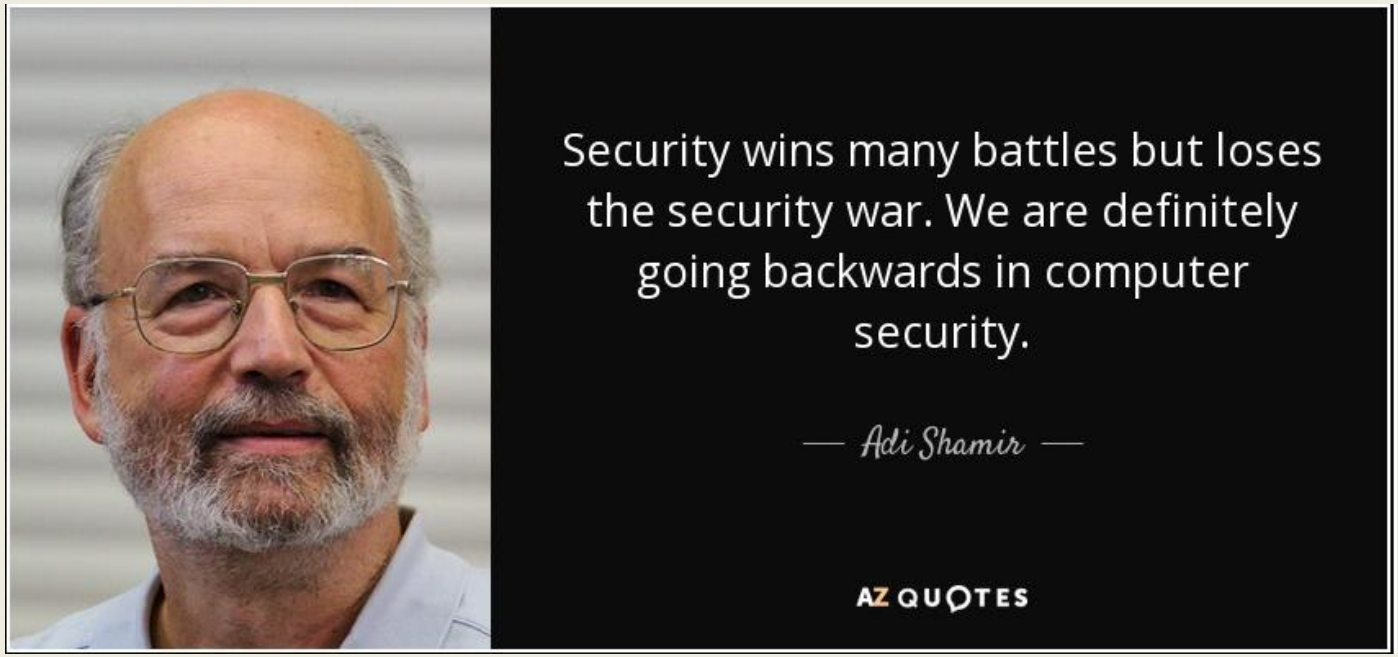
Emission Security
אבטחת דליפה

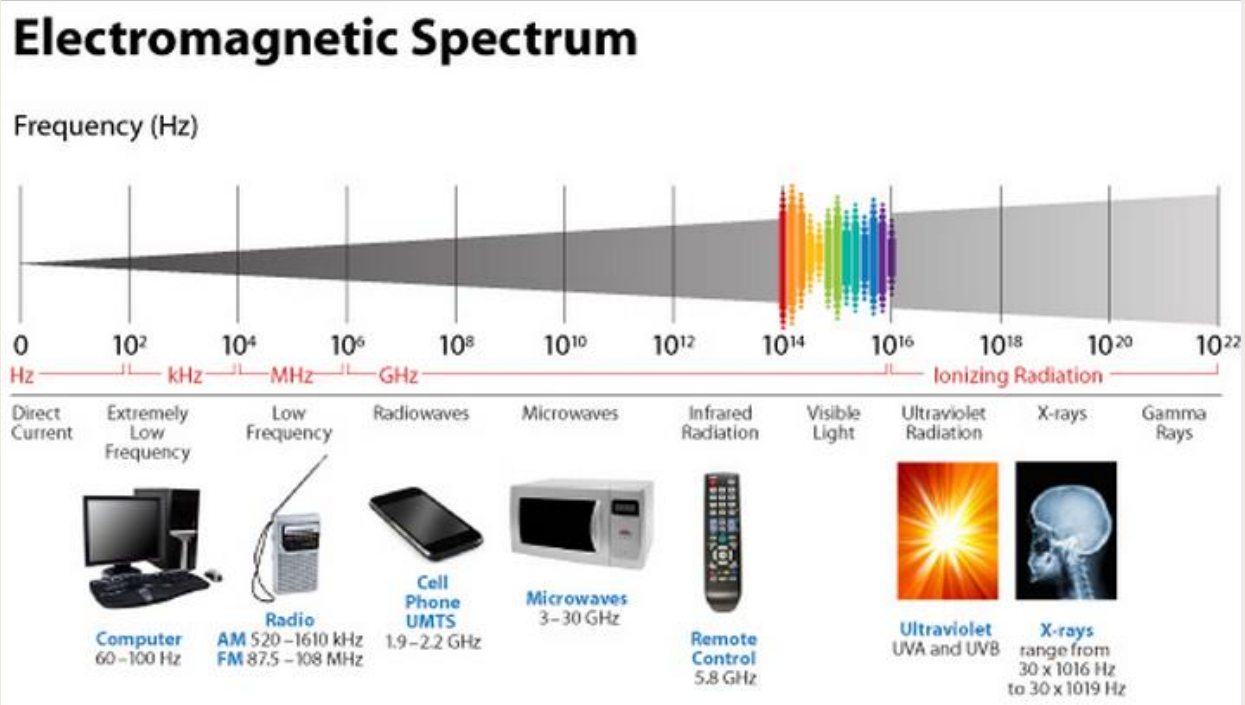


סמינר באבטחת מידע
פרק 17 מתוך הספר "Ross Andresson's "Security Engineering

מרצה – פרופ' אור דונקלמן
מוגש ע"י – דוד טריגר

מהי דליפה (Emission)

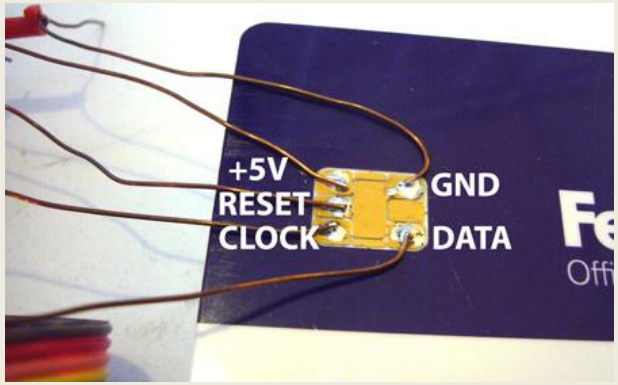
- העולם של היום מנוהל ע"י מכשירים חשמליים
- זרם חשמלי => שינוי בשדה אלקטרומגנטי
- <u>Side channel attacks – מנצלים חולשת מימוש פיזי</u>



מתוך ויקיפדיה

אבטחת דליפה – למה?
Emission Security – why?

- בארגונים צבאיים דליפה של מידע = חיי אדם



dangerousprototypes.com

- כרטיסים חכמים:
  - כרטיסי אשראי
  - SIM
  - כרטיסי עובד

  ניתנים לגניבה, פתיחת הכרטיס לשימוש שלא נועד אליו

- דליפה אופטית (אור), תרמית (חום), ואקוסטית (קול)

אבטחת דליפה – למה?
Emission Security – why?

- נגיש לתוקפים
- מהירות המעבדים עולה, וכך גם עוצמת הקרינה הדולפת
- התקפה כמעט ולא משאירה עקבות

ויקיפדיה

הקושי (למה לא?)

- יקר
- דורש תכנון של הסביבה
- "זה עובד אז אל תיגע"
- קשה לבדוק עמידות של מערכת ל**כל** ההתקפות האפשריות

קצת היסטוריה

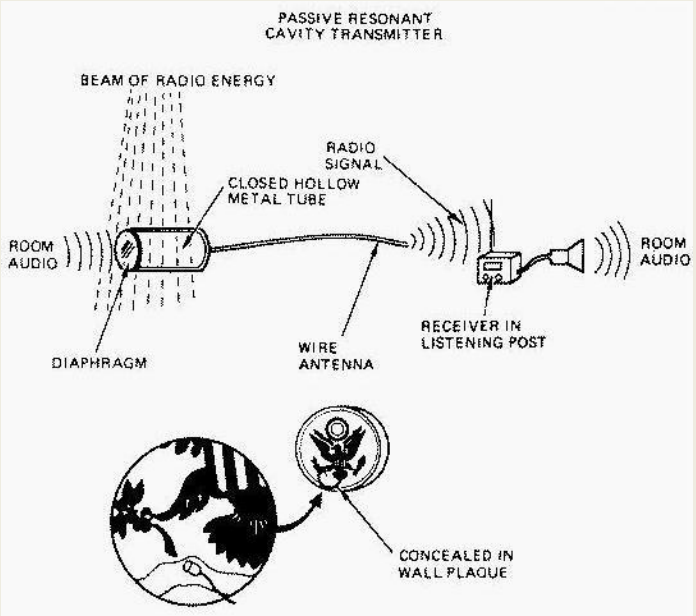
- **1914** – האזנה לדליפה בקווי טלפון חד-חוטיים
- **1915** – מכשירי האזנה:

  - טווח 30 מטר לשיחות טלפון

  - טווח 100 מטר למורס
- **1916**- נאסר השימוש בקווי תקשורת חד-חוטיים בטווח קילומטר מאזור מלחמה
- **1939**- ניווט באמצעות רדיו

קצת היסטוריה

- כיתת תלמידי יסודי ברוסיה הביאה מתנה נדיבה לשגרירות האמריקאית ב1946
- הסמל הלאומי חצוב בעץ
- בשנת 1952 התגלתה חציבה בגב המתנה הנ"ל שבעצמה לא כללה משדר, אך כאשר הוקרנו עליה גלי מיקרו, היא אפשרה האזנה



התמונות מתוך ויקיפדיה

קצת היסטוריה

- **1960** – רשות המס הבריטית מחפשת מעלימי מס טלוויזיה
- **1960** - בחלק מקווי התקשורת נוסף על התעבורה המוצפנת עובר עוד אות חלש - המידע עצמו (לא מוצפן)
- **1970** – Emission security נמחק מהספרות ונהיה תחום צבאי\מדיני חסוי ביותר
- **1985** – התחום חוזר עקב מאמר של Wim van Eck- שחזור תמונת מסך ממרחק

מעקב באמצעות טכנולוגיה

- ההתקפות הנפוצות ביותר משתמשות בפונקציונאליות קיימת וחורי אבטחה קיימים
- בסופו של דבר - קלט של מערכת מוקלד ע"י משתמש דרך מקלדת או מוקלט דרך מיקרופון
- הפעלת פלאפון או מצלמה\מיקרופון של לפטופ ע"י קוד זדוני

מעקב באמצעות טכנולוגיה

- אמצעים העומדים לרשותנו:

- בזול , נוכל לרכוש "bug"

- בטווח הבינוני, "bug" יותר מתקדם ומשדרים\מקלטים מתקדמים

- בטווח היקר, האזנה אופטית

התגוננות ממעקב באמצעות טכנולוגיה

Kjbsecurity.com

- **nonlinear junction detector** – מכשיר השולח גלים בתדרים שונים, אם הגל המוחזר עבר מודולציה אז כנראה הוחזר מרכיב חשמלי

- **surveillance receiver** – קולט גלים בתדרים 10KHz – 3GHz על מנת לחפש סיגנלים משונים

Shutterstock

- הגנה מפני האזנה בעזרת מכשירי לייזר – תשתלו עצים במשרד...

התגוננות ממעקב באמצעות טכנולוגיה

- **בעיה**: על כל התקדמות קטנה בטכנולוגיה אצל התוקפים, ההגנה עולה לנו פי כמה וכמה
- נשים את הבסיסים הצבאיים מתחת לאדמה ונקיים שיחות סודיות רק בחדר ממוגן אחד...
- Furby, צעצוע שלומד לדבר על פי דיבור שהוא שומע, נאסר להכנסה לכל המתקנים של NSA

Badforyoubook.com

התקפות פאסיביות

- <u>התקפות פאסיביות הינן התקפות שלא מצריכות התערבות המתקיף במתרחש, אלא רק האזנה</u>

- מחולק לשתי קבוצות:

- **Hijack** : סיגנל חשמלי – חוטי חשמל, קווי טלפון...
- **Tempest** : קרינה אלקטרומגנטית – רדיו, מסך...

- לפעמים נעבוד בשילוב של שתיהן

התקפות פאסיביות – דליפה במוליכים

- עוד מתחילת המאה ה19 שמו לב לתופעה
- התדרים הגבוהים נוטים לדלוף יותר
- כמות הדליפה של כבל משפיעה על העלות שלו

התקפות פאסיביות - הפרדת אדום-שחור

- ציוד מחולק ל2 קטגוריות:

1. **אדום – מכיל מידע רגיש כמו Plaintext**
2. **שחור – נגיש לכולם**

- התקנים של NATO ושל הNSA בתחום הינם חסויים

- החלוקה מגדירה איזה ציוד צריך תשומת לב מיוחדת ואבזור מתאים

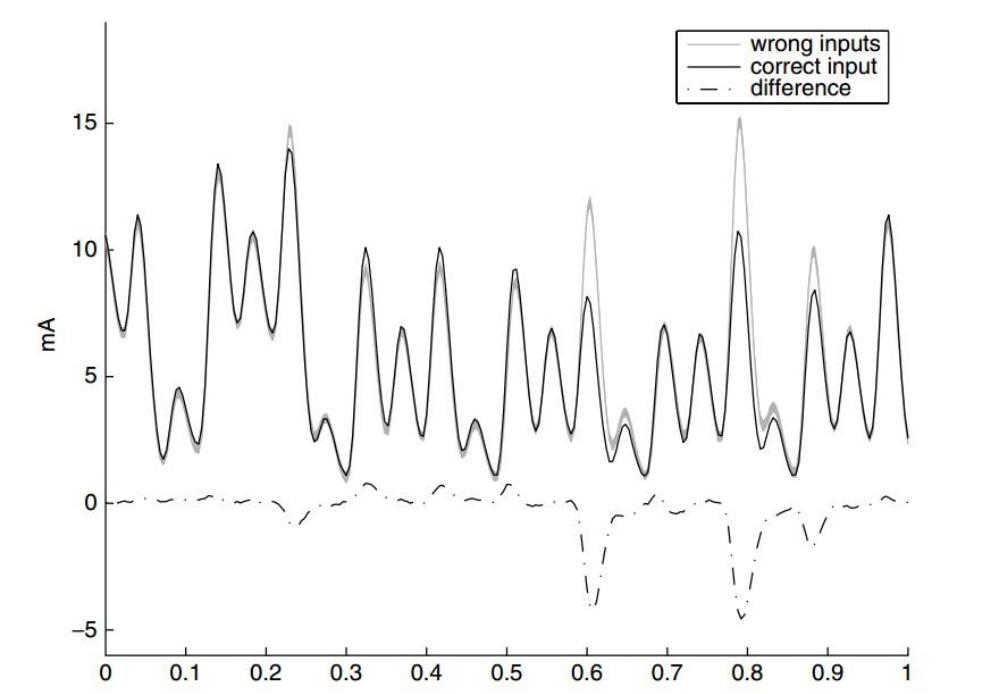
התקפות פאסיביות – התקפות תזמון

- ניתן לתקוף בהצלחה אלגוריתמי הצפנה הנמצאים בשימוש רחב (כמו הRSA וDSA)

- התקפות המבוססות על Cache misses - ניתן לגלות את המפתח של AES ע"י התבוננות בכמה מאות הצפנות

התקפות פאסיביות – צריכת כוח

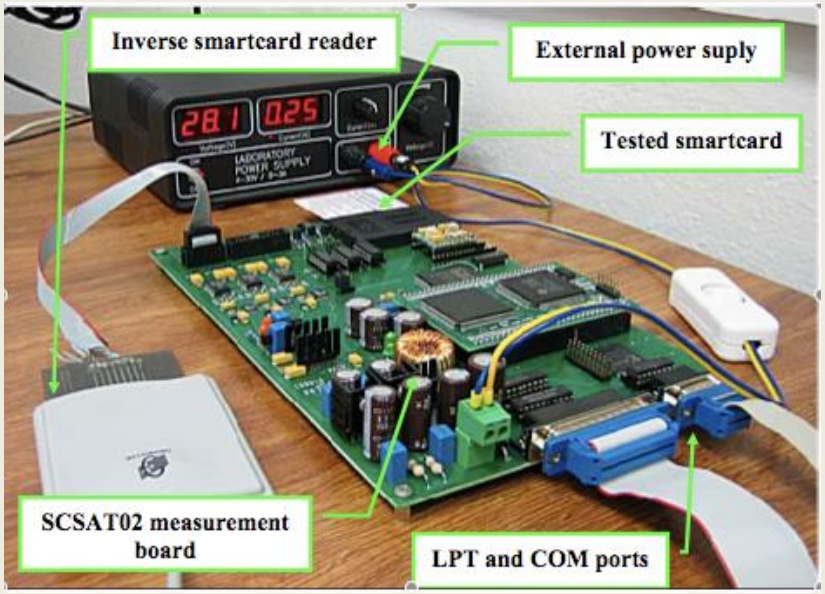
- התפתח בעיקר בשביל לפרוץ כרטיסים חכמים
- נראה בגרף צריכת הכוח כי כאשר מנחשים Byte לא נכון, הגרף קבוע. כאשר מנחשים נכון, הגרף משתנה:



תמונה מתוך הספר

התקפות פאסיביות – צריכת כוח

- 1998 - Paul Kocher הראה כי ניתן למצוא 48 מתוך 56 ביטים של המפתח בDES ע"י השוואת זוגות קלטים



smartarchitects.co.uk

- Counter של אשראי
- לא משאיר עקבות
- ברגע שההכנה להתקפה בוצעה, היא יכולה לשמש לתקוף מספר רב מאוד של מטרות

התקפות פאסיביות – דליפה של סיגנל רדיו

- במחשבים הישנים יותר (1972), היה אפשר לכוון רדיו לתדר של המעבד ולשמוע רעש משתנה לפי המידע שמעבדים
- מסכים פולטים את התמונה המוצגת כקרינה
- הקרינה הזו נגישה בכמה מקומות בדרך מהמחשב למסך
- הציוד הדרוש – מקלט רדיו, ותוכנה מתאימה לפענוח

התקפות פאסיביות – דליפה של סיגנל רדיו

- פתרון ראשוני – Jammers
- להלן דוגמה לשחזור תמונת מסך מתוך קרינה

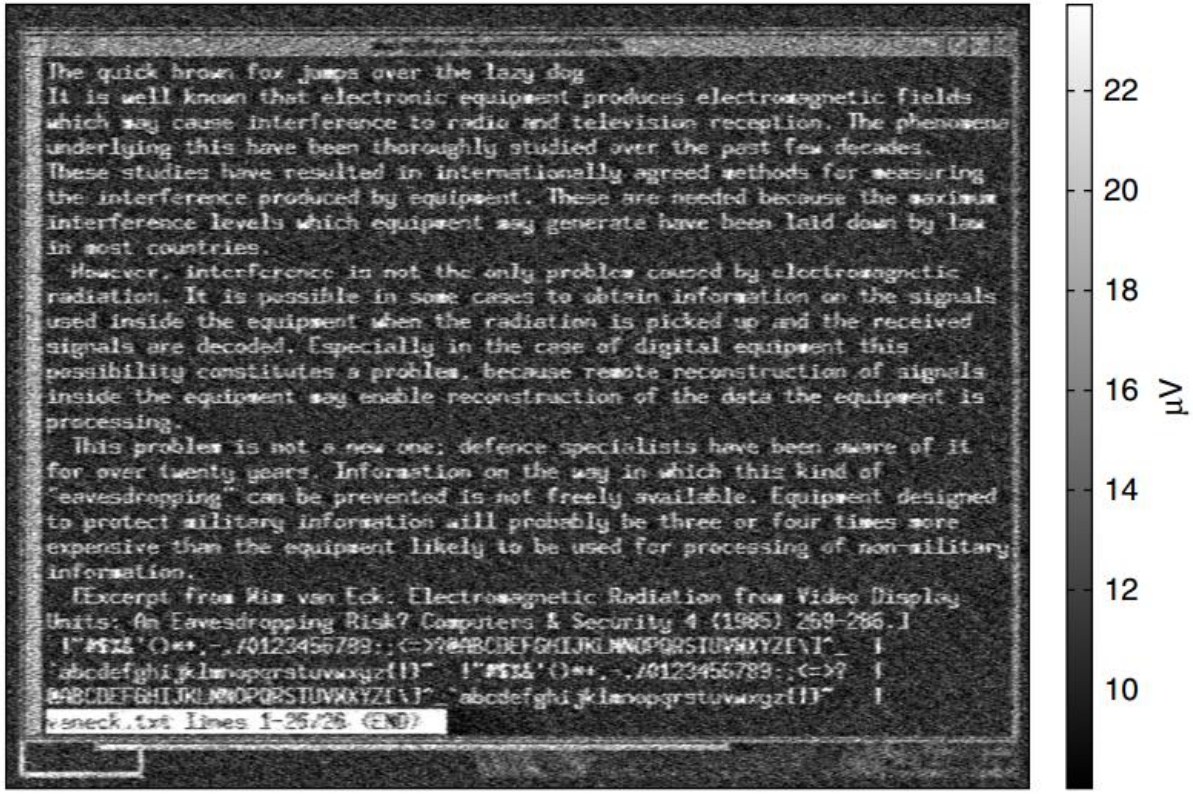


Figure 17.2: RF signal from a Toshiba laptop reconstructed several rooms away, through three plasterboard walls (courtesy of Markus Kuhn [752]).

תמונה מתוך הספר

התקפות פאסיביות – דליפה של סיגנל רדיו
שיטת הZones

- בשביל להתגונן מהתקפות רדיו, מכשירים מחולקים ל4 קבוצות:

1. **Zone 0** – אין דליפה ברדיוס של מטר **אחד**
2. **Zone 1** – אין דליפה ברדיוס של **20** מטרים
3. **Zone 2** – אין דליפה ברדיוס של **120** מטרים
4. **Zone 3** – אין דליפה ברדיוס של **1200** מטרים

- החלוקה מאפשרת לדעת איזה מהציוד ניתן להציב בשולי המתחם ואיזה מצריך חדר ממוגן

התקפות פאסיביות – דליפה של סיגנל רדיו Soft Tempest

- Soft Tempest הינה עוד דרך הגנה מפני התקפות רדיו המשתמשת בתוכנה על מנת למזער דליפה
- ידוע שרוב המידע הנגיש מהקרינה של המסך מרוכז בתדרים הגבוהים
- Soft Tempest יכולה להוריד Zone שלם!

Figure 17.3: Normal text

Figure 17.4: Text low-pass filtered

הדוגמה מתוך הספר

התקפות פאסיביות – דליפה של סיגנל רדיו Soft Tempest

- אין הבדל משמעותי בהצגה של התוכן על המסך

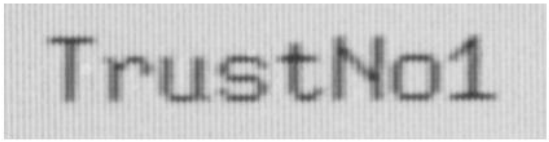


Figure 17.5: Screen, normal text

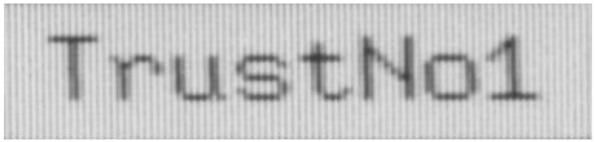


Figure 17.6: Screen, filtered text

- אך בשחזור התמונה מקרינה, לא ניתן להבין מה היה בה

Figure 17.7: Page of normal text

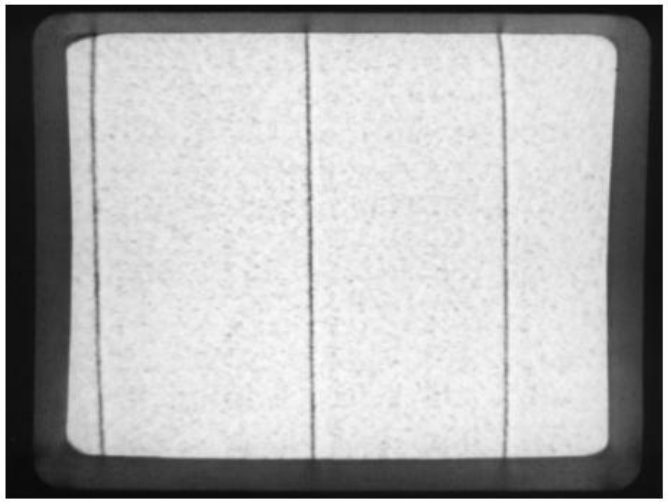


Figure 17.8: Page of filtered text

הדוגמה מתוך הספר

התקפות פאסיביות – דליפה של סיגנל רדיו

- דוגמה נוספת לדליפות רדיו בתוכנה היא סריקה של המקשים במקלדת בשביל לראות מתי ואיזה אחד מהם נלחץ

- נתגונן ע"י הצפנת הסדר שבו מתרחשת הסריקה

התקפות אקטיביות

- <u>התקפות אקטיביות הן התקפות הכוללות התערבות בפועל של המתקיף בסביבת המותקף</u>
- נקרין את המקלדת בתדר מסויים ונקלוט את האות המוחזר
- בשביל להתגונן – נצפין גם את התעבורה בין המקלדת למחשב

התקפות אקטיביות – Tempest Viruses

- נוכל לכתוב וירוסים המשדרים תוכן ע"י דליפת הרדיו של המסך
- ניתן לאסוף כך מידע ממחשב שאפילו לא מחובר לאינטרנט
- בNSA, מילת הקוד Teapot פירושה:

"מחקר ושליטה על דליפה מכוונת באמצעי תקשורת, ציוד אוטומטי, ומערכות מידע"

התקפות אקטיביות – Tempest Viruses

- ניתן לחשוף מערכות שהן ממוגנות מפני טווח תדרים מסויים לתדר שמחוץ לטווח המוגן
- בשביל ליצור ציוד הבטוח בפני התקפות אלה נצטרך להשקיע הרבה מאוד מאמץ

התקפות אקטיביות - Nonstop

- ניצול אותות שמתערבבים עם מידע רגיש במכשירים סמוכים
- נהוג לאסור שימוש בפלאפון ברדיוס 5 מטרים מציוד רגיש
- ספינות ומטוסים צבאיים חשופים ביותר להתקפות אלה

התקפות אקטיביות – שיבוש - Glitching

- שינוי בשעון או באספקת הכוח של מערכת בשביל לגרום לה לשגיאה
- תוקף מכניס פעימת שעון מיותרת בשביל לגרום לפקודה להיות NOP
- מאפשר Selective code execution

התקפות אקטיביות - התקפת שיבוש אקראי
Differential Fault Analysis

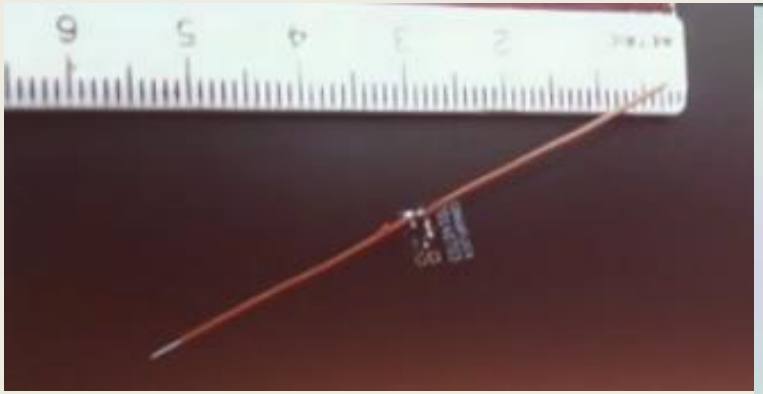
- תוקף לא חייב לדעת את הממשק הפנימי של כרטיס חכם בשביל לממש התקפה
- מספר רב של אלגוריתמי הצפנה פומביים אינם עמידים בפני שגיאות אקראיות
- אם יש לנו את היכולת לגרום לביט לקבל ערך שאנו רוצים, ואנו יודעים למצוא היכן שמור המפתח בזיכרון, נוכל לגלות אותו

התקפות משולבות

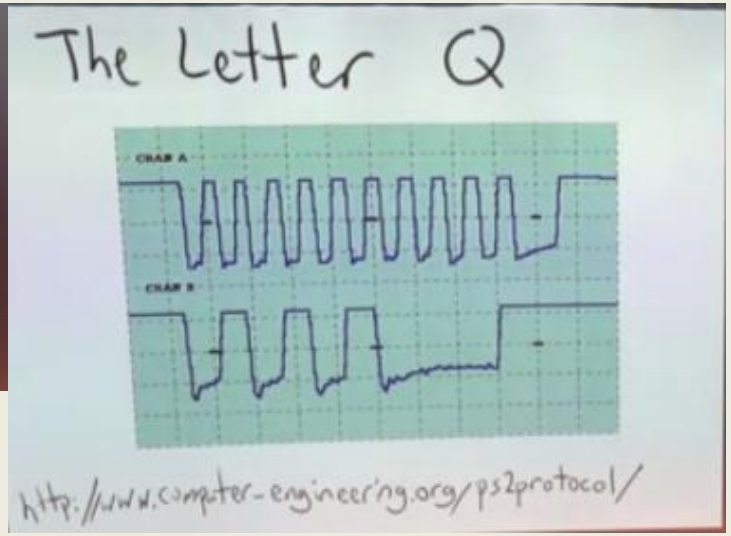
- התקפות המשלבות התקפה אקטיבית ופאסיבית
- דגימה אופטית - דגימה של מצב של רכיב במעגל חשמלי ע"י קרן לייזר - בשילוב עם ניתוח צריכת כוח
- ניתן לגרום לקרן הלייזר להשפיע על הולכה של רכיבים

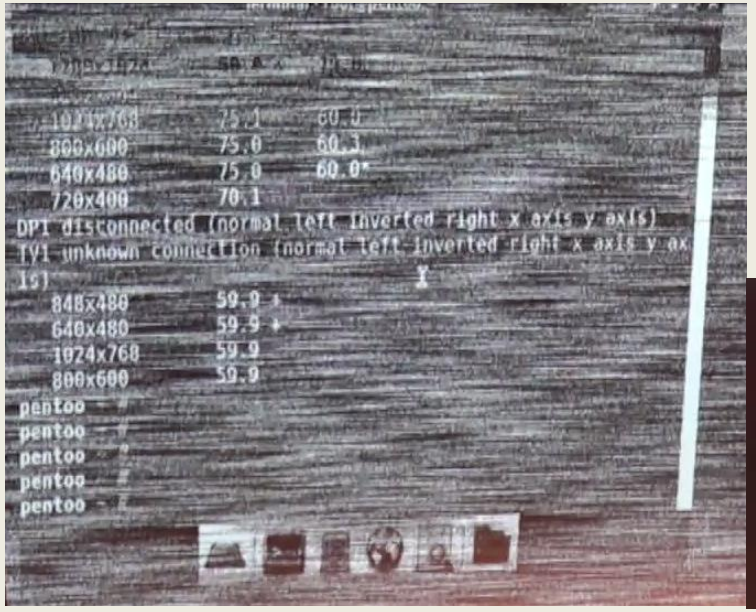
Software Defined Radios – HackRF one (27.3.15)

Radio receiver+ transmitter



Single wire retroreflector (keyboard)





VGA retroreflector (Video signal)

התקפות דליפה ביום-יום (היבט חוקי)

- חברה אמריקאית עוקבת אחר תחנת הרדיו אליה מקשיבים נהגים בסביבת הבניינים שלה
- ידוע גם כי ציוד האזנה דומה נמכר ליצרניות של מכוניות, בעלי קניונים, ולתחנות רדיו
- אין עקבות = אין ראיות

התקפות Side channel בהקשר לאופטיקה

- LED indicators המחוברים לSerial data
- כמה מידע אפשר לשחזר על התמונה של המסך מאור המוחזר ממשטח כלשהו (בן אדם, קיר)?
- בשנת 2002 Markus Kuhn השתמש בציוד נגיש והראה כי ניתן לשחזר תמונה מלאה מהשתקפות

התקפות Side channel בהקשר לתרמיקה (חום)

Cece.re

- בשנת 2006 Steven Murdoch שם לב שלשעון של מחשב יש מחזור סטייה יומי
- הוא הסיק כי הסטייה נובעת מטמפרטורת הסביבה
- ניתן למדוד את עומס הCPU של מחשב מהטמפ'

- מאפשר להעריך מיקום של מחשב כאשר:

- הLongtitude מגיע מהשעה והתאריך במחשב

- הLatitude ניתנת לחישוב ע"פי העונות ומזג האוויר

עתידן של התקפות Emsec

- יש קהילה מאוד פעילה בתחום, כנסים אקדמים ותחרויות בנושא (לדוגמה – CHES,Blackhat)

- פרופ' עדי שמיר (הS שבRSA) ופרופ' אלוביץ' הראו כי ניתן לשלוט על Malware ע"י שליחת מידע דרך קרני אור לסורק
- ישנה האפשרות שגם ההפך אפשרי

- פרופ' שמיר, דניאל גנקין מהטכניון וד"ר ערן טרומר מאוניברסיטת תל אביב, פרסמו מאמר ובו הסבירו כי ניתן לחלץ מפתח הצפנה באורך של 4096 ביט ע"י האזנה למעבד

התקפות והגנות דליפה בעולם האמיתי

- אם אין הרבה מה להסתיר – העלויות של Emsec לא מצדיקות את עצמן
- ההתקפות נגישות ואפשריות כאשר הן מכוונות

לסיכום

- התחום התחיל בצבא, אך הפך לבעיה אזרחית במהרה
- הרבה מאוד מהמכשירים והכלים ההכי מתקדמים ומאובטחים נופלים דווקא בEmsec
- דליפה היא לא מודעת, לכן ההתקפות האלה רובן שקופות ללא עקבות
- **תנסו לספור את כמות הדרכים שהיה ניתן "להתארח" בהרצאה הזו בלי שאף אחד מאתנו הרגיש...**