



TEL AVIV UNIVERSITY

מערכות הפעלה

מרצה: ערן טרומר
סמסטר א' תשע"ב

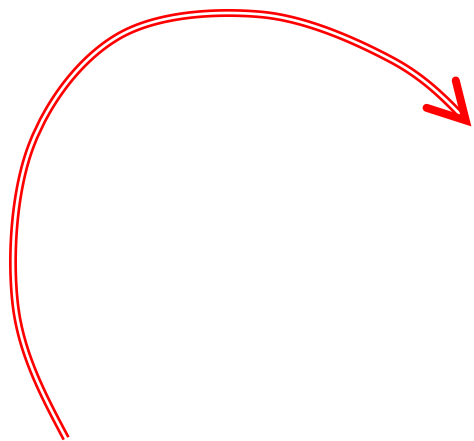
הרצאה 12

הגנה ואבטחה

הקדמה

- ❖ הסכנות האורבות למערכות מחשב: פריצות ותקיפות
 - מי שאינו משתמש לגיטימי מצליח לבצע פעולות
 - משתמש לגיטימי מצליח לבצע פעולות שאינו מורשה לבצע
 - גורם חיצוני גורם נזק בלי להשיג תועלת ישירה

- ❖ אימות זהות (authentication) : מי שם?
- ❖ הרשאות (permissions, access control): איזה פעולות מותרות לכל משתמש?
- ❖ מנגנוני רישום (logging) : מי עשה מה?
- ❖ הגברת הרשאות והתחזות מותרת



נזקים

❖ קריאת מידע על ידי מי שאינו מורשה

- מבחן, מידע פיננסי
- סיסמאות גישה, מפתחות הצפנה

❖ שינוי או הוספת מידע

- שינוי ציון, שינוי יתרה בבנק
- שינוי הרשאות

❖ מחיקת מידע

- תיק פלילי, עדויות לעבירה
- עדויות לפריצה

❖ מניעת שירות

- הפלת אתרי אינטרנט
- הפלת שרות ניטור

❖ שימוש במשאבים ללא תשלום

- כוח חישוב, נייר
- תקשורת

דרכי פריצה

❖ גישה פיזית לחומרה

- גניבה של מחשב או רק של דיסקים או סרטים
- ציטוט לקו תקשורת או לתקשורת אלחוטית
- חדירה לחדר מחשב שממנו ניתן להשתמש במחשב ללא אימות זהות

❖ התחזות (גניבת זהות של משתמש לגיטימי)

- מבחינת מערכת ההפעלה, מי שעובר את מנגנון אימות הזהות (סיסמה למשל) הוא משתמש לגיטימי

❖ הרצת קוד זדוני

- תוכנית שגורמת למשתמש לגיטימי לבצע פעולות שמותרות לו מבלי שהוא מודע לכך שהוא מבצע אותן
- הפעולות הללו משרתות את הפורץ (למשל שולחות לו מידע) ו/או מזיקות למשתמש הלגיטימי

❖ ניצול שגיאות בקוד קיים

- שליחת קלט הגורם לתוכנה אשר כבר רצה לפעול באופן לא מתוכנן
- כולל שגיאות במערכת ההפעלה עצמה

קוד זדוני (malware)

וירוסים, תולעים, סוסים טרויאניים ושאר חיות רעות

❖ קבצי הרצה שמגיעים כתוספת לדואל

- המשתמש מריץ תוכנית או פותח קובץ שמכיל גם קובץ הרצה
- הקוד הזדוני יכול לקרוא את רשימת כתובות הדואל המוכרות למשתמש, ולשלוח אל כל מכריו דואל דומה

❖ קבצים באתרי אינטרנט

❖ תוספים ותוכן דינמי בדפדפן

- plug-ins, ActiveX controls, Java applets וכו'
- דורשים אישור משתמש וחתימה אלקטרונית להרצה

❖ "הפתעות" בתוכנה לגיטימית

- תוכנות מסחריות ששולחות מידע פרטי חזרה לחברה
- Amazon "1984" recall, Sony rootkit

❖ ניצול שגיאות בקוד קיים כדי להריץ תוכניות אחרות

מינוח

- ❖ Bug
might be a
- ❖ Vulnerability
for which someone will write an
- ❖ Exploit
that hijacks control and runs
- ❖ Shellcode
that typically installs a
- ❖ Rootkit
that “Own” the computer and hides the traces,
often making the computer a part of a
- ❖ Botnet

הקטנת החשיפה לקוד זדוני

- ❖ הימנעות משימוש בתוכניות ממקור לא ידוע
 - סיכויים פחותים לסוס טרויאני בתוכנה של חברה ידועה משום שגם לחברה יש אינטרס למנוע הימצאות סוס טרויאני בתוכנה (בשמה)
- ❖ במקרים קיצוניים, הימנעות מהרצת תוכנה שלא ניתן לבדוק את קוד המקור שלה
 - תוכנות פופולריות עם קוד פתוח נקראות על ידי רבים והסיכוי לסוס טרויאני קטן
- ❖ הרצת תוכנות שרת שעלולות להיות חשופות לתקיפה (שרתי HTTP למשל) עם הרשאות מינימליות לביצוע תפקידן
- ❖ שימוש בתוכניות אנטי-וירוס אשר מזהות קוד זדוני מוכר, או דפוסי פעולה לא נורמליים
- ❖ ביקורות על גישה לקבצים ועל מידע שיוצא לרשת

תקיפות מניעת שירות (Denial of Service)

- ❖ שימוש אינטנסיבי במשאבים שגורם למניעת שירות או מתן שירות איטי למשתמשים לגיטימיים
- ❖ בדרך כלל התקיפה מתבצעת על ידי שימוש בשירות שניתן לכל מחשב ברשת, לא רק לקבוצת משתמשים קטנה, למשל
 - שרתי HTTP מספקים קבצים לכל דורש
 - שרתי דואר אלקטרוני מוכנים לקבל דואר מכל מקור
- ❖ הצפת שרתים כאלה בבקשות שירות מאיטה או מפילה את השרת
 - נפילות בגלל פגמים שלא מתגלים תחת עומס רגיל או בגלל מיצוי של משאבים, כמו קבצי יומן אירועים שממלאים את הדיסק
- ❖ קשה למנוע כאלה תקיפות כי הבקשות לגיטימיות באופיין

אימות זהות: סיסמאות

- ❖ מחרוזת שרק המשתמש הלגיטימי יודע
- ❖ אמצעי זיהוי נוח ואמין
- ❖ אנשים נוטים לשכוח סיסמאות שאינם משתמשים בהן בתדירות
- ❖ אנשים רושמים סיסמאות קשות לזכירה או שמתחלפות תדיר
 - פורצים עלולים למצוא או לגנוב את הרישומים הללו
- ❖ אנשים בוחרים סיסמאות צפויות אם נותנים להם לבחור
 - שמות פרטיים, ימי הולדת, וכדומה

גניבת סיסמאות

- ❖ ניחוש (אם הן קלות)
- ❖ בדיקת סיסמאות רבות באופן אוטומטי על ידי תוכנית
 - אפשרי אם ניתן להפעיל את תוכנית ההתחברות באופן לא אינטראקטיבי
- ❖ ציטוט לסיסמה כאשר היא עוברת ברשת או בקו תקשורת
- ❖ גישה לקובץ שסיסמאות רשומות בו
- ❖ שימוש במידע שדולף ממנגנון בדיקת הסיסמה (מעבר לכן/לא)
 - דוגמה: פריצת סיסמאות ב-Tenex בעזרת חריגי דף
- ❖ הרצת תוכנית שמתחזה לתוכנית ההתחברות הרגילה של המחשב וקולטת את שם המשתמש והסיסמה שלו

התגוננות מגניבת סיסמאות

- ❖ להכריח משתמשים לבחור סיסמאות ארוכות וקשות לניחוש
 - ניתן גם להכריח משתמשים להחליף סיסמאות לעיתים קרובות
 - בומרנג: אנשים נוטים לרשום הסיסמאות קשות או משתנות תדיר
- ❖ מנגנון בדיקת הסיסמאות צריך לענות רק כן/לא ולא לאפשר ניסיונות התחברות חוזרים מהירים
- ❖ סיסמאות צריכות להיות מועברות בקווי תקשורת ולהיות שמורות בקובץ בצורה מוצפנת
 - מערכת ההפעלה שומרת רק פונקציה $f(p)$ של הסיסמה p . בכל פעם שהמשתמש מקליד את p מחשבים מייד את $f(p)$ על מנת לבדוק את הסיסמה, ומוחקים מייד את p מהזיכרון
 - עדיין פגיע לחיפוש ממצה, לכן קובץ הסיסמאות צריך להיות מוגן מפני קריאה על ידי משתמשים רגילים (`/etc/passwd` /עומת `/etc/shadow`)
- ❖ מנגנון הפעלה מיוחד, בלתי ניתן להתחזות, לבקשת סיסמה: Security Attention Key (בחלונות: `Ctrl+Alt+Del`)

אימות זהות: אתגרים וסיסמאות חד-פעמיות

❖ סיסמה חד פעמית:

- דף מודפס שבכל התחברות משתמשים בסיסמה אחרת שבו
- מחשבון מיוחד שמייצר סיסמה חדשה כל פרק זמן קצר (כדקה)
- המחשב יודע מהי הסיסמה הבאה בסדרה או הסיסמה לכל נקודת זמן
- ציטוט אינו מאפשר התחברות

❖ אתגר

- מחשבון שעונה על חידות שהמחשב שמתחברים אליו מציג
- המחשב יודע מה התשובה הנכונה לכל חידה (תלוי בזמן ובמחשבון)
- ❖ בשני המקרים: אימות זהות על ידי הוכחת בעלות על חפץ פיזי
- ❖ בדרך כלל בשילוב סיסמה רגילה למניעת פריצה על ידי גניבת החפץ
- ❖ שיטה יקרה (מחשבוני), מסורבלת ליישום ושימוש, אך בטוחה

אימות זהות ביומטרי

❖ זיהוי אדם על פי תכונות פיזיות: מאפייני קול, טביעת אצבע, פנים, נימי דן ברשתית, צורת כף היד וכו'

❖ לחלק מהתכונות דרושים אמצעי קלט מיוחדים, לאחרים רק מיקרופון או מצלמה

❖ אחוז טעויות מסוים בדרך כלל

▪ סירוב למשתמש לגיטימי או אישור מתחזה

❖ ניתן לעיתים לשטות במנגנון האימות על ידי הצגת הקלטה/תמונה/בובה של המשתמש

▪ יש דרכים להתגבר על כך, למשל על ידי כך שמבקשים מהמשתמש

לומר משפט אקראי ובודקים גם את תוכן הדברים וגם את חתימת הקול

❖ ייחודי אבל לא בהכרח סודי; בלתי ניתן להחלפה

