



Chapter 21 - Network Attack & Defense

ג'רית בארנס

סמינר אבטחת מידע

אביב 2014

אוניברסיטת חיפה

* קיימים היום סוגים שונים של התקפות נגד מחשבים.

* ההתקפות האסכות ונהיות ממוקדות יותר ויותר ברשת ובתקשורת מחשבים.

* הרבה התקפות מופיעות במלכא לכו יש מספר רב של מחשבים שמחברים יחד לרשת.

- עובד מחוץ עם קובץ מצורף לנשלח אליו במייל.
הקובץ מזביק את המחשב שלו בתוכנה צדונית לפוגעת
במחשבים אחרים במשרד ע"י חיפוש סיסמאות למסתובבות
ב LAN.

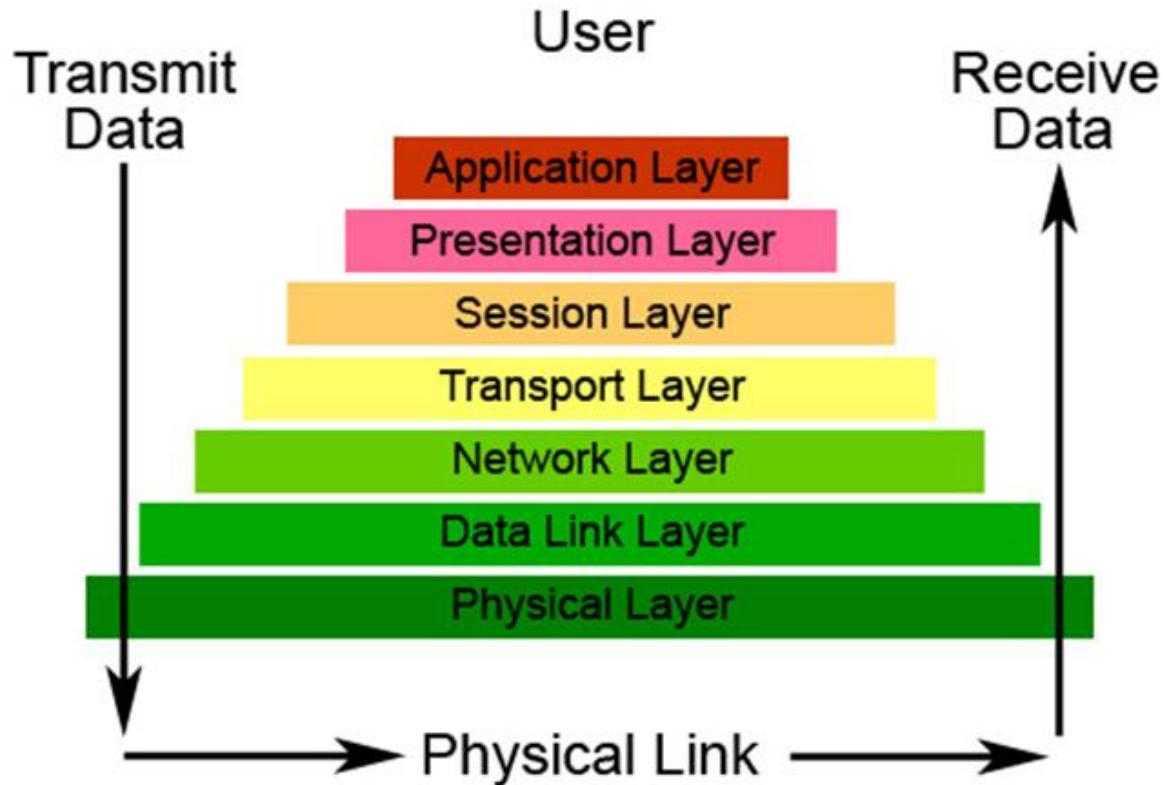
- הסיבה שהעובד מחוץ עם הקובץ היא שהמייל הגיע מאמא
שלו.

- התוכנה הצדונית התקיפה את המחשב של אמא שלו ולמחה
עותקים של מיילים אחרונים לנשלחו - ולירפה את עצמה
כקובץ!

- אמא שלו, בתורה, הוזבקה בתוכנה הצדונית מחבר ותיק
לחור סיסמא נפוצה לחשבון המייל שלו....

מודל 7 השכבות

The Seven Layers of OSI

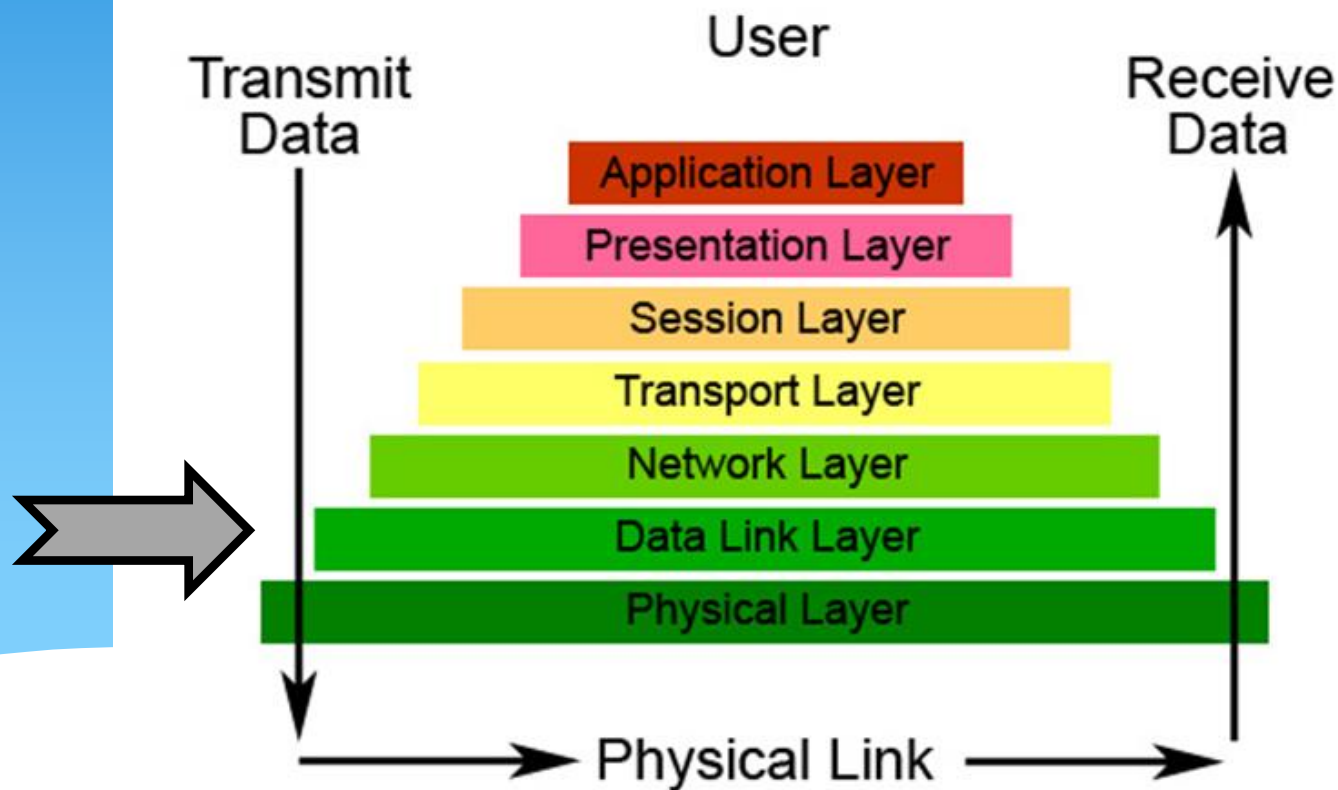


מודל 7 השכבות

- שכבה 1 - השכבה הפיזית - אחראית עם לסיחת הביטים עלמס.
- שכבה 2 - שכבת הקו/הקרה - אחראית עם לסיחה בין לני רכיבים קרובים ללא לגיאה.
- שכבה 3 - שכבת הרשת - IP - אחראית עם ניתוב החביסה מנקודה A לנקודה B
- שכבה 4 - שכבת ההובסה - TCP - סיפוא בסיסי בחביסה, דואגת להעביר את המידע בצורה אמינה.
- שכבה 7 (5-7) - שכבת היישום - השכבה בה מתרחשת "התקשורת האמתית" עם המשתמש

שכבה 2 – שכבת הבקרה

The Seven Layers of OSI



Arp Spoofing / Poisoning

- Address Resolution Protocol - ARP •
פרוטוקול תרגום כתובות.

פרוטוקול תקשורת המשלם ברשת מחשבים לאיתור כתובת ה-MAC
לא תחנה ברשת עפ"י כתובת ה-IP לשה ע"י בקשות ARP.

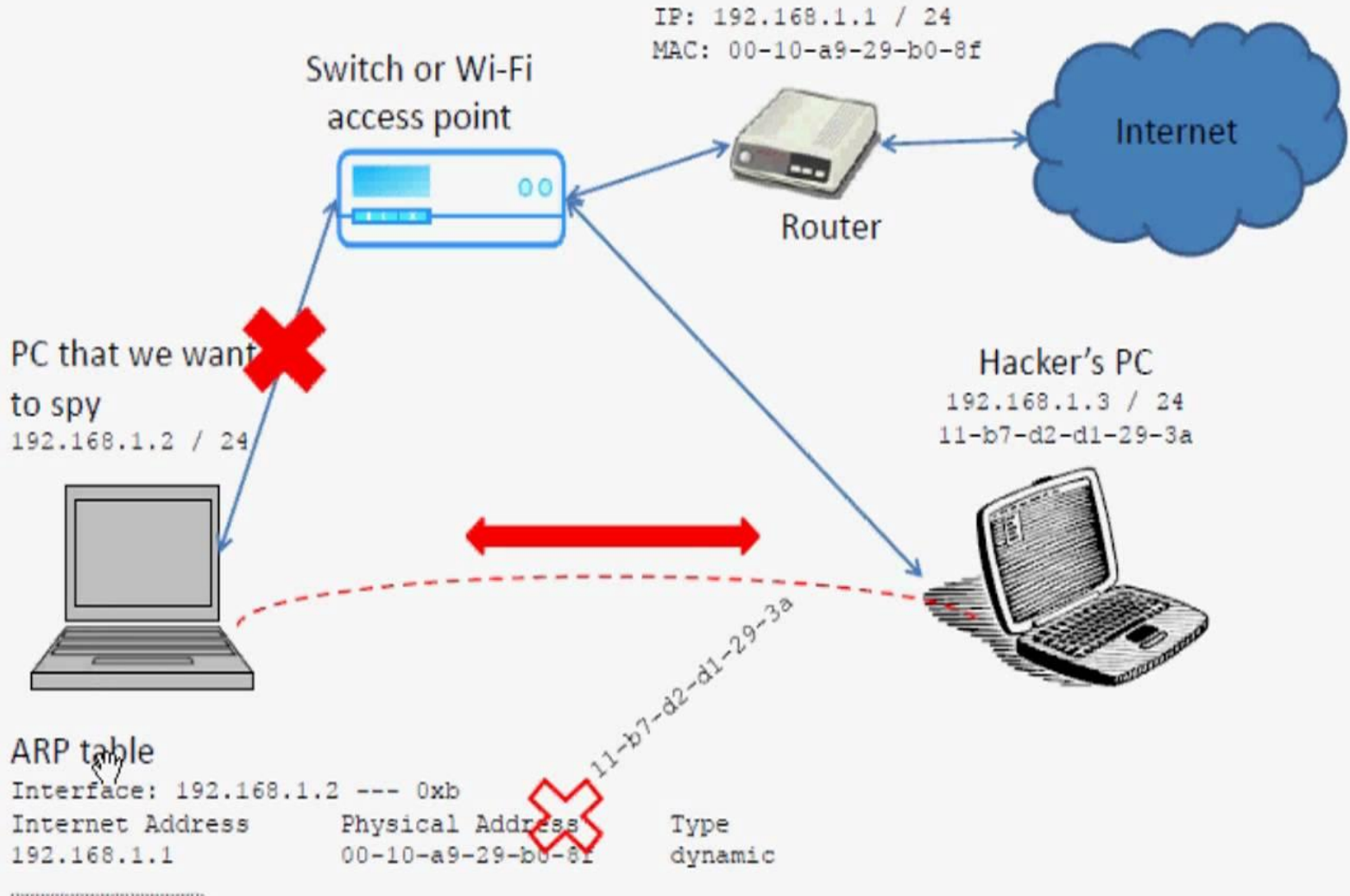
* איך מתבלע איתור כתובת ה-MAC?

Arp Spoofing / Poisoning

* עקב אובדן של פרוטוקול ה-ARP (אין אימות - אוטנטיקציה) הוא חלוף לניכול ע"י "גניבת זהות".

* ARP Spoofing - משתמש צדוני יכול להמתין לברקשת ARP מתחת המקור / להשתמש בכסיס מיוחדים, ובעת הגעתה לשדר בחזרה כתובת MAC פיקטיבית.

What ARP poisoning (spoofing) means ?



“How to spy a PC with Arp Poisoning”
youtube – by softgenes -

Arp Spoofing / Poisoning

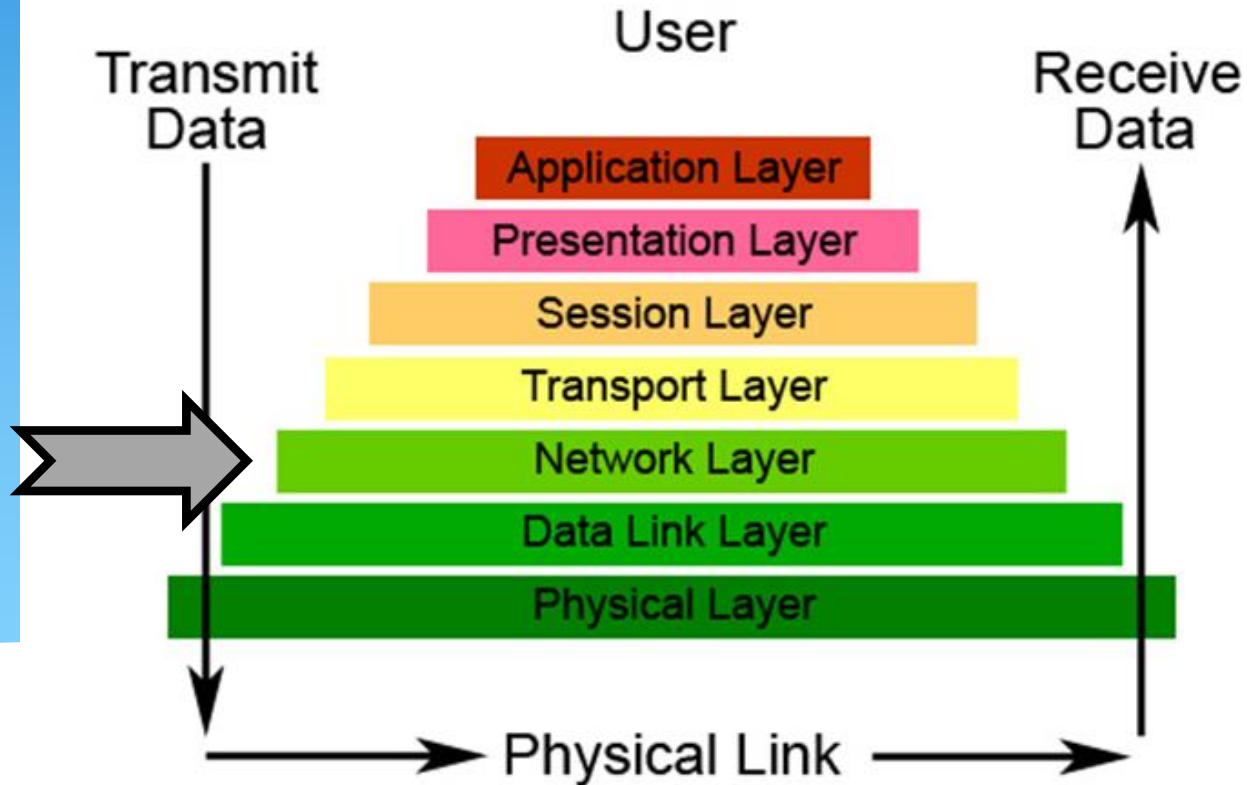
: ARP Spoofing שימוש להתקפת

.Man In The Middle התקפת – MITM *

.Denial Of Service – DoS *

שכבה 3 – שכבת הרשת

The Seven Layers of OSI



BGP Hijacking

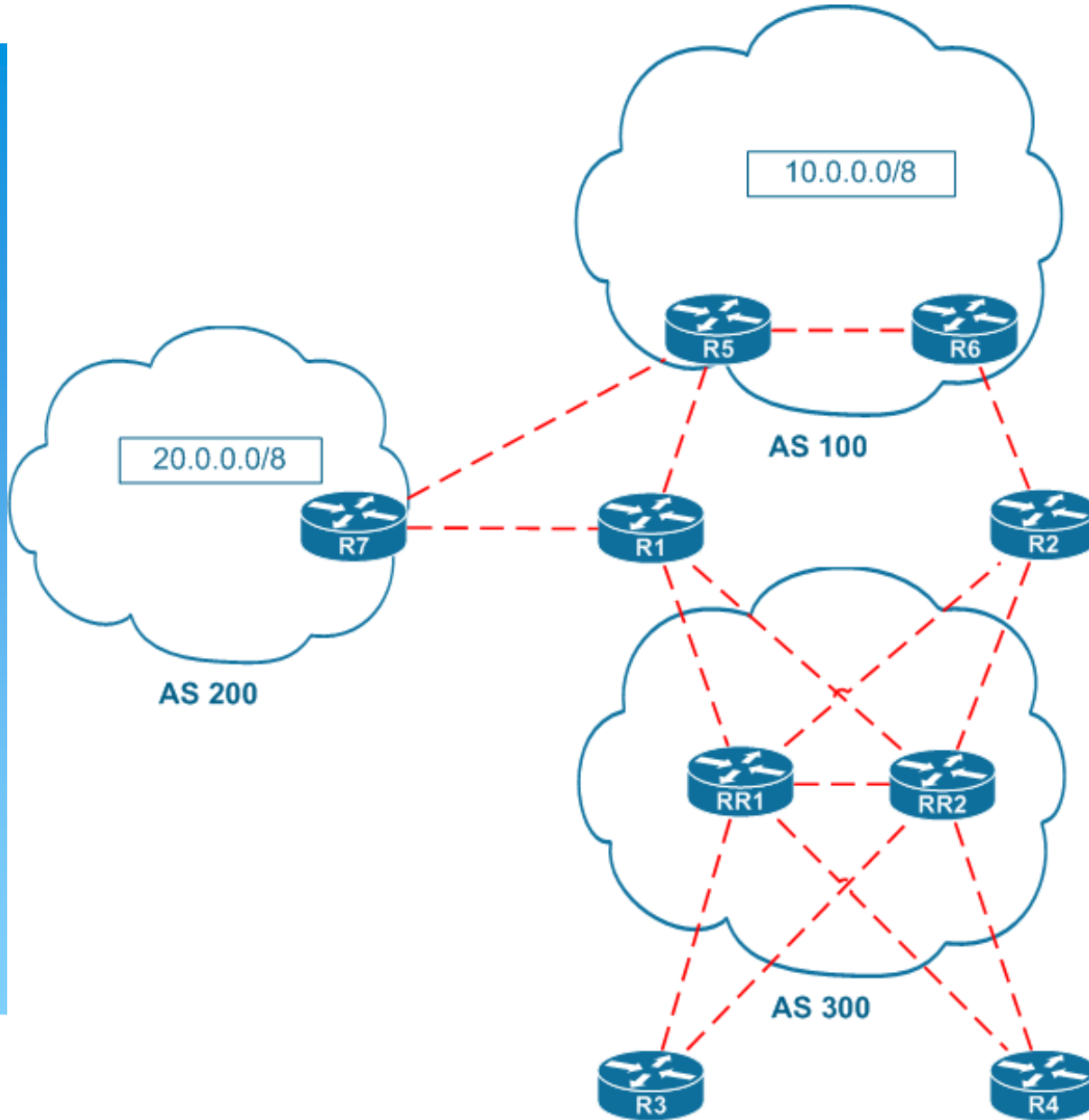
– Border Gateway Protocol – BGP

פרטאקאָל נײַתובֿ המהווה את ליבת מערכת הניתוב של רשת האינטרנט.

גרף המכיל למתים וקלטות עם מלקרים ביניהם.

AS – Autonomous Systems – אולט עם תחום מסוים של כתובות IP.

(IANA – Internet Assigned Numbers Authority)



BGP Hijacking

* כל AS מפרסם רשימת תחיליות (prefix) של כתובות אלו
הוא יכול להעביר תעבורה.

*אמל: 192.0.2.0/24 נמצאת ב AS **64496**.

* ככל שהקידומת יותר מזויקת – כך ה AS מקבל קדימות.
"המסלול הקל ביותר".

BGP Hijacking

חטיבת BGP יכולה לקרות באופן לא צדוני (בלעזת) בדרכים
הבאות:

* AS מסוים מודיע שיש לו קיזומת לש כתובת מסוימת שאין לו
באמת.

* AS מסוים מודיע שיש לו קיזומת יותר סבליבית ממה לבאמת
יש לו.

* AS מסוים מודיע שהוא יכול להעביר תעבורה בדרכ "קלה"
יותר ממה לכהר קיים (בין אם זה נכון ובין אם לא).

BGP Hijacking

חטיבת BGP יכולה להיות גם צדונית.

* בשנת 2013 הייתה כתבה בכאכאיסט שאכן פורצים הצליחו
לפרוץ לשרתי ה-BGP ולשנות את מסלולי הניתוב - והאיום הפך
מתיאורטי לממשי.

אדוני השוטר חטפו לי את האינטרנט!

עברייני הסייבר הצליחו לבצע "חטיפה" של תשדורות אינטרנט תוך פריצה לשרתי התעבורה. האיום צריך להדאיג מאוד מכיוון שכרגע אין אפשרות למנוע אותו

רפאל קאהאן

11:56, 20.11.13

3 תגובות

Like 15

0 +1

✉ המייל האדום | 🗨 תגובה לכתבה | 💬 הדפסת כתבה | ✉ שלחו כתבה | 🗨 שתף כתבה

האזנות סתר ויירוט תשדורות הפכו לנושא חם השנה בצל הגילויים על תכנית המעקב של ה-NSA. אולם, לא רק לרשויות יש יכולות מעין אלה. חברת Renesys המתמחה במודיעין עסקי פרסמה בבלוג החברה גילוי חדש בתחום לוחמת הסייבר.

קראו עוד בכלכליסט:

- [אדובי: שוד הסיסמאות הגדול הפך לתשביץ](#)
- [פרצת אבטחה באופיס משמשת לגניבה והונאות פיננסיות](#)
- ["אימי הסייבר הגדולים ביותר מכוונים דווקא אל השוק האזרחי"](#)

על פי החברה, האיום החדש מתבסס על יכולת יירוט תעבורת אינטרנט על ידי פריצה לשרתי התעבורה העולמיים (שרתי BGP). יכולת זו שעד היום הייתה יותר תיאורטית מאשר מעשית, התממשה במספר מקרים בשנה האחרונה.

לדברי מומחי האינטרנט של החברה, כ-150 אירועים של יירוט תעבורה נצפו בשנה האחרונה. השיטה מאפשרת להאקרים ל"שתות" את המידע שמועבר בין שרתי האינטרנט על ידי כך שהם משנים את הניתוב של המידע, בעיקר על ידי זיוף כתובות IP.

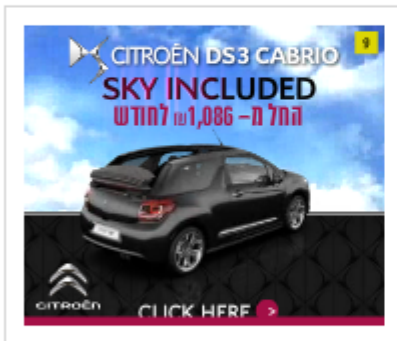
התוצאה היא דאגה רבה עבור חברות האשראי, הבנקים והחברות אשר מסתמכים על הרשת על מנת לבצע העברות פיננסיות או משלוח של מידע רגיש. המזל של הרשויות הוא שסוג כזה של פעילות סייבר ניתנת לזיהוי די בקלות, בעיקר בגלל שלל העקבות שההאקרים משאירים.

החשודות המיידיות: איסלנד ובלרוס

עיקר האירועים התבצעו על ידי ניתוב מחדש של התעבורה דרך שרתים באיסלנד ובבלרוס. אירוע אחד למשל כלל ניתוב מחדש של תעבורה בין שני שרתים בדנבר, כאשר המידע מצא את עצמו מועבר לאיסלנד, ללא כל סיבה הגיונית.

בבדיקה שנעשתה מול ספקית ניתוב איסלנדית נטען על ידה כי האירוע נבע מבאג בשרתי התעבורה. אולם, קשה להניח שבאג בודד בשרת מדגם מסוים עומד מאחורי כל האירועים שנצפו. למעשה, ספקית הניתוב האיסלנדית לא סיפקה כל מידע מעבר לתשובה הלקונית, גם לאחר בקשות חוזרות ונשנות של חברת רנסיס.

למעשה, עד שכל נתיבי תעבורת האינטרנט יאובטחו, משהו שברנסיס לא מאמינים שיקרה אי פעם, יש לקחת בחשבון שהפיתרון היחיד בינתיים הוא שימוש בהצפנת מידע וכן חשיפה של מקרים על מנת ליצור הרתעה יעילה כנגד החוטפים.



<http://www.calcalist.co.il/internet/articles/0,7340,L-3617476,00.html>

China 18-Minute Mystery

China BGP Hijack

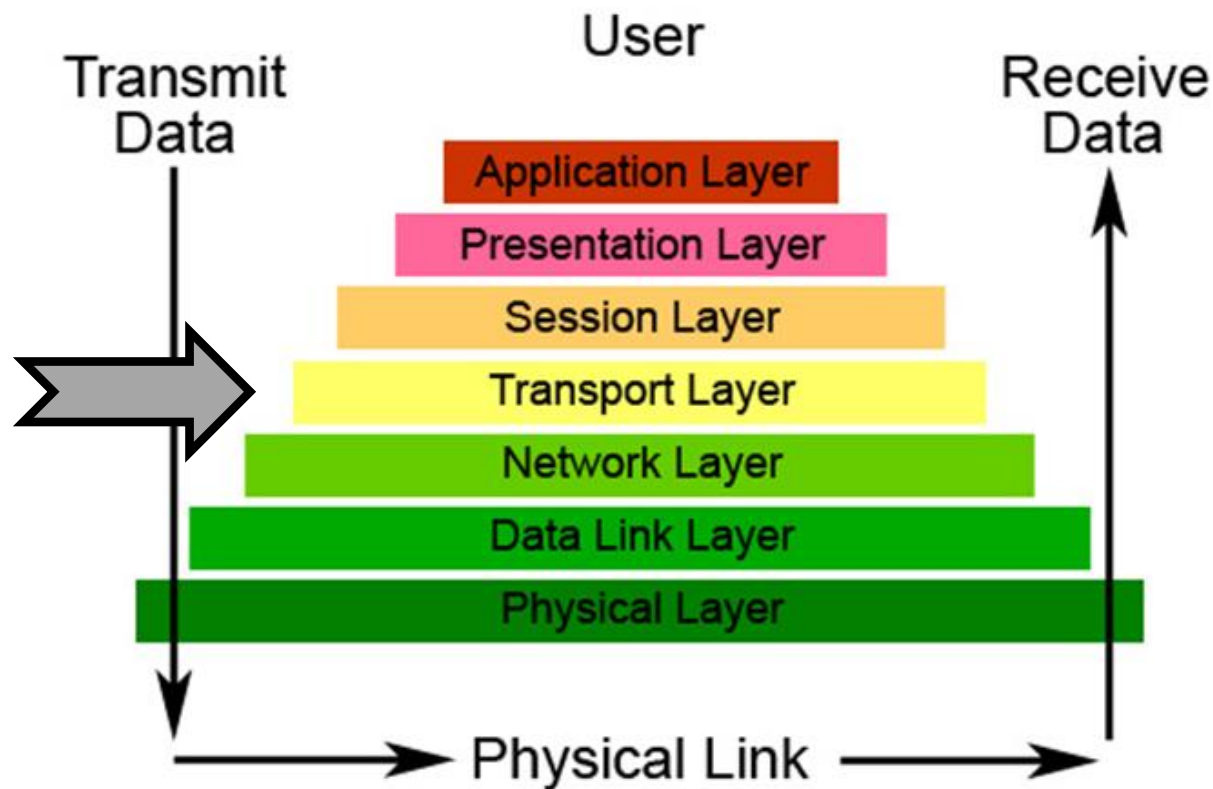
ב-8 באפריל 2010 AS – China Telecom מספר
23724 בה"ג"ן הכריז בטעות שיש לו בעלות על יותר
מ-50,000 באוקיינוס של כתובות IP.

"כ-15% ממקורות האינטרנט" – כך נאמה.

איש לא חשב שאם האינטרנט היה כזה – AS מוכר ואמין.

שכבה 4 – שכבת ההובלה

The Seven Layers of OSI

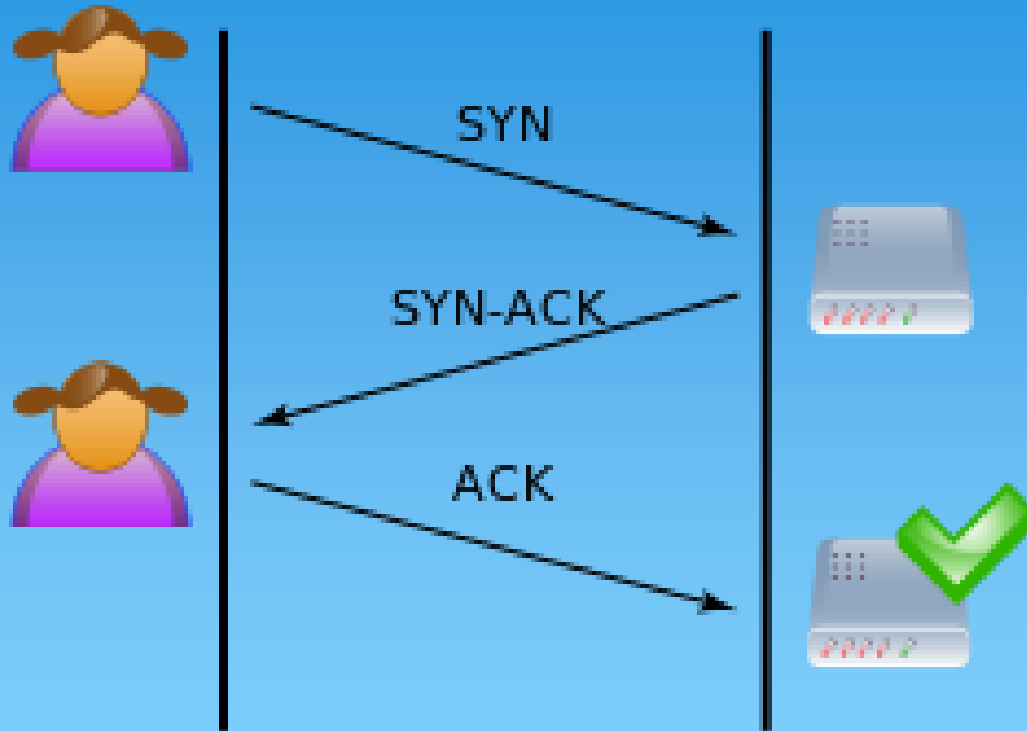


Syn Flood (TCP)

- התקפה מסוג Denial Of Service.
- ניצול פרצת אבטחה במנגנון הקמת הקשר של TCP.
- הקמת הקשר – 3-way handshake.

32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
פורט היעד																פורט המקור															
מספר סידורי																															
מספר אישור (ACK)																															
גודל חלון השליחה																דגלים						שמור				אורך הפתיח					
מיקום מידע דחוף																Checksum															
ריפוד באפסים																אפשרויות שונות (אופציונלי)															

Syn Flood (TCP)



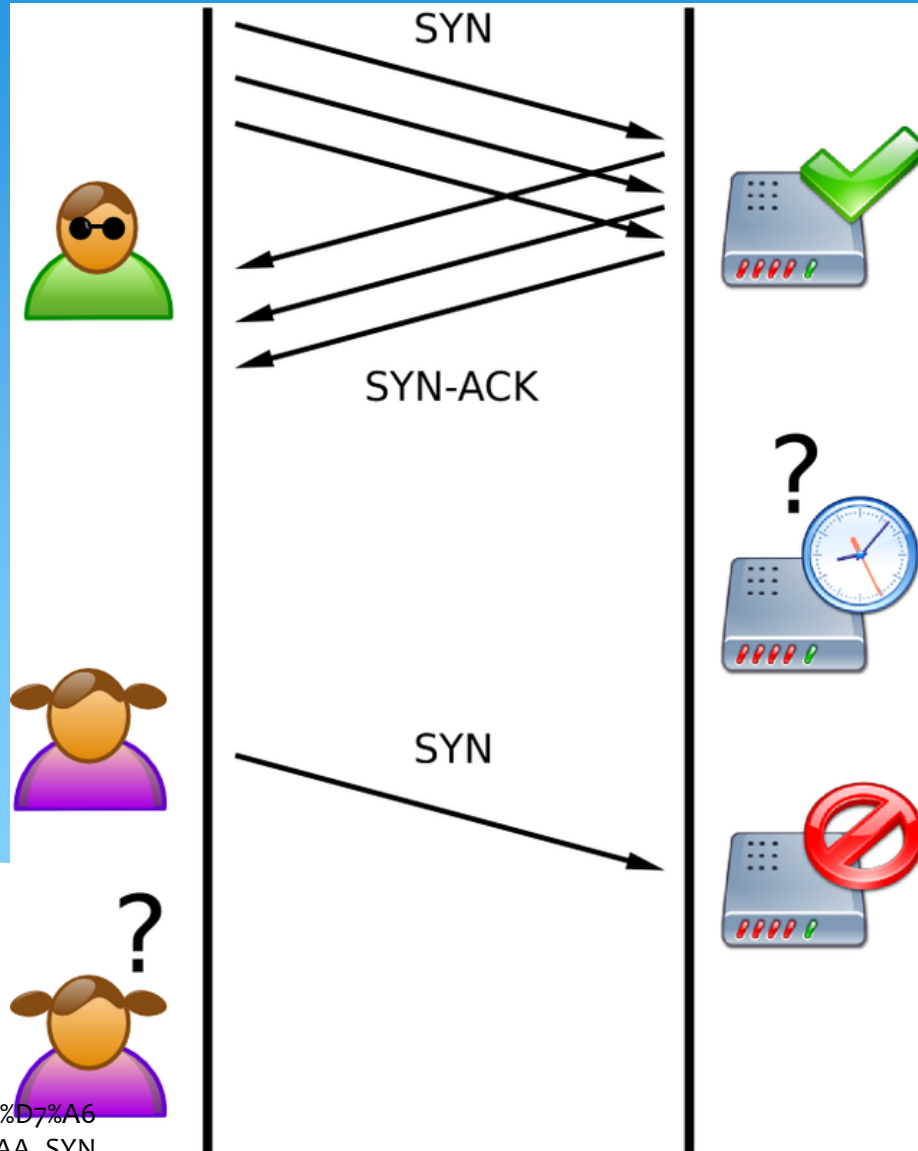
Syn Flood (TCP)

- הזנת SYN מנצלת למעשה את ההמתנה להגרת מחויב שה עז לקבאת האישור מהסקות.

- איך מתבלעת התקיפה?

ע"י שליות חביסות SYN רבות לשרת.
התוקף מאלף את השרת שהלאור קלרים רבים "חלי פתוחים".
בלא הגבאת מלאבים - השרת מאבז מיכואתו שהעניק לירות
למלתמלים התמ"מ"ס. - Denial Of Service.

Syn Flood (TCP)



Syn Flood (TCP)

התמוצות:

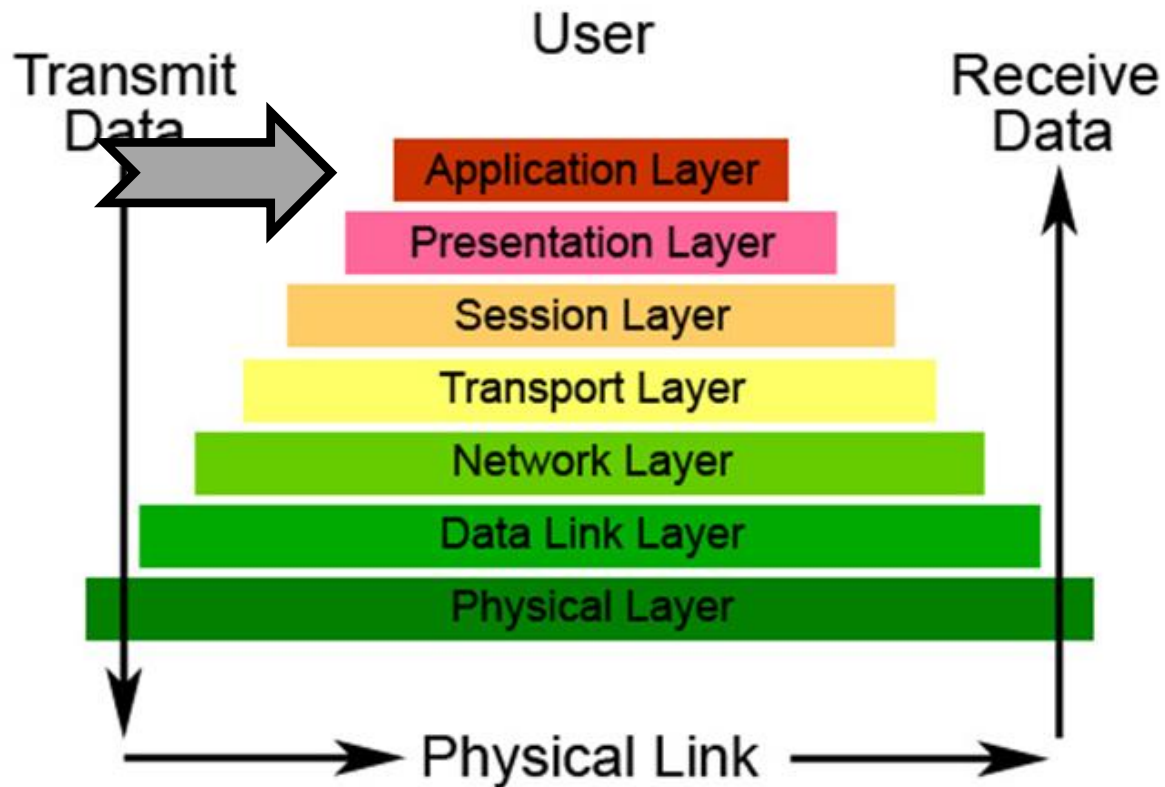
- הגדלת קיבולת הקשרים החלי-פתוחים לבה השרת יכולה לתמוך.

- עוג'ית SYN - מאפ'ר לשרת שהימנע אחלוט'ין מהקבל'ת מל'אבים לקשרים חלי פתוחים ע"י הוספת נתונים לחבי'ת ה-SYN-ACK הנשלחת חזרה לסקוח מחלב מחזל את המס' הסידורי שהוא עכ'נו הגר'ים ובכך ליכור את הקשר באופן לקוף.

```
A → B: SYN; my number is X
B → A: ACK; now X+1
        SYN; my number is Y
A → B: ACK; now Y+1
        (start talking)
```


שכבה 7 – שכבת היישום

The Seven Layers of OSI





Heart Bleed

SSL – Secure Sockets Layer

פרוטוקול תקשורת ארשתות מחשבים המאפשר
תקשורת מאובטחת ומובטחת בין שני יישומים.

Open SSL – ספריית תוכנה חופשית המממשת את פרוטוקול
ה-SSL. זוהי תוכנת ההכפנה הפופולרית ביותר באינטרנט.

משתמשים בו: Gmail, Facebook, Instagram ועוד רבים.



Heart Bleed

Heart Beat – אחד הפיצ'ורים של Open SSL בו נמצא

הפגם.

מנג'ון זה מאפשר למחשב בקצה האחד של קו מוצקן לשלוח
אות למחשב שלי כדי לבדוק שהוא עדיין מקוון.

• הפרצה הייתה קיימת יותר משנתיים לפני שהתגלתה.

* "הבאג המשמעותי ביותר שהתגלה אי פעם"

HOW THE HEARTBLEED BUG WORKS:



SERVER, ARE YOU STILL THERE?
IF SO, REPLY "HAT" (500 LETTERS).



User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long. User Karen wants to change account password to "Karen". User Isabel requests pages about...



HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long. User Karen wants to change account password to "Karen". User Isabel requests pages about...

User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long. User Karen wants to change account password to "Karen". User Isabel requests pages about...





Heart Bleed

הבאג בעצם מאפשר לתוקף לקרוא עז 64KB של זיכרון

למכיוס בין היתר:

את המפתחות הסודיים, שמות משתמש וסיסמאות מייסדי,
מסמכים סודיים ועוד...

The bug

The fix starts here, in *ssl/dl_both.c*:

```
int
dtls1_process_heartbeat(SSL *s)
{
    unsigned char *p = &s->s3->rrec.data[0], *pl;
    unsigned short hbtype;
    unsigned int payload;
    unsigned int padding = 16; /* Use minimum padding */
}
```

So, first we get a pointer to the data within an SSLv3 record. That looks like this:

```

typedef struct ssl3_record_st
{
    int type;                /* type of record */
    unsigned int length;    /* How many bytes available */
    unsigned int off;       /* read/write offset into 'bu
    unsigned char *data;    /* pointer to the record data
    unsigned char *input;   /* where the decode bytes are
    unsigned char *comp;    /* only used with decompressi
    unsigned long epoch;    /* epoch number, needed by DT
    unsigned char seq_num[8]; /* sequence number, needed
} SSL3_RECORD;

```

Records have a type, a length, and data. Back to `dtls1_process_heartbeat`:

```

/* Read type and payload length first */
hbtype = *p++;
n2s(p, payload);
pl = p;

```

The first byte of the SSLv3 record is the heartbeat type. The macro `n2s` takes two bytes from `p`, and puts them in `payload`. This is actually the *length* of the payload. Note that the actual length in the SSLv3 record is not checked.

The variable `pl` is then the resulting heartbeat data, supplied by the requester.

Later in the function, it does this:

```
unsigned char *buffer, *bp;
int r;

/* Allocate memory for the response, size is 1 byte
 * message type, plus 2 bytes payload length, plus
 * payload, plus padding
 */
buffer = OPENSSL_malloc(1 + 2 + payload + padding);
bp = buffer;
```

So we're allocating as much memory as the requester asked for: up to 65535+1+2+16, to be precise. The variable *bp* is going to be the pointer used for accessing this memory. Then:

```
/* Enter response type, length and copy payload */
*bp++ = TLS1_HB_RESPONSE;
s2n(payload, bp);
memcpy(bp, pl, payload);
```

The macro *s2n* does the inverse of *n2s*: it takes a 16-bit value and puts it into two bytes. So it puts the same payload length requested.

Then it copies *payload* bytes from *pl*, the user supplied data, to the newly allocated *bp* array. After this, it sends this all back to the user.

The fix

The most important part of the fix was this:

```
/* Read type and payload length first */
if (1 + 2 + 16 > s->s3->rrec.length)
    return 0; /* silently discard */
hbtype = *p++;
n2s(p, payload);
if (1 + 2 + payload + 16 > s->s3->rrec.length)
    return 0; /* silently discard per RFC 6520 sec. 4 */
pl = p;
```

This does two things: the first check stops zero-length heartbeats. The second check checks to make sure that the actual record length is sufficiently long. That's it.

הגנה

בהגנה נגד התקפות רשת ישנם 4 כלים עיקריים:

- **Management** – שמירה על המערכות מעודכנות

ומגדרות באופן שיקטין את משטח התקיפה.

- **Filtering** – שימוש בfirewalls.

- **Intrusion Detection** – גילוי פריצה – שימוש בתוכנות

לעוקבות אחר הרשת והמחשבים שלנו ומצהות סימני התנהגות

עוינת.

- **Encryption** – הצפנה – פרוטוקולים שמאפשרים הגנה

על חלקים ספציפיים של הרשת מפני תקיפות ספציפיות.

Management

* לריק לשמור עם המחשב מעודכן ומקונפג ככה הניתן.

Patch Tuesday:

- מייקרוסופט מוליבאים סט תיקוני אבטחה אחת לחודש (Patch Tuesday).

- התוקפים עולים להם reverse engineering – ומבינים

היכן בולעו התיקונים – ובכך חולפים את נקודות התורפה.

- התוקפים מנסים לתקוף מחשבים לעדיין לא התקינו את סט תיקוני האבטחה.

Management

* בנוסף כדאי לדאוג לסיסמאות לאינ מוכרות ולרמת האבטחה שלהן גבוהה (אותיות גדולות קטנות ספרות !@#\$%&).

- הסרת לירותים לאין בהם לורק - הקטנת מלח התקיפה.

- התקנה מחזל לעתים תכופות.

Filtering

הפתרון הנמכר ביותר בעולם המספק מענה ל"בעיות אבטחת האנטרנט" הוא ה-firewall.

זוהי בעצם מכונה העומדת בין המערכת המקומית והאנטרנט ומסננת את התעבורה שעשויה להיות מזיקה.

ישנן שיטות נוספות לסינון תעבורה. בד"כ נחשק ל-3 סוגים עפ"י הלכבה בה הם מתבלעים:
IP, TCP או Application.

Intrusion Detection

- קופסאות ליוזבות עם הרשת ומחפלות סימני תקיפה או מערכות למראות סימני פריצה.

- נקראות באופן כללי - IDS – Intrusion Detection Systems.
- למשל תוכנת האנטי-וירוס.

- דוגמאות:

- ספאס המגייע ממכונה ברשת לסק.

- פקטות עם כתובת מקור מצויפת.

- מכונה המנסה ליצור קשר עם לירות הידוע כ"רע".

- במקרים כאלה ה-IDS יודיע למכונה מסוימת לריכה לעבור התקנה מחזל.

Intrusion Detection- Types

השיטה הפשוטה ביותר – השמעת אזעקה בעת חציית סף מסוים.



ממשל:

- 3 סיסמאות התחברות לגויות
- הוצאות כרטיס אשראי מאן סבירות
- שיחת טלפון של יותר מ-6 לעות.

Intrusion Detection- Types

מערכות מתוחכמות יותר בז"כ נחשקות א-2 קטגוריות:

- Misuse Detection Systems – מערכות גילוי שימוש ארעה – מחפלות "חתימה" – התנהגות אופיינית א הפולס.

- Anomaly Detection Systems – מערכות גילוי התנהגות חריגה. חיפול תבניות א התנהגות חריגה בהיעדר מודם ברור א זרק הפעולה א התוקא.

Encryption

בהקשר של מניעת התקפות רלת – רוב האנשים נוטים לחשוב עם
הזכנה.

“Whoever thinks his problem can be solved using cryptography – doesn’t understand his problem and doesn’t understand cryptography”

Butler Lampson and Roger Needham

Encryption-SSH

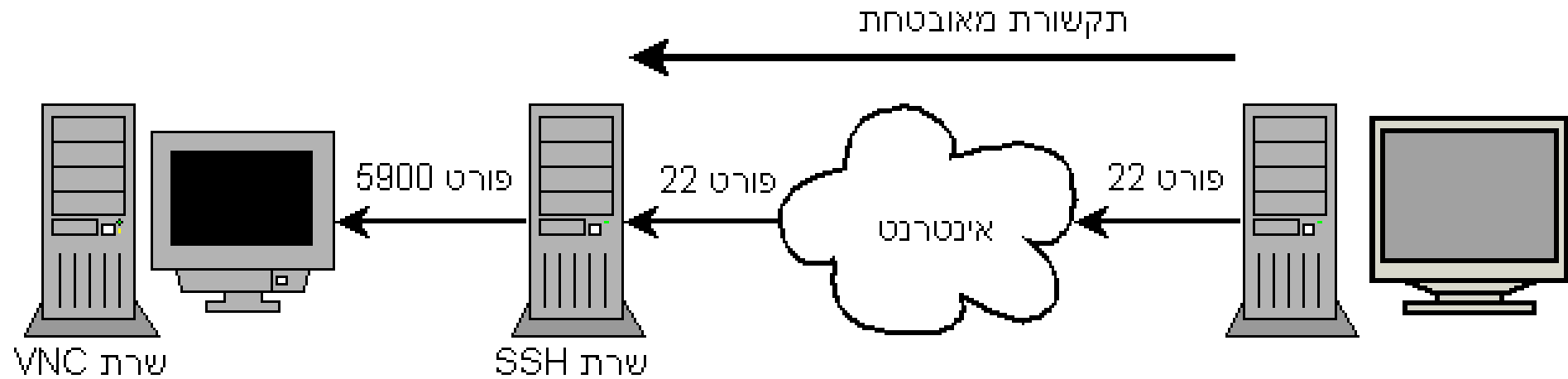
.Secure Shell – SSH

פרוטוקול שתקשורת מחשבים המאפשר ביצוע פעולות עם מחשב מרוחק לאחר תהליך הצדהות.

נועד לאפשר תקשורת מאובטחת ומזכנת בין שני מחשבים לא תלויים ברשתות לא מאובטחות.

תומך ה"תיעוד" תעבורה ממחשב אחד לשני בצורה מאובטחת דרך תוכנות SSH.

Encryption-SSH



סיכום

* סקרנו בקצרה את עולם אבטחת המידע בתחום הרשתות.

* רוב הבעיות בתחום נובעות מטעויות של design ולא תכנות
למשל ה- HeartBleed.

* האינטרנט לעולם לא יהיה בטוח לחלוטין – תמיד יהיו טעויות.

* מוצעות לעולם התקפות הרשת – התבוננות מנקודת מבט של
התוקף.

The

End !