The Net's Good Ol' Boys: Hacking the Arpanet

by Geoff Dutton via claire - Counterpunch *Thursday, Jan 4 2018, 5:17am*
international / prose / post

Part I.

> It's hard to imagine now, but there was a time before the Internet, a time when computers took up more space than the acolytes who tended to their needs. In the 70s I was one such boffin, a postgrad hacking away in a university R&D lab. Computers then were still quite dear, and so we made do with terminals that sucked electrons from the teat of a minicomputer several blocks away through fiber cable.

Our digital host had recently been hooked up to the Arpanet, the Internet's predecessor, giving us real-time access to several dozen academic, government, and military computers scattered across the US. We used it to chat and exchange files and email with people we knew here and there, but mostly we wasted time and bandwidth psyching out the robot psychotherapist Eliza and playing text-based games like Adventure and Hunt the Wumpus, just like today's youth do but more primitively.

DoD's Advanced Research Project Agency (ARPA) had funded the network to develop a prototype military communications system. They let scientists play with it and observed what they were up to—how carefully, nobody without an appropriate security clearance can really say. For we geeks, it was a cozy play-space with a few thousand presumably collegial users. No spam, no malware, no ads, no Web, and so it would remain for another dozen years. But it did not remain free of intruders for long.

Soon it became evident that strangers were snooping around the Net—mystery hackers who, after a guy who called himself the Lone Ranger befriended and ratted them out to the FBI, turned out to be a bunch of teenagers. An odd collection of middle- and high school misfits who traded exploits on dial-up hosts, hacking long-distance calls to get to Arpanet portals with purloined credentials they passed around. An Atari 400 or a Radio Shack TRS80 and a modem was all the hardware needed for a kiddie to sneak in, swipe logins (most people used default passwords or none at all), read files and emails, and for a lark change file and account names and passwords to whatever they felt like. Few of these kids ever met face-to-face. They bonded through online bulletin boards—the social media of the day—hidden behind screen names. At a tender age, these kids instinctively knew that real business gets transacted under the radar.

It was innocent fun for the "whiz kids," as they were then labeled. Had ransomware been in circulation then, they wouldn't have used it; they were explorers, not thieves. Their only ill-gotten gains were slices of computer time and free phreaked phone calls. Things are different now that everyone and everything is online. Empires are at stake, or so key players believe, and that makes it so. After all, did not the military create the Internet in service to empire?

Today as perhaps then the underlying task of the Internet is surveillance, but nobody who does it admits to it or that maximizing ad revenues is the main concern of corporate news media is. And now that Net Neutrality is a lost cause, muffling anti-establishment messages, enforcing ignorance and shaping opinions will become much easier to them to do. They just want us to have such a good time indulging in online pastimes that we stop caring who's filtering facts and following our mousetracks.

By the 80s, some of us saw this coming. Not so much all the mining, trading, and manipulating of personal data, but what seemed like a dash to create Big Brother, antennae on down. In this century, every netizen is quickly becoming inured not just to the personal data complex sorting through our lives, preferences, and opinions, but to being tracked wherever we may go. As Max Barry writes in Lexicon,

"*...I don't care that much if these organizations want to know where I go and what I buy. But what bothers me is how HARD they're working for all that data, how much money they're spending, and how they never admit that's what they want. It means that information must really be valuable for some reason, and I just wonder to who and why.*"

I hardly recall the cyber-experts asking that. Seldom did Computer Science literature from that formative era broach network technology's totalitarian potential. The high priests endlessly discuss computer system vulnerabilities and how to prevent them, but mostly focus on fending off intrusions from hackers and criminals, not spooks, the military, or law enforcement. Even the acolytes who knew why the DoD was building the Arpanet did not seem particularly interested in discussing any undesirable consequences. As Matt Novak remarks in an article about Arpanet in PaleoFuture:

"*When you look at how the early internet was used by the intelligence and defense communities, you see that our internet infrastructure was never the Wild West. It was built deliberately and strategically. Some of the earliest uses of the ARPANET were for monitoring the military activities of America's adversaries, decades before most people even knew what networked computing was.*"

Novak compiled an animation that visualizes the Arpanet extending its tentacles over its 20 years of existence. Halfway through, by 1980, the Arpanet had proven itself. By then it was already clogged with civilian email messages, something DoD disapproved of. Understanding that Arpanet was inherently insecure, the Pentagon established its own communications network (MILNET), as did the NSA with its COINS II network (Community On-line Information System), built to internally share intelligence data away from prying eyes. As these networks were based on and had gateways to the Arpanet, they were similarly open to compromise.

The Internet wasn't designed to be secure; quite the opposite, it is rife with holes in its backdoor code and protocols deliberately put there for reasons that might or might not have to do with government surveillance. A frequent and well-informed commenter on Bruce Schneier's security blog notes (12/16/2017):

"*... most Internet vulnerabilities at the protocol and standards layers have been there since day one. Because they were quite deliberately built in from day zero.*

It was almost certainly not done maliciously but to "solve problems within resource constraints" that no longer apply.

The thing is nobody wants to spend money to solve these problems, usually portrayed with the excuse of "don't break legacy systems" as it's the almost perfect "get out clause". As well as the biggest soirce [sic] of not just technical debt but building in security vulnerabilities across the board."

The Arpanet was hacked not long after it came out. See this timeline to read up on the highlights. Some of its vulnerabilities stem from its architects' inability to credit malicious actors the cleverness to find their way in. Others developed over time as engineers applied patch upon patch, desperately trying to keep up with the Internet's burgeoning size and traffic levels of online transactions, big

data, and multimedia. In essence no roadmap, no anticipation of criminal use or how to thwart it, compounded by a general reluctance on the part of IT vendors, their customers, and government agencies to assume the cost and complexities securing of their systems.

Of course, spy agencies are happy to exploit the security holes and seem to snoop everywhere they care to. The question here is, did the architects of Arpanet deliberately laden their standards, protocols, software, and machinery with features that would allow the government to intercept traffic and penetrate computers on the Net and disregard security flaws when brought to their attention?

That's quite possible. After the NSA seeded doubt in 2012, companies around the world refused to purchase network routers from Chinese maker Huawei, concerned that they concealed "back doors" in their code that would let a knowledgeable hacker log on to intercept or interject network packets. This after Der Spiegel broke news that NSA had infiltrated Huawei's IT system to retrieve source code for their products, as well as "a list of 1,400 customers as well as internal documents providing training to engineers on the use of Huawei products, among other things."

There's no direct evidence that NSA slipped spyware into Huawei equipment, but in 2014 the Intercept revealed NSA documents indicating that NSA was "interdicting" shipments of US-made networking equipment destined overseas to inject its own code before buyers took delivery. A network router or a switch may have 30M lines of code, not easy for a customer to verify that it's spook-free. And should NSA's bugs be discovered, the manufacturer's reputation and stock price will certainly take hits.

We can only speculate whether there are similar trapdoors in routers sold in the US market, but it almost doesn't matter. NSA has many other ways to sniff out your packets to archive your messages for future reference, along with data on your computer's Internet traffic generously supplied by your ISP. And for that robust surveillance capability, give thanks to Bobby Inman and the unsung architects of the Arpanet who paved the way.

Further reading:

Wired Magazine 5/9/06: Ex-NSA Chief Assails Bush Taps

DefenseTech News 5/9/06: Ex-NSA Chief Blasts Taps, Calls for CIA Breakup

Max Barry, Lexicon, Penguin Books, 2013

Der Spiegel 3/22/14: NSA Spied on Chinese Government and Networking Firm

CNET News 5/12/14: NSA reportedly installing spyware on US-made hardware

Washington Post 5/30/15: Net of Insecurity: A Flaw in the Design

Washington Post 6/22/15: Net of Insecurity: A disaster foretold — and ignored

Gizmodo 2/20/15: A History of Internet Spying, Part 2

Gizmodo 8/15/15: The Secret Project to Turn the Internet into an Anti-Soviet Spy Network

PC World 11/17/15: How Cisco is trying to keep NSA spies out of its gear

Read Part II here.

https://www.counterpunch.org/2018/01/04/the-nets-good-old-boys-hacking-the-arpanet/
