Games without Frontiers: Whither Information Security and Privacy?

It took less than a decade for “nomophobia” (no mobile phone anxiety) to become symptomatic of modern society and for social networks to become many people’s second (and even preferred) life. Current and emerging industrial initiatives prompted by Internet-of-Things (IoT) fever promise to “connect the (heretofore) unconnected.” So-called “smart” embedded computing devices are increasingly percolating into many spheres of everyday life. Such devices include household appliances, industrial machinery, and automotive and avionic components as well as many kinds of personal gadgets. Consequently, we expect exciting novel technologies to appear beyond simply equipping every device with a wireless interface and IP address.

On the other hand, rapidly rising dependence on computerized technologies comes at a price of new vulnerabilities and attacks and poses a number of new security and privacy challenges compared to the last decade.

New Challenges

The first challenge concerns the known knowns: our IT systems are increasingly complex owing to new features and greater automation and connectivity. We’re all aware that implementation bugs, hardware vulnerabilities, legacy software (often written in unsafe languages), and the lack of common security engineering principles collectively offer adversaries a vast and attractive attack surface. However, we’re still facing the challenge of securing legacy systems. For instance, it’s curious that the decades-old problem of memory corruption vulnerabilities remains a persistent threat to modern software. In particular, the growing number and sophistication of recent attacks, such as code reuse techniques, show that the default protection mechanisms offered by many of today’s systems are insufficient. Stagefright, a bug that affected millions of Android devices, is only one of many recent examples. Academic and industry researchers are currently investing considerable efforts into improving defenses against such exploits, at least for general-purpose computing platforms. However, although recently proposed solutions substantially raise the bar for exploits, attackers continually discover new bypasses, and the arms race continues.

The situation is much bleaker in embedded systems, whose security and privacy aspects seem to have been less explored. Numerous vulnerabilities have been discovered in areas such as IoT devices, vehicles, transportation systems, and critical infrastructure components. This will also affect emerging technologies, such as industrial Internet, smart factories, and autonomous systems, in which thousands of devices are supposed to be interconnected. The challenge is to design systems-scalable and usable security and privacy for a very large number of connected devices while accounting for the embedded devices’ heterogeneity and constraints.

Another challenge concerns universal adversaries of a different nature: the known unknowns that might directly or indirectly affect everyone. On one side is the nation-state adversary attempting to infiltrate and attack other nations’ sensitive IT systems, conduct global mass surveillance, or support industrial espionage. The Snowden revelations demonstrated how mass surveillance can violate the data and privacy protection legislation of many free societies. The recent decision of Europe’s highest Court of Justice fundamentally questions the compliance of the Safe Harbor data transfer framework with European privacy law. Safe Harbor is an agreement between the EU and the US that allows...
more than 3,000 US companies, including Google, Facebook, and Apple, to repatriate European personal data. Unfortunately, despite a large body of literature, modern cryptography solutions still can’t protect against mass surveillance or provide practical cryptographic primitives with a long life span. Further, we still lack usable encryption “for the masses” that would allow individuals to protect their personal data at rest and in transit (assuming their devices remain uncompromised by malware).

On the other side is the terrorism and extremism that’s increasingly abusing the digital world, especially social networks, to conduct crimes, recruit and brainwash followers, propagate hate, and plan (and even execute) both digital and real-world attacks. It’s believed that sad and horrific terrorist attacks, such as occurred in France, Lebanon, California, and Tunisia, as well as the near-constant terrorist warfare in countries such as Iraq, Syria, Nigeria, and Libya are partially prepared and communicated through social networks and online games. This reopens the debate on how to respond to this phenomenon and its possible consequences for data privacy and surveillance—some nation-states have already been requesting more restrictions on the Internet. There are many issues to tackle, including understanding extremists’ communication means from social and technical perspectives, identifying and filtering propaganda messages as such or detecting them when they’re communicated covertly, and reconciling freedom of speech and peace in this “free” environment. In this context, we also need to explore the roles and reactions of the global enterprises that have access to massive user data.

These challenges underscore that “security and privacy by design” goes far beyond the technical aspects. Ours is a highly interdisciplinary field with many facets—research requires knowledge of mathematics, physics, engineering, and computer science as well as socioeconomic and human sciences. Security is not only an enabling technology for many applications and businesses but is increasingly important for our society.

**Modern cryptography solutions still can’t protect against mass surveillance or provide practical cryptographic primitives with a long life span.**

**Looking Ahead**

As the new editor in chief of *IEEE Security & Privacy*, I aim to publish content that’s just as multifaceted as security and privacy research. Since its first issue in 2003, *IEEE S&P* has mirrored cybersecurity and privacy developments and advances, always with an eye toward cutting-edge topics. I’d like to continue the legacy of my predecessors George Cybenko, Carl Landwehr, John Viega, and Shari Lawrence Pfleeger and the excellent editorial board members who’ve made *IEEE S&P* one of the most important peer-reviewed security and privacy magazines. I thank them for their great work.

To ensure *IEEE S&P*’s high quality and reputation, I’d like to highlight some of what’s in store for the next two years.

Two exciting new offerings are myCS and the Fast Track Review option. Starting this January, *IEEE S&P* Issues will be available as eBooks in the myCS digital platform. This new online approach enables more versatile access to content. For Fast Track, a subset of our editors will review short articles on hot topics, which will allow timely acceptance of highly relevant articles that will be made available digitally.

In addition, we’re adding new experts to the editorial board, with the goal of obtaining an affiliation-, geographic-, gender-, seniority-, and topic-balanced set of researchers.

As I mentioned, security and privacy research demands interdisciplinary solutions. So I welcome submissions with an interdisciplinary flavor, such as usable security and privacy, which has become a bona fide area with its research community; mass surveillance in the post-Snowden era; cyberterrorism and extremism; privacy in domains beyond modern Western society; postquantum security systems; usable IoT security and privacy; and many more topics.

Safely and correctly deploying security and privacy technologies in practice is crucial for establishing trust in general and in these technologies in particular. We should continue to explore lessons learned from implementation errors, methodologies for analyzing and detecting weaknesses in open source software, sensibility of security standards and evaluation criteria (and how to improve and simplify them), and investigating privacy-protecting as well as privacy-violating approaches and technologies deployed in practice by many enterprises and organizations. For instance, while we’re debating the use of encryption in many Western countries, more and more cameras and sophisticated sensors are being installed in public places to collect various kinds of information.

In a dynamic field like security and privacy, it’s vital that we learn from one another. I’d like to strengthen interactions with hacker community events such as Blackhat as well as industry conferences such as RSA. These groups offer relevant
and cutting-edge results in practical security that are increasingly cited in publications at high-profile scientific security conferences. Collaborations with a heterogeneous group of independent experts, scholars, and IT specialists will grant our readers insight into best practices. I’m gratified to see the changing relationship between academia and the hacking community, which has increased awareness of many security and privacy issues.

Besides establishing an even closer collaboration with the IEEE Symposium on Security and Privacy, I’d like to broaden our coverage and approach to top-tier venues, including ACM CCS, NDSS, USENIX Security, Crypto, EUROCRYPT, and DAC.

The past decade has clearly shown that even the best security solutions won’t eliminate threats once and for all, and that there will always be unknown unknowns. However, new large-scale technologies and threat types require novel, sophisticated solutions to meet our current and future security and privacy demands.

IEEE S&P is a valuable platform for disseminating innovative ideas and research in the form of high-quality articles. It allows readers to see the big picture, think outside the box, and gain inspiration for novel technologies. The excellent team of associate editors in chief, associate editors, and department editors aims to maintain IEEE S&P’s mission and high standards. I hope that the (growing) pool of readers will enjoy the results of our efforts in the coming years.

Your feedback is always very welcome!

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.

www.computer.org/security