

# Edge Cryptography and the Codevelopment of Computer Networks and Cybersecurity

Quinn DuPont\*  
University of Toronto

Bradley Fidler\*  
University of California, Los Angeles

\*Equal Author Contributions

The Private Line Interface was a cryptographic cybersecurity device used on the Arpanet, operating at the edge of the network with little modification of the network infrastructure. As a result of the historical trajectory furthered and illustrated by the PLI, significant cryptographic resources remain at the edges (or ends) of the networks that constitute the Internet today. This study is an entry into the historical relationship between cryptography and computer network.

In this initial study of the development of cryptographic security technologies for use on early computer networks, we demonstrate how the end-to-end security that remains an architectural feature of the modern Internet is a consequence of sociotechnical negotiations that emerged within development efforts on the early Arpanet. In tracing this lineage, we historicize the relationship between computer security and networks and the emergence of what we call “edge cryptography,” as an architecture and infrastructure, with the development of the private line interface (PLI) on the Arpanet—the first large-scale, general purpose, packet-switched computer network. We examine the means through which the PLI was developed and implemented and how the understanding that security was to be located at the networks’ edge migrated to subsequent cybersecurity discourse, which in turn shaped contemporary cybersecurity technologies. We characterize this history as codevelopment because, beginning with the emergence of the PLI, computer networks and cybersecurity communities and technologies began to impact each other in significant ways for the first time.

Our investigation sheds light on the relationship between computer security and networking first identified by Donald Mackenzie and Garrel Pottinger<sup>1</sup> that was later anthologized in Mackenzie’s book *Mechanizing Proof*.<sup>2</sup> MacKenzie argued that the “classical computer security problem”—of how to embody security in shared (multiprogrammed) computer systems—was resolved through research and development on securitizing communication on networks.<sup>3</sup> However, MacKenzie focused his historical research on cryptographic technology developed and tested in the 1980s, with the National Security Agency project called Blacker. However, we argue that this shift actually occurred prior to Blacker, with the PLI and its development on the Arpanet. Furthermore, we argue that the network security architecture that followed, what we call edge cryptography, was a consequence of this shift. During PLI’s development, the location of cryptography on network structures was still relatively unsettled, but as a result of technical and institutional decisions associated with its development, these possibilities were closed, which therefore altered the course of later understandings of cybersecurity and, correspondingly, our historical view of the topic.

We use the term edge cryptography to refer to the location of cryptographic resources in (packet-switched) network architecture, as well as in that architecture's implementation as infrastructure. As we will explain, we differentiate the "edge" of the network from the oft-used terminology of the network's "end," as instantiated in the famous "end-to-end" principle.<sup>4</sup> By "cryptography" we mean the broad set of deterministic, discrete technologies implemented for security (minimally, confidentiality and integrity), rather than the [56] mathematics sometimes used in associated algorithms. When referring to packet-switching computer networks, we mean the networks within the historical and technological trajectory that led, directly or indirectly, to the technical and institutional basis of the modern (post-1983) Internet, which transmits data in blocks over shared communication channels.

We do not attempt to shed light on the histories of the "classical computer security" challenges that emerged on early time-shared computer systems. In addition to MacKenzie's pioneering work, and that of others we will discuss (especially with regard to the formalization and specification of these early computing issues), promising research is currently underway by Thomas Misa and Jeffrey Yost, who have a multiyear computer security oral history project in progress. We expect that in the future it will be possible to draw thick connections between their histories of computer security and the history of online security technologies we address here. Rather than engage in the histories of these classical computer security challenges, we instead look to the architectural and infrastructural placement of security technologies and to its impact on the contemporary cybersecurity framework.

Today, discussions of information security and privacy often refer to cryptographic technologies as they exist on computer networks and typically the Internet. It is precisely this online security that is the subject of our investigation, rather than cryptographic technologies in isolation. We feel justified in focusing on this complex set of technologies and institutions because, typically, when the features or faults of the modern Internet are addressed, or make it to major news organizations,<sup>5</sup> it is usually due to

concern for online security. Crucially, these concerns for online security put focus on the ways that security technologies have been designed to work (or not work) with the Internet—now the subject of numerous efforts to design for security by default. And yet, the core technical foundations of the Internet were designed to work in the absence of any security or cryptography.

In fact, in the period between 1968 and 1976, the rough outlines of our contemporary online world emerge with what we call edge cryptography. On the Arpanet, the majority of users were using a totally unencrypted network. In 1968, when the request for proposals for the Arpanet was released by ARPA and later (in 1969) won by the defense contractor Bolt Beranek and Newman (BBN), there was no mention of security; the network's design was fundamentally insecure in the sense that it worked without cryptography. It was only by 1976 when BBN began deploying the first PLIs, a technology in development since 1973, that it was possible, for the first time ever, to have encrypted communication over an unencrypted packet-switched computer network. As a consequence of this history, secure communications over the Arpanet operated with encrypted packet payloads (such as user/application data), but unencrypted network metadata (such as network addressing and other machine-readable information required to deliver the packet). This distinction between plaintext metadata and encrypted data remains with us, often informing the technical foundation of modern debates over security and privacy on the Internet.<sup>6</sup>

This article details the PLI's development as an entry into the hitherto unexplored historical relationship between cryptography and packet-switched computer networks. Although in popular culture and victor hagiography the Arpanet is certainly over-emphasized,<sup>7</sup> nonetheless, by 1983 it became the core of an emerging Inter-network, or modern Internet, on which its architectural traditions were influential. The Arpanet was the long-haul network that modern TCP/IP was designed and implemented on, and it was also where early edge network cryptography was designed, tested, and implemented as an

operational infrastructure. These aspects of the Arpanet, in contrast with its role in the development of the modern Internet, are less well known.<sup>8</sup>

We argue that the technical, historical, and institutional links between packet switching [57] and cryptography that codeveloped on the Arpanet remain with us today. This is not because there were no other computer networks in existence in 1983, or even in 1973 or 1969, and it is certainly not because these particular technical and institutional dimensions are the only ones that count as proper history. Rather, it is because it was DARPA's Arpanet, and the subsequent DARPA Internet, that absorbed or erased the influences of its competitors that might have altered the edge cryptography trajectory we trace here, thereby providing a different path to the cybersecurity present.

To draw these conclusions, we discuss the histories and historiographies of networking and cryptography as well as newer research on the histories of computer security. Then, we analyze the ways that the histories of computer networking and security were traditionally thought to be separate, but were in fact linked. To demonstrate how these histories were linked, we detail the codevelopment of the Arpanet and PLI. Finally, we offer conclusions about what this case study offers the historiography of computer networking and cybersecurity. Namely, that the later histories of cybersecurity assume a tidy connection between computer networking and security, when in fact, such a connection was hard fought in the development of the PLI. This history also demonstrates that although end-to-end cybersecurity is lionized today,<sup>9</sup> the actual development (following from the PLI) was largely the consequence of the foreclosure of other architectural configurations.

### **Historiographies of Packet Switching and Cryptography**

Practitioner communities of both the networked computing and cryptography fields remained largely separate until, as we argue, the need to develop network security brought them into greater contact. This separation of communities has, until recently,

been reflected in historiography: histories of computer networks tended to neglect cryptography, and histories of cryptography tended to neglect computer networks. In other words, the separation is uncontested. Our approach is to survey both histories, and both historiographies, in order to understand the historical and scholarly components in the separation we describe. Later, we argue that the PLI is an artifact that reflects the initial separation, but also early entanglement, of those two communities. We also discuss newer research on computer security and its relationship to the historical separation and gradual entanglement of these communities and technologies.

### **Historiography of Networking**

Prior to the 1970s, the computer communication technologies that we now know as instant messaging and email were alive on time-shared systems, usually at institutions such as universities and firms, although they could not communicate with other (incompatible or remote) systems. By 1970, one general purpose, packet-switching computer network of heterogeneous machines was in existence: the Arpanet. It was at just five nodes—University of California, Los Angeles; Stanford Research Institute (now SRI International); University of California, Santa Barbara; and the University of Utah on the west coast and BBN on the east. Also, the distributed routing technologies that would power the network were in their working infancy. By 1972, the network had a working host-host protocol enabling easy interprocess communication, and communication services to be used over the network (such as mail and messaging). During this same year, France's Cyclades and the UK's MARK 1 packet-switched networks were online and making important contributions to networking. By the mid-1970s, networks and internetworks (often circuit switched), such as the European Informatics Network (EIN) in Western Europe, TRANSPAC in France, and DATAPAC in Canada were being planned or established as infrastructure. By 1977, the first multinet TCP/IP experiments were a success, as were the first experiments with IP routers. On the Arpanet, cultural communities were forming

around listserv discussion groups, including a precursor to social networking, the online status “finger” file. At the end of the decade, Minitel and bulletin board systems (BBSs), wide- and local-area time-sharing systems (respectively), were rolled out experimentally.<sup>10</sup>

The Arpanet pioneered the ability to connect heterogeneous computers over a shared communications subnetwork that utilized a distributed and adaptive routing algorithm. Designed for resource sharing between expensive computing centers, but quickly utilized by users for interpersonal communication such as email, the Arpanet was born out of a general interest by DARPA and elsewhere in the DoD for more effective command and control technologies.<sup>11</sup> Once established, the Arpanet quickly became a success, demonstrating not only the technical feasibility of [58] packet-switched computer networks but also the inherent usefulness of large-scale interpersonal communication with computers.

The ARPA contractor based in Cambridge, Massachusetts, that built, maintained, and ran the Arpanet, BBN began its work in January 1969; its initial charge was to make operational the network’s basic functions of moving data from computer to computer. Over Labor Day weekend in 1969, BBN delivered UCLA’s IMP and connected it to the SDS Sigma 7 host. The IMP, a minicomputer slightly narrower and taller than a consumer refrigerator, was engineered to serve as the host’s link to the future network of other IMPs and hosts. Within the same year, other computing centers joined the UCLA node, including the SRI, UCSB, and the University of Utah. One of BBN’s early tasks, a massive one, involved establishing a working subnetwork and maintaining and increasing its reliability as the Arpanet grew in size and complexity. The subnetwork—or subnet—included all the IMPs and links that interconnected them, comprising the core physical infrastructure responsible for transporting data between the hosts. Building a working subnet entailed more than simply putting hardware into place. To ensure that data packets would flow successfully through the IMP network, BBN developed custom IMP hardware and software, including the crucial routing algorithm. Importantly, the subnet

had to be invisible to users, shuttling data between hosts automatically.<sup>12</sup>

Host computers were not connected directly to each other, but rather, they were connected to a local IMP. When one IMP received a message from a connected host, it would break the message into packets and send each packet to the IMP it decided was the next best “hop” toward the destination IMP connected to the destination host computer. Each packet was encapsulated in header metadata that included information such as its destination address. Once the packets arrived at the destination IMP, it would reassemble them into a message that the destination host computer would interpret and transport it to the destination host through another set of protocols.

The Arpanet saw the modularity pioneered in early operating systems formalized in networking as layering. Above the routing algorithm, through which the IMPs passed information across the network, each host computer ran an implementation of the Host-Host Protocol, called the Network Control Program (NCP), providing host machines with a uniform way of communicating across the network, thereby overcoming differences in operating systems, character sets, and the like.<sup>13</sup> Although the Arpanet was not an end-to-end architecture like TCP/IP (in that the ends of the subnet, not the hosts, handled the majority of the error correction and flow control), the source and destination IMPs functioned as “ends” given their role in dynamically establishing connections that governed the flow of packets and acknowledgements between the source and destination IMP. Although the Arpanet’s layered protocol suite did not have the same number of layers as the later OSI-inspired TCP/IP stack, it did have discrete layers.<sup>14</sup> The consequence of this layered, or modular design, was that there were many options—and infrastructural tensions<sup>15</sup>—for where to fit cryptography into the system.

The first four nodes of the Arpanet were online in 1969, and by 1972, the first discussions leading to the formation of the International Packet Network Working Group (INWG) were already underway. A key outcome of the INWG is that it sought

international consensus on an internetwork architecture.<sup>16</sup> The TCP/IP protocol suite was then implemented on the Arpanet in 1983, and for the next few years, the Arpanet was the central network on what was then often referred to as the “DARPA Internet.” By this time, the large host machines of 1969 were often connected to local area networks, scaled down mainframes, and even personal computers, with TCP/IP running over the Arpanet, and a rapidly increasing number of networks were being connected. By the time the Arpanet was decommissioned in 1989–1990, it was a small (and obsolete) part of a rapidly expanding and global Internet.

Although certainly not the Internet we know today, the Arpanet created standards [59] and traditions that continued on it. Many of the programs written on top of the NCP protocol suite, such as telnet and email, were rewritten for TCP/IP. Architectural features such as a layered architecture and network sockets survived as well.<sup>17</sup> Importantly, the decision to put significant computation or “intelligence” at the edges of the network not only continued, but intensified in the move from the Arpanet’s NCP to the Internet’s TCP/IP. The Arpanet was the network around which the Internet’s autonomous systems and border router architecture (EGP and BGP) were developed.

The Internet’s public success and rapid development created two waves of network historiography: the first in the 1990s and the second (with academic historians and other scholars) beginning around 2010. The first wave of historiography documented the key technical achievements and personalities of an Arpanet- and Internet-centric corner of network history, from a US perspective. It included key works by Peter Salus; Michael Hauben and Ronda Hauben; Katie Hafner and Matthew Lyon; and Arthur Norberg, Judy O’Neill, and Kerry Freedman.<sup>18</sup> Janet Abbate presented a break from a personality- and technology-driven linear narrative by seeking to rewrite this history from within a science and technology studies (STS) lens.<sup>11</sup> Largely beginning in the 2000s, a new generation of scholars began to explore new topics, such as networking technologies and practices that fall outside of the US story, as well as

the social and cultural forms that took shape around computer networks.<sup>19</sup>

These two generations of scholarship on computer networking technologies have made considerable progress toward creating a broad, general history of computer networking. Nonetheless, they do not attend to cryptography in a systematic way, an essential aspect of computing and culture today, or explore its role in the development of the networks themselves. This is because, we argue, by the time that cryptography entered the public domain—and left its semiclassified state of development by defense contractors for defense and intelligence networks—its architectural location on the Internet had been settled and could be taken for granted.

The emergence of computer networks also gave rise to discussions of the information society, detailing the ways in which communication and computation technologies are remaking the economy, polity, and culture.<sup>20</sup> Popular recent works on the social impact of surveillance powers, in the wake of the Snowden leaks, have also addressed some of the normative questions surrounding the information society.<sup>21</sup> Moreover, it is now common to analyze the world in “network” terms.<sup>22</sup> In addressing packet switching and using it and related protocols as a metaphor for modern society, however, we note that this is a vision of technology free of cryptography or security. The discourse of the “networked world” that is chalk full of computer network metaphors elides the fact that these networks were built alongside security technologies—not the ones envisioned early on by Paul Baran, as we will address here, where security was to be tightly integrated into the architecture of the network—but instead, configured to the edges, and present at its inception and persistently co-determining the development of the network.

### Historiography of Cryptography

Well before networked computers (and in any practical sense, before “computers” themselves), at the beginning of “modern” cryptography, Claude Shannon made important mathematical and analytical discoveries that closely aligned the later develop-

ments of cryptography and packet-switched networks. In 1945, Shannon wrote a memorandum in which he developed the (logarithmic) mathematics to calculate the statistical properties of language for the purpose of cryptanalysis<sup>23</sup> and worked out what is required for “perfect secrecy.”<sup>24</sup> Of special relevance to later developments in digital communication, Shannon noted (in his later, declassified version of the same work, from 1949), “the [cryptography] problem is closely related to questions of communication in the presence of noise, and the concepts of entropy and equivocation developed for the communication problem find a direct application in this part of cryptography.”<sup>24</sup> Later, Shannon again echoed his view that information theory and cryptography were essentially linked; in interviews Shannon argued that “this cryptography problem was very closely related to the communications problem”<sup>25</sup> and that the two ideas developed concurrently: “the mathematical theory of communications and the cryptology went forward concurrently from about 1941... I worked on both of them together and I had some of the ideas while working on the other.”<sup>26</sup> Framing the information communication question in terms of syntactic change of discrete symbols (citing R.V.L. Hartley’s work on telegraphy),<sup>27</sup> [60] Shannon understood problems of cryptography as fundamentally similar to the information and communication challenges getting taken up in computing, and later, computer networking.<sup>28</sup>

Cryptography in Shannon’s day used mechanical, and then increasingly, electro-mechanical devices to encrypt and decrypt messages by deterministically rearranging and substituting plaintext letters for some ciphertext representation (for example, with rotor disks, used in machines like Enigma, Purple, and SIGABA or with XOR or table-based shift registers, as later used in the Data Encryption Standard).<sup>29</sup> Encryption works by obscuring the original meaning of the message by some syntactic “diffusion” and “confusion” techniques, such that without knowledge of the original encryption algorithm and (where applicable) key information, eavesdroppers are unable to understand the ciphertext message.<sup>23</sup> Decryption reverses the encryption process, reproducing the original message. The critical aspect of

secure cryptography in Shannon’s day was that it was necessary to ensure secrecy of at least some part of the system, usually the keying material (as per Kerchoff’s principle), but often also the encrypting algorithm. Cryptography remained in this form until the 1970s, when two significant changes occurred.

The first, somewhat slower change of the 1970s, was a structural realignment of the entities and institutions who produced and consumed cryptography. In Shannon’s day, cryptology was exclusively the purview of governments, and even then it typically only used for important military or high-level state communications. Rather, it was common for data storage and message transmission to be kept physically secure, using hardened lines or kept in guarded locations, in addition to (or often instead of) cryptographic protections. It is within this context that, independently, in the 1970s, as computer use flourished and quickly proved a necessary part of business processes,<sup>30</sup> that computers were also being connected and interconnected—often at great distances from each other. Such “online” connections forced governments and businesses to face the challenges and risks that arise from nonsecure transmission. It soon became clear that if networked computers were going to be vital and useful to modern society, they would need to solve the issue of security.

Therefore, to address this new computer reality, critical forms of software encryption were developed in the 1970s, causing the second major change. Software encryption was developed in response to, and alongside, computer security work from the 1950s onward—on cybersecurity standardization, the development of time sharing systems, and a search for provably secure computing kernels.<sup>31</sup> In the early 1970s, the US Air Force (USAF) requested the production of an encryption algorithm for the Multics system, first delivered through a three-party joint effort by Honeywell Information Systems, Massachusetts Institute of Technology (MIT), and the USAF.<sup>32</sup> The Multics encryption algorithm was unusual for the time because cryptography was not typically performed by software; it was in fact perhaps only the second time encryption had been realized in software, although non-cryptographic computer

access control systems had been in development since the 1950s.<sup>32,33</sup> By the late 1970s, multiple computer security projects were running in parallel, funded variously by DARPA, the DoD, National Institute of Standards and Technology, and private companies, culminating by 1983 with the development of the Trusted Computer System Evaluation Criteria (TCSEC), known colloquially as the Orange Book.<sup>34</sup>

Within months of the release of the Multics encryption algorithm (which had been in production for some years), Horst Feistel published the article “Cryptography and Computer Privacy” in *Scientific American*, detailing his Lucifer algorithm, developed from years of work on Identification Friend or Foe (IFF) systems originally while at the Air Force Cambridge Research Center, then MIT’s Lincoln Laboratory, MITRE, and finally coming to fruition at IBM.<sup>35</sup> In the same month as Feistel’s *Scientific American* publication, the National Bureau of Standards put out a formal request for a new data encryption standard for unclassified information, which would eventually (in 1976) become the Data Encryption Standard (DES), more or less based on Feistel’s design. DES was innovative in that it was a [61] “block” design—not encrypting individual bits as previous “stream” ciphers did—but instead, like the packet-switched networks in development at the same time, encrypting a fixed-length group of bits and padding as necessary. These data encryption designs marked one of several paths for how cryptography would be integrated with computing.

These software cryptography technologies, designed for encrypting static data, however, used the same key distribution model as always, which required both communicating parties to possess identical keys that must be kept absolutely secret. This would typically mean that keys needed to be distributed synchronously across every element in the communications network in advance or, alternatively, keyed and routed through a centralized switching center.<sup>36</sup> Alternatively, individual nodes may also be keyed at the edges of the network, creating cryptographic subnetworks.

However, around the same time, a new model for cryptographic key distribution developed, known as public-key cryptography—first in secret at the Government Communications Headquarters (GCHQ) and then again in public, by Whitfield Diffie and his collaborators.<sup>37</sup> As it developed in public, this research fell within the purview of the Arpanet, already in development, but in fact developed independently, drawing on different resources, architectures, and institutions. At first, ARPA’s Director of Information Processing Techniques Office (IPTO) Larry Roberts approached the NSA to request research into new models for cryptography that might be suitable for a large, distributed network, such as the Arpanet.<sup>38</sup> Roberts was brushed off, but the problem eventually made its way to John McCarthy and his Stanford Artificial Intelligence team, where Diffie was working. This challenge sparked Diffie’s fascination with the problem of key distribution for large networks, which was similar to issues he had been working on. After some years of research, Diffie devised a unique solution to cryptographic key management, worked out in detail with the help of Martin Hellman and Ralph Merkle. In 1976, Diffie and Hellman published the influential paper “New Directions in Cryptography,”<sup>39</sup> setting out the conceptual model for public-key cryptography.

Diffie and Hellman proposed a radical new way to handle the keys necessary for secure cryptography. Rather than require each participant in encrypted communication to possess identical keys, Diffie and Hellman saw key production as a kind of reciprocal interaction, adapted from challenge and response technique developed in the 1950s for IFF systems.<sup>40</sup> The model that eventually emerged was to split a single key into two mathematically linked halves, which could be used separately by the communicating parties. The model required a one-way, trapdoor, or knapsack mathematical function to link the two halves, which a year after Diffie and Hellman’s influential paper, was supplied by Ralph Merkle, who had been previously working on the problem at the University of California, Berkeley.<sup>41</sup>

With this brief history of modern cryptography, we can already see the points of convergence where cryptography could have directly intersected with

the emerging Arpanet or other computer networks, but did not. Indeed, the aim of Abbate's pioneering work on the history of the Internet was "to show how military concerns and goals were built into the Internet technology," which she accomplished in a study of the elements of architecture and infrastructure that did not involve the security technologies we address here.<sup>42</sup> We are led to wonder why this is the case: distinct from the history of public-key cryptography, which is fairly well known to historians, how did the first communications encryption tool emerge on the Arpanet? To understand how encryption developed on the Arpanet, we offer another history, as one example of the complicated interrelations between computer networking and cryptography.

Unlike the generations of historiography on computer networking technologies, the academic history of cryptology is still largely unwritten. To the extent that it does exist, it is largely occupied by technology and personality-driven accounts. Although the history of cryptography is long, rich, and varied, extant histories have tended to look like traditional history of technology scholarship, which in the case of the history of cryptography, has focused on military histories, technological descriptions, and code-breaking (cryptanalysis) efforts, with an emphasis on events of the 20th century.<sup>43</sup> Journalistic and general audience accounts have tended to fill in the many gaps where the small community of academic historians have not yet covered.<sup>44</sup> Some modern and premodern historians have also addressed the topic, with a longer view of the subject.<sup>45</sup> Consequently, the hallmarks of a well-developed historiography are largely absent from the history of cryptology. [62]

In addition to cryptology historiography, a newer area of investigation on computer security also informs our topic. In security parlance, this is the history of communications security, or COMSEC, which has traditionally been thought to emerge out of what MacKenzie calls "classical computer security." While this literature informs our account, we also make a contribution to it. At the outset, we note that the history of the PLI can be understood as the convergence of networking and (cryptographic) communications security communities. Computer

security itself though—including the security of computers that exist online—is not the result of such a combination. This is another reason why we locate the PLI, and the edge cryptography path it set in motion, as distinct from the early history of computer security.

This "classical computer security problem" was described by MacKenzie as a search for solutions "to embody security in the system software of 'large multi-programmed system with remote terminals.'"<sup>46</sup> The challenges the emergence of shared systems presented to communities interested in security were in the first instance coming up with ways to prevent one user's program from inadvertently (or purposely) overwriting or reading a memory location being used by another user. To address such issues, research at the time focused on developing ways to secure operating systems by establishing verifiably secure designs, implementing security kernels, and developing a system of "flags" to indicate the security status of users, files, and terminals.<sup>47</sup> This system of security flags would eventually be modeled and formally specified, as with what eventually became the Orange Book, and its application to multi-level systems (such as Blacker).<sup>48</sup>

Much of this modeling, verification, and specification work was being done at the same time as work on the PLI and, in some ways, was in dialogue with the work of developing computer network security. One significant project to develop a verifiably secure operating system was the SRI's Provably Secure Operating System, in development from 1973, the same year research begun on PLIs. However, the PLI was more proximately associated with blurring the existing (cryptographic) communications security research than it was with this classical computer security problem. One such computer networking project associated with the developments taking place to solve the classical computer security problem and the challenges of networking was the Encrypted Packet Interface, which was developed between 1977 and 1981. The Encrypted Packet Interface was an encryption system (using DES symmetric-key algorithms) that was tested (but never implemented) on the Arpanet and had the unique quality of being built from verifiable code, in precisely the



same way as the efforts to create secure operating systems, like the Provably Secure Operating System.<sup>49</sup> However, these developments occurred largely after the critical developmental steps of the PLI.

Research on the history of the classical computer security problem has been well attended to. In particular, an important collection of historical scholarship on cybersecurity is found in a 2015 special issue of *IEEE Annals* of on computer security (part one in a two-part series that concludes with this issue). This scholarship can be organized into two categories: work analyzing histories that coalesce around the classical computer security problem of securing time-shared systems or around the newer problem of building effective and secure computer systems that would provide security on, and over, the Internet. These problems are, to be sure, deeply intertwined, and the newer security issues may also be understood as a new paradigm added to the first. (For this reason, some articles in the *Annals* special issue deal with both.) Either way, our work is an effort to understand the genealogy of this newer problem of systems that are secure on and over the Internet. Crucially, we want to identify the way that online security was first implemented on the Arpanet and Internet, [63] and its consequences for the ways that security was subsequently implemented and understood. As such, our work sits between the two types of histories in the first special issue and may be used as a way to build tentative links between early efforts to secure individual systems, on the one hand, and the difficulties associated with edge cryptography, on the other.

Here, we can also note that the public-key encryption architecture and infrastructure studied by Laura DeNardis and Dongoh Park emerged in the lineage of edge cryptography, and we hope our study can add historical context to these works, perhaps further linking their investigations.<sup>50</sup> Steven Lipner traced the origins the Orange Book and with it policy for security standards within and outside the DoD.<sup>51</sup> Michael Warner further explored this link between the NSA and networking communities, as well as detailed important reasons for the split be-

tween networking and security research communities.<sup>52</sup> We see ways for future study on how risk management and the specification of “security” emerged alongside the history we trace.<sup>53</sup> Perhaps most importantly, future research might draw links to the actors and history we document, and computer security products in the private sector.<sup>33</sup>

### **The Early Development of Cryptography and Computer Communications**

Computer networking and cryptography are thought to be historically separate. Yet, beginning in the 1970s, this division emerged as a disciplinary artifact and thus is not necessarily historically justified. As we have already seen, the genealogical codetermination of the origins of information theory and cryptography can be traced to Claude Shannon’s groundbreaking work after World War II, leading indirectly to the development of modern information and communications technologies, including the development of packet switching.<sup>54</sup> Following Shannon’s work, Paul Baran further established links between cryptography and computer communications, although these links ultimately proved to be historical dead-ends. After Baran’s pioneering work, several efforts within the US military attempted to fuse cryptography and computer networking, with varied levels of success. The success of emerging packet-switched networking, however, demonstrated how these multiple networks could be united, but still required an answer to the issue of security. Given the network architectures by then in place, the natural place for security technologies was at the edge.

In 1959, Paul Baran joined Rand’s computer science department, and in the shadow of the Cold War, he became interested in developing a network of nuclear-strike survivable communications.<sup>55</sup> Over the next three years, Baran developed the ideas for a new system he called “distributed communications,” where network redundancy would guard against any one nuclear strike stopping service.<sup>56</sup> Baran’s design advocated for ubiquitous, or what we now call “opportunistic,” cryptography (where all communication is encrypted to some degree, even for messages with no need for secrecy).<sup>57</sup> According to Baran,

there are three types of secure networks: end-to-end cryptography, link-by-link cryptography, and double encryption, which Baran envisioned as a combination of end to end and link by link. (In terms of technology, Baran envisioned encryption and decryption occurring through linear shift register machines, in the style that Shannon described previously.) Link-by-link cryptography leads to the impractical situation, where for each link added, additional links needs to be keyed because encrypting and decrypting machines must be identically keyed at the ends of the communication channel. Baran also anticipated multilevel security (of the sort advocated in the Orange Book standard), in which a single channel could (and in his mind, should) carry both classified data and civilian data. According to Baran, a mixed-use channel achieves greater security through obscurity, by increasing the information load for potential cryptanalysis, but also by obscuring packet traffic. (In the autokey, or linear shift register type of encryption Baran proposed, every single packet is needed for potential cryptanalysis, because each packet is encrypted using a key derived from the prior.) Crucially, such mixed-use security is only possible because messages are packetized and individually routed.

Baran's favored model was double encryption, which works by creating a set of quasi-circuits that are strongly encrypted at each end, with the header of each message weakly encrypted, link by link. That is, the message is encrypted a second time (super-encrypted) when the header is encrypted with link-by-link encryption. To make the double-encryption system work, Baran suggested that encryption ought to be built right into the network architecture, applied at both the ends [64] and at the switches. Baran wrote, "Thus, the distributed network shall use both link-by-link and end-to-end encryption. Rather than adding boxes to each switching center, the cipher encoder and decoder circuits shall be designed as an integral part of the Switching Nodes and Multiplexing Stations."<sup>58</sup> This pertinent research, however, was scarcely noticed by the institutions and engineers who would later implement the Arpanet, the Internet, and network security.

In the 1960s, the US military had a range of service-specific and tactical networks, few of which could communicate with the other. The Defense Communications Agency (DCA; now Defense Information Systems Agency, or DISA) was formed in 1960 with the purpose of creating cross-service, common-user communication. As part of this mission, they used the USAF's logistics supply network, COMLOGNET, as the basis of the Automatic Digital Network (AUTODIN), which provided secure and authenticated communication across the services. AUTODIN was a homogenous digital store-and-forward (not packet-switched) network that consisted of a small number of switches, which were attached to a larger number of staffed communication centers. This strategy was also employed on the Worldwide Military Command and Control System (WWMCCS) network, a store-and-forward network that connected the US military's theater command structures. For these systems, the security architecture consisted of totally secure facilities with link encryption, of the traditional style, between the nodes. A major shift occurred in 1972, when the WWMCCS architects began to consider a switch to new, packet-switching technologies, which by then were demonstrating their technological superiority, in use for DARPA's Arpanet experiment.

As an entrée to the development of the PLI, the DCA conducted early, successful experiments to test the feasibility of IMPs communicating securely by passing all their communications through a key generator (KG) unit. The main technological challenge, in fact, was to get the Arpanet packet switches working with a KG unit. This was also the beginning of edge cryptography, in which packet switching was made secure by adding cryptographic technologies not within the switches (as Baran imagined), but modularly, at the edges of the networks. For packet switching to remake the ecosystem of defense and intelligence networks, demonstrating the advantages of packet switching was only the first part. Demonstrating that such systems could be made secure, in a variety of environments, was equally if not more important than proving the utility of packet switching, and the first experimental connection of an IMP to

a cryptographic device was a key step in this process.<sup>59</sup>

On Arpanet-type networks, the “edge” was logically the source and destination IMPs because this was where packets were reassembled and provided to the host machines. Source and destination IMPs typically (but not always) were the last word on error correction and buffering.<sup>60</sup> By placing a PLI (and KG unit) between the source or destination IMP and the host computer, cryptography was added modularly, in that it was not integrated with either an IMP or a host. This also meant that the PLI was located at the network’s edge, beyond the destination IMP, and between the destination IMP and the host computer.

We use the term “edge” in order to avoid confusion with the technical and political effort to define and defend the “end” of the network (hosts) as the appropriate place of the maximum amount of network-related intelligence,<sup>4</sup> and as an analytical distinction, the early decision to locate cryptographic technologies at the “edge,” but logically before the “end.” BBN and IPTO’s decision to locate cryptographic intelligence at the edge of the network, circa 1973, was in fact prior to the gradual articulation of the “end-to-end principle” in civilian networking communities, and it was well before the establishment of cryptography best practices, now considered to be “end to end” encryption.

The end-to-end principle in computer networking argues that because of the inefficiencies inherent in sharing tasks between the network and host applications (specifically, no matter how well a network [65] accomplishes a task, such as through error correction, a host process or application will still need to function as the final word), it is better to locate functions entirely in the hosts, or network ends, whenever possible.<sup>61</sup> For example, by the time Steven Kent’s influential 1976 dissertation informed the development of the BCR encryption system, what we call edge cryptography was already a given, as shown by Kent’s reasonable assumption that intermediate routers and lines would be in the clear and not up for redesign.<sup>62</sup> In the canonical “End-to-

End Arguments in System Design” paper that systematized the prior end-to-end arguments, however, network security is mentioned only briefly, and no argument is given to the utility or philosophy behind the application of end-to-end principles to security.<sup>63</sup> Thus, the decision to use “edge” over “end” terminology denotes a distinction between the to-be-determined state of the relationship of early decisions to place cryptographic resources at the network’s edge and the subsequent design decisions that further located network computing resources—now including cryptographic security—even beyond the “edge,” to the “end,” in the hosts themselves. Once networking computing resources were moved to hosts, which became the new “ends” with TCP/IP, cryptography was, in different ways, moved there as well. Thus we also use the term “edge” to refer to the PLI system because the “end” of the network moved further outward when the Arpanet became, after its conversion to TCP/IP, the backbone of the Internet.

Prior to this move to the “edge,” in the early years of the Arpanet, a technology existed to create Arpanet-style packet networks that were secure at a single level (the experimental WWMCCS network, or PWIN). However, the defense and intelligence communities were interested in utilizing single-packet-switched backbones at multiple levels of security. This would allow them to mix classified and civilian traffic and, more importantly, to have different levels of classification on a single network—a functional requirement made necessary by the structure of multiple levels of classification in the American defense and intelligence communities.<sup>64</sup> To accomplish this, they would need to be able to modify the security architecture so that groups of hosts could communicate securely over an unsecured network. For this capability, in 1973 DARPA directed BBN to begin development of the PLI.

### **The Codevelopment of the Arpanet and PLI**

In the second quarter of 1973, research begun on security for the Arpanet, at ARPA’s request.<sup>65</sup> At this point, the Arpanet’s core functionalities—its packet-switching subnet, as well as its host-level NCP and

key applications such as email and telnet—were already developed and in use, and the network already connected international partners. Security for the Arpanet was expected to be conservative, accomplished with link encryption using a PLI minicomputer in conjunction with a military KG-34 encrypting/decrypting machine, which together would appear to the IMP as a “fake” host, thereby establishing secure subnetworks within the broader Arpanet. By 1976, BBN had successfully deployed PLI units, and by 1980, the units were deployed on the NSA’s Community Online Intelligence System (COINS) network.<sup>66</sup> Later, the PLIs were supposed to be replaced by Internet PLIs (IPLI), which did not see wide deployment.

In available documentation, discussion on the PLI first arise in the second quarter of 1973.<sup>65</sup> From this early planning stage, the PLI was understood to be part of the successor High Speed Modular IMP (HSMIMP) project, which would later be called Pluribus (in April 1974).<sup>67</sup> The HSMIMP project had two stated goals: be significantly faster (one megabit and above transmission speeds) and have a modular design, which would create fault tolerance and radically increase reliability, as well as, of course, to add security.<sup>68</sup>

As part of the HSMIMP/Pluribus project, the PLI did not only provide security. In fact, [66] it appears that security was simply a feature of the HSMIMP/Pluribus project’s broader ambitions, which was in turn were part of the broader narrative and development effort to create end or edge network intelligence. Early on, BBN was only “considering” adding the “additional” feature of the PLI “to drive a security unit as a peripheral.”<sup>69</sup> The primary goal of the PLI was to provide IMP-like access to the Arpanet so that “‘simple-minded’ systems [could]... take advantage of the ARPA Network technology.”<sup>70</sup> The PLI hardware was chosen for its modularity and compatibility, so it could physically accommodate different arrangements and peripherals. Additionally, repurposing the “multi-programming techniques” developed while programming the HSMIMP/Pluribus IMP allowed the PLI system designers to reap the same benefits, reducing labor and

speeding development for when it came time to develop the PLI software.<sup>71</sup> Fairly quickly, however, the Pluribus and PLI projects became tightly aligned; in 1973, it was projected that the PLI “will also handle all of the IMP/Host” protocol.<sup>72</sup> By replacing the existing private but non-cryptographic lines with a PLI subnetwork, it was reasoned, there would be no negative impact—only a probable improvement in the network’s reliability and a decrease in communications costs.<sup>72</sup>

Between 1973 and 1974, many of the architectural design decisions for where network intelligence would be located were still in flux. On the one hand, there was a significant desire to establish a simple way to isolate questions of communications security from design decisions of the network.<sup>72</sup> Yet, the security role quickly grew to prominence within BBN and its sponsors, soon surpassing all other stated roles for the PLI (as a product of the Pluribus project). BBN engineers would begin to formally distinguish between the roles, calling the “secure” version of the system the PLI/1 and the high-speed version the PLI/2 (or bitstream PLI).<sup>73</sup> The PLI/2 machine was built for speed, but capabilities for high speed was also in part motivated by security needs, thought to be useful for providing sustained, logically separated throughput, as would be needed for connection to the Lincoln Laboratory continuously variable slope delta (CVSD) vocoder device. Work also continued on the development of Pluribus IMPs for reliability and satellite communications applications.

By the end of 1974, BBN had resolved the architectural issues remaining for the secure PLI, opting for a conservative design that placed an encrypting device in series, between two PLI units, one “red” (plaintext) and one “black” (ciphertext), housed in a single TEMPEST-approved housing (see Figure 1).<sup>74,75</sup> Each PLI unit would interface with an encrypting/decrypting device, the KG-34,<sup>76</sup> a decision made in consultation with the NSA.<sup>77</sup> The KG-34 is a cryptographic device in the KG-30 family, which remains classified, so little is known about its design and operation.<sup>78</sup> Nonetheless, the KG-34 was probably older technology for the time and perhaps a linear shift register (similar in design to what Baran had

suggested a decade earlier).<sup>79</sup> The KG-34 unit was manually keyed (and rekeyed as needed) by authorized personnel who carried small handheld “fill” devices and accessed the “permuter boards” inside the KG unit.<sup>80</sup>

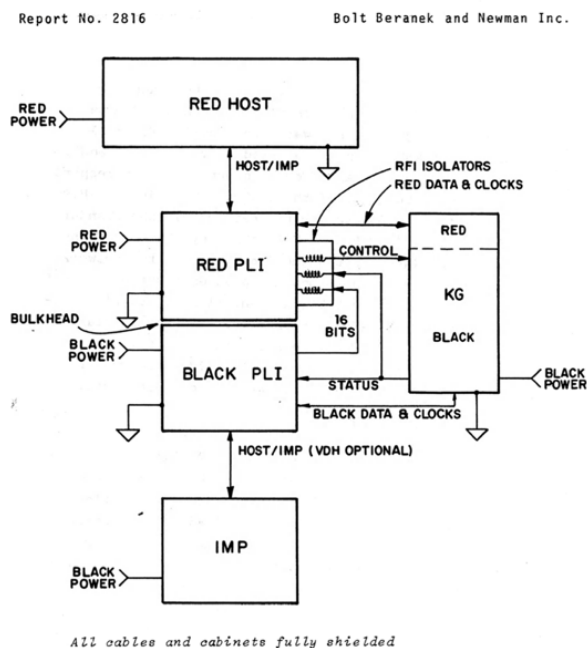


Figure 1. PLI Configuration.

Figure 1. PLI configuration. The “red” (plaintext) and “black” (ciphertext) connections between hosts and IMPs were housed in a single TEMPEST-approved housing.<sup>75</sup>

The secure communications process on the Arpanet with the PLI works as follows: communication is initiated by the (source) host, and the red (plaintext) PLI initiates a control signal to request a key-sequence from the KG-[67]34. The red PLI strips off the header and sends the plaintext into the KG-34 unit along with control data for the destination red PLI. The KG-34 then encrypts all the data and sends it to the black PLI (physically located in the same housing). The black PLI then constructs a new header containing subrouting information (previously programmed into the PLI as a numeric value corresponding to the available PLIs in the subnetwork) and passes the encrypted data and new

(plaintext) header to the standard IMP, which receives the message as a normal Arpanet message.<sup>81</sup> On the destination end, the process is reversed, with the black PLI stripping the subrouting header, the KG-34 decrypting the message, and the red PLI adding the original header. For both the host and the IMP, each side of the PLI appear as part of the normal Arpanet infrastructure—when sending a message the red PLI appears as a (local, distant, or very distant) IMP to the host and on receiving a message, the black PLI appears as a host to the IMP.<sup>82</sup>

The PLI did not create multilevel security over a network, nor did it deal with the complexities of key distribution (. From a cryptographic standpoint, it was a conservative device, not intended to push technological boundaries. Rather, it was designed to create reliably secure communication between designated groups of hosts over the Arpanet. PLIs, and the “logical subnetworks” of hosts they created, were used to connect a range of projects, including research on phased array radar and fire control systems.<sup>83</sup> PLIs were also used to connect secure sites on the Arpanet to fully secure networks linked to it by gateways.<sup>84</sup> In this way, PLIs further integrated the Arpanet into the classified defense and intelligence world, while still allowing it to function as a host to civilian communities. Crucially, the PLI was the first successful system to blur the distinctions between computer security and communications security, forging what would soon be understood as computer networking security, or simply, cybersecurity.

A major missing feature of the PLIs was key distribution. To reduce the labor and security risks generated by manually keying PLIs, in the late 1970s, BBN embarked on the Black/Crypto/Red (BCR) Project, an encrypting/decrypting device that included key distribution infrastructure and would work on TCP/IP internetworks. According to Steve Kent, a communications security specialist working at BBN at the time, BCR was developed between 1975 and 1980 by Collins Radio or Rockwell, under DARPA funding.<sup>85</sup> This history of computer networking security finally intersects with the history of cryptography, as BCR operated with TCP/IP and

used the first DES chips certified by the National Bureau of Standards, keyed and authenticated by an automated key distribution center. By 1980, BCR was undergoing substantial performance testing, however, it was shelved shortly thereafter.

Then, using BCR as a model, BBN developed the IPLI for inter-network secure communication. Like BCR, the IPLI used TCP/IP and a newer encryption/decryption device (the KG-84), but it was still manually keyed. The IPLI was intended as a backup program, funded by DARPA and DCA, in case the more ambitious, multilevel security Blacker program was delayed (which was the case). Some IPLIs were deployed in the mid-1980s, however, again only briefly, and shelved before seeing wide deployment.

Finally, Blacker was, at least briefly, implemented on the Defense Data Network (DDN) before it transformed into the Non-Secure Internet Protocol Router Network (NIPRNET), the Secret Internet Protocol Router Network (SIPRNET), and the Joint Worldwide Intelligence Communications System (JWICS). The goal of Blacker was communication security (COMSEC) through multilevel cryptography, and system security (COMPUSEC) through provably secure system design. Blacker was also somewhat different structurally, in that unlike the PLI (and perhaps BCR), the Blacker front ends (BFEs) sat between the host and its local packet switch (what would later become the personal computer and the local packet switch).<sup>86</sup> Nonetheless, the narrative that ties together Blacker, IPLI, BCR, and the PLI is that they were all structurally similar in terms of where cryptography was implemented—at the edge.

### Codevelopment and Edge Cryptography

The PLI provided communications security over the Arpanet and a number of Arpanet-like networks implemented by BBN. PLIs worked by traditional encryption, interfacing with a traditional encrypting device. For TCP/IP internetworks, the BCR experiment and the IPLI were developed to work on the DDN. Finally, Blacker, long delayed, replaced the IPLI and implemented strong, traditional, multilevel security on private networks. However, the military

and intelligence lineage that began with the PLI is surprisingly [68] distinct from the trajectory that later emerged in the civilian world with public-key cryptography, which secures the modern Internet.

According to MacKenzie, the advent of computer networking brought new social and technical challenges “as it crossed the divide between COMPUSEC and COMSEC.”<sup>87</sup> MacKenzie believed the NSA Blacker system, developed in the 1980s, “underlined the blurring” caused by the introduction of computer networking.<sup>87</sup> Yet, as we have argued, much of this critical “blurring” work occurred with the development of the PLI, nearly a decade prior to Blacker’s development (which was itself an outcome of the heritage of the PLI). In fact, by the early 1970s, development of computer network security was already emerging in unorthodox institutions, as seen by the PLI’s development inside DARPA, by DARPA contractors (but informed by the NSA), or later the establishment of the National Computer Security Center (responsible for the development of the Orange Book) as a entity distinct from the NSA (which decades later would then be integrated into the NSA). In demonstrating the priority and importance of the relatively forgotten PLI system, we corroborate the lesson that MacKenzie sought to demonstrate—computer network security bridged the fields of computer security and communications security. However, our research downplays the role of the history MacKenzie first researched: the systems, principles, and specifications associated with verifiable and provably secure computing and networking systems.

It is in this context that the secret Blacker project from the 1980s should be placed. By the time the Arpanet switched to TCP/IP (1983) and became the backbone network of the modern Internet, the edge cryptography trajectory was strongly in place. Moreover, by then the public was gaining access to cryptography and deploying it across open networks without reference to its military and intelligence applications, utilizing public-key technologies and infrastructures. Indeed, Whitfield Diffie and Martin Hellman’s “New Directions” paper was published in 1976, the same year that PLIs were implemented on the Arpanet and while BCR research was underway

at BBN.<sup>39</sup> By the early 1980s, RSA Security supplied public-key systems commercially and was the hot startup of its day. In a way, we consider public-key cryptography, as applied to the IP Internet, within the edge or end cryptography trajectory because it too saw modular cryptographic resources added at the end of the network. This is not a belated criticism that the development of online security technologies should have progressed in a different fashion or for different ends. Instead we only note that, following the PLI, both traditional and public-key technologies were developed to function at the network's edge or end, leaving a foundationally unsecure network (and as we noted before, with unencrypted metadata and encrypted payloads).

Just as the IPII BLACKER removed the need for individual keying by creating key distribution centers, with their own security requirements, public-key cryptography removed the necessity for key distribution centers by allowing users to engage in secure communication without exchanging keys in advance. This new infrastructure made sense in an environment where the Internet's core infrastructure, despite its much-touted decentralized nature, was off-limits to anyone outside of trusted defense contractors (and later large governance organizations and private firms). Indeed, save for a massive redesign of the Arpanet or early Internet, the edge was the only place where cryptography could have been added. With its development, public-key cryptography moved the architecture of cryptographic technology even further away from the network, to the hosts and now often to personal devices. This design cemented the network's edge as the place for cryptographic computation and control. These examples bring us to the question we started with: How did cryptography and packet switching influence each other, and to what consequence?

It was this foundation—a fundamentally nonsecure Internet with cryptography added in a modular fashion—that is widely described [69] as originating from a different era in which security was not part of the design. However, as we argued here, security was part of the original design (or at least, was designed early on), and it was design choices made between

networking and cryptographic communities that determined the place of cryptography within the network infrastructure. This was a design decision that created the (technological) infrastructure context in which projects such as Domain Name System Security Extensions (DNSSEC), Internet Protocol Security (IPsec), and the security extension for the Border Gateway Protocol (BGPSEC) would begin to add cryptography to different places across the existing architecture.

One of the consequences of the architectural decision to place cryptography at the edge (and later end) is that it meant security on the Arpanet and the subsequent Internet featured encrypted packet payloads and unencrypted packet metadata, which set the stage for privacy debates. These debates have turned on the ways in which modern cybersecurity architectures permit intelligence agencies easy access to Internet metadata and little (or no) access to the content of communication. We note that surveillance based on findings drawn from metadata analysis is of a particular type, lending itself to particular forms of knowledge.<sup>88</sup> Indeed, as a thought experiment, we can ask ourselves, what would surveillance debates look like if government actors had easy access to message content, but not metadata?

Another consequence of this history is that the location where cryptography and computing resources were added to networks produced issues of ownership and control. For a variety of historical reasons, users often control (portions of) the “end” computers, whereas the private sector and governance institutions control the Internet's router core. “Edge” cryptography, then, is not merely an innocent architectural feature, but it is the result of historical arrangement of actors and institutions, invoking power and control. Although the end-to-end principle and the architecture attributed to it are often described as a feature of the Internet, in the case of cryptography, this principle also speaks to the place where those without institutional power were relegated when they sought to implement civilian security technologies on the Internet. Correspondingly, those seeking power and control of the Internet, in historically unprecedented ways, have estab-

lished the battleground for cybersecurity even beyond the edge, to the end—way up in the stack, beyond networking protocols, on personal devices. Such political decisions for end-to-end encryption across the Internet are pursued in a world only where alternative modes of encryption and security have already been foreclosed. Therefore, although end-to-end encryption is a celebrated feature of the modern Internet, in reality it is pursued by individuals only because more robust (and flexible) arrangements are unavailable.

### Acknowledgments

The authors are listed in alphabetical order and made equal contributions to this article. They wish to thank the three anonymous reviewers for their extremely valuable suggestions and insights. Fidler wishes to thank his interviewees, as well as Dave Walden and Alex McKenzie. All mistakes remain the authors'.

### References and Notes

1. D. Mackenzie and G. Pottinger, "Mathematics, Technology, and Trust: Formal Verification, Computer Security, and the U.S. Military," *IEEE Annals of the History of Computing*, vol. 19, no. 3, 1997, pp. 41–59; doi:10.1109/85.601735.
2. D.A. MacKenzie, *Mechanizing Proof: Computing, Risk, and Trust*, MIT Press, 2001.
3. MacKenzie, *Mechanizing Proof*, p. 190.
4. T. Gillespie, "Engineering a Principle: 'End-to-End' in the Design of the Internet," *Social Studies of Science*, vol. 36, no. 3, 2006, pp. 427–457.
5. C. Timberg, "Quick Fix for an Early Internet Problem Lives on a Quarter-Century Later," *Washington Post*, 31 May 2015, [www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/](http://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/).
6. F.B. Schneider, "Trust in Cyberspace," Nat'l Academy Press, 1999; <http://cryptome.org/jya/tic.htm>.
7. R. Rosenzweig, "Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet," *The American Historical Rev.* vol. 103, no. 5, 1 Dec. 1998, pp. 1530–1552, doi:10.2307/2649970; A.L. Russell, "Histories of Networking vs. the History of

the Internet," *Proc. SIGCIS Workshop, Traditional Papers III: Histories of Network(s)*, 2012, <http://arusell.org/papers/russell-SIGCIS-2012.pdf>; T. Haigh, A.L. Russell, and W. H. Dutton, "Histories of the Internet: Introducing the Special Issue of Information and Culture," SSRN Scholarly Paper, Social Science Research Network, 31 Oct. 2014, <http://papers.ssrn.com/abstract=2517598>; M. Katz-Kimchi, "Singing the Strong Light Works of [American] Engineers: Popular Histories of the Internet as Mythopoetic Literature," *Information and Culture*, vol. 50, no. 2, 2014, pp. 160–180.

8. A pioneering work by Janet Abbate did not initially lead to a rise in computer networking histories focused on institutions and sociotechnical matters, as perhaps she hoped. In the 20 years since, however, a new generation of network historiography, referred to as "histories of networking" by A.L. Russell, was emerging. See J. Abbate, *Inventing the Internet, Inside Technology*, MIT Press, 2000; Russell, "Histories of Networking vs. the History of the Internet."

9. E. Snowden, "Google's Decision to Disable End-to-End Encryption by Default in Its New #Allo Chat App Is Dangerous, and Makes It Unsafe. Avoid It for Now.," 19 May 2016, <https://twitter.com/snowden/status/733253324301053952>.

10. M. Campbell-Kelly, "Data Communications at the National Physical Laboratory (1965–1975)," *Annals of the History of Computing*, vol. 9, no. 3, 1987, pp. 221–427, doi:10.1109/MAHC.1987.10023; A.L. Fletcher, "France Enters the Information Age: A Political History of Minitel," *History and Technology*, vol. 18, no. 2, 2002, pp. 103–119, doi:10.1080/07341510220150315; R. Després, "X.25 Virtual Circuits: Transpac in France: Pre-Internet Data Networking," *Comm. Magazine*, vol. 48, no. 11, 2010, pp. 40–46, doi:10.1109/MCOM.2010.5621965; A.L. Russell and V. Schafer, "In the Shadow of ARPANET and Internet: Louis Pouzin and the Cyclades Network in the 1970s," *Technology and Culture*, vol. 55, no. 4, 2014, pp. 880–907, doi:10.1353/tech.2014.0096; P. Dourish, "Not the Internet, But This Internet:



- How Othernets Illuminate Our Feudal Internet,” Proc. 5th Decennial Aarhus Conf. Critical Alternatives (AA), 2015, pp. 157–168, doi:10.7146/aahcc.v1i1.21200.
11. Abbate, *Inventing the Internet*.
12. B. Fidler and M. Currie, “The Production and Interpretation of ARPANET Maps,” *IEEE Annals of the History of Computing*, vol. 37, no. 1, 2015, pp. 44–55, doi:10.1109/MAHC.2015.16.
13. B. Fidler and A. Acker, “Metadata, Infrastructure, and Computer-Mediated Communication in Historical Perspective,” *J. Assoc. for Information Science and Technology*, Mar. 2016, pp. 44–57, doi:10.1002/asi.23660.
14. B. Fidler and A. Acker, “Metadata and Infrastructure in Internet History: Sockets in the Arpanet Host-Host Protocol,” *Proc. Am. Soc. for Information Science and Technology*, vol. 51, no. 1, 2014, pp. 1–8, doi:10.1002/meet.2014.14505101054.
15. S.J. Jackson et al., “Understanding Infrastructure: History, Heuristics and Cyberinfrastructure Policy,” *First Monday*, vol. 12, no. 6, 2007; <http://firstmonday.org/ojs/index.php/fm/article/view/1904>.
16. A. McKenzie, “INWG and the Conception of the Internet: An Eyewitness Account,” *IEEE Annals of the History of Computing*, vol. 33, no. 1, 2011, pp. 66–71, doi:10.1109/MAHC.2011.9; Russell and Schafer, “In the Shadow of ARPANET and Internet”; J. Day, “The Clamor Outside as the INWG Debated: Economic War Comes to Networking,” *IEEE Annals of the History of Computing*, vol. 38, no. 3, 2016, pp. 58–77, doi:10.1109/MAHC.2015.70.
17. Fidler and Acker, “Metadata, Infrastructure, and Computer-Mediated Communication in Historical Perspective.”
18. P.H. Salus, *Casting the Net: From ARPANET to INTERNET and Beyond*, 1st ed., Addison-Wesley Professional, 1995; M. Hauben and R. Hauben, *Netizens: On the History and Impact of Usenet and the Internet*, 1st ed., IEEE CS Press, 1997; K. Hafner and M. Lyon, *Where Wizards Stay Up Late: The Origins Of The Internet*, Simon and Schuster, 1999; A.L. Norberg, J.E. O’Neill, and K.J. Freedman, *Transforming Computer Technology: Information Processing for the Pentagon, 1962–1986*, Johns Hopkins University Press, 1999.
19. W. Aspray and P.E. Ceruzzi, *The Internet and American Business*, MIT Press, 2008; E. Medina, *Cybernetic Revolutionaries: Technology and Politics in Allende’s Chile*, MIT Press, 2011; Russell and Schafer, “In the Shadow of ARPANET and Internet”; Haigh, Russell, and Dutton, “Histories of the Internet”; J. Rankin, “From the Mainframes to the Masses: A Participatory Computing Movement in Minnesota Education,” *Information & Culture*, vol. 50, no. 2, 2015, pp. 197–216, doi:10.7560/IC50204.
20. D. Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting*, Basic Books, 1976; J.R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society*, Harvard Univ. Press, 1986; J. Gleick, *The Information: A History, a Theory, a Flood*, 1st ed., Pantheon Books, 2011.
21. R. Deibert, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*, expanded ed., Signal, 2013; B. Schneier, *Data and Goliath: The Hidden Battles To Capture Your Data And Control Your World*, W.W. Norton & Company, 2015; P.W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford Univ. Press, 2014.
22. M. DeLanda, “Deleuze, Diagrams, and the Genesis of Form,” *Am. Studies*, vol. 45, no. 1, 2000, pp. 33–42; A.R. Galloway, *Protocol: How Control Exists After Decentralization*, MIT Press, 2004; J. Parikka, *Insect Media: An Archaeology of Animals and Technology*, Univ. of Minnesota Press, 2010; M. Fuller and A. Goffey, *Evil Media*, MIT Press, 2012; L. Manovich, *Software Takes Command, International Texts in Critical Media Aesthetics*, Bloomsbury Academic, 2013; L. Floridi, *The 4th Revolution: How the Infosphere Is Reshaping Human Reality*, 1st ed., Oxford Univ. Press, 2014.
23. C. Shannon, “A Mathematical Theory of Cryptography,” Bell Labs, 1 Sept. 1945; <https://www.iacr.org/museum/shannon/shannon45.pdf>.

24. Shannon's 1945 memorandum was declassified and published in the Bell System Technical Journal in 1949; C. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical J.*, vol. 28, no. 4, 1949, pp. 656–715.
25. F. Ellersick, "A Conversation with Claude Shannon," *IEEE Comm. Magazine*, vol. 22, no. 5, 1984, p. 124.
26. D. Kahn, *The Codebreakers, Abridged*, Sphere Books Limited, 1977.
27. R.V.L. Hartley, "Transmission of Information," *Proc. Int'l Conf. Telegraphy and Telephony*, 1927.
28. F. Ludwig Bauer, *Origins and Foundations of Computing*, Springer, 2010.
29. See W. Diffie and S. Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, updated and expanded ed., MIT Press, 2007, p. 24.
30. J.W. Cortada, "Researching the History of Software from the 1960s," *IEEE Annals of the History of Computing*, vol. 24, no. 1, 2002, pp. 72–79, doi:10.1109/85.988584; Diffie and Landau, *Privacy on the Line*.
31. MacKenzie, *Mechanizing Proof*; S.B. Lipner, "The Birth and Death of the Orange Book," *IEEE Annals of the History of Computing*, vol. 37, no. 2, 2015, pp. 19–31, doi:10.1109/MAHC.2015.27.
32. W.O. Sibert and R.W. Baldwin, "The Multics encipher\_Algorithm," *Cryptologia*, vol. 31, no. 4, 2007, pp. 292–304.
33. J.R. Yost, "The Origin and Early History of the Computer Security Software Products Industry," *IEEE Annals of the History of Computing*, vol. 37, no. 2, 2015, pp. 46–58, doi:10.1109/MAHC.2015.21.
34. MacKenzie, *Mechanizing Proof*; J.R. Yost, "A History of Computer Security Standards," *The History of Information Security: A Comprehensive Handbook*, 1st ed., K.M.M. de Leeuw and J. Bergstra, eds., Elsevier Science, 2007, pp. 595–621; Lipner, "The Birth and Death of the Orange Book."
35. H. Feistel, "Cryptography and Computer Privacy," *Scientific Am.*, 1 May 1973; Diffie and Landau, *Privacy on the Line*, pp. 64–65.
36. Diffie and Landau, *Privacy on the Line*, p. 43.
37. J.H. Ellis, "The Possibility of Secure Non-Secret Digital Encryption," Jan. 1970; J.H. Ellis, "The History of Non-Secret Encryption," *Cryptologia*, vol. 23, no. 3, 1999, pp. 267–273, doi:10.1080/0161-119991887919.
38. S. Levy, *Crypto: Secrecy and Privacy in the New Code War*, Penguin, 2002, p. 20.
39. W. Diffie and M.E. Hellman, "New Directions in Cryptography," *IEEE Trans. Information Theory*, vol. 22, no. 6, 1976, pp. 644–654.
40. W. Diffie, "First Ten Years of Public-Key Cryptography," *Proc. IEEE*, vol. 76, no. 5, 1988, p. 560.
41. Diffie, "First Ten Years of Public-Key Cryptography."
42. Abbate, *Inventing the Internet*, p. 5.
43. There is, however, a small community of historians treating the modern and premodern histories of cryptography. Outside of monographs, the only source for these histories is the journal *Cryptologia*.
44. Kahn, *The Codebreakers*; S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor, 2000; Levy, *Crypto*; F.B. Wrixon, *Codes, Ciphers, Secrets and Cryptic Communication: Making and Breaking Secret Messages from Hieroglyphs to the Internet*, Black Dog & Leventhal Publishers, 2005.
45. P. Pesic, *Labyrinth: A Search for the Hidden Meaning of Science*, MIT Press, 2000; G.F. Strasser, "The Rise of Cryptology in the European Renaissance," *The History of Information Security: A Comprehensive Handbook*, 1st ed., K.M.M. de Leeuw and J. Bergstra, eds., Elsevier Science, 2007, pp. 277–325; K. Ellison, "Millions of Millions of Distinct Orders: Multimodality in Seventeenth-Century Cryptography Manuals," *Book History*, vol. 14, no. 1, 2011, pp. 1–24.
46. MacKenzie, *Mechanizing Proof*, p. 156.
47. MacKenzie, *Mechanizing Proof*, p. 158.
48. MacKenzie, *Mechanizing Proof*; Lipner, "The Birth and Death of the Orange Book."
49. M.K. Smith et al., "A Verified Encrypted Packet Interface," *ACM SIGSOFT Software Eng. Notes*, vol. 6, no. 3, 1981, pp. 13–16, doi:10.1145/1010832.1010838.

50. L. DeNardis, "The Internet Design Tension between Surveillance and Security," *IEEE Annals of the History of Computing*, vol. 37, no. 2, 2015, pp. 72–83, doi:10.1109/MAHC.2015.29; D. Park, "Social Life of PKI: Sociotechnical Development of Korean Public-Key Infrastructure," *IEEE Annals of the History of Computing*, vol. 37, no. 2, 2015, pp. 59–71, doi:10.1109/MAHC.2015.22.
51. Lipner, "The Birth and Death of the Orange Book."
52. M. Warner, "Notes on the Evolution of Computer Security Policy in the US Government, 1965–2003," *IEEE Annals of the History of Computing*, vol. 37, no. 2, 2015, pp. 8–18, doi:10.1109/MAHC.2015.25.
53. R. Slayton, "Measuring Risk: Computer Security Metrics, Automation, and Learning," *IEEE Annals of the History of Computing*, vol. 37, no. 2, 2015, pp. 32–45, doi:10.1109/MAHC.2015.30.
54. We should note that, in this section, portions of our evidence come from a sole source, sometimes based on a single technical report. This is a consequence of two things. First, some of the research and development we address was classified, and as such, there is less documentary evidence than would exist otherwise. Second, this field of research is still in its infancy, and as subsequent investigations occur, we expect more documentary evidence and the production of relevant oral histories.
55. Abbate, *Inventing the Internet*, p. 10.
56. Abbate, *Inventing the Internet*, p. 11.
57. P. Baran, "On Distributed Communications: IX. Security, Secrecy, and Tamper-Free Considerations," Rand, Aug. 1964.
58. Baran, "On Distributed Communications," p. 17.
59. E. Elsam, interview with B. Fidler, 2015.
60. M. Barwolff, *End-To-End Arguments in the Internet: Principles, Practices, and Theory*, Createspace, 2010.
61. J.H. Saltzer, D.P. Reed, and D.D. Clark, "End-to-End Arguments in System Design," *ACM Trans. Computer Systems*, vol. 2, no. 4, 1984, pp. 277–288, doi:10.1145/357401.357402.
62. S. Kent, "Encryption-Based Protection Protocols for Interactive User-Computer Communication," tech. report, MIT, 1976, <http://dl.acm.org/citation.cfm?id=889762>.
63. Saltzer, Reed, and Clark, "End-to-End Arguments in System Design," p. 285.
64. F.L. Maybaum and H.C. Duffield, "Defense Data Network an Overview," *Proc. IEEE Military Comm. Conf.: Communications-Computers: Teamed for the 90s* (MILCOM), vol. 1, 1986, article no. 15, doi:10.1109/MILCOM.1986.4805713.
65. "Interface Message Processors for the ARPA Computer Network: Quarterly Technical Report No. 2," BBN, July 1973.
66. E. Elsam, "COINS II/ARPANET: Private Line Interface (PLI) Operations Manual," BBN, Oct. 1980. The COINS network utilized the Community On-Line Intelligence System for End-Users and Managers (COLISEUM), a front-end system for the network, varyingly described as a production/requirements management system or as a way to track and submit information requests; see M.E. Quinn, "What's a JIC to Do?," final report, Joint Military Operations Dept., Naval War College, 18 May 2004.
67. "Interface Message Processors for the ARPA Computer Network: Quarterly Technical Report No. 5," BBN, Apr. 1974. The Pluribus name appears was chosen as an homage to the Infinibus of the Lockheed SUE minicomputer that was selected for the Pluribus. The SUE was unique in that it contained modest hardware specifications but could be expanded as needed with additional peripherals, even including more central processor boards, all attached to a high speed bus; see Lockheed Electronics Company, "SUE Computer Handbook," July 1973.
68. "Interface Message Processors for the ARPA Computer Network: Quarterly Technical Report No. 12," BBN, Jan. 1972, p. 4.
69. "Interface Message Processors for the ARPA Computer Network: Quarterly Technical Report No. 2," p. 12.
70. "Interface Message Processors for the ARPA Computer Network: Quarterly Technical Report No. 2," p. 10.

71. "Interface Message Processors for The ARPA Computer Network: Quarterly Technical Report No. 5," p. 8.
72. "Interface Message Processors for The ARPA Computer Network: Quarterly Technical Report No. 2," p. 12.
73. "Interface Message Processors for The ARPA Computer Network: Quarterly Technical Report No. 7," BBN, Oct. 1974, p. 24.
74. TEMPEST is the term given to methods of securing electronic equipment from accidental electromagnetic radiation. During the World War II, it was discovered that the Bell 131-B2 telephone "mixer" emitted radiation (detectable on an oscilloscope across the room) each time the encrypting "stepper" advanced. By the 1950s and 1960s, these accidental emissions were operationalized by intelligence-gathering organizations and led to strict requirements designed to frustrate eavesdroppers; see "TEMPEST: A Signal Problem," *Cryptologic Spectrum*, vol. 2, no. 3, Summer 1972.
75. "Interface Message Processors for The ARPA Computer Network: Quarterly Technical Report No. 5."
76. To resolve these issues BBN "met extensively with representatives of NSA and ARPA;" see "Interface Message Processors for The ARPA Computer Network: Quarterly Technical Report No. 5," p. 6.
77. The hardware interface is based on the NSA CSEEB-9B specification, which is also classified; see "Interface Message Processors for The ARPA Computer Network: Quarterly Technical Report No. 7," p. 25.
78. Baran, "On Distributed Communications," p. 14.
79. Elsam, "COINS II/ARPANET," p. 26.
80. "Interface Message Processors for The ARPA Computer Network: Quarterly Technical Report No. 5," p. 7.
81. "Interface Message Processors for The ARPA Computer Network: Quarterly Technical Report No. 7," p. 2.
82. The exceptions to this rule are for priority-traffic information and network problem information, which are unable to pass through the PLI; see "Interface Message Processor: Specifications for the Interconnection of a Host and an IMP," BBN, Jan. 1976, p. H-26.
83. "Defense Computer Resources Technology Plan," June 1979.
84. Elsam, "COINS II/ARPANET."
85. See "Network Encryption: History and Patents," [www.toad.com/gnu/netcrypt.html](http://www.toad.com/gnu/netcrypt.html).
86. C. Weissman, "BLACKER: Security for the DDN Examples of A1 Security Engineering Trades," *Proc. IEEE Computer Society Symp. Research in Security and Privacy*, 1992, pp. 286–292, [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=213253](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=213253).
87. MacKenzie, *Mechanizing Proof*, p. 190.
88. B. Schneier, "Metadata = Surveillance," *IEEE Security & Privacy*, vol. 12, no. 2, 2014, pp. 84–84, doi:10.1109/MSP.2014.28

Preprint self-archived version. [Published version available at IEEE.](#)