computermuseum
muenchen

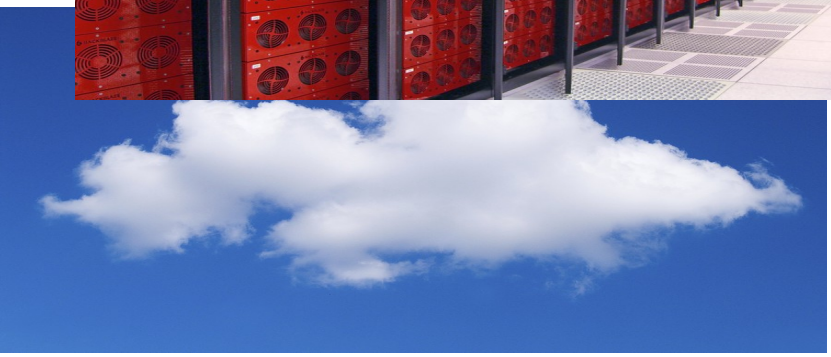
Cloud und Sicherheit 1960 bis 1990 – Alles schon mal da gewesen, inklusive Lösungen

John G. Zabolitzky

Definitionen – Personal vs. Cloud Computing

Personal – Daten im physischen Besitz (Datenträger) des Anwenders
Anwender trägt Verantwortung für Backup, Diebstahlsicherheit, Verlustgefahr
Verarbeitungseinheit im physischen Besitz (Rechner) des Anwenders
Anwender trägt Verantwortung für Zuverlässigkeit der Hardware, Software
Im optimalen Falle keine Kabel- oder anderen Verbindungen in die Außenwelt

Definitionen – Personal vs. Cloud Computing



Cloud – Daten werden an unbekanntem Ort, jedenfalls entfernt aufbewahrt, kein physischer Zugriff
Dienstleister trägt Verantwortung für Backup, Diebstahlsicherheit, Verlustgefahr
Verarbeitung „hinter dem Kabel“ - auf im Detail unbekannter Hardware, Software
Dienstleister trägt Verantwortung für Zuverlässigkeit der Hardware, Software
Kabel- oder andere Verbindung in die Außenwelt notwendig und unerlässlich erforderlich

Ursprung: Personal Computing 4000 BC - Aegyptian Cloud ???

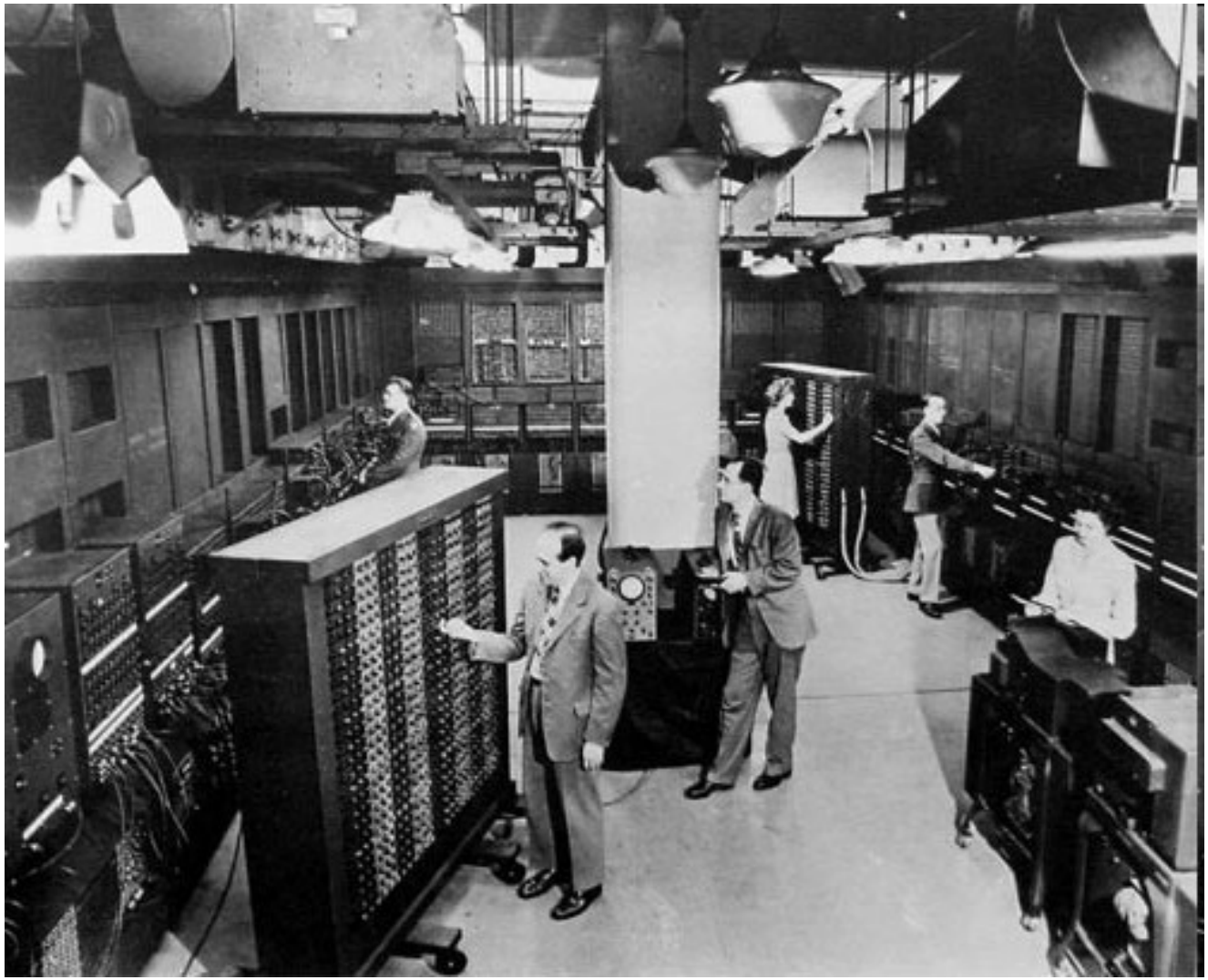
Papier + Bleistift + Mensch = Turing vollständig

Rechner = Berufsbezeichnung

Warum war der reitende Bote in vielen Fällen bewaffnet ? Was hat das mit uns zu tun ?

Lochkartenverarbeitung, 1890 – 196x = Cloud

ENIAC (1946) Electronic Numerical Integrator and Computer



Wird in USA bisweilen für den ersten Computer gehalten

Programmiert durch Steckverdrahtung

20 Speicherplätze

10 Dezimalstellen

17468 Röhren

früher Personal Computer

Warum Personal Computer ?

John von Neumann reist 1946 von Los Alamos nach Philadelphia mit der Bahn (mehrere Tage !)

„Programm“ (Gleichungen) und Daten mit dabei in Aktentasche

Vorher und nachher keine Spuren der Aufgabenstellung am ENIAC

Telefon und Fernschreiber existierten, zuverlässige Verbindungen

Man hätte ENIAC mit etwas Personal zur Datenkommunikation in einen Cloud-Rechner verwandeln können ….. Missverständnisse zu leicht?

Hat das was mit Sicherheit zu tun ?

- Los Alamos und Philadelphia militärisch gesicherte Bereiche
- frühe Simulationen zur Wasserstoffbombe

Es war eine ENTSCHEIDUNG das nicht zu tun …

Hat Sicherheit vielleicht vorrangig etwas mit unseren Ansichten, Meinungen, Entscheidungen zu tun ???

Besuch von Interessanten Menschen sicherlich vorrangig

John von Neumann (1903-1957)

Sicherheit und Personal Computing: OK falls keine Verbindung zur Außenwelt

Grossrechner, 195x bis heute CDC 6600, 1964 8 M$ = 50 M$ heute CLOUD

Netzwerk von I/O-Stationen (Lochkarten), später interakt. Terminals über **sep. Kommunikations-R.**

typisch ein/mehrere Zentralrechner je Firma, Universität, Forschungslabor, **Dienstleister**, ...

Betrieb durch typisch 10 Personen in 3 Schichten, 4 Servicetechniker, 4 Operateure, 2 Systemprog.

Änderung Systemdatei **NUR** von dieser Konsole aus möglich (Sammlung aller ausführbaren nicht-privaten oder priviligierten Objekte)

BETRIEBSSYSTEM ??

Berechtigungen ??

Wertesystem

Bequemlichkeit – Features – Gadgets **<====>** **Sicherheit**

Systemänderungen vom Terminal zu Hause — physische Anwesenheit
Maschinenüberwachung dto. — im Rechenzentrum
Bedienung, Optimierung dto.

Technische Absicherung — Zutrittskontrolle
Ist das zuverlässig sicher ?
Passwort-/ID-Handhabung ? — Gesichtskontrolle durch andere Mitarbeiter

Alle Kommunikation verfügbar, hoch integriert — Getrennte Kommunikations-Rechner, Übersetzung

komplex — einfach

Betriebssysteme

IBM (1964: System /360) und die sieben Zwerge 196x

- Control Data Corp. CDC — COS, Scope, Kronos, NOS, **NOS/VE (1980-1996)**
- Burroughs — MasterControlProgram
- UNIVAC — EXEC I, II, 8
- NCR — long list
- Honeywell — IBM, **Multics on 6180(1972), DPS-8/70M (1982-1987)**
- RCA — DOS, TDOS, VMOS, IBM
- General Electric — GECOS, Mark II, III, **Multics (1963 – MIT, Bell labs)**
  - » **GE645 erweiterte Hardware**

US Government Research Labs, Militär, NSA besonders wichtige Kunden für CDC

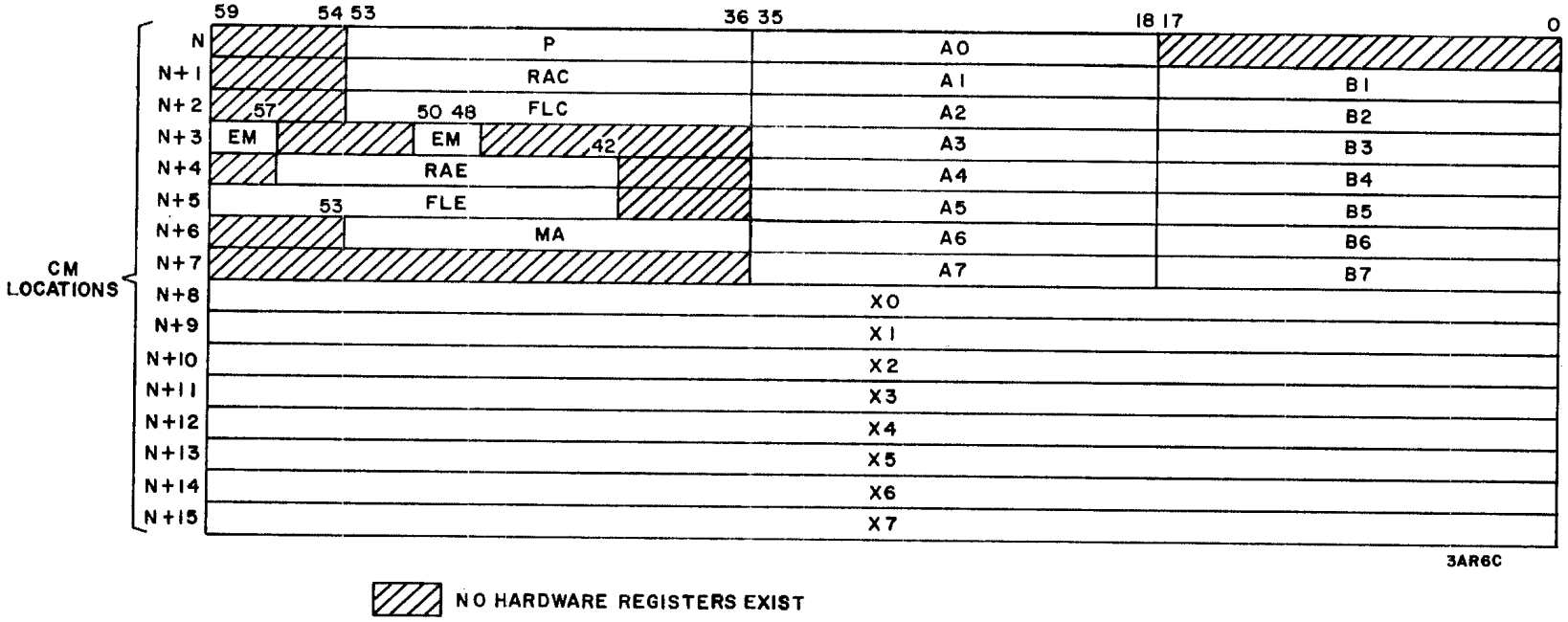
==> Sicherheit ist wichtiger Gesichtspunkt von Anfang an

Proprietär – Hardware und Software optimal aufeinander abgestimmt

- Sicherheit ==> spezielle Hardware-Anforderungen
- MÜSSEN ABER VON SOFTWARE AUCH GENUTZT WERDEN

The time during which a particular exchange package resides in the CP hardware registers is the execution interval. The execution interval begins with an exchange jump that swaps the exchange package information in CM with the information contained in the CP registers. The execution interval ends with the next exchange jump.

A hardware flag called a monitor flag (MF) indicates the type of program the CP is executing. When the flag is set, the program executing is a monitor program. When the flag is clear, the program executing is a user program.



Monitor Mode <== Figure 5-1. Exchange Package ===> User Mode

MF = 1 CDC 6600 (1964) MF = 0

CDC 6000 / Cyber Scope/Kronos/NOS Betriebssysteme 1964-1996

Hardware:

- kein Paging, physischer Speicher in einem zusammenhängenden Block
- Effiziente I/O, Verschiebung im Speicher
- Leistungsfähigste Time-Sharing Systeme bis in die 198x Jahre
- Im Betrieb bis 2015 (militärische Festprogrammierung)
- Netzwerkankopplung durch **separate Kommunikations-Rechner**, KEINE Abbildung von Netzwerkfunktionen in die Benutzer-Ebene, dort reine I/O-Operationen ausgeführt durch das Betriebssystem, Datensätze
- NOS = Network Operating System, Verteilung auf multiple CPUs, zentrales Management des GESAMTEN Netzwerks (CDCNET, alles aus einer Hand)

User Mode:

- Keine Zugriffe außerhalb zugewiesener Feldlänge
- Keine Zugriffe auf Hardware
- Exchange Jump zur Anforderung von Systemfunktionen
- Ausgefeiltes, feinkörniges System von Berechtigungen je Benutzer

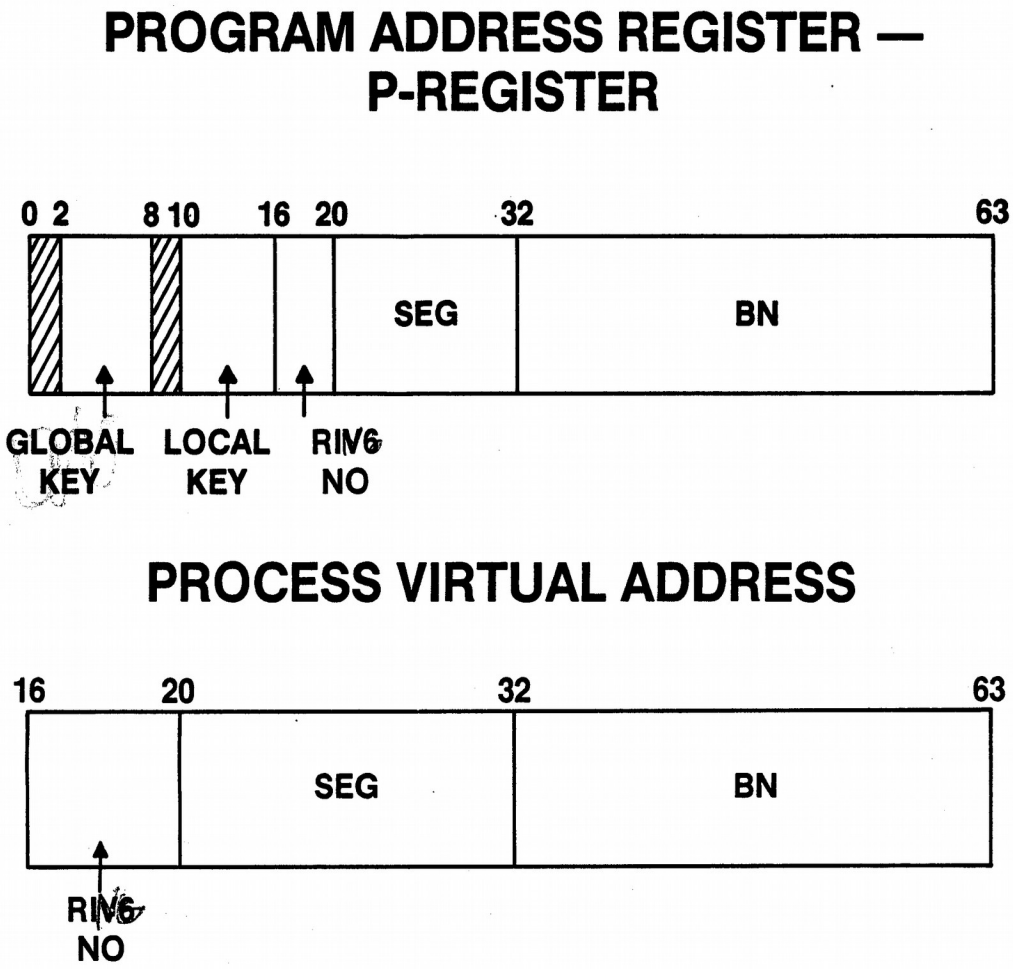
CDC NOS/VE Network Operating System Virtual Environment 1982-1996

Wesentlich beeinflusst von Multics

BN Byte Number < 2 G / Segment
SEG pointer 4k into table
RING NO = protection ring, 1-15

= hierarchical protection

KEY = capability
= capability protection



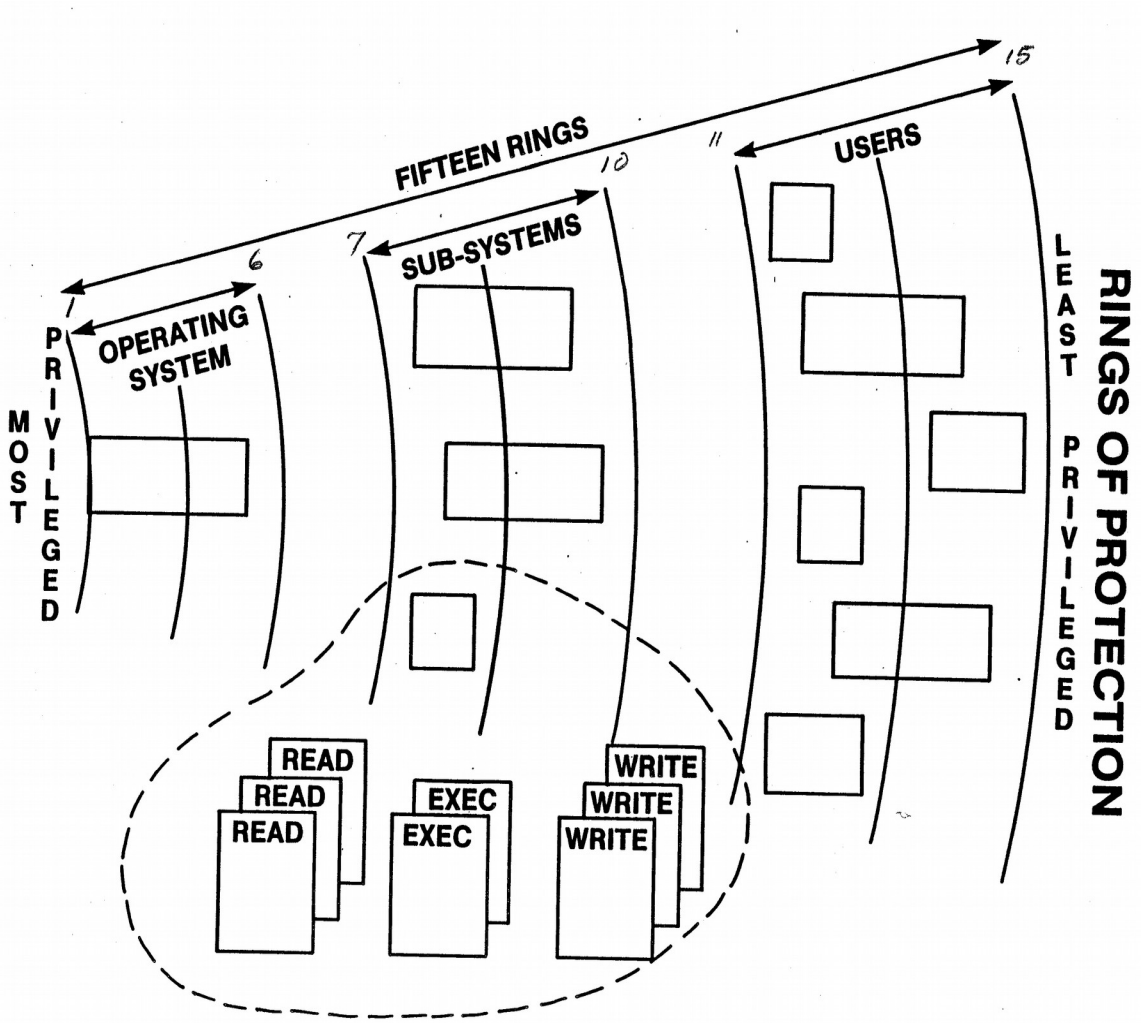
NOS/VE
Rings of Protection, similar to Multics

Ring 0 for virtualization,
Multitude of simultaneously active
Operating systems (2 widel used)

No shaing of peripherals

Read – write – execute
within ring brackets
(property of segments)

Hardware and Software
fully codesigned



NOS/VE Exchange Package

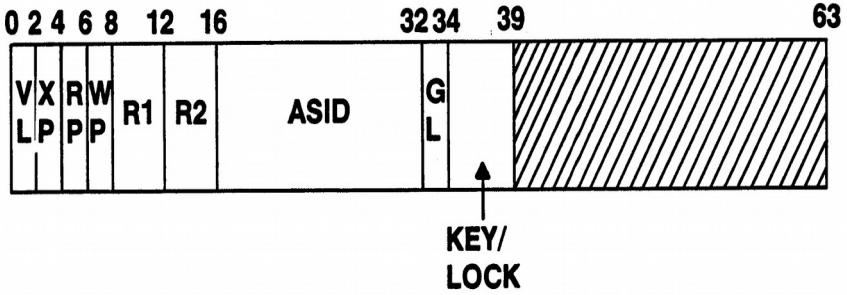
BYTE(HEX)	00	07 08	15 16	WORD(DEC) 63	
0	P				0
8	VMID	UVMID	A0		1
10	Flags	Trap Enables	A1		2
18	User Mask		A2		3
20	Monitor Mask		A3		4
28	User Condition		A4		5
30	Monitor Condition		A5		6
38	Kypt. Class	LPID	A6		7
40	Keypoint Mask		A7		8
48	Keypoint Code		A8		9
50			A9		10
58	Process Int. Timer		AA		11
60			AB		12
68	Base Constant		AC		13
70			AD		14
78	Model Dependent Flags		AE		15
80	Segment Table Length		AF		16
88	X0				17
90	X1				18
C0					24
C8	X8				25
D0	X9				26
D8	XA				27
E0	XB				28
E8	XC				29
F0	XD				30
F8	XE				31
100	XF				32
108	Model Dependent Word				33
110	Segment Table Address		Untranslatable Pointer		34
118			Trap Pointer		35
120	Debug Index	Debug Mask	Debug List Pointer		36
128	Largest Ring Number		Top of Stack Ring Number 1		37
198			Top of Stack Ring Number 15		51
	00	07 08	15 16	63	

P Keys, Ring-No., Segment-No., Byte Adrs

VMID Virtual Machine ID (z.B. NOS; NOS/VE)

Segment Table Segment-Deskriptoren

- Read Ring Bracket
- Write Ring Bracket
- Execution Ring Bracket



CDC Cyber 2000 (1989, 5 Stück deinstalliert Zürich 2008; Ende CDC 1996)

letzte und leistungsfähigste NOS/VE-Maschine: 9.4 nsec = 106 MHz, 14k ECL gate arrays, 512 Mbyte Hauptspeicher 848 Mbyte/sec (= 1 Wort / Takt je Port), 128 kByte cache, several page sizes bis 64 kByte, 13 MFLOPS, 51 MIPS

Quellcode des NOS/VE-Systems

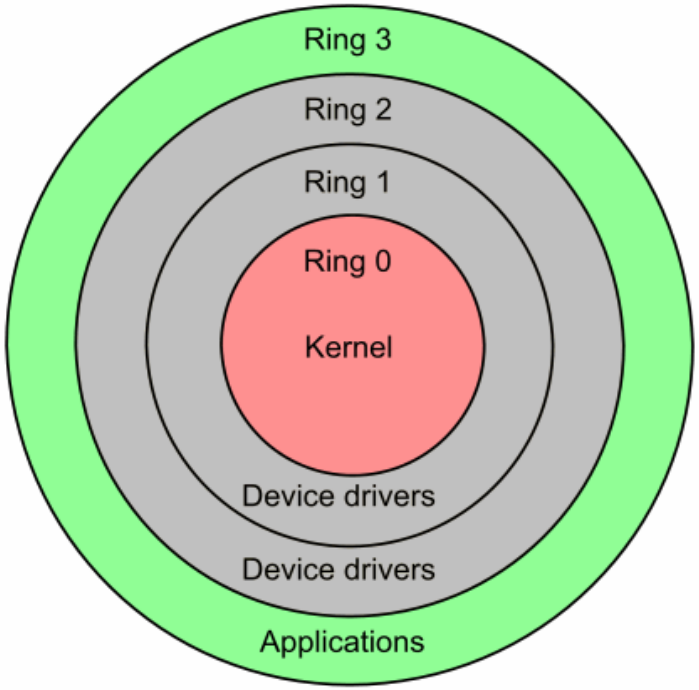
Microcode und Microcode-Entwicklungssystem

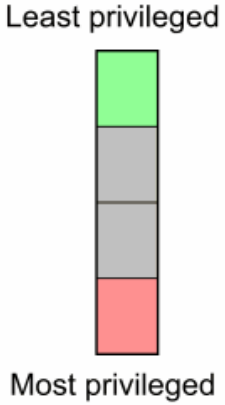
Objectcode NOS/VE-System, Produktionssystem (viele Compiler), Anwendungen

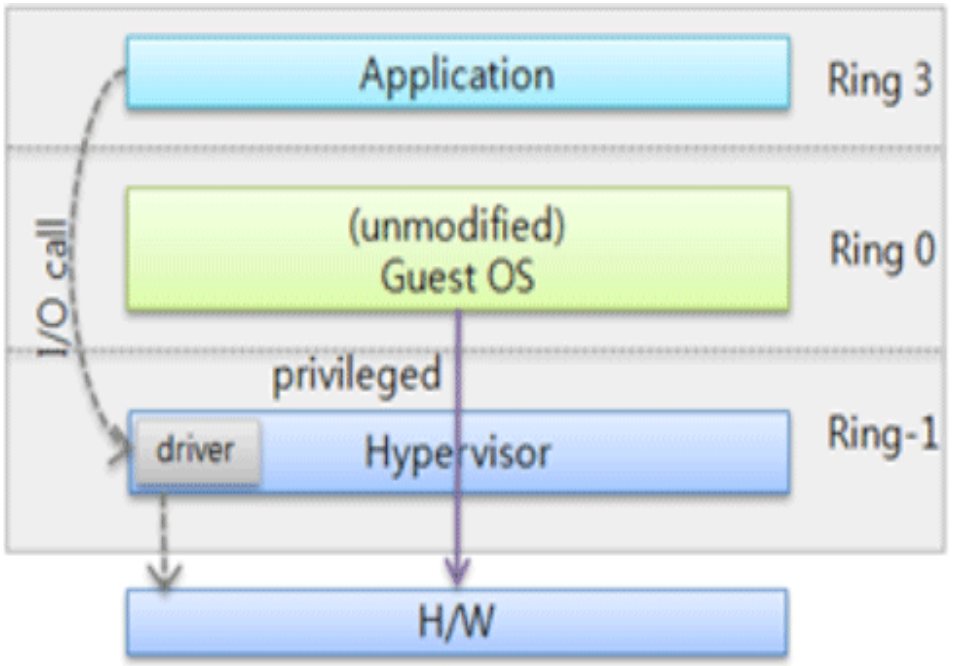
NOS/VE lief auf unserer Cyber 960 mehrere Jahre dual-state parallel mit real-mode NOS Betriebssystem

Intel: 4-Ring Hardware
aber nur 0,3 benutzt: Monitor Mode / User Mode Monitor, User = Niveau von 1964
Virtualization: neuer Ring -1 zusätzlich eingeführt

Multics ==> Unix / Linux ?????

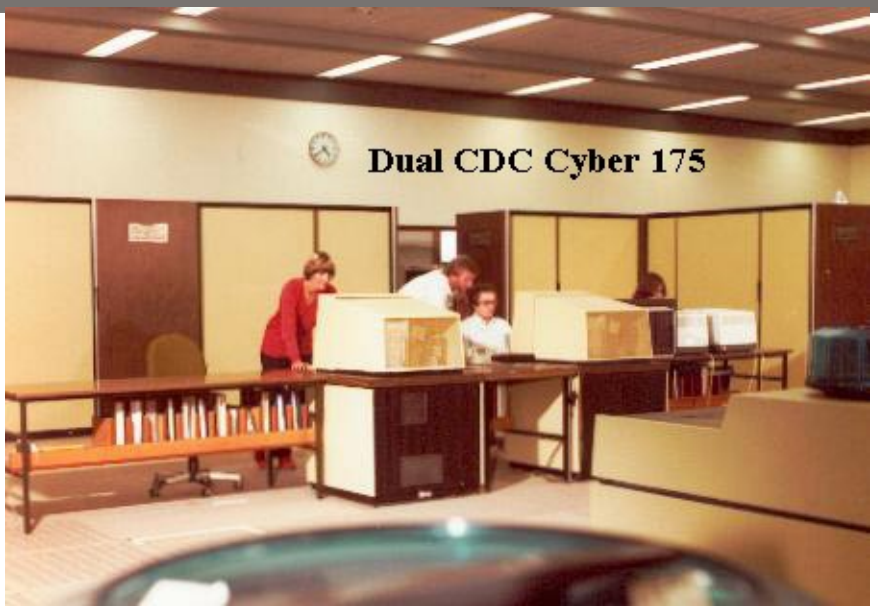


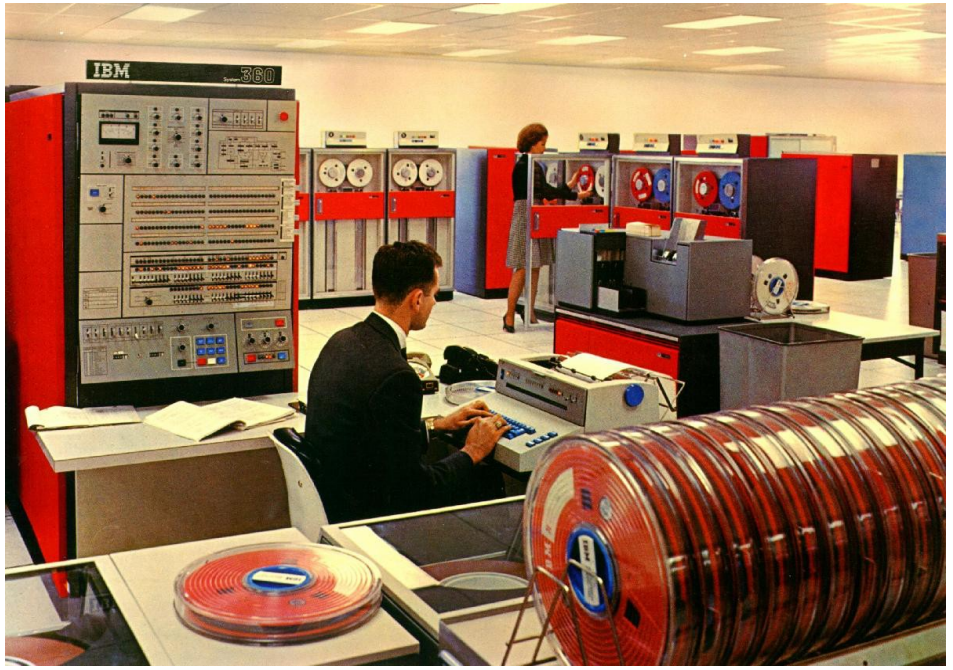




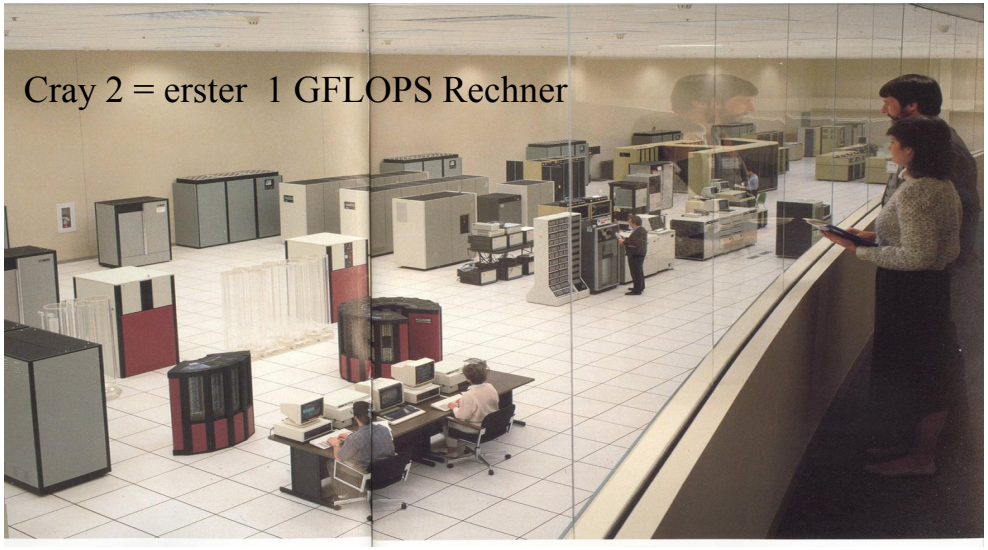
IBM 1970, LRZ 1979, MSC 1986 : Cloud

computermuseum muenchen





180 Mbyte/Spindel 256 Mbyte/Bandspule



computermuseum
muenchen

Control Data CDC 160A 1960

12 bit, diskrete Transistoren

Digital Equipment PDP-8 1965

12 bit, Transistoren => ICs

1970 PDP-11 16-bit ICs

frühe Personal Computer

Häufig für dedizierte Aufgaben = Überwachung/Steuerung real-time Experiment, Prüfstand, etc.

1975 8080 systems, CP/M

1981 IBM PC, Intel CPU,MSDOS

Cloud heute: Microsoft, Amazon, usw., usw.; Tianhe-2 China 3M Kerne
34 PFLOPS, 18 MW, 720 qm, RAM 1375 TByte, Mass 12,4 ExaByte, Linux

Lektion

Bequemlichkeit, „Features“ <==> Sicherheit
Abschottung
Verzicht

Vorkehrungen in Hardware
Vorkehrungen in Software (System)

Codesign von Anfang an

Haltung, Werteskala

Sicherheit hat genau den Stellenwert den wir ihr geben
Existierende Hardware ???
Existierende Software ???

Letztendlich: Verdrängen, unter den Teppich kehren, „Nachrüsten (!!!)“
<==> den Kosten ins Auge schauen, akzeptieren, und ausführen

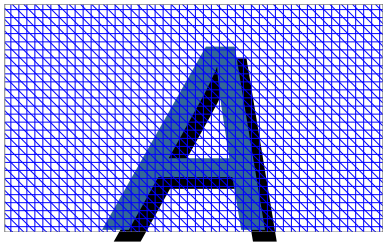
Sicherheit und Personal Computing: mit Verbindung zur Außenwelt ?????

Sicherheit und Personal Computing: mit Firewall zur Außenwelt ?????

von 4000 BC bis heute

keine neuen Aufgaben, nur alte Aufgaben in neuer Verkleidung

erkenne die Verkleidung, kenne die Vergangenheit, dafür ist das Computermuseum hilfreich



Risikofaktor Mensch

Feb 2016, Zugunglück Bad Aibling – Fahrdienstleiter will noch einen weiteren Zug auf Strecke

März 2011, Fukushima: gemessen Erdbeben Stärke 9, Tsunami 10-12m (lokal bis zu 23m)

- Spezifikation: Erdbeben Stärke 8, Tsunami 7m
- 1926 Erdbeben Stärke 9 bereits vorgekommen
  - Stärke +1: Zeitintervall *10
  - Spezifikation an diesem Ort hätte Stärke 10 sein müssen
- Simulation: max. 30m Tsunami war bekannt

April 1986, Tschernobyl:

- Verstoß gegen Sicherheitsvorschriften
- absichtlich in den unzulässigen Bereich gefahren

Überstimmung des Menschen durch den Computer zulässig ?
Überstimmung des Computers durch den Menschen zulässig ?
==> automatisierte PKW, rechtliche/versicherungstechnische Probleme ?

2006-2013, CDs mit Daten Schweizer Bankkunden an Deutsche Steuerbehörden verkauft