A View of Security as 20 Subject Areas in Four Themes

Paul C. van Oorschot Version: 12 Oct 2021[1]

We give a detailed example of organizing security knowledge into themes and subject areas. The aim is to stimulate further independent thought on how to distribute security topics into subject areas around which to build courses supporting a coherent undergraduate security curriculum.

This article conveys a view on organizing major topics in computer and Internet security. We represent the field as twenty subject areas grouped into four themes. This organization serves as an overview of the field, a list of topics for instructors to consider for planning security courses and in building out security curricula, and a reference framework for experts and researchers to consider as broader context for their work. The diversity of topics also illustrates the many different aspects of the term *security*.

This complements a September 2021 article [4], which reviewed various efforts to identify and organize knowledge areas and define standard security curricula reflecting the body of knowledge in the field of computer and network security. Here we give a personal view, noting that identifying specific areas and assigning them to themes is rather subjective.

Our classification gives relatively high visibility to the role of operational security, and beyond this we hope that it may influence some academics to extend their view of what is valuable for students to learn beyond a narrow set of topics that were popular 25 years ago.

There is of course no single "correct" set of areas, themes, or groupings—other classifications will be more suitable for different communities with varying backgrounds and goals. Our view combines industrial experience, academic research, university teaching, and study of prior frameworks [4]. Having been active across a variety of problem areas, engaging with many colleagues over the years, I find the organization given here useful as a framework for considering how subject areas are related, and how topics and themes support each other. My hope is that others, especially those new to the field of security, also find utility in this perspective—and in the exercise of trying to build their own such framework.

Overview of Four Themes

We partition the identified security subject areas into themes labelled as quadrants Q1–Q4. One reason is to identify clusters of topics that are complementary to explore together; others are noted later. It is not our intention to suggest any one theme is more important than others.

We first introduce the themes, then discuss the subject areas. Figure 1 gives the big picture.

Q1: *Software-based Security and Mechanisms.* This theme contains areas that involve the design of software mechanisms and tools that provide defenses, the methods primarily *host-based* in that network communication is not a primary focus (see Q2).

Q2: *Security Engineering, Networking and Hardware.* The areas in this theme primarily involve building systems and products with a large role played by network communication to enable component interaction in distributed systems.

Q3: *IT Operations Security, Incident Response and Recovery.* Areas here involve real-world operation of Information Technology (IT) systems and products (vs. designing and build-

[1] (c)IEEE *Security & Privacy* 20(1): 102–108, 2022, at `https://ieeexplore.ieee.org/document/9693428`

ing). This includes addressing instances of malicious activity to keep enterprise organizations running, and system administrators (sysadmins) configuring deployed systems.

Q4: *Security in Society and Human Organizations.* This addresses policy, governance, legal issues and human factors, also privacy, anonymity, and related issues. These are often under-represented in courses with narrow focus on technical aspects dominating Q1–Q3.

Any pigeonholing of subject areas into themes will be imperfect—subjects rarely fit single groups perfectly, and each subject can be explored from several angles (thus Fig. 1 often suggests a second theme to which an area is closely related). Nonetheless, we believe that an understanding of the field is aided by having in mind *some* framework for organizing topics, even if only as a starting point to develop one's own preferred framework.

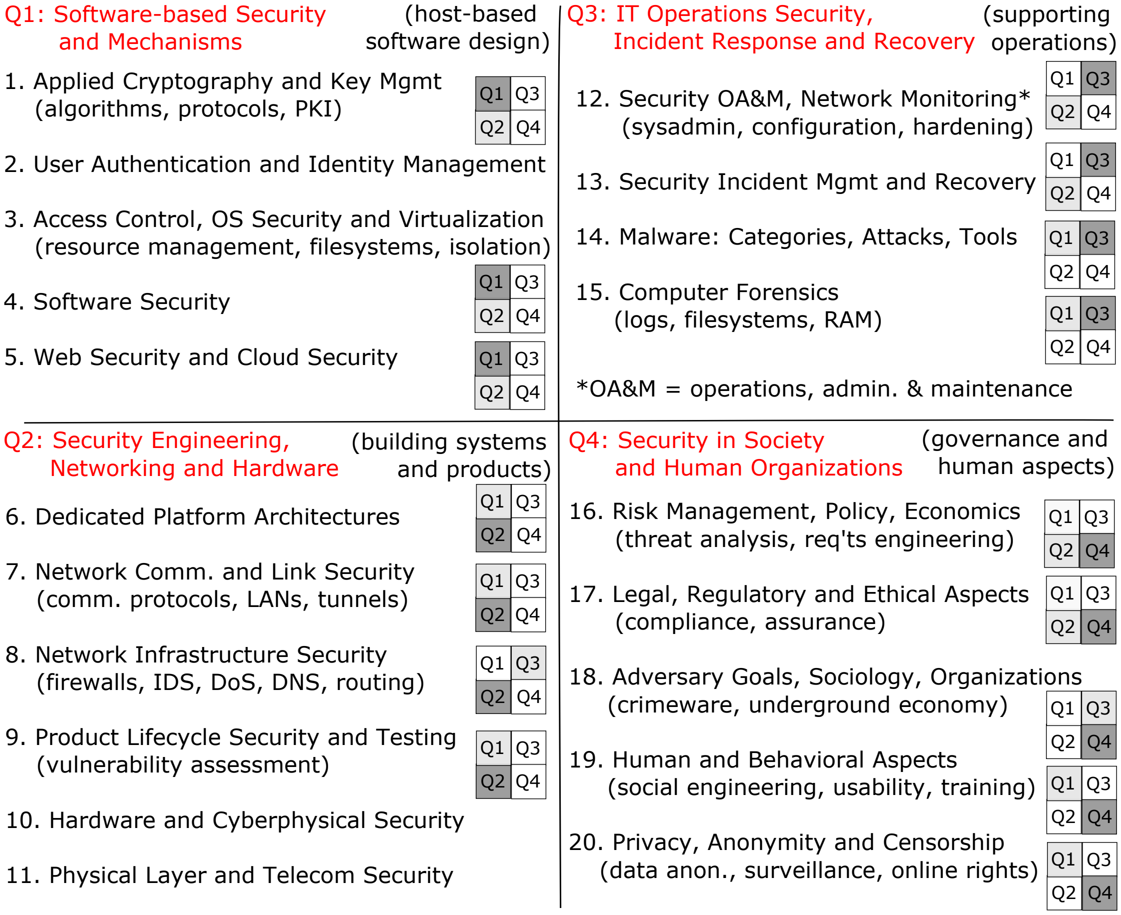
Q1: Software-based Security and Mechanisms
(host-based software design)
1. Applied Cryptography and Key Mgmt (algorithms, protocols, PKI)
Q1 Q3 Q2 Q4
2. User Authentication and Identity Management
3. Access Control, OS Security and Virtualization (resource management, filesystems, isolation)
4. Software Security
Q1 Q3 Q2 Q4
5. Web Security and Cloud Security
Q1 Q3 Q2 Q4
Q2: Security Engineering, Networking and Hardware
(building systems and products)
6. Dedicated Platform Architectures
Q1 Q3 Q2 Q4
7. Network Comm. and Link Security (comm. protocols, LANs, tunnels)
Q1 Q3 Q2 Q4
8. Network Infrastructure Security (firewalls, IDS, DoS, DNS, routing)
Q1 Q3 Q2 Q4
9. Product Lifecycle Security and Testing (vulnerability assessment)
Q1 Q3 Q2 Q4
10. Hardware and Cyberphysical Security
11. Physical Layer and Telecom Security
Q3: IT Operations Security, Incident Response and Recovery
(supporting operations)
12. Security OA&M, Network Monitoring* (sysadmin, configuration, hardening)
Q1 Q3 Q2 Q4
13. Security Incident Mgmt and Recovery
Q1 Q3 Q2 Q4
14. Malware: Categories, Attacks, Tools
Q1 Q3 Q2 Q4
15. Computer Forensics (logs, filesystems, RAM)
Q1 Q3 Q2 Q4
*OA&M = operations, admin. & maintenance
Q4: Security in Society and Human Organizations
(governance and human aspects)
16. Risk Management, Policy, Economics (threat analysis, req'ts engineering)
Q1 Q3 Q2 Q4
17. Legal, Regulatory and Ethical Aspects (compliance, assurance)
Q1 Q3 Q2 Q4
18. Adversary Goals, Sociology, Organizations (crimeware, underground economy)
Q1 Q3 Q2 Q4
19. Human and Behavioral Aspects (social engineering, usability, training)
Q1 Q3 Q2 Q4
20. Privacy, Anonymity and Censorship (data anon., surveillance, online rights)
Q1 Q3 Q2 Q4

Figure 1: **Partition of security subject areas into four themes.** Shaded boxes note a secondary quadrant for given areas. Short forms: Mgmt (management), PKI (public key infrastructure), OS (operating system), Comm (communication), LAN (local area network), IDS (intrusion detection systems), DoS (denial of service), DNS (domain name system), sysadmin (system administration/administrator), RAM (random access memory), req'ts (requirements).

Characteristics of the Themes

We now explain the ideas underlying the theme-based organization. The first three themes progress from fundamentals and basic design, to building hardware-software systems, to operating these in practice; the fourth is cross-cutting, holding thorny interdisciplinary issues.

Theme	Characterization	Natural Home Department	Target Participants
Q1	software and algorithms for defensive purposes	computer science (CS), also mathematics (for cryptography)	security mechanism experts, cryptography experts
Q2	systems with comm. networks and physical components	systems and computer engineering (SCE)	security engineers and system builders
Q3	operations to mitigate actual security incidents	information tech. training and industry certification programs	IT operations, sysadmins, security consultants
Q4	policy and societal aspects of security	social sciences, management, international affairs, law schools	users, managers, regulators in society, bad actors

Table 1: **Themes to trigger thought on how to cluster complementary security subject areas**

Each theme has a few dominant characteristics, as given in Table 1—for example, software and algorithms characterize Q1, with Q2 more about hardware-software networked systems.

The themes also broadly reflect discipline-based approaches to security, mirroring historical foci of university departments (again see Table 1) ranging from CS/Math departments, to Systems and Computer Engineering (SCE), Information Technology (IT) schools, and an interdisciplinary collection of departments providing expertise in Q4.

The themes also tend to map to required skills or perspectives of different classes of target participants (again, Table 1). For example, Q1 addresses the interests of security mechanism experts and cryptography experts, and Q3 those of security operational staff in enterprise organizations. This and the discipline-based approaches suggest that many subjects may be approached from the perspective of several themes, to reflect priorities of different target participants and instructor end-goals.

To make informed selections of subject areas to learn or teach, we suggest explicitly identifying the target of a given course—is it software designers aiming to be security experts or generic developers? Hardware designers and builders of physical systems? Sysadmins and IT specialists who will operate existing technology products? Or management staff responsible for business operations; policy experts; or all of society, as non-expert everyday computer end-users?

Keeping these targets in mind may also help learners and instructors to make conscious choices of which subject areas and themes to prioritize. In contrast, note that in many non-security domains the set of potential target participants is far narrower—e.g., a CS course in data structures and algorithms may target students likely to go on to be software programmers, or a fraction proceeding to grad studies for research careers.

This breadth of target participants and academic units spanned by security justifies the Association for Computing Machinery (ACM) treating security (Cybersecurity) as an independent discipline alongside five others (Computer Science, Computer Engineering, Software Engineering, Information Technology, and Information Systems) in their Computing Curricula 2020 [2].

The various approaches to security across academic units may also confuse practitioners interested mainly in security outcomes and what actually goes wrong in practice. While a tussle between theory and practice appears in many domains, an example in security is the dominance of cryptography (the oldest and most mature subarea) by mathematicians who excel in theory, formalisms and proofs. The mathematical nature of computer programs led this same group to play a major role in establishing the first computer science departments (along with hardware engineers). This is perhaps one reason that cryptography still dominates security course offerings at many institutions—together with the maturation of cryptography ahead of other security subareas, plus academic inertia—despite arguments that other subject areas such as systems security and software security are of greater utility to the many computer science and engineering students who will enter the workforce as software developers.

As a side note, one danger in theory-based approaches to security is over-confidence in models [3]. Models necessarily omit details, but details impact security; and, assumptions underlying models may simply fail in a practical environment. Given the gaps between theory, and real products fielded in hostile environments, the framework of Figure 1 leans towards practical security, informed but not dominated by theory. Being relatively high-level (focusing on core topics), it also does not cover all research areas (e.g., see [5]), nor finer sublevels as given in the *Security and Privacy* taxonomy of the ACM Computing Classification System [1].

The many different meanings of the term *security* across academic disciplines often leads to confusion. In CS and engineering, security is synonymous with information technology; in the social sciences, it may mean international policies and agreements. Non-experts commonly conflate cryptography (mathematics-based algorithms and protocols), security (encompassing broader engineering and systems issues, including idiosyncrasies of programming languages and run-time support), and privacy (often focused on controlling personally identifiable information). However, other complex fields such as health sciences have analogous challenges.

We now discuss in turn, the subject areas that we have identified within the four themes.

Q1: Software-based Security and Mechanisms

In quadrant Q1, the subject or knowledge areas (labelled K*i*) provide defensive security mechanisms and technologies built largely in software.

K1: Applied Cryptography and Key Management. This area begins with cryptographic algorithms for encryption and authentication, and includes key establishment protocols to provide keying material for those algorithms, and broader public key infrastructure (PKI) mechanisms for management of public and private keys. PKI overlaps with systems topics in Q2's domain.

K2: User Authentication and Identity Management. Here methods include, e.g., passwords, biometric authentication, and physical tokens (often implementing protocols based on public key algorithms). These fall under the broader area of identity management, with user identities commonly serving as the basis for access control decisions implemented by local or remote operating systems. Approaches include password managers and single-sign-on systems.

K3: Operating System Security. Many core elements of computer security are included here, such as filesystem permissions, isolation mechanisms, and general resource management (e.g., of CPU cycles, network communication ports, RAM and secondary storage, input-output peripherals such as keyboards and printers). Security design principles are often introduced here.

K4: Software Security. This addresses attacks that aim to exploit vulnerabilities related to software implementation, specific programming languages, and their runtime support systems, in many cases involving exploitable flaws in the management of dynamically allocated memory. The headline example is a buffer overflow vulnerability, and related attacks that alter program control flow; other categories include exploitation of race conditions, errors in resolving filenames to their intended resources, and integer-based vulnerabilities (e.g., unexpected errors in the automated conversion of short to long integers in the C programming language). Since such software security issues exist in both dedicated security products and generic software, knowledge about software security is relevant to all software developers, not security experts alone.

K5: Web Security and Cloud Security. The web security elements of this area include security issues related to the browser-server ecosystem involving the HTTP protocol, HTTPS (HTTP secured using the TLS protocol), web servers supporting these protocols, and web-related exploits such as cross-site scripting, cross-site request forgery, and SQL injection. Cloud security elements involve security issues related to the architecture and use of infrastructure and applications outsourced to cloud services, often accessed via web protocols. This overlaps with secure OS isolation and virtualization (K3), trusted computing (K6 overlapping K10), and secure remote access (K7).

Not all security topics fit cleanly into one subject area or quadrant. For example, while we see Internet browser security fitting best under web security (K5 in Q1), it also fits K6 in Q2 if one views browsers as platforms. Also, while we place operating systems themselves in Q1, the majority of other "systems" subareas are assigned to Q2. Two reasons are that we make Q1 the focal point for the many security mechanisms that comprise OSs; and in operating systems, the networking aspects (a central characteristic of Q2) are largely isolated in network stack components. We do, however, place into Q2 real-time OSs (under K10), as they address critical timing requirements arising in physical systems, and their systems engineering aspects fit Q2 better.

Likewise, smartphones fit several areas, based on whether they are viewed from the perspective of an OS (K3), a platform (K6), a product (K9), or telecom device (K11); they also commonly support Wi-Fi (K7), and have unique characteristics as mobile systems, and hardware devices with a multitude of sensors. In our view, smartphones and other mobile systems are complex platforms best fitting K6; this also avoids creating a separate knowledge area for every class of hardware-software device.

Q2: Security Engineering, Networking and Hardware

A main theme of quadrant Q2 is systems—building them, and checking to the best extent possible, that they meet security requirements. We also make Q2 the primary home of security issues related to networking and communication protocols. As background review: the Internet *network stack* is composed of a Link layer (Ethernet, 802.11), above which is the Network layer (IP, ICMP, IPsec), then the Transport layer (TCP, UDP, TLS), and the Application layer.

K6: Dedicated Platform Architectures. This area covers security related to special-purpose platforms that offer an application programming interface (API) to other applications. Examples are database systems; social network platforms; distributed computing platforms such as Bitcoin and Ethereum supporting blockchain applications; and cloud-based platforms supporting third-party software (e.g., Samsung's *SmartThings* Internet of Things platform for smarthome devices). We also include so-called trusted execution environments (TEEs), often categorized under *trusted computing* (overlapping K10); and *distributed applications* (including distributed filesystems and peer-to-peer file-sharing applications), i.e., applications with components running on distinct processors, often geographically separated.

K6 excludes general OSs (K3), generic software security (K4), and routine security analysis of applications (K4, K9). It aims to capture classes of problems unique to dedicated platforms, with a focus on major frameworks that other applications trust (rely on). K6 may be treated as a specialty (vs. core) area, due to the nature and number of dedicated platforms.

K7: Network Communications and Link Security. This area includes security issues at the link layer of the network stack—corresponding to both wired and wireless local area network (LAN) links, e.g., respectively Ethernet and IEEE 802.11 (Wi-Fi); virtual private networks (VPNs) and IPsec (the IP security suite); security tunnels and secure remote communications, e.g., using Secure Shell (SSH); and the address resolution protocol (ARP), which maps media access control (MAC) addresses to IP addresses.

K8: Network Infrastructure Security. Example topics are network perimeter defenses such as firewalls and intrusion detection systems (IDS); the domain name system (DNS), mapping domain names to IP addresses; methods to mitigate denial of service (DoS) attacks; and routing security.

K9: Product Lifecycle Security and Testing. This area covers security in the product development lifecycle, including security assessment both throughout design stages and (overlapping Q3) in deployed environments; static and dynamic analysis including *fuzzing*; and secure software update, part of product maintenance (again overlapping K12).

K10: Hardware and Cyberphysical Security. This area includes customized hardware to support security operations such as cryptographic acceleration, random number generation from hardware sources, and trusted computing (K6); security in real-time and embedded systems, and in cyberphysical systems (which join the digital world to the physical world including the Internet of Things or IoT); and hardware-based security protection, physical tamper-resistance, physical interfaces to chips (e.g., JTAG interfaces), and defenses against *side-channel attacks* that leverage physical properties (e.g., timing, power analysis, speculative execution).

K11: Physical Layer and Telecom Security. This area includes communication security issues at the physical layer (layer 1 in the ISO stack, or the physical part underlying the Internet stack's data-link layer); security issues related to (evolving) telecommunications networks, which mobile devices may leverage through wireless access links; jamming of radio signals; and TEMPEST technologies (electromagnetic emanation intelligence gathering and defences).

We add here a comment on *network security*. When this term was used in the early 1990s, a main focus was (often software-based) encryption and authentication algorithms used for remote login and access. This term has evolved and now often signals a focus on security issues related to routers, hardware middleboxes, firewalls, network IDSs, and their interaction with network infrastructure protocols. Our organization of security per Figure 1 concentrates network security in Q2, supported by other areas including K1 (PKI), K2 (authentication) and K3 (access control).

Q3: IT Operations Security, Incident Response and Recovery

The theme of quadrant Q3 is security in the operation (vs. the design or building) of computer and communication networks and infrastructures, and methods to respond and recover from the actions of bad actors. Thus a focus is reactive measures when something goes wrong (vs. purely preventative measures); these often involve tools that require ongoing monitoring, as opposed to "set-and-forget" defenses.

K12: Security OA&M and Network Monitoring. Operations, administration and maintenance (OA&M) is a familiar term in telecommunications. This area includes security issues related to OA&M in the deployment, management, and monitoring of computer systems by information technology staff; and security-related tasks carried out by sysadmins such as system setup and *hardening*, e.g., configuring software systems and tailoring functionality to reduce risks. These activities are prior to or separate from analysis of specific security incidents (K13). *Pen-testing* (penetration testing, related to K9) on live systems may also be included here, as it is specific to a given deployment environment.

K13: Security Incident Management and Recovery. Here the focus is responding to malicious activity instances that impact an organization's computer and communications infrastructure and user systems, through use of network and system defensive technologies largely from Q2. This includes analysis of host and network logs, and use of intrusion detection and anti-malware tools to understand and report on incidents, and restore software and data (e.g., from automated backups) as necessary for recovery and continuity of business operations.

K14: Malware Categories, Attacks and Tools. This area focuses on understanding the methods and technologies used by malicious parties, and distinct classes of malware such as computer viruses and worms, ransomware, and rootkits. Malware may employ social engineering (tricking users into installing otherwise unauthorized software), or self-install by exploiting software security vulnerabilities (K4). Important skillsets (also for K4, K13, K15) include binary analysis and tools for reverse engineering and modifying executable code.

K15: Computer Forensics. This area involves preserving and extracting information from digital sources, often to aid prosecution of criminal activity (organized crime, fraud, child exploitation) or civil litigation (e.g., discovery of electronic documents), ideally so as to retain its utility as legal evidence. Data may be recovered from, e.g., log files, volatile memory (RAM), or filesystems, including metadata on secondary storage, and by reconstructing deleted files. Different techniques and customized tools tend to be required for individual memory management schemes, operating system versions, and filesystems used within such versions.

Q4: Security in Society and Human Organizations

The theme of quadrant Q4 is security governance, policies, and human aspects. It may be viewed as covering, in part, what some call layers 8–10 [6] above the 7-layer OSI network stack, namely the organization, government, and international layers (others may refer to users as layer 8).

K16: Risk Management, Policy and Economics. This area addresses practical aspects of risk modeling, security policies, and threat analysis, taking into account not only technical security requirements but economic factors such that the costs of defenses do not exceed projected benefits. This also involves requirements engineering (intersecting K9).

K17: Legal, Regulatory and Ethical Aspects. This area addresses national and international laws specific to computer security (e.g., cybercrime laws, law enforcement access and key escrow, compliance with commercial regulations), formal product assurance through product certification programs, and privacy laws related to K20. Examples of ethical issues are responsible disclosure for product vulnerabilities, leaving vulnerabilities unfixed, ethical hacking, and addressing ransomware demands.

K18: Adversary Goals, Sociology and Organizations. This area covers sociological and sociotechnical (vs. purely technical) aspects of agents behind crimeware and related attacks, classes of adversaries, their motivations, and the organization of underground economies.

K19: Human and Behavioral Aspects. This area involves human factors related to security and privacy, such as social engineering, phishing, user-centered security and usability, user compliance with policies, training, and online rights (related to K17, K20).

K20: Privacy, Anonymity and Censorship. This area addresses privacy issues such as anonymity, pseudonymity, untraceability, surveillance, censorship, and data anonymization. To centralize discussion, K20 covers both technical and non-technical aspects related to privacy, with clear ties to human-centric issues (K19) and legal issues (K17).

Systems Security

We have no subject area dedicated to *systems security*, viewing it as too broad—spanning several subject areas of Q1 and Q2, including operating systems (although some OS courses are light on networking and hardware aspects). We have also not explicitly defined a theme around systems security, despite Q2 being largely about building systems and products; doing so would leave as leftovers an odd set of "non-system" areas.

Here *systems*, short for *computer systems* or *systems and networking*, generally refers to computer-related systems that include computing and communications, and typically also hardware components. *Systems security* includes issues related to the design, function, and side effects of all components that may influence the behavior of other components; in our view, it includes network security. Systems security anticipates malicious agents; if only benign failures are of interest, the term *dependable systems* is often used.

Methodology-based Subject Areas

Some specialized security courses are built on specific methodological approaches, such as:

- formal methods for analysis of cryptographic protocols, e.g., as heavily used in the evolution of TLS 1.3, or to establish system properties as in the formal verification of the seL4 microkernel, where proofs were given to support the attainment of first functional properties and then selected security properties;
- use of binary analysis tools on executable code, e.g., to reverse engineer malware, or binary rewriting tools to add control flow integrity checks to legacy software; and
- user studies as a methodology to understand and advance human-centered security, e.g., in the usability analysis of user authentication methods or security toolkit interfaces.

None of our subject areas are defined solely on a methodological approach. We prefer instead to introduce methodologies (multiple where useful) as elements of a subject area, when the fit to the problems of that area is strong. Thus our subject or knowledge areas are defined by problems to be addressed, rather than specific solution methodologies.

Concluding Remarks

While some areas could equally well be assigned to other themes, we have declared one "home" theme for each, as a baseline for discussion. Any questions this raises are themselves likely more important than the ultimate placement of a subject area in a particular theme.

Independent of the theme a subject area is assigned to, a course on that subject may be delivered emphasizing the characteristics of any theme. Consider a course on malware (K14). If delivered from the perspective of Q3 (IT Operations), the operational aspects of addressing malware incidents may be covered, whereas if delivered from the perspective of Q1, it might instead focus on the design of anti-malware mechanisms. In this spirit, to train students for jobs in operational security, all subjects in Q3 deserve consideration before subjects in other themes.

If one views Q1 as the realm of computer science and Q2 as engineering, then we may expect a course spanning Q1 and Q2 to be delivered differently if taught in a CS rather than an engineering department—e.g., the latter may give heavier focus to hardware or network aspects.

While our high-level view omits many specialized topics and research areas, these can be placed into context using our themes and subject areas as a top-level taxonomy. Specialized topics may draw heavily from all themes—e.g., electronic voting has strong ties to K6 (dedicated platforms) and K3 (software security), but involves technical, operational and societal elements.

Historically, security courses and textbooks have focused heavily on Q1 and parts of Q2, leaving Q3 to be picked up in practice, and often avoiding Q4's non-technical topics (beyond the expertise and interest of old-school security experts). In contrast, enterprise users and managers may see Q3 as the center of action, and elements of Q4 critically important to ensure that organizational security goals and obligations are met. There is now a growing recognition that achieving security in practice requires a holistic combination of elements from all themes and essentially all the listed subject areas. How to find space in curricula and textbooks for all these is an open problem.

It should be clear that many alternative criteria could be used to identify subject or knowledge areas and themes in security. We have provided one instance of such an exercise, at a relatively coarse-grained level. As such, this article may also serve as an overview of core topics in computer and Internet security, for those new to the field.

References

[1] Association for Computing Machinery. ACM Computing Classification System (2012), "Security and Privacy" category, https://dl.acm.org/ccs

[2] Association for Computing Machinery (ACM). Computing Curricula 2020 (CC 2020). https://www.acm.org/education/curricula-recommendations.

[3] C Herley, P C van Oorschot. Science of Security: Combining Theory and Measurement to Reflect the Observable. *IEEE Security & Privacy* 16(1):12-22, Jan-Feb 2018.

[4] P C van Oorschot. Coevolution of Security's Body of Knowledge and Curricula. *IEEE Security & Privacy* 19(5):83-89, Sept-Oct 2021.

[5] A Rashid, H Chivers, G Danezis, E Lupu, A Martin. CyBOK: The Cyber Security Body of Knowledge. Version 1.0, 31 Oct 2019, https://www.cybok.org

[6] P P Swire. A pedagogic cybersecurity framework. *Commun. ACM* 61(10):23–26, Oct 2018.