תקשורת ומחשוב / אבטחת רשתות

פרק א' – מהי אבטחת רשתות

<u>עקרונות אבטחת רשתות</u>

- הצפנה, וכל השימושים השונים מלבד סודיות / פרטיות
- אימות
- שלמות המסר ונכונותו
- חלוקת מפתחות (הפצת מפתח)

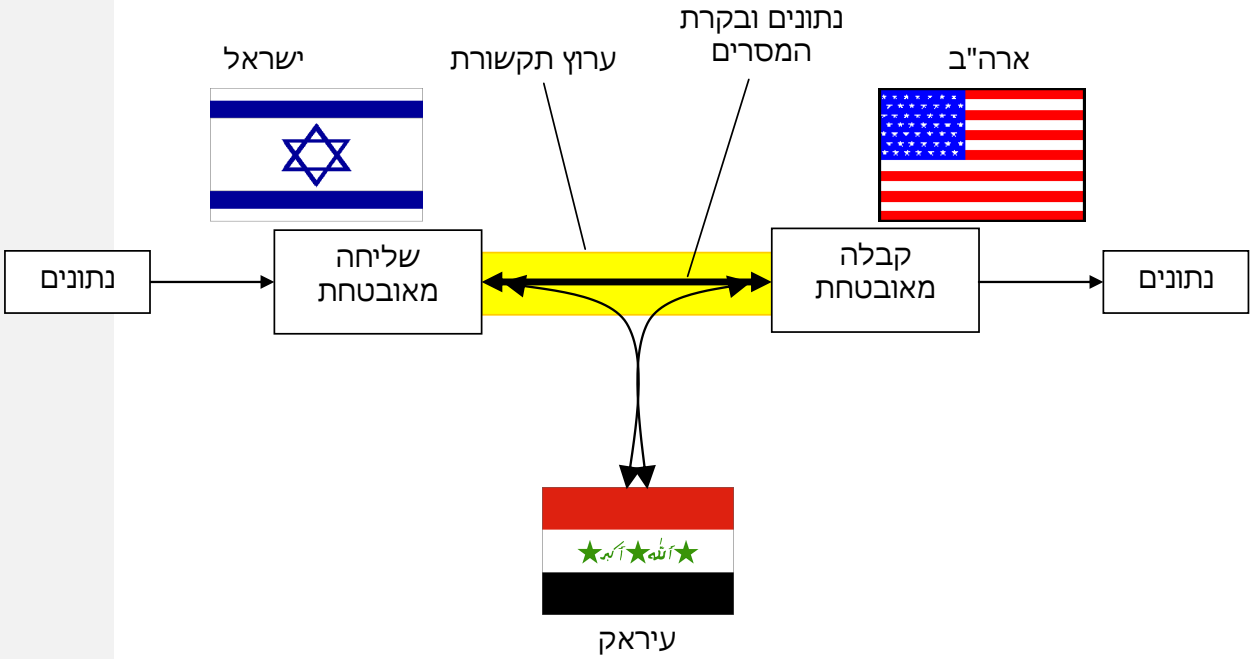
<u>אבטחה למעשה</u>

- FireWall
- אבטחה בישומים, בתעבורה, רשת, link layer

מה היא אבטחת רשתות?

באבטחת רשתות ישנם מספר אספקטים:
סודיות – רק השולח והנמען אמורים "להבין" את תוכן המסר באופן הבא: השולח מצפין את המסר ורק הנמען מסוגל לפענח אותו. כך נשמרת הפרטיות, כלומר – קיים מידור, כל אחד בענייניו הוא.
אימות – השולח והנמען מאשרים אחד את שהותו של השני.
שלמות ונכונות המסר – השולח והנמען מוודאים כי המסר הגיע ללא שינויים (בשידור או לאחריו) מבלי לחשוף את תוכן המסר בבדיקה.
גישה וזמינות – השירותים חייבים להיות נגישים וזמינים למשתמשים.

חברים ואויבים : ארה"ב ישראל ועיראק...



ארה"ב וישראל רוצות לתקשר ביניהן בצורה מאובטח, אולם עיראק עלולה לעכב / לשנות / להוסיף / למחוק מסרים.

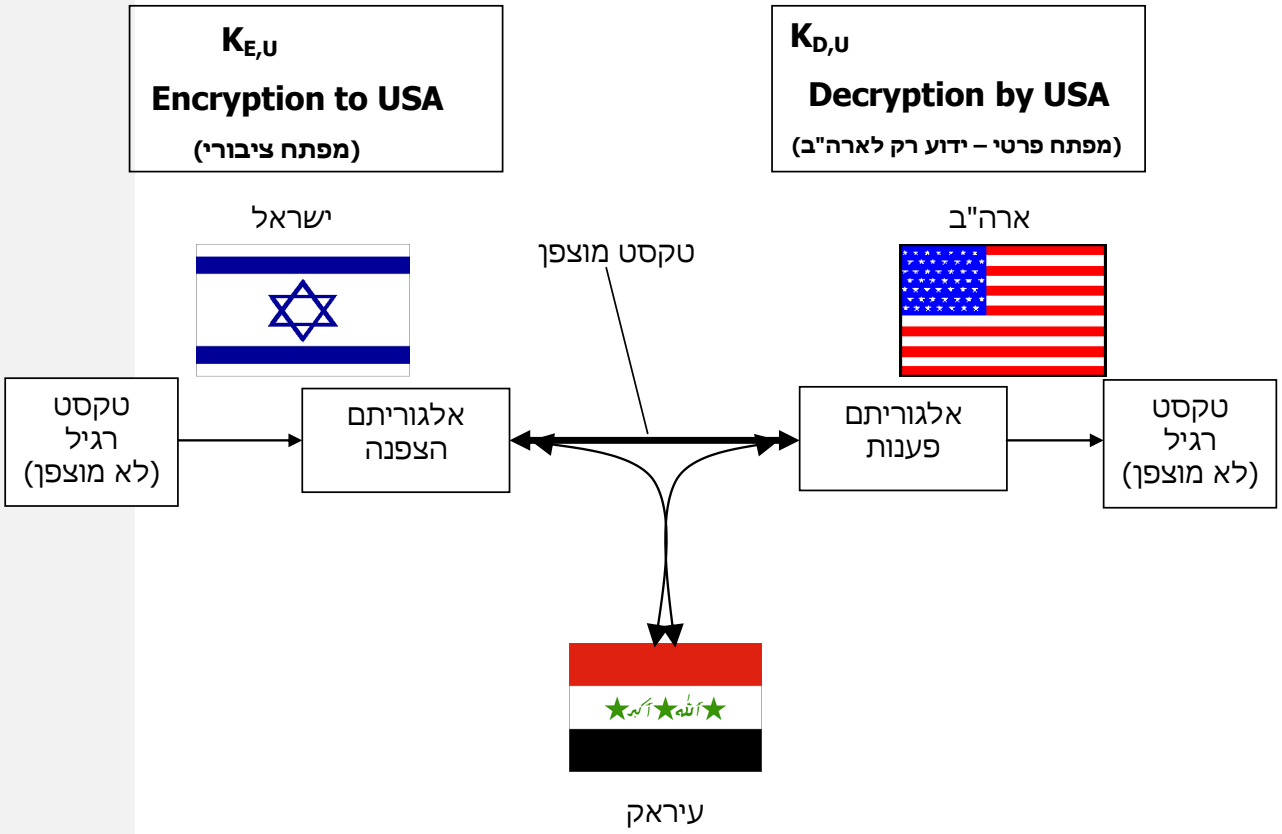
דוגמאות נוספות לצורך בתקשורת מאובטחת בין גופים שונים:

- חברות מסחריות - הגנה על סודיות מקצועית
- תקשורת בין מוסדות רפואיים - חיסיון רפואי
- תקשורת בין ארגונים מודיעיניים שונים , ובתוך הארגון עצמו - שמירה על מידור פנימי וחיצוני
- תקשורת בין בנקים
- שרתי DNS
- עדכון טבלאות בין נתבים
- קניות באמצעות הרשת – ע"מ למנוע גניבות
- ועוד..

מה עלול אויב ברשת לעשות?

- ציתות – אויב המצותת לקו התקשורת עלול לגרום לעיכוב ו/או מניעת הגעת המסרים לנמען.
- הכנסת מסרים כוזבים בשם השולח לנמען.
- התחזות - זיוף מקור המסר בחבילת המידע.
- חטיפה – השתלטות על ערוץ תקשורת ע"י הסרת אחד המשתמשים וכניסה במקומו.
- מניעת שימוש בערוץ התקשורת ע"י משתמשים אחרים (למשל, ע"י העמסת נתונים על הערוץ).

פרק ב' – עקרונות ההצפנה



סוגי הצפנות:

- הצפנת מפתח סימטרי – השולח והנמען מצפינים ומפענחים באמצעות אותו מפתח החייב להיות סודי.
- הצפנת מפתח ציבורי – הצפנה מתבצעת באמצעות מפתח ציבורי הידוע לכל, פענוח מתבצע ע"י מפתח סודי (אישי) לכל משתמש.

הצפנת מפתח סימטרי – פרוט:

צופן החלפה – החלפת תו אחד באחר.

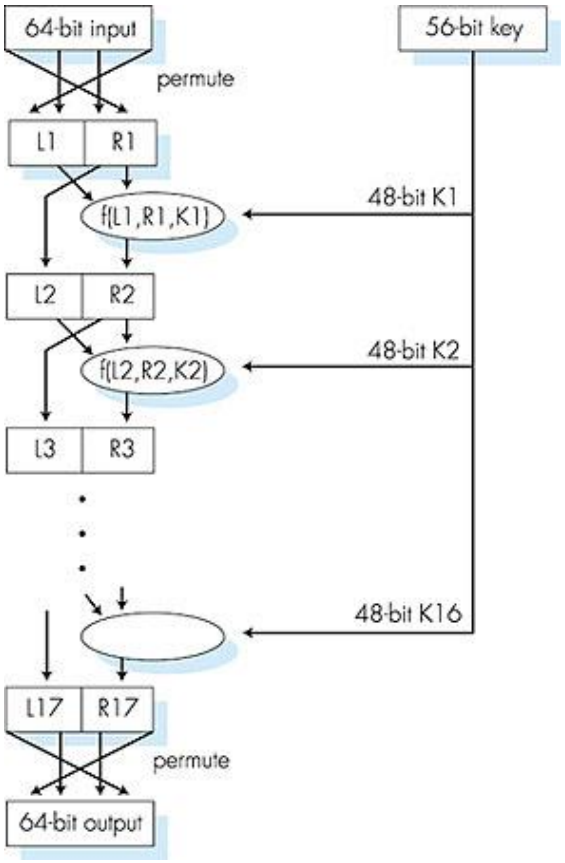
א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת - טקסט פשוט (לא מוצפן)

ת ש ר ק צ פ ע ס נ מ ל כ י ט ח ז ו ה ד ג ב א - טקסט מוצפן

ארה"ב. נתקוף מחר בבוקר. ישראל
תגצ"ש. יאדפו כסג ששפדג. נבגתכ

הצפנת סימטרית DES (Data Encryption Standart).

- סטנדרט הצפנה של ארה"ב (NIST 1993).
- מפתח סימטרי בגודל 56 ביט (2^{56} אפשרויות) וקלט טקסט פשוט בגודל 64 ביט.
- עד כמה מאובטח סטנדרט DES?
  - 56 ביט מוצפנים, דורשים 4 חודשי פענוח. כמו שנאמר : "הצפנה חזקה יוצרת עולם בטוח יותר.
  - לא קיימת "דלת אחורית" / שיטה חלופית לפענוח.



פעולת ה- DES

פרמוטציה התחלתית

נבצע 16 סיבובים זהים של פונקצית ההצפנה כך שבכל סיבוב נשתמש במפתחות שונים בגודל 48 ביט כל אחד.

בסופו של דבר, נקבל את הפרמוטציה הסופית.

הצפנה סימטרית מתקדמת – AES (Advanced Encryption Standard)

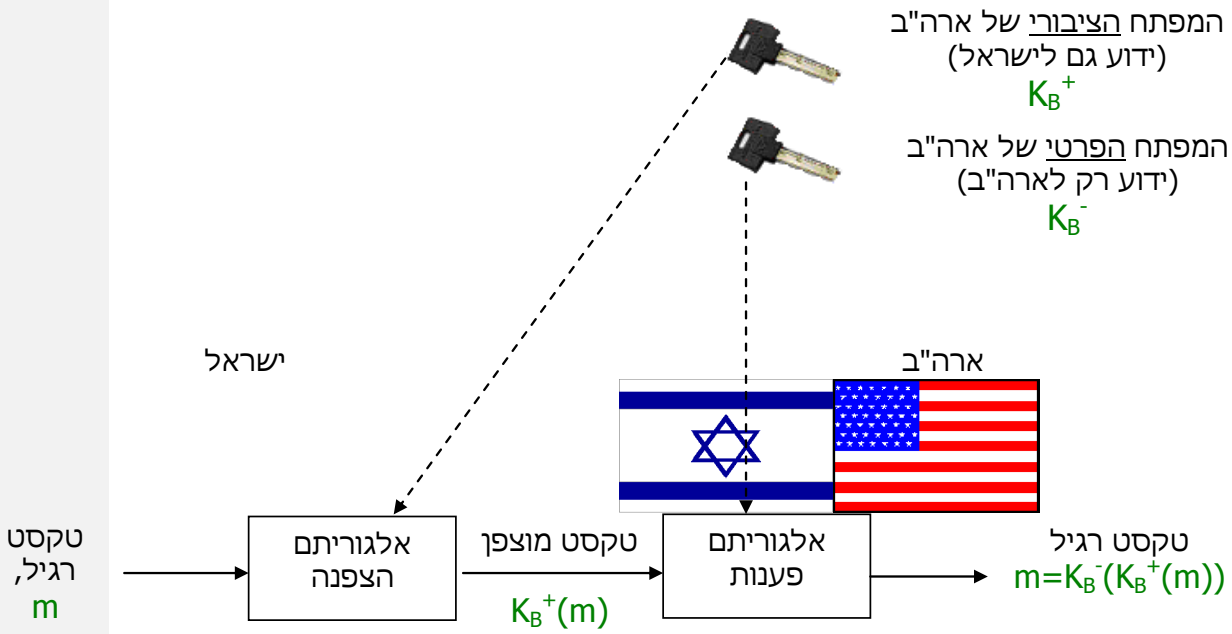
- בשל התחזקות המחשבים והפיכתם למהירים יותר, נאלצו להתקדם ל- AES המשתמש ב- 128 ביטים (2^{128} אפשרויות).
- מפתח סימטרי חדש (נוב' 2001) מחליף את ה- DES.
- מעבד בלוק מידע בגודל 128 ביט (לעומת 64 ביט ב- DES).
- מפתחות בגדלים שונים: 128,192,256 ביט.
- פענוח "בדרך הקשה" (מנסים כל מפתח) כך שפענוח שניה אחת ב- DES שווה ערך ל – 149 טריליון שנה לפענוח קוד זהה ב- AES.

הצפנת מפתח ציבורי – פרוט

- השולח והנמען בעלי אותו מפתח סודי.
- איך מסכימים שני הצדדים על מפתח זהה, במיוחד אם השולח והנמען מעולם לא נפגשו?

הצפנת מפתח ציבורי:

הגישה היא שונה לחלוטין, השולח והנמען אינם חולקים את אותו המפתח. המפתח הציבורי ידוע לכל, לעומת זאת, המפתח לפענוח הפרטי ידוע רק לנמען. שיטה זו יותר איטית.


המפתח הציבורי של ארה"ב
(ידוע גם לישראל)
K_B^+
המפתח הפרטי של ארה"ב
(ידוע רק לארה"ב)
K_B^-
ישראל
ארה"ב
טקסט
רגיל,
m
אלגוריתם
הצפנה
טקסט מוצפן
$K_B^+(m)$
אלגוריתם
פענות
טקסט רגיל
$m=K_B^-(K_B^+(m))$

אלגוריתמים להצפנת מפתח ציבורי

דרישות:

1. יש לוודא כי $K_B^+(...)$ ו- $K_B^-(...)$ יקיימו:

$$K_B^-(K_B^+(m)) = m$$

2. אם נתון מפתח ציבורי K_B^+ , חישוב המפתח הפרטי K_B^- צריך להיות בלתי אפשרי.

אלגוריתם Rivest, Shamir, Adelman – RSA

בחירת מפתחות:

1. בחר שני מספרים ראשוניים גדולים p, q (למשל 1024 ביטים כל מספר).
2. חשב : $n=p*q$, $z=(p-1)(q-1)$
3. בחר e (כך ש- $e < n$), אשר אין לו שום גורם משותף עם z (כלומר $g.c.d\ (z,e) = 1$).
4. מצא d כך ש- ed-1 מתחלק ב- z ללא שארית (כלומר $ed \bmod z = 1$).
5. מפתח ציבורי הוא $\underbrace{(n,e)}_{K_B^-}$ ומפתח פרטי הוא $\underbrace{(n,d)}_{K_B^+}$.

RSA – הצפנה ופענוח:

1. נתונים (n,e) ו- (n,d) כמחושב לעיל.
2. על מנת להצפין את המסר m יש לחשב:
$c = m^e \bmod n$ (כלומר, c יהיה השארית של חילוק m^e ב- n).
3. על מנת לפענח את המסר c יש לחשב:
$m = c^d \bmod n$ (כלומר, m יהיה השארית של חילוק c^d ב- n).

ניסים קורים!!

$$m = \underbrace{(m^e \bmod n)}_{C}{}^d \bmod n$$

דוגמא ל- RSA

ארה"ב בוחרת : $p = 5, q = 7$ $\Leftarrow$ $n = 35, z = 24$

בנוסף, תבחר ארה"ב $e = 5$ (יוצא: e , z זרים - כלומר: $g.c.d\ (z,e) = 1$)

נמצא $d = 29$ $(29*5 \mod 24 = 1)$

הצפנה:

אות	m	m^e	$c = m^e \mod n$
ל	12 (האות ה- 12 לפי הסדר הלקסיקוגרפי)	$12^5 = 1524832$	$152843 \mod 35 = 17$

פענוח:

c	c^d	$m = c^d \mod n$	אות
17	17^{29}	12	ל

כיצד מתרחש הנס כך ש- $(m^e \mod n)^d \mod n = m$?

נראה את החישוב, שלב אחר שלב:

<u>משפט עזר:</u>

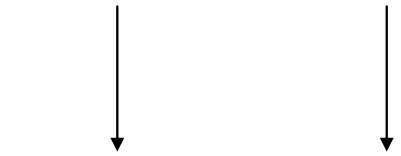
אם p , q ראשוניים, וכן $n = p*q$ אזי:

$$x^y \mod n = x^{y \mod (p-1)(q-1)} \mod n$$

$$(m^e \mod n)^d \mod n$$
$$= m^{ed} \mod n$$
$$= m^{ed \mod (p-1)(q-1)} \mod n$$
(נשתמש במשפט העזר)
$$= m^1 \mod n$$
= (ed mod (p-1)(q-1) = 1 מאחר ובחרנו)
$$= m$$

מאפיין חשוב נוסף של RSA:

$$K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$$



שימוש במפתח הפרטי תחילה ולאחר מכן במפתח הציבורי

שימוש במפתח הציבורי תחילה ולאחר מכן במפתח הפרטי

התוצאה תהיה זהה!

פרק ג' – אימות

ארה"ב רוצה שישראל תאמת את זהותה בפניה (תוכיח שזו אכן היא).

<u>פרוטוקול ap1.0:</u>

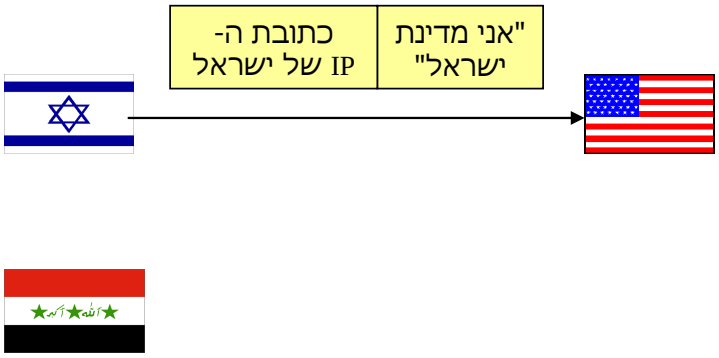
ישראל: "אני מדינת ישראל"

הבעיה היא, שברשת ארה"ב אינה יכולה "לראות" את ישראל ולכן עיראק יכולה להתחזות לישראל:

<u>פרוטוקול ap2.0:</u>

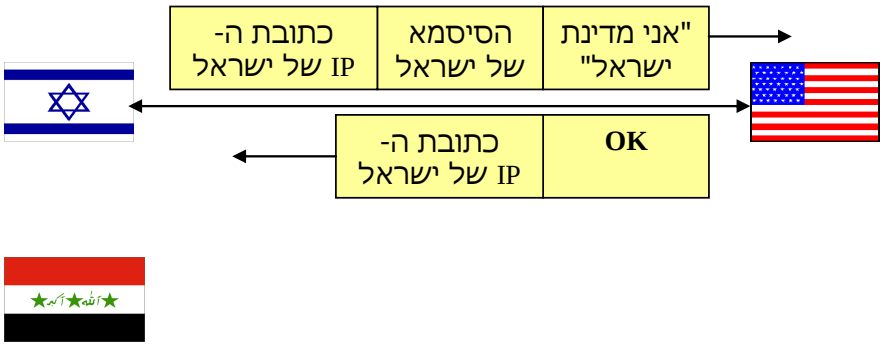
ישראל: "אני מדינת ישראל" => נשלח בחבילה המכילה את כתובת המקור (IP)

הבעיה היא, שעיראק יכולה להתחזות ולשלוח את ההודעה עם כתובת ה- IP של ישראל.

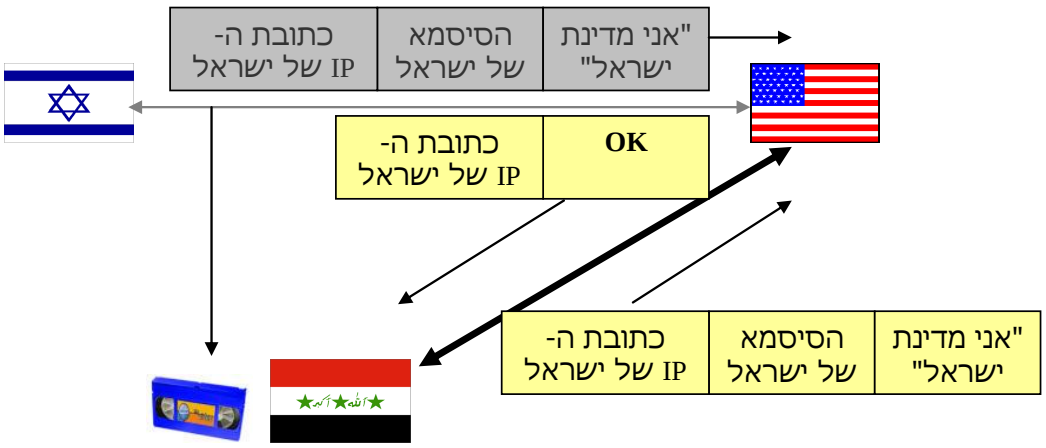


<u>פרוטוקול ap3.0:</u>

ישראל: "אני מדינת ישראל" => נשלח בחבילה המכילה את כתובת המקור (IP) + סיסמא מזהה.

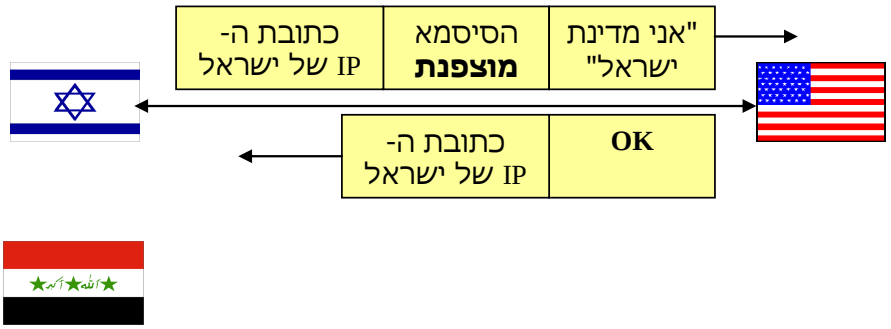


הבעיה היא שעיראק יכולה לקלוט ולשכפל את החבילה של ישראל ומאוחר יותר לשלוח את זה בעצמה לארה"ב.

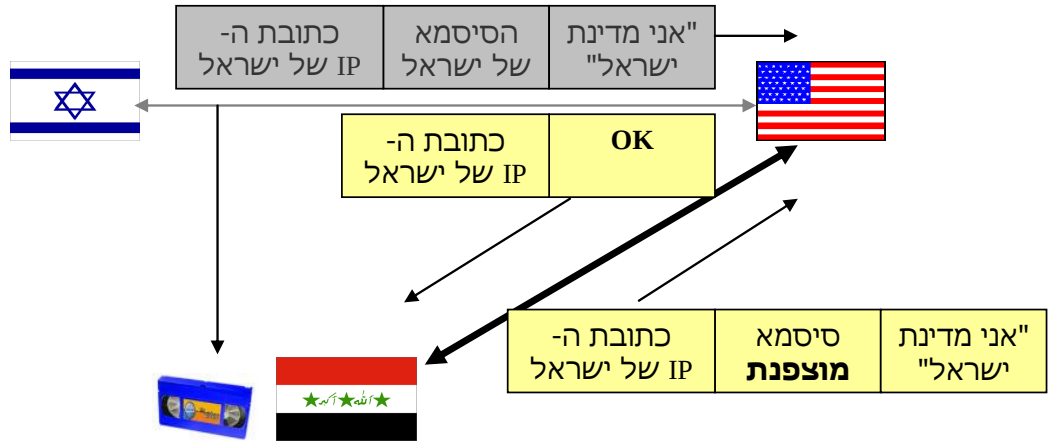


<u>פרוטוקול ap3.1:</u>

ישראל: "אני מדינת ישראל" => נשלח בחבילה המכילה את כתובת המקור (IP) + סיסמא מזהה <u>מוצפנת</u>.



הבעיה היא שעיראק **עדיין** יכולה לקלוט ולשכפל את החבילה של ישראל ומאוחר יותר לשלוח את זה בעצמה לארה"ב.



כעת, ננסה בדרך אחרת:

המטרה היא להימנע מאפשרות שכפול המסר.
נבחר כל פעם מספר מסוים R ונשתמש בו באופן חד פעמי.

<u>פרוטוקול ap4.0:</u>

על מנת להוכיח שישראל נמצאת כרגע ברשת, ארה"ב שולחת לישראל את אותו מספר R, וישראל חייבת לשלוח בחזרת את אותו מספר, מוצפן על-פי מפתח הצפנה סימטרי סודי.

ישראל נמצאת כרגע ברשת ורק היא יודעת להצפין את המספר R ולכן ארה"ב יודעת שזו חייבת להיות ישראל.

האם ניתן לאמת זהות משתמש ע"י שימוש בטכנולוגיות הצפנה ציבורית?

<u>פרוטוקול ap5.0:</u>

פרוטוקול זה משתמש באותו מספר R , ובהצפנה על ידי מפתח ציבורי.

ארה"ב מחשבת $K_A^+(K_A^-(R)) \stackrel{?}{=} R$ ואם יצא R , היא יודעת שרק לישראל יש את המפתח הפרטי ולכן זו אכן ישראל.

<u>הבעיה היא שיש לנו פירצה באבטחה!</u>

עיראק עלולה להאזין לאורך כל הדרך, וארה"ב וישראל לא יוכלו לדעת זאת!
כיצד?
ישראל שולחת מסר הזדהות : "אני ישראל", עיראק קולטת את המסר ומעבירה אותו כמו שהוא לארה"ב. ארה"ב מחזירה לישראל את המספר הייחודי (R), עיראק קולטת אותו ומעבירה אותו לישראל. עד כאן, לכאורה הכל בסדר. אולם, כעת ישראל שולחת לארה"ב את המספר, כשהוא מוצפן בעזרת המפתח הפרטי שלה. עיראק קולטת את המסר, ושולחת לארה"ב את אותו מספר (R), מוצפן בעזרת המפתח הפרטי של **<u>עיראק</u>**. ארה"ב רוצה לאמת את זהות ישראל, ולכן היא מבקשת את המפתח הציבורי של ישראל ע"מ לבדוק שזהו אכן אותו R. ישראל שולחת כביכול לארה"ב את המפתח הציבורי שלה, אולם עיראק קולטת אותו בדרך, ובמקומו שולחת לארה"ב את המפתח הציבורי שלה!! מכאן והלאה, עיראק מפענחת כל מסר שהיא מקבלת מארה"ב באמצעות המפתח הפרטי שלה, מצפינה אותו באמצעות המפתח הציבורי של ישראל ומעבירה את המסר לישראל.
ארה"ב אכן בטוחה שישראל היא ברשת, בעוד שעיראק היא זו המאזינה לשתי המדינות בלא ידיעתן!
ארה"ב וישראל לעולם לא יוכלו לגלות שעיראק מאזינה להן, מאחר ועיראק שקופה מבחינתן, היא רק מצותת ולא משנה / מעכבת את המסרים.

פרק ד' – חתימה דיגיטלית

טכנולוגיה דיגיטלית המקבילה לחתימה בכתב – יד:

- השולח חותם על המסמך בחתימה דיגיטלית, וכן קובע שהוא יוצר המסמך.
- הנמען יכול להוכיח שהשולח הספציפי הזה, הוא אכן יוצר המסמך ולא מישהו אחר.

<u>סוגי חתימות דיגיטליות:</u>

<u>חתימה דיגיטלית פשוטה:</u>

ארה"ב חותמת ע"י הצפנת m במפתח הפרטי שלה, ושולחת את המסר עם החתימה המוצפנת לישראל.

$$m \longrightarrow K_B^-(m)$$

פירוט השלבים:

- נניח שהנמען מקבל את המסר m חתום בעזרת המפתח הפרטי של השולח $K_B^-(m)$.
- הנמען מוודא שאכן זהו השולח, ע"י הפעלת המפתח הציבורי של השולח על המסר, ובדיקת : $K_B^+(K_B^-(m)) = m$.
- אם $K_B^+(K_B^-(m)) = m$ הרי שמי שחתם על המסר (הצפין), היה חייב להשתמש במפתח הפרטי של השולח.
- היחיד שיש לו את המפתח הפרטי – הוא השולח!

הנמען מוודא את העובדות הבאות:

- השולח הוא זה שחתם m
- אף אחד אחר לא חותם m
- השולח חותם m ולא m'

פונקציות Hash:

פונקצית Hash מקבלת מסרים באורכים שונים, ומייצרת מסרים מתומצתים באורך קבוע.

$$m \longrightarrow H(m)$$

מאפייני פונקצית Hash:

- הרבה לאחד
- מייצרת מסר בגודל אחיד קבוע
- בהינתן קוד מוצפן x , פענוח m כך ש- $x = H(m)$ הוא בלתי אפשרי.

דוגמא:

בדיקת מספר הסיביות בתקשורת בין מחשבים, על מנת לגלות שהמסר הועבר בשלמותו, גם היא מעין פונקצית HASH (אם כי אינה חד- ערכית).

המאפיינים דומים למאפייני פונקצית HASH:

- הפונקציה מייצרת קוד בגודל קבוע ואחיד (16 ביטים)
- הרבה לאחד

אולם כמו שנאמר לעיל, הפונקציה אינה חד ערכית. כלומר, ניתן למצוא שני מסרים שונים שיש להם את אותו קוד .

MAC – Message Authentication Code

- קוד עם מפתח משותף סודי, שאיתו נאמת את זהות השולח.
- שיטה זו מהירה יותר מאשר יצירת ובדיקת חתימה.
- הנמען מוודא שאכן זהו השולח, ע"י הפעלת MAC על המסר, ובדיקת : $MAC_{A-B}(m,MAC_{A-B}(m)) = OK$
- ב- MAC לא ניתן להוכיח מי השולח האמיתי של המסר, מאחר וניתן לחשב את $MAC_{A-B}(m)$.

- **תווך אמין**

בעיקרון ישנן דרכים טרוויאליות על מנת לחלק לשני הצדדים מפתח סודי, לדוגמא:

- פגישה ראשונית פנים אל מול פנים, להחלטה על המפתח המשותף.
- בתוך ארגון – לכל עובד חדש ישימו מפתח על מחשבו האישי.
- נצפין את המפתח המשותף בעזרת מפתח ציבורי, שכבר ידוע (בעזרת E-mail, עיתון, אינטרנט וכו').

	בעיה	פתרון
מפתח סימטרי	איך שני הצדדים מסכמים על המפתח הסודי הזהה ברשת?	**"המרכז להפצת מפתחות"** (KDC) הוא הגורם המתווך בין הצדדים
מפתח ציבורי	כאשר ישראל מקבלת את המפתח הציבורי של ארה"ב , כיצד היא יודעת בוודאות שזהו המפתח הציבורי של ארה"ב ולא של עיראק?	CA Trusted Certification Authority

המרכז לחלוקת מפתחות (KDC)

- ארה"ב וישראל זקוקות למפתח סימטרי משותף
- KDC – לכל משתמש שמקושר ל- KDC יש מפתח סודי שונה (ישנם משתמשים רבים)
- ארה"ב וישראל, גם הן משתמשות בשרות ה- KDC , יודעות כל אחת מהו המפתח הסודי שלה. (K_A-KDC K_B-KDC)

איך ה- KDC מאפשר לארה"ב וישראל לקבוע את המפתח הסימטרי הסודי על מנת לתקשר זו עם זו?

=> ארה"ב שולחת ל- KDC את רשימת המעוניינים להשתמש במפתח הסימטרי: ארה"ב וישראל, כאשר המסר מוצפן ע"י המפתח הפרטי של ארה"ב מול KDC.

=> ה- KDC מחזיר לארה"ב את המפתח הסימטרי R1 שמעתה תשתמש בתקשורת עם ישראל, וכן את המפתח R1 מוצפן ע"י המפתח הפרטי של ישראל וה- KDC.

=> ארה"ב שלחת לישראל את המסר שקיבלה בדיוק: המפתח R1 מוצפן ע"י המפתח הפרטי של ישראל וה- KDC.

=> עתה: ישראל וארה"ב יכולות לתקשר אחת עם השנייה בעזרת המפתח הסימטרי R1.

<u>CA – רשות אישור</u>

- CA קושרת בין מפתח ציבורי מסוים לישות מסוימת.
- המפתח הציבורי של הישות (שם משתמש, ונתב) נרשם ב- CA :
  - הישות מספקת הוכחה לאימות זהותה ל- CA
  - CA יוצרת אישור המחבר בין הישות למפתח הציבורי שלה.
  - האישור מכיל את המפתח הציבורי של הישות עם חתימה דיגיטלית של ה- CA האומרת " זהו המפתח הציבורי של הישות".
  - לכולם יש את המפתח הציבורי של הרשות.
  - לכל מסמך יש חתימה חדשה.

- כאשר ארה"ב רוצה לדעת את המפתח הציבורי של ישראל:
  - מקבלת את האישור של ישראל
  - פותחת באמצעות המפתח הציבורי של ה- CA, ובודקת שאכן יש את החתימה שזהו המפתח הציבורי של ישראל.
  - כעת ארה"ב יודעת את המפתח הציבורי של ישראל.

<u>אישור ה- CA</u>

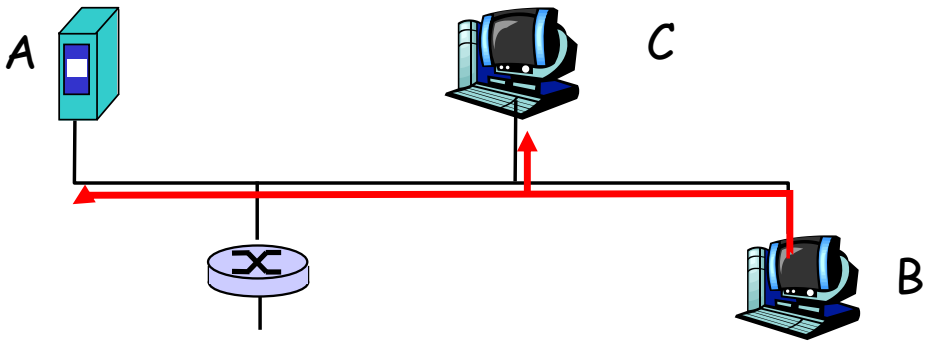
אישור ה- CA מכיל:

- מספר סידורי (ייחודי למנפיק)
- מידע אודות בעל האישור, כולל אלגוריתם ואת מפתח ההצפנה עצמו (מידע זה מוסתר).

"האזנה" לנתונים הנשלחים ברשת משותפת:

- ככלל, NIC – כרטיס הרשת, יכול להיות מותאם למצבים שונים : קריאת נתונים מכתובות מקור שונות, זאת על מנת לאפשר גילוי שגיאות ותיקונם.
- קריאת כל הנתונים הלא מוצפנים
- לעיתים, המאזין יכול אף לזייף את כתובת השולח.

דוגמא: C מאזין לנתונים הנשלחים מ- B ל- A



זיוף כתובת ה- IP של השולח

מחשב מסוים ברשת מסוגל לשלוח מסר עם כתובת IP מזויפת, למחשב אחר ברשת.
אולם, הנתב יכול לגלות את הזיוף (למשל אם הכתובת אינה בין המחשבים המחוברים אליו ברשת), ולחסום את החבילה.
הנתב הראשון בלבד חוסם את כניסת החבילה בעזרת מנגנון סינון (Ingress Filtering). לא כל נתב מסוגל לבצע את תהליך הסינון.

נקיטת אמצעים נגד זיוף כתובת ה- IP

- מנגנון סינון מעבר בנתבים : הנתבים לא יעבירו חבילות עם מקור שגוי. אולם, יש לציין כי לא ניתן ליישם מנגנון זה בכל הרשתות.
- נדרשת חבילות "אותנטיות" של ה-IP.

הערה[ah1]: להסביר למה...

הערה[ah2]: מה הכוונה?

- את ההתקשרות עצמה חובה לבצע רק אחרי ביצוע "לחיצת היד" (דבר שמתבצע ב-TCP אבל לא ב-UDP.

הערה[ah3]: ניסוח לא מוצלח

הגנות כנגד תקיפת הרשת

בהתקפות על ערוץ בודד, נחשב שקל יותר להאזין וקשה יותר ליצור הודעות מזויפות. באינטרנט, יותר קל לדחוף הודעות מזויפות (למשל בעזרת IP-Spoofing). זה נותן מוטיבציה חזקה לעבוד עם Hand Shake (ולכן לעבוד עם TCP שמשתמשת בשיטה זו). המונה שמחזיר מספר ב- Hand Shake הוא רנדומאלי ולא סידורי וזה מקשה על המתחזים לדעת מראש לאיזה מספר הצד השני מחכה.

- חטיפת נתיב – הנוכל משנה את הדרך כך שההודעה תגיע אל הנתב עליו השתלט הנוכל.
- חטיפת כתובת – השולח ישלח את ההודעה שלו לתוקף במקום לנמען האמיתי.

על מנת למנוע מצב כזה שבו הנוכל יהיה בתווך בין השולח לנמען, נבצע בנוסף ל- Hand Shake הוספת יחידת זמן לכל הודעה, כדי שתוקף לא ישלח הודעת "Request" שכבר נשלחה ומספר אקראי N אותו שומרים, ואסור שאותו מספר אקראי יחזור פעמיים.

הערה[ah4]: חסרים כאן פרטים ראו בהרצאה...

מניעת שרות מהמשתמש

התוקף מנסה "להתיש" את משאבי המחשב של המשתמש (שרת, נתב, רשת).
דוגמאות למשאבי מחשב:

- זמן CPU
- זיכרון
- קישורי TCP:

  הגבלת מס' ההודעות (תלוי חומרה / מערכת הפעלה),

  סגירת קישורים פתוחים שלא מקבלים Response

  תקיפת SYN

תקיפת SYN

ה- Server שולח Cookies (מלשון קוקיה המטילה ביציה בקינים של אחרים, ולא עוגייה...) ל- Client, ובשליחה הבאה, הוא כבר יודע שללקוח יש את ה- Cookie ולכן לא צריך לשלוח שוב. הלקוח שולח את ה- Cookie שלו עם כל בקשה אל השרת.

ה- Cookies לוקחים זמן חישוב, וזהו זמן יקר ולכן השרת יבזבז משאבים בשליחת המידע ללקוח רק אם ה- Cookies תקין.

הערה[ah5]: לא נכון... אמנם יש הצעה לתרגם לעברית ע"י קוקיה אבל באנגלית המשמעות דווקא עוגיה (וזאת ממתן עוגיה לדוב במשחק Zork)

הערה[ah6]: לא מספיק ברור!

תוקפים

- תקיפה מבפנים: מתבצעת על – ידי אדם בעל הרשאת כניסה למערכת.
- תוכנה "מרושעת" – סוס טרויאני, וירוס. תקיפה באמצעות תוכנה שרצה במערכת.
- האקר – תקיפת ערוצי התקשורת.

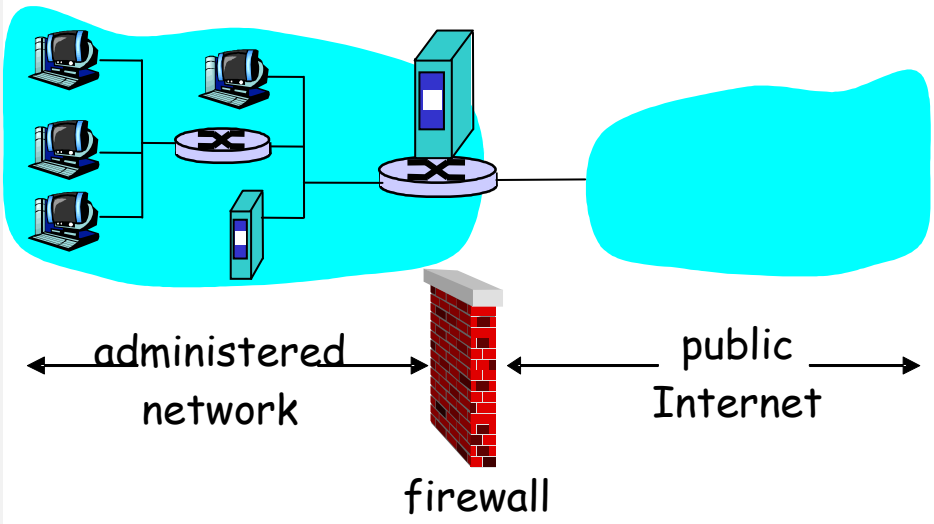
מרגע גילו התקיפה, בדרך כלל קל לנטרל את התוקף.

<u>התקנים בעזרתם ניתן להגן על המידע ברשת:</u>

1. FIREWALLS – מעין קיר / חסם
2. תעלות בטוחות / ערוצים בטוחים

FIREWALLS

כל חברה מתחברת ע"י Firewall – מכונה שמאובטחת ונמצאת בין רשת פנימית של הארגון לרשת החיצונית.



<u>תפקידים:</u>

סוג אחד של פילטרים, משמשים כנתב- מסתכלים על כל IP שנכנס ויוצא, מחליט האם החבילה יכולה להיכנס / לצאת מהארגון ואליו. החלטה זו מבוססת על: כתובת השולח והנמען, הפרוטוקול (TCP ,UDP), ה- PORT שבו משתמשים, הודעות SYN ו – ACK המסמנות שמישהו מבחוץ מבקש ליצור קשר TCP. לפעמים ה- FireWall לא יאפשר כניסה לשרתים בתוך רשת פנימית.

תפקיד ה- Firewall הוא לנטרל את התוקף כאשר הוא בא מבחוץ: לא לאפשר לו כניסה פנימה.
אם התוקף כבר בפנים (למשל אתי אלון...) ה- Firewall לאו דווקא יכול לאבטח את הרשת מבפנים. כאשר התוקף כבר בפנים, הוא יכול לתקשר החוצה (וה- Firewall לא יכול לעצור בעדו, מאחר והוא מתחזה למחשב ברשת), ואף לשלוח וירוסים מוצפנים ולהתקיף את הרשת. יחסית קל לתוקפים לחדור למחשבי הארגון.

כלי נוסף מלבד ה- Firewall – **<u>תעלות בטוחות</u>**

אבטחה שמשתמשת בקריפטוגרפיה. אבטחה זו תגן על ידי הצפנה בשתי דרכים:

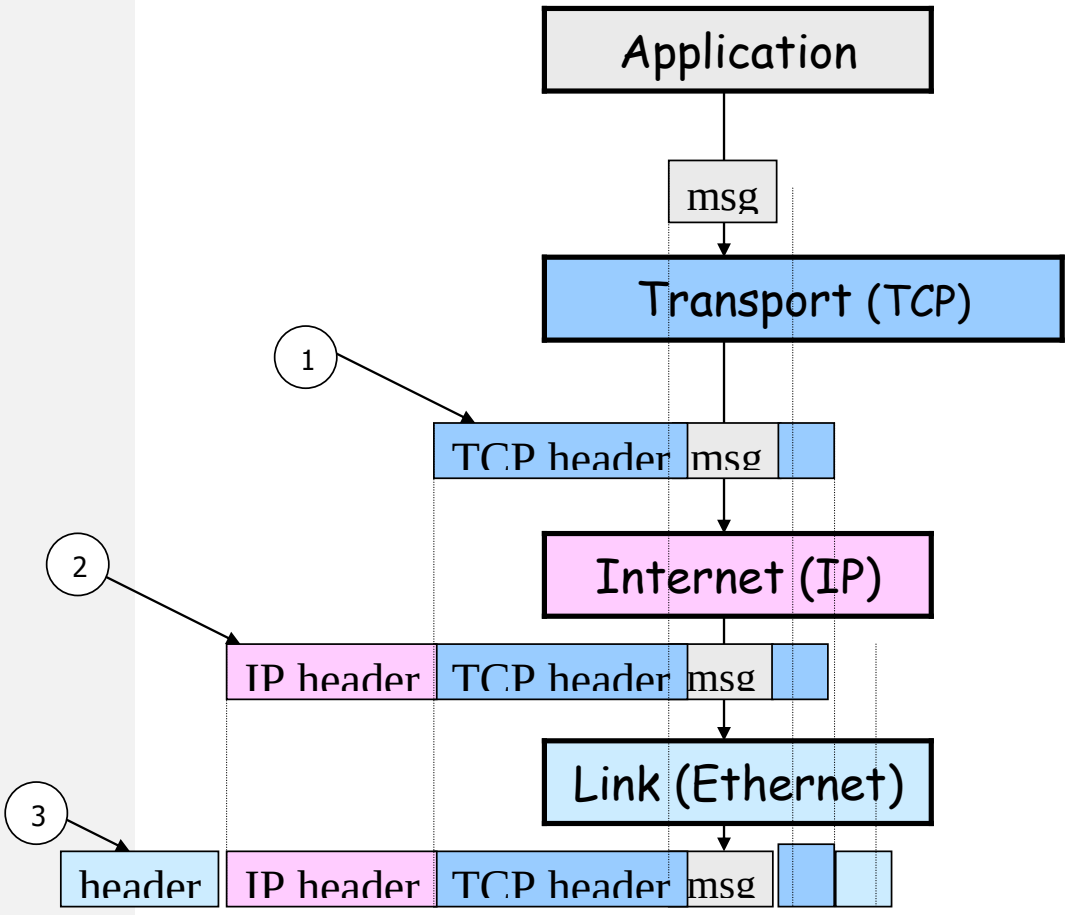
- קצה לקצה – מלקוח אל שרת דרך הנתבים (כל האינטרנט).
- מ- HOP ל - HOP ב- Link layer (תקשורת אלחוטית - הצפנה בין מכשיר נייד לבין תחנת הקצה).

IP-SEC – פרוטוקול הצפנה ברמת ה-IP - למשל, הגנה על מחשב נייד שמשדר לארגון.
SSL / TLS – בין שרת ללקוח.

<u>כימוס – תהליכי העטיפה של חבילות (Encapsulation)</u>

הודעה עובר מהאפליקציה אל הערוץ. תוך כדי עיבוד החבילה נוספים לה פרטים נוספים בהתחלה ובסופה.
דוגמאות (ראה תרשים):

1. האפליקציה מעבירה את ההודעה במרת ה- Transport בעזרת Socket וההעברה מוסיפה אל ה- TCP Header.
2. רמת ה- IP מוסיפה גם היא Header המזהה את ה- PORTS של השולח ושל הנמען (מזהה לאיזו אפליקציה לחזור).
3. רמת הערוץ מוסיפה את כתובת הרשת – הכתובת הפיזית של השולח ושל הנמען.



<u>איך עושים כימוס בשימוש בפרוטוקול IP-SEC?</u>

החבילה מתקבלת ע"י שכבה של IP-Security ושם נעשית ההצפנה. החבילה חוזרת באותו הגודל + overhead קטן (פונקצית האימות מגדילה את האורך).
למשל, להודעה מתווסף ה- IP-header על מנת שנוכל להגיע חזרה יעד, מאחר וההודעה כבר מוצפנת!.