Aufgaben zum Thema „Sicherheit“

S1. Beschreiben Sie Gemeinsamkeiten und Unterschiede von Zugriffssteuerlisten (access control lists) und Zugriffsberechtigungen (capabilities)! 95/5

S2. In einem Unix-System soll für die Person P, die zu einer Gruppe G gehört, ein Terminkalender implementiert werden. Die Datenbasis des Kalenders liege als ASCII-Text in einer Unix-Datei *kaldb*. Für alle Gruppenmitglieder und nur für diese soll das Lesen der Datenbasis (z.B. mit einem beliebigen Editor) möglich sein, das Vornehmen von Einträgen dagegen nur unter Nutzung eines P gehörenden Unix-Programms *kaleintr*. Geben Sie die Schutzattribute von *kaldb* und *kaleintr* an (in symbolischer Form)! 97/1

S3. In einem Unix-System gebe es die Benutzer Adalbert (A), Balthasar (B), Conradin (C) und Melchior (M). Alle gehören der Gruppe Skatclub (SC) an. Melchior besitzt ein Programm (P) zur Führung von Ranglisten, das folgendes leistet: Je drei Spieler können mit Hilfe von P gegeneinander spielen, P überwacht die Einhaltung der Regeln und registriert in einer Ergebnisdatei (ED) den Spielstand. Melchior ist Eigentümer von P und ED.

Setzen Sie die Schutzattribute von ED und P so,
- daß nur Mitglieder von SC das Programm P benutzen dürfen,
- daß Gruppenmitglieder (außer Melchior) nicht in ED schreiben dürfen,
- daß aber jeder Spieler Spielergebnisse mittels P in ED schreiben kann.

Erläutern Sie Ihre Lösung! 97/7

S4. Erläutern Sie für jedes der nachfolgend angegebenen Schutzprobleme, inwieweit die Mechanismen Capabilities – Zugriffskontrollisten – Schutzbits *rwx* in UNIX geeignet sind
- Anton möchte, daß seine Dateien für jeden Benutzer außer Berta lesbar sind.
- Cäsar und Dora möchten einige geheime Daten gemeinsam benutzen.
- Emil möchte einige seiner Daten öffentlich zugänglich machen. 97/11

S5. Erläutern Sie die Notwendigkeit, in verteilten Systemen Verschlüsselungsverfahren anzuwenden! Gehen Sie auf die Unterschiede von secret-key-Verfahren und public-key-Verfahren ein! 97/11

S6. Anton besitzt ein Zertifikat $\{\text{Berta}, K^{pub}_{\text{Berta}}\}K^{priv}_{C}$ der Certificationauthority C und erhält eine Nachricht, die angeblich von Berta kommt. Was müssen Anton und Berta tun, damit Anton sich sicher sein kann, daß Bertas Nachrichten wirklich von Berta kommen? 98/2

S7. Angenommen, es gebe für die miteinander kooperierenden Institutionen TUD und IBM sowie deren Abteilungen certification authorities (CA) folgender Art:

CA für TUD: zertifiziert Schlüssel der CA's für Fakultäten und der Kooperationspartner
CA für INF: zertifiziert Schlüssel der CA von TUD und der Mitarbeiter der Fakultät Informatik
CA für IBM: zertifiziert Schlüssel der CA's für IBM-Abteilungen und der Kooperationspartner
CA für Watson Research Center: zertifiziert Schlüssel der CA von IBM und der Mitarbeiter des Watson Research Center.

Geben Sie die Zertifizierungskette an, die erforderlich ist, damit der Schlüssel des Mitarbeiters Meier der Fakultät Informatik für den Mitarbeiter Johnson der IBM-Abteilung Watson Research Center zertifiziert wird! 98/7

S8. Zwei Personen, Hinz und Kunz, wollen in einem vernetzten System unter Nutzung einer Certification Authority C sicher miteinander kommunizieren. Konkret will Kunz Nachrichten an Hinz senden.

a) Welches Zertifikat muß dazu Hinz besitzen?

b) Welche Art von Angriff ist dennoch möglich? Beschreiben Sie die Aktivitäten von Hinz und Kunz, diesem Angriff zu begegnen! 99/8

S9*. Erläutern Sie den Begriff „ACL“ im Sinne eines Glossars: Einordnung in das Gebiet Betriebssysteme – Erklärung – Bedeutung (wozu, Vor-/Nachteile, Umfeld, vergleichbare Begriffe o.ä.)! 01/2

S10. Ein Server führe zu zwei Dateien D1 und D2 folgende Zugriffssteuerlisten (ACL's):

D1:	Nutzer A:	r-x	D2:	Nutzer A:	r-x
	Nutzer B:	--x		Nutzer B:	rwx
	Nutzer C:	rwx		Nutzer C:	r-x
	Nutzer D:	--x		Nutzer D:	rwx

Jeder Nutzer X erzeuge einen Prozeß P_X,..., der genau dieselben Rechte wie der erzeugende Nutzer besitzt. Stellen Sie für jeden dieser Prozesse eine Capability-Liste auf! Erläutern Sie daran kurz Gemeinsamkeiten und Unterschiede der beiden Schutzmechanismen! 02/11

S11. Erklären Sie die Begriffe „ACL“ und „capability“! Welchem Zweck dienen diese Begriffe? Erläutern Sie zwei Gesichtspunkte, in denen sie sich unterscheiden! 04/3

S12. Jemand schlägt folgendes Verfahren zur Bestätigung dessen vor, daß zwei Partner A und B im Besitz desselben geheimen Schlüssels S sind.

A erzeugt auf Zufallsbasis eine Bitkette, die genau so lang wie der Schlüssel ist. Mit dieser Bitkette und dem Schlüssel S führt A eine XOR-Verknüpfung durch und sendet das Ergebnis an B. B verknüpft die eingehende Nachricht gleichfalls durch XOR mit S und sendet das Ergebnis an A zurück. A prüft den empfangenen Block mit der zufällig gewählten Zeichenkette; bei Übereinstimmung ist er sich sicher, daß B denselben geheimen Schlüssel S besitzt, ohne daß S jemals übertragen worden ist.

Hat dieses Verfahren eine Schwachstelle? Begründung! 04/8

S13. Angenommen, die Ergebnisse (Noten) dieser Klausur sind beim verantwortlichen Hochschullehrer *Prof* in zwei Dateien *infnot*, *mednot* abgelegt, die den beteiligten Studiengängen *INF* und *MED* entsprechen. Der Hochschullehrer möchte folgendes ermöglichen:

- ein Student kann genau die Notenliste seines Studienganges einsehen, aber nicht verändern;
- er selbst kann alle Listen sowohl lesen als auch bearbeiten;
- das gleiche ist auch den Mitarbeitern des Prüfungsamts *Prüfamt* gestattet;
- weitere Zugriffe sollen nicht möglich sein.

Außerdem möchte er die Einsichtmöglichkeit für die Studenten zu einem bestimmten, nicht von vornherein bekannten Termin beenden.

Erläutern Sie (möglichst durch Angabe der entsprechenden Zuordnungen), wie die drei Mechanismen

ACL (Zugriffssteuerlisten) – Capabilities – Rechteschema von Unix

zur Lösung dieses Schutzproblems eingesetzt werden können bzw. welche Probleme dabei auftreten! 08/2, 05/2

S14. Zur Vorbereitung auf eine Prüfung haben sich drei Studenten *A*, *B*, *C* zu einer Lerngruppe zusammengefunden. Jeder Student legt für sich eine Datei *DA*, *DB* bzw. *DC* an, in die er seine Lösungen von Aufgaben schreibt. Außerdem haben die Studenten einen Tutor *T* gewonnen, der bereit ist, die Lösungen durchzusehen und ggf. zu korrigieren. Jeder Student *X* hat die folgenden Schutzziele:

- die eigene Datei *DX* kann von *X* lesend und schreibend genutzt werden;
- die beiden anderen Studenten $Y \neq X$ können die Datei *DX* nur lesen;
- der Tutor kann auf alle Dateien sowohl lesend als auch schreibend zugreifen;
- weitere Personen sollen keinerlei Zugriffsmöglichkeiten auf die Datei haben.

a) Geben sie eine Lösung auf der Basis einer „einfachen“ ACL (ohne Nutzung von Gruppen) an!

b) Lösen Sie die Aufgabe mittels Capabilities! Welches Problem ergibt sich, wenn die Lerngruppe dynamisch ist (Studenten also ständig die Gruppe verlassen oder hinzukommen)?

c) Warum lassen sich die angegebenen Schutzziele mit dem Unix-Rechtesystem nicht erreichen?

09 /8, 06/8