The Technologist and Internet Security and Privacy Practices

Greg Adamson

IEEE Society on Social Implications of Technology, Australia
18 Fourth St, Parkdale, Victoria, Australia

Abstract. The Internet's underlying architecture poorly supports many users' current security and privacy needs. This architecture reflects decades-old design decisions by technologists involved in creating the Internet. It can be viewed as an example of the separation between the interests and understanding of technologists and those of the subsequent technology end users. Alternatively, it can be considered the outcome of the needs of a particular set of users, technologists. This view, of the technologist as part of a technology culture among many cultural groupings using the Internet, goes further in explaining the security and privacy characteristics of the Internet today than an alternative critique of technology and usage, that there is an inevitable divide between technologists and non-technologist users.

Keywords: Internet, technology usage, engineering and society.

1 Introduction

Existing limitations in the implementation of security and privacy within the Internet are well documented. This paper examines some of these limitations and the assumptions of technologists who developed this technology. Most examinations of the role of technologists in the development of technology focus on the separation between technology tradition and practice and broader society (a separation variously seen as positive, neutral, or negative). I propose that Internet technologists can be seen as one (or more) particular cultural group. This moves the discussion from a choice between a technical view or a culturally informed view, to one in which technical players can be understood as part of the cultural landscape.

In this research I drew on a historical perspective of the Internet's development. The research examines the changing requirement for security, from the development of packet switching in the US military research environment in the early 1960s to the 1989 design of what would become the World Wide Web in a European science-research environment.

A second basis of this research is the philosophy of technology. I examined Winner's concept of 'autonomous technology'. The concept states that technology itself, rather than societal or usage factors, determine the development of technology.

This research also looked at usage theory, including the technologist as a user. The network technologist as user can be observed at least since the late 19th century. At

N. Aykin (Ed.): Usability and Internationalization, Part II, HCII 2007, LNCS 4560, pp. 295–304, 2007.

that time the number of people employed in the electric, telegraph and telephone industries had grown from a handful to hundreds of thousands in less than two decades. However, rather than seeing themselves as users, technologists have typically presented themselves as problem solvers standing outside the social context, providing the necessary solutions.

This paper examines the period of the Internet's technical development, an unusual period for the technologists involved. Technologists had broad opportunity to influence the Internet's architecture, free from commercial constraints, prior to the Internet's commercialisation around 1995. This makes the Internet atypical of technology uptake, but provides an opportunity to examine the direction in which technologists themselves may take a technology.

In this paper I am not considering the issue of unexpected implications of technology, in order to focus attention on the technologist as user. This is not to suggest that any new technology has exactly and only the effect that its developer or promoter expects. However, for simplicity, issues related to this have been removed from this discussion.

I have not considered whether an alternate set of design decisions, for example the construction of a secure network such as proposed by Baran [1], would have affected the Internet's subsequent success (for example due to increased cost or limits on accessibility). This research has been limited to the field of Internet technology. While important, the development path, structures and current state of Internet technology are not typical of technology in general. Further investigation could examine whether the 'technologist as user' has influenced the development of other technology fields.

2 How the Internet Got Its Security and Privacy Characteristics

The Internet has significant limitations in providing security and privacy. By default, the Internet's set of technical rules, or 'protocols', takes no responsibility for these. Specifically the Internet provides very little inherent support for the three requirements of secure and private communication: confidentiality, integrity and authentication.

- Confidentiality involves keeping information hidden from parties other than the intended recipient. As the Internet transmits clear (unencoded) text, confidentiality is not provided by default.
- Integrity of a message is whether it has been deliberately or accidentally altered. Has the figure or name on an order or cheque been changed? Have words been added to or deleted from a document? The Internet technology is based on 'packet switching', breaking messages into small discrete packets that are then sent across the network. Packets traversing the Internet infrastructure, which is owned by thousands of separate companies and organisations, will travel by an unspecified path that could include almost any country in the world, even when communicating between two users in the same city. By default all data is sent in a form that can be read and modified.
- Authentication is ensuring that each party in an exchange of information is who they claim to be. The Internet by design is an anonymous network. The Internet's

protocol suite TCP/IP provides no mechanism to certify parties to a communication. Co-inventor Cerf [2] identifies this as one of the key weaknesses of the protocol.

This lack of inbuilt security and support for privacy may appear surprising, given the origin of the Internet's technology in the US military environment. Its absence reflects the 'accidental' origins of the Internet. In his seminal work on packet switching Baran [1] included a chapter on security. This involved a complex two-level security approach built into the network providing encryption both between network devices and end-to-end across the network:

> One key difference between a civilian and a military communications system is the provision made in the latter for the preservation of secrecy and for immunity from destructive tampering. These considerations are most effectively integrated into a network as an integral part of the switching mechanism, rather than in the form of 'black boxes' tacked on as an afterthought... It is acknowledged that the approach represents a departure from conventional practices, which have traditionally maintained a separation between the design of the communications network itself (which is most often a slight modification of a system originally designed for civilian use) and the design and implication of cryptographic safeguards. (section IX, p. v)

Baran's comments on integrating security into initial design, rather than adding it on later, are now accepted standard practice within the IT security field. Baran's proposed network was never build. However, his work came to the attention of the US Department of Defence group working on Arpanet, which would later become the core of the Internet. Project manager Larry Roberts described his response on reading Baran's work: 'Suddenly I learned how to route packets' [3]. (p. 37) While the first network devices were steel-encased military-grade computers, and funded by the Department of Defence, Baran's security approach was not included. Two histories of the Internet [4, 5] make no reference to security considerations in describing the development of Arpanet ('security' does not even appear in their index). The first Internet standard to mention security problems is dated December 1973 [6]. Eighteen years later, a further standard echoes the same security concerns [7]:

> Because the Internet itself is neither centrally managed nor operated, responsibility for security rests with the owners and operators of the subscriber components of the Internet. Moreover, even if there were a central authority for this infrastructure, security necessarily is the responsibility of the owners and operators of the systems which are the primary data and processing resources of the Internet. There are tradeoffs between stringent security measures at a site and ease of use of systems (e.g., stringent security measures may complicate user access to the Internet).

The Internet developed in the 1970s and the 1980s. For much of this period technologists were the primary end users, as well as the Internet's developers. Technologists found that the services which the Internet provided, primarily e-mail and file transfer, were useful and valuable. In the absence of more pressing military applications, this provided technologists with the opportunity to develop a network to do what they wanted and needed. Technologists developed a technology that was well designed for their user needs.

By the early 1990s the Internet had grown into a widely dispersed network used by millions of people. The rapid uptake of the World Wide Web from 1993 created the Internet that users recognise today. This was based on work at the CERN European physics research centre. In his original proposal for what became the Web, Berners-Lee [8] addressed the issue of security as follows:

> Non requirements: Discussions on Hypertext have sometimes tackled the problem of copyright enforcement and data security. These are of secondary importance at CERN, where information exchange is still more important than secrecy. Authorisation and accounting systems for hypertext could conceivably be designed which are very sophisticated, but they are not proposed here. In cases where reference must be made to data which is in fact protected, existing file protection systems should be sufficient. (p. 12)

3 The Internet and Technology Tradition

These brief historical points on the origin of the approach to security during the Internet's development emphasise the central role of the technologists who developed the Internet's standards. There is a large body of literature examining the role of technologists in such decision making. Winner [9] summarises this debate including the work of Galbraith [10] on technocracy. At times the influence of technologists on decision making reaches into the political field. Winner quotes US President Dwight D. Eisenhower, who identified a 'danger that public policy could itself become the captive of a scientific technological elite.' (p. 148)

While the literature on technocracy points to controlling and centralising tendencies, the Internet's development history has been very different from that of other major technologies [11]. The single over-riding design requirement for Baran [1] in inventing packet switching was to build a network capable of continuing to wage war after a nuclear bombardment of the United States. He begins his introduction: 'Let us consider the synthesis of a communication network which will allow several hundred major communications stations to talk with one another after an enemy attack.' (section I, p. 1) This was achieved using packet-switching over a distributed network, in contrast to the centralised structure of the US telephone system of the 1960s. This explains the apparent contradiction of a hierarchical US military environment producing a distributed and difficult to control Internet technology.

The culture of the Internet was similarly non-hierarchical, as shown by its standards development process. The Request For Comment (RFC) standards are semi-formal documents available without charge and freely contributed by a community of thousands of technologists. This was possible because until the mid-1990s, from an infrastructure or business point of view, the Internet just wasn't very important. Handley [12] describes the last major change to the Internet's architecture in the 1980s:

> No-one likes changing such a key part of an operational network – such changes are driven by necessity. However, as the Internet was not a key

> infrastructure in the 1980s, the pain caused during transitions was comparatively low. Besides, many people regarded the Internet as an interim solution that would eventually be replaced by the [International Organisation for Standards'] OSI protocols, and therefore, with the glare of political attention diverted elsewhere, the engineers of the Internet were allowed to do good engineering. They learned from their mistakes by trying things out for real and fixed problems as they became pressing. (p. 120)

Despite its 'humble' origins, by the turn of the century the Internet had become critical infrastructure for the global economy. While the relative importance of large centralised information technology systems such as the mainframe, and the predominant mainframe communication protocol, a hierarchical technology from IBM called SNA, were in decline, the importance of the technologist was not diminishing. The introduction of CIOs (Chief Information Officers) to leading roles in corporations during the 1990s showed this strong and continuing importance of the technologist.

The rapid and unexpected growth of the Internet from 1995 created a demand for experts who 'understood' the Internet. While a new communications medium had been anticipated for the previous decade, and promised as an 'information superhighway', the actual Internet was far less predictable or controllable than previous technologies such as television or the telephone. In this sense the technology was 'out of control'. While the traditional technocrat was seen to have power through holding arcane technical knowledge, the Internet-era technologist in addition is expected to anticipate the direction and impact of complex technology. Stefik [13] provides a technologist's perspective on understanding the Internet. He presents four metaphors for what the Internet does, based on personality characteristics: the keeper of knowledge or conservator, the communicator, the trader, and the adventurer. He presents these four views as collectively exhaustive, missing the technologist (creator, planner of the Internet), and thereby providing no reflective examination of the Internet itself. This validates Winner [9], 'Technological society ... has never shown any great commitment to self-reflection, self-criticism, or the study of its own history.' (p. 128) In this view, the technologist sits above or outside of the world of problems to be solved. If technology is out of control (in either a negative or positive sense), who better than a technologist to intercede on an organisation's behalf?

Despite technologists' ability to do things with technology, and the clear role provided by technologists in the design of the Internet, there is no evidence that technologists in general have a greater ability to predict or control the direction and effect of technology than other professional groups. Technologists may be less prepared for unexpected results of technology. For example, uncritical enthusiasm for technology's promise can be found among technologists working for technology vendors. The experience of technology-led network vendor Cisco after the 2000 dot.com financial crash shows this. In 2000, one description of Cisco's production process [14] glowingly describes Cisco's inventory system:

> Because real-time information on sales requests and inventory levels is constantly online and available to Cisco and its manufacturers, Cisco can maintain lower inventory levels without increasing the risk of part shortages. Direct delivery from the factory cuts lead times at least in half—from four or

> five weeks to two. As a result of the inventory online connection, Cisco has reduced its own inventory by 45 percent, saving $5.6 million. (p. 150)

Cisco shareholders were surprised in early 2001 when Cisco wrote off $US2.5 billion of $US4.1 billion inventories on its books. Looking back on this period some years later:

> CIO Brad Boston found that Cisco had nine order status tools. Each of them used data from different sources, which used different definitions for key terms. As a result, the systems couldn't give the company a clear picture of its orders. There were similar problems in the sales organization' [15]. (p. 146)

In retrospect the issue becomes clear, while at the time confidence in the technology left no room for doubt.

4 A Technologist Culture

The self-confidence of the technological profession is examined by Winner [9] in terms that go beyond the technical, to the basis of technology knowledge:

> A typical response of engineers ... is to announce that they are merely problem solvers. 'Tell us the problem,' they demand. 'We will find a solution. That's our job. But you may not presume to question the nature of our solution. You are not a member of a technical profession and, therefore, know nothing of relevance. If you insist on raising questions about the appropriateness of the means we devise, we can only conclude that you are antitechnology.' ... It soon becomes clear that in this enlightened age there is almost no middle ground of rational discourse, no available common language with which persons of differing backgrounds can discuss matters of technology in thoughtful, critical terms... Indeed, anyone seriously critical of conditions in the technological society soon meets up with the demand from technically trained persons that in order to speak at all, one must first 'learn technology.' A version of the mode of legitimisation through expert knowledge, this advice is, in my experience, usually less a plea for understanding than an urging to compliance. (p. 11)

Marvin [16] describes the creation of the electrical engineering profession within the United States. Electrical engineering first emerged as a profession in the 1870s. The American Institute for Electrical Engineers (AIEE) was founded in 1884. *Electrical World* estimated in 1890 that at the time 250,000 people depended on the electrical industry (including telegraph and telephone) for their livelihood. While investment in electrical technology created the engineering workforce, the creation of an engineering profession was not an inevitable consequence. Marvin describes this as a process of 'inventing the expert', and summarises the experts' goals as:

> …to harness public adulation to improve their own social and professional standing while keeping public admirers at arm's length... The proper naming of persons, gadgets, and concepts in their electrical contexts and relations

> was among the most important performative indicators of technological literacy. (pp. 15-16)

In recent decades there has been evidence of a more reflective attitude among technologists, partly responding to commentary from professionals outside the technology field. Schneier, author of *Applied Cryptography*, a seminal work on information technology security [17], for example reflectively examines the issue of technology security practices:

> A colleague once told me that the world was full of bad security systems designed by people who read *Applied Cryptography*. Since writing the book, I have made a living as a cryptography consultant: designing and analyzing security systems. To my initial surprise, I found that the weak points had nothing to do with the mathematics. They were in the hardware, the software, the networks, and the people. Beautiful pieces of mathematics were made irrelevant through bad programming, a lousy operating system, or someone's bad password choice [18] (p. xi).

Schneier summarises this: 'If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.' (p. 385)

The discussion of whether there is a technological or other basis for discussion of technology approaches goes beyond the field of technology. I suggest that we can think of technologists as one or more groups, with their own culture. The discussion of technologist as expert then becomes a discussion of the way in which various cultures approach technology, with the technologist's culture as one or more particular instance. (On cursory examination the approach of technologists across different countries and the existence of technical standards established by international organisations such as the International Telecommunication Union and International Organisation for Standards suggest a shared global technologists' culture.)

The tradition of technology described by Winner above has both strengths and weaknesses. A strength is that a great deal of valuable technology has been introduced into the world. A weakness is that technologists often believe that technologically satisfactory solutions are generally satisfactory for users. A recent and widely discussed debate between technologists and a non-technologist (business) audience occurred following the publication in *Harvard Business Review* of an article, 'IT doesn't matter' [19]. This took up the well established business concept of 'competitive advantage', a term coined and defined by Michael Porter [20]. Competitive advantage describes a situation in which a company has some ongoing advantage in relation to its rivals. For example, this could be lower cost production techniques, favored access to raw materials or markets, a more desirable product, key patents, or turnover of skilled staff at a rate substantially lower than an industry average. It doesn't mean high productivity, advanced technology or fast time to market if all its competitors also have these or can quickly get them. Competitive advantage is easy for a company to understand, but is outside the realm of practical experience for a technologist, who will generally promote the wide uptake of technology.

Carr suggested that information technology has become a commodity item, and does not provide competitive advantage in itself. In the following press debate, Carr [21] examines the technologist's view, provided by *Fortune* technology writer David Kirkpatrick.

> The most telling quote comes from the CEO of a software company that, Kirkpatrick tells us, 'builds sophisticated software for collaboration.' Says this CEO: 'We just closed several deals with leading Fortune 100 companies using our software to differentiate their ability to get vast international sales and marketing ecosystems working together to respond faster and more correctly to customers. "This is not a 'me too!"' But if he's already sold the same system to 'several' Fortune 100 companies, one has to wonder how differentiating the technology really is. It's difficult to purchase competitive advantage from an outside supplier who's peddling the same 'advantage' to your peers.

While it is easy to point to areas where technologists have a narrow technically defined view of a problem, there are many examples of technologists showing an awareness of the limitations of this approach. The Institute of Electrical and Electronic Engineers (IEEE) is a mainstay of the global technology community. Writing in the journal *IEEE Internet Computing*, Gong and Sandhu [22] describe a significant difficulty with security resulting from a disconnection between technology potential and uptake:

> The focus on deployment reflects the frustration, shared by the majority of the computer security research community, over the glaring gap between state-of-the-art security research and state-of-the-art security practice. Although a tremendous amount of new research is published each year ... the commercial adoption rate of this research is miserably low compared with adoption rates for other technologies, such as high-speed networking. In fact, you can count on one hand the number of innovative and effective security technologies that have been widely deployed in the past three decades... Why such a gap exists is a mystery, and to attempt an analysis is beyond the scope of this article. Our emphasis on deployment for this special issue is a small effort toward narrowing this gap. In the end, we failed to attract articles that explain why certain security technologies are adopted while others are not—Any historians out there reading this? (pp. 38-39)

The Xerox PARC laboratory in the US has a reputation for taking a non-technical view of technology challenges. Brown [23] describes his experience there:

> …innovation is not about technology alone but also about the work practices in which technologies are used. In fact, we have anthropologists, psychologists, and sociologists on our research staff to help us find better techniques for linking to the world, listening in different ways for latent needs and tacit knowledge, and learning from actual work practices... Instead of merely hurling inventions over the transom into the hands of business developers, technologists share in the responsibility for making inventions into innovations. (pp. xii-xiv)

Brown calls this alternative approach among technologists ‘seeing differently’. This complements the self-awareness of security researchers mentioned above. Such an approach increases the relevance of developed technology by linking technologists to the broader society for which they are developing and implementing technology.

5 Conclusion

This research has described the role of a technological perspective in the state of security and privacy functionality within the architecture of the Internet. The technological perspective has established a global data network which despite being used by hundreds of millions of people poorly supports security and privacy in its fundamental design. This could be cited as an example of the limitation of having a technological focus during technology design. I am proposing a different approach. This is to consider the Internet’s architecture as representing the intentions of technologists in the 1970s and 1980s designing a network for the technologist user. Once incorporated into the Internet’s architecture in the 1970s and 1980, these characteristics have been difficult to change.

In this view, technologists represent one or more groups of technology users with their own particular culture. From this perspective technologists can be considered as one voice among many in decision-making with regard to technology, rather than as the exclusive holders (or withholders) of expertise necessary to understand and manage technology.

References

1. Baran, P.: On Distributed Communications. In: United States Air Force Project RAND, RAND Corporation, viewed 25 January 2007 (1964), http://www.rand.org/about/history/-baran.list.html
2. Cerf, V.: Vint Cerf Talks About Internet, Slashdot, viewed 17 October 2002 (2002), http://interviews.slashdot.org/
3. Abbate, J.: Inventing the Internet. MIT Press, Cambridge, MA (1999)
4. Hafner, K., Lyon, M.: Where Wizards Stay Up Late: The Origins of the Internet, Touchstone, New York (1998)
5. Naughton, J A: Brief History of the Future: The Origins of the Internet, Phoenix, London (2000)
6. Metcalfe, R.M.: The Stockings Were Hung By the Chimney with Care, RFC 602, viewed 1 February 2007 (1973), ftp://ftp.rfc-editor.org/in-notes/rfc602.txt
7. Pethia, R., Crocker, S., Fraser, B.: Guidelines for the Secure Operation of the Internet, RFC 1281, viewed 1 February 2007 (1991), ftp://ftp.rfc-editor.org/in-notes/rfc1281.txt
8. Berners-Lee, T.: Information Management: A Proposal, internal CERN document, viewed 21 August 2006 (1989), http://www.w3.org/History/1989/proposal.html
9. Galbraith, J.K.: The New Industrial State, New American Library, New York (1968)
10. Winner, L.: Autonomous Technology: Technics-Out-of-Control as a Theme in Political Thought. MIT Press, Cambridge, MA (1978)
11. Adamson, G.: The Mixed Experience of Achieving Business Benefit from the Internet: A Multi-disciplinary Study, RMIT University, Melbourne, Viewed 31 July 2006 (2004), http://adt.lib.rmit.edu.au/adt/public/adt-VIT20041105.112155

12. Handley, M.: Why the Internet Only Just Works. BT Technology Journal 24(3), 119–129 (2006)
13. Stefik, M.: Internet Dreams: Archetypes, Myths, and Metaphors. MIT Press, Cambridge, MA (1996)
14. Bunnell, D., Brate, A.: Making the Cisco Connection: The Story Behind the Real Internet Superpower. John Wiley & Sons, New York (2000)
15. McAfee, A.: Mastering the Three Worlds of Information Technology, Harvard Business Review, pp. 141–149 (November 2006)
16. Marvin, C.: When Old Technologies Were New: Thinking About Electric Communication in the Late Nineteenth Century. Oxford University Press, New York (1988)
17. Schneier, B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd edn. John Wiley & Sons, New York (1996)
18. Schneier, B.: Secrets and Lies: Digital Security in a Networked World. Wiley Computer Publishing, New York (2000)
19. Carr, N.G.: IT Doesn't Matter. Harvard Business Review 81(5), 41–49 (2003)
20. Porter, M.E.: Competitive Advantage: Creating and Sustaining Superior Performance. Free Press, New York (1985)
21. Carr, N.I.: Doesn't Matter: Responses, viewed 16 February 2007 (2003), http://www.nicholasgcarr.com/articles/matter.html
22. Gong, L., Sandhu, R.: What Makes Security Technologies Relevant? IEEE Internet Computing 4(6), 38–41 (2000)
23. Brown, J.S.: Seeing Differently: Insights on Innovation, Harvard Business School Press, Boston (1997)