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 BRISTOL, UK

Security 101:

Core Topics:

- Intro/Unit outline/Assessment; who am I online: user/roles, access rights, authentication
- How can I proof my identity online? Authentication cont.: passwords (storing passwords?), authentication tokens (one-time passwords), signatures (hint towards public key cryptography)
- CIA: how does cryptography help to achieve confidentiality, integrity, authenticity, what does 'secure' mean?
- Securing data at rest: revisit passwords, file/disk encryption
- Securing data in transit: TLS, SSH, email encryption
- Staying clear from malware: viruses, worms, trojans 7
- Computer security: what is inside WinOS, MacOS, Unix to improve security

Optional Topics:

- Developing secure software: checking inputs to avoid exploiting buffer overflows, stack smashing
- Security challenges in the context of embedded devices: physical security
- Security challenges in the context of large and complex systems: deduplication (clouds), maybe a little on computing on encrypted data
- Privacy: Tor, security of web applications, web fingerprinting
- Failing gracefully: disaster recovery
- Psychology of security: how do human biases inform how we judge risk and uncertainty
- Banking security: EMV standard
- Mobile security: GSM vs. UMTS
- IoT security: connects with small devices: D/TLS
- Critical infrastructures

1.1 Formation Phase:

University of Bristol, UK

Core Topics:

- Intro/Unit outline/Assessment; who am I online: user/roles, access rights, authentication
- How can I proof my identity online? Authentication cont.: passwords (storing passwords?), authentication tokens (one-time passwords), signatures (hint towards public key cryptography)
- CIA: how does cryptography help to achieve confidentiality, integrity, authenticity, what does 'secure' mean?
- Securing data at rest: revisit passwords, file/disk encryption
- Securing data in transit: TLS, SSH, email encryption
- Staying clear from malware: viruses, worms, trojans
- Computer security: what is inside WinOS, MacOS, Unix to improve security

Optional Topics:

- Developing secure software: checking inputs to avoid exploiting buffer overflows, stack smashing
- Security challenges in the context of embedded devices: physical security
- Security challenges in the context of large and complex systems: deduplication (clouds), maybe a little on computing on encrypted data
- Privacy: Tor, security of web applications, web fingerprinting
- Failing gracefully: disaster recovery
- Psychology of security: how do human biases inform how we judge risk and uncertainty
- Banking security: EMV standard
- Mobile security: GSM vs. UMTS
- IoT security: connects with small devices: D/TLS
- Critical infrastructures

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	Systems Security	AAA	Authentication	User authentication	who am I online: user/roles (user authentication)	Found and Recorded
2	Systems Security	AAA	Authorisation	Access control	access rights (Access control)	Found and Recorded
3					authentication	Found but Not Recorded – "Not mapped as broad and already covered by 1 and 2)
4	Systems Security	AAA	Authentication	User authentication	How can I proof my identity online (user authentication)	Found and Recorded
5	Attacks and Defences	WAM	Fundamental concepts and approaches	Passwords and alternatives	Passwords (storing passwords)	Found and recorded
6					authentication tokens	Not found
7					one-time passwords	Not found
8					signatures (hint towards public key cryptography)	Not found
9					confidentiality, integrity, authenticity	Found but not recorded (Not relevant as per the context
10					what does 'secure' mean?	Not found
11					Securing data at rest : revisit passwords	Not found
12					Securing data at rest : file/disk encryption	Not found
13	Systems Security	C	Schemes	TLS	Securing data in transit: TLS	Found and recorded
14					Securing data in transit: SSH	Not found

15					Securing data in transit:email encryption	Not found
16					Staying clear from malware : viruses, worms, trojans	Not found
17					Computer security: what is inside WinOS, MacOS, Unix to improve security	Not Found
18					Developing secure software: checking inputs to avoid exploiting buffer overflows	Not found
19					Developing secure software : stack smashing	Not found
20					Security challenges in the context of embedded devices: physical security	Not found
21					Security challenges in the context of large and complex systems: deduplication (clouds)	Not found
22					computing on encrypted data	Not found
23					Privacy : Tor	Not found
24					Privacy : security of web applications	Not found
25					Privacy : web fingerprinting	Not found
26					Failing gracefully: disaster recovery	Not found
27	Human, Organisational, and Regulatory Aspects	RMG	Risk assessment and management principles	Risk Assessment and Management Methods	Psychology of security: how do human biases inform how we judge risk and uncertainty (Risk Assessment and Management Methods)	Found and Recorded
28					Banking security: EMV standard	Not found
29					Mobile security: GSM vs. UMTS	Not found
30	Infrastructure Security	NS	Advanced network security topics	Internet of things security	IoT security connects with small devices: D/TLS (Internet of things security)	Found and Recorded

31					Critical infrastructures	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
6	Systems Security	AAA	authentication tokens	Found and Recorded
7	Human, Organisational & Regulatory Aspects	HF	one-time passwords	Found and Recorded
8	Systems Security	C	signatures (hint towards public key cryptography) (Digital Signature)	Found and Recorded
9			confidentiality, integrity, authenticity	Found but not recorded (Not relevant as per the context
10			what does 'secure' mean?	Not found
11	Human, Organisational and Regulatory Aspects	AAA, HF	Securing data at rest : revisit passwords	Found and Recorded (Selected HF as Relevant)
12			Securing data at rest : file/disk encryption	Not found
14	Infrastructure Security	NS	Securing data in transit: SSH	Found and Recorded
15	Systems Security	C	Securing data in transit:email encryption	Found and Recorded
16	Attacks and Defences	MAT	Staying clear from malware : viruses, worms, trojans (Malware)	Found and Recorded
17	Systems Security	OSV	Computer security: what is inside WinOS, MacOS, Unix to improve security (OS security principles)	Found and Recorded
18	Systems Security	SS	Developing secure software : checking inputs to avoid exploiting buffer overflows (Buffer overflow - security controls)	Found and Recorded
19			Developing secure software:stack smashing	Not found
20	Infrastructure Security	CPS	Security challenges in the context of embedded devices: physical security (Embedded systems)	Found and Recorded
21	Systems Security	DSS	Security challenges in the context of large and complex systems: deduplication (clouds) (Encryption - cloud computing)	Found and Recorded
22	Systems Security	C SOIM	computing on encrypted data (Encryption)	Found and Recorded (Selected C as relevant)
23	Human, Organisational, and Regulatory Aspects	POR	Privacy : Tor	Found and Recorded
24			Privacy : security of web applications	Not found
25			Privacy : web fingerprinting	Not found
26	Attacks and Defences	SOIM	Failing gracefully: disaster recovery (Disaster-recovery)	Found and Recorded
28			Banking security: EMV standard	Not found
29	Infrastructure Security	PLT	Mobile security: GSM vs. UMTS (GSM)	Found and Recorded
31			Critical infrastructures	Found but not recorded as it is not relevant as per the context

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
6	Systems Security	AAA	Authentication	User Authentication	authentication tokens	Found and Recorded
7	Human, Organisational, and Regulatory Aspects	HF	Fitting the task to the human	Short-term memory	one-time passwords	Found and Recorded
8	Systems Security	C	Public key cryptography	Public key signature	signatures (hint towards public key cryptography) (Digital Signature)	Found and Recorded
11	Human, Organisational and Regulatory Aspects	AAA, HF	Stakeholder Engagement	Software developers	Securing data at rest : revisit passwords	Found and Recorded (Selected HF as Relevant)
14	Infrastructure Security	NS	Internet Architecture	Application layer security	Securing data in transit: SSH	Found and Recorded
15	Systems Security	C	Symmetric Cryptography	Symmetric encryption and authentication	Securing data in transit:email encryption	Found and Recorded
16	Attacks and Defences	MAT	Malware taxonomy	Kinds	Staying clear from malware : viruses, worms, trojans (Malware)	Found and Recorded
17	Systems Security	OSV	Primitives for isolation and mediation	***	Computer security: what is inside WinOS, MacOS, Unix to improve security (OS security principles)	Found and Recorded
18	Systems Security	SS	prevention of vulnerabilities	Coding practices	Developing secure software : checking inputs to avoid exploiting buffer overflows (Buffer overflow - security controls)	Found and Recorded

20	Infrastructure Security	CPS	CPS Domains	***	Security challenges in the context of embedded devices: physical security (Embedded systems)	Found and Recorded (This is mapped to CPS domains due to the broader focus on security challenges but note that physical security is out of scope of CyBOK)
21	Systems Security	DSS	Classes of Distributed Systems	Coordinated clustering across distributed resources and services	Security challenges in the context of large and complex systems: deduplication (clouds) (Encryption - cloud computing)	Found and Recorded
22	Systems Security	C SOIM	Public-Key Schemes with Special Properties	***	computing on encrypted data (Encryption)	Found and Recorded (Selected C as relevant)
23	Human, Organisational, and Regulatory Aspects	POR	Confidentiality	Metadata Confidentiality	Privacy : Tor	Found and Recorded
26	Attacks and Defences	SOIM	Plan: Security Information and Event Management	***	Failing gracefully: disaster recovery (Disaster-recovery)	Found and Recorded
29	Infrastructure Security	PLT	Physical Layer Security of Selected Communications Technologies	Cellular networks	Mobile security: GSM vs. UMTS (GSM)	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
9	CyBOK Introduction	CI	Foundational Concept	Objectives of cyber security	confidentiality, integrity, authenticity	Found and Recorded
10	CyBOK Introduction	CI	Foundational Concept	***	what does ‘secure’ mean?	Found and Recorded
12	Systems Security	OSV	Primitives for Isolation and Mediation	***	Securing data at rest : file/disk encryption	Found and Recorded
19	Software and Platform Security	SS	Categories of vulnerabilities	Memory management vulnerabilities	Developing secure software : stack smashing	Found and Recorded
24	Software and Platform Security	WAM	Fundamental concepts and approaches	***	Privacy : security of web applications	Found and Recorded

25	Human, Organisational and Regulatory Aspects	POR	Confidentiality	Metadata confidentiality	Privacy : web fingerprinting	Found and Recorded
28	Software and Platform Security	***	***	***	Banking security: EMV standard	(Depending on details, there may be several relevant KAs and it is not possible to map without more detailed context)
31	Infrastructure Security	CPS	CPS Domains	***	Critical infrastructures	Found and Recorded

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.

Not Applicable - All the keywords have been mapped by using Step A to D

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
Systems Security	AAA	Authentication	User authentication	who am I online: user/roles
Systems Security	AAA	Authorisation	Access control	access rights
			Not mapped as broad and already covered by 1 and 2	authentication
Systems Security	AAA	Authentication	User authentication	How can I proof my identity online
Attacks and Defences	WAM	Fundamental concepts and approaches	Passwords and alternatives	Passwords (storing passwords)
Systems Security	AAA	Authentication	User Authentication	authentication tokens
Human, Organisational, and Regulatory Aspects	HF	Fitting the task to the human	Short-term memory	one-time passwords
Systems Security	C	Public key cryptography	Public key signature	signatures (hint towards public key cryptography)
CyBOK Introduction	CI	Foundational Concept	Objectives of cyber security	confidentiality, integrity, authenticity
CyBOK Introduction	CI	Foundational Concept	***	what does 'secure' mean?
Human, Organisational and Regulatory Aspects	HF	Stakeholder Engagement	Software developers	Securing data at rest : revisit passwords
Systems Security	OSV	Primitives for Isolation and Mediation	***	Securing data at rest : file/disk encryption
Systems Security	C	Schemes	TLS	Securing data in transit: TLS
Infrastructure Security	NS	Internet Architecture	Application layer security	Securing data in transit: SSH

Systems Security	C	Symmetric Cryptography	Symmetric encryption and authentication	Securing data in transit: email encryption
Attacks and Defences	MAT	Malware taxonomy	Kinds	Staying clear from malware : viruses, worms, trojans
Systems Security	OSV	Primitives for isolation and mediation	***	Computer security: what is inside WinOS, MacOS, Unix to improve security
Systems Security	SS	Prevention of vulnerabilities	Coding practices	Developing secure software : checking inputs to avoid exploiting buffer overflows
Software and Platform Security	SS	Categories of vulnerabilities	Memory management vulnerabilities	Developing secure software : stack smashing
Infrastructure Security	CPS	CPS Domains	***	Security challenges in the context of embedded devices: physical security [1]
Systems Security	DSS	Classes of Distributed Systems	Coordinated clustering across distributed resources and services	Security challenges in the context of large and complex systems: deduplication (clouds)
Systems Security	C	Public-Key Schemes with Special Properties	***	computing on encrypted data
Human, Organisational, and Regulatory Aspects	POR	Confidentiality	Metadata Confidentiality	Privacy : Tor
Software and Platform Security	WAM	Fundamental concepts and approaches	***	Privacy : security of web applications
Human, Organisational and Regulatory Aspects	POR	Confidentiality	Metadata confidentiality.	Privacy : web fingerprinting
Attacks and Defences	SOIM	Plan: Security Information and Event Management	***	Failing gracefully: disaster recovery
Human, Organisational, and Regulatory Aspects	RMG	Risk assessment and management principles	Risk Assessment and Management Methods	Psychology of security: how do human biases inform how we judge risk and uncertainty
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: EMV standard
Infrastructure Security	PLT	Physical Layer Security of Selected Communications Technologies	Cellular networks	Mobile security: GSM vs. UMTS
Infrastructure Security	NS	Advanced network security topics	Internet of things security	IoT security connects with small devices: D/TLS
Infrastructure Security	CPS	CPS Domains	***	Critical infrastructures

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.

[1] This is mapped to CPS domains due to the broader focus on security challenges but note that physical security is out of scope of CyBOK

2 SOURCE OF MODULE CONTENTS

https://www.bris.ac.uk/unit-programme-catalogue/UnitDetails.jsa?ayrCode=19%2F20&unitCode=COMS10005