CyBOK

From CyBOK 1.0 to 1.1
What's new and why it matters?

Awais Rashid and Steve Schneider

contact@cybok.org
www.cybok.org

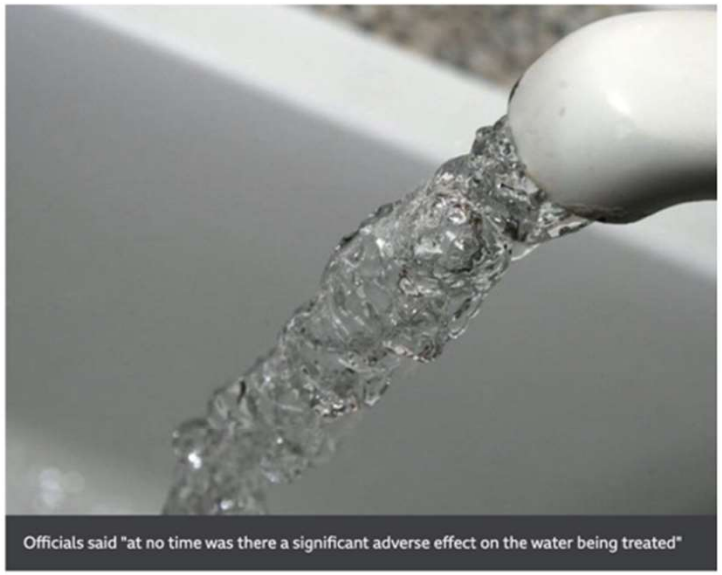
US passes emergency waiver over fuel pipeline cyber-attack

By Mary-Ann Russon
Business reporter, BBC News

5 hours ago

Hacker tries to poison water supply of Florida city

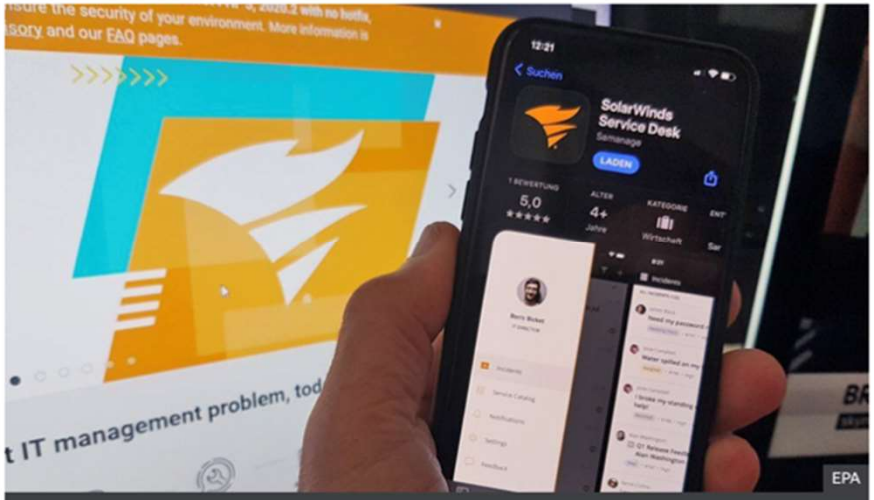
8 February



Officials said "at no time was there a significant adverse effect on the water being treated"

US cyber-attack: Around 50 firms 'genuinely impacted' by massive breach

20 December 2020



Hackers accessed major organisations by compromising software developed by Texas IT firm SolarWinds

US passes emergency waiver over fuel pipeline cyber-attack

By Mary-Ann Russson
Business reporter, BBC News

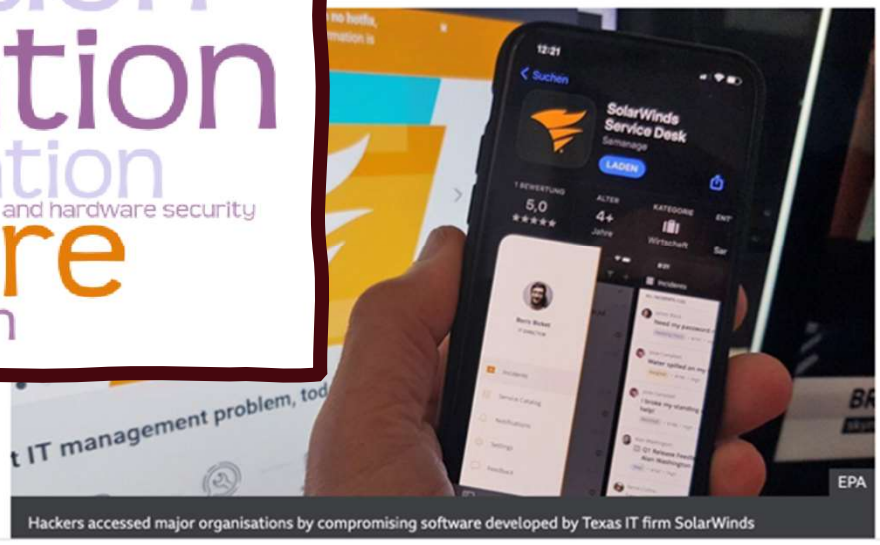
5 hours ago

Hacker tries to poison water supply of Florida city

8 February

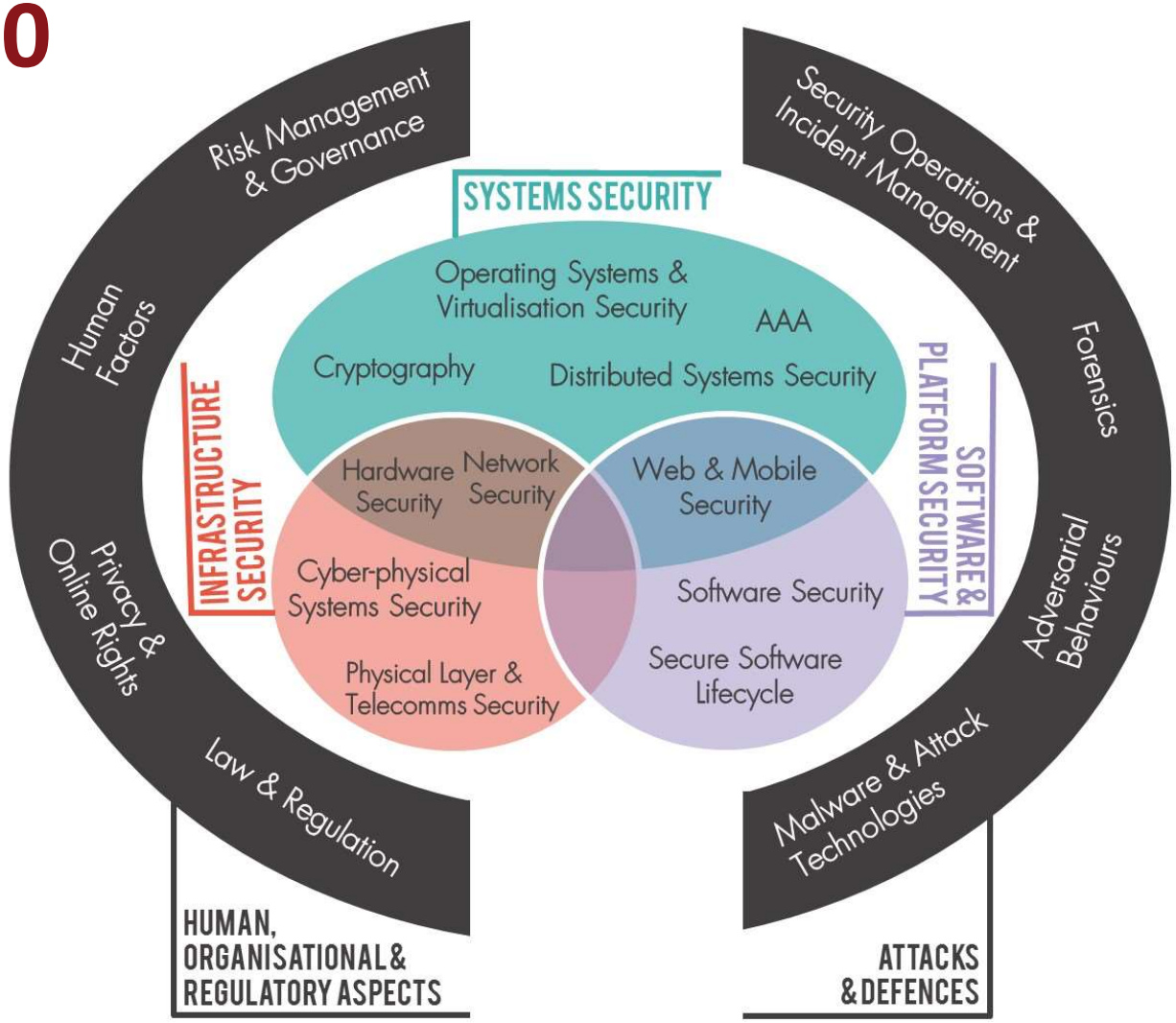
People and security
Risk Management
Intrusion detection
Authorisation
Authentication
Secure communication
Secure networks
Security operations
Software and hardware security
Malware
Supply chain

ck: Around 50 firms pacted' by massive



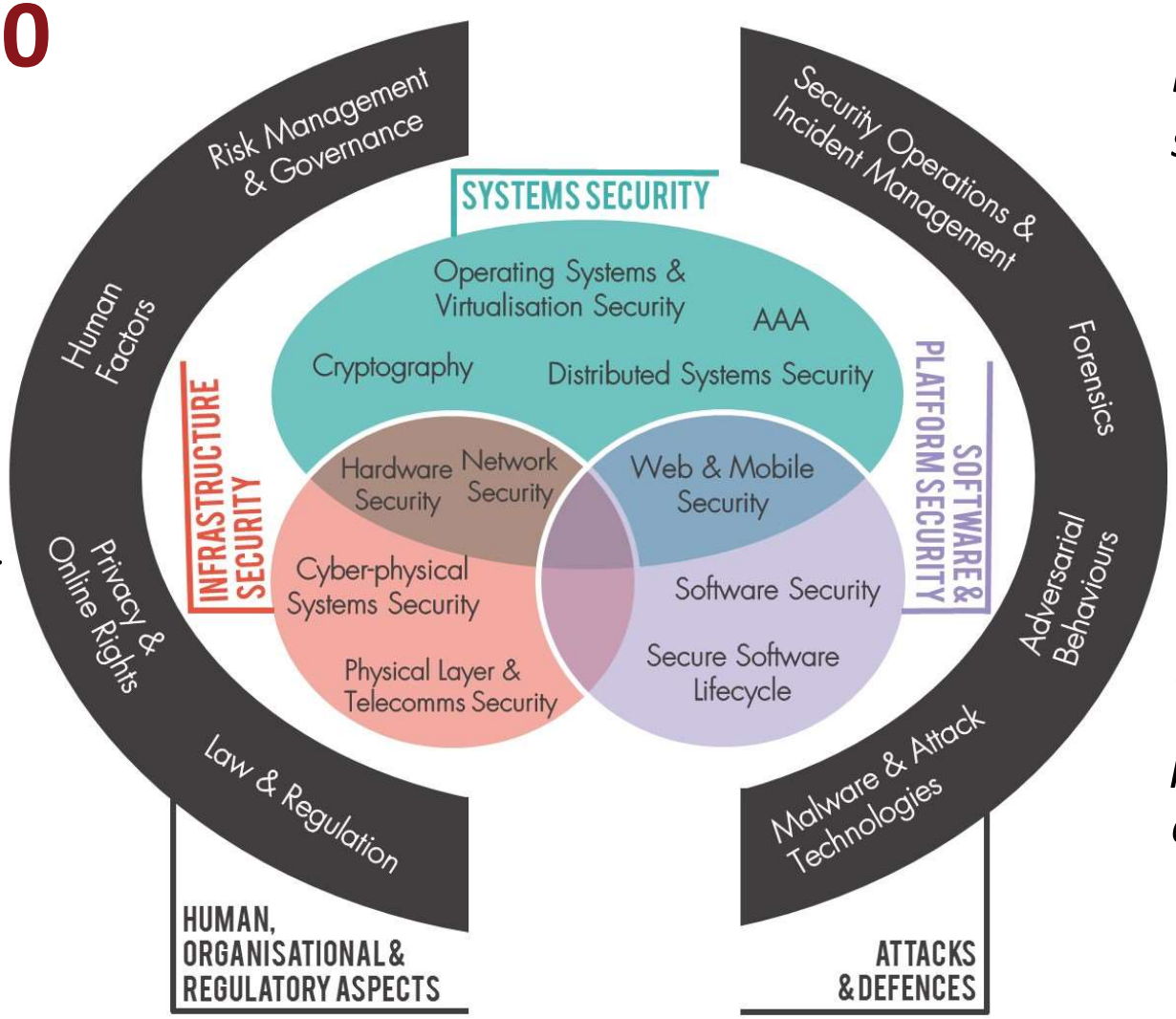
Hackers accessed major organisations by compromising software developed by Texas IT firm SolarWinds

CyBOK 1.0


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

CyBOK 1.0

Understanding different types of network architectures and their security requirements

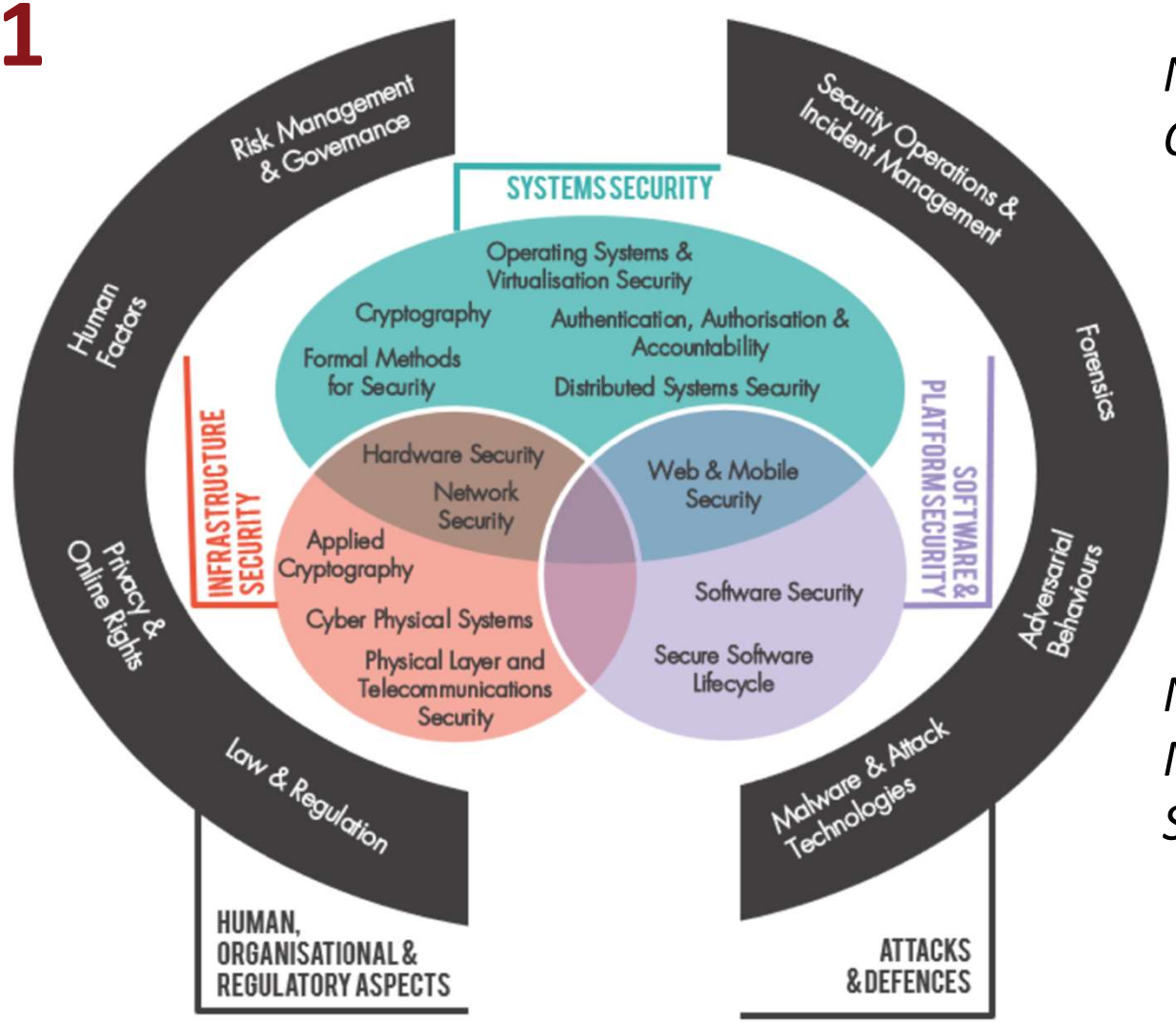


Deploying crypto systems in practice

Verifying security properties of critical systems

CyBOK 1.1

Updated to Network Security KA



New KA on Applied Cryptography

New KA on Formal Methods for Security

>115 Experts: Authors, Reviewers, Advisors

>1000 Pages

>2200 Authoritative sources

>1600 Comments from wider community

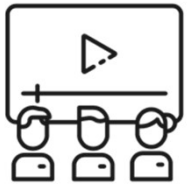
>25 Invited talks, panels and keynotes

CyBOK

The Cyber Security Body of Knowledge

Version 1.1.0
31st July 2021
https://www.cybok.org/

EDITORS
Awais Rashid | University of Bristol
Howard Chivers | University of York
Emil Lupu | Imperial College London
Andrew Martin | University of Oxford
Steve Schneider | University of Surrey
PROJECT MANAGERS
Helen Jones | University of Bristol
Yvonne Rigby | University of Bristol
PRODUCTION
Chao Chen | University of Bristol
Joseph Hallett | University of Bristol



Webinars

Mapping reference with > 13000 terms

An index for easy look up of terms

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

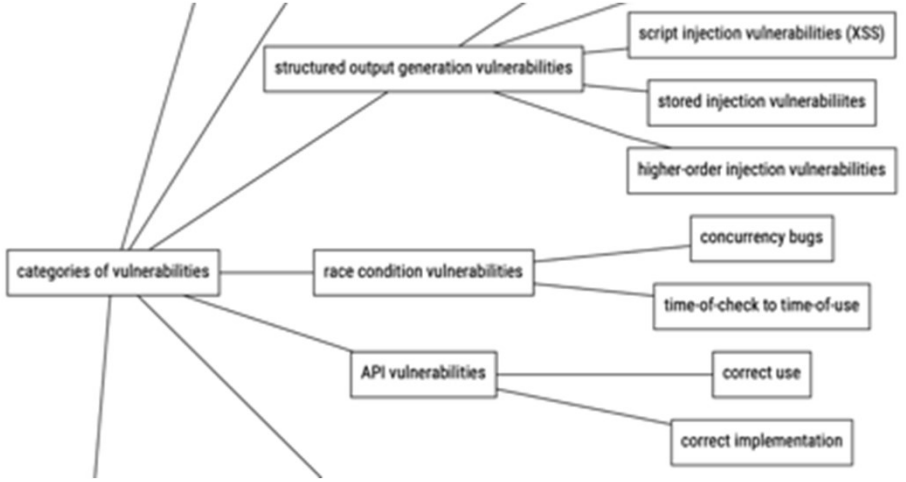
CONTENT

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)

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

A ***guide*** to the body of knowledge: ***established foundation*** of the subject (not on everything that has ever been written or on still-emerging, nascent, topics)

New KA in Applied Cryptography

New KA in Formal Methods for Security

Hacker tried to poison Florida city's water supply

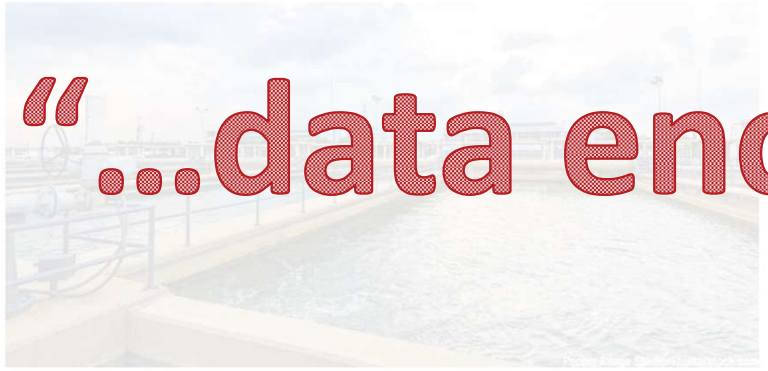
National Security Agency | Cybersecurity & Infrastructure Security Agency | Cybersecurity Advisory

NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems

Summary

Over recent months, cyber actors have demonstrated their continued willingness to conduct malicious cyber activity against Critical Infrastructure (CI) by exploiting Internet-accessible Operational Technology (OT) assets [1]. Due to the increase in adversary capabilities and activity, the criticality to U.S. national security and way of life, and the vulnerability

"Cybersecurity Infrastructure and Security Agency … issued a warning in July that urged all critical infrastructure sectors to be prepared for attacks on operational technology and reduce remote access to OT networks and devices. If such access is required, ***plant operators should ensure networks are segmented, data encrypted and traffic limited to known IP addresses.***"



“…data encrypted…”

Hacker tried to poison Florida city’s water supply

Cybersecurity Infrastructure and Security Agency … issued a warning in July that urged all critical infrastructure sectors to be prepared for attacks on operational technology and urged … remote access to OT networks and devices be secured … required, *plant operators should ensure networks are segmented, data encrypted and traffic limited to known IP addresses.”*

key handling

crypto schemes and strength

Cybersecurity Advisory

NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems

Summary

Over recent months, cyber actors have demonstrated their continued willingness to conduct malicious cyber activity against Critical Infrastructure (CI) by exploiting Internet-accessible Operational Technology (OT) assets [1]. Due to the increase in adversary capabilities and activity, the criticality to U.S. national security and way of life, and the vulnerability

data

implementation

New KA on Applied Cryptography

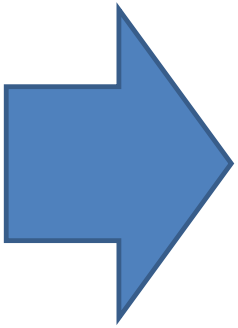
Deploying crypto systems in practice

Author: Kenny Paterson
ETH Zurich

Complementary to Cryptography KA

General principles and practice for use

How to deploy and use cryptography



- Algorithms, Schemes and Protocols
- Implementation
- Standards
- Key Management

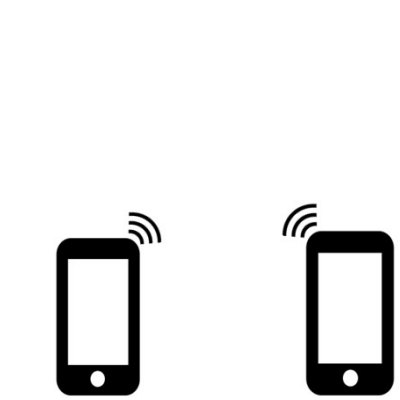
Case Study: COVID19 Contact Tracing

Privacy preservation

Rapid development

2-way privacy preserving 'ping'

Phones exchange beacons

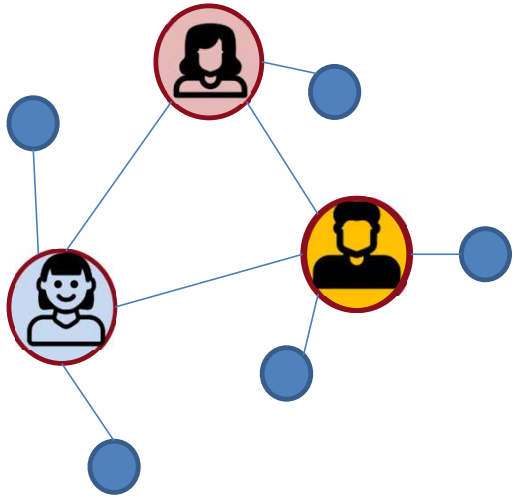


No central lists of contacts

Cryptography at the core

Off-the-shelf cryptography

Simplicity of core design



Used in Google-Apple Exposure Notification (GAEN) system

Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

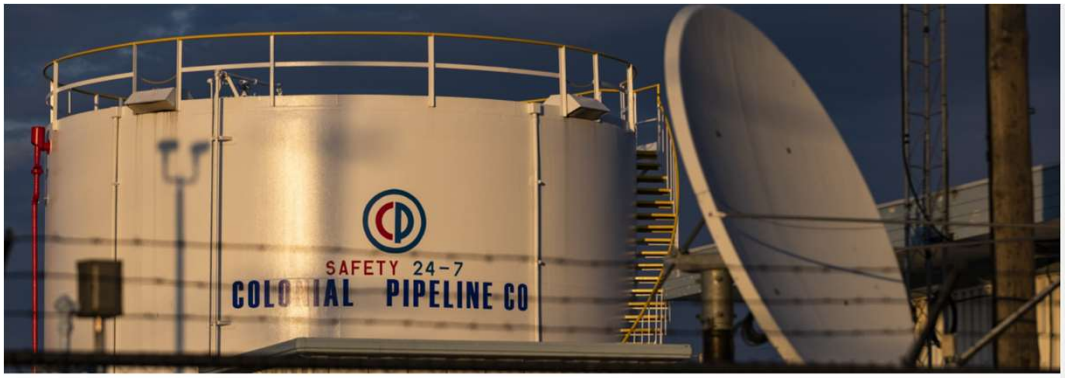
"The account was **no longer in use** at the time of the attack **but could still be used** to access Colonial's network"

X *Inconsistent state*

X *Configuration failure*

Penetrate and patch not adequate for critical systems

Management of detail critical



Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

"The account was **no longer in use** at the time of the attack **but could still be used** to access Colonial's network"

New KA on Formal Methods for Security

verifying properties of critical systems

Rigorous development and reasoning about systems and their components based on mathematics and logic

Author: David Basin
ETH Zurich

Foundations and Methods

Specification via logics, models or code
Verification via algorithms and **tools**

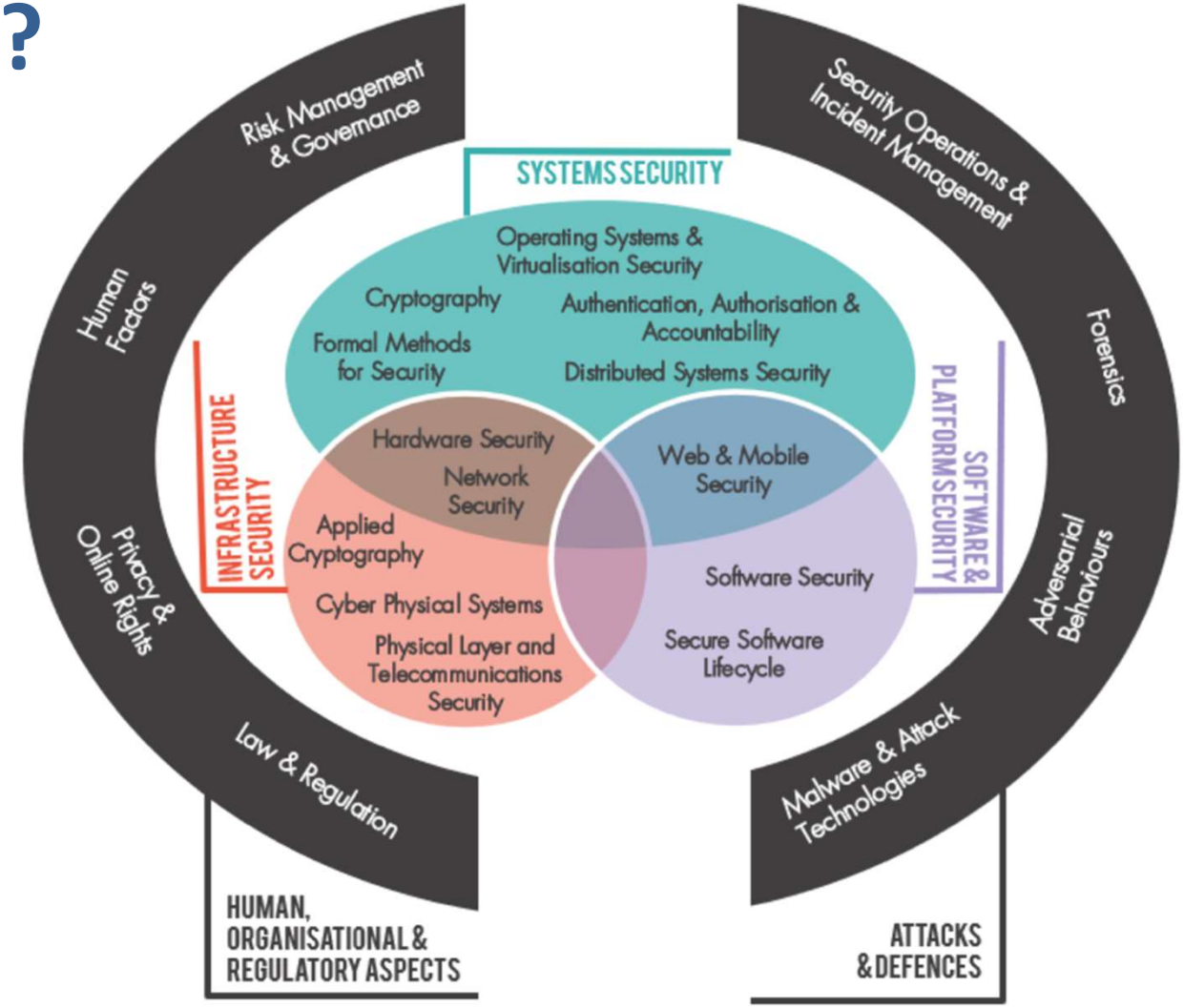
…applied to
Hardware
Protocols
Software and Systems
Configurations

Verifying properties of critical systems

- **SeL4 microkernel verification**
  - **OS critical for security of overall systems**
  - **Data separation**: processes cannot read each other's data
  - **Temporal separation**: processes use resources sequentially, sanitized before being passed on
  - **Damage limitation**: effects of compromises limited

- AWS: Provable Security
- Facebook: Continuous Reasoning

Questions?


Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
Cryptography
Authentication, Authorisation & Accountability
Formal Methods for Security
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Applied Cryptography
Cyber Physical Systems
Physical Layer and Telecommunications Security
SOFTWARE & PLATFORM SECURITY
Web & Mobile Security
Software Security
Secure Software Lifecycle
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
ATTACKS & DEFENCES