Experiences from the dawn of the Internet





SATELLITE CONNECTIONS)

The state of things in 1976

- it was before cell phones
- it was the "mainframe era"





- some hobbyists had IMSAI or Altair micro-computers.





- TCP still being developed and tested
- Unix version 6 (before BSD and any other variants)
- No domain names or DNS
- No email

•

• No ethernet

The state of things in 1976

- Frustration with the "mainframe priesthood"
 users wanted more control and access
- 1975 "Computer Lib" and "Dream Machines" published
 - envisioned things like "Hypertext"





The state of things in 1976 ARPANET

- Protocol: NCP (Network Control Program)
 - 8 bit addresses
 - 2 bits for host part, 6 bits for IMP number
 - in that era, computers were expensive mainframes and nobody could envision a site with more than 4 computers.
- My IMP was node #3
 - addresses separation used a "/"
 - our address was 0/3, which could be shortened to just "3".
 - Later, our IP address became 10.0.0.3. (Class A no CIDR)
- One used the "BBN 1822 protocol" to connect a host to an IMP.
 - interfaces types were "LH", "DH", or "VDH"
- Circuits between IMPs were 50 Kb/s wideband analog modems
 - very large: you could fit 2 of them in a rack



The front panel from IMP #3 BBN Model C/30

San Diego, 2012

Boot from cassette tape



Connecting your terminal

- Terminal IMP (TIP) serial connection to IMP for terminals (teletype)
- 110 or 300 baud modem for remote access (later 1200)
- Later called Terminal Access Controller (TAC)
- Centralized authentication used a newly invented protocol "TACACS"
- You were sent a "TAC card" in the mail with your userid/password.



ASR33 TTY

Transition from NCP to TCP: There was a plan

INTERNET PROTOCOL TRANSITION WORKBOOK

March 1982



Network Information Center SRI International Menio Park, CA 94025 (NIC@NIC)

Network Working Group	J. Poste
Request for Comments: 801	November 19
NCP/TCP TRANSITION PLAN	
Introduction	
ARPA sponsored research on computer network of the ARPANET. The installation of the AR 1969, and regular operational use was under has been an operational service for at leas has provided a reliable service in support research activities, it has itself been a s research, and has evolved significantly dur	way by 1971. The ARPANE the to years. Even while of a variety of computer subject of continuing
In the past several years ARPA has sponsore computer networks, principally networks bas communication techniques, in particular, di radio and satellite networks. Also, in the been significant work on local networks.	ed additional research or ed on different underly: cital packet broadcast
It was clear from the start of this researce the base host-to-host protocol used in the use in these networks. In 1973 work was in protocol for use across all these networks. effort is the Internet Protocol (IP) and the Protocol (TCP).	itiated on a host-to-ho The result of this lo
These protocols allow all hosts in the inte metworks to share a common interprocess con The collection of interconnected networks (sometimes called the "Catenet").	nmunication environment.
The Department of Defense has recently ado and the IP and TCP protocols in particular all DOD packet networks, and will be trans architecture over the next several years. networks will be using these protocols exc	as DoD wide standards t itioning to this All new DoD packet
The time has come to put these protocols i ARPANET, and extend the logical connectivi include hosts in other networks participat	ty of the ARPANET hosts
As with all new systems, there will be som robust and efficient as we would like (jus ARPANET). But with your help, these probl	t as with the initial
ostel	[Pag

Transition to TCP/IP

- There was a published plan
- Both protocols supported during transition
- There was a deadline: Jan 1, 1983
 NCP was turned off
- Organizations were highly motivated to transition
 - Lessons learned to apply to IPv6 transition?
- New era: "packet switching"
 - no longer needed to connect host directly to IMP
 - network of networks ightarrow Internet
 - Router: enable forwarding on Unix, run "routed" or "gated" using EGP (precursor to BGP)
 - Ethernet: yellow cable and vampire taps
- Most exciting test: "telnet ucl", get login prompt



Tracking names and addresses

- All computer names and IP addresses were kept in the "hosts file"
 - HOSTS.TXT
 - one would have to download it from the NIC using FTP every so often
- Soon, all the good names were taken and conflicts started, so there was a need to have multiple name spaces (domains)

– DNS was born (specified 1983, BIND in 1984)

 my email address changed from ron@nosc-cc to ron@nosc.mil

Our first security incident August 1983

- Password guessing from UCLA over the ARPANET
- No longer a friendly research playground where you trusted everyone.
- Everyone needed to start locking their doors.



Associated Press

LOS ANGELES — A 19-year-old UCLA student was charged yesterday with using a home computer to break into a Defense Department communications system linking government and private computers throughout the United States and Europe.

Ronald Mark Austin was arrested at his Santa Monica home and booked into Los Angeles County Jail on a district attorney's complaint accusing him of 14 felony counts of maliciously gaining access to a computer system. Bail was set at \$10,000, and a Municipal Court arraignment was expected today.

"This is not some childish prank," District Attorney Robert Philibosian told a news conference. "We're talking about an individual who has cost the federal government, private organizations and universities literally hundreds of thousands of dollars in reprogramming costs."

Philibosian said some of the information Austin allegedly gained access to was "very sensitive."

The complaint also charged Austin with one count each of theft and receiving stolen property in connection with four allegedly stolen airline tickets to Europe found at his home. If convicted, he faces up to six years in prison.

District attorney spokesman Al Albergate said the tickets were made out to people who lived in Austin's neighborhood. He said investigators also found \$800 in \$100 bills, possibly proceeds from the sale of other tickets.

Investigators said they did not know if the tickets were - mited to the computer scheme.

Austin's arrest followed an investigation by the instrict attorney's Electronic Crimes Section in cooperation with the UCLA Computer Sciences Department.

Philibosian said the investigation infrated that the unauthorized access to computer systems at include the same state of the same state o

Philibosian - of the computer systems reached by Austin all had to be reprosed and a system of the s

"Using local telephone connections, Austin gained access not only by oreal computer accounts but also, through the UCLA system, to the Advanced Research Projects Agency Network" linking computers that store data on research projects for several agencies, includinthe Defense Department, Philibosian said.

"Some of the information was very sensition one district attorney said. "We can't give a more complete description at this time."

The complaint all a within gained access to more than 200 computer a set 14 different locations, and that in some cases he mocked out legitimate account users.

"We don't know what he was doing with the data," Philibosian said,



United Press Internation

L.A. District Attorney Robert Philibosian displays material confiscated from a UCLA student who was charged with maliciously accessing a computer system.

adding that Austin's motives are still under investigation.

Austin allegedly gained access to computers at the Naval Ocean Systems Center in San Diego, Naval Research Laboratory in Washington, D.C., Norwegian Telecommunication Administration in Norway

and Rand Corp. in Santa Monica. Rand spotkesman Paul Weeks said the company determined that on Aug. 29 an unauthorized person used "a Rand computer that is used to forward electronic mail on a national network of computers."

Weeks said the computer was used only "sort of like a relay" to tie into other computers in the Advanced Research Projects Agency Network and "there was no penetration of any Rand data or files."

NOSC

TRS-80

Early security references

The "Orange book" (1985)
– "Trusted Computer Systems"
– part of the "Rainbow series".



more on security

- Additional notable incidents
 - Morris Worm (Nov 2, 1988)
 - El Griton (1995)



- Fighting back:
 - "hack back"

Sharing with Friends

- Connected neighboring Universities via Serial Line Internet Protocol (SLIP). This was before PPP existed. Examples:
 - UCSD via 2.4Kb dialup modem
 - Univ of Hawaii (9.6Kb across Pacific Ocean to Hawaii, then SLIP over dialup to Honolulu)
- We provided authoritative DNS for numerous large domains.
- This all changed after NSFNet arrived (1988) and connections were more generally available.
- 1992 Internet becomes mainstream

Summary

- Birth of the Internet led to many subsequent innovations
- Multiple transitions along the way
 - From NCP to TCP
 - From circuit switching to packet switching
 - From open and friendly research environment to something needing protections
 - From government to commercial
- History can help explain why things are they way they are, and can provide valuable lessons.

END

Contact: ron@nosc.mil