The First Twenty Years of *IEEE Security & Privacy*

Sean Peisert, Editor-in-Chief

January 6, 2023

IEEE Security & Privacy published Volume 1, Issue 1 20 years ago, in January/February 2003. This year, beginning with this issue of *IEEE Security & Privacy*, we aim to celebrate those first 20 years with retrospectives on some of the challenges that we have overcome in that time, as well as some of those that we have not made as much progress as we had hoped to achieve. We also reflect on new challenges and even entire subdisciplines of computer security and privacy that didn't even exist 20 years ago.

As I reflect on the times in which *IEEE Security & Privacy* was simmering as an idea and being developed into its current form, certainly many events of the day come to mind. September 11, 2001 and the subsequent U.S. invasion of Afghanistan (2001) and Iraq (2003), amont other aspects of the "war on terror" certainly stand out in my mind.

September 11 was in fact referenced numerous times in his inaugural editorial by founding Editor-in-Chief George Cybenko himself as one of the motivations for creating the magazine. Indeed, Cybenko referenced the impact of the event on computing not just for security but also particularly for privacy issues:

> "Another consequence of 11 September has been the mounting concern about privacy in a digital society. While privacy has been traditionally largely a consumer concern driven by the desire to protect an individual's identity and activities in the commercial arena, the push to enhance "homeland security" in the US and other countries has raised a different set of challenges." [1]

As alluded to by Cybenko, another prominent event relating to cybersecurity that comes to mind is the creation of the United States Department of Homeland Security (DHS), as part of the Homeland Security Act of 2002. Among very many other elements, the DHS ended up containing the National Cyber Security Division (NCSD), which included US-CERT as an operational element. In Cybenko's decadal reflection published in 2014 [2], "homeland security" continues to be an important theme that he had felt that the magazine had addressed, noting particularly Gary McGraw's "Silver Bullet" interview with Richard Clarke [3] — a veteran of the U.S. Executive Branch's cybersecurity leadership. DHS also was home to the Cyber Security Division of the DHS Science and Technology (S&T) Directorate, which supported significant transitions to practice of important cybersecurity research findings and approaches [4].

The early 2000's were a significant period of major computer worms, bringing large corporate academic, and government networks — and even the entire Internet — to a grinding halt at times. In 2001, these worms notably included Anna Kournikova, Code Red, and Nimda, which all attacked various Microsoft software systems. A few months later, Microsoft founder and then-CEO, Bill Gates, famously issued his "trustworthy computing memo" on January 15, 2002, declaring:

> "So now, when we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve." [5]

Though the exact impact of the Gates memo is difficult to determine — these three worms were, for example, followed by Blaster and SQL Slammer/Sapphire in 2003, Sasser in 2004, Conficker in 2008 — again, all attacks against Microsoft software — it was nonetheless a watershed moment in which the CEO of a for-profit company, rather than a government science policy board, decided that security could be better for business than features. Of course, the first year of *IEEE Security & Privacy* contained one of the seminal articles covering the worm events [6].

Prior to its first issue, the first *IEEE Security & Privacy* product was actually a "teaser" to promote the new magazine that was included as a supplement in the April 2002 issue (volume 35, issue 4) of *Computer*, which included discussions of securing electric infrastructure, a discussion of "bug hunting," and a history of intrusion detection. The very first issue of *IEEE Security & Privacy* contained pieces on sanitizing disks, wireless security, the security of open-source software systems, and the security of Windows systems, the latter in fact being an examination of the aftermath of the Gates memo inside Microsoft [7].

In his editor's message from the 2002 teaser in *Computer*, Cybenko made the statement, "As computing professionals, we have an undeniable need to better understand the security and privacy aspects of our work. Recent and ongoing events have elevated that need from an afterthought to an obligation." He went on to pose these challenge questions: "We certainly have security and privacy problems today. How did we get here? How might we move forward?" [8]

20 years later, these challenges to continue to resonate. At the same time, so have solutions. Usable security [9], high assurance [10, 11], security-enhanced and open source hardware architectures [12], cyber-physical system security [13, 14, 15], and privacy-preserving data analysis [16] are just a handful of subdisciplines that have all gone from niche topics or almost entirely unknown subjects to mainstream approaches [17, 18, 19, 20, 21, 22].

In this issue, I am pleased to publish several articles celebrating *IEEE Security & Privacy*'s first 20 years. These articles include retrospectives by Crispin Cowan [23] and Steve Lipner and Mike Howard [7] on their prescient — in the view of this Editorial Board — writings on security from the first issue of the magazine. We also feature a delightful roundtable, "Looking Backwards (and Forwards): NSF Secure and Trustworthy Computing 20-year retrospective panel transcription" organized and edited by Carl E. Landwehr — the second Editor-in-Chief of this magazine — and featuring numerous other security and privacy luminaries in the field including current editors Trent Jaeger, Apu Kapadia, Tadayoshi Kohno, and Laurie Williams.

Thanks to Terry Benzel and Hilarie Orman, we present an article reprising the 2003 IEEE Symposium on Security and Privacy, widely recognized as the flagship academic security conference both then and now, and therefore serves as a valuable time capsule of the challenges and solutions of any given time to provide additional context for our anniversary celebration. Next up, Elissa Redmiles, Mia Bennett, and Tadayoshi Kohno present a provocative challenge to the community on the need to apply *critical theory* to security and privacy in the evaluation of existing systems and the development of new ones. Finally, we are pleased to feature an article based on a podcast episode of *Over the Rainbow: 21st Century Security and Privacy* moderated by Bob Blakley and Lorrie Cranor and featuring three of the magazine's early Editors-in-Chief: George Cybenko, Carl E. Landwehr, and Shari Lawrence Pfleeger.

Throughout the rest of 2023, readers will see additional articles appearing in future issues continuing this celebration as well. On behalf of *IEEE Security & Privacy* Editorial Boards both past and present, I invite readers to enjoy the pieces in this issue and throughout the year, celebrating

the past 20 years, and also of course to continue to look to *IEEE Security & Privacy* for the best in forward-looking security and privacy articles the next 20 years as well.

References

[1] George Cybenko. A Critical Need, an Ambitious Mission, a New Magazine. *IEEE Security & Privacy*, 1(1):5–9, Jan/Feb 2003.

[2] George Cybenko and Kathy Clark-Fisher. IEEE Security & Privacy: The Early Years. *IEEE Security & Privacy*, 12(3):18–19, May/June 2014.

[3] Gary McGraw. Silver Bullet Talks with Richard Clarke. *IEEE Security & Privacy*, 8(4):5–11, Jul/Aug 2010.

[4] Douglas Maughan, David Balenson, Ulf Lindqvist, and Zachary Tudor. Crossing the "Valley of Death": Transitioning Cybersecurity Research into Practice. *IEEE Security & Privacy*, 11(2):14–23, Mar/Apr 2013.

[5] Bill Gates. Memo from Bill Gates. `https://news.microsoft.com/2012/01/11/memo-from-bill-gates/`, January 11, 2002.

[6] David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver. Inside the Slammer Worm. *IEEE Security & Privacy*, 1(4):33–39, July/August 2003.

[7] Michael Howard and Steve Lipner. Inside the Windows Security Push. *IEEE Security & Privacy*, 1(1):57–61, Jan/Feb 2003.

[8] George Cybenko. Editor's message - The Long March. *Computer*, 35(4):1–4, April 2002.

[9] Dirk Balfanz, Glenn Durfee, Diana K Smetters, and Rebecca E Grinter. In Search of Usable Security: Five Lessons from the Field. *IEEE Security & Privacy*, 2(5):19–24, Sept/Oct 2004.

[10] Steve Lipner, Trent Jaeger, and Mary Ellen Zurko. Lessons from VAX/SVS for High-Assurance VM Systems. *IEEE Security & Privacy*, 10(6):26–35, Nov/Dec 2012.

[11] Gernot Heiser, Toby Murray, and Gerwin Klein. It's Time for Trustworthy Systems. *IEEE Security & Privacy*, 10(2):67–70, Mar/Apr 2012.

[12] Peter G. Neumann, Sean Peisert, and Marv Schaefer. The IEEE Symposium on Security and Privacy, in Retrospect. *IEEE Security & Privacy*, 12(3):15–17, May/June 2014.

[13] Ralph Langner. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy*, 9(3):49–51, May/June 2011.

[14] Sean Peisert, Jonathan Margulies, David M Nicol, Himanshu Khurana, and Chris Sawall. Designed-in Security for Cyber-Physical Systems. *IEEE Security & Privacy*, 12(5):9–12, Sept/Oct 2014.

[15] Roland L. Trope and Eugene K. Ressler. Mettle Fatigue: VW's Single-Point-of-Failure Ethics. *IEEE Security & Privacy*, 14(1):12–30, Jan/Feb 2016.

[16] Jaideep Vaidya and Chris Clifton. Privacy-Preserving Data Mining: Why, How, and When. *IEEE Security & Privacy*, 2(6):19–27, Nov/Dec 2004.

[17] Mary Ellen Zurko. Disinformation and Reflections From Usable Security. *IEEE Security & Privacy*, 20(3):4–7, May/June 2022.

[18] William Martin, Patrick Lincoln, and William Scherlis. Formal Methods at Scale. *IEEE Security & Privacy*, 20(3):22–23, May/June 2022.

[19] Paul C. van Oorschot and Sean W. Smith. The Internet of Things: Security Challenges. *IEEE Security & Privacy*, 17(05):7–9, Sept/Oct 2019.

[20] David Kohlbrenner, Shweta Shinde, Dayeol Lee, Krste Asanovic, and Dawn Song. Building open trusted execution environments. *IEEE Security & Privacy*, 18(5):47–56, 2020.

[21] Nathalie Baracaldo and Alina Oprea. Machine Learning Security and Privacy. *IEEE Security & Privacy*, 20(5):11–13, Sept/Oct 2022.

[22] Priyanka Nanayakkara and Jessica Hullman. What's Driving Conflicts Around Differential Privacy for the US Census. *IEEE Security & Privacy*, 20(1):2–11, Jan/Feb 2022.

[23] Crispin Cowan. Software Security for Open-Source Systems. *IEEE Security & Privacy*, 1(1):38–45, Jan/Feb 2003.