# MULTILEVEL SECURITY

## CHAPTER 8 IN SECURITY ENGINEERING
## AMIR SHWARTZ


https://www.centos.org/docs/5/html/Deployment_Guide-en-US/sec-mls-ov.html

# MULTI-LEVEL SECURITY

- מערכות-מחשוב כוללות לרוב מידע רגיש.
- יש צורך בסיסי לאבטח את המידע כך שלא ייחשף לגורם לא-רצוי.
- שיקולים עיקריים לאבטחת-מידע:
  - פרטיות.
  - בטחון.
  - מידע עסקי בעל ערך.

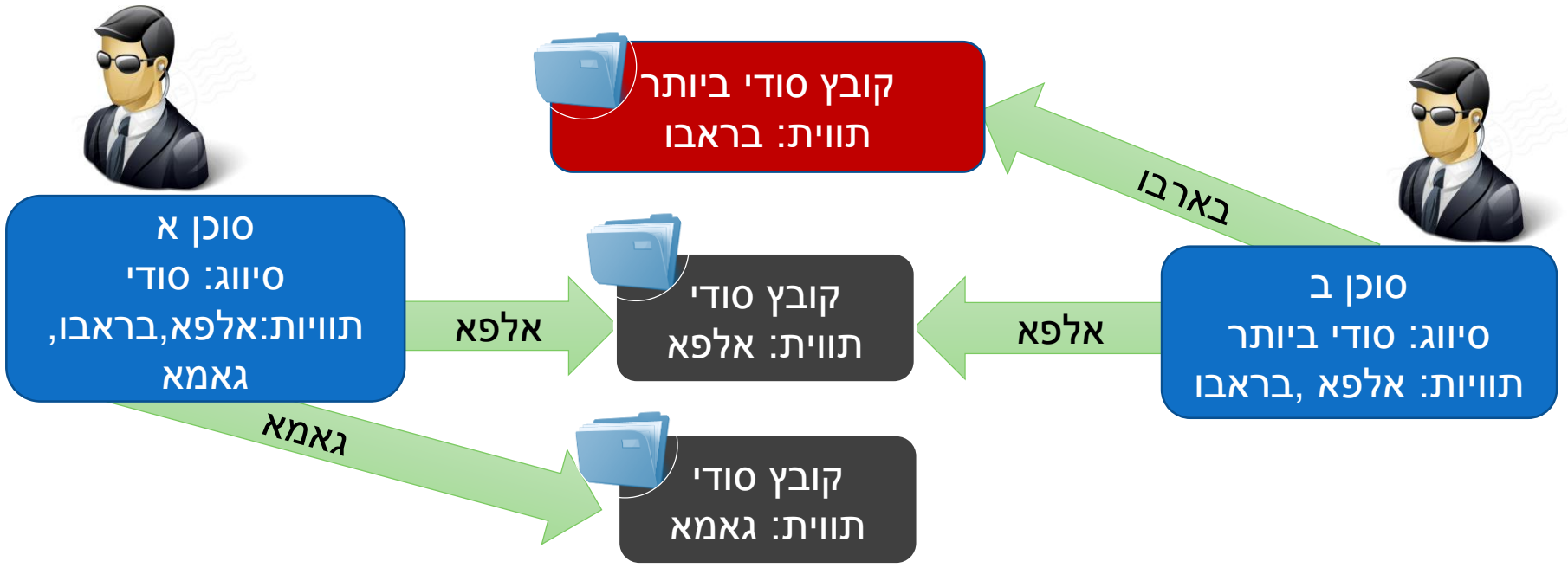
# MULTI-LEVEL SECURITY


- בעקבות מלחמת העולם ה-II והמלחמה הקרה, מעצמות NATO קבעו סכמת סימון מסמכים לפי **רמות סיווג**: לא-מסווג, שמור, סודי, סודי ביותר.
- גישה למסמך ניתנה רק מי שהיה בעל **רמת סיווג** גבוהה לפחות כמו סיווג המסמך.
- **שימוש בתוויות:** (מילות-קוד) שמאפשר הפרדה לפי רלוונטיות מבצעית.
- מכאן נולד הצורך ב- MULTI-LEVEL SECURITY **בקיצור: MLS**



https://www.centos.org/docs/5/html/Deployment_Guide-en-US/sec-mls-ov.html

# MLS – דוגמא


קובץ סודי ביותר
תווית: בראבו
סוכן א
סיווג: סודי
תוויות:אלפא,בראבו,
גאמא
קובץ סודי
תווית: אלפא
סוכן ב
סיווג: סודי ביותר
תוויות: אלפא ,בראבו
קובץ סודי
תווית: גאמא
בארבו
אלפא
אלפא
גאמא

# מדיניות אבטחה

- כשבאים לתכנן מערכת "מאובטחת" יש להגדיר **מדיניות-אבטחה**.

- **מדיניות-אבטחה:** מגדירה במדויק מה מנגנון האבטחה במערכת באים להשיג.
  - מציינת במפורש את סוג המידע שכל משתמש רשאי לגשת.
  - מצריכה הבנה טובה של האיומים הקיימים נגדם יש להגן.
  - לרוב הגדרתה לא מבוצעת כראוי.

# מדיניות אבטחה - דוגמא

דוגמא למסמך מדיניות אבטחה של מערכת נתונה:

1. מדיניות האבטחה מאושרת על-ידי ההנהלה.
2. כל העובדים מחויבים למלא אחר מדיניות האבטחה.
3. המידע יהיה זמין רק לעובד בעל-צורך להכיר אותו.
4. כל פגיעה במדיניות האבטחה תדווח מיד לצוות האבטחה.

האם ניתן להבין מהמסמך מה מדיניות האבטחה במערכת?

# מדיניות אבטחה - פירוט

מדיניות אבטחה תורכב מהחלקים הבאים:

- **מודל מדיניות האבטחה:** תיאור תמציתי של מאפייני ההגנה ומטרות ההגנה כפי שהוסכם ע"י ההנהלה.
- **מטרת האבטחה:** תיאור מפורט של מנגנוני ההגנה תוך התייחסות לאופן המימוש. מהווה בסיס לבדיקות והערכת המערכת.
- **פרופיל הגנה:** תיאור של מנגנוני ההגנה באופן כללי. בלתי-תלוי במימוש. מאפשר השוואה בין מערכות שונות.
  דרישת-חובה בתקן Common Criteria.

**Common Criteria:** תקן בינלאומי להסמכת רמת-אבטחה של מערכות. מהווה ערובה לכך שמנגנוני האבטחה המוצהרים ע"י היצרן הוטמעו כראוי.

# בקרת גישה

- **הרשאה:** מתן אפשרות למשתמש לבצע פעולה במשאב מערכת.
  - לדוגמא קריאת קובץ, כתיבה לקובץ, הרצת תהליך.
- **בקרת גישה:** תפקידו לאכוף שימוש במשאבי המערכת.
  - באופן שרק משתמש מורשה יוכל לגשת למשאב מסוים (בהתאם למדיניות האבטחה)

- **TCB:** אוסף הרכיבים שמבצע את האכיפה בפועל (**Trusted Computing Base**).
  - רכיב TCB יכול להיות רכיב תוכנה, חומרה או קושחה (firmware).
  - תקלה באחד הרכיבים עלולה לחשוף פרצה במדיניות האבטחה.

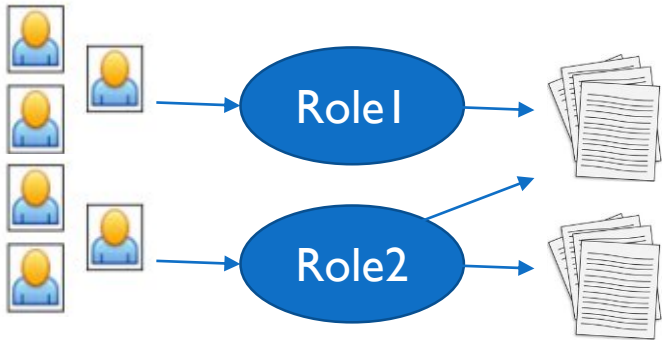
- נראה מספר מודלים של בקרת גישה.

# מודלים של בקרת גישה

- **Discretionary Access Control - DAC**
  **(בקרת גישה תלוית שיקול-דעת)**
  - הרשאת גישה למסמך נקבעת ישירות לכל משתמש.
  - משתמש בעל הרשאה למשאב יכול לאפשר או למנוע ממשתמש אחר לגשת אליו.
  - בקרת גישת קבצים ב-UNIX מבוסס על מודל זה.

- **Mandatory Access Control - MAC**
  **(בקרת גישה מחויבת)**
  - מדיניות האבטחה מחייבת את כל המשתמשים והם כפופים לכלליה.
  - אין למשתמש יכולת לשנות הרשאת גישה למשאב באופן שיפר את מדיניות האבטחה.

# מודלים של בקרת גישה




- **Role-Based Access Control - RBAC**
  **(בקרת גישה תלוית תפקיד)**
  - ההרשאה למשאבים ניתנת על פי הגדרת תפקיד.
  - משתמש משויך לתפקיד.
  - כך מורשה לגשת למשאבים הדרושים לביצוע עבודתו.

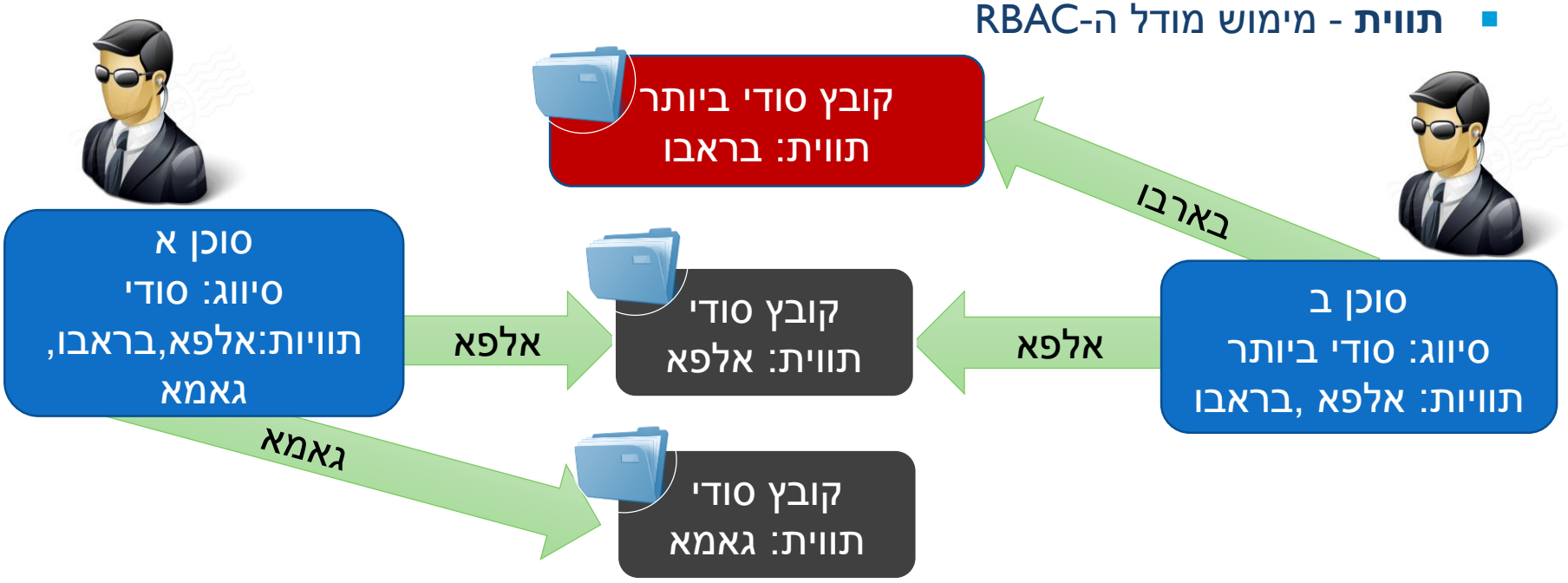
- **Type Enforcement – TE**
  **(בקרת גישה תלוית אכיפת-סוג)**
  - מדיניות-האבטחה מגדירה במפורש זוגות:
    **תהליך-סוג:** תהליכים שמורשים לגשת למשאבים מסוגים שונים.

| | File Types | | |
|---|---|---|---|
| **Process Domains** | Web pages | Mailbox file | Mail Aliases |
| WWW Server | r | | |
| Mail System | | rw | r |

http://www.blacksheepnetworks.com/security/info/misc/handbook/136-139.html

# שימוש במודלים

- **סיווג** - מימוש מודל ה-MAC
- **תווית** - מימוש מודל ה-RBAC



# מודלים של מדיניות אבטחה

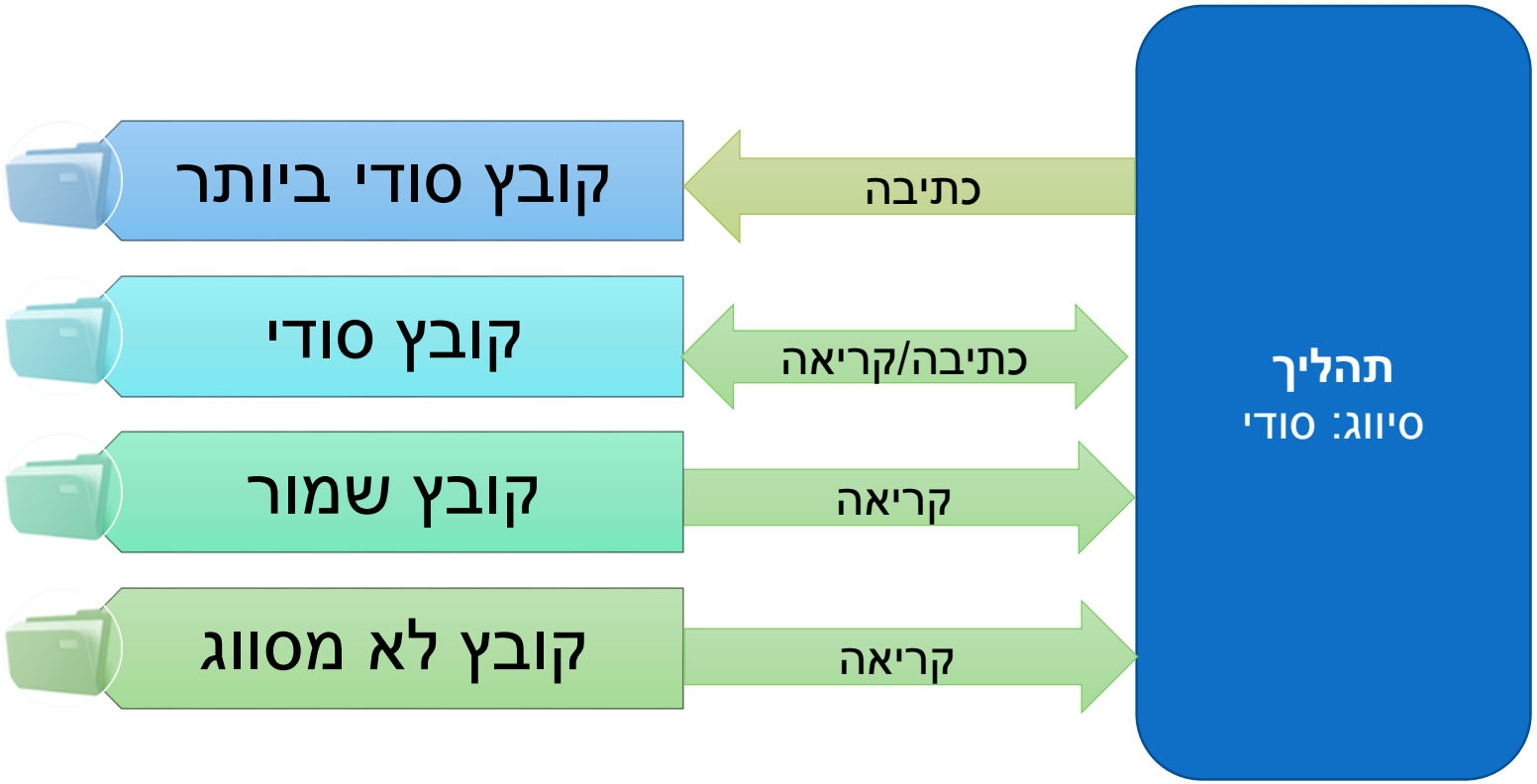
- בשנות ה-70 הבינו שמערכות-הפעלה קיימות סובלות מכשלי אבטחה חמורים.
- ריבוי חורי-האבטחה הגבירו את החשש מהשתלת קוד-עוין.
- **דו"ח אנדרסון** הדגיש את החשיבות בפיתוח **מנגנוני-אבטחה פשוטים**.
  - מדיניות-אבטחה שאינה מורכבת מדי.
  - מספר מצומצם של רכיבי TCB.
  - פשוטים לבדיקה והערכה.

# מודל BLP

- **[1973] מודל Bell-LaPadula (BLP)**
מודל שהוצע עבור חייל-האוויר האמריקאי.
- מאפשר להבטיח שמירה על חשאיות המידע במערכת.
- למודל BLP יש שני מאפיינים מרכזיים:
  - **מאפיין קריאה:** משתמש לא יכול לקרוא מידע ברמת סיווג גבוהה משלו.
  - **מאפיין כתיבה:** משתמש לא יכול לכתוב לרמת סיווג נמוכה משלו.

- מפשט את הערכת מצב-ההגנה במערכת.
(תוך התעלמות מצורך בשינוי רמת סיווג למידע קיים)

# מודל BLP






Based on:
https://www.centos.org/docs/5/html/Deployment_Guide-en-US/sec-mls-ov.html

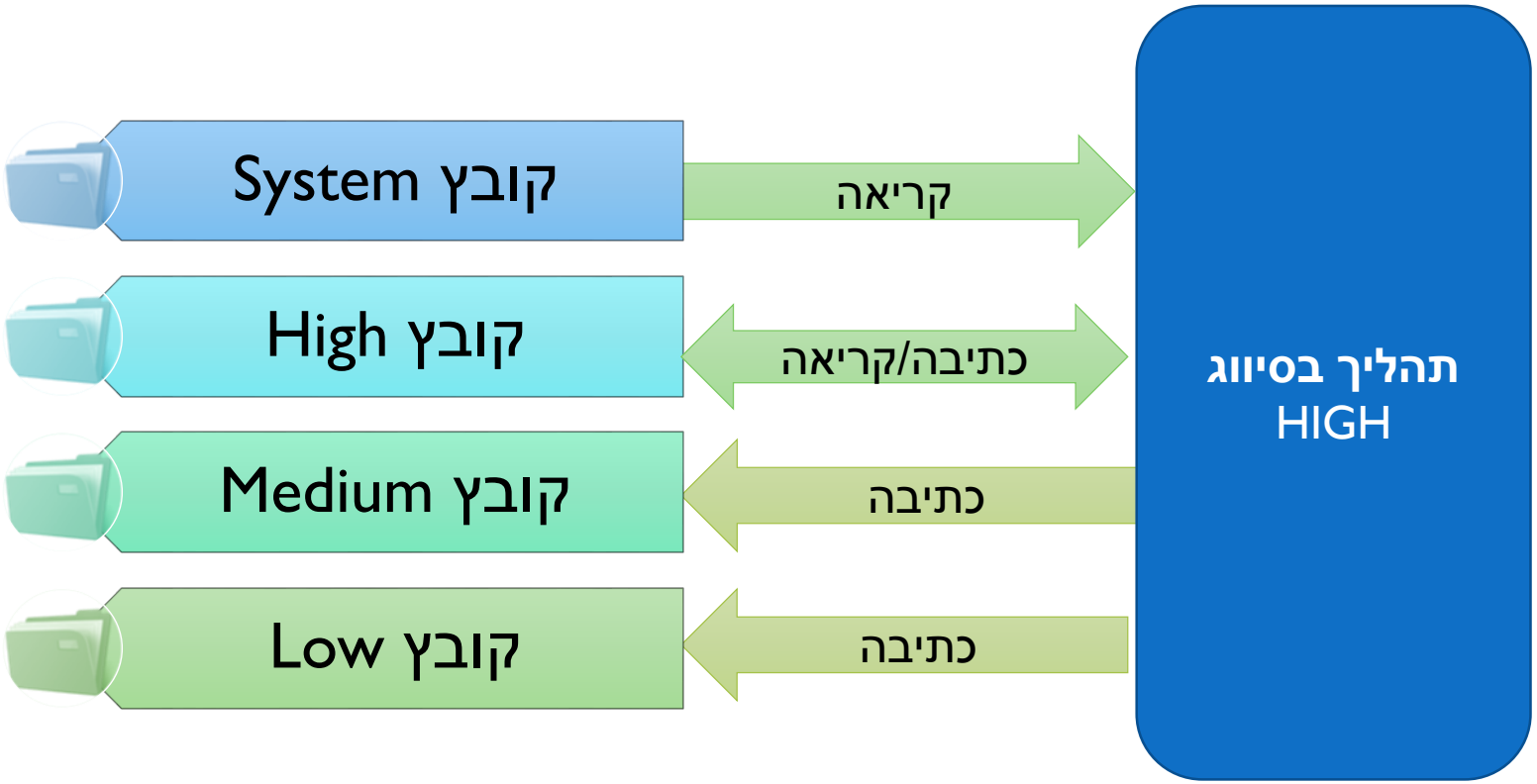
# מודל BLP - מימוש

- **System-Z:** הרחבה של BLP. ניסיון להגמיש את המודל.
- כל משתמש רשאי לבקש ממנהל-המערכת להוריד זמנית סיווג של קובץ מסוים.
- שינוי רמת סיווג נובע מצורך "לשבור" את מדיניות האבטחה לעתים.
- מבטא התייחסות ל**מאפיין שלווה** (Tranquility)
  - **מאפיין חזק:** רמת סיווג של תהליך/קובץ לעולם לא משתנה.
  - **מאפיין חלש:** רמת סיווג עשויה להשתנות כל-עוד לא נעשית עבירה על מדיניות האבטחה.

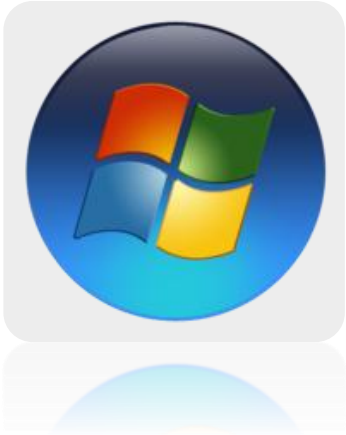
# מודל BIBA

- **[1975] מודל BIBA:** מכונה גם "BLP הפוך"
- מאפשר להבטיח שמירה על שלמות המידע. מתעלם מחשאיות.
- מאפייני BIBA:
  - **מאפיין קריאה:** משתמש לא יכול לקרוא מידע ברמת סיווג נמוכה משלו.
  - **מאפיין כתיבה:** משתמש לא יכול לכתוב לרמת סיווג גבוהה משלו.
- **שמירה על שלמות**: תהליך ברמת סיווג גבוהה לא ייחשף לתוכן "באמינות נמוכה" כי נכתב ברמת סיווג נמוכה ממנו.
- **אין חשאיות.** למה?

# מודל BIBA


קובץ System
קובץ High
קובץ Medium
קובץ Low
קריאה
כתיבה/קריאה
כתיבה
כתיבה
תהליך בסיווג
HIGH

# מודל BIBA - מימוש



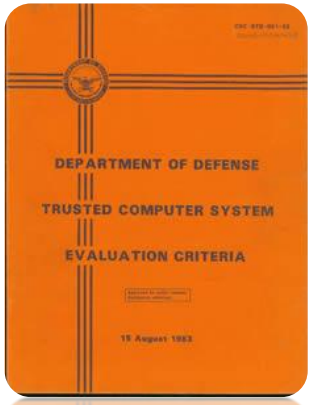
- **Windows Vista:** המערכת נחלקת לרמות סיווג:
  - מערכת הפעלה: SYSTEM
  - מנהל-מערכת: HIGH
  - תהליכי-משתמשים: MEDIUM
  - תהליך דפדפן Internet-Explorer: LOW
- תהליך שהמשתמש הוריד מהרשת דרך IE יעלה מ-LOW רק באישור המשתמש.

- VISTA זנח את איסור-הקריאה למטה לצרכים פרקטיים (אין שלמות).
- הקשחה של VISTA : ניתן להוסיף איסור קריאה-למעלה (חשאיות)

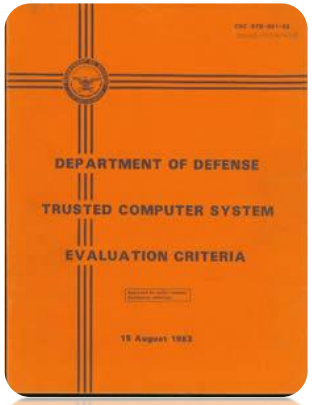
# SCOMP והספר הכתום

- **SCOMP [1983]:** מערכת תקשורת של משרד-ההגנה האמריקאי.
  - שימשה לאבטחת מידע על דואר ותקשורת-מסרים צבאיים.
  - מידע עבר בכיוון-אחד: מרמת סיווג נמוכה לרמת סיווג גבוהה.
  - הופכת למערכת הפעלה מסחרית כשנרכשת ע"י Honeywell.
  - תרומתה הגדולה כשהיוותה מודל מוצלח עבור "הספר הכתום".

- **הספר הכתום [1985]**:
  - תקן אמריקאי שקבע קריטריונים לרמת-אבטחת של מערכות.
  - היווה השראה על ממשלות נוספות: ביניהן בריטניה, גרמניה וקנדה.
  - בשנת 2000 הוצא משימוש. הוחלף ע"י Common Criteria



# SCOMP והספר הכתום



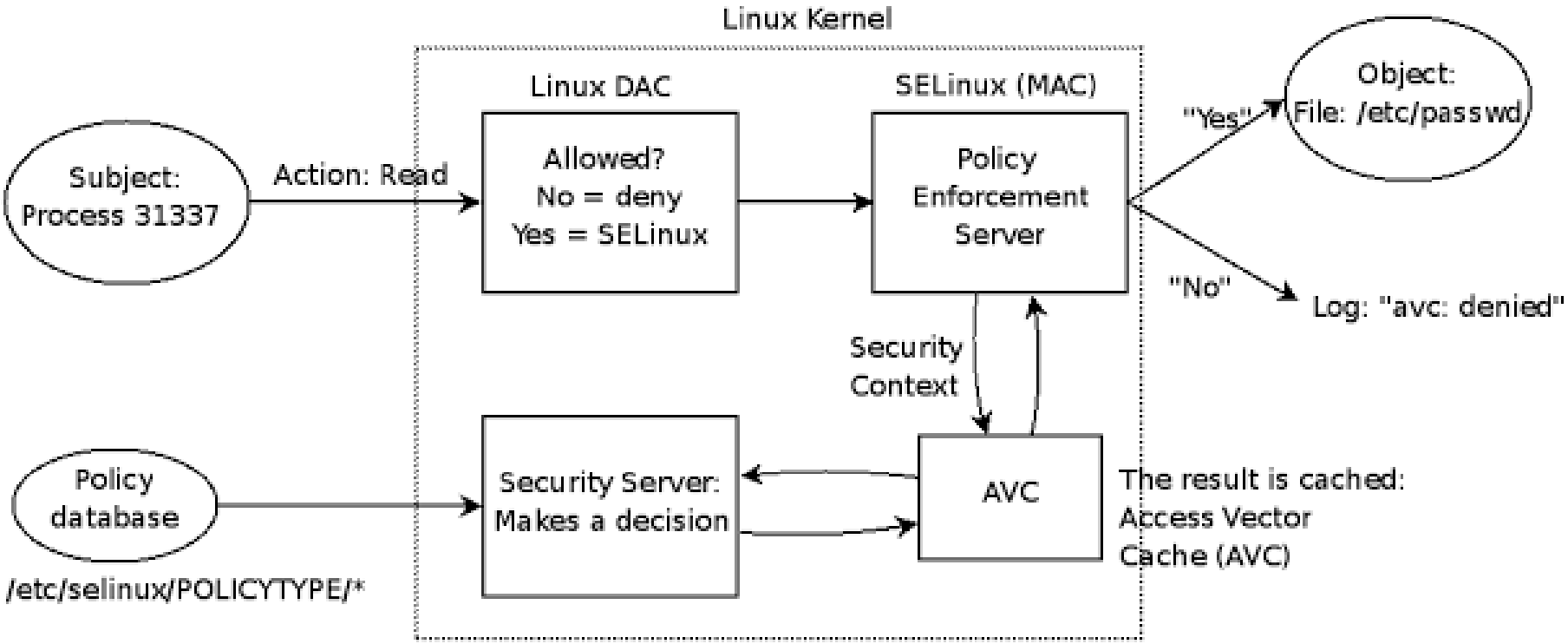

- **הספר הכתום** הגדיר עד כמה מערכת נחשבת אמינה על-פי דירוג:
  - **רמה A1:** רמת הגנה מאושרת.
    שימוש ב-MAC. מספק הוכחות פורמליות ליעילות TCB
  - **רמות B3 / B2 / B1:** הגנה מחויבת
    שימוש ב- MAC. שימוש ב-TCB פורמלי.
  - **רמות C2 / C1:** הגנה מבחינה
    שימוש ב-DAC.
  - **רמה D:** הגנה מינימלית.
- המערכת SCOMP הוגדרה ברמה A1 הגבוהה ביותר.

- הספר הכתום היה חלק מ-**"סדרת הקשת"**.

# SELINUX

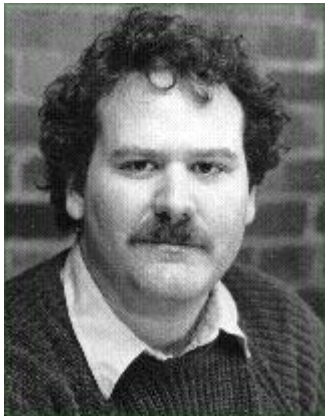
- **(Security-Enhanced Linux) SELinux [2000]**
  - פיתוח של ה-NSA. כולל התאמות במדיניות האבטחה לעומת לינוקס "קלאסי".
  - מציג מודל בקרת-גישה "משולב": DAC + MAC , RBAC , TE
  - כל תהליך רץ **במרחב מבודד** במערכת.
    הבידוד מונע מפגיעה בתהליך מסוים לחלחל ליתר החלקים במערכת.
  - בשנת 2003 מוזגה לתוך ה KERNEL הראשי של לינוקס.

# SELINUX




http://blog.larsstrand.no/2007/11/rhel5-selinux-benchmark.html

# MLS – בעיות



- **הוירוס הראשון:** ב-1983 פרד כהן הצליח להשתלט על מערכות MLS
  - לקח לו 8 שעות לכתוב קוד שפרץ למערכת שנחשבה מוגנת.
  - הקוד הסתתר בתוך תוכנת מחשב לגיטימית שהותקנה באמצעות דיסקט.
  - הגה לראשונה את המונח "וירוס מחשב" שכולנו מכירים.
- ניתן להשתלט על מערכת אם פורצים לאחד מרכיבי ה-TCB.
- תהליך בסיווג גבוה שנדבק יכול "להדליף" מידע לסיווג נמוכה תוך שימוש במשאב משותף. למשל כתיבה לתא בזיכרון, שינוי סיבובי-שעון במעבד.

# MLS – בעיות

## ריבוי-מופעים (Polyinstantiation)

- **דוגמא:** משתמש ברמה גבוהה מקצה לספינה מטען בסיווג "סודי". מה יראה משתמש ברמת סיווג נמוכה?
  - **המודל האמריקאי:** המערכת תציג "סיפור-כיסוי" לסוג המטען וליעד:

| Level | Cargo | Destination |
|---|---|---|
| Secret | Missiles | Iran |
| Restricted | — | — |
| Unclassified | Engine spares | Cyprus |

  - **המודל הבריטי:** המערכת תציג שהמטען והיעד בסיווג "שמור":

| Level | Cargo | Destination |
|---|---|---|
| Secret | Missiles | Iran |
| Restricted | Classified | Classified |
| Unclassified | — | — |

# MLS – העתיד: וירטואליזציה

- התקדמות הטכנולוגיה למחשוב וירטואלי מסייעת לייצר את ההפרדה הרצויה ב-MLS.
- ארגון ה-NSA פיתח גרסה מוקשחת של VMWare.
  - משלבת הרצת מכונות וירטואליות של Windows בתוך SELinux.
  - נהנית ממדיניות אבטחה מוקפדת של SELinux בשילוב עם פונקציונליות של יישומי Windows.

# סיכום

- ראינו מודלים למדיניות-אבטחה שמנסים לתת מענה לחשאיות ולשלמות המידע.
- הבנה עמוקה של היתרונות כמו גם המגבלות שלהן היא קריטית בתכנון ופיתח מערכת חדשה.