Understanding history

David Clark

MT CSAIL

January 2023

An important vision:

- J.C.R. Licklider with Robert Taylor--“The Computer as a Communication Device”, 1968
  - (Larry Roberts says that in 1962 Lick wrote an internal memo called “Galactic Networks”.)

Lick and Taylor I

- What will go on inside? Eventually, every informational transaction of sufficient consequence to warrant the cost. Each secretary's typewriter, each data-gathering instrument, conceivably each dictation microphone, will feed into the network.
- You will not send a letter or a telegram; you will simply identify the people whose files should be linked to yours and the parts to which they should be linked-and perhaps specify a coefficient of urgency. You will seldom make a telephone call; you will ask the network to link your consoles together.
- You will seldom make a purely business trip, because linking consoles will be so much more efficient. When you do visit another person with the object of intellectual communication, you and he will sit at a two-place console and interact as much through it as face to face.

Lick and Taylor II

- Available within the network will be functions and services to which you subscribe on a regular basis and others that you call for when you need them. In the former group will be investment guidance, tax counseling, selective dissemination of information in your field of specialization, announcement of cultural, sport, and entertainment events that fit your interests, etc. In the latter group will be dictionaries, encyclopedias, indexes, catalogues, editing programs, teaching programs, testing programs, programming systems, data bases, and—most important—communication, display, and modeling programs.

Lick and Taylor III

- “When people do their informational work “at the console” and “through the network,” telecommunication will be as natural an extension of individual work as face-to-face communication is now. The impact of that fact, and of the marked facilitation of the communicative process, will be very great—both on the individual and on society.

Lick and Taylor IV

- First, life will be happier for the on-line individual because the people with whom one interacts most strongly will be selected more by commonality of interests and goals than by accidents of proximity. Second, communication will be more effective and productive, and therefore more enjoyable. Third, much communication and interaction will be with programs and programmed models, which will be (a) highly responsive, (b) supplementary to one's own capabilities, rather than competitive, and (c) capable of representing progressively more complex ideas without necessarily displaying all the levels of their structure at the same time-and which will therefore be both challenging and rewarding. And, fourth, there will be plenty of opportunity for everyone (who can afford a console) to find his calling, for the whole world of information, with all its fields and disciplines, will be open to him—with programs ready to guide him or to help him explore.

Lick and Taylor V

- For the society, the impact will be good or bad, depending mainly on the question: Will “to be on line” be a privilege or a right? If only a favored segment of the population gets a chance to enjoy the advantage of “intelligence amplification,” the network may exaggerate the discontinuity in the spectrum of intellectual opportunity.
- On the other hand, if the network idea should prove to do for education what a few have envisioned in hope, if not in concrete detailed plan, and if all minds should prove to be responsive, surely the boon to humankind would be beyond measure.
- Unemployment would disappear from the face of the earth forever, for consider the magnitude of the task of adapting the network’s software to all the new generations of computer, coming closer and closer upon the heels of their predecessors until the entire population of the world is caught up in an infinite crescendo of on-line interactive debugging.”

Which inspired:

- The ARPAnet
- The Packet Radio Network
- The trans-Atlantic satellite network

- And the Internet, to hook them all together.
  - Original goal: resource sharing.
    - ARPA initially tried to suppress email as an unjustified use of resources.

Next topic: early thinking about Internet security

- There is this idea that the Internet was designed by a bunch of academics that did not care about security.
  - This idea is total nonsense.
- From the beginning, ARPA (a part of the DoD) understood that their goal for the Internet was to coordinate tactical warfighting, and the networked machines would be attacked by hostile state actors.
- What the DoD and NSA understood was multi-level secure time-sharing. The implications of networking were totally unclear.
- The trajectory of thinking about security was shaped by the following assumptions and uncertainties.

Assumptions

- To build a secure system the developers must have security clearances.
- The civilian Internet need not and should not be secure. Only a military variant needs to be secure.
- The threat to the military was theft of classified information.
- Computing was on multi-level secure time-sharing systems.
- The military did not do COTS networking.
- In 20 years or so, malware would be an issue.
- Encryption:
  - Had to be done in hardware at the time.
    - Very tricky to build.
  - All schemes of any rigor were classified.
  - Was protected from export as a munition (ITAR).

Uncertainties

- In detail, what is the threat model?
  - What are the capabilities of the adversary.
  - If the goal if prevention of de-classification, the solution must be perfect.
- What is the correct modularity of a potential “solution” to security.
  - Network vs. host, for example.
    - The moment of the Morris worm.
  - Complicated by limits on encryption technology.
- How are remote credentials verified?

So what happened?

- The team with clearances floundered.
  - My oddest ever consulting gig.
- The challenge of hardware encryption was a serious challenge.
  - Packets confounded them.
- DOD attempt to build their own hardware failed.
  - They ended up falling back on COTS tech, and dealing with its insecurity.
- NSA fought the civilian use of encryption until at least 2000.
  - National Research Council. 1996. *Cryptography's Role in Securing the Information Society*. Washington, DC: The National Academies Press. https://doi.org/10.17226/5131.
  - 1999, RFC 2725 still questions legality of software with encryption.
- The legacy of “net vs. host” continues. We have now looped back to zero trust, which is where NSA started.
  - But quickly then moved to perimeter model. NSA relies on trust as well as technology.

Thinking about security

- The focus (then, as now) was on the security of the end-node.
  - The DoD focused on multi-level secure time sharing systems.
  - The ”Orange Book”, Bell-LaPadula model, *-property
- DoD failed to understand that commercial world cared about integrity.
  - Clark-Wilson paper 1987…
- We understood the risk of a mis-behaving router. In 1982, Rosen [41] first documented this vulnerability in RFC 827, in the context of a predecessor of BGP called the Exterior Gateway Protocol (EGP):
  - *If any gateway sends an NR [neighbor reachability] message with false information, claiming to be an appropriate first hop to a network which it in fact cannot even reach, traffic destined to that network may never be delivered. Implementers must bear this in mind.*
- An important (and perhaps first) effort to understand securing a routing protocol: Radia Perlman, PhD, 1988, “Network Layer Protocols with Byzantine Robustness”.
  - Basic idea: Every routing has public-private key, signs announcements, routers have per-key round-robin queues so all sources get share of capacity.

What did we not initially understand

- The implications of personal computers and local area networks.
- How to deal with networks that were malicious.
  - See Radia's thesis.
  - Note: BGP starts in 1989, 10 years before encryption is a practical option.
- Asymmetric encryption.
  - NSA knew all about it, was just hoping no one without a clearance figured it out.
- The reality of key management.

Availability was and is central

- See my “Design principles” paper.
- An enduring tension:
  - We teach that availability is a part of security.
  - But security keeps (hopefully only bad) things from happening.
  - Lack of attention to availability as a part of security makes availability seem like the enemy of security.