Opening sentences in academic writing

How security researchers defeat the blinking cursor

Anonymous Author(s)

ABSTRACT

Education in information technology focuses on stakeholders like teachers, undergraduate students, and employers. Researchers also educate themselves about new results, technologies, and research areas. An important vehicle in this self-education process is reading peer-reviewed academic papers, which also form the basis of some graduate-level research courses. Technical writing skills are important in this domain as well. In this paper, we study the first sentence used by researchers in opening their academic papers to draw the reader in. We used a corpus of 379 top tier research papers in cybersecurity and applied coding techniques from grounded theory to create a taxonomy of 14 types of opening sentences, categorized into 5 general types. In this paper, we discuss each type with numerous examples, and we reflect on what we learned about writing after examining all of these sentences.

CCS CONCEPTS

• **Social and professional topics** → **Information technology education**.

KEYWORDS

Scientific Writing, Information Systems, Education, Cybersecurity

1 INTRODUCTION

How do researchers start their papers? The opening sentence of a paper needs to be bold, convey the importance of the subject of the paper, and hook the reader. That is a lot to put into a single sentence. The novelist Stephen King is said to spend "months or even years" writing an opening sentence [31]. The academic Steven Pinker notes that,

> "Good writing starts strong. Not with a cliché ('Since the dawn of time'), not with a banality ('Recently, scholars have been increasingly concerned with the question of . . . '), but with a contentful observation that provokes curiosity." [62]

In this paper, we study 379 papers from the field of information systems security. We use a variant of grounded theory [36] to classify the opening sentences of each of these papers according to what the sentence is doing to advance an argument and engage with the reader. For example, a paper might start with a historical fact, argue the importance of the subject, tell a story, or open with a question (as this paper itself does). We develop 5 main categories, with 14 sub-types in total. We provide many examples of each and a guide to distinguishing them.

While this project might seem superfluous, we want to raise awareness about the importance of good writing within research papers. We have noted that the education of information technology and computer science (*e.g.,* SIGITE and SIGCSE) domains have a blindspot for technical writing skills when it comes specifically to research papers. We hope to instigate research in this area given the important role that papers play in allowing experts to educate other experts, as well as in the training of students.

Relevance to Education. An important aspect of education is setting an effective curriculum within the classroom. Technical writing is now considered an essential communication skill (ACM/IEEE Computing Curricula 2020 [21, 22]). In part, this is founded on research dating back to the 1990s on how to move writing from the English department into computer science and information technology [33, 42, 61, 71].

In this paper, we look at technical writing from a different angle. We concentrate on peer-reviewed research papers and assert that academic papers are one of the primary vectors for communication and education of new ideas between researchers. A written paper can reach a much wider audience than attendees at a conference where the research is presented or those with who benefit from direct communication with an author. Beyond this, academic papers are used in the classroom, particularly in course offered to graduate students.

Source Data. Before initiating our work, we were unsure if it would be possible to understand the opening sentences of academic papers without some domain knowledge of the field (we discuss our conclusions on this in Section 4). Thus we made the initial decision to look at papers from our own research area: security.

The field of security has hundreds of conferences and workshops but is recognized as having four top conferences (as ordered within a calendar year): *The Network and Distributed System Security Symposium (NDSS)*, *IEEE Symposium on Security and Privacy*, *USENIX Security Symposium*, and *ACM Conference on Computer and Communications Security (CCS)*. These conferences have considerable overlapping authors[1] and program committee members, and we hypothesize (but did not test) that the analysis would be invariant to which conference the papers came from.

We selected *USENIX Security*, which has always offered its proceedings as open access, allowing us to side-stepping any potential copyright issues with opening our dataset and work. It also offers its proceedings in formats that were useful for our project: *i.e.,* all papers in a single file; and epub format in addition to pdf. We used three consecutive years (2014–2016) for a total of 379 papers [1–3].

[1] System Security Circus 2020: http://s3.eurecom.fr/~balzarot/notes/top4

SIGITE '21, October 06–09, 2021, Snowbird, UT

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

We analysed every opening sentence from the main body of the paper (as opposed to the abstract).

Access. Our raw data, the full set of original papers, and the full set of our codes are available as an NVIVO database as a public GitHub repository: (link removed for anonymity).

2 PRELIMINARIES AND RELATED WORK

Opening Sentences. Our idea to examine opening sentences came from Pinker's style guide [62], which is devoted in part to improving technical, scientific, and academic writing. Pinker also devotes a section of the book to the role of the opening sentences of a work (illustrating with popular non-fiction books). When we reflected on our own difficulty with 'getting a paper going,' we conceived of this project. To our knowledge, opening sentences have not been systematically categorized before. In an older paper, King looks at opening sentences in medical research [44]. The article provides stylistic advice—draw the readers' attention, be concise and clear about stating the main theme of the paper—and he gives examples from medical writing and explains different ways to simplify overcomplicated sentences by shortening them. By contrast, our paper is not normative at all (it is not on how to improve an opening sentence) but is instead a neutral classification of how others have decided to open their papers, looking for trends and the variations in approach.

Academic Writing. Other research has examined the role of academic writing, however academic from other disciplines. Cameron *et al.* explains the struggles of the writing process and suggests strategies to helps novice writers to overcome them [16]. Hartley presents a bilingual study in English and Spanish on research papers in psychology [38]. The paper focuses on improving different aspects of academic writing to increase readability. Biber *et al.* discuss the stereotypical characteristics of academic writing like complex grammar structures [11].

Grounded Theory. Grounded theory is an analysis method for qualitative data [36]. In ground theory, one or more practitioners will examine the data to divisions between different concepts. The data is then partitioned at these points and concepts are labeled with a code. By performing coding, the aim is to come up with new high-level theories and concepts at the end of the process. Coding is an iterative process and several rounds of coding can be performed to refine the categories. At the end of the process, a new theory that is based on the data is presented.

Grounded theory is used as a methodology in security and privacy research. Some examples include: user mental models of cryptocurrency systems [51], how blockchain technology is perceived and how it is used [65], preferences for security warning types [24], the factors that influence software developers' motivation towards security [8], how users manage their online security posture [66], and how users manage their passwords [70].

3 CATEGORIZATION

Figure 1 shows the taxonomy of our codes where the area of the box is proportional to how many times they were used. We provide a description of each category, as well as several examples, later in this section.

To arrive at this figure, we followed the coding techniques of grounded theory assisted by the qualitative analysis software tool NVIVO. The process consisted of first partitioning out the opening sentence of each paper. We read many sentences without coding them to have an initial sense of the variety of sentences. We then started 'open coding' by creating codes that were as general as possible. Roughly every 50 papers, we would review only the papers with a specific code and try to sub-categorize them ('code upon'), while also vetting the codes and moving papers to other codes as needed. We also re-categorized the codes many times ('axial coding'), eventually arriving at Figure 1. We did a final code-by-code pass to ensure all the sentences matched the code description and were coherent with each other.

Grounded theory has a natural halting condition when no new codes are observed, and we halted after three years of proceedings. That is not to say that our categorization does not miss other kinds of sentences, only that new kinds should be rare if the dataset is representative. The final step of grounded theory is to pull general theories out of the codes and their categorization, which we do not pursue since our end goal was classification. We also were not coding the *content* of the sentences, only the kind of writing they exhibit. For these reasons, we emphasize that we used the coding techniques of grounded theory rather than exactly grounded theory itself.

One further note about citations: we do not include individual citations to the paper that each sentence is extracted from, as the bibliography for this paper would exceed the page limit. The sentences are from the following three proceedings: [1–3]. A full length version of this paper is available with individual citations (linked remove for anonymity). Finally, several quoted sentences have citations embedded within them. We leave these quoted verbatim, noting that the citation numbers within the quoted sentences are relevant to the context of the quoted paper and make no reference to the bibliography of this paper.

3.1 Facts

3.1.1 Facts: Definition or Description. Many papers start with a straightforward definition of the subject of the paper. These tend to be neutral and like something you would read in a glossary.

- "Malware sandboxes are automated dynamic analysis tools that execute samples in an isolated and instrumented environment." [37]
- "Secure two-party computation allows two parties to process their sensitive data in such a way that its privacy is protected." [26]
- "HMAC is a cryptographic authentication algorithm, the 'Keyed-Hash Message Authentication Code,' widely used in conjunction with the SHA-256 cryptographic hashing primitive." [10]

Similarly, papers might provide a description of what the subject of a sentence does or how it works. These are also neutral statements and like something you'd read in a textbook.

- "Traditionally, digital investigations have aimed to recover evidence of a cyber-crime or perform incident response via analysis of non-volatile storage." [67]

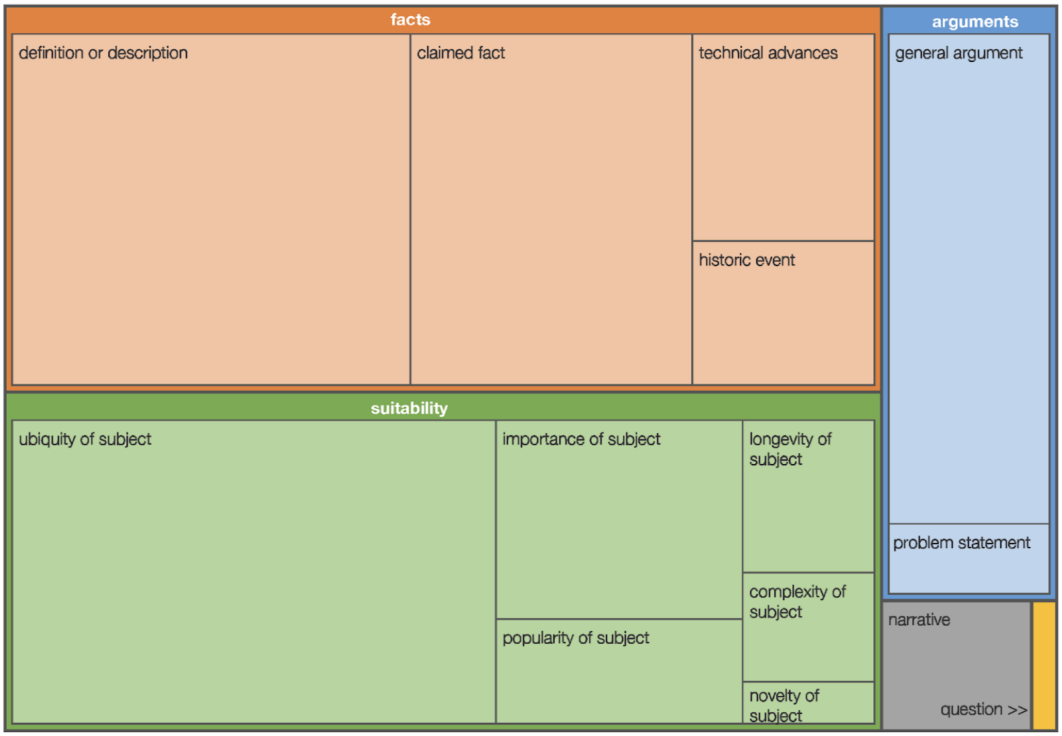

Figure 1: A treemap of our codes for the opening sentences of 379 research papers. The size (in area) of each visualized code is proportional to the number of sentences with that code.

- "Mobile social applications discover nearby users and provide services based on user activity (what the user is doing) and context (who and what is nearby)." [49]
- "To reduce the memory footprint of a system, the system software shares identical memory pages between processes running on the system." [77]

3.1.2 Facts: Claimed Fact. Another neutral approach to an opening sentence is to provide a fact that is relevant to the subject of the paper. Later we will discuss arguments which are often expressed as if they are facts but are only debatably true. A claimed fact's correctness should either be apparent or at least provable (i.e., falsifiable).

- "Users are often advised or required to choose passwords that comply with certain policies." [45]
- "Mobile apps frequently demand access to private information." [73]
- "For several decades, car keys have been used to physically secure vehicles." [35]

Some sentences use stronger and more vivid language but are still factually based.

- "In spite of extensive industrial and academic efforts (e.g., [3, 41, 42]), distributed denial-of-service (DDoS) attacks continue to plague the Internet." [32]

3.1.3 Facts: Technical Advances. Many opening sentences lay out a technical advance in the subject of the sentence. This creates a window of opportunity for the researcher to later identify a novel research problem caused by the changing technology. It is common to see words like: evolve, become, transition, and improve.

- "Recent advances in cloud computing enable customers to outsource their computing tasks to the cloud service providers (CSPs)." [60]
- "Browsers have evolved over recent years to mediate a wealth of user interactions with sensitive data." [40]
- "Since its beginning in the early nineties, the Web evolved from a mechanism to publish and link static documents into a sophisticated platform for distributed Web applications." [48]

3.1.4 Facts: Historic Events. A final type of neutral opening sentence will refer to some historic event.

- "In 1996, Wagner and Schneier performed an analysis of the SSL 3.0 protocol [67]." [74]
- "In February 2011, a new Tor hidden service [16], called "Silk Road," opened its doors." [69]
- "The Network Time Protocol (NTP) is one of the Internet's oldest protocols, dating back to RFC 958 [15] published in 1985." [29]

In some cases, a paper opens with a "compound" sentence that makes reference to a historic event in one clause of the sentence, while having additional clauses of a different category. For example, the following sentence refers to a historic event as well as a technical advance.

- "Starting from Denning's seminal work in 1986 [9], intrusion detection has evolved into a number of different approaches." [18]

In our analysis, some sentences are coded with more than one code but we do so sparingly.

3.2 Arguments

3.2.1 Arguments: General Argument. Many opening sentences issue a subjective argument that represents the authors' opinion. Unlike a fact, it isn't straightforward that the reader will accept it as true. While arguments are less neutral than facts, they can be more interesting and provocative, which can help draw the reader into the paper.

The arguments we categorize under "general arguments" do not fit elsewhere in our categorization system. As we go through more categories, we will see other more specific kinds of arguments.

- "It is a truth universally acknowledged, that password-based authentication on the web is insecure." [50]
- "The dismissal of human memory by the security community reached the point of parody long ago." [12]
- "In recent years, unwanted software has risen to the forefront of threats facing users." [72]
- "The phenomenal growth of Android devices brings in a vibrant application ecosystem." [19]

3.2.2 Arguments: Problem Statement . A special type of argument is a "problem statement" which uses the opening sentence to establish a problem or challenge to be solved.

- "A key challenge when running untrusted virtual machines is providing them with efficient and secure I/O." [68]
- "Determining the semantic similarity between two pieces of binary code is a central problem in a number of security settings." [30]
- "It is difficult to keep secrets during program execution." [63]
- "For some sentences, the problem is not stated explicitly but can be inferred from what is said. For example, the "pressure to respond" in the following sentence implies a problem."
- "As popular applications rely on personal, privacy-sensitive information about users, factors such as legal regulations, industry self-regulation, and a growing body of privacy-conscious users all pressure developers to respond to demands for privacy." [34]

3.3 Suitability

3.3.1 Suitability: Importance of subject. A large set of sentences make a special kind of argument: that the subject of the opening sentence is suitable or worthy of research. The exact reasons they are suitable fall into a few sub-categories: the subject is important, ubiquitous, complex, novel, popular with other researchers, or has been around a long time.

Many opening sentences state that their subject is important, with the implication that it is thus suitable for research.

- "Security has now become an important and real concern to connected and/or automated vehicles." [20]
- "Error handling is an important aspect of software development." [41]
- "SSL/TLS is, due to its enormous importance, a major target for attacks." [53]

Some sentences do not explicitly use the word "important" but find other ways to convey the same notion. For example, a concern or component might be described as essential or crucial or serious.

- "The threat of data theft in public and private clouds from insiders (e.g. curious administrators) is a serious concern." [28]
- "The same-origin policy (SOP) is a cornerstone of web security, guarding the web content of one domain from the access from another domain." [79]

3.3.2 Suitability: Ubiquity of subject. The most popular kind of opening sentence argues that a subject is suitable for research because it is ubiquitous and widely used.

- "Billions of users now depend on online services for sensitive communication." [52]
- "Embedded systems are omnipresent in our everyday life." [23]
- "Android is the major platform for mobile users and mobile app developers." [58]

3.3.3 Suitability: Popularity of subject. While the ubiquity of a subject corresponds to how widely it is used, a closely related variant points out that the subject has received a lot of attention. Often, this means attention from other researchers which lends credibility to the subject for further research.

- "Protecting the privacy of user data within mobile applications (apps for short) has always been at the spotlight of mobile security research." [56]
- "The black-market economy for purchasing Facebook likes, Twitter followers, and Yelp and Amazon reviews has been widely acknowledged in both industry and academia [6, 27, 37, 58, 59]." [75]
- "Since the first widely-exploited buffer overflow used by the 1998 Morris worm [27], the prevention, exploitation, and mitigation of memory corruption vulnerabilities have occupied the time of security researchers and cybercriminals alike." [27]

3.3.4 Suitability: Longevity of subject . In this category, how long a subject has been around is the key component to why it is a suitable subject for study. In some cases, a specific duration is provided and in others, it is implied that the amount of time is significant.

- "Redaction of sensitive information from documents has been used since ancient times as a means of concealing and removing secrets from texts intended for public release." [7]
- "Since its beginning in the early nineties, the Web evolved from a mechanism to publish and link static documents into a sophisticated platform for distributed Web applications." [48]

3.3.5 Suitability: Complexity of subject. In this category, the complexity of the subject is highlighted, implying that the complexity creates new issues or requires further research. The complexity might be inherent to the subject itself. Or there might be a complex set of external factors to consider.

- "Today, large and complex software is built with many components integrated using APIs." [78]
- "The capabilities and limitations of disassembly are not always clearly defined or understood, making it difficult for

researchers and reviewers to judge the practical feasibility of techniques based on it." [6]
- "As popular applications rely on personal, privacy-sensitive information about users, factors such as legal regulations, industry self-regulation, and a growing body of privacy-conscious users all pressure developers to respond to demands for privacy." [34]

3.3.6 Suitability: Novelty of subject. Finally, a degree of novelty is an important component in any research question so it is unsurprising that papers begin arguing novelty from their opening sentence. In this category, sentences focus on something that is new or emerging.

- "In the last few years, a new class of cyber attacks has emerged that is more targeted at individuals and organizations." [46]
- "Although the operating system (OS) kernel has always been an appealing target, until recently attackers focused mostly on the exploitation of vulnerabilities in server and client applications— which often run with administrative privileges—as they are (for the most part) less complex to analyze and easier to compromise." [43]

This sentence manages to appeal to both longevity and novelty by relating two subjects.

- "While cryptocurrency has been studied since the 1980s [22, 25, 28], bitcoin is the first to see widespread adoption." [39]

3.4 Narrative

A potentially interesting way to draw a reader into a paper is by establishing a narrative: a scenario that gets the reader thinking about themselves or other people and what they might do.

- "Consider that you are a domain owner, holding a few domain names that you do not have a better use of." [5]
- "Consider the setting where a client owns a public input x, a server owns a private input w, and the client wishes to learn z := F(x,w) for a program F known to both parties." [9]

Narratives might also set a scene, like the academic version of an establishing shot from films and TV.

- "Our phones are always within reach and their location is mostly the same as our location." [54]
- "We live in a "big data" world." [47]
- "The battle for the living room is in full swing." [59]

3.5 Question

Making the reader curious is another good way to begin a paper, and this can be accomplished using a question. In our sample, this was underused with only one example.

- "Do programmers leave fingerprints in their source code?" [15]

4 DISCUSSION

Domain Expertise. We pondered whether we could apply our analysis to a domain in which we were not experts. Obviously a non-expert in security would not understand the technical content of many of our sentences, but would they be able to tell the difference between, say, a historic fact and a suitability argument?

We are unsure but skeptical. Consider the following sentence: "The widespread adoption of DEP, which ensures that all writable pages in memory are nonexecutable, has largely killed classic code injection attacks." [17] A non-expert who is unfamiliar with DEP or code injection could understand the gist of the sentence: code injection is an *attack*, therefore it is *bad*; DEP is *good* because it reduces something that is bad. But what if the authors of the sentence had dropped the word 'attack' and instead simply ended: "DEP…has largely killed classic code injection." Now it is ambiguous to a non-expert whether DEP is good or bad, in fact the strength of the word 'kills' might lead the non-exert to conclude DEP is bad. While most sentences are not like this, we see this as evidence that our analysis should be undertaken by domain experts and not general readers.

Sentence Length. We examined the shortest and longest sentences in our dataset. Short sentences are striking and easy to remember. The shortest ones from our data set were four words long: "Video is ineffably compelling" [14] and "Software bugs are expensive." [64] Long sentences can obviously convey more information or make a complex argument, but they might have to be read a few times to fully parse what they are saying. King has a similar argument in [44], where he gives an example of a long opening sentence in medical writing and he simplifies the sentence by shortening it and as a result making it more concise and easier to parse.

Security-specific Approach. There was one set of sentences that usually fell under the *suitability: importance of subject* code that was very specific to security. In security, it is important to researchers to tackle the biggest threats. Many use their opening sentence to position themselves as doing so. Many of them flatly state that their research area is the most prevalent threat ("In recent years, unwanted software has risen to the forefront of threats facing users;" [72] "Today, runtime attacks remain one of the most prevalent attack vectors against software programs;" [25] "Remote malware downloads currently represent the most common infection vector.' [57]). Some prefer to make their point in a stronger way with a colorful choice of words ("In spite of extensive industrial and academic efforts (e.g., [3, 41, 42]), distributed denial-of-service (DDoS) attacks continue to plague the Internet" [32]). We look at colorful sentences next, with another example using the word 'plague.'

Color. We also analyzed to what extend the authors add 'colour commentary' in the opening sentence. The decision to use this type of commentary is related to how researchers perceive and define the seriousness of their topic. Is avoiding all colour in the text a way to prove that the problem is significant and should be taken seriously? Or should writers add some colour to make the writing more engaging and easier to hook the reader? Examples of sentences that use a more vivid choice of words include: "The defacement and vandalism of websites is an attack that disrupts the operation of companies and organizations, tarnishes their brand, and plagues websites of all sizes, from those of large corporations to the websites of single individuals;" [13] "The dismissal of human memory by the security community reached the point of parody long ago;" [12] "Video is ineffably compelling" [14].

Using colorful language is probably best in moderation. Text that is very ornate and elaborate is deridingly called 'purple prose.' We

did not find any examples in our data set, but to what extent is this a reflection of writing in information technology? An interesting area of future work is to examine the usefulness of our taxonomy in both other STEM domains, but also in academic writing in arts and the humanities.

The Arc of Time. Appealing to the notion that a domain is important because of its longevity is also a common way to start a paper in our data set. The idea of appealing to years or decades of work is extremely common ("Over the last few years there have been numerous reports…" [55] "The last decade in cryptography…" [4] "Over the past few years, face authentication systems…" [76] "For several decades, car keys…" [35]). The longest timeframe in our dataset is: "Redaction of sensitive information from documents has been used since ancient times as a means of concealing and removing secrets from texts intended for public release." [7]

5 CONCLUSION

As researchers ourselves, we have often found ourselves staring at a blinking cursor, trying to come up with a compelling way to start our paper. After completing our analysis, we find ourselves proactively choosing how to start our writing. The taxonomy also allows us to try on different approaches (*e.g.,* 'what if we started with a narrative instead of the importance of the domain?') to find one that works. We hope that our results are interesting, but that they also raise consciousness of thoughtful writing in research papers. We hope to see further research on academic writing in information technology.

REFERENCES

[1] 2014. *SEC'14: Proceedings of the 23rd USENIX Conference on Security Symposium* (San Diego, CA). USENIX Association, USA.

[2] 2015. *SEC'15: Proceedings of the 24th USENIX Conference on Security Symposium* (Washington, D.C.). USENIX Association, USA.

[3] 2016. *SEC'16: Proceedings of the 25th USENIX Conference on Security Symposium* (Austin, TX, USA). USENIX Association, USA.

[4] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. 2016. Post-quantum key exchange—a new hope. In *USENIX Security*. 327–343.

[5] Sumayah Alrwais, Kan Yuan, Eihal Alowaisheq, Zhou Li, and XiaoFeng Wang. 2014. Understanding the dark side of domain parking. In *USENIX Security*. 207–222.

[6] Dennis Andriesse, Xi Chen, Victor Van Der Veen, Asia Slowinska, and Herbert Bos. 2016. An in-depth analysis of disassembly on full-scale x86/x64 binaries. In *USENIX Security*. 583–600.

[7] Frederico Araujo, W Kevin, et al. 2015. Compiler-instrumented, dynamic secret-redaction of legacy processes for attacker deception. In *USENIX Security*. 145–159.

[8] Hala Assal and Sonia Chiasson. 2018. Motivations and amotivations for software security. In *SOUPS Workshop on Security Information Workers (WSIW). USENIX Association*.

[9] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. 2014. Succinct non-interactive zero knowledge for a von Neumann architecture. In *USENIX Security*. 781–796.

[10] Lennart Beringer, Adam Petcher, Q Ye Katherine, and Andrew W Appel. 2015. Verified Correctness and Security of OpenSSL {HMAC}. In *USENIX Security*. 207–221.

[11] Douglas Biber and Bethany Gray. 2010. Challenging stereotypes about academic writing: Complexity, elaboration, explicitness. *Journal of English for Academic Purposes* 9, 1 (2010), 2–20.

[12] Joseph Bonneau and Stuart Schechter. 2014. Towards reliable storage of 56-bit secrets in human memory. In *USENIX Security*. 607–623.

[13] Kevin Borgolte, Christopher Kruegel, and Giovanni Vigna. 2015. Meerkat: Detecting website defacements through image-based object recognition. In *USENIX Security*. 595–610.

[14] Matthew Brocker and Stephen Checkoway. 2014. iSeeYou: Disabling the MacBook Webcam Indicator {LED}. In *USENIX Security*. 337–352.

[15] Aylin Caliskan-Islam, Richard Harang, Andrew Liu, Arvind Narayanan, Clare Voss, Fabian Yamaguchi, and Rachel Greenstadt. 2015. De-anonymizing programmers via code stylometry. In *USENIX Security*. 255–270.

[16] Jenny Cameron, Karen Nairn, and Jane Higgins. 2009. Demystifying academic writing: Reflections on emotions, know-how and academic identity. *Journal of Geography in Higher Education* 33, 2 (2009), 269–284.

[17] Nicholas Carlini and David Wagner. 2014. {ROP} is still dangerous: Breaking modern defenses. In *USENIX Security*. 385–399.

[18] Marco Caselli, Emmanuele Zambon, Johanna Amann, Robin Sommer, and Frank Kargl. 2016. Specification mining for intrusion detection in networked control systems. In *USENIX Security*. 791–806.

[19] Kai Chen, Peng Wang, Yeonjoon Lee, XiaoFeng Wang, Nan Zhang, Heqing Huang, Wei Zou, and Peng Liu. 2015. Finding unknown malice in 10 seconds: Mass vetting for new threats at the google-play scale. In *USENIX Security*. 659–674.

[20] Kyong-Tak Cho and Kang G Shin. 2016. Fingerprinting electronic control units for vehicle intrusion detection. In *USENIX Security*. 911–927.

[21] Alison Clear and Allen Parrish. December 31, 2020. *A Computing Curricula Series Report, CC2020.* Technical Report. Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS).

[22] Alison Clear, Allen Parrish, Ming Zhang, and Gerritt C van der Veer. 2017. CC2020: A Vision on Computing Curricula. In *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education*. 647–648.

[23] Andrei Costin, Jonas Zaddach, Aurélien Francillon, and Davide Balzarotti. 2014. A large-scale analysis of the security of embedded firmwares. In *USENIX Security*. 95–110.

[24] Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2020. One size does not fit all: a grounded theory and online survey study of developer preferences for security warning types. In *2020 IEEE/ACM 42nd International Conference on Software Engineering (ICSE)*. IEEE, 136–148.

[25] Lucas Davi, Ahmad-Reza Sadeghi, Daniel Lehmann, and Fabian Monrose. 2014. Stitching the gadgets: On the ineffectiveness of coarse-grained control-flow integrity protection. In *USENIX Security*. 401–416.

[26] Daniel Demmler, Thomas Schneider, and Michael Zohner. 2014. Ad-hoc secure two-party computation on mobile devices using hardware tokens. In *USENIX Security*. 893–908.

[27] Alessandro Di Federico, Amat Cama, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna. 2015. How the {ELF} Ruined Christmas. In *USENIX Security*. 643–658.

[28] Tien Tuan Anh Dinh, Prateek Saxena, Ee-Chien Chang, Beng Chin Ooi, and Chunwang Zhang. 2015. M2r: Enabling stronger privacy in mapreduce computation. In *USENIX Security*. 447–462.

[29] Benjamin Dowling, Douglas Stebila, and Greg Zaverucha. 2016. Authenticated network time synchronization. In *USENIX Security*. 823–840.

[30] Manuel Egele, Maverick Woo, Peter Chapman, and David Brumley. 2014. Blanket execution: Dynamic similarity testing for program binaries and components. In *USENIX Security*. 303–317.

[31] Joe Fasser. 2013. Why Stephen King Spends 'Months and Even Years' Writing Opening Sentences. *The Atlantic* (July 2013).

[32] Seyed K Fayaz, Yoshiaki Tobioka, Vyas Sekar, and Michael Bailey. 2015. Bohatei: Flexible and elastic ddos defense. In *USENIX Security*. 817–832.

[33] Harriet J Fell, Viera K Proulx, and John Casey. 1996. Writing across the computer science curriculum. *ACM SIGCSE Bulletin* 28, 1 (1996), 204–209.

[34] Matthew Fredrikson and Benjamin Livshits. 2014. ZØ: An optimizing distributing zero-knowledge compiler. In *USENIX Security*. 909–924.

[35] Flavio D Garcia, David Oswald, Timo Kasper, and Pierre Pavlidès. 2016. Lock it and still lose it—on the (in) security of automotive remote keyless entry systems. In *USENIX Security*.

[36] Barney G Glaser and Anselm L Strauss. 1967. The discovery of grounded theory; strategies for qualitative research. (1967).

[37] Mariano Graziano, Davide Canali, Leyla Bilge, Andrea Lanzi, Elaine Shi, Davide Balzarotti, Marten van Dijk, Michael Bailey, Srinivas Devadas, Mingyan Liu, et al. 2015. Needles in a haystack: Mining information from public dynamic analysis sandboxes for malware intelligence. In *USENIX Security*. 1057–1072.

[38] James Hartley. 2012. New ways of making academic articles easier to read. *International Journal of Clinical and Health Psychology* 12, 1 (2012), 143–160.

[39] Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. 2015. Eclipse attacks on bitcoin's peer-to-peer network. In *USENIX Security*. 129–144.

[40] Nav Jagpal, Eric Dingle, Jean-Philippe Gravel, Panayiotis Mavrommatis, Niels Provos, Moheeb Abu Rajab, and Kurt Thomas. 2015. Trends and lessons from three years fighting malicious extensions. In *USENIX Security*. 579–593.

[41] Suman Jana, Yuan Jochen Kang, Samuel Roth, and Baishakhi Ray. 2016. Automatically detecting error handling bugs using error specifications. In *USENIX Security*. 345–362.

[42] David G Kay. 1998. Computer scientists can teach writing: an upper division course for computer science majors. In *Proceedings of the twenty-ninth SIGCSE technical symposium on Computer science education*. 117–120.

[43] Vasileios P Kemerlis, Michalis Polychronakis, and Angelos D Keromytis. 2014. ret2dir: Rethinking kernel isolation. In *USENIX Security*. 957–972.

[44] Lester S King. 1967. The Opening Sentence. *JAMA* 202, 6 (1967), 535–536.

[45] Saranga Komanduri, Richard Shay, Lorrie Faith Cranor, Cormac Herley, and Stuart Schechter. 2014. Telepathwords: Preventing weak passwords by reading users' minds. In *USENIX Security*. 591–606.

[46] Stevens Le Blond, Adina Uritesc, Cédric Gilbert, Zheng Leong Chua, Prateek Saxena, and Engin Kirda. 2014. A look at targeted attacks through the lense of an {NGO}. In *USENIX Security*. 543–558.

[47] Mathias Lécuyer, Guillaume Ducoffe, Francis Lan, Andrei Papancea, Theofilos Petsios, Riley Spahn, Augustin Chaintreau, and Roxana Geambasu. 2014. Xray: Enhancing the web's transparency with differential correlation. In *USENIX Security*. 49–64.

[48] Sebastian Lekies, Ben Stock, Martin Wentzel, and Martin Johns. 2015. The unexpected dangers of dynamic javascript. In *USENIX Security*. 723–735.

[49] Matthew Lentz, Viktor Erdélyi, Paarijaat Aditya, Elaine Shi, Peter Druschel, and Bobby Bhattacharjee. 2014. {SDDR}: Light-Weight, Secure Mobile Encounters. In *USENIX Security*. 925–940.

[50] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song. 2014. The emperor's new password manager: Security analysis of web-based password managers. In *USENIX Security*. 465–479.

[51] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. 2020. User Mental Models of Cryptocurrency Systems—-A Grounded Theory Approach. (2020).

[52] Marcela S Melara, Aaron Blankstein, Joseph Bonneau, Edward W Felten, and Michael J Freedman. 2015. {CONIKS}: Bringing Key Transparency to End Users. In *USENIX Security*. 383–398.

[53] Christopher Meyer, Juraj Somorovsky, Eugen Weiss, Jörg Schwenk, Sebastian Schinzel, and Erik Tews. 2014. Revisiting SSL/TLS implementations: New bleichenbacher side channels and attacks. In *USENIX Security*. 733–748.

[54] Yan Michalevsky, Aaron Schulman, Gunaa Arumugam Veerapandian, Dan Boneh, and Gabi Nakibly. 2015. Powerspy: Location tracking using mobile device power analysis. In *USENIX Security*. 785–800.

[55] Gabi Nakibly, Jaime Schcolnik, and Yossi Rubin. 2016. Website-targeted false content injection by network operators. In *USENIX Security*. 227–244.

[56] Yuhong Nan, Min Yang, Zhemin Yang, Shunfan Zhou, Guofei Gu, and XiaoFeng Wang. 2015. Uipicker: User-input privacy identification in mobile applications. In *USENIX Security*. 993–1008.

[57] Terry Nelms, Roberto Perdisci, Manos Antonakakis, and Mustaque Ahamad. 2015. Webwitness: Investigating, categorizing, and mitigating malware download paths. In *USENIX Security*. 1025–1040.

[58] Marten Oltrogge, Yasemin Acar, Sergej Dechand, Matthew Smith, and Sascha Fahl. 2015. To Pin or Not to Pin—Helping App Developers Bullet Proof Their {TLS} Connections. In *USENIX Security*. 239–254.

[59] Yossef Oren and Angelos D Keromytis. 2014. From the aether to the ethernet—attacking the internet using broadcast digital television. In *USENIX Security*. 353–368.

[60] Erman Pattuk, Murat Kantarcioglu, Zhiqiang Lin, and Huseyin Ulusoy. 2014. Preventing cryptographic key leakage in cloud virtual machines. In *USENIX Security*. 703–718.

[61] Linda H Pesante. 1991. Integrating writing into computer science courses. In *Proceedings of the twenty-second SIGCSE technical symposium on Computer science education*. 205–209.

[62] Steven Pinker. 2015. *The sense of style: The thinking person's guide to writing in the 21st century*. Penguin Books.

[63] Ashay Rane, Calvin Lin, and Mohit Tiwari. 2015. Raccoon: Closing digital side-channels through obfuscated execution. In *USENIX Security*. 431–446.

[64] Alexandre Rebert, Sang Kil Cha, Thanassis Avgerinos, Jonathan Foote, David Warren, Gustavo Grieco, and David Brumley. 2014. Optimizing seed selection for fuzzing. In *USENIX Security*. 861–875.

[65] Scott Ruoti, Ben Kaiser, Arkady Yerukhimovich, Jeremy Clark, and Robert Cunningham. 2019. Blockchain technology: what is it good for? *Commun. ACM* 63, 1 (2019), 46–53.

[66] Scott Ruoti, Tyler Monson, Justin Wu, Daniel Zappala, and Kent Seamons. 2017. Weighing context and trade-offs: How suburban adults selected their online security posture. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 211–228.

[67] Brendan Saltaformaggio, Zhongshu Gu, Xiangyu Zhang, and Dongyan Xu. 2014. {DSCRETE}: Automatic rendering of forensic information from memory images via application logic reuse. In *USENIX Security*. 255–269.

[68] Igor Smolyar, Muli Ben-Yehuda, and Dan Tsafrir. 2015. Securing self-virtualizing ethernet devices. In *USENIX Security*. 335–350.

[69] Kyle Soska and Nicolas Christin. 2015. Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In *USENIX Security*. 33–48.

[70] Elizabeth Stobert and Robert Biddle. 2014. The password life cycle: user behaviour in managing passwords. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 243–255.

[71] Harriet G Taylor and Katharine M Paine. 1993. An interdisciplinary approach to the development of writing skills in computer science students. *ACM SIGCSE Bulletin* 25, 1 (1993), 274–278.

[72] Kurt Thomas, Juan A Elices Crespo, Ryan Rasti, Jean-Michel Picod, Cait Phillips, Marc-André Decoste, Chris Sharp, Fabio Tirelo, Ali Tofigh, Marc-Antoine Courteau, et al. 2016. Investigating commercial pay-per-install and the distribution of unwanted software. In *USENIX Security*. 721–739.

[73] Omer Tripp and Julia Rubin. 2014. A bayesian approach to privacy enforcement in smartphones. In *USENIX Security*. 175–190.

[74] Tom Van Goethem, Mathy Vanhoef, Frank Piessens, and Wouter Joosen. 2016. Request and conquer: Exposing cross-origin resource size. In *USENIX Security*. 447–462.

[75] Bimal Viswanath, M Ahmad Bashir, Mark Crovella, Saikat Guha, Krishna P Gummadi, Balachander Krishnamurthy, and Alan Mislove. 2014. Towards detecting anomalous user behavior in online social networks. In *USENIX Security*. 223–238.

[76] Yi Xu, True Price, Jan-Michael Frahm, and Fabian Monrose. 2016. Virtual u: Defeating face liveness detection by building virtual models from your public photos. In *USENIX Security*. 497–512.

[77] Yuval Yarom and Katrina Falkner. 2014. FLUSH+ RELOAD: A high resolution, low noise, L3 cache side-channel attack. In *USENIX Security*. 719–732.

[78] Insu Yun, Changwoo Min, Xujie Si, Yeongjin Jang, Taesoo Kim, and Mayur Naik. 2016. Apisan: Sanitizing {API} usages through semantic cross-checking. In *USENIX Security*. 363–378.

[79] Xiaofeng Zheng, Jian Jiang, Jinjin Liang, Haixin Duan, Shuo Chen, Tao Wan, and Nicholas Weaver. 2015. Cookies lack integrity: Real-world implications. In *USENIX Security*. 707–721.