY AND PRIVACY CONCERNS	CYBER-PHYSICAL SYSTEMS	CPS
SECURITY ARCHITECTURE AND LIFECY- CLE	CROSS-CUTTING THEMES	CI
SECURITY CULTURE	RISK GOVERNANCE	RMG
SECURITY DOMAINS	ROLE OF OPERATING SYSTEMS	osv
SECURITY ECONOMICS	CROSS-CUTTING THEMES	CI
SECURITY HYGIENE	HUMAN ERROR	HF
SECURITY METRICS	RISK ASSESSMENT AND MANAGEMENT PRINCIPLES	RMG
SECURITY MODELS	OS SECURITY PRINCIPLES	osv
SECURITY MODELS	MODELLING AND ABSTRACTION	FMS
SECURITY OPERATIONS AND BENCH MARKING	PLAN: SECURITY INFORMATION AND EVENT MANAGE- MENT	SOIM
SECURITY PROPERTIES	MODELLING AND ABSTRACTION	FMS
SEL4	REAL-WORLD EXAMPLES	FMS
SELF-HELP DISFAVOURED: SOFTWARE LOCKS AND HACK-BACK	COMPUTER CRIME	LR
SEMANTICS - BASED	ANALYSIS AND VERIFICATION	FMS
SIMULATION - BASED	ANALYSIS AND VERIFICATION	FMS
SENSOR COMPROMISE	COMPROMISING EMANATIONS AND SENSOR SPOOF-	PLT



INDICATIVE MATERIAL	TOPIC	CyBOK KA
SERVER-SIDE MIS-CONFIGURATION AND VULNERABLE COMPONENTS	SERVER-SIDE VULNERABILITIES AND MITIGATION'S	WAN
SERVICES	CLOUD FORENSICS	1
SERVICES COORDINATION CLASS	COORDINATION CLASSES AND ATTACKABILITY	DSS
SESIP	MEASURING HARDWARE SECURITY	HS
SETUP ASSUMPTIONS	CRYPTOGRAPHIC SECURITY MODELS	(
SHADOW SECURITY	HUMAN ERROR	н
SHIELDS FROM LIABILITY	INTERNET INTERMEDIARIES	LF
SHORT TERM MEMORY	FITTING THE TASK TO THE HUMAN	н
SIDE CHANNEL VULNERABILITIES	CATEGORIES OF VULNERABILITIES	S
SIEM PLATFORMS AND COUNTERMEA- SURES	EXECUTE: MITIGATION AND COUNTERMEASURES	SOIN
SIGMA PROTOCOLS	ADVANCED PROTOCOLS	(
SIGNAL ANNIHILATION AND OVER- SHADOWING	JAMMING AND JAMMING-RESILIENT COMMUNICA- TIONS	PL
SIMULATION OF CRYPTOGRAPHIC OP- ERATIONS	CRYPTOGRAPHIC SECURITY MODELS	(
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 DEFINED NETWORKING	ADVANCED NETWORK SECURITY TOPICS	N:
SOFTWARE DEVELOPERS	STAKEHOLDER ENGAGEMENT	н
SOUNDNESS	DETECTION OF VULNERABILITIES	S
SPECIALISED SERVICES	ELEMENTS OF A MALICIOUS OPERATION	Al
STATE ACTORS	CHARACTERISATION OF ADVERSARIES	Al
STATE CYBER OPERATIONS IN GEN- ERAL	PUBLIC INTERNATIONAL LAW	LI
STATIC DETECTION	DETECTION OF VULNERABILITIES	S
STORAGE FORENSICS	OPERATING SYSTEM ANALYSIS	1
STRATEGIES	PRIVACY ENGINEERING	POI
STRUCTURED OUTPUT GENERATION VULNERABILITIES	CATEGORIES OF VULNERABILITIES	S
STRUCTURED OUTPUT GENERATIONS MITIGATION'S	PREVENTION OF VULNERABILITIES	S
STRUCTURED P2P PROTOCOLS	DECENTRALISED P2P MODELS	DS
SUBJECT MATTER AND REGULATORY FOCUS	DATA PROTECTION	LI
SYMMETRIC ENCRYPTION AND AU- THENTICATION	SYMMETRIC CRYPTOGRAPHY	(
SYMMETRIC PRIMITIVES	SYMMETRIC CRYPTOGRAPHY	(
SYSLOG	MONITOR: DATA SOURCES	SOIN
SYSTEM AND KERNEL LOGS	MONITOR: DATA SOURCES	SOIM
SYSTEMS COORDINATION STYLES	COORDINATED RESOURCE CLUSTERING	DS
T TAKE-DOWN PROTECTION	INTEDNET INTEDMENIADIES	L
	INTERNET INTERMEDIARIES	AA
TECHNICAL ASPECTS	ACCOUNTABILITY	H
TERMS TESTING AND VALIDATING INTRUSION DETECTION SYSTEMS	AWARENESS AND EDUCATION ANALYSE: ANALYSIS METHODS	SOIN
THE BASE-RATE FALLACY	ANALYSE: ANALYSIS METHODS	SOIN
THE BASE-RATE FALLACY THE ENFORCEMENT OF, AND PENAL- TIES FOR, CRIMES AGAINST INFORMA- TION SYSTEMS WARRANTED STATE AC- TIVITY	COMPUTER CRIME	LI
THE LAW OF ARMED CONFLICT	PUBLIC INTERNATIONAL LAW	L



INDICATIVE MATERIAL	TOPIC	CyBOK KA
THEOREM-PROVING TOOLS	TOOLS	FMS
THEORY	AUTHORISATION	AA
THINKING FAST AND SLOW	HUMAN ERROR	HI
THREAT MODEL	HARDWARE DESIGN CYCLE	H
THREATS TO SECURITY FOR MODERN OSS	ATTACKER MODEL	OSI
TIME	HARDWARE DESIGN PROCESS	H
TLS	SCHEMES	
TOUCH POINTS	PRESCRIPTIVE PROCESSES	SS
TRANSPORT LAYER SECURITY	INTERNET ARCHITECTURE	N:
TRANSPORTATION SYSTEMS AND AUTONOMOUS VEHICLES	CYBER-PHYSICAL SYSTEMS DOMAINS	CP
TROJAN CIRCUITS	HARDWARE DESIGN PROCESS	H
TRUSTED COMPUTER SYSTEM EVALUA- TION CRITERIA	PRIMITIVES FOR ISOLATION AND MEDIATION	OS
TRUSTED COMPUTING	MOTIVATIONS FOR SECURE SOFTWARE LIFECYCLE	SS
TRUSTED EXECUTION ENVIRONMENT	HARDWARE SUPPORT FOR SOFTWARE SECURITY	H
TRUSTED PLATFORM MODULE (TPM)	SECURE PLATFORMS	Н
U		
UNCOORDINATED SPREAD SPECTRUM TECHNIQUES	JAMMING AND JAMMING-RESILIENT COMMUNICA- TIONS	PL
UNDERGROUND ECO-SYSTEM	MALICIOUS ACTIVITIES BY MALWARE	MA
UNDERSTANDING INTELLECTUAL PROPERTY	INTELLECTUAL PROPERTY	LI
UNIVERSAL COMPOSABILITY	CRYPTOGRAPHIC SECURITY MODELS	(
UNSTRUCTURED P2P PROTOCOLS	DECENTRALISED P2P MODELS	DS
USER AUTHENTICATION	AUTHENTICATION	AA
V		
VERIFICATION AND FORMAL METHODS	CROSS-CUTTING THEMES	C
VIRTUAL MACHINES	ROLE OF OPERATING SYSTEMS	081
VIRTUAL MACHINES	HARDWARE SUPPORT FOR SOFTWARE SECURITY	H
VULNERABILITIES CAN BE EXPLOITED WITHOUT BEING NOTICED	MOTIVATIONS FOR SECURE SOFTWARE LIFECYCLE	SS
VULNERABILITY TESTING	ETHICS	LI
W		
WARRANTIES AND THEIR EXCLUSION	CONTRACT	L
WARRANTED STATE ACTIVITY	COMPUTER CRIME	LI
WEB PKI AND HTTPS	FUNDAMENTAL CONCEPTS AND APPROACHES	WAN
WEBIFICATION	FUNDAMENTAL CONCEPTS AND APPROACHES	WAN
WEP	WIRELESS LAN SECURITY	N
WORKFLOWS AND VOCABULARY	FUNDAMENTAL CONCEPTS	SOIM
WPA	WIRELESS LAN SECURITY	N
WPA2	WIRELESS LAN SECURITY	N:
WPA3	WIRELESS LAN SECURITY	N
Z		
ZERO KNOWLEDGE	ADVANCED PROTOCOLS	(