



הפקולטה למדעי המחשב
הטכניון

הנדסה לאחור **236496**

מרצה : עמר קדמיאל

מתרגל : אלעד קינסבורגר

© Eli Biham, Omer Kadmiel and Aviad Carmel

אַתָּה רְאֵנָה

- שפות עיליות
 - C
- אסמבי- Intel 32-bit IA32 assembly
 - למד בקורס בתרגול
 - לא נתייחס לגרסאות 64 סיביות
- ידע בסיסי במערכות הפעלה
 - הבנת דרך הפעולה של מערכת הפעלה והמבנה שלה
 - השימוש בחלונות, כולל תכנות וDİBOW
 - ניסיון כמשתמש וירטואלייזציה
- ידע בסיסי באבטחת מידע
 - וחולשות אבטחה



2



קזנימ

- קדם חובה

- מערכות הפעלה 234123 או 046209 או שקול

- צמוד חובה

- הגנה במערכות מתוכנות (הגנה ברשות) 236350
- או אבטחת מחשבים 236652 או 236653 או 236607
- או השלמה עצמית של שיעור חולשות ב-236350

- מומלץ

- קומפילציה

- כדאי לזכור

- את'ם



3



הפטת איזע אט האקזא

- הודעות וציונים יועברו דרך מערכת GR
 - עליכם לוודא רישום במערכת GR כדי לקבל הודעות ושנוכל להזין לכם ציונים
 - זה אמור להתבצע אוטומטית למי שרשום רשמי למקצוע
 - הירשמו ליוםן של GR, וכן הסדנאות, הבוחן, המבחןים ותרגילי הבית יופיעו לכם אוטומטית ביוםן שלכם
- שקי הרצאות והתרגולים, פרטי צוות המקצוע ושעה קבלה, הודעות, ציונים, ופרטים נוספים באתר המקצוע

<http://webcourse.cs.technion.ac.il/236496/>

הסכין - מכון טכניולוגי לישראל

Reverse Engineering and Malware - 236653

אביב 2014

סילבוס

הודעות

מידע בללי

סילבוס

סגל

הנדסת תוכנה לACHINE – חורף תשפ"א

במסגרת הקורס נעסק בהנדסה לאחר של תוכנה. נלמד את השיטות המקובלות להנדסה לאחר, ואיך משתמשים בהן בפועל. נישם טכניקות אלה לחקר נזקот, ונלמד גם טכניקות אחרות המאפשרות דיזיין תוכנה או מיצע מתוך הנתונים על הדיסק, מתקשרת מחשבים והתקפות נוספות.



4



סיאום, תרגום וסיכום

- החלוקת בין השיעור והתרגול תהיה גמישה
 - לדוגמה – היום שעתיים שעתה הרצאה, בשבוע הבא שעתיים הרצאה + תרגול
- יתקיימו מספר סדנאות (תרגולי on-hands)
 - בשעות של השיעורים והתרגולים
 - בשאיפה – אחת לשולשה שבועות
- הסדנאות מבוססות על עבודה עצמית על מחשב
 - במקרה הצורך אפשר להפעיל את המחשב הווירטואלי הפוקולטי מהמחשב שלכם
 - במקרה שתקיימו שיעורים פרונטאליים – אנא הקפידו להביא מחשבים ניידים.



5



אפקט – מרכיבים

- המטלות במקצוע כוללות כ-4 תרגילי בית
 - כולם או רובם רטוביים
 - כולל תרגילים שדורשים השקעה רבה
 - משקלים לא זהים
 - בזוגות
 - ציון תקף
 - אין הגשה באיחור
 - במקרה מוצדקים (מילואים וכו') חובה לבקש אישור מהתרגל האחראי לפחות 24 שעות מראש



6



אבחן איזייל

- **מבחן –**

- בשני חלקים בני שלוש שעות (עם הפסקה ביניהם)
 - יש לגשת לשני החלקים באותו מועד

- **ציון סופי**

- מבחן 70%, תרגילים 30%
- ציון מבחן נמוך מ-54 לא ישוקל עם ציוני התרגילים



7



יואר קקזני

- העובדה היא שلق – כתוב אותה בעצמך
 - אין להעתיק מזרים
 - אל תשתמש בניתוחים קודמים של החומר אותו אתה מנתח
 - אחרת הציון יגיע למי שכותב אותו
 - אין לשתמש בדה-קומפיאלירים
 - הਪתרונות שלכם מהתחלה ועד הסוף
 - צטט מקורות
- ואם בכלל זאת עשית משהו אסור – אמרו זאת בפירוש
- **העוברים על הכללים יוננסו בחומרה**



המכשורות פאייזר

- **אתם מ提בקשים להתכוון לשיעורים**
 - על ידי קריית שקי השיעור הבא לפני השיעור
- כך נוכל לדון בעקרונות, ולא לעסוק בפרטים משנהים



9



סיכום

- רשימת הספרות נמצאת באתר המקצוע
 - ספרים נמצאים בספרייה
- בנוסף, קיים חומר רב באינטרנט
 - בפרט, תיאור מלא של אסמבלי של אינטל
 - link באתר המקצועי



10



אֲהָרְפָּאָקְ אַקְזִעָּא?

- המוצע יקנה כלים בסיסיים ל-RE של תוכנות וnoxious
 - בעיקר בהקשר של תוכנה שקובץ הרצאה שלה זמין
 - בחלקו הראשון של המוצע נציג עקרונות וכליים
 - בחלקו השני ניישם את הידע ונחקור נזקות פשוטות
 - בחלקו השלישי נרחיב גם לMKRI RE בעלי טכנולוגיות אחרות
- המוצע מתמקד בסביבת חלונות 32 סיביות
 - אך העקרונות זהים למערכות הפעלה ומעבדים אחרים
- נתיחס גם למניפולציות של קוד, ניתוח וירוסים, סביבות תוכנה שונות, ו-RE לMKRI ייחודיים אחרים
 - וגם נתיחס ל-RE של חומרה והתקפות ערוץ צד



11



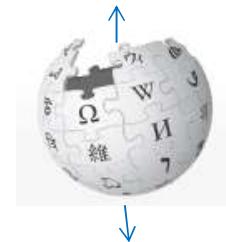
פרק 1

הנתקה מהרץ



נקודות

הנדסה לאחור היא תהליך של גילוי עקרונות טכנולוגיים והנדסיים של מוצר דרך ניתוח המבנה שלו ואופן פועלתו.



Reverse engineering is the process of discovering the technological principles of a device, object, or system through analysis of its structure, function, and operation.

הנדסה לאחור (RE) גם כוללת גילוי של מבני פרוטוקולים ושל קוד תוכנה, וכן גילוי מידע לא ידוע על מערכת עיינית ניתוח המבנה שלה ואופן פועלתה.



13



?RE מה



Apache
openO



Impress



Draw



- "זה לא עובד"

- "זה לא עובד מספיק טוב"

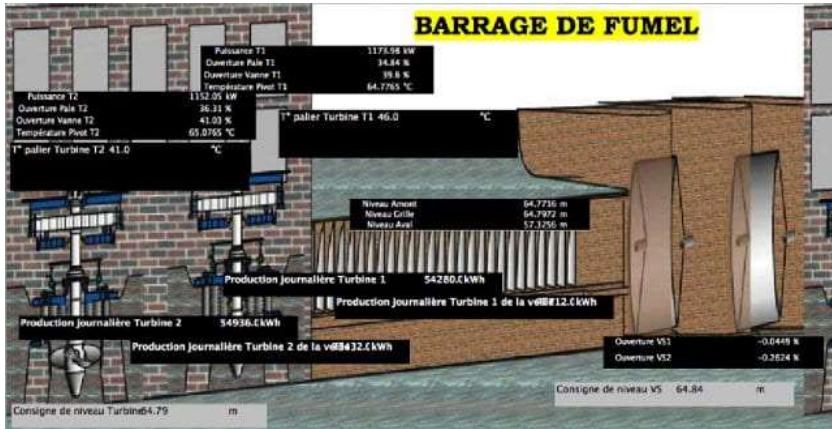
- "זה לא עובד איך שאני רוצה"

- "אני רוצה גם"

- "אני רוצה חלק מהשוק"



כראת הקיואם



- תשתיות לאומיות

- השתלטות על תחנות כוח והפסקת פעילותן
 - או שrifת הגרנטורים על ידי הגברת מהירותם מעבר למוטר
- השתלטות על אספקת המים
- מערכות רמזורים, מחלפי רכבות, וכו'
- מצלמות מהירות, ומצלמות אבטחה
- נניח שהיא מאגר ביומטרי שנטען להיות מוגן...

Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says

By NICOLE PERLROTH and DAVID E. SANGER MARCH 15, 2018

The Trump administration accused Russia on Thursday of engineering a series of cyberattacks that targeted American and European nuclear power plants and water and electric systems, and could have sabotaged or shut power plants off at will.



15

הנדסה לאחור – חורף תשפ"א

© פרופ' אלי ביהם, אביעד קרמל, עמר קדמייאל

22.03.2023



כראת ה-*סנואזון*

- נניח שבמקרים שלנו יש באג שמאפשר להחביא ממנו מטוסים או שנייתו לכבות אותו מרחוק – חיבטים לגלוות ולתקון
- על פי סנוואזון, ה-NSA גילתה עשרות בעיות אבטחה במערכות הפעלה וטלפוניים חכמים, ומשתמש בהם להאזנה
- דלתות אחוריות שהושתלו על ידי יצרן המערכת
 - או ש"טופלו" על ידי גורם אחר לפני או אחרי ההתקנה
- נפילת מזלייט בידי האויב : מה הוא יכול להבין ממנו?
 - וначיתת מטוס מיג בארץ... או הטרסקות מזלייט...
- השתלטות על מזלייט מרחוק, או השתלטות על לוין



חדשנות בעולם

אראן הציגה את המל"ט האמריקאי החמקן שהופל

מפקד חיל האוויר במשמרות המהפקה חשף את המל"ט הסודי שמרגל בשנים האחרונות לאחר אתרי הגראן: "יחידת הלוחמה האלקטרונית שלם הפילה אותו"

הארץ | פורסם להأشנה: 09.12.2011 | 18:47 | 08.12.2011 | עדכן ב: 00:07 | 09.12.2011 | 18:47 | 08.12.2011 |

| 45 | [↳ תגובה](#)

Ewen MacAskill in Washington
Sunday 22 April 2012 10.50 BST

the guardian
Winner of the Pulitzer prize

Iran claims to have reverse-engineered US spy drone
General says Tehran has extracted data and figured out workings of Sentinel craft captured last year



16



הנדסה לאחרית אחורית



- בעידן התעשייתי, עוד לפני עידן המחשב, הנדסה לאחרית הייתה נפוצה מאד
 - עוד לפני חוקי הפטנטים וזכויות היוצרים
- קל יחסית לבצע הנדסה לאחרית של מכונות
 - רכיבים פיסיים גדולים
 - אבל לעיתים מסתמכים על חומרים ייחודיים
 - בעלי תכונות מסוימות
 - למשל בשעוניים



17



גֶּזֶסָה מִזְמֹרֶת מִזְמֹרֶת

- בעידן המחשב – מסובך יותר – בגלל הקוטן והמורכבות
 - והקושי של פירוק למרכיבים
- אבל לא בלתי אפשרי
 - יתכן שהצורה של המוצר מדילפה מידע או שנייתן לזהות כזו באופן ויוזאלי
 - במעבדים מודרניים:
 - מיקרוסקופים ומיקרוסקופים אלקטרוניים
 - מדידת מתח בזמן הפעולה
 - הזפקת מתח למעבדים ומעקב אחריו התגובה
 - גרים מה לשגיאות בחישוב, ומעקב אחריו השינויים
 - קרייאת זיכרון, או האזנה ל-*bus*, אם אפשר
 - ועוד



18



גלאסה של תוכנה

נתרכז במרקדים
הלו רוב הזמן



- הבנת קוד תוכנה בשפה עילית
- הבנת קבצי הרצה (כגון EXE או a.out)
 - אוליזה סטטית – זה-קומpileציה
 - אוליזה סטטית – שפת מכונה
 - אוליזה דינמית – דיבגרים
- קוד בינאים ו-JIT – Java bytecode & .NET.
- רלונטי גם ל-
 - אופטימיזציה של קוד ע"י המהדר
 - בהינתן קוד המקור או ייצוג פנימי של המהדר
 - Post-link optimization
 - כלומר אופטימיזציה בהינתן קבצי הרצה
 - בדיקות אבטחה של קוד
 - תלויות במה הקוד עושה



גזרה מתחם: פלאוקסימ אקסים

- הבנת המבנה של פרוטוקולי תקשורת וקבצים
- טכניקות יכולות לשלב
 - האזנה לתקשורת (sniffing)
 - RE של התוכנה המתקשרת
 - שינוי נתוניים שנשלחו, או משלוח חבילות חדשות, ומעקב אחריו התגובה
 - בחינת קבצים
- **בכל המקרים הללו החוקר מתנהג כבלש : בוחן עדויות, חוקר, מחפש מידע חדש, מנתח מידע שהשיג, ואולי משנה תוכן ועוקב אחריו השינויים**



20



מה הנקה מתקנה?

- מחקר תוכנות תקינה לצורך פיתוח אמצעי הגנה ב��דים
 - למשל לצורך Antivirus
- חיפוש חולשות – לצורך פיתוח הגנות ב��דים
- Interoperability
 - צורכי פיתוח – לעיתים יש לבדוק את המערכת שעובדת כותבים קוד (לא הכל מתועד)
 - ניפוי הקוד שכתבנו
 - זיהוי מגבלות
 - הרחבה או שינוי בתוכנה שקשה לבצע דרך שינוי קוד המקור
 - תמיכה במוצר שהיצרן לא תומך בו או הפסיק לתמוך
 - בחינה אם אחרים העתיקו קוד שלך
- Forensics
 - זיהוי API של תוכנות, מ"ה, וכו'
 - וידוא שספריות מספקים אחרים עומדות בדרישות האבטחה של המוצר



21



מה הנקה מתקנה?

- סיבות לא חוקיות
 - עקיפת הגנה בתוכנה
 - פריצת תוכנה – Crack
 - חיפוש חולשות – מחקר לצורך פיתוח שיטות תקיפה
 - גניבת קוד ממוצר מתחילה
- כמובן שבמקרה זה לא עוסוק בפעולות לא חוקיות



22



אקלים יקואים בקורס

- RE של תוכנה
 - RE של BIOS של PC IBM, יצר את תעשיית תואמי ה-PC
 - פרויקט SAMBA של שיתופי קבצים תואם מיקרוסופט
 - Wine (биוצע RE ל-API של חלונות כדי להיות תואם לו)
 - RE של מבנה קבצים
 - Openoffice : פענוח מבנה קבצי DOC
 - RE של מכונת הצפנה וצפנים
 - RE של אניגמה על ידי הפולנים ממידע חלקי והודעות מוצפנות
 - פרסום צופן RC4
 - פרסום צפני A5 של הטלפונים הניידים
 - פריצת אייפון ואנדרואיד
 - Jailbreaking, Rooting
 - פריצת הגנות על זכויות יוצרים
 - DVD-CSS
- | | |
|-------------|--|
| 1980's | ▪ RE של BIOS של PC IBM, יצר את תעשיית תואמי ה-PC |
| 1990's | ▪ פרויקט SAMBA של שיתופי קבצים תואם מיקרוסופט |
| 1990-2000's | ▪ Wine (биוצע RE ל-API של חלונות כדי להיות תואם לו) |
| 1990's | ▪ Openoffice : פענוח מבנה קבצי DOC |
| 1932 | ▪ RE של אניגמה על ידי הפולנים ממידע חלקי והודעות מוצפנות |
| 1994 | ▪ פרסום צופן RC4 |
| 1999 | ▪ פרסום צפני A5 של הטלפונים הניידים |
| 2010's | ▪ Jailbreaking, Rooting |
| 2000's | ▪ DVD-CSS |



23



...התקלה מוחלטת

Intel AMT vulnerability. Life after CVE-2017-5689

The intention of this report is not only to show the story of "her majesty" Intel AMT vulnerability, or the CVE-2017-5689. This report describes possible ways and scenarios of exploiting the vulnerability as well. In addition this white paper outlines some new interesting "undocumented features" of Intel ME/AMT that can be used by an attacker. However, this will demonstrate how the capabilities of Intel ME/AMT can be used to their full extent to tinker with the very platform.

Beyond the Dark Portal:

Further research revealed, that there are some more things to worry about:

- Firmware (Intel ME/AMT) has security issues. Thus, web interface security weakness can be used to obtain remote access Intel AMT system.
- Hardware (Intel ME/AMT) has undocumented features. An illustrative example to it is MEI (HECI) communication protocol that can be reverse-engineered, thus making it possible for attackers to intercept the data and use it for their own benefit.
- There is a possible New stealth infecting computer system with malware that uses only common Intel AMT SoL capabilities to keep communication stealthy and evade security applications.
- If successfully exploited by attackers Intel ME/AMT capabilities become attackers' capabilities. Thus legit functionality will be used to perform non-legit actions



הפרק האחרון – הגנה מפני זיהוי

- קיימות מספר שיטות להגן נגד RE של תוכנה (או חומרה)
 - לדוגמה
 - יצירת קוד מורכב וקשה להבנה – Obfuscation
 - טכניות לבלבול והקשות על פענוח קוד – Anti-debugging
 - זיהוי האם הקוד רץ תחת דיבגר או מכונה וירטואלית
- משמש עבור
 - הגנת תוכנה נגד פריצה, העתקה, או שימוש לא חוקי
 - הגנה על נזקה מפנוי זיהוי וניתוח



25



סינרים גורוקוט

- מפתחי נזקות מהפשים אחרי חולשות לא מוכרות
 - חן צרכות לדעת
 - אין להסתיר את עצמו
 - אין להדביק תוכנות ומערכות אחרות
 - אין לגרום נזק
 - אין להגן נגד RE
 - RE משמש לגילוי החולשות ולהבנה של התוכנות המותקפות
- מגנים נגד נזקות צריכים להבין את דרך פעולה הנזקה
 - וחולשותיה, כולל כל ה"איך" לעיל
 - RE משמש למחקר נזקות, ולפיתוח שיטות זיהוי וניקוי שלהן



26



האם?



27

הנדסה לאחור – חורף תשפ"א

© פרופ' אלי ביהם, אביעד כרמל, עמר קדמייאל

22.03.2023



?RE פיראט



הנדסה לאחור – חורף תשפ"א

© פרופ' אלי ביהם, אביעד כרמל, עמר קדמייאל

22.03.2023



28



קאנט נייזט – כלwis מכם

- נמצא בהרבה מאוד מקומות



- כרטיסי אשראי
- כרטיסי כניסה
- ממיריים
- טלפונים סלולריים
- ועוד...



29

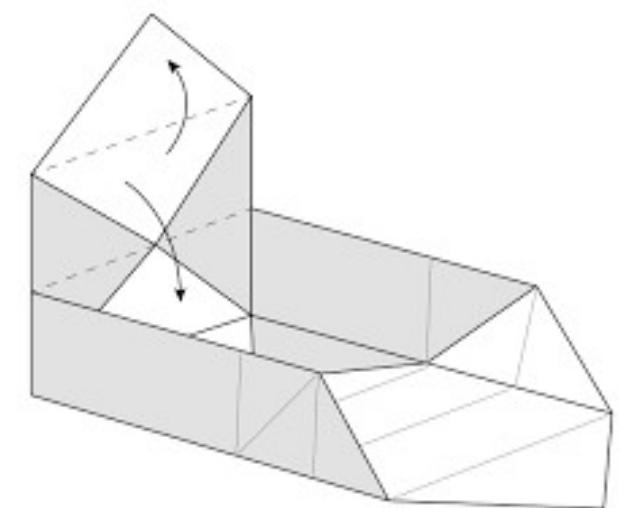
הנדסה לאחור – חורף תשפ"א

© פרופ' אליא ביהם, אביעד קרמל, עמר קדריאל

22.03.2023



Life as a box



30

הנדסה לאחור – חורף תשפ"א

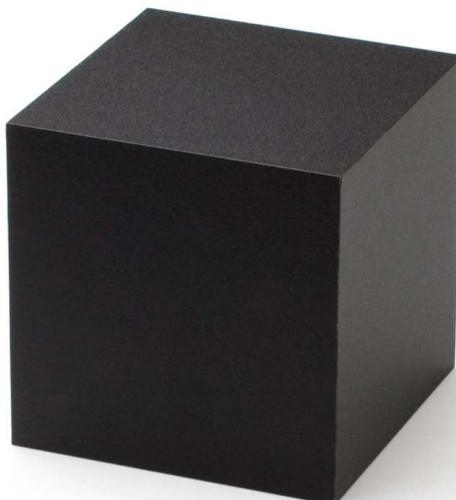
© פרופ' אלי ביהם, אביעד כרמל, עמר קדריאל

22.03.2023



Black Box

- הפעלה של המערכת הנבדקת
 - יתכן תוך איתgorה
- איפיון התוצאות

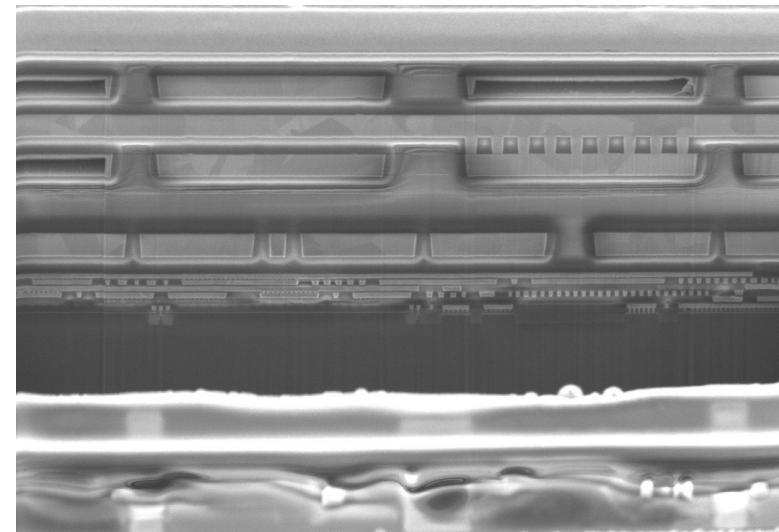
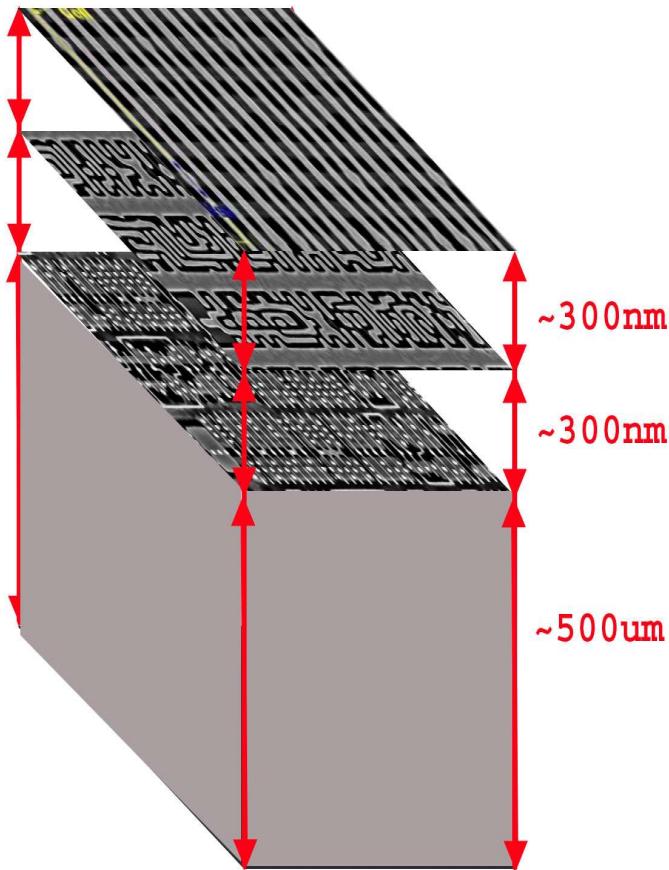


31



White Box

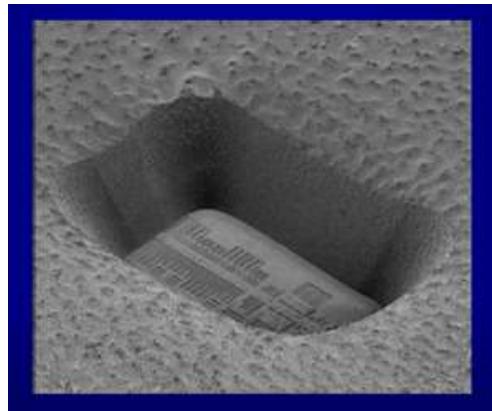
- הינה אינטימית של כל פעולה ופועלה במערכת



32



SEM



- מכשיר גדול ויקר ...
ומוגבל ברזולוציה

- יודע להבחין בין מטען חיובי
لمטען שלילי.

- דורש הכנה – עבודה על הכרטיס
וקילוף שכבות מעטפת



33

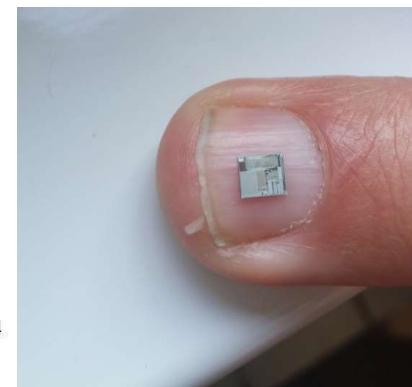
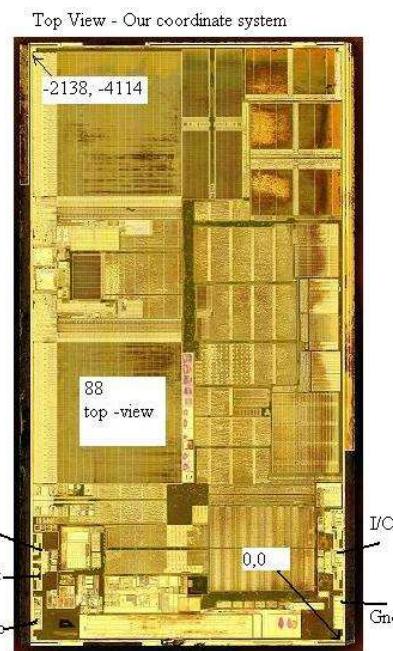
הנדסה לאחור – חורף תשפ"א

© פרופ' אליא ביהם, אביעד כרמל, עמר קדמייאל

22.03.2023



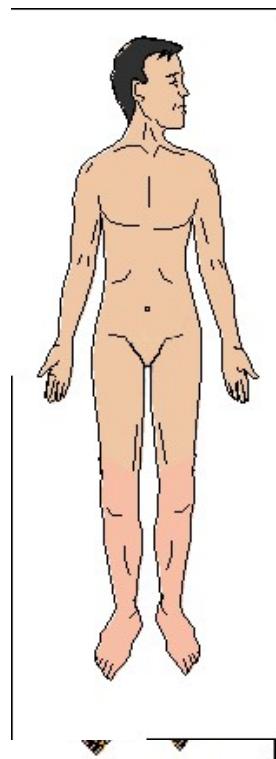
Chip Preparation



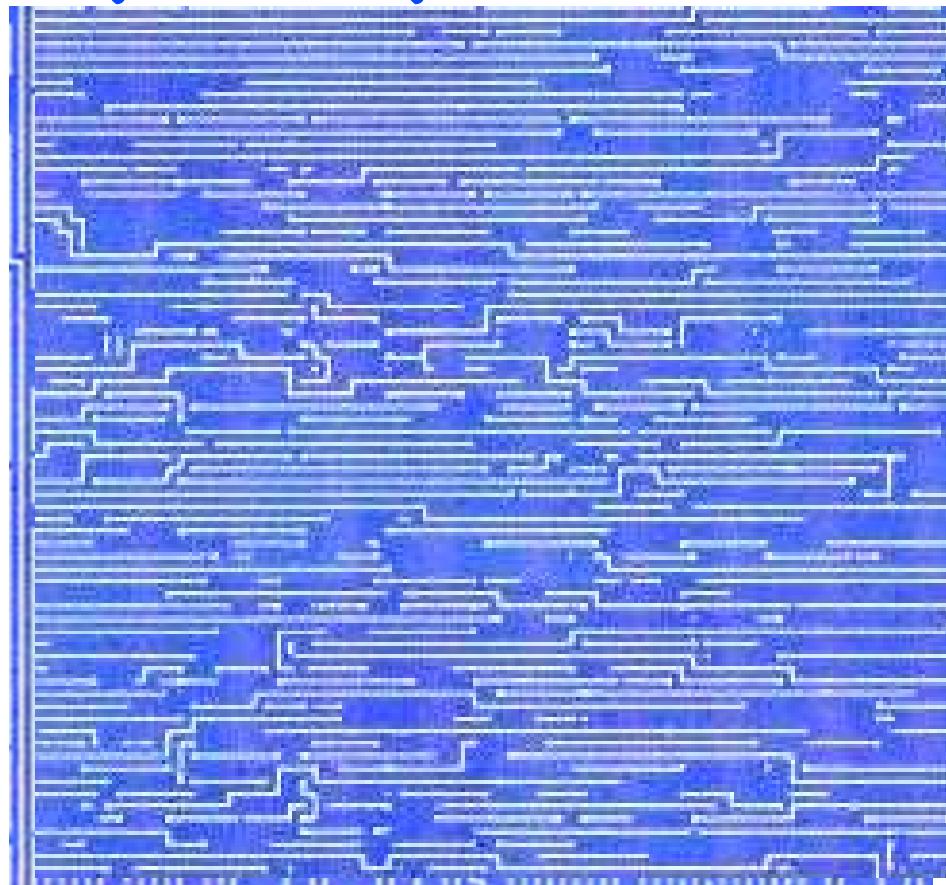
3

5

הגאומטריה - קווארכיהם



2/3/18



35

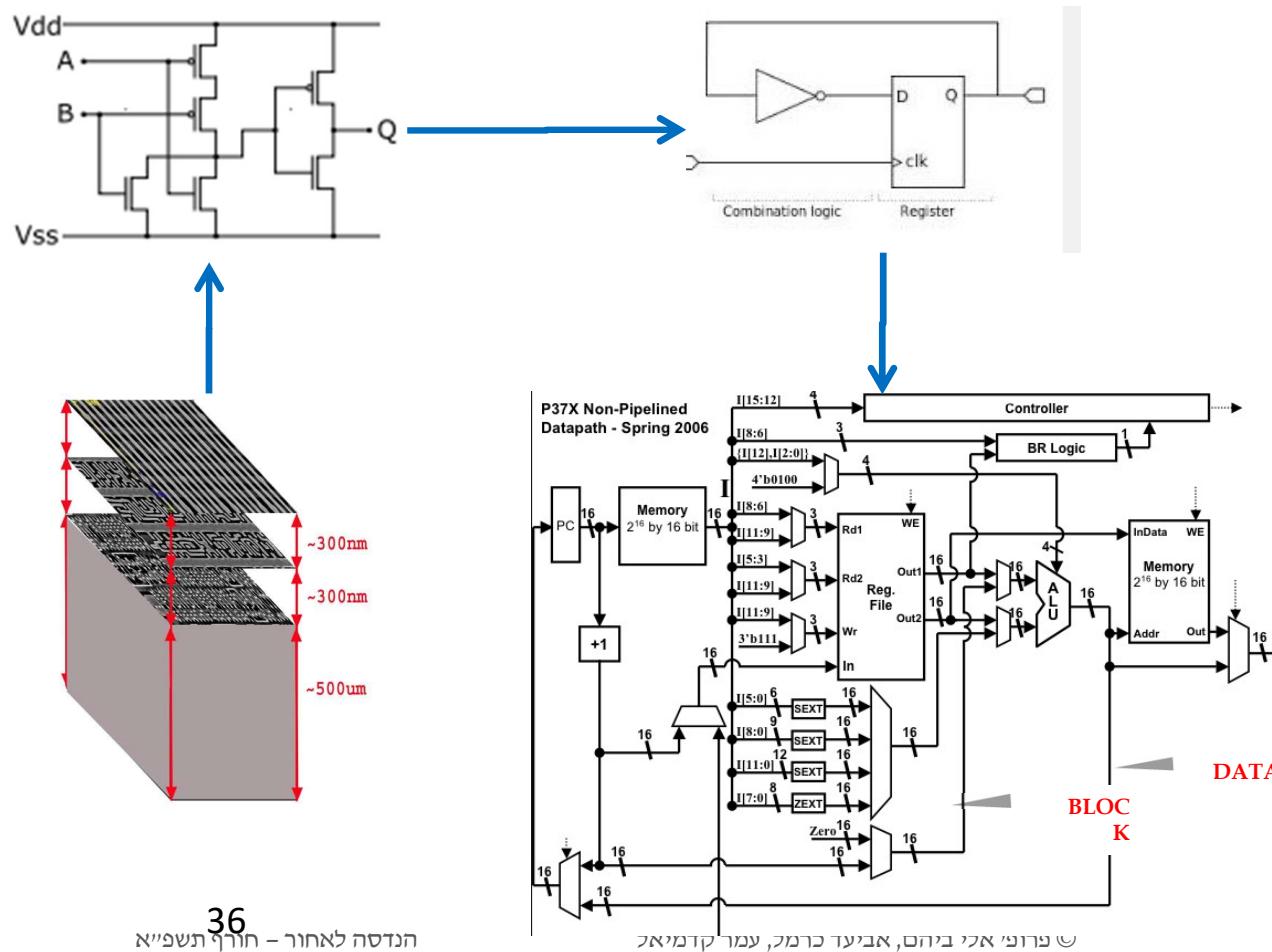
הנדסה לאחור – חורף תשפ"א

© פרופ' אלי ביהם, אביעד כרמל, עמר קדמיאל

22.03.2023



האנדרה הסופית - הינה בפניהם



36

הנדסה לאחור – חורף תשס"א

22.03.2023



אַלְפּוֹגָם Gray Box

- איתgor יותר מסיבי של המערכת הנבחנת
 - תוך בחינת ערוצים לא צפויים והכנסת שינויים במערכת
- מניפולציות אפשרות לחוקר להבין טוב יותר את המערכת הנבחנת ע"י
 - הוספה קוד לצורך דיבוג
 - משלוח הודעות נוספות לבחון את התגובה
- אבל גם כדי לשנות את פעלת המערכת
 - תיקון באגים, חולשות אבטחה, או התנהגות אחרת במערכות בהן אין לנו קוד מקור
 - הדבקת קובץ הרצה קיים על ידי וירוס
 - הוספה פונקציונליות לקוד קיים או לסדריות מערכת
 - עבورو אין לנו קוד מקור

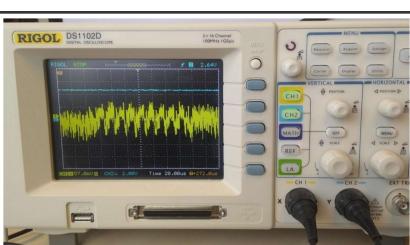


37



סינור סגיה ...

- בשנת 1943 חברת מעבדות בל מייצרת את המצפן (Python 131-B1) לצבא ולצי האמריקני.



- תיאורטיות : בלתי ניתן לשבייה (OTP)
- אחרי האספקה שמיים לב שכאשר מפעילים את המכונה, יש שינוי באוסילוסקופ שנמצא ליד...
 - אחרי מחקר מתברר שאפשר לפענה 75% מהקוד מרחק 30 מטר
 - אז מגדרים שאסור להתקרב...
- בשנת 1951 ה-CIA מגלה שהוא יכול לפענה את ההצפנה למרחק 400 מטר כשהוא יושב על קווי החשמל למכונה
 - הוסיפו פילטרים לחשמל, הרחיקו ל70 מטר ודרשו להפעיל 10 מכונות במקביל...



38



... כך היה

- חשו גם מרעש ייחודי של המכונה.
- ניסו למגן מפני רעש – והדבר הפך את הרעש ליוטר קל לזיהוי
- בשנת 1964, 40 מיקרופונים וסבכט מתכת הוכנסו לתוך תקרה של השגרירות האמריקאית במוסקבה.



39



אכז'ן

- לא תוקף את האלגוריתם אלא את מימוש מערכת המחשב
- מזlig מידע על החישוב הפנימי
 - מפתח קריפטוגרפי לדוגמא
- מדוע שיהיו ערוצי צד?
 - התוכנה לא רצה ב"חלל ריק"
 - אלא במסגרת פיזית ש"זולגת" אל הסביבה
- חלוקה
 - אקטיבי לעומת אסיבי



40



אכז'ן קסואיט

- תזמון
- אנרגיה (חשמל)
- פליות EM
- אקוסטי
- רعش מאוורר לדוגמא



41



קאנט ניינט – כלאים מכם

- נמצא בהרבה מאוד מקומות
 - CRTİSİ ASRÄİ
 - CRTİSİ CNIŞA
 - MMİRİM
 - TELEFONİM SİLOLARİYİM
 - VEBİD...
- הרבה פעמים הלוגיקה ידועה או קלה להשגה או לניחוש והדבר המעניין המרכזי הוא מפתח קריפטוגרפיה.



42



RSA Algorithm

- Encryption $C = M^d$
- Decryption $M = C^e$
- $C = M^{10011011} = (((((((((1*M)^2)^2)^2 *M)^2 *M)^2 *M)^2 *M)$

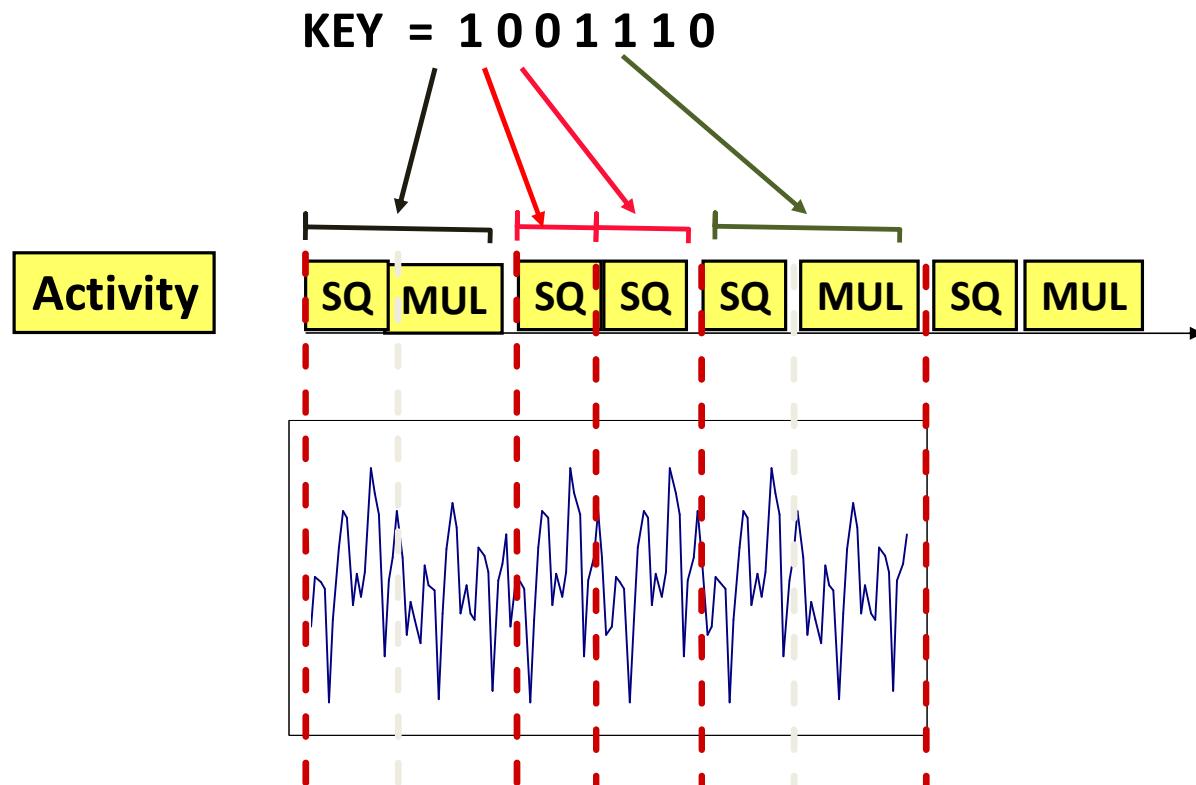
$$D_i = \begin{cases} 0 & \text{if } M \text{ is even} \\ 1 & \text{if } M \text{ is odd} \end{cases}$$



43



Using SPA to extract RSA key



Timing Attack 1

Compare two strings:

1st Case:

A: M O S K I T O

B: K ? ? ? ? ? ?

2nd case:

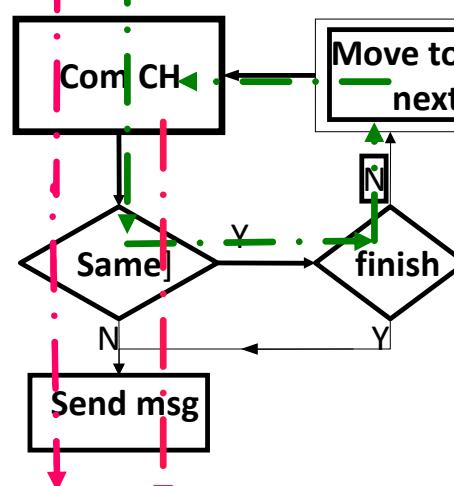
A: M O S K I T O

B: M L ? ? ? ? ?



$$A_0 \neq B_0 \quad A_0 = B_0$$

$$A_1 \neq B_1$$



Timing Attack 2

Secret String: **M O S K I T O**

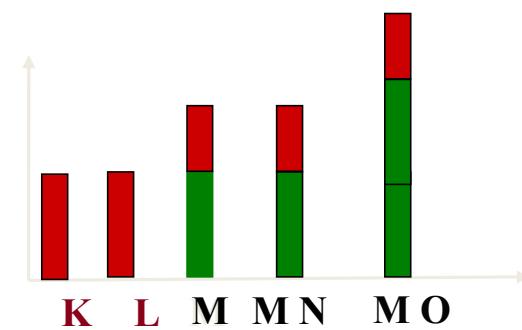
K X X X X X X

L X X X X X X

M X X X X X X

M N X X X X X

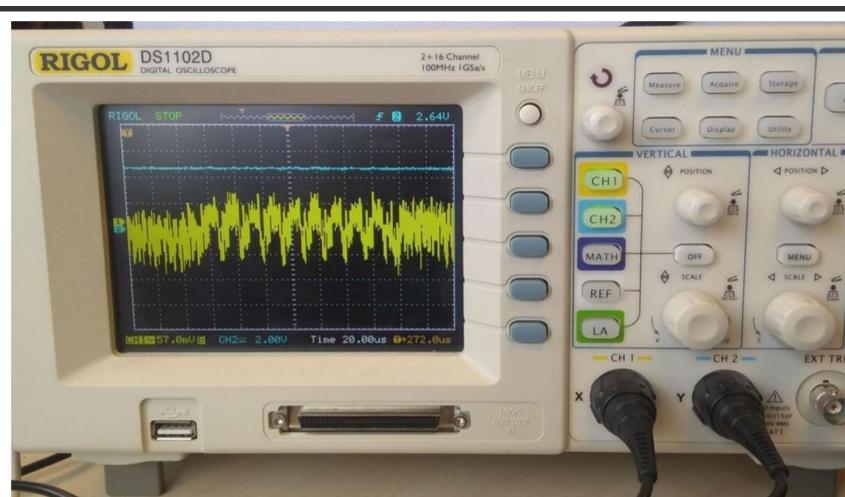
M O X X X X X



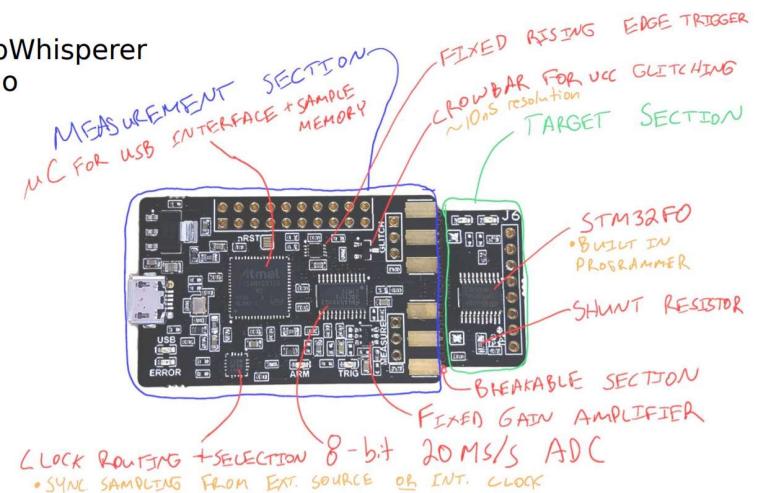
Complexity: $(7 * 26)$ instead of $26^7 = 8*10^9$



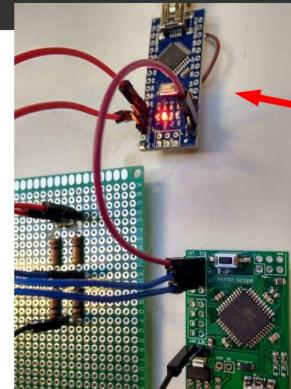
?kf - המ��לן



ChipWhisperer
Nano



Real world setup



We have:

“Target”:
Arduino Nano + AES

“Oscilloscope”:
HorrorScope

22.03.2023

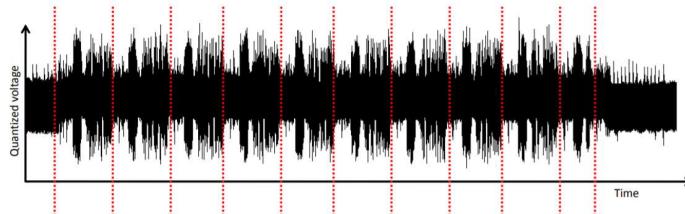


47

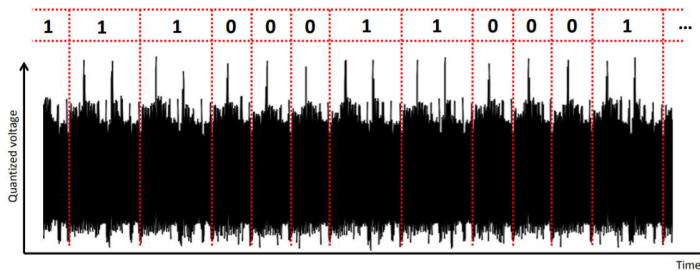


ההמפה!! ...

- ניתוח של Power על
כרטיס חכם...



- Unprotected software implementation of AES-128 on 8-bit µC
 - Ten rounds, last round shorter, without MixColumns
- Zoom-in until patterns appear:
 - Always point doubling
 - Sometimes point addition



48



WHAT IF WE TRIED
MORE POWER?

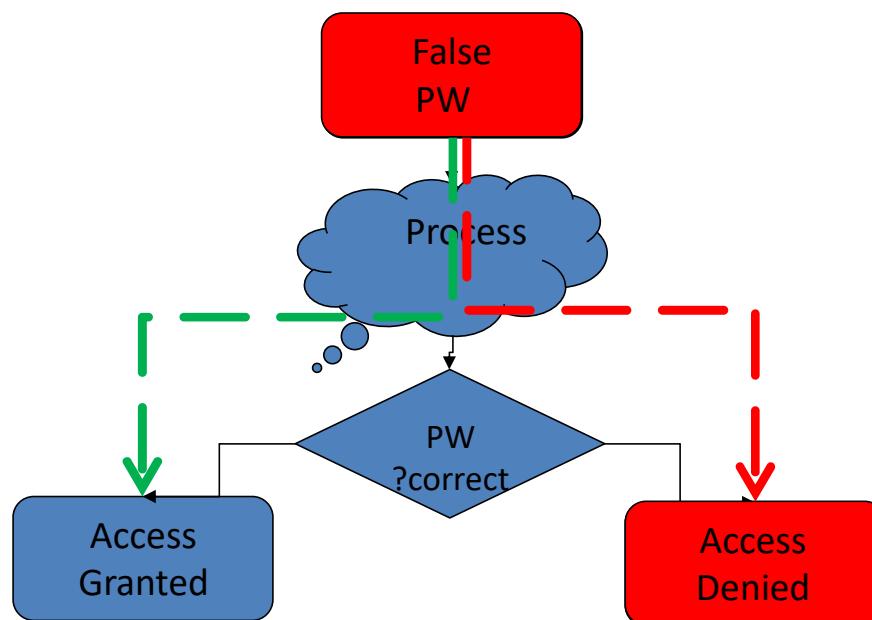
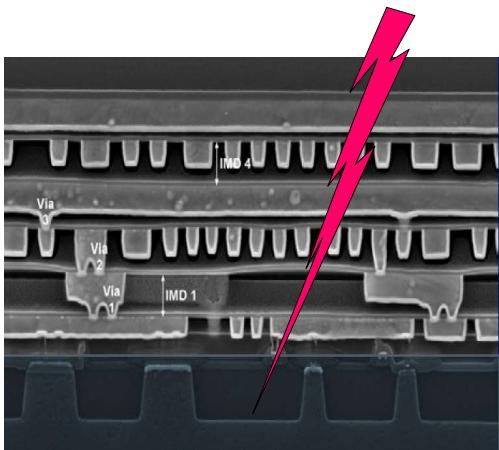


49



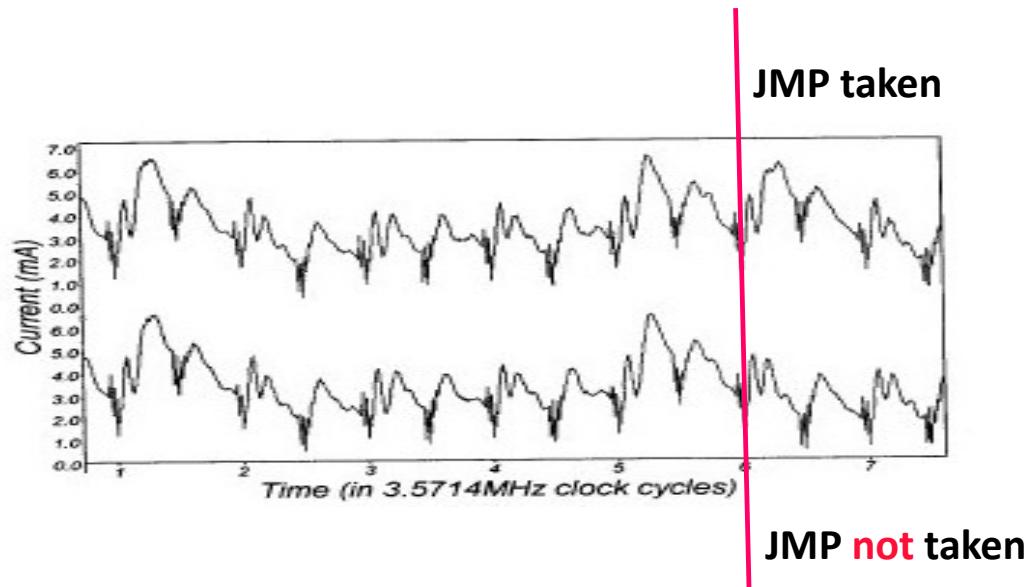
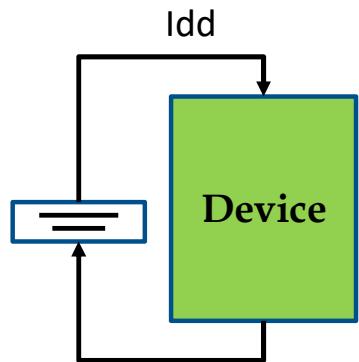
Optical Glitch Demonstration Bypassing Password

Light assist fault injection



SPA Simple Power Analysis

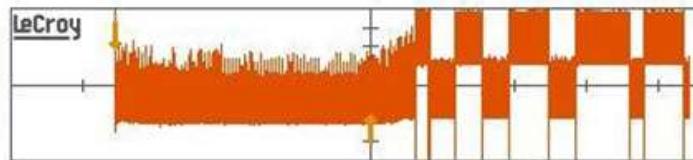
The current's profile reflects the internal activity



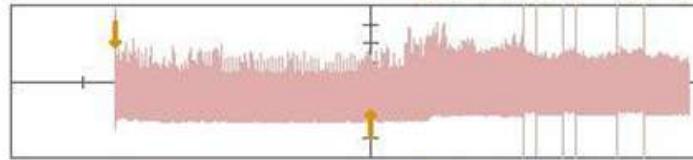
When to Glitch?

Monitor Power Consumption

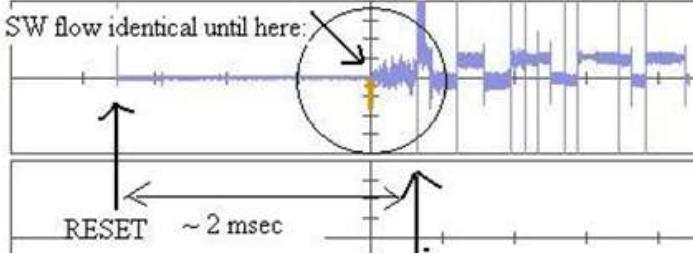
Idd for Flag = True



Idd for Flag = False



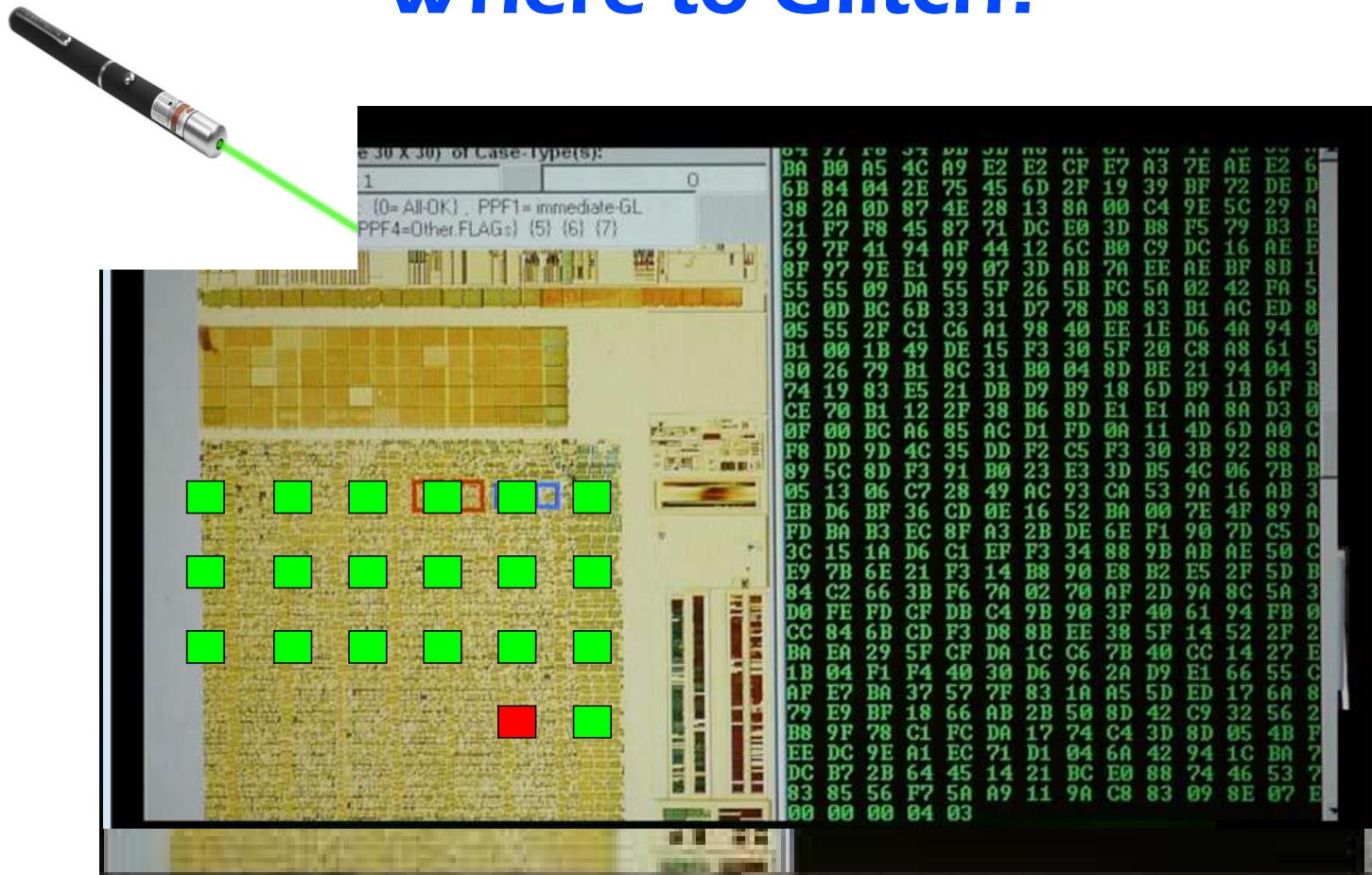
Idd Difference



52



Where to Glitch?



53



וְאֵה אָמָר מִיכָּרָה?



הנדסה לאחור – חורף תשפ"א

© פרופ' אלי ביהם, אביעד כרמל, עמר קדמייאל

22.03.2023



54



המסקה אמואזית: אלכנת הפעלה והלכדרון



55

הנדסה לאחור – חורף תשפ"א

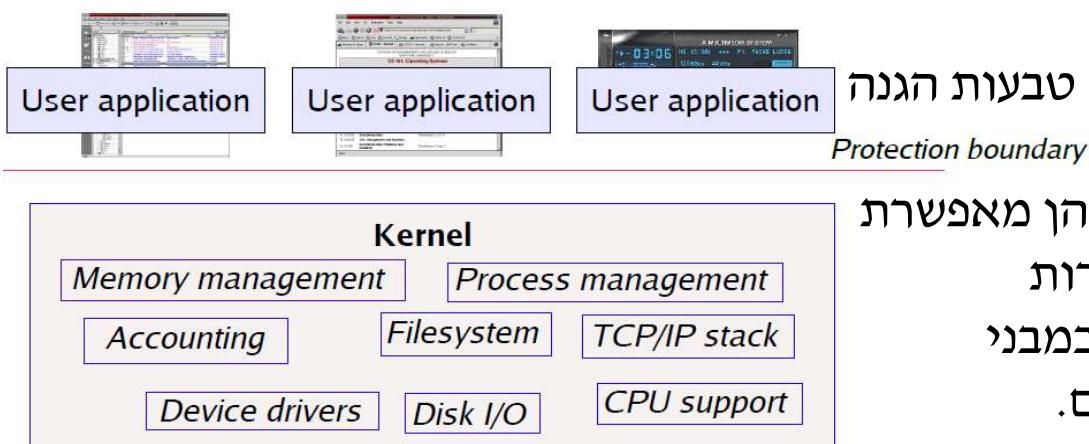
© פרופ' אלי ביהם, אביעד כרמל, עמר קדמייאל

22.03.2023



ארכיטקטורת הפעלה

- מתוכנת בין החומרה לבין התוכנה באופן "שקוף למשתמש"
 - אינה מאפשרת גישה ישירה לחומרה
- ניהול משאבי המחשב
- מייצרת לכל תהליך סביבה שבה הוא רץ
 - הפרדה בין תהליכיים
 - קשר בין תהליכיים
- מגנה על עצמה
 - ארבע (שתי) טביעות הגנה

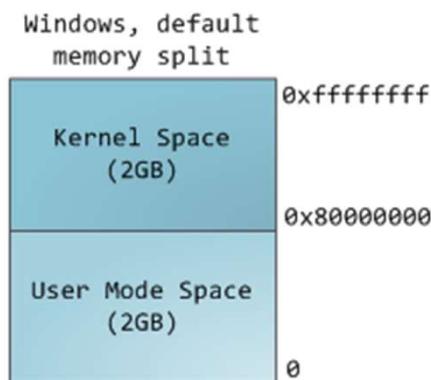


שכל אחת מהן מאפשרת
פקודות אחירות
ומשתמשת במבנה
זכרון אחרים.



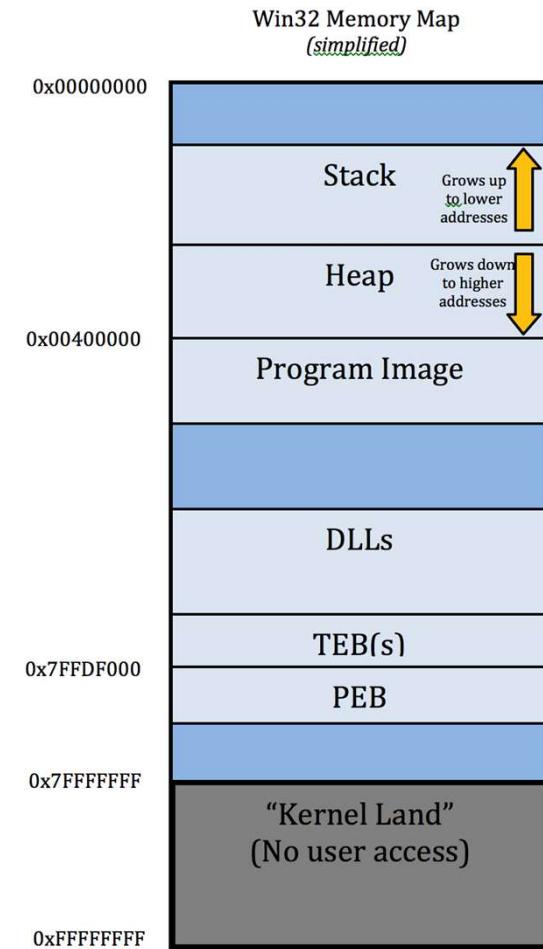
ריבוי זכרון

- לכל תהליך "יוזר" יש את מרחב הזכרון הווירטואלי שלו.
- כל קוד הkernel חולק מרחב זכרון וירטואלי יחיד.
- במערכת 32 ביט מרחב הזכרון הוא 2^{32} בתים (4GB)
 - החלק התחתון הוא מרחב הזכרון של היוזר
 - החלק העליון משמש למרחב הזכרון של הkernel.
- לקוד שרצה באזור היוזר אין גישה למרחב הזכרון של הkernel
 - האם הדבר נכון גם לkernel? למה?



ארכיטקטורת מחשוב

- **קוד** – Program Image■
עצמו. מכיל את הקוד (.text) ואת המידע (.data) של התהילה.
- **DLL-ים** – סדריות הנטענות למרחב הזיכרון של התהילה.
- **מבנה ניהול זכרון**■
Stack (מחסנית) – מחזיקה משתנים מקומיים, פרמטרים וכתובות חוזרת (עד בהמשך).
- **Heap** – משמש להקצת זכרון בזמן ריצה, מיועד למידע שנשאר אחרי הפונקציה שיצרה אותו.
- **טבלאות**■
لتהlixir (TEB) thread (PEB) ו�לאר (Peb) שמכילות את כל המידע הדרוש לצרכי ריצה.

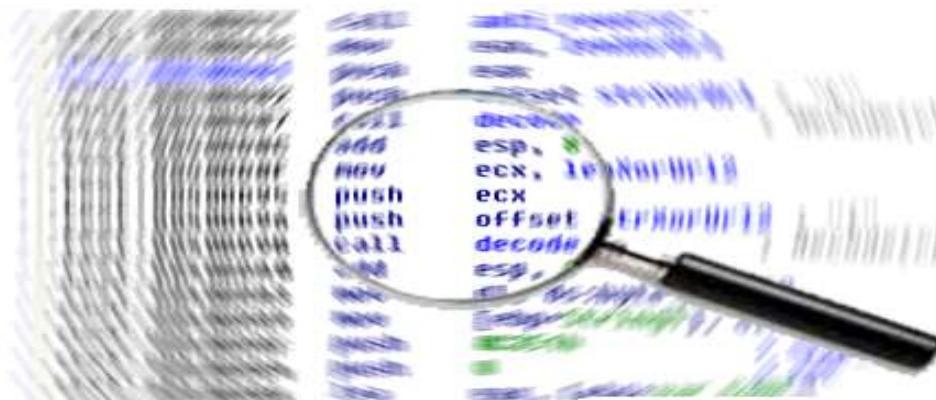


58



BlackBox \ GrayBox

מוכנה fe



59

הנדסה לאחור – חורף תשפ"א

© פרופ' אלי ביהם, אביעד כרמל, עמר קדמייאל

22.03.2023



אפקט וילסומר

- לעיתים מספיק להבין מה תוצרת הפעולה ללא להבין בדוק מה נעשה
 - שינוי קבצים אחרים
 - שינוי ה-registry
 - קריאה לפקודות מערכת הפעלה "משונות"
 - תקשורת החוצה
- הרבה מאוד מניתוח הנזקotas נעשה מ"בחוץ" ולא " מבפנים"
 - בדרך כלל מספיק להבין את התוצרים על מנת להבין שהמדובר בנזקה.
- אז מתי בכלל עושים (או מנסים לעשות) ניתוח קוד?



60



רימאות סירוסים באנט

SysInternals •

- סט כלים ותוכנות לניטוח וניהול מחשבי windows :

Process Explorer ○
Process Monitor ○
Autoruns ○
RootkitRevealer ○
ועוד כ-60 כלים.

- חברת שנקנתה על ידי MS

RegShot •

- הקלטה מצב המערכת registry וגם קבצים והשוואה למול מצב הבא.

• WINDBG Detours

- בדיקה אלו פונקציות מערכת הפעלה הופעלו..



61



קאנדיקן: קראפט

TextOutA	GDI32
GetStockObject	GDI32
VirtualAlloc	KERNEL32
GetCurrentProcess	KERNEL32
GetStartupInfoA	KERNEL32
GlobalAlloc	KERNEL32
GetWindowsDirectoryA	KERNEL32
GetWindowsDirectoryW	KERNEL32
lstrcmpW	KERNEL32
GetProcessHeap	KERNEL32
CreateFileW	KERNEL32
CreateWindowExA	USER32
RegisterClassExA	USER32
LoadCursorA	USER32
DefWindowProcA	USER32
ShowWindow	USER32
EndPaint	USER32
BeginPaint	USER32
InvalidateRect	USER32
SendMessageA	USER32
DestroyCaret	USER32
HideCaret	USER32
ShowCaret	USER32
CreateCaret	USER32
SetCaretPos	USER32
GetFocus	USER32
MessageBoxA	USER32
ReleaseDC	USER32
GetDC	USER32
UpdateWindow	USER32
GetMessageA	USER32
TranslateMessage	USER32
DispatchMessageA	USER32
LoadIconA	USER32

- הֆונקציות אליהן הקובץ עושה Import:

(נראה כי מדובר בתהליך עם ממashing שמתmesh. לא אופייני לנוזקה)



Process Explorer

▪ נשתמש ב- Process Explorer ▪

		3,913 K	1,999 K	104 Local Session (Explorer.exe)
explorer.exe		33,840 K	30,100 K	1856 Windows Explorer
vm	vmtoolsd.exe	9,960 K	7,920 K	1980 VMware Tools Core Service
	PwRISOVM.EXE	904 K	544 K	2000 PowerISO Virtual Drive Man...
	ctfmon.exe	1,056 K	1,632 K	160 CTF Loader
	cmd.exe	2,280 K	72 K	2084 Windows Command Processor
	procexp.exe	2.94	10,004 K	5940 Sysinternals Process Explorer
	Procmon.exe	16,092 K	1,372 K	2068 Process Monitor
	7faad9ed4a2e68d77a0d32ca2917e39f.exe	3.13	5,964 K	2632 Назначенные задания
	svchost.exe	8.82	12,596 K	5964 Generic Host Process for Wi...
	TPAutoConnect.exe	12,392 K	4,240 K	2496 ThinPrint AutoConnect comp...
IEXPLORE.EXE		7,416 K	17,252 K	4732 Internet Explorer
IEXPLORE.EXE		67,924 K	81,116 K	3220 Internet Explorer

- התחליק מפעיל את svchost.exe ונסגר.
 - חלק מהנוזקות מתחזות ל-svchost.exe.
 - אבל במקרה הזה הנזקה מפעילה את ה-svchost המקורי שבא עם הווינדוס.



63



הצאת sysinternals

- נשתמש ב-Process Monitor :

	svchost.exe	4788 CreateFile C:\Documents and Settings\Administrator\Desktop\sql\7faad9ed4a2e68d77a0d32ca2917e39\7faad9ed4a2e68d77a0d:
	svchost.exe	4788 QueryInformatio... C:\Documents and Settings\Administrator\Desktop\sql\7faad9ed4a2e68d77a0d32ca2917e39\7faad9ed4a2e68d77a0d:
	svchost.exe	4788 QueryAllInformat... C:\Documents and Settings\Administrator\Desktop\sql\7faad9ed4a2e68d77a0d32ca2917e39\7faad9ed4a2e68d77a0d:
	svchost.exe	4788 CreateFile C:\Documents and Settings\Administrator\Local Settings\Application Data\gapvfbsv.exe
	svchost.exe	4788 CreateFile C:\Documents and Settings\Administrator\Local Settings\Application Data
	svchost.exe	4788 WriteFile C:\Documents and Settings\Administrator\Local Settings\Application Data\gapvfbsv.exe
		4788 ReadFile C:\Documents and Settings\Administrator\Local Settings\Application Data\gapvfbsv.exe

- העתק את הווירוס למקום אחר בשם אקראי.
 - שם קובץ .gapvfbsv.exe
 - אפשר למצוא עוד דברים.



64



הצהמת sysinternals

■ נשתמש ב-Autoruns :

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\Software\Microsoft\Windows\CurrentVersion\Run				
Command Pro...			c:\windows\system32\cmdprompt.pif	8/4/2013 1:46 PM
fpro32			c:\windows\system32\fpro32.pif	5/30/2014 6:06 PM
Norton anti virus			c:\windows\rsv32.pif	5/30/2014 6:06 PM
PwRISOVM.E...	PowerISO Virtual Drive Man...	Power Software Ltd	c:\program files\poweriso\pwrisovm.exe	7/20/2013 3:18 PM
vm	VMware User ...	VMware Tools Core Service VMware, Inc.	c:\program files\vmware\vmware tools\vmtoolsd.exe	2/26/2013 5:30 AM
HKLM\Software\Microsoft\Active Setup\Installed Components				8/4/2013 1:30 PM
Address Book 6	Outlook Express Setup Libr...	Microsoft Corporation	c:\program files\outlook express\setup50.exe	4/13/2008 9:30 PM
Microsoft Outlo...	Outlook Express Setup Libr...	Microsoft Corporation	c:\program files\outlook express\setup50.exe	4/13/2008 9:30 PM
HKCU\Software\Microsoft\Windows\CurrentVersion\Run				9/22/2013 3:00 PM
nvjfrpja			c:\documents and settings\administrator\local settings\application data\gapvfbsv.exe	2/6/2014 4:51 PM
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce				3/22/2013 3:00 PM
FlashPlayerUp...	Adobe® Flash® Player Inst...	Adobe Systems Incorporated	c:\windows\system32\macromed\flash\flashutil32_11_5_502_110_activex.exe	10/29/2012 4:55 AM
HKCU\Software\Microsoft\Internet Explorer\Desktop\Components				8/4/2013 1:46 PM
0			File not found: About:Home	
HKLM\Software\Classes\ShellEx\ContextMenuHandlers				8/4/2013 4:20 PM
AnotePad++	ShellHandler for Notepad++		c:\program files\notepad++\nppshell_05.dll	6/18/2012 6:24 PM

■ רץ עם אתחול המערכת gapvfbsv.exe



65



סיכון קולאדי

- נסיק את המסקנות הבאות:
 - הווירוס הזריק קוד ל-svhost בזמן ריצה.
 - כי רץ svhost המקורי אך הוא התנהג בצורה שונה.
 - הווירוס הסתיר את ה-Import table שלו וייתכן שהוא שימוש ב-Packer.
 - הרי אנחנו יודעים שהוא שימוש ב-CreateProcess וזה לא הופיע ב-.Import table.
 - הווירוס ביצע עוד פעולה:
 - העתיק את עצמו למיקום אחר בשם אקראי.
 - הגדר את עצמו לרוץ עם אתחול המערכת.
 - ועוד פעולה שהיא ניתנת לגלוות באמצעות Procmon.
 - לפק לנו מספר דקודות לגלוות את כל זה.



66



כאי אקלים - לאי רקע

- בכל רגע נתון יש אלף גישות למערכת קבצים וכמו כן לא מעט תקשורת יוצאת/נכנסת.
 - הוירוס מהויה חלק קטן מהגישות האלו.
- יש צורך להכיר את המצב הנורמלי של המערכת על מנת להצליח לזהות את הפעולות החשודות.



67



Blaster – מוגפת קואקסיאלי

- תולעת Blaster הייתה פעילה החל מאוגוסט 2003
- הייתה התפשטה למאות אלפי מחשבים עם נזק מוערך של כ-320 מיליון דולר

זכורים?



68



Blaster – מוגפת קואקס

- כיצד התולעת הדביקה מחשבים?
- MS03-026 מתיחס לחולשת אבטחה מטיפוס חריגה מחוץ במנגנון RPC במערכות חלונות השונות (XP בין היתר)

Microsoft Security Bulletin MS03-026

Buffer Overrun In RPC Interface Could Allow Code Execution (823980)

Originally posted: July 16, 2003

Revised: September 10, 2003

- השירות היה פתוח כברירת מחדל בפורט 445, ולכן כל מחשב שהתחבר לאינטרנט היה בסיכון
- מציאת החולשה וכתיבת קוד שמנצל זאת (Exploit) הינו תהליך ארוך
 - שרובו נעשה באמצעות Reverse Engineering



69



Blaster מומצת - *knock*

- כיצד עצרו את התולעת?
- RE של התולעת אפשר לדעת
 - כיצד היא מתפשטת? (איזו חולשה צריך לסגור)
 - כיצד להסיר אותה מהמחשב?
 - איך לגלוות בזמן אמת שמחשב מודבק על מנת למנוע זאת?
 - מה המטרה של התולעת?
 - כיצד היא מקבלת פקודות מהמעביל?
 - וכו'



70



תאכלה RE



הנדסה לאחור – חורף תשפ"א

© פרופ' אלי ביהם, אביעד כרמל, עמר קדמייאל

22.03.2023



גאַפֿאָט אֲכֵלְה גָּזֶסֶת פְּאַמְּרָה מִוְכָּרָה?

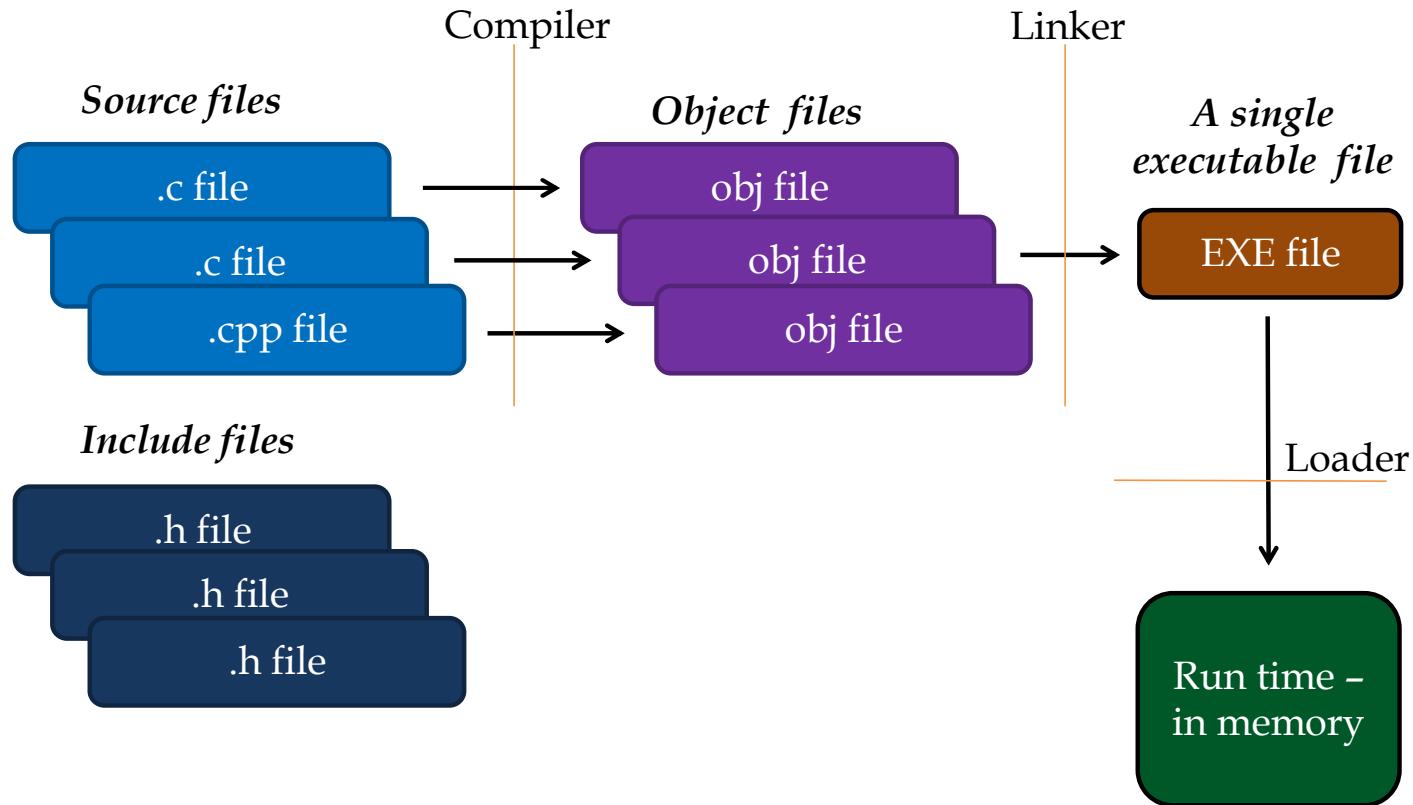
- הנדסה לאחר של תוכנה היא עצם ניסיון להבין למה המתכונת התכוון
- לצורך כך מאד חשוב להכיר את השפה שבה הקוד נכתב ואת מערכת הפעלה לעומקן
- ואיך מהדר מייצר קוד בשפת מכונה לפקודות שונות בשפה העילית
- ומאד מועיל גם להבין את צורת החשיבה של המתכונת המקורי ואת סגנון כתיבתו, שייעזרו להבין את מה שהוא התכוון לעשות
- ולהשווות ל"איך אני הייתי כותב את זה"



72



C++/ C-ה הרכבת וההציג



73



איךagi קידוך

- למרות שקובץ ההרצאה בחלונות הוא תמיד באותו פורמט ואוֹתָה שפת מכונה, כל מהדר יוצר קוד שונה
 - 3 שורות ב-C יכולות להתדר למספר שורות באסמליל, בעוד שאותו קוד שנכתב ב-VB יכול להתדר למאות שורות
 - ואתו קוד ב-C יתרגמו על ידי מהדר אחר באופן אחר
 - וכמובן, ניתן להוראות מהדר לבצע אופטימיזציות מסווגים שונים וכך ליצור קוד שונה (כפי שתראו בתרגיל הבית)

קוד

הידור וlienck

EXE file



74



המהפיק הפק

- כדי להבין קובץ הרצאה, כדאי לדעת מהי השפה שבה נכתב הקוד ואיזה מהדר היה בשימוש
 - בהרבה מקרים קל לשלוּף את המידע הזה מקובץ הרצאה, על פי הספריות שבשימוש, ומידע אחר הנמצא בקובץ
- לעיתים בקובץ הרצאה יש מידע נוסף לינקר וואו לדיבגר שיכול לכלול שמות פונקציות ושמות משתנים
- ידע זה עוזר לזהות מבנים באסמבלי ולתרגם בקלות לקוד
- כמו כן, משתמשים בכלים שעוזרים לפענח את פקודות המכונה לקוד ברמה גבוהה יותר

קוד או אלגוריתם

← RE

EXE file



75



מה קורע זה לא ?knclz

```
mov    ebp, esp
mov    eax, 186F8h
call   sub_4180E0
mov    eax, dword_41F094
xor    eax, ebp
mov    [ebp+var_10], eax
call   anti_reverse
mov    eax, lenXorUrl
push   eax
push   offset strXorUrl ; "("
call   decode           ; decode(char *buf, unsigned int len)
add    esp, 8
mov    ecx, lenXorUrl2
push   ecx
push   offset strXorUrl2 ; "("
call   decode           ; decode(char *buf, unsigned int len)
add    esp, 8
mov    dl, ds:byte_41ACF9
mov    [ebp+String1], dl
push   0C351h           ; size_t
push   0                 ; int
lea    eax, [ebp+var_C38F]
push   eax               ; void *
call   _memset
add    esp, 0Ch
mov    cl, ds:byte_41ACFA
mov    [ebp+var_186F0], cl
push   0C351h           ; size_t
push   0                 ; int
lea    edx, [ebp+var_186EF]
push   edx               ; void *
call   _memset
add    esp, 0Ch
mov    al, ds:byte_41ACFB
mov    [ebp+var_30], al
xor    ecx, ecx
```

כמה זמן לוקח להבין מה הקוד הבא
עשה? (אל תנסו)

האם זה אפשרי למצוא את קטע
הקוד הרלוונטי לנו מתוך מיליון
שורות אסמבלי?

האם כותב הווירוס יכול להוסיף
cosaוי נוסף במכובן?

לפי שמות הפונקציות הנקראות
מקוד זה, אפשר לנחש שהקוד כתוב
ב-C (למשל קוראים ל-memset על ידי
שהוא מנסה להגן נגד RE על ידי
פעולות נגד RE וע"י הצפנה).



Java Bytecode & .NET

- ישנן שפות שמהוודרות לקוד ביניים (Bytecode)
 - לכל שפה כזו את יש מכונה וירטואלית
 - שמרתגמת בזמן ריצה מקוד הביניים לאסמבלי (JIT)
- אחד היתרונות בשיטה זאת הוא האפשרות להריץ את אותו הקוד במערכות הפעלה שונות וארכיטקטורות שונות בקלות
 - Java רצה בכל מערכות הפעלה לרבות פלאפונים ושעונים
- תכניות.NET. (למשל C#) מהוודרות לקבצי הריצה (EXE)
 - הכוללים קוד אסמבלי וקוד ביניים (CIL, נקרא בעבר MSIL)
 - קוד האסמבלי שנמצא שם אחראי להרצת קוד הביניים C-JIT
 - זיהוי: קבצי EXE משתמשים ב-.dll(msil) נכתבו ב-.NET.
- בדרך כלל מחקר Bytecode לא נחשב מסובך
 - המון מידע נשמר בקובץ
 - ניתן לחסית בקלות להבין מה היה הקוד בשפה העילית
 - יש כלים אוטומטיים שמקלים על כך



קונסיסטנטיות כבידה בסקירה

מה עושה הקוד הבא?

```
mov    DWORD PTR [ebp-16], 0          → s
mov    DWORD PTR [ebp-12], 0
jmp    L2
L1:   mov    eax, DWORD PTR [ebp-12]    → i
      add    DWORD PTR [ebp-16], eax
      add    DWORD PTR [ebp-12], 1
L2:   cmp    DWORD PTR [ebp-12], 99
      jle    L1
```



קואקסיאלי knf מודול

הוא שקול לקוד הבא, בהחלפת הgiשות לזיכרונו ברגיסטרים :

```
mov s, 0
mov i, 0
jmp L2
L1: nop          (was: mov i, i)
      add s, i
      add i, 1
L2: cmp i, 99
      jle L1
```



קואקסיאלי knf כבידה

בחירה מושכלת של שמות משתנים תקל علينا את ההבנה של הקוד :

```
mov s, 0           sum=0;  
mov i, 0           i=0;  
jmp L2             goto L2  
L1: nop            L1:  
    add s, i        sum += i;  
    add i, 1        i++;  
L2: cmp i, 99      L2:  
    jle L1           if(i<=99) goto L1;  
                           Here i=100 and  
                           sum=0+1+2+3+...+99=4950
```



חוק

- במדינות רבות הנדסה לאחרור אינה חוקית בעוד באחרות מותר
 - האיסור תלוי בין השאר בהסכם של הלוקה עם הספק, חוקי זכויות יוצרים, וחוקים מיוחדים נגד RE
 - כמעט בכל הסכם תוכנה כתוב שאסור לבצע RE
- ברוב המדינות מותר לבצע RE לשם השגת interoperability
 - אבל לא ליצירת מוצר מתחילה המעתיק את המקור
 - בחלק מהמדינות חל איסור גורף לפרסם מידע שהושג על ידי RE
- שימושו לב שקוד תוכנה עשוי להיות מוגן בזכויות יוצרים
 - ולכן צוותים המבצעים RE לשם פיתוח מוצר אינם מתקשרים ישירות עם הגורמים שמשתמשים בתוצרי ה-RE
 - אלא דרך מסמכים בלבד המפרטים את הנדרש
 - ולא פירוט בכתב קוד



אכג"ג: חוק ה-DMCA

The Digital Millennium Copyright Act

- חוק אמריקאי המסדיר זכויות יוצרים של מידע דיגיטלי
 - למשל, מוסיקה, סרטים
- במקרים מסוימים, הוא אוסר על אנליזה של מערכות המיועדות להגנה על זכויות יוצרים, אפילו לצורך מציאת חולשות והבנת הנדרש לחיזוק המוצר
 - דוגמא: קוד ה-CSS לסרטים וידאו ב-DVD



מה Ifke?



83

הנדסה לאחור – חורף תשפ"א

© פרופ' אליאב יהם, אביעד כרמל, עמר קדריאל

22.03.2023

