בקרת גישה - Access Control

פרק 4 בספר "Security Engineering" של רוס אנדרסון

סמינר באבטחת מחשבים עם פרופ' אור דונקלמן

מוצג ע"י: מוסטפא מחאמיד

19.04.2015

הקדמה

- מה זה בקרת גישה (Access control) ?
- למה משתמשים ב-Access control ?
- מי משתמש ב-Access control ?

הקדמה

- Access control עובד ב-4 שכבות:

Application

Middleware

Operating system

Hardware

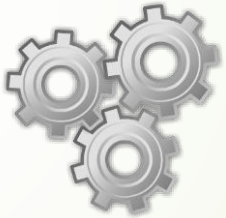
הקדמה

- Access control עובד ב-4 שכבות:
  - Application: אישור מנהל להחזר כספי.
  - Middleware: ניהול חשבון בבנק.
  - Operating system: קבצים.
  - Hardware: גישה לכתובות בזיכרון.

Access control במערכת הפעלה

- מערכת הפעלה מספקת בקרת גישה ל-principals.
- Principal יכול להיות:

משתמש



תהליך יישום

מחשב

קבוצה

Access control במערכת הפעלה

- אפשר לשמור את הנתונים של access control במטריצה.

User	Operating System	Accounts Program	Accounting Data
Sam	rwx	rwx	rw
Alice	x	x	rw
Bob	rx	r	r

- איפה נמצאת הבעיה בתכנון ההרשאות ?

Access control במערכת הפעלה

- הפתרון: הוספת תהליך שיטפל ב-Accounting Data

User	Operating System	Accounts Program	Accounting Data
Sam	rwx	rwx	r
Alice	rx	x	-
Accounts Program	rx	r	rw
Bob	rx	r	r

Access control במערכת הפעלה

- דרך אחרת לשמור נתונים של access control: Access Control Lists (ACLs)

User	Accounting Data
Sam	r
Alice	-
Accounts Program	rw
Bob	r

Access control במערכת הפעלה

- דרך אחרת לשמור נתונים של access control: Capabilities

User	Operating System	Accounts Program	Accounting Data
Bob	rx	r	r

קבוצות ותפקידים

- אפשר לכווץ בנתונים של access control ע"י:
  - קבוצות
  - תפקידים

Access control במערכת הפעלה Unix

- ב-Unix, לקבצים ותיקיות יש מאפיינים מסוג "rwx".
- המאפיינים מתייחסים ל-:
  - בעל הקובץ / תיקייה.
  - קבוצה.
  - כל העולם.

<<FLAGS>> “Owner” “Group”

- ב-Linux, חשבון root מופעל.

Access control במערכת הפעלה Unix

- Flags (empty):

Directory / File	Owner	Group	World
-	---	---	---

- Flags (full):

Directory / File	Owner	Group	World
d	rwx	rwx	rwx

- -rw-r----- Alice Accounts

Directory / File	Owner	Group	World
-	rw-	r--	---

Access control במערכת הפעלה Apple OS/X

- כדומה ל-Unix, Apple OS/X מתייחס לקבצים ותיקיות באופן דומה.

- ב-Apple OS/X:
  - יש הגנה על הזיכרון.
  - כברירת מחדל, חשבון root מופסק.

Access control במערכת הפעלה Microsoft Windows

- מאפיינים נוספים:
  - "AccessDenied"
  - "AccessAllowed"
  - "SystemAudit"
- "everyone" הינו principal.

Access control במסדי נתונים

- מסובך יותר מזה של מערכת הפעלה.
- נתונים של access control נשמרים כשילוב של:
  - Access control lists.
  - Capabilities.

הגנה על החומרה

- "Rings of Protection"
- "Trusted Computing": הוספת צ'יפ Trusted Platform Module.

מנגנונים אחרים

- Sandboxing
- Virtualization

שיבושים

- למרות כל המנגנונים מקודם, ייתכנו שיבושים:
  - "Unix Finger command"
  - SQL insertion attacks.
  - כשלים בממשק המשתמש.
    - Trojan Horse.
    - תוכנה בשם זהה לפקודה במערכת.

שיבושים

בכל זאת, כשלים... למה ?

סיכום

תכנון חכם של access control יכול למנוע התקפות זדוניות וקשות

תודה על ההקשבה...