CyBOK

Cyber Security Body of Knowledge

Awais Rashid (PI)
Professor of Cyber Security, University of Bristol

contact@cybok.org
www.cybok.org

Andrew Martin

Emil Lupu

Howard Chivers

Yvonne Rigby

George Danezis

Andrew Martin

Emil Lupu

Howard Chivers

Helen Jones

Steve Schneider

Andrew Martin

Emil Lupu

Howard Chivers

Helen Jones

Steve Schneider

Lata Nautiyal

Joseph Hallett

Claudia Peersman

Makalya Lewis

Ben Shreeve

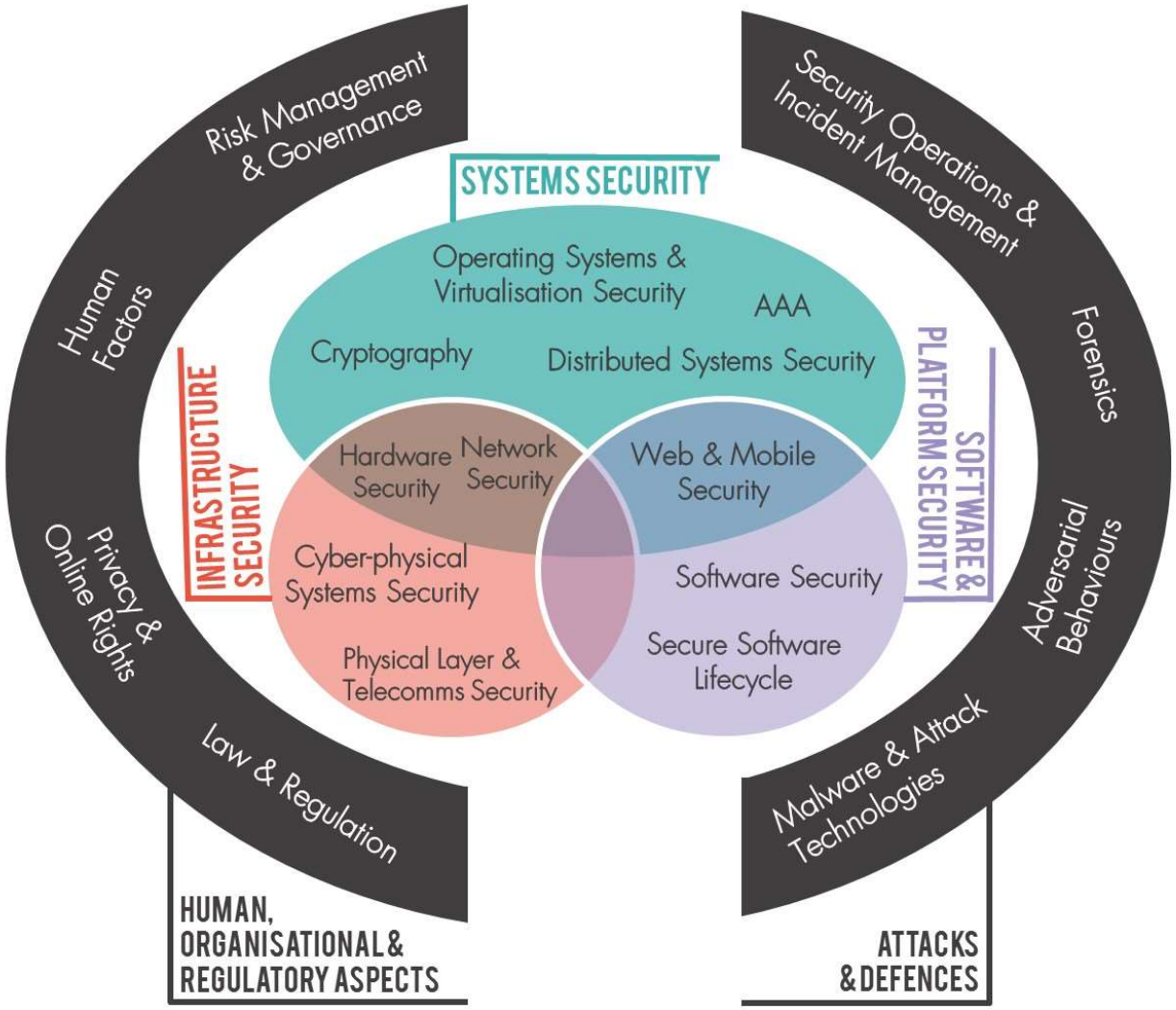
Rob Larson

Codify ***foundational*** and generally recognised knowledge in cyber security following broad community engagement nationally and internationally

A ***guide*** to the body of knowledge

Focus is on ***established foundation*** of the subject (not on everything that has ever been written or on still-emerging, nascent, topics)

International effort
For the community by the community
Open and freely accessible
Transparency


Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
AAA
Cryptography
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Cyber-physical Systems Security
Physical Layer & Telecomms Security
SOFTWARE & PLATFORM SECURITY
Web & Mobile Security
Software Security
Secure Software Lifecycle

110 Experts: Authors, Reviewers, Advisors

828 Pages

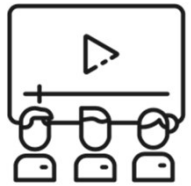
1839 Authoritative sources

1597 Comments from wider community

>20 Invited talks, panels and keynotes

CyBOK

The Cyber Security Body of Knowledge



Webinars

Version 1.0
31st October 2019
https://www.cybok.org/

EDITORS
Awais Rashid | University of Bristol
Howard Chivers | University of York
George Danezis | University College London
Emil Lupu | Imperial College London
Andrew Martin | University of Oxford
PROJECT MANAGER
Yvonne Rigby | University of Bristol
PRODUCTION
Joseph Hallett | University of Bristol

A Living Resource

Two new Knowledge Areas

Formal Methods for Security

Applied Cryptography

Revised Knowledge Area

Network Security

Minor updates to some other KAs

Open call for comments/updates

CyBOK Use Cases

Design new university or professional training programmes

Design new certification schemes

Postgraduate Master's Degrees providing a general, broad foundation in cyber security
Based on the Cyber Security Body of Knowledge (CyBOK).

PDF • 797 KB • 54 PAGES

Postgraduate Master's Degrees focusing on a specialised area of Cyber Security
Based on the Cyber Security Body of Knowledge (CyBOK).

PDF • 849 KB • 56 PAGES

Bachelor's in Computer Science and Cyber Security
Two certifications; A) providing a general broad foundation and B) focusing on a specialised area of...

PDF • 753 KB • 69 PAGES

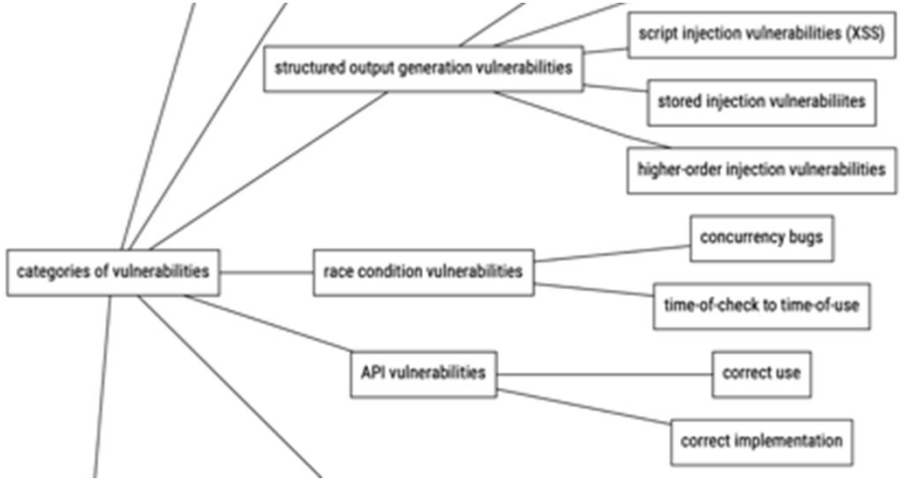
CONTENT

1 CATEGORIES OF VULNERABILITIES

[3][4, c4,c5,c6,c7,c10,c11][5, c6,c9] [6, c17][7, c5,c9,c11,c13,c17]

As discussed in the Introduction, we use the term *implementation vulnerability* (sometimes also called a *security bug*) both for bugs that make it possible for an attacker to violate a security objective, as well as for classes of bugs that enable specific attack techniques.

Implementation vulnerabilities play an important role in cybersecurity and come in many forms. The Common Vulnerabilities and Exposures (CVE) is a publicly available list of entries in a standardised form describing vulnerabilities in widely-used software components, and it lists close to a hundred thousand such vulnerabilities at the time of writing. Implementation vulnerabilities are often caused by insecure programming practices and influenced by the programming language or APIs used by the developer. This first topic covers important categories of implementation vulnerabilities that can be attributed to such insecure programming practices.



CyBOK Use Cases

Traceably meeting certification requirements

Contrasting different programmes

Knowledge requirements for job roles

Benchmarking capacity

CyBOK Mapping Framework

Key Words or Phrases (KWoPs)

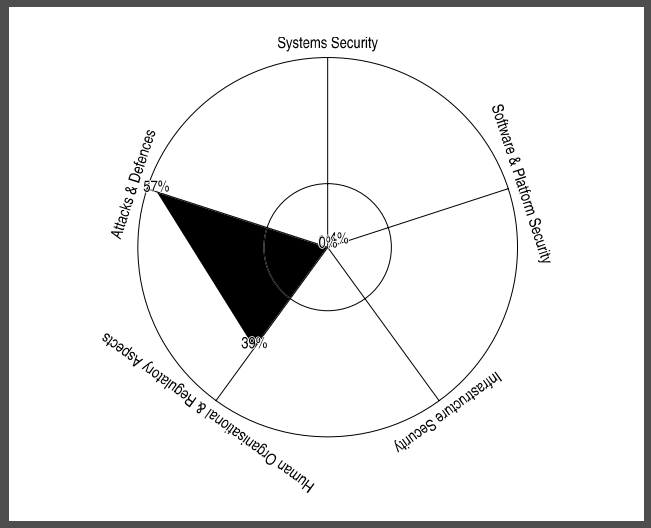
Additional Lookup Mechanisms

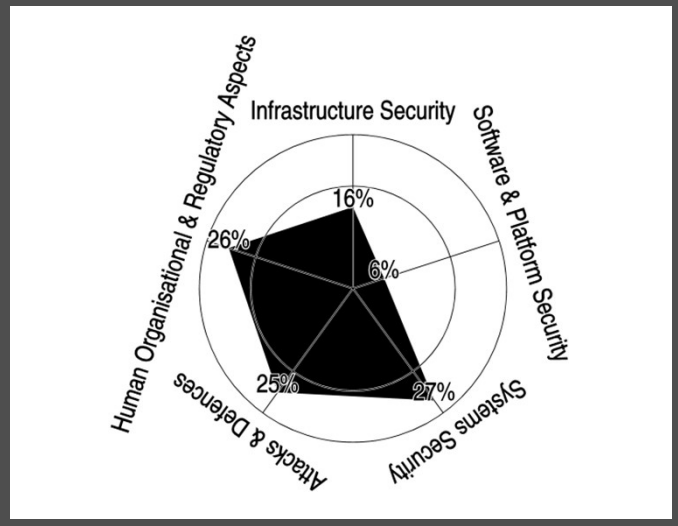
CyBOK Mapping Reference

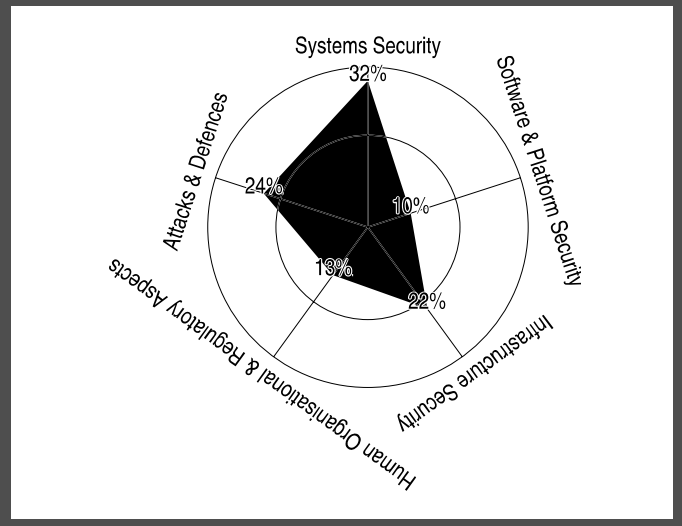
Tabular Representation

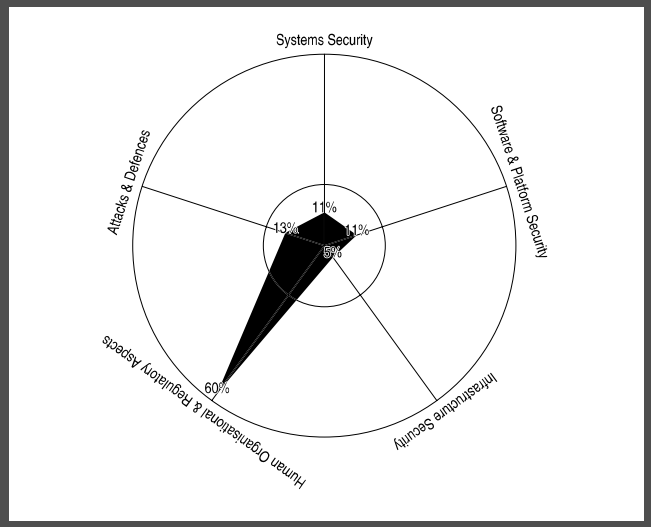
Knowledge Tree

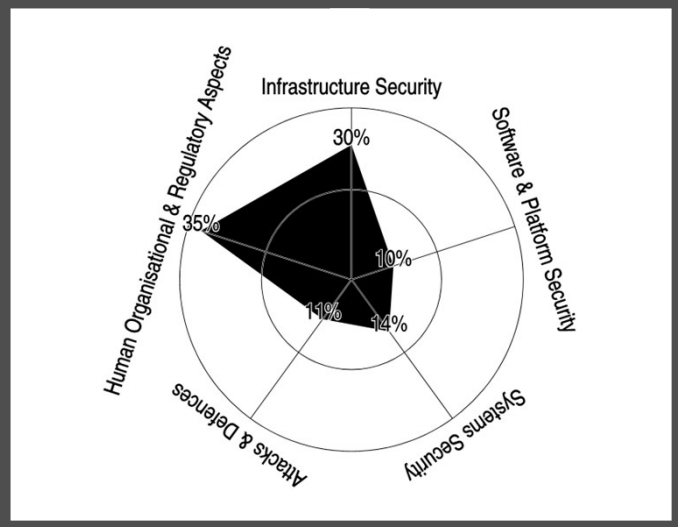
Knowledge Area (Detailed Text)

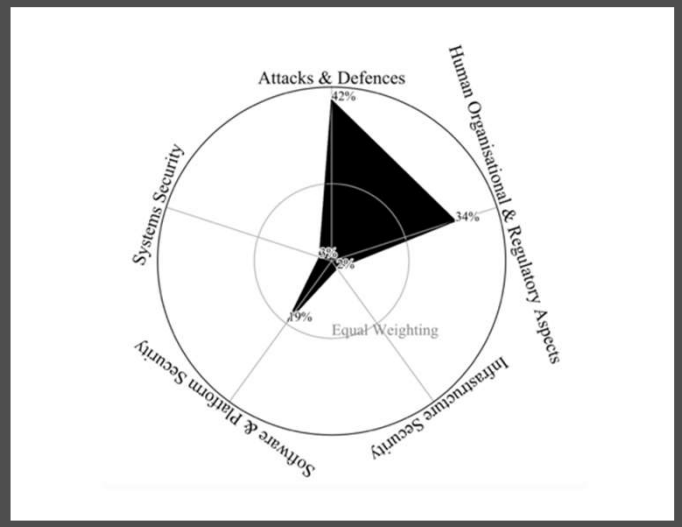

Systems Security
Software & Platform Security
Infrastructure Security
Human Organisational & Regulatory Aspects
Attacks & Defences
0%
4%
39%
37%


Infrastructure Security
Software & Platform Security
Systems Security
Attacks & Defences
Human Organisational & Regulatory Aspects
16%
6%
27%
25%
26%


Systems Security
Software & Platform Security
Infrastructure Security
Human Organisational & Regulatory Aspects
Attacks & Defences
32%
10%
22%
13%
24%


Systems Security
Software & Platform Security
Infrastructure Security
Human Organisational & Regulatory Aspects
Attacks & Defences
11%
11%
5%
13%
60%


Infrastructure Security
Software & Platform Security
Systems Security
Attacks & Defences
Human Organisational & Regulatory Aspects
30%
10%
14%
11%
35%


Attacks & Defences
Human Organisational & Regulatory Aspects
Infrastructure Security
Software & Platform Security
Systems Security
42%
34%
5%
5%
19%
Equal Weighting

cybok.org in 2020

~3.84M Total 2020 website hits

Monthly average: 349.5K

Daily average: 11.5K

>377K Total downloads

>291K Downloads of CyBOK 1.0