The umbrella of computer security

Aslan Askarov
2024-08-28

In their 2024 keynote during the Matchpoints conference, Christiane Kirketep de Viron, the head of the European Commission's unit on Cybersecurity and Digital Policy said that [paraphrasing]

> just until a few years ago, cybersecurity was for nerds; now we hear about it everywhere

For us – the prototypical nerds – the newly founded public interest in cyber security is an invitation to reflect upon the knowledge about the area we work in, and think about opportunities we may be missing given all the attention.

The rest of this essay is my personal take on the perspectives of cybersecurity. The write up is biased by my own research in foundations of computer security and formal methods. While there is no shortage of loud opinions about computer security, I hope this text contributes with more signal than noise.

Classical discipline

As a scientific area, computer security has deep roots within computer science. Classical literature in computer security goes back to the mid 1970s, with annual conferences starting in the early 1980s. Foundations and insights underlying the area have remained relevant through the generational changes in computing, from mainframes to desktops to mobile. For example, the 1975 paper by Saltzer and Schroeder notes how "passwords as a general technique have some notorious defects" discussing the familiar tension between the passwords being easy to guess for attackers and hard to memorize for users.

New tech comes and goes, but the classical principles stay. When today we look at the so-called prompt injections of LLMs, it is hard not to see the resemblance to the buffer overflows or sql injection attacks of the 1990s: when systems have no distinction between code and data, this confusion invites injection attacks.

Why now? "Real"-world risks and newsworthiness vs research-worthiness.

Butler Lampson, one of the pioneers of computer security, and a 1992 Turing-award winner, writes that "practical security balances the cost of protection and the risk of loss". It is the increase in real-world risks that brings the classical discipline of computer security into the news spotlights. At the same time, the security community has learned to appreciate the distinction between the newsworthiness and research-worthiness. In their 2012 CACM opinion on the value of publishing attacks, David Basin and Srdjan Capkun of ETH Zurich write:

> As our physical and digital worlds become more tightly coupled, the incidence of attacks will increase as well as their consequences. Many of these attacks will be newsworthy, but most will not be research-worthy.

They stress that scientifically novel attack literature should “be contributing with new insights into both systems and their vulnerabilities, and adversaries and their capabilities”.

Consider the 2024 CrowdStrike incident. Once some information about the incident was released (albeit heavily concealed in tech jargon) it appears that what happened was

> *A parsing error in a virtual machine that was pretending to be a device driver (which was cryptographically signed by Microsoft) running in a privileged mode in the OS kernel; the latter turn was apparently necessitated by an EU policy that prevented Microsoft to develop an appropriate kernel-level API; the whole thing driven by the necessity to quickly respond to ransomware, which is part of the CrowdStrike's business model.*

Read that aloud and notice textbook-grade anti-patterns layered upon anti-patterns that we teach our students not to do. This incident is still too recent for us to conclude what it is that we should be really learning from it, if anything.

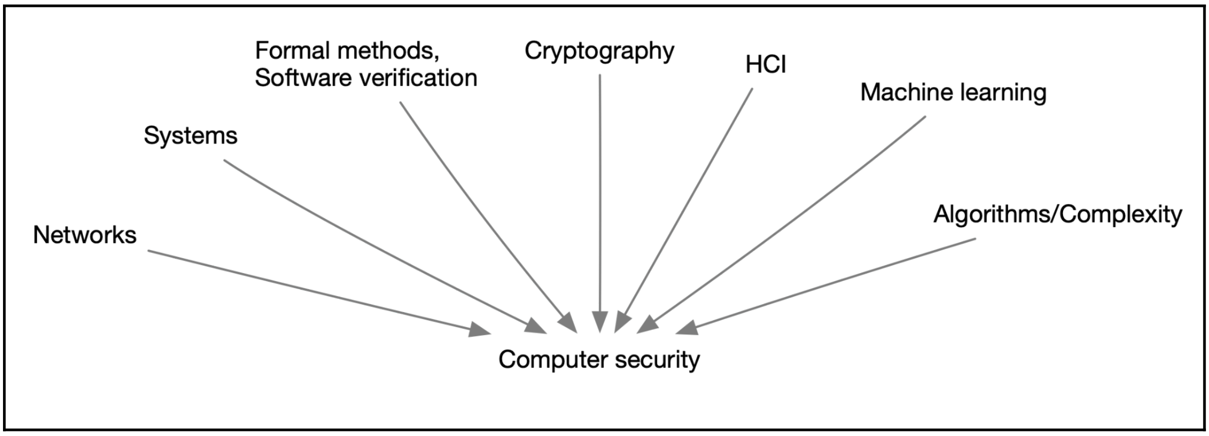
Negative requirements, leaky abstractions, and security “umbrella”

In the same 1975 paper, Saltzer and Schroeder note that a characteristic aspect of security is that it is about what is *not* supposed to happen. It is a negative requirement that is difficult to test. Unlike functionality, where one can test for expected behavior, one cannot test what they don’t know. It is also why formal methods are necessary. The use of formal methods in security is driven by need – we do it because otherwise we have no assurance.

As computer scientists, we are in the business of building abstractions. Yet, abstractions are often leaky, and adversaries seek weaknesses in between abstraction layers. They succeed because reasoning about what is not supposed to happen across abstraction layers is difficult. As the well-known slogan in security says, a system is as secure as its weakest link. Here, it is important to acknowledge that there is no silver bullet, no single technology that can solve security alone.

What we have instead is **a vast design space where research and engineering compromises need to be resolved in principled ways.** This requires consolidated expertise across many disciplines, under the metaphorical “umbrella” of security.

The illustration below depicts this metaphorical umbrella. Note the inwards orientation of the arrows, which is another way of appreciating how computer security differentiates from other areas. For the majority of the CS areas, e.g., HCI, or, programming languages, or machine learning, the arrows would be outward oriented (perhaps with the distinction of systems, if broadly interpreted).



Now what?

As a placeholder for a stronger conclusion, we should see that Computer Security is an area of opportunity for many Computer Scientists to apply our tools and techniques. As an application area, the problems here are grounded in real life, but there is a sufficient degree of abstraction that even pure theory papers can be motivated and appreciated.

The broad aspects

I conclude with a few bullet points of broader aspects, each probably deserving an own elaboration

- The technology does not exist in vacuum, and there are broad societal aspects such as cybercrime, privacy regulations, societal norms, etc. Understanding how the technology of computer security interplays with these aspects is an important aspect of the security umbrella.
    - Just as we celebrate the breadth of problems we tackle in Computer Science, it's important to learn to recognize when we're out of our own depth, and depend on input from other sciences.
        - Scientists in other research areas still have fundamental misunderstanding about "how the internet really works"; probably because they never had the right degree of introduction.
            - CS basics education is broadly important.
    - The law is important, but still a lot of work needs to be done to have legislation that aligns well with technology.
- The perceived “magic of technology” (in the words of Arthur C. Clarke) means most people also have the failure of imagination when it comes to how catastrophic certain errors may be.
- Some changes takes generations to materialize
    - Many solutions are simple but we tackle broad social issues, such as programmers set in the old-school ways of doing things.
    - Continuous education of the classical principles together with the deep nuances of each area is important.
- Privacy and security are related but not the same
    - Privacy is rooted deeply in personal needs, and is certainly bigger than what we can cover in the CS alone. Is the so-called "privacy paradox" really a paradox?

Acknowledgments

This write up is a by-product of a few invited talks on the topic of security and formal methods I gave in the first half of 2024 and discussions with my colleagues and collaborators. Thanks to Boel Nelson, Amin Timany, Carla Griggio, Brandi S. Morris, Rene Rydhof Hansen, Magnus Madsen, Bas Spitters, and Lars Birkedal.