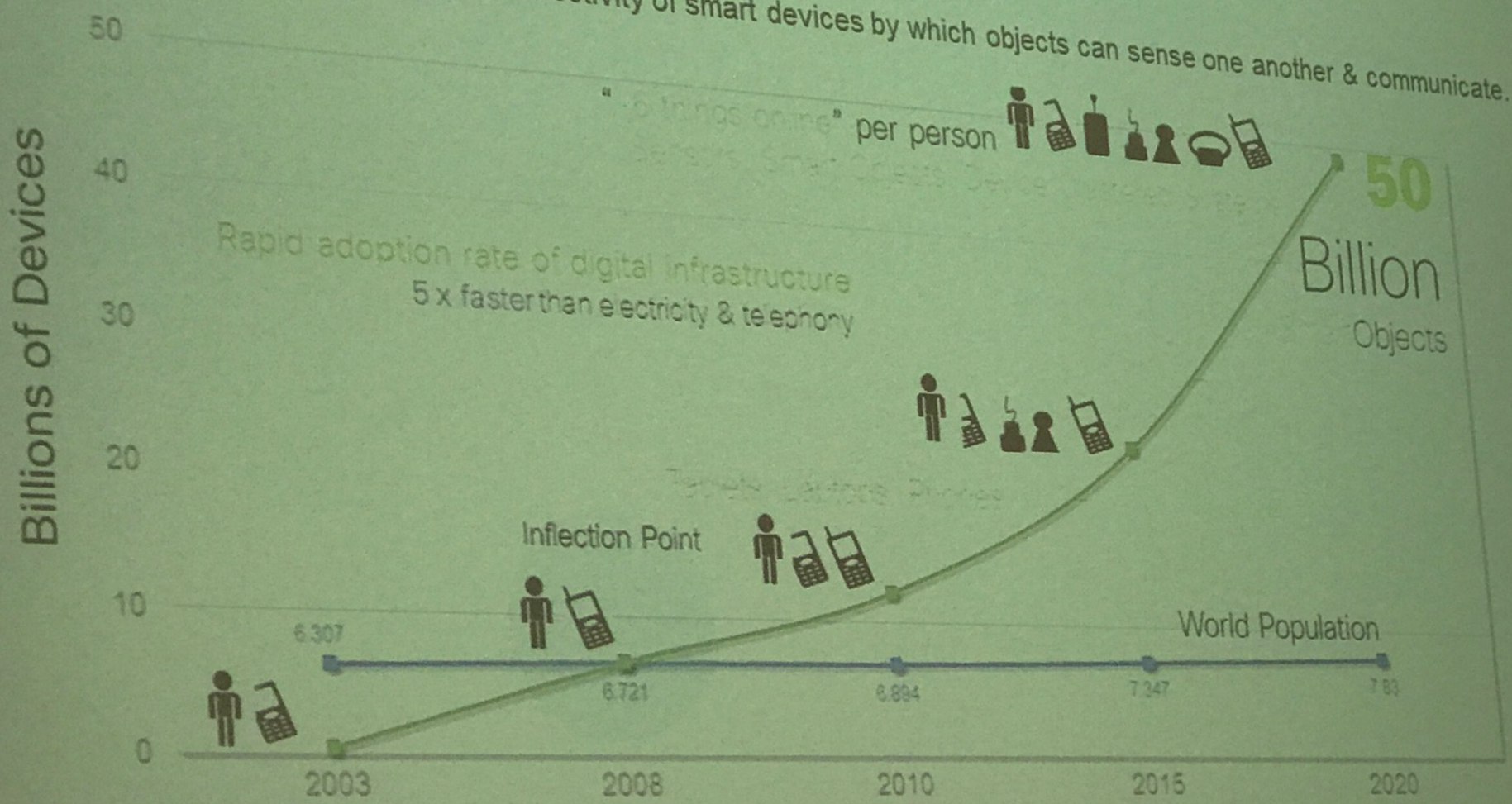
Identifying the Cybersecurity Body of Knowledge for a Postgraduate Module in Systems Engineering

S von Solms*, University of Johannesburg & L Futcher, Nelson Mandela University

UNIVERSITY OF JOHANNESBURG

Introduction

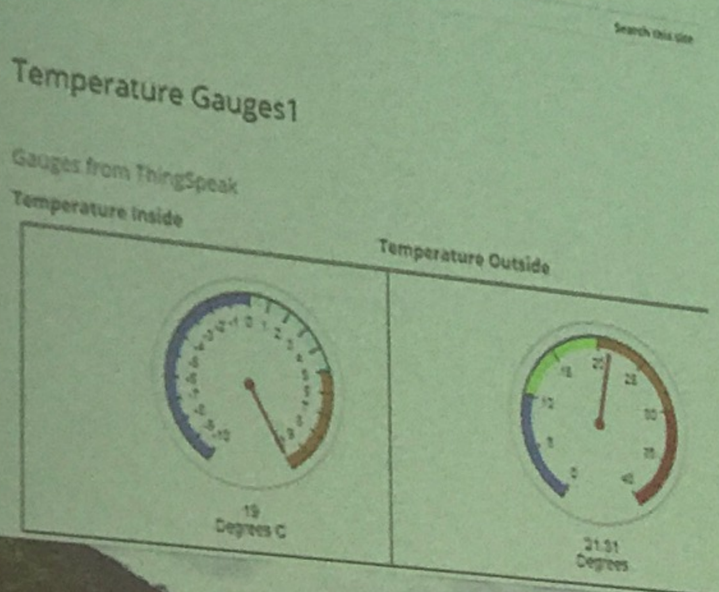
Internet of Things (IoT): the intelligent connectivity of smart devices by which objects can sense one another & communicate.

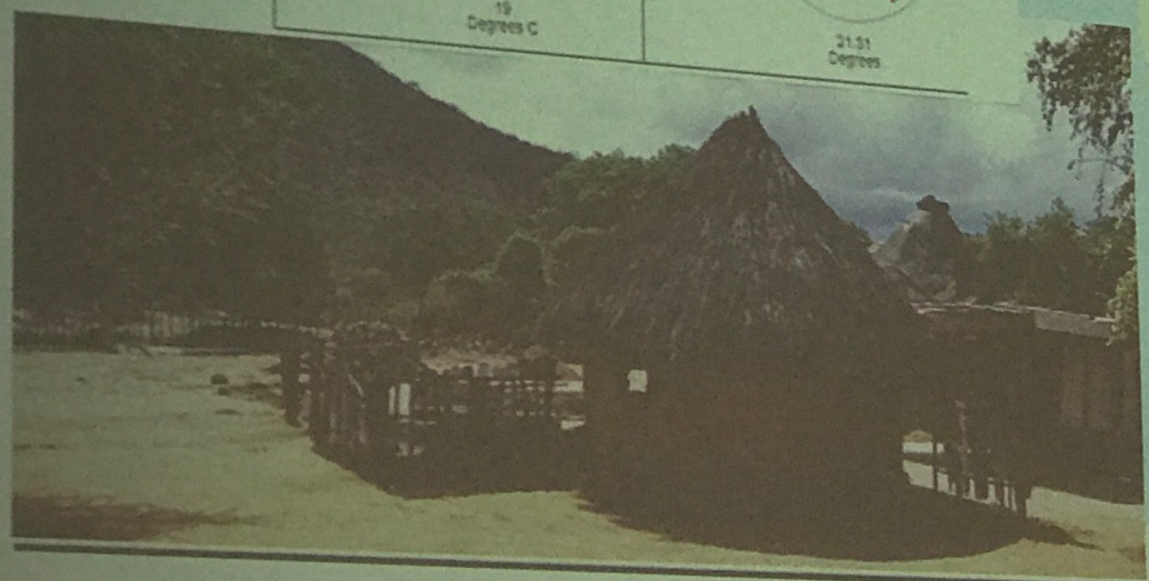


Source: Cisco IBSG projections, UN Economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf

Introduction

Gwakwani Coldstorage





Introduction

Vulnerability increases with connection - Gardner, 2016

- The interconnected nature of systems – extensive effects due to cyberattacks
- Starting to see vulnerabilities in integrated systems. Engineers designing, developing, managing and operating systems - treat security as a key concern.
- SA engineering graduates - lack cybersecurity knowledge & skills needed within specific engineering industry.
- Mission – determine the cybersecurity body of knowledge which can be considered in a postgraduate cybersecurity module for Systems Engineering in SA.

Smart mirror & ambient control

IoT greenhouse monitoring and automation system

Integrated solar tracking system

Optical sensors for monitoring concrete foundations

Bakery management system and monitoring system for rural solar bakeries

Online platform for urban farmers & consumers

Smart bus tracking systems

Building air-conditioning maintenance monitoring

Smart hard hats for safety monitoring

Voice controlled home automation system

Rural container business monitoring and management system

Curriculum development for the cybersecurity skills gap

"(W)hen it comes to cybersecurity, systems engineers typically cede the responsibility to the security profession." - INCOSE System Security Engineering Working Group, 2016

- South African case:
  - Organizations starting to recognize- security integration in engineering systems cannot be limited to IT industry
  - Cybersecurity skills shortage- high demand for cybersecurity professionals in engineering
  - No known cybersecurity courses offered by South African universities.

The lack of cybersecurity content in SA engineering education & need for cybersecurity professionals point toward a gap in cybersecurity knowledge amongst engineers in industry

Introduction

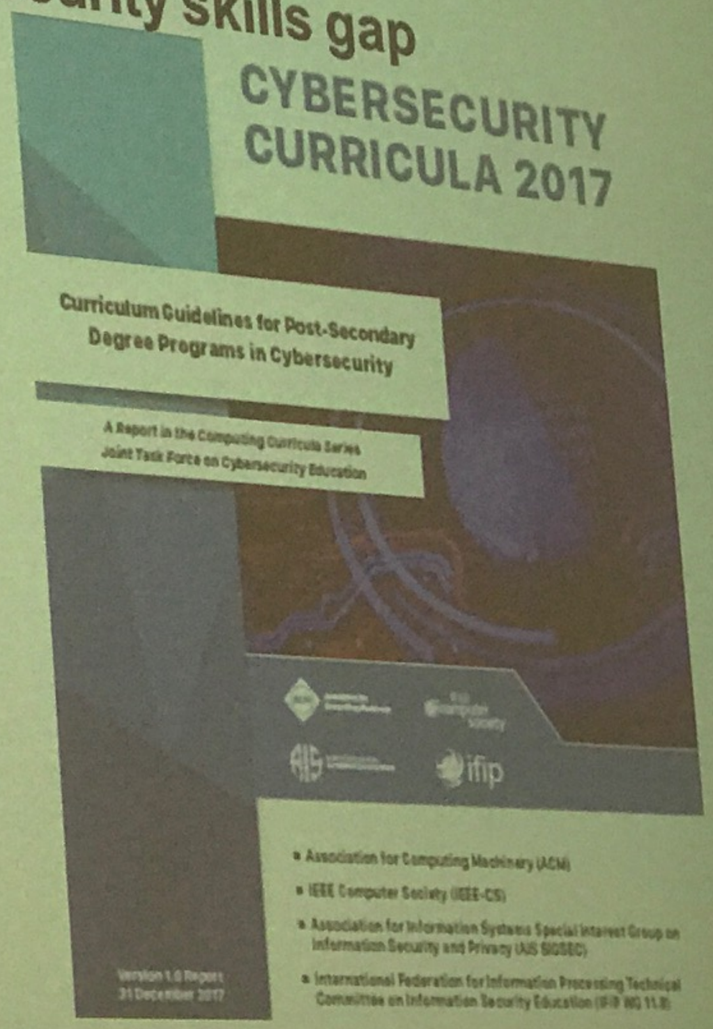
- The cyber security domain is suffering a skills shortage:
  - 58% of organizations say that lack of skilled resources is one of the main obstacles to addressing cyber security (E&Y GISS 2017-18)
  - UK's National Audit Office (2013) suggested it could take up to 20 years to bridge the gap
  - $(ISC)^2$ (2017) suggested the gap could reach 1.8m by 2022

S Furnell - yesterday

Curriculum development for the cybersecurity skills gap

Joint Task Force on Cybersecurity Education (CSEC2017):
To develop comprehensive curricular guidance in cybersecurity education that will support future program development and associated educational efforts at the post-secondary level.

- Provides guidance - utilized in development of cybersecurity courses in engineering in SA
- Development of an engineering cybersecurity module requires input from the engineering industry - ensure competencies & knowledge included in module accurately map to industry needs

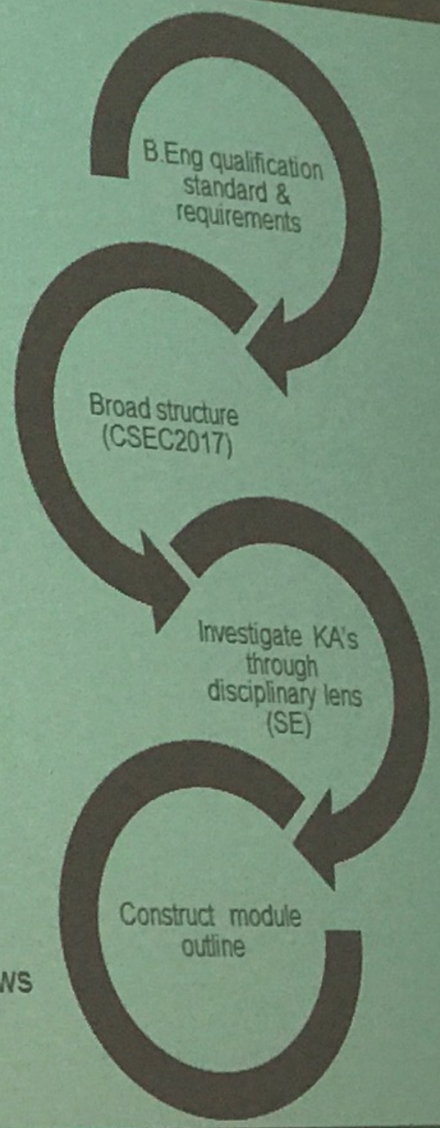


Methodology & Research Process

Objective: identify knowledge areas & competencies which can be included in engineering programs to provide engineers with CS knowledge.

- The proposed CS module: part of a course work Master's qualification:
  - working engineering professionals,
  - set of modules & minor research dissertation
  - two-year period.

- Methodology:
  1. Investigate qualification standard & educational requirements
  2. Determine the broad structure for module development (CSEC2017)
  3. Investigate CSEC2017 KA's viewed through the disciplinary lens – elite interviews with Systems Engineers (SE's).
  4. Construct a module outline



Towards determining the structure/context for cybersecurity engineering module

Overview of South African postgraduate engineering degrees

1 B.Eng:

Provide a coherent core in mathematics, natural sciences & engineering fundamentals - solid platform for further studies

Provide graduates with a well-rounded, broad education to prepare them for "professional training, post-graduate studies or professional practice in a wide range of careers"

2 B.Eng or M.Phil:

Research Master's degree by dissertation: single advanced research project in a specialized field of study

Coursework Master's degree: coursework programme to provide a broad exposure to a field & minor research project

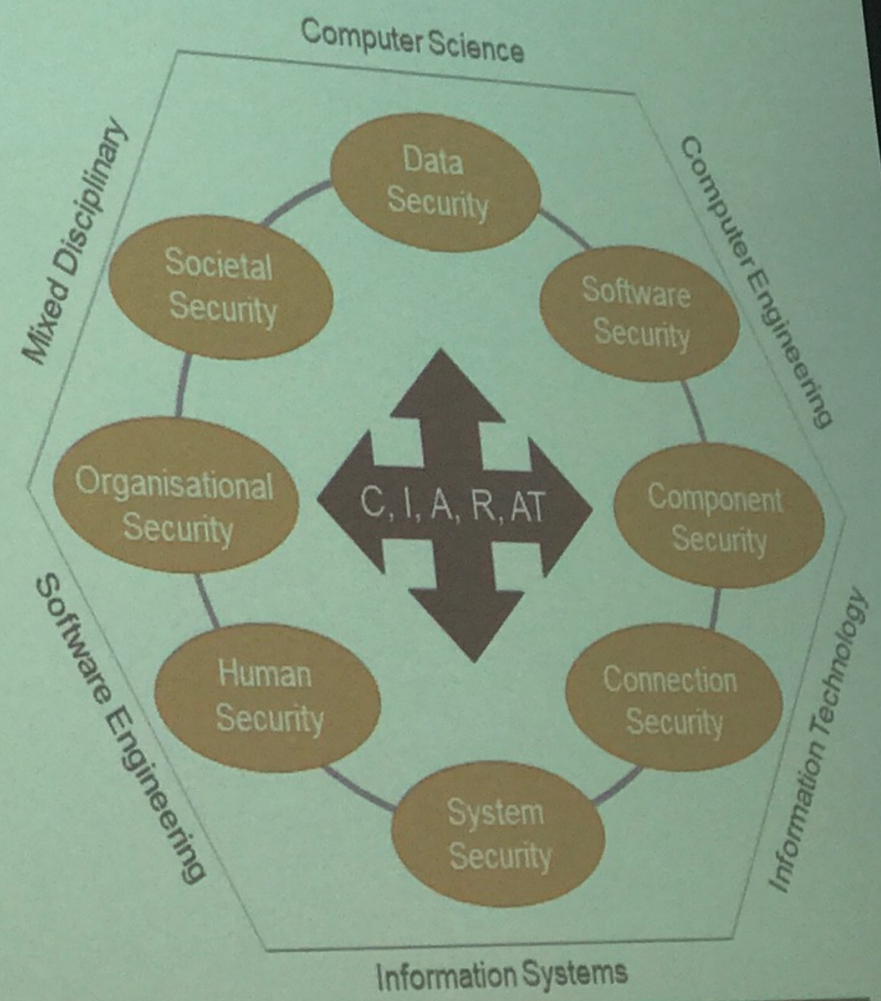
Coursework Master's → preferred by engineering professionals from industry

University of Johannesburg: coursework Master's degree in Systems Engineering. Aim to include cybersecurity module

Towards determining the structure/context for cybersecurity engineering module

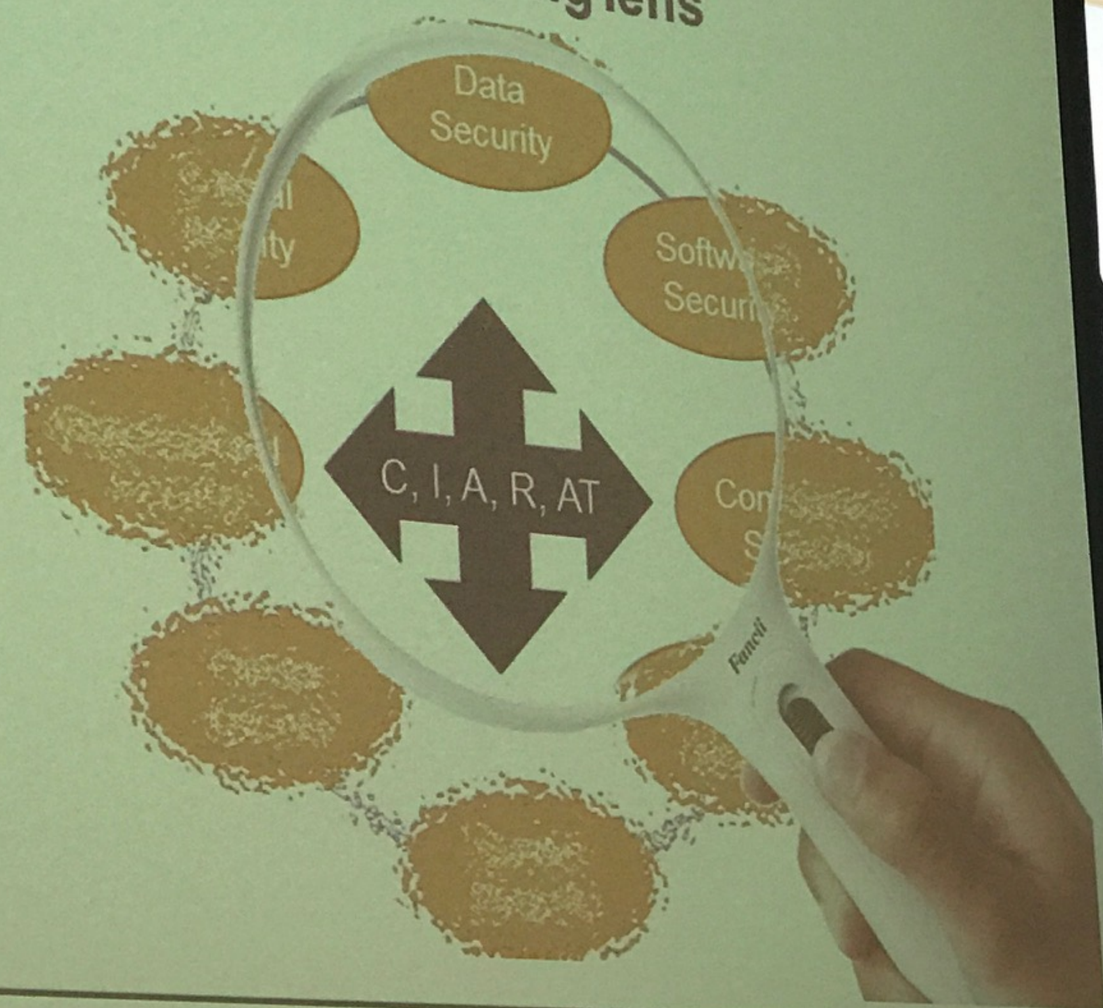
Cybersecurity curricular guidelines

- ACM, IEEE, IFIP WG 11.8 and others- developed the Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity:
  - conceptual knowledge essential to understanding cybersecurity
  - balance of "breadth and depth, along with an alignment to workforce needs"
  - knowledge areas and concepts must be viewed through a disciplinary lens which represents the underlying discipline
- Structure:
  - 8 Knowledge areas (KA's)
  - Essential topics of KA's
  - Cross-cutting concepts
  - **Disciplinary lens**



Cybersecurity knowledge through the engineering lens

- **8 knowledge units:** presented to engineering professionals
- In-depth & semi-structured elite interviews:
  - Engineering professionals in academia (Academic 1 and Academic 2)
  - Engineering professionals in industry (Industry 1 and Industry 2)
  - Professionally registered engineers with ECSA
  - Experienced in systems engineering



Cybersecurity knowledge through the engineering lens

- Detailed table of all knowledge units in 8 KA's presented to participants

Knowledge Area 1-8	Academic 1	Academic 2	Industry 1	Industry 2
Essentials				
Knowledge unit 1				
Knowledge unit 2				
Knowledge unit 3				
…				
Knowledge unit X				

- Essential (E): Included in depth in the module. All essential topics were automatically marked "E" for essential.
- Overview (O): Included to provide a high level knowledge on the topic.
- Too Technical (TT): Not included due to the high technical nature of the topic.
- Additional Content (AC): Relevant and nice to have as additional content.
- Not Relevant (NR): Topic not directly relevant to systems engineering as task might sit with another professional.

Cybersecurity knowledge through the engineering lens

Connection Security. This knowledge areas covers the aspects relating to securing the connections between components, including physical and logical connections.

Knowledge units	Academic 1	Academic 2	Industry 1	Industry 2
Essentials	E	E	E	E
Physical Media	TT	TT	TT	O
Physical Interfaces and Connectors	TT	TT	TT	O
Hardware Architecture	O	TT	TT	O
Distributed Systems Architecture	E	TT	TT	O
Network Architecture	O	TT	TT	O
Network Implementations	TT	TT	TT	O
Network Services	TT	TT	TT	O
Network Defense	TT	TT	TT	O

- Essential (E)
- Overview (O)
- Too Technical (TT)
- Additional Content (AC)
- Not Relevant (NR)

* Same trend with data, component and communication security. No in depth content, only a sufficient overview knowledge

Basic outline of cybersecurity KA's for postgraduate SE studies

General observations:

- SE needs to maintain a holistic view of the system. Technical details of **Data**, **Component** & **Communication** security are not required in depth, only sufficient overview to understand the role of these aspects in system

→**Inclusion of essential topics**

- Good overview of **Human** & **Societal** Security are required by SE.

→Included as overview knowledge units (exception of ethics)

- **Software, Systems** and **Organizational** Security were deemed most important for in depth inclusion

→ Included in overview & in depth

Knowledge Area	Knowledge units included	
	In depth	Overview
Data Security	Essential topics only	-
Software Security	Essentials; Fundamental Principles; Design; Ethics	Implementation; Analysis & Testing; Deployment & Maintenance; Documentation;
Component Security	Essential topics only	-
Connection Security	Essential topics only	-
System Security	System Thinking; System Management; System Testing	System Access; System Control; System Retirement
Human Security	Essential topics	All knowledge units
Organizational Security	Essentials; Risk Management; Security Governance & Policy	Remaining knowledge units
Societal Security	Essentials; Cyber Ethics	Remaining knowledge units

Conclusion

Vulnerability increases with connection - *Gardner, 2016*

- Creation of systems complying with Industry 4.0 environments = highly connected. Must be able to withstand various types of cyberattacks.
- Lack of cybersecurity content in SA engineering education → creates a gap in cybersecurity knowledge amongst systems engineers
- Determine the body of knowledge for the creation of a postgraduate cybersecurity module in systems engineering
- Limitation of this work: input from only 4 professionals - deemed sufficient for preliminary investigation providing a baseline.
- Future work: collection of input from broader spectrum of top-level professionals.