Betriebssystemsicherheit am Beispiel UNIX

Motivation

Der Anteil von UNIX-Systemen in vernetzten Umgebungen, insbesondere als Server in TCP/IP-basierten Netzen, ist sehr gross und immer noch weiter ansteigend.

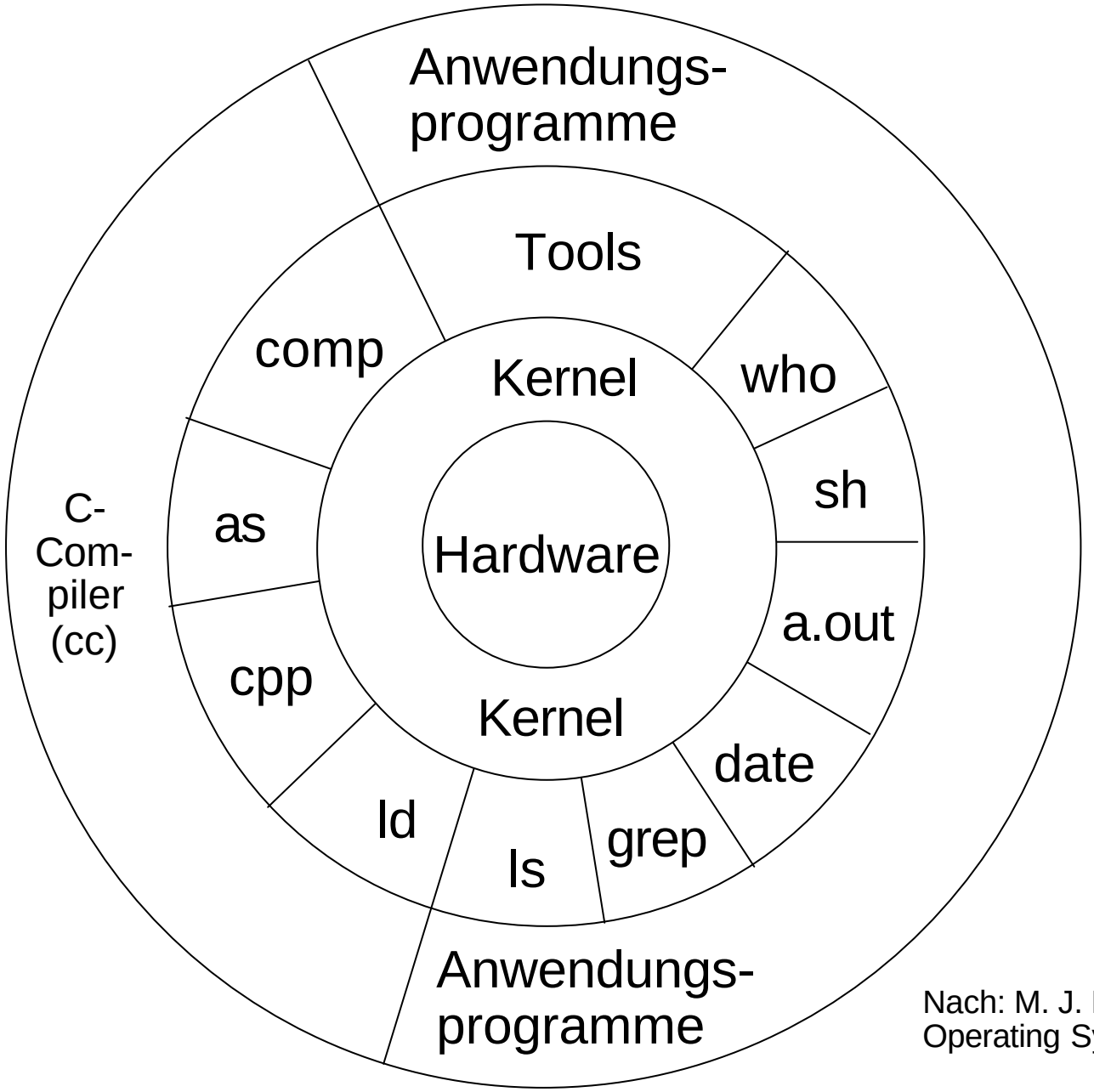
Daher kommt Sicherheitsbetrachtungen in Bezug auf die Einbindung von UNIX-Systemen in Rechnernetze eine besondere Bedeutung zu. Viele Erkenntnisse gelten jedoch auch für andere Betriebssysteme.

Inhaltsübersicht

- UNIX-Rekapitulation
- Spezifische Schwachstellen
- Verfügbare Software und Informationsquellen
- Literaturhinweise

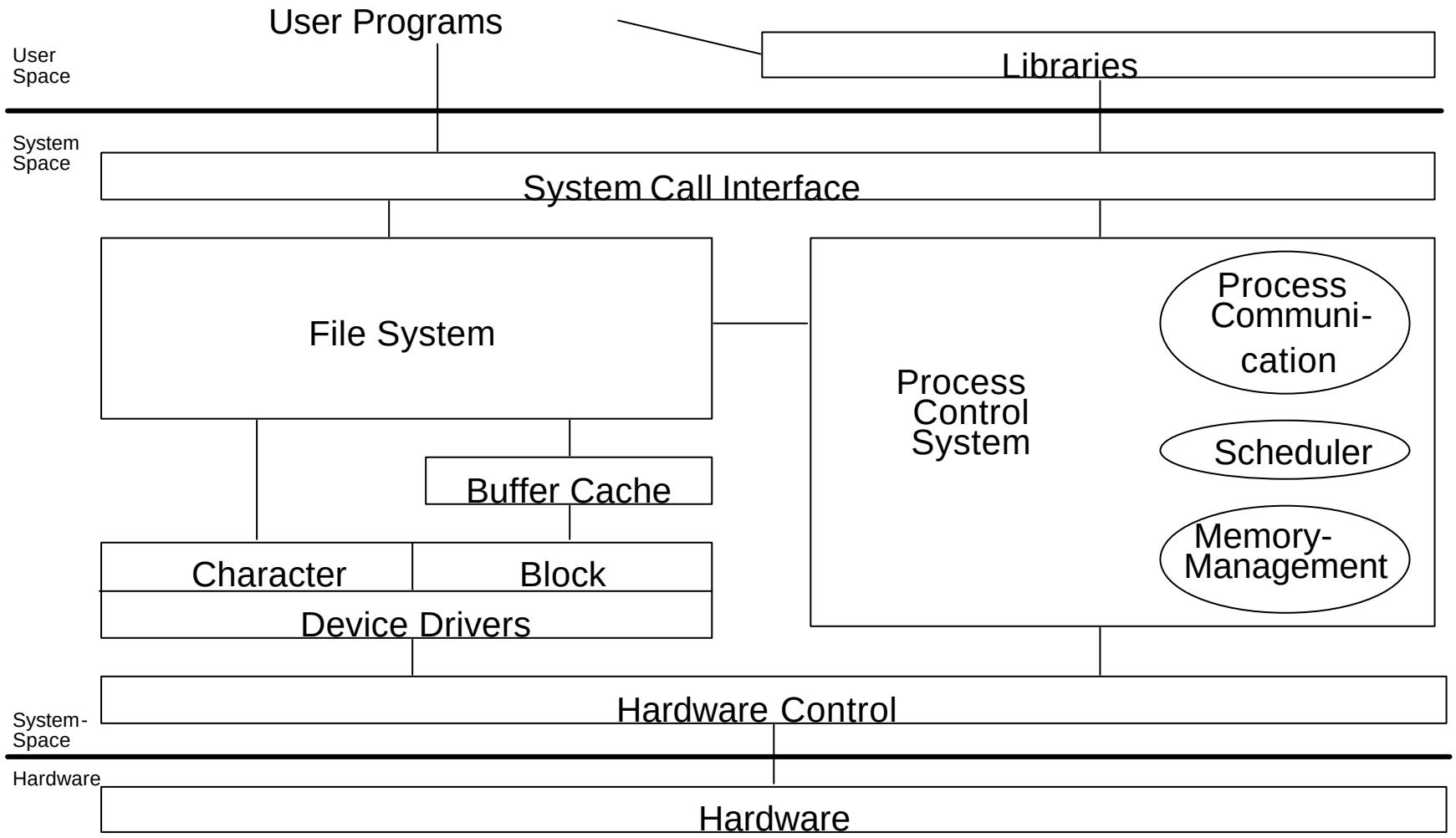
UNIX-Rekapitulation

- Im Internet sehr weit verbreitetes Betriebssystem
- TCP/IP wird in der Regel mitgeliefert
- Architektur als offenes System
- Sicherheit war kein primäres Entwurfsziel



Nach: M. J. Bach, The Design of the UNIX Operating System, Prentice Hall, 1989

Blockdiagramm des UNIX Kerns



Aus: M.J. Bach, The Design of The UNIX Operating System, Figure 2.1

UNIX-bezogene Sicherheitsaspekte

- Betriebssystem-Anforderungen
- Installation von Netzwerk-Software
- Schnittstellen zum Betriebssystem
- Administration und Überwachung

Betriebssystem-Anforderungen

- Verschiedene Ausführungsmodi
- Speicherarchitektur
- Dateisystem
- Netzwerk-Schnittstellen
- Administrationsprogramme
- “Normale” Endbenutzer-Programme und Programmentwicklung

Installation von Netzwerk-Software

- Kernel Konfiguration durch Definition von Schnittstellen und entsprechenden Flags in der Kernel-Konfigurationsdatei.
- Einbindung einer TCP/IP Implementation (Objekt-Code) in den Kern, sofern der Hersteller dies noch nicht getan hat.
- Einbindung entsprechender Gerätetreiber in den Kern und Neu-Übersetzung/-Installation des Kerns (sofern nicht dynamisch).
- Anlegen entsprechender “device special files” unter “/dev”.
- Installation von Administrations- und Anwendungsprogrammen
- Installation von Programm-Bibliotheken
- Erstellung und/oder Erweiterung von Konfigurationsdateien

Netz-Schnittstelle zum Betriebssystem

- Komplexes Protokoll, dessen Wirkungen und Nebenwirkungen nicht intuitiv einsichtig sind
- Belegung von Ressourcen (Speicher/Puffer, Files, Rechenzeit usw.) mit Auswirkungen auf das Betriebssystem
- Server- oder Hintergrund-Prozesse mit ggf. hohen Privilegien
- Anwendungssoftware mit hohen Privilegien und Nebeneffekten
- Programmierschnittstelle und Programmier-Bibliotheken

Administration und Überwachung

- Shadow Passwords, ggf. Password Ageing
- Quota System und Accounting
- Verwendung von “.rhosts” Dateien oder ähnlichen Mechanismen durch die Anwendungssoftware
- Temporäre/selektive Bewilligung von “root” Privilegien
- Suche nach “setuid/setgid” Dateien und Scripts (!)
- …

- Binärvergleich “sensitiver” Dateien
- Konsequente Anlage und Auswertung von Logging-Information

Schlussfolgerungen

- Die meisten UNIX-Sicherheitsprobleme beruhen auf fehlerhafter Installation und Überwachung, nicht in Fehlern in der Konzeption oder Implementierung der eigentlichen Betriebs- oder Netzwerk-Software.

- In den meisten Fällen sind die entsprechenden Schwach-stellen schon sehr frühzeitig bekannt. Daher ist regelmässiger Zugang zu entsprechender Information im Internet überlebenswichtig.

- Bei jeder erkannten Schwachstelle muss der Administrator SOFORT handeln. Bezüglich Sicherheit im Internet gibt es keine “kleinen” Probleme, ggf. aber Kompetenz-Unsicherheiten.

Software und Informationsquellen

Sicherheits-Toolkits und Programme:

COPS
CRACK
ISS
SATAN

Informationsangebote:

Usenet: comp.security.unix, comp.security.announce, alt.security
WWW: http://www.tansu.com.au/Info/security.html
WWW: http://www.switch.ch/switch/cert
ftp: info.cert.org

Literatur

- S. Garfinkel, G. Spafford,“Practical UNIX Security”, O’Reilly, Sebastopol, CA, 1991
- D. Curry, “UNIX System Security”, Addison-Wesley, 1993
- D. Smith, “UNIX Computer Security Checklist (Version 1.1)”, Australian Computer Emergency Response Team