CyBOK Mapping Framework for NCSC Certified Degrees

Guidance Document for UK Higher Education

Lata Nautiyal | University of Bristol

Awais Rashid | University of Bristol

1 STEP BY STEP IMPLEMENTATION OF MAPPING PROCESS BY TAKING EXAMPLE OF ONE MODULE DESCRIPTION FROM UNIVERSITY OF OXFORD, UK

Security Principles:

Introduction

- The need for security; types of security (confidentiality, authentication; non-repudiation; service integrity); big picture (network security; host OS security; physical security); multi-level security; trusted systems.

Contexts

- Data protection/privacy, electronic payment, secret communications, government security. Risk assessment and social factors.

Cryptography

- Number theory: inverses, primes. Basic encryption and decryption: terminology, substitution, stream, and block ciphers; characteristics of good ciphers. Symmetric and asymmetric encryption. Encryption algorithms: DES, RSA, AES, etc. Hashing.

Security Protocols

- Goals of protocols: key distribution, authentication, key confirmation. Protocols and attacks: use of public-key and symmetric-key cryptography; Needham-Schroeder Protocols; Kerberos; Diffie-Helmann key exchange; dangers of key compromise. Key management. Advanced protocols: Encrypted Key Exchange; secret sharing.

Applications

- Public-key cryptography and ISO authentication framework: design of X.509 certificates, and their uses. Secure sockets layer: SSL and encryption, key exchange protocols, use of X.509 certificates; secure web pages. Electronic signatures: role of hashing and cryptography; MD5 etc.; potential attacks, such as the 'birthday book'.

Case Studies

- Banking security, ATM, SWIFT, SET standards. Common criteria. Internet security; SSL/TLS, IPsec.

1.1 Formation Phase:

Security Principles:

Introduction

- The need for security; types of security (confidentiality, authentication; non-repudiation; service integrity); big picture (network security; host OS security; physical security); multi-level security; trusted systems.

Contexts

- Data protection/privacy, electronic payment, secret communications, government security. Risk assessment and social factors.

Cryptography

- Number theory: inverses, primes. Basic encryption and decryption: terminology, substitution, stream, and block ciphers; characteristics of good ciphers. Symmetric and asymmetric encryption. Encryption algorithms: DES, RSA, AES, etc. Hashing.

Security Protocols

- Goals of protocols: key distribution , authentication, key confirmation. Protocols and attacks: use of public-key and symmetric-key cryptography; Needham-Schroeder Protocols; Kerberos; Diffie-Helmann key exchange; dangers of key compromise. Key management. Advanced protocols: Encrypted Key Exchange; secret sharing.

Applications

- Public-key cryptography and ISO authentication framework: design of X.509 certificates, and their uses. Secure sockets layer: SSL and encryption, key exchange protocols, use of X.509 certificates; secure web pages. Electronic signatures: role of hashing and cryptography; MD5 etc.; potential attacks, such as the 'birthday book'.

Case Studies

- Banking security, ATM, SWIFT, SET standards. Common criteria. Internet security; SSL/TLS, IPsec.

1.2 Connecting Phase:

Searching for those highlighted ***keywords*** or a ***set of keywords*** using the resources in the ***"CyBOK Mapping Structure Guide"***. This phase is comprised of 5 steps (**Steps A** to **E)**.

Step A: – Mapping with an alphabetical version of the CyBOK's knowledge areas indicative material from NCSC's certification document: –

Start your search with this document. If your Highlighted/Underlined ***keywords*** or a ***set of keywords*** are found in this part, then record these in the table and move on to the next ***keywords*** or a ***set of keywords***. Repeat the process until the last ***keywords*** or a ***set of keywords***. **(Move to step B)**

S.No.	Broad Category	KA	Topic	Indicative Material	Keyword or a Set of Keywords	Mapping with an alphabetical version of the CyBOK knowledge areas indicative material
1					The need for security	Not Found
2					types of security (confidentiality, authentication; non-repudiation; service integrity);	Not Found
3					network security	Not Found
4					host OS security	Not Found
5					physical security	Not Found

6					multi-level security	Not Found
7	Software and Platform Security	SSL	Motivations for secure software lifecycle	Trusted computing	Trusted Systems	Found and Recorded
8	Human, Organisational, and Regulatory Aspects	POR	Confidentiality	Data Confidentiality	Data protection/privacy (Data Confidentiality)	Found and Recorded
9					electronic payment	Not Found
10					secret communications	Not Found
11					government security	Not Found
12	Human, Organisational and Regulatory Aspects	RMG	Risk definition	Risk assessment	Risk assessment and social factors	Found and Recorded
13					Number theory: inverses, primes	Not Found
14					Basic encryption and decryption: terminology	Not Found
15					substitution	Not Found
16					stream, and block ciphers	Not Found
17					characteristics of good ciphers	Not Found
18	Systems Security	C	Symmetric cryptography	Symmetric encryption and Authentication	Symmetric and asymmetric encryption	Found and Recorded
19	Systems Security	C	Schemes	AES/RSA/DES	Encryption algorithms: DES, RSA, AES	Found and Recorded
20					Hashing	Not Found
21					key distribution	Not Found
22					authentication	Not Found
23					key confirmation	Not Found
24					Protocols and attacks	Not Found
25	Systems Security	C	Public-key cryptography	Public key encryption	use of public-key and symmetric-key cryptography	Found and Recorded
26					Needham-Schroeder Protocols	Not Found
27	Systems Security	C	Schemes	Kerberos	Kerberos	Found and Recorded
28					Diffie-Helmann key exchange	Not Found
29					dangers of key compromise	Not Found
30					Key management	Not Found
31					Advanced protocols	Not Found
32					Encrypted Key Exchange	Not Found
33	Systems Security	C	Information-theoretically secure constructions	Secret sharing	secret sharing	Found and Recorded

34	Systems Security	C	Public-key cryptography	Public key encryption	Public-key cryptography	Found and Recorded
35					ISO authentication framework	Not Found
36					design of X.509 certificates	Not Found
37					Secure sockets layer	Not Found
38					SSL and encryption	Not Found
39	Systems Security	C	Standard protocols	Key agreement protocol	key exchange protocols (Key agreement protocol	Found and Recorded
40					Use of x.509 certificates	Not Found
41					secure web pages	Not Found
42	Human, Organisational and Regulatory Aspects	LR	Dematerialisation of documents and electronic trust service	Electronic signatures and identity trust service	Electronic signatures	Found and Recorded
43					Role of hashing and cryptography	Found but not recorded as it is not relevant as per the context
44					MD5	Not Found
45					potential attacks, such as the 'birthday book'	Not Found
46					Banking security, ATM SWIFT, SET standards	Not Found
47	Software and Platform Security	SSL	Assess the secure software lifecycle	Common Criteria	Common Criteria	Found and Recorded
48					Internet security	Not Found
49					SSL/TLS, IPsec (TLS)	Not Found

Step B: – Mapping with CyBOK Mapping Reference 1.1: –

Continue your search with this document. If your remaining **(Not Found)** ***keywords*** or a ***set of keywords*** are found in this part, then record these in the table and move on to the next ***keywords*** or a ***set of keywords***. Repeat the process until the last ***keywords*** or a ***set of keywords***. **(Move to step C)**

S.No.	Broad Category	KA	Keyword or a Set of Keywords	Mapping with CyBOK Mapping Reference 1.1
1			The need for security	Not Found
2			types of security (confidentiality, authentication; non-repudiation; service integrity);	Not Found
3	Infrastructure Security	NS	network security	Found and Recorded
4	Systems Security	OSV	host OS security (OS security principles)	Found and Recorded
5			physical security	Not Found
6	Systems Security	AAA	multi-level security (multi-level security policies)	Found and Recorded
9	Attacks and Defences	AB	electronic payment	Found and Recorded

10	Systems Security	C	secret communications (Secure Communication Channels)	Found and Recorded
11	Systems Security	C	government security (Secure Communication Channels)	Found and Recorded
13	Systems Security	C	Number theory: inverses, primes (Modular arithmetic)	Found and Recorded
14	Systems Security	C	Basic encryption and decryption: terminology	Found and Recorded
15	Systems Security	C	substitution	Found and Recorded
16	Systems Security	C	stream, and block ciphers	Found and Recorded
17	Systems Security	C	characteristics of good ciphers	Found and Recorded
20	Systems Security	C	Hashing	Found and Recorded
21	Systems Security	C	key distribution	Found and Recorded
22	Systems Security	AAA WAM	authentication	Found and Recorded (Selected AAA as relevant)
23	Systems Security	C	Key confirmation	Found and Recorded
24			Protocols and attacks	Not Found
26	Systems Security	AAA	Needham-Schroeder Protocols	Found and Recorded
28	Systems Security	C	Diffie-Helmann key exchange	Found and Recorded
29	Systems Security	C	dangers of key compromise	Found and Recorded
30	Systems Security	C	Key management	Found and Recorded
31	Systems Security	C	Advanced protocols	Found and Recorded
32	Systems Security	C	Encrypted Key Exchange	Found and Recorded
35			ISO authentication framework	Not Found
36	Systems Security	C	design of X.509 certificates	Found and Recorded
37	Infrastructure Security	NS	Secure sockets layer	Found and Recorded
38	Infrastructure Security	NS	SSL and encryption	Found and Recorded
40	Systems Security	C	Use of x.509 certificates	Found and Recorded
41	Software Platform Security	WAM	secure web pages	Found and Recorded
43			Role of hashing and cryptography	Found but not recorded as it is not relevant as per the context
44	Systems Security	C	MD5	Found and Recorded
45			potential attacks, such as the 'birthday book'	Not Found
46			Banking security, ATM SWIFT, SET standards	Not Found
48	Infrastructure Security	NS	Internet security	Found and Recorded
49	Infrastructure Security	NS	SSL/TLS, IPsec (TLS)	Found and Recorded

Step C: – Complete the missing Topics and Indicative Material from CyBOK Knowledge Trees for all the recorded keywords or a set of keywords found through CyBOK Mapping reference 1.1: –

Searching topics and indicative materials from CyBOK Knowledge Trees for all the recorded ***keywords*** or a ***set of keywords*** found through CyBOK Mapping reference 1.1 as CyBOK Mapping reference 1.1 provides relevant CyBOK knowledge areas but not the topic and indicative material, therefore CyBOK Knowledge Trees are used. **(Move to step D)**

S.No.	Broad Category	KA	Topic	Indicative Material	Keyword or a set of Keywords	Mapping missing Topics and Indicative Material from CyBOK Knowledge Trees
3	Infrastructure Security	NS	***	***	network security	Found and Recorded (Very Broad)
4	Systems Security	OSV	OS security principles	***	host OS security (OS security principles)	Found and Recorded

6	Systems Security	AAA	Authorisation	Access control	multi-level security (multi-level security policies)	Found and Recorded
9	Attacks and Defences	AB	Characterisation of Adversaries	Cyber-dependent organized crime	electronic payment	Found and Recorded
10	Systems Security	C	Public key cryptography	***	secret communications (Secure Communication Channels)	Found and Recorded
11	Systems Security	C	Public key cryptography	***	government security (Secure Communication Channels)	Found and Recorded
13	Systems Security	C	Cryptographic security models	Hard problems	Number theory: inverses, primes (Modular arithmetic)	Found and Recorded
14	Systems Security	C	Symmetric Cryptography	Symmetric encryption and authentication	Basic encryption and decryption: terminology	Found and Recorded
15	Systems Security	C	Cryptographic security models	Hard problems	substitution	Found and Recorded
16	Systems Security	C	Symmetric Cryptography	Symmetric primitives	stream, and block ciphers	Found and Recorded
17	Systems Security	C	Symmetric Cryptography	Symmetric primitives	characteristics of good ciphers (Ciphers)	Found and Recorded
20	Systems Security	C	Symmetric Cryptography	Symmetric primitives	Hashing	Found and Recorded
21	Systems Security	C	Standard Protocols	Key agreement protocols	key distribution	Found and Recorded
22	Systems Security	AAA WAM	Authentication	User authentication or Facets of authentication	authentication	Found and Recorded (Selected AAA as relevant)
23	Systems Security	C	Standard Protocols	Key agreement protocols	key confirmation	Found and Recorded
26	Systems Security	AAA	Authentication	Authentication in distributed systems	Needham-Schroeder Protocols	Found and Recorded
28	Systems Security	C	Cryptographic security models	Hard problems	Diffie-Helmann key exchange	Found and Recorded
29	Systems Security	C	Standard Protocols	Key agreement protocols	dangers of key compromise	Found and Recorded
30	Systems Security	C	Standard Protocols	Key agreement protocols	Key management	Found and Recorded
31	Systems Security	C	Advanced protocols	***	Advanced protocols	Found and Recorded
32	Systems Security	C	Standard Protocols	Key agreement protocols	Encrypted Key Exchange (Key encryption)	Found and Recorded
36	Systems Security	C	Cryptographic security models	***	design of X.509 certificates. (PKI (Public Key Infrastructure)	Found and Recorded
37	Infrastructure Security	NS	Internet Architecture	Transport-layer security	Secure sockets layer	Found and Recorded
38	Infrastructure Security	NS	Internet Architecture	Transport-layer security	SSL and encryption	Found and Recorded

40	Systems Security	C	Cryptographic security models	***	Use of x.509 certificates. (PKI) (Public Key Infrastructure)	Found and Recorded
41	.Software Platform Security	WAM	Fundamental concepts and approaches	***	secure web pages	Found and Recorded
44	Systems Security	C	Symmetric Cryptography	Symmetric primitives	MD5	Found and Recorded
48	Infrastructure Security	NS	Internet Architecture	Network layer security	Internet security (BGP)	Found and Recorded
49	Infrastructure Security	NS	Internet Architecture	Transport-layer security	SSL/TLS, IPsec (TLS)	Found and Recorded

Step D:– Mapping with CyBOK Knowledge Trees: –

Continue your search with this document. If your remaining **(Not Found)** ***keywords*** or a ***set of keywords*** are found in this part, then record these in the table and move on to the next ***keywords*** or a ***set of keywords***. Repeat the process until the last ***keywords*** or a ***set of keywords***. **(Move to step E)**

S.No.	Broad Category	KA	Topic	Indicative Material	Keyword or a set of Keywords	Mapping with CyBOK Knowledge Trees
1	CyBOK Introduction	CI	Foundational Concepts	***	The need for security;	Found and Recorded
2	CyBOK Introduction	CI	Foundational Concepts	***	types of security (confidentiality, authentication; non-repudiation; service integrity);	Found and Recorded
5					physical security	Not Found
24					Protocols and attacks (attacks)	Too Broad to map as mapped with CPS, HS POR, PLT, C, SS
35	Systems Security	C	Public key cryptography	***	ISO authentication framework (Public Key Infrastructure)	Found and Recorded
43	Systems Security	C	Symmetric Cryptography	***	Role of hashing and cryptography	Found and Recorded
45	Systems Security	C	Cryptographic Security Models	Basic security definitions	potential attacks, such as the 'birthday book'	Found and Recorded
46	Software and Platform Security	***	***	***	Banking security, ATM SWIFT, SET standards. (Online transaction processing oltp)	(Depending on details, there may be several relevant KAs and it is not possible to map without more detailed context)

Step E:– Complete final missing keywords using the Tabular representation of CyBOK broad categories, knowledge areas and their description: –

If the ***keywords*** or a ***set of keywords*** are not found in any of the materials provided to support the mapping process then identify the most relevant knowledge area using this document and then record the relevant KA.

S.No.	Broad Category	KA	Topic	Indicative Material	Keyword or a set of Keywords	Searching in Tabular representation of CyBOK broad categories, knowledge areas
5					physical security	Out of Scope

1.3 Finalising Phase:

This phase is a result of the mapping process; the results are transferred from the various tables to the **Final table**. It will be helpful to fill **Table (3.3)** in the application for NCSC certification. **Table (3.3)** is required as a part of the application for NCSC certification.

Broad Category	KA	Topic	Indicative Material	Keyword/ Set of Keywords/Course keywords
CyBOK Introduction	CI	Foundational Concepts	***	The need for security;
CyBOK Introduction	CI	Foundational Concepts	***	types of security (confidentiality, authentication; non-repudiation; service integrity);
Infrastructure Security	NS	***	(Very Broad)	network security
Systems Security	OSV	OS security principles	***	host OS security
***	***	***	Out of Scope	physical security
Systems Security	AAA	Authorisation	Access control	multi-level security
Software and Platform Security	SSL	Motivations for secure software life- cycle	Trusted computing	Trusted Systems
Human, Organisational, and Regulatory Aspects	POR	Confidentiality	Data confidentiality	Data protection/privacy
Attacks and Defences	AB	Characterisation of Adversaries	Cyber-dependent organized crime	electronic payment
Systems Security	C	Public key cryptography	***	secret communications
Systems Security	C	Public key cryptography	***	government security
Human, Organisational and Regulatory Aspects	RMG	Risk definition	Risk assessment	Risk assessment and social factors
Systems Security	C	Cryptographic security models	Hard problems	Number theory: inverses, primes
Systems Security	C	Symmetric Cryptography	Symmetric encryption and authentication	Basic encryption and decryption: terminology
Systems Security	C	Cryptographic security models	Hard problems	substitution
Systems Security	C	Symmetric Cryptography	Symmetric primitives	stream, and block ciphers
Systems Security	C	Symmetric Cryptography	Symmetric primitives	characteristics of good ciphers
Systems Security	C	Symmetric cryptography	Symmetric encryption and Authentication	Symmetric and asymmetric encryption
Systems Security	C	Schemes	AES/ RSA/DES	Encryption algorithms: DES, RSA, AES
Systems Security	C	Symmetric Cryptography	Symmetric primitives	Hashing

Systems Security	C	Standard Protocols	Key agreement protocols	key distribution
Systems Security	AAA	Authentication	User authentication or Facets of authentication	authentication
Systems Security	C	Standard Protocols	Key agreement protocols	Key confirmation
***	***	***	Too Broad to map as mapped with CPS, HS POR, PLT, C, SS	Protocols and attacks
Systems Security	C	Public-key cryptography	Public key encryption	use of public-key and symmetric-key cryptography
Systems Security	AAA	Authentication	Authentication in distributed systems	Needham-Schroeder Protocols
Systems Security	C	Schemes	Kerberos	Kerberos
Systems Security	C	Cryptographic security models	Hard problems	Diffie-Helmann key exchange
Systems Security	C	Standard Protocols	Key agreement protocols	dangers of key compromise
Systems Security	C	Standard Protocols	Key agreement protocols	Key management
Systems Security	C	Advanced protocols	***	Advanced protocols
Systems Security	C	Standard Protocols	Key agreement protocols	Encrypted Key Exchange
Systems Security	C	Information-theoretically secure constructions	Secret sharing	secret sharing
Systems Security	C	Public-key cryptography	Public-key encryption	Public-key cryptography
Systems Security	C	Public key cryptography	***	ISO authentication framework
Systems Security	C	Cryptographic security models	***	design of X.509 certificates.
Infrastructure Security	NS	Internet Architecture	Transport-layer security	Secure sockets layer
Infrastructure Security	NS	Internet Architecture	Transport-layer security	SSL and encryption
Systems Security	C	Standard protocols	Key agreement protocol	key exchange protocols
Systems Security	C	Cryptographic security models	***	Use of x.509 certificates.
Software Platform Security	WAM	Fundamental concepts and approaches	***	secure web pages
Human, Organisational and Regulatory Aspects	LR	Dematerialisation of documents and electronic trust service	Electronic signatures and identity trust service	Electronic signatures
Systems Security	C	Symmetric Cryptography	***	Role of hashing and cryptography
Systems Security	C	Symmetric Cryptography	Symmetric primitives	MD5
Systems Security	C	Cryptographic Security Models	Basic security definitions	potential attacks, such as the 'birthday book'
Software and Platform Security	***	***	Depending on details, there may be several relevant KAs and it is not possible to map without more detailed context	Banking security, ATM SWIFT, SET standards.
Software and Platform Security	SSL	Assess the secure software lifecycle	Common Criteria	Common Criteria
Infrastructure Security	NS	Internet Architecture	Network layer security	Internet security
Infrastructure Security	NS	Internet Architecture	Transport-layer security	SSL/TLS, IPsec

Note :- Some topics are too broad to be covered in a single KA, therefore if terms are so broad, they can't be mapped without more context. It is better to consider the context and then record the appropriate Indicate Material, Topic, Knowledge Areas and Broad Category.

*** Indicated that there is no direct mapping of keyword with Indicative material but with Topic coverage.

2 SOURCE OF MODULE CONTENTS

http://www.cs.ox.ac.uk/softeng/subjects/SPR.html