הרצאה מס' (3)

כלי אבטחה: אימות, בקרת גישה וקריפטוגרפיה.

1)

Authentication

אימות

LECTURE 3

2)

Security tools: authentication, access control and cryptography

A security professional analyzes situations by finding threats and vulnerabilities to the confidentiality, integrity, and/or availability of a computing systems.

Often, controlling these threats and vulnerabilities involves a policy that specifies *who* (which subjects) can access *what* (which objects) *how* (by which means).

The property of accurate identification is called authentication.

איש מקצוע באבטחת מנתח מצבים על ידי מציאת איומים ופגיעויות לסודיות, לשלמות ו/או לזמינות של מערכות מחשוב.
לעיתים קרובות, שליטה באיומים ופגיעויות אלו כרוכה במדיניות המפרטת מי (אילו נושאים) יכולים לגשת לאילו (אילו אובייקטים) כיצד (באילו אמצעים).
המאפיין של זיהוי מדויק נקרא אימות.

זיהוי לעומת אימות

3)

Identification vs. Authentication

- Identification is the act of asserting who the person is.
- Authentication is the act of proving that asserted identity: that the person is who he says he is.
- The two concepts of identification and authentication are easily and often confused. Identities, like names, are often well known, public and not protected. On the other hand, authentication is necessary protected. If someone's identity is public, anyone can claim to be that person. What separates the pretenders from the real person is proof by authentication.

- הזדהות היא מעשה הקביעה מיהו האדם.
- אימות הוא מעשה ההוכחה על אותה זהות: שאדם הוא מי שהוא אומר שהוא.
- שני המושגים של זיהוי ואימות מתבלבלים בקלות ולעיתים קרובות. זהויות, כמו שמות, ידועות היטב, פומביות ולא מוגנות. מנגד שני, אימות בטוח מוגן. אם זהותו של מישהו היא ציבורית, כל אחד יכול לטעון שהוא אותו אדם. מה שמפריד בין המתחזים לאדם האמיתי הוא הוכחה על-ידי אימות.

מנגנוני אימות

4)

Authentication mechanisms

Authentication mechanisms use any of three qualities to confirm a user's identity:

- Something the user *knows*. Passwords, PIN numbers, passphrases, a secret handshake, and mother's maiden name are examples of what a user may know.
- Something the user *is*. These authenticators, called biometrics, are based on a physical characteristics of the user, such as a fingerprint, the pattern of a person's voice, or a face (picture).
- Something the user has. Identity badges, physical keys, a driver's license are examples of things people have that make them recognizable.

מנגנוני אימות משתמשים בכל אחד משלוש איכויות כדי לאשר את זהותו של המשתמש:

- משהו שהמשתמש יודע. סיסמאות, מספרי PIN, ביטויי סיסמה, לחיצת יד סודית ושם הנעורים של האם הם דוגמאות למה שמשתמש עשוי לדעת.
- משהו שהמשתמש הוא. מאמתים אלו, המכונים ביומטריה, מבוססים על מאפיינים פיזיים של המשתמש, כמו טביעת אצבע, דפוס הקול של אדם או פנים (תמונה).
- מה שיש למשתמש. תגי זהות, מפתחות פיזיים, רישיון נהיגה הם דוגמאות לדברים שיש לאנשים שהופכים אותם לזהים.

התקפות והגנה על סיסמאות

5)

סיסמאות
Passwords

- Security questions — שאלות אבטחה
- Password use — שימוש בסיסמה
  - o *Use*. Supplying a password for each access to an object can be inconvenient and time-consuming.
  - o *Disclosure*. If a user discloses a password to an unauthorized individual, the object becomes immediately accessible.
  - o *Revocation*. To revoke one user's access right to an object, someone must change the password, thereby causing the same problems as disclosure.
  - o Loss. Depending on how the passwords are implemented, it may be impossible to retrieve a lost or forgotten password.

- שימוש. אספקת סיסמה עבור כל גישה לאובייקט יכולה להיות לא נוחה וגוזלת זמן.
- גילוי נאות. אם משתמש חושף סיסמה לאדם שאינו מורשה, האובייקט הופך להיות נגיש מיידית.
- ביטול. כדי לבטל את זכות הגישה של משתמש אחד לאובייקט, מישהו צריך לשנות את הסיסמה, וככה לגרום לאותן בעיות כמו הגילוי.
- אובדן. תלוי באופן היישום של הסיסמאות, יתכן שאי אפשר לאחזר סיסמה שאבדה או נשכחה.

6)

Attacking and Protecting Passwords

The password guessing steps: — שלבי ניחוש הסיסמה

- no password
- the same as the user ID
- is, or is derived from, the user's name
- on a common word list (e.g., password, secret, private) plus common names and patterns (e.g., qwerty, aaaaaa)
- contained in a short college dictionary
- contained in a complete English word list
- contained in a short college dictionary with capitalizations (PaSsWorD) or substitutions (digit 0 for letter O, and so forth)

- אין סיסמה.
- זהה לזהות המשתמש.
- הוא או נגזר משם משתמש
- ברשימת מילים נפוצה (למשל סיסמה, סודי, פרטי) בתוספת שמות ודפוסים נפוצים (למשל, qwerty, aaaaa)
- הכלול במילון קצר של המכללות
- הכלול ברשימה מלאה של מילים באנגלית.
- כלול במילון קולג' קצר עם רישיות (PaSsWorD) או החלפות (ספרה 0 לאות O וכדומה).

(7)

Dictionary Attacks

Several network sites post dictionaries of phrases, science fiction characters , names, places, mythological names, Chinese words, Yiddish words, and other specialized lists. These list help site administrators identify users who have chosen week passwords, but the same dictionaries can also be used by attackers of sites that do not have such attentive administrators.

(8)

Inferring Passwords likely for a user

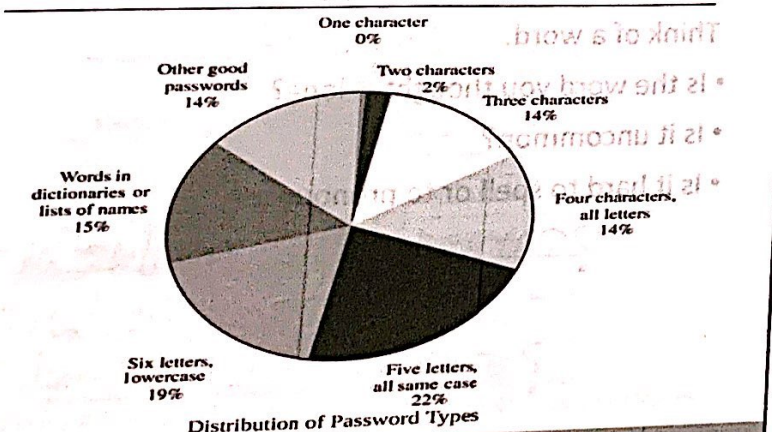
- Do we choose passwords at random?
- How long would it take for a computer to guess a personal password?

Password characteristics and types

Number	Percentage	Structure
15	<1%	Single ASCII character
72	2%	Two ASCII characters
464	14%	Three ASCII characters
477	14%	Four alphabetic letters
706	21%	Five alphabetic letters, all the same case
605	18%	Six lowercase alphabetic letters
492	15%	Words in dictionaries or lists of names
2831	86%	Total of all categories above

Password Characteristics

Password characteristics and types



Distribution of Password Types

Defeating Concealment

Easier than guessing a password is just to read one from table:

Identity	Password
Jane	qwerty
Pat	aaaaaa
Phillip	oct31witch
Roz	aaaaaa
Herman	guessme
Claire	aq3wm$oto!4

Sample Password Table

Guessing Possible Passwords

Think of a word.

- Is the word you thought is long?
- Is it uncommon?
- Is it hard to spell or to pronounce?

13)

Defeating Concealment

Operating systems store passwords in hidden (encrypted) form so that compromising the id-password list does not give immediate access to all user accounts.

Identity	Password
Jane	0x471aa2d2
Pat	0x13b9c32f
Phillip	0x01c142be
Roz	0x13b9c32f
Herman	0x5202aae2
Claire	0x488b8c27

Sample Password Table with Concealed Password Values

14)

Defeating Concealment

Identity	ID+password (not stored in table)	Stored Authentication Value
Jane	Jan+qwerty	0x1d46e346
Pat	Pat+aaaaaa	0x2d5d3e44
Phillip	Phi+oct31witch	0xc23c04d8
Roz	Roz+aaaaaa	0xe30f4d27
Herman	Her+guessme	0x8127f48d
Claire	Cla+aq3wm$oto!4	0x5209d942

Sample Password Table with Personalized Concealed Password Values

15) סיסמאות טובות

Good Passwords

If you do use passwords, we can improve their security by a few simple practices:

- *Use characters other than just a-z.*
- Choose long passwords.
- Avoid actual names or words.
- Use a string you can remember (UcnB2s), but don't be too obvious (I10v3U is already in the search file).

- אם אתה משתמש בסיסמאות, אנו יכולים לשפר את האבטחה שלהם על-ידי מספר שיטות פשוטות:
- השתמש בתווים שאינם רק a-z.
- בחר סיסמאות ארוכות.
- הימנע משמות או מילים נפוצות.
- השתמש במחרוזת שתוכל לזכור (כגון UcnB2s), אך אל תהיה ברור מדי (I10v3U כבר נמצא בקובץ החיפוש).

16) סיסמאות טובות

Good Passwords

- Use variants for multiple passwords (e.g., Ih1b2s – I have 2 brothers 1 sister – and append the other pattern: Ih1b2slvs – for Visa).
- Change the passwords regularly.
- Don't write it down.
- Don't tell anyone else.

- השתמש בווריאנטים לסיסמאות שונות (למשל, Ih1b2s – יש לי 2 אחים 1 אחות – והוסף את התבנית האחרת: Ih1b2slvs – עבור ויזה).
- שנה את הסיסמאות באופן קבוע.
- אל תכתוב אותם.
- אל תספר לאף אחד אחר.