Technologic Papers

מבוא לקריפטואנליזה אקוסטית

מאת בר טופליאן

הקדמה

מאמר זה ממשיך את הקו של המאמר שפורסם בגליון 171[1] ("מבוא לקריפטוגרפיה מבוססת וידאו"). אני מניח שלא כל הקוראים קראו את המאמר הקודם, ולכן הרקע יהיה כמעט זהה, לקודם.

את המאמר הקודם כתבתי כמטלת רשות בקורס "מבוא לקריפטוגרפיה", וכשחיפשתי נושא לסקירה, ידעתי מראש שעלי לבדוק קודם אם החוקרים ישראלים, ורק אז לבחון את מידת העניין שלי (למען הסר ספק, לא היו דרישות בנוגע למוצאם של הכותבים, זו בחירה אישית שלי). הסמסטר חלף, אבל נשאר לי טעם של עוד, ולכן כאשר הגיע העת להרשם לסמינר, לא הייתה לי התלבטות, ולכן בחרתי סמינר בקריפטוגרפיה.

באותו אופן, כשחיפשתי מאמרים פורצי דרך בתחום הקריפטואנליזה, ובפרט העוסק בהתקפות ערוץ צדדי (Channel Attacks Side) התמקדתי במחקרים ישראליים בולטים. שם אחד עלה מיד בראשי, **עדי שמיר**, לא אני ולא אתם זקוקים להסבר מי זה עדי שמיר, ולכן לא היה לי ספק שבמאגר הפרסומים שלו אמצא מחקר פורץ דרך.

> חשוב לי לציין: המאמר מבוסס על העבודה המדהימה של קבוצת חוקרים ישראלים[2], שפורסמה בשנת 2014 ומאז עברה כמה עדכונים, תחת השם "Acoustic Cryptanalysis[3]" (קריפטואנליזה אקוסטית). עבודה זו, מתארת שיטה המאפשרת חילוץ מפתח RSA סודי, באורך של כ-4096 סיביות, באמצעות ניתוח אותות שמע הנפלטים מרכיבים אלקטרוניים במהלך ביצוע פעולות קריפטוגרפיות.

במאמר זה, נציג מספר תרחישים המובאים במאמר, המדגימים את הפוטנציאל של התקפות ערוץ צדדי המבוססות על ניתוח אותות שמע. נציג את השלבים המרכזיים לזיהוי, הבחנה והתקפה של מפתחות RSA פרטיים תוך שימוש באותות המתוארים ונציין דרכי הגנה ואמצעי מנע כנגד התקפות אלו. בדומה לגישתנו כלפי המאמר הקודם, ננסה להתמקד בעיקרי הדברים ולהעביר מידע רב ככל האפשר בצורה תמציתית, ללא כניסה לפרטים טכניים מיותרים שאינם חיוניים להעברת הרעיון המרכזי.

רקע

אבטחת מידע הוא תחום הניצב בקדמת חזית הטכנולוגיה, ומתמודד עם הצורך ההולך והגובר לשמור על סודיות ולמנוע גישה לא מורשית למידע. בעידן שלנו, כמות החידושים הטכנולוגיים, המידע ושיטות עיבוד הנתונים, מתפתחים בקצב מסחרר. בהתאם לכך, הצורך בהגנה על מידע, ושמירתו מפני ניצול לרעה על ידי גורמים חיצוניים, הפך לחיוני מתמיד. תחום אבטחת המידע כולל בתוכו קשת רחבה ומגוונת של תתי נושאים ותחומי מחקר שונים, אך במרכזו עומדים שני תחומים עיקריים, השזורים זה בזה יחדיו:

- **קריפטוגרפיה** - העוסקת בפיתוח שיטות לתקשורת ואבטחת נתונים.
- **קריפטואנליזה** - הממוקדת בזיהוי חולשות במערכות הקריפטוגרפיה, ובחיפוש אחר דרכים לשבור את הצפנתן.

מאז ומתמיד, מידע מוצפן מושך את תשומת לבם של אלה המנסים לפענחו. כתוצאה מכך, התפתחות הקריפטוגרפיה (שיטות הצפנה) מלווה תמיד בהתקדמות מקבילה בקריפטואנליזה (שיטות פיצוח)."כמספר הפרוטוקולים הקריפטוגרפיים (חתימה דיגיטלית, אימות משתמשים וכיוצא בזה), וכמספר אבני הבניין הקריפטוגרפיות (הצפנה סימטרית, הצפנה א-סימטרית, מפתח פומבי ועוד), כך מספרן של השיטות הקריפטואנליטיות".

כפי שקריפטוגרפיה ניתנת למימוש הן בחומרה והן בתוכנה, באופן דומה מתנהלת הקריפטואנליזה.

איפה כל זה פוגש אותנו? ומה צופה העתיד?

מיקרופונים מהווים איום על פרטיותנו. הם משולבים בכל מכשיר נייד וניתנים להסוואה כך שלא יעוררו חשד (למשל בתוך עטים, מנורות, או אפילו אריחים), ובכך מאפשרים הקלטה בסתר. לא משנה היכן נהיה, תמיד נמצא תחת טווח הקליטה של חיישנים רבים, שמסוגלים במקרים מסוימים לפגוע בפרטיותנו.

סכנות הפרטיות בעידן המודרני הן לא כולן ידועות לנו, ניתן לשער שרבות הדרכים לפגוע בפרטיותנו כיום באמצעות כלים וטכניקות שטרם התגלו או שידועות ונשמרות בסתר. אנו מוקפים באמצעים טכנולוגים ובחיישנים כל הזמן, GPS, מיקרופון, מצלמה, סורק פנים וחיישן תנועה הם רק חלק קטן מאותם חיישנים שנמצאים בסביבתנו ללא מפריע ברוב שעות היום.

שמירת המידע הרבה בימינו ובשילוב עידן ה-Big Data, מעלה את הסיכון לשימוש במידע למען מטרות שפוגעות בפרטיותנו. החלק המפחיד ביותר הוא, שלמרות שכרגע לא בהכרח יש את הכלים לדלות מידע רגיש מחיישנים ואמצעים טכנולוגיים, שמירת המידע מאפשרת לנסות לחלץ מידע בעתיד, בו יתווספו כלים חדשים וזמינים. אם לא נחקור ונהיה מודעים לסכנות הסובבות אותנו, אנו עלולים לגלות את ההשלכות כשכבר יהיה מאוחר מידי.

הסיכון להיחשף לפגיעות פרטיות הוא תמידי, והצורך בהבנת הדינמיקה של טכנולוגיות מתקדמות והשלכותיהן על חיינו הופך לקריטי. הכרה בסכנות הללו והגברת המודעות הציבורית יכולות לסייע ביצירת כלים ומנגנונים שיגן על פרטיותנו, ולמנוע שימוש לרעה במידע שלנו.

מילה קצרה על התקפת ערוץ צדדי

התקפת ערוץ צדדי היא התקפה קריפטוגרפית המנצלת מידע מהיישום הפיזי של מערכת ההצפנה, ולא מהאלגוריתם עצמו. היא נעשית באמצעות ניתוח פרטים כמו זמני עיבוד, צריכת אנרגיה, קרינה אלקטרומגנטית, רעשים, השתיירות מגנטית על מדיה והזרקת שגיאות. זאת עקב זיהוי וניצול מגבלות טכניות או כשלים ביישום, העלולים לחשוף מידע שיסכן את ביטחון המערכת.

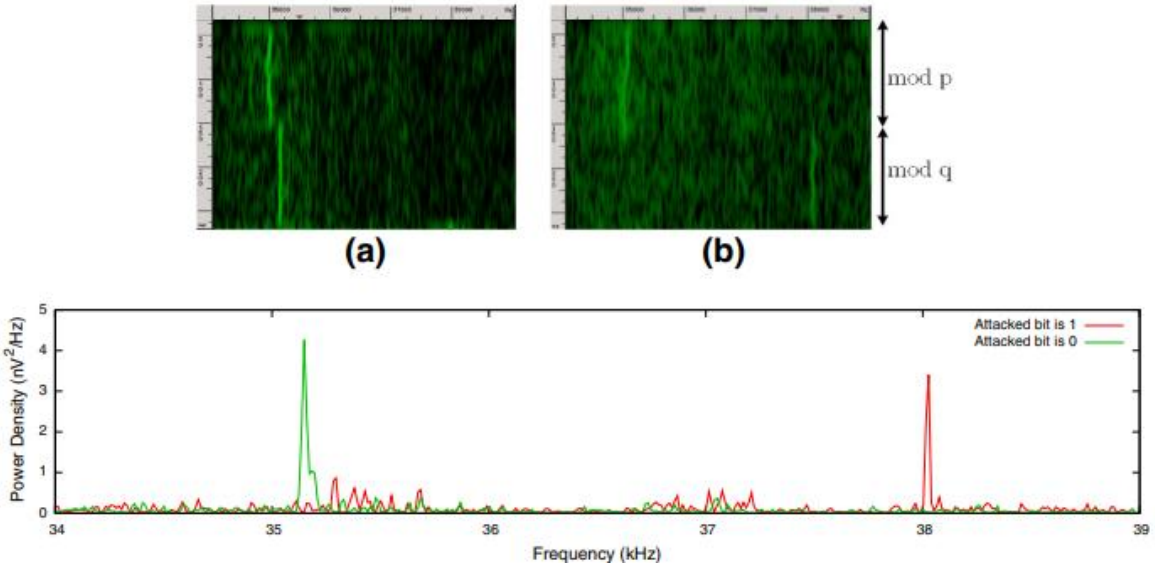
תוכן המאמר

המחקר מתאר התקפת ערוץ צדדי המבוססת על ניתוח אותות שמע הנפלטים מרכיבים אלקטרוניים במהלך ביצוע פעולות קריפטוגרפיות. המחקר מתמקד ברעידות הנוצרות במעגלי ויסות מתח, אשר מפיקות רעשים בתדרים גבוהים (המכונים לעיתים "coil whine"). רעשים אלו נגרמים כתוצאה מהבדלים בצריכת המתח של המעבד, המשתנה בהתאם לפעולות שהוא מבצע.

החוקרים מתארים בעבודתם כיצד ניתן לנצל את אותות השמע הללו כדי לחשוף מידע על התוכנה הרצה במחשב ואף לדלוף מידע רגיש הקשור לחישובים קריפטוגרפיים. בפרט, המחקר מתאר התקפה המאפשרת שחזור מלא של מפתחות RSA פרטיים באורך של 4096 סיביות תוך כשעה בלבד, על ידי ניתוח האותות הנפלטים במהלך פענוח הודעות מוצפנות. ההתקפה ניתנת לביצוע באמצעות טלפון נייד רגיל הממוקם בקרבת המחשב המותקף, או באמצעות מיקרופון רגיש הממוקם במרחק של עד 10 מטרים.

ההתקפה המתוארת במחקר מתבצעת באמצעות יצירת טקסט מוצפן שנבחר באופן מיוחד, הגורם לביטולים מספריים בעומק האלגוריתם לביצוע חישובי חזקות מודולריות של תוכנת ההצפנה GnuPG (תוכנת GnuPG היא תוכנת קריפטוגרפיה היברידית, התומכת בביצוע פעולות קריפטוגרפיות סימטריות ופעולות קריפטוגרפיות מסוג מפתח פומבי[4]).

ביטולים אלו גורמים להופעה שכיחה של מילים המכילות אפסים בלבד בלולאה הפנימית ביותר של האלגוריתם, מה שמוביל לבחירת מסלול קוד מסוים אך ורק אם הביט במפתח המותקף הוא '1'.



[איור 1: פליטות אקוסטיות במהלך פענוח RSA, עבור ערכים שונים של הביט המותקף באותו מפתח]

תרחישי התקפה אקוסטית

על מנת להבהיר את ההשלכות האפשריות של התקפות אקוסטיות, החוקרים מציינים מספר תרחישים היפותטיים שבהם התקפות אלו מציבות איום חדש. בניגוד לשאר המידע המובא במאמרם, החוקרים מציגים את הרעיון הכללי של כל תרחיש, אך בכל זאת ניתן להתרשם מהיקף התרחישים.

אפליקציית התקפה אקוסטית

טלפונים ניידים הם שכיחים ומצוידים במיקרופונים פנימיים המסוגלים להקליט אותות בתדרים המתאימים להתקפה. אפליקציה ייעודית יכולה לנצל את יכולות עיבוד האותות של הטלפון ולבצע את ההתקפה בזמן אמת. תוקף יכול להניח את הטלפון בסמוך למחשב היעד, למשל במהלך פגישה ולשחזר את המפתח הקריפטוגרפי עד לסיומה.

האזנת סתר באמצעות מכשיר נייד שנפרץ

מכשיר נייד יכול להיפרץ מרחוק על ידי התקפות ידועות או אפליקציה זדונית במסווה של אפליקציה רגילה ותמימה לחלוטין[5] המותקנת על המכשיר. וכאשר בעל המכשיר הפרוץ מניח אותו בסמוך למחשב היעד, המכשיר יכול להקליט את האותות האקוסטיים, לנתח אותם ולשלוח את התוצאות לתוקף, ולמעשה לשמש כמרגל אוטונומי.

בנוסף, נציין כי כיום מִדִינִיוּת איסוף הנתונים ושקיפות הפעילויות הרצות ברקע של אפליקציות הן מעורפלות ולא תמיד גלויות לציבור, וישנן אפליקציות שאוספות מידע רב תוך כדי השימוש ביישום. לדוגמה, טיקטוק (TikTok) שהיקף שמירת המידע שלה שנוי במחלוקת, ומוערך כי ישנו שימוש במידע הנאסף בעת השימוש[6].

האזנה עצמית

מחשב שבו לפעמים מתבצעות פעולות קריפטוגרפיות וכולל מיקרופון, עשוי לרגל אחרי עצמו. במידה ולתוקף ישנה גישה לא מורשית להקלטות המיקרופון בעת ביצוע פעולות קריפטוגרפיות, הוא יכול להקליט ולנתח פעולות קריפטוגרפיות המבוצעות על ידי תהליכים אחרים במכשיר עצמו.

מכשירים להאזנה בסתר

האזנת סתר אקוסטית באמצעות שימוש במכשירי ציתות היא מרכיב בסיסי בריגול. מכשירים להאזנה בסתר יכולים להיות קטנים מאוד ואף בגודל של קופסת גפרורים. מכשירים אלו פועלים על סוללות, מצוידים במיקרופונים מובנים ובעלי יכולת חיבור לרשת סלולארית, והם זמינים בעלות נמוכה יחסית. בנוסף, ישנם מכשירים היכולים להיות מופעלים ממרחק, כגון מיקרופוני לייזר.

באופן מסורתי, מכשירים אלו שימשו להאזנה לשיחות, אך כעת הם עשויים למצוא שימוש נוסף בתחום הקריפטואנליזה.

מכשירי התקפה ממוקדים

השגת אות בצורה מיטבית יכולה להיות מושגת באמצעות מיקום מראש מכשירי האזנה בסתר באזור הסמוך או בקרבה מיידית למקום בו מחשב המטרה יונח בעתיד. מיקרופונים נסתרים יכולים להיות ממוקמים מראש באזורים שבהם מחשבים מונחים באופן צפוי, כמו תחנות טעינה, בימות מוגבהות לנאומים ומצגות, ושולחנות צפופים.

האזנה רוחבית

האזנה רוחבית (במקור: 'Eavesdropping En Masse') מתאפשרת בסביבה שבה ממוקמים מספר מחשבים בסמיכות, למשל חדר שרתים. התוקף יכול לפרוץ למכשיר הנמצא שם ובעל מיקרופון, או לשתול מכשיר האזנה. לאחר מכן, התוקף יקליט את המכשירים בסביבה, יבצע זיהוי ובידוד של האותות השונים ויתקוף כל אחד מהמכשירים הללו.

במקרה שבו מכשיר כלשהו ייפרץ על מנת לבצע את המתקפה, היה ניתן להעביר את הנתונים אל התוקף ולמחוק את התוכנה מרחוק ובכך לא להשאיר ראיות.

התנהגות מול אמצעי מנע

במערכות רגישות, יש הכרה בחשיבות הסכנות הכרוכות על ידי מתקפות ערוץ צדדי, ולכן קיימים אמצעי הגנה על מחשבים ורשתות, כגון כלובי פאראדיי (במקור: 'Faraday cages', מתקן שמונע משדות חשמליים מלחדור לתוכו[7]), רשתות מבודדות (במקור: 'Air gap', רשתות או מערכות מחשבים המבודדות מרשתות שאינן מאובטחות ולרוב מנותקות כלל מרשתות חיצוניות[8]) ומסננים אלקטרונים (במקור: 'Power supply filters', מסנן זה הוא מרכיב במערכות אלקטרוניות שונות שמסנן אותות לא רצויים[9]), המספקים בידוד האותות המשתקפים על ידי ספק המתח.

למרות שמסננים אלו מצמצמים בצורה משמעותית את הקרינה האלקטרומגנטית, הם כמעט שקופים לדליפות אקוסטיות. לכן, גם אם כל יתר ערוצי התקשורת וההגנה נשלטים בקפידה, דליפות אקוסטיות יכולות לחדור את שכבת ההגנה ולהיקלט על ידי מכשירים קרובים בסביבה, ובכך ומתאפשר לתוקף לבצע מתקפות אקוסטיות.

מבנה הניסויים

החוקרים מציגים שלוש תצורות שונות של מערכי ניסוי המייצגים איזונים שונים בין עלויות, ניידות ויכולות מדידה. הראשונה היא תצורת מעבדה, המספקת את יכולות המדידה הטובות ביותר, אך יקרה ואינה ניידת. השניה היא תצורה ניידת, מדויקת פחות, אך מופעלת באמצעות סוללה ונכנסת למזוודה. השלישית היא תצורת מכשיר טלפון נייד, תצורה זו פשוטה, זמינה ונכנסת לכיס.

תצורת מעבדה

תצורה זו נועדה על מנת להשיג תוצאות מדידה הטובות ביותר מבחינת איכות אות, רגישות, רעש ומענה התדרים. בתצורה זו יש שימוש בציוד מעבדה מקצועי, יחד עם רכיבים אלקטרוניים ייעודיים. ציוד המעבדה בתצורה זו פועל על מתח חילופין (AC) ולכן ניידותו מוגבלת.

החלק הראשון בשרשרת המדידה, והרכיב היחיד שרגיש למיקום ויש להציבו בקרבת היעד, הוא המיקרופון. מיקרופון הוא רכיב המרה ההופך אותות אקוסטיים שמקורם בשינויים בלחץ אוויר לאותות חשמליים. מערך המעבדה משתמש במיקרופונים קונדנסריים (במקור: 'condenser', מיקרופון הקולט אותות אקוסטיים באמצעות שינוי קיבול חשמלי בין ממברנות) של חברת 'Brüel&Kjær', במיקרופונים אלו, רכיב המרת האותות האקוסטיים לאותות חשמליים משולב בגוף המיקרופון.

החוקרים בחרו להשתמש בשלושה מיקרופונים מהסוג המתואר למעלה, בעלי יחס תדר לרגישות שונים:

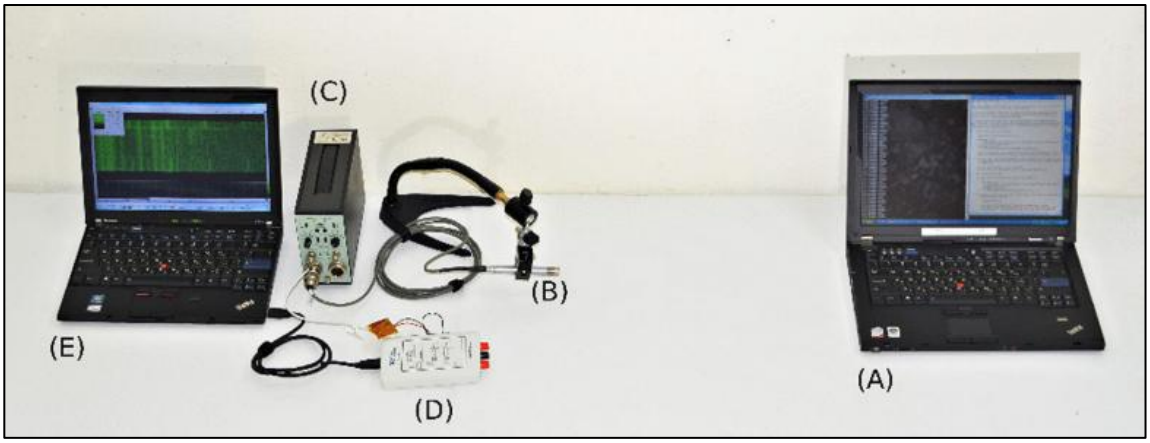
- Brüel&Kjær דגם 4939 (עד $350kHz$)
- Brüel&Kjær דגם 4190 (עד $40kHz$)
- Brüel&Kjær דגם 4145 (עד $21kHz$)

[איור 1: קפסולות המיקרופונים (מימין לשמאל): דגם 4145, דגם 4190 ודגם 4939. עפרון רגיל עבור קנה מידה]

הקפסולות מופעלות על ידי קדם מגבר Brüel&Kjær 2669, המוזן באמצעות ספק כוח למיקרופון Brüel&Kjær 2804. האות מוגבר בעזרת מגבר רעש נמוך שעבר התאמה אישית Mini-Circuits ZPUL-30P, מסונן ומומר לאות דיגיטלי (בקצב של עד 1.25 מיליון דגימות לשנייה) באמצעות כרטיס דגימת נתונים National Instruments 6356.

תצורה ניידת

תצורה זו לא דורשת ספק מתח רגיל, אלא מופעלת על ידי סוללה, תוך כדי שמירה על רגישות גבוהה ורמת רעש נמוכה (עד $100kHz$). בדומה לתצורת המעבדה, נעשה שימוש בקפסולות מיקרופון וקדם - מגבר זהה, אך רכיב ההגברה, אספקת המתח ורכיב המרת האותות האנלוגיים לדיגיטאליים הוחלפו:



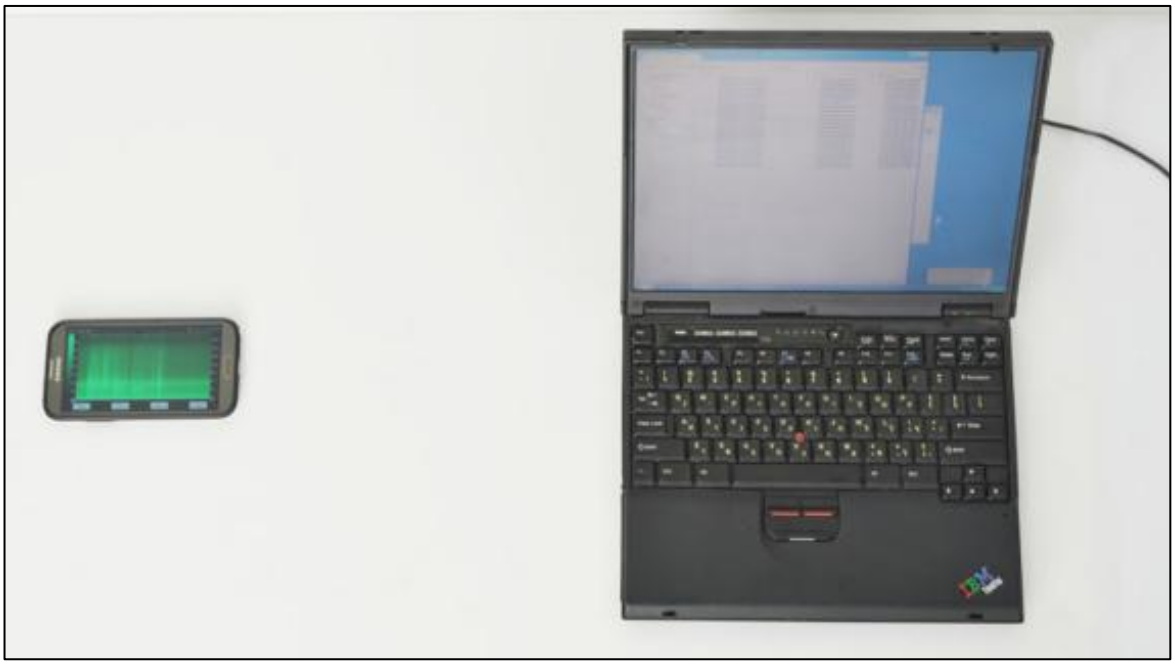
[איור 3: תצורה ניידת]

תצורת מכשיר טלפון נייד

בתצורה זו נעשה שימוש בחומרה קומפקטית ונפוצה, הזמינה לכל תוקף פוטנציאלי, היתרון בגודל קטן ובעלות נמוכה מגיע על חשבון איכות נמוכה של המיקרופון והמגבר שאינם, מתוכננים לקליטת התדרים והעוצמות הרלוונטיים להתקפה.

החוקרים מתארים כי נבדקו מספר אפשרויות למכשירי טלפון ניידים מבוססים אנדרואיד, שהניבו תוצאות דומות. ההקלטה בוצעה באמצעות אפליקציית אנדרואיד ייעודית, אשר ניגשת למיקרופון הפנימי ומשדרת את האות המוקלט לעמדת עיבוד לניתוח נוסף.

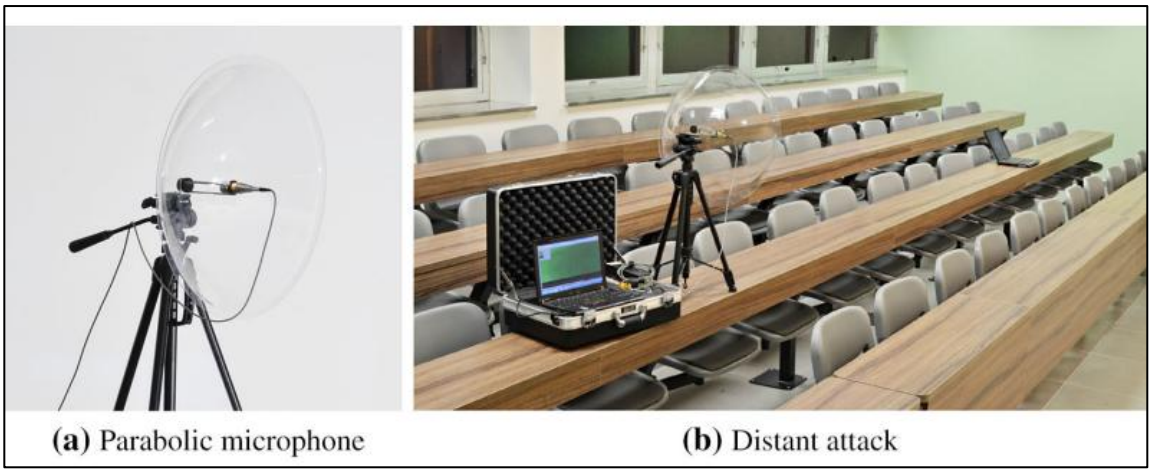
המפרט הטכני של המיקרופון, ההגברה, הסינון וההמרה לאותות דיגיטאליים, לא היו זמינים לחוקרים. אך הם מצאו כי הרגישות נמוכה יותר ורמת הרעש גבוהה יותר בהשוואה למערכים הקודמים. תגובת התדר מוגבלת משמעותית ותקרתה התיאורטית היא עד $24kHz$, אך בפועל היא נמוכה בהרבה (בדרך כלל מכשירי טלפון ניידים מסננים צלילים מעל $4kHz$).



[איור 4: תצורת מכשיר טלפון נייד (Samsung Note II) ממוקם כ-30 סנטימטרים ממכשיר המטרה]

החוקרים מציינים כי ניתן להרחיב את טווח ההתקפה בצורה משמעותית, בעזרת מחזיר פרבולי (parabolic reflector), אשר ממקד גלי קול מישוריים לנקודה אחת.

מיקום קפסולת המיקרופון בנקודת המוקד של מחזיר פרבולי מאפשרת להגדיל את טווח שחזור המפתחות ממטר אחד לכעשרה מטרים:



[איור 5: קפסולת מיקרופון Brüel&Kjær 4145 יחד עם קדם-מגבר Brüel&Kjær 2669, מחוברים למחזיר פרבולי שקוף (בקוטר של 56 סנטימטרים)]

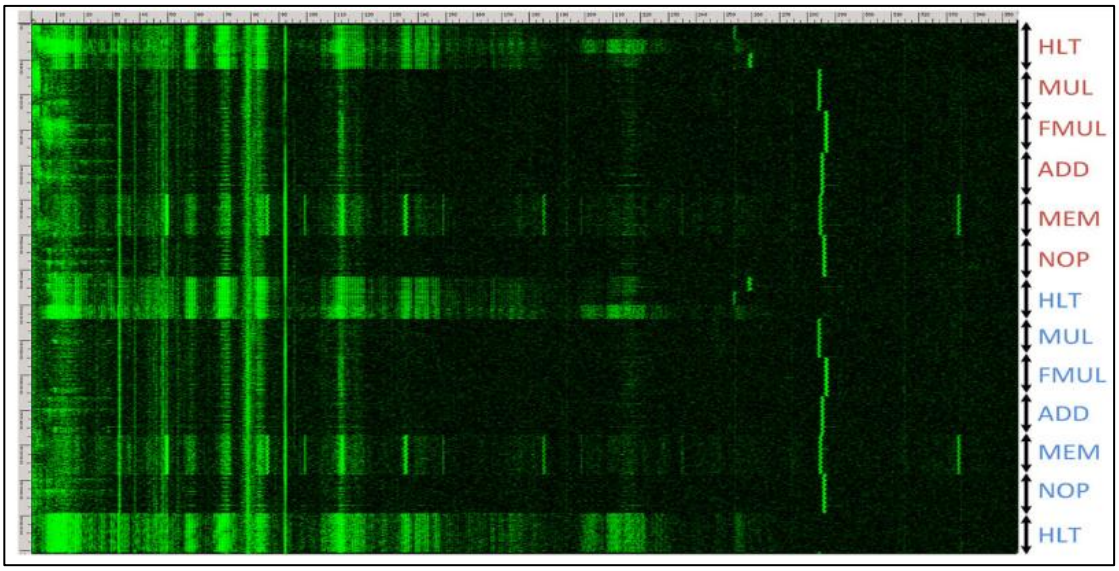
זיהוי זליגת מידע אקוסטי

החוקרים ניסו להבדיל בין פעולות שונות שמבצע המעבד של מחשב היעד, במטרה לנתח זליגת מידע אקוסטי. לשם כך, הם כתבו תוכנית פשוטה שהריצה לולאות עם פריסה חלקית (הסבר בהמשך), שכללו כל אחת מהפקודות הבאות בארכיטקטורת $x86$:

- HLT - הכנסת המעבד למצב שינה
- MUL - כפל מספרים שלמים
- FMUL - כפל נקודה צפה
- גישה לזיכרון הראשי - יצירת החטאות בזיכרון מטמון L1 ו- L2
- REP NOP - המתנה קצרה

באמצעות תצורת המעבדה, החוקרים הצליחו להבדיל בין חלק מהפעולות ברוב המחשבים שנבדקו, עם זאת, הם גילו כי מחשבים מסוימים (כמו, *Compaq Evo N200* או *Sony Vaio VGN-T350P*) מציגים ספקטרום זליגה עשיר במיוחד.

כך זה נראה:



[איור 6: הספקטרוגרם של מדידת תדרים אקוסטית של פעולות שונות של מעבד שבוצעו על מחשב Compaq Evo N200, תוך שימוש במערך המעבדה ובקפסולת המיקרופון Brüel&Kjær 4939.]

לולאות פריסה חלקית

האזנה כפי שהוזכר קודם לכן, החוקרים כתבו תוכנית המריצה לולאות פריסה חלקיות, נסביר בקצרה על מושג זה לצורך הבנה מלאה של עקרון פעולת החוקרים. לולאת פריסה חלקית, (במקור: '*partially unrolled loop*') היא טכניקת אופטימיזציה שבה חלק מהאיטרציות של הלולאה נפרשות (*unrolled*) כדי להפחית את העומס על בקרת הלולאה. פריסה חלקית הינה פשרת ביניים בין פריסה מלאה (שבה כל הלולאה נפרשת לחלוטין) לבין לולאה רגילה שבה כל איטרציה מתבצעת בנפרד[10].

לשיטה זו כמה יתרונות:

- הפחתת העומס של בקרת הלולאה - פחות פעולות התקדמות והשוואה
- שיפור ביצועים - מאפשר ביצוע מקבילי טוב יותר
- שיפור ניצולות זיכרון מטמון - גישה יותר מסודרת לזיכרון

לדוגמא, ניקח את הלולאה הרגילה הבאה:

```
for (int i = 0; i < 100; i++) {
    arr[i] = arr[i] * 2;
}
```

[איור 7: לולאה רגילה, המכפילה את אברי מערך בגודל 100]

הלולאה מבצעת כ-100 איטרציות שבכל אחת מהן יש הגדלה של משתנה הלולאה, השוואה ופקודת קפיצה לתחילת הלולאה.

ניתן לכתוב על ידי שימוש בלולאת פריסה חלקית (בגורם של 4) באופן הבא:

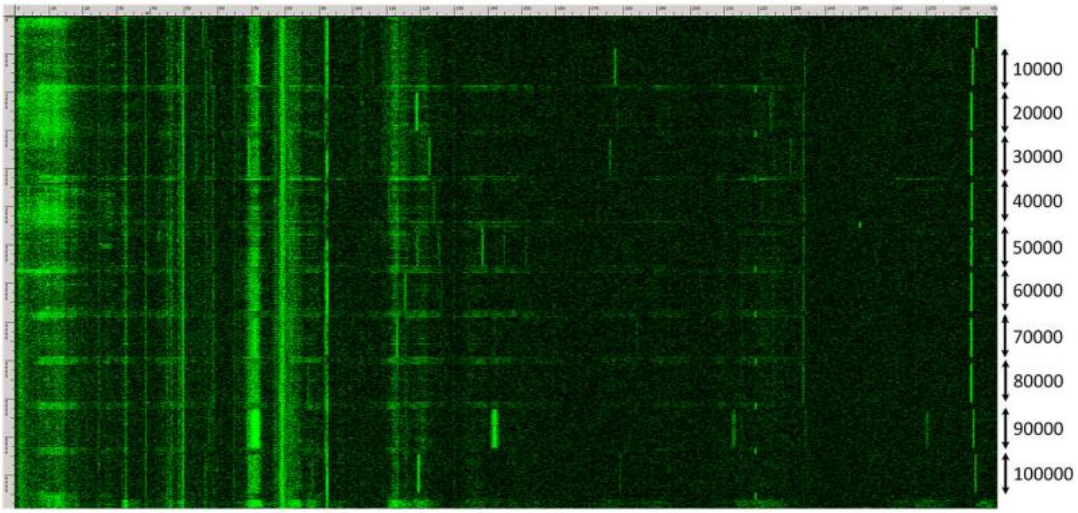
```
for (int i = 0; i < 100; i += 4) {
    arr[i] = arr[i] * 2;
    arr[i + 1] = arr[i + 1] * 2;
    arr[i + 2] = arr[i + 2] * 2;
    arr[i + 3] = arr[i + 3] * 2;
}
```

[איור 8: לולאת פריסה חלקית עם גורם בגודל 4, המבצעת הכפלה של אברי מערך בגודל 100]

במקום 100 איטרציות, כעת נבצע רק כ-25. כמות הקפיצות פוחתת והמעבר יכול לבצע כמה פעולות במקביל (בהנחה ויש תמיכה למקביליות).

הבחנה בין אורכי לולאות שונים

מדידות אקוסטיות יכולות לשמש גם להבדיל בין לולאות באורכים שונים שמבצעות את אותן סוג פקודות. לדוגמא, הזליגה שנוצרת על ידי תוכנית המבצעת 20,000 פקודות ADD בלולאה אינסופית שונה מהזליגה של תוכנית המבצעת 50,000 פקודות ADD בלולאה אינסופית.



[איור 9: החתימה האקוסטית (שש שניות, 0-290 קילו הרץ) של לולאות באורכים שונים של פקודות ADD שבוצעו על מחשב ה- Evo N200אורך הלולאה מצוין ליד חתימתה האקוסטית]

מקור הזליגה

החוקרים דנים בזיהוי וסיווג לזליגה אקוסטית או לזליגה אלקטרומגנטית. על מנת לוודא שהאות שנמדד הוא אכן זליגה אקוסטית ולא הפרעה אלקטרומגנטית שנתפסת על ידי המיקרופון, הניחו החוקרים יריעת חומר סופג קול שאינו מוליך חשמלי מול המיקרופון וביצעו הקלטה אקוסטית בתצורת המעבדה, החוקרים הבחינו כי האות נחלש בצורה משמעותית.

לאחר ניסוי עם יריעות מחומרים שונים ובעלי תכונות שונות, הבחינו החוקרים כי הזליגות האקוסטיות המנוצלות נובעות לא מהפעלת המאוורר, פעילות הדיסק הקשיח או הרמקולים (דבר שנבדק על ידי השבתה של רכיבים אלה). אלא, מדובר ברעידות של רכיבים חשמליים במעגל אספקת החשמל.

המקור הפיזי המדויק של הזליגות האלה קשה לאפיון מדויק, שכן הוא משתנה בין המחשבים הנבדקים ובדרך כלל ממוקם באזורים קשים לגישה ובנוסף, קביעת מיקום המקור הפיזי קשה עקב קישור מכני והשתקפויות אקוסטיות של רכיבים מולחמים.

בחלק זה של המאמר, מתואר לפרטים מהלך בדיקות ואיתור מקורות זליגה בתצורות שונות, לא נרחיב ונכנס לעומק של נושא זה, נציין כי הצליחו החוקרים לקבוע כי רוב הזליגות המשמעותיות נמצאו בסמוך למעגל וויסות המתח של המעבד.

ובנוסף, מסקנה חשובה שגילו היא שיש קשר אנקדוטי בין תקלות שמקורן בהידרדרות של האלקטרוליט הפנימי של קבלים אלקטרוליטים (נפוץ מאוד ככל שהמחשבים מתיישנים) לבין זליגות אקוסטיות חזקות (למרות שצפו גם במחשבים רועשים ללא קבלים פגומים ברורים). ולכן ישנה קורלציה חיובית חזקה בין גיל המחשב (הן במונחים של זמן קלנדרי והן במונחים של שימוש) לבין השימושיות הקריפטוגרפית של הזליגות האקוסטיות.

מיקום המיקרופון

נמצא כי מיקום המיקרופון ביחס לגוף המחשב הנייד משפיע באופן משמעותי על האותות שהתקבלו. באופן אידיאלי, החוקרים רצו למדוד את הקרינה האקוסטית הקרובה ביותר למערכת הספק הכוח של המעבד, הממוקמת על לוח האם של המחשב. אך, פעולה זו דורשת התעסקות פיזית רבה במחשב, כמו פירוק המקלדת או אף פירוקו לחלוטין. פעולה כזו הייתה עלולה להתגלות מיד, ולכן הוסכמה כבלתי מעשית.

למזלם של החוקרים, מחשבים ניידים מודרניים מצוידים במערכת קירור משמעותית לפיזור חום, הכוללת מאוורר שמצריך חורי כניסת ויציאת אוויר גדולים. ובנוסף, ישנם חורים וחריצים רבים עבור יציאות וכניסות למחשב (USB, כרטיס SD, שקע אתרנט, כיוצא בזה). כל אחד מהחורים הללו נמצא כיעיל למדידה האקוסטית במחשבים מסוימים.

זיהוי מפתח RSA ב- GnuPG

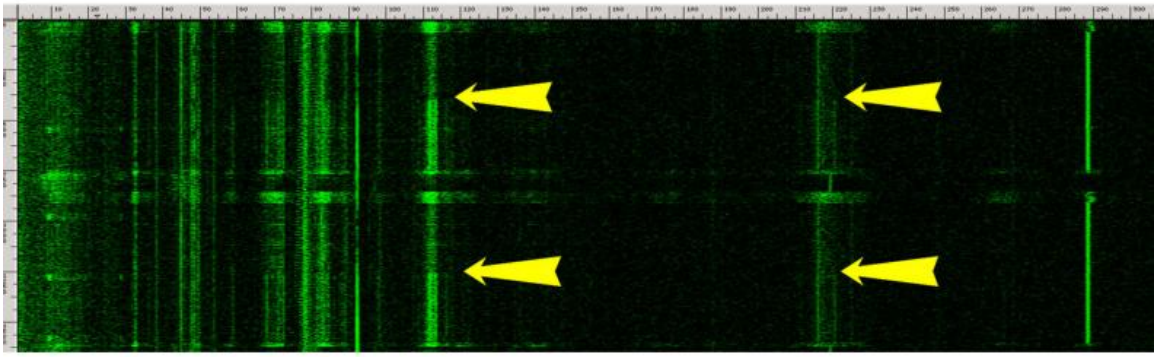
תוצאות הניסויים שערכו החוקרים בשלב הקודם של המאמר (זיהוי זליגת מידע אקוסטי), הדגימו כי ניתן להשיג מידע על הקוד המבצע מעבד מכשיר המטרה, גם על ידי שימוש במכשירי מדידה ברוחב פס נמוך מאוד.

למרות שהצליחו החוקרים להראות כי ניתן להסיק תובנות ולזהות חלקים שונים של פקודות קוד על ידי פענוח הזליגה האקוסטית, לא ברור כיצד ניתן להשתמש במידע זה על מנת לבצע מתקפה של חילוץ מפתח אמיתי ממחשב מטרה. החוקרים מציגים כי ניתן להפיק מידע שימושי על מפתח סודי שהמחשב היעד משתמש בו ובפרט, הם מציגים כי המידע האקוסטי שנמדד במהלך פעולה סודית ב-RSA (כמו פענוח הודעה מוצפנת או יצירת חתימה) מספיק בכדי לקבוע איזה מתוך מספר מפתחות אקראיים נבחרים שימש את המחשב היעד במהלך אותה פעולה.

במהלך המאמר כולו, החוקרים התמקדו במימוש סטנדרטי ונפוץ של GnuPG (GNU Privacy Guard), מימוש קוד פתוח של תקן ה-OpenPGP הנתמך על ידי כל מערכות ההפעלה המרכזיות. המתקפה בוצעה על שילובים רבים של רכיבי מערכת, אך ברוב הניסויים במאמר השתמשו ב- Windows XP, עם גרסת GnuPG מספר 1.4.14 ללא שינויים בקוד המקור.

חתימה אקוסטית של מפתח RSA סודי יחיד

האיור הבא מציג הספקטרוגרמה של שתי פעולות חתימה RSA זהות שבוצעו ברצף תוך שימוש באותו מסר ואותו מפתח בגודל 4096 bit. לפני כל פעולת חתימה, מבוצעת השהייה קצרה של המעבד אשר במהלכה המעבד נמצא במצב שינה.



[איור 2: חתימה אקוסטית (1.6 שניות, 0 - 300 קילו הרץ) של שתי חתימות RSA שבוצעו על ידי Evo N200. ההקלטה בוצעה באמצעות תצורת המעבדה, עם מיקרופון 4939. המעברים בין p ל- q מסומנים בחיצים צהובים]

איור זה מציג מספר תופעות מעניינות:

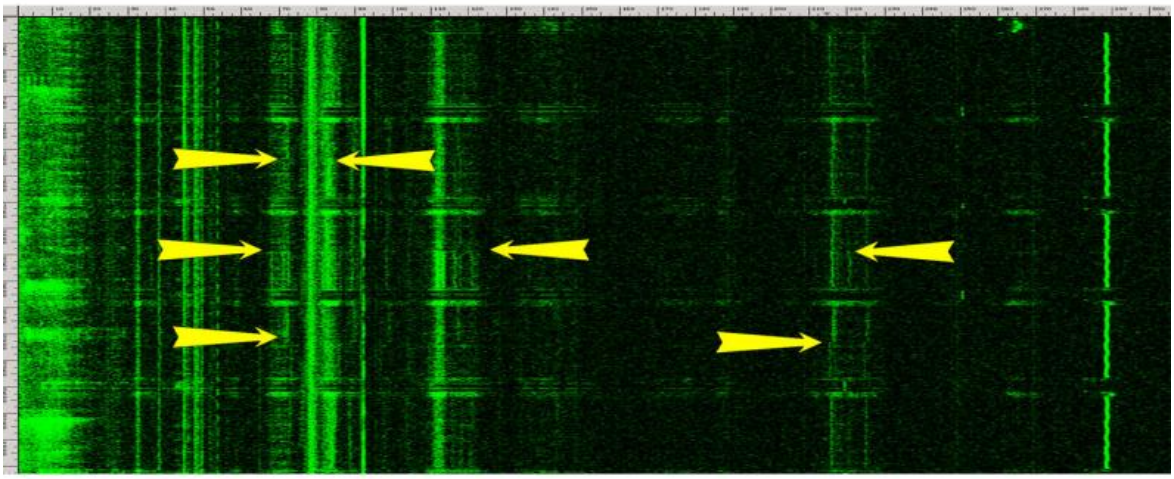
- השהיית המעבד מתבטאת באמצעות פסים אופקיים בהירים.
- בין הפסים האופקיים של השהיית המעבד, ניתן להבחין בבירור בין שתי פעולות החתימה.
- באמצע כל פעולת חתימה, ישנו שינוי בכמה פסי תדר (מסומנים בחצים צהובים).

התופעה האחרונה שציינו, מתארת שינוי בהתאם למימוש RSA של GnuPG: עבור המפתח הציבורי $n = pq$, חתימת ה-RSA $s = m^d \bmod n$ מחושבת על ידי ביצוע $m^{d \bmod (p-1)} \bmod p$ ו-$m^{d \bmod (q-1)} \bmod q$ ושילובם על ידי משפט השאריות הסיני. החלק הראשון של החתימה מתאר את פעולת ההעלאה בחזקה מודולו p והחלק השני מתאר את פעולת העלאה בחזקה מודולו q.

הבחנה בין מפתחות RSA סודיים שונים

בנוסף למדידת הזמנים וזיהוי התכונות הפנימיות של פעולות RSA בשימוש מפתח סודי, החוקרים בחנו את ההשפעה של מפתחות שונים. לאחר שראו כי החתימה האקוסטית של פעולת העלאה בחזקה מודולרית של מספרים שלמים תלויה במודולוס, ניתן להסיק כי מפתחות שונים יגרמו לחתימות אקוסטיות שונות.

כפי שניתן לראות באיור הבא, החוקרים השתמשו ב-GnuGPעל מנת לחתום על הודעה קבועה באמצעות חמישה מפתחות RSA סודיים שונים (בגודל $4096\ bit$), בדומה לשלב הקודם, לפני כל פעולת חתימה בוצעה השהייה של המעבד (בכדי לבצע הפרדה וויזואלית בין החתימות).



[איור 3: חתימה אקוסטית (4 שניות, 0 - 300 קילו הרץ) של חמישה מפתחות RSA שונים ב-GnuPG שבוצעו על Evo N200. ההקלטה בוצעה באמצעות תצורת המעבדה, עם מיקרופון 4939. המעברים בין p ל- q מסומנים בחיצים צהובים]

מודל ההתקפה

ההתקפה המתוארת במאמר היא התקפת בחירת צפנים אדפטיבית, התקפה זו (במקור: 'chosen- adaptive ciphertext attack)', היא סוג של התקפת קריפטוגרפיה שבה התוקף יכול לשלוח סדרת הודעות מוצפנות שנבחרו באופן אדפטיבי. ההבדל המרכזי מהתקפה כזו שאינה אדפטיבית, הוא התוקף יכול לבצע שאילתות אחרי שהתגלו תוצאות הצופן היעד, אך לא יכול לשאול ישירות לגבי הצופן עצמו [11].

התקפה זו מפענחת את הגורם הסודי q ביט אחרי ביט. מהביט החשוב ביותר (MSB) אל הביט החשוב פחות (*LSB*). באופן דומה מפענחים את הגורם הסודי p, אך חשוב לציין כי החוקרים הבחינו כי במכונות רבות, החישוב של העלאה בחזקה המודולרית השנייה מודולו q מציג יחס אות לרעש טוב יותר במעט, כנראה משום שמערכת ההספק של המטרה הספיקה להתייצב בזמן זה.

נקודות חשובות על אלגוריתם ההעלאה בחזקה המודולרי של GnuPG

שיטה:

- אלגוריתם 1, מציג את האופן שבו מתבצעת פעולה של העלאה בחזקה מודולרית ב-GnuPG.
- הספרייה המתמטית של GnuPG מייצגת מספרים שלמים גדולים בתור מערך של חוליות (במקור: 'limbs', כל חולייה מיוצגת על ידי מילה באורך 32 סיביות).
- בשורה השנייה של האלגוריתם ישנה בדיקה המשווה את מספר החוליות של הטקסט המוצפן מול אלו של q. אם הטקסט המוצפן אינו גדול מ-q, ה-GnuPG לא מבצע חישוב מודולו מיותר, אלא פשוט ממשיך בתהליך החישוב הרגיל.
- שורות 10 ו-12 יתנהגו באופן שונה (אורך שונה) בהתאם לאם הערך המחושב גדול מ-q לעומת המקרה שבו הוא קטן מ-q.

Algorithm 1 GnuPG's modular exponentiation (see function mpi_powm in mpi/mpi-pow.c).

Input: Three integers c, d, and q in binary representation, where $d_k \cdots d_1$ are the bits of d.
Output: $m = c^d \mod q$.

```
1:  procedure MODULAR_EXPONENTIATION(c, d, q)
2:      if SIZE_IN_LIMBS(c) > SIZE_IN_LIMBS(q) then
3:          c ← c mod q
4:      m ← 1
5:      for i ← k downto 1 do
6:          m ← m^2                          ▷ Karatsuba or grade-school squaring
7:          if SIZE_IN_LIMBS(m) > SIZE_IN_LIMBS(q) then
8:              m ← m mod q
9:          if SIZE_IN_LIMBS(c) < KARATSUBA_THRESHOLD then      ▷ defined as 16
10:             t ← MUL_BASECASE(m, c)       ▷ Compute t ← m · c using Algorithm 3
11:         else
12:             t ← MUL(m, c)                ▷ Compute t ← m · c using Algorithm 5
13:         if SIZE_IN_LIMBS(t) > SIZE_IN_LIMBS(q) then
14:             t ← t mod q
15:         if d_i = 1 then
16:             m ← t
17:     return m
18: end procedure
```

[אלגוריתם 1: פעולת העלאה בחזקה של GnuPG]

נבחן את פעולת האלגוריתם 1 לאחר הסרה של השורה השניה וכתוצאה מכך השורה השלישית תמיד תבוצע. GnuPG תמיד יוצר מפתחות RSA כך שהביט החשוב ביותר של q הוא 1, משמע $q_{2048} = 1$.

ניתן לשחזר את מחצית הסיביות האחרונות של q במידה ופענחנו את החצי הראשון (מתאפשר באמצעות התקפת קופרשמידט[12] ואחרי זאת כפי שעשו ריווסט ושמיר[13]). נסמן ב-$g^{i,1}$ להיות הטקסט המוצפן באורך 2048 ביטים, כך ש- $i-1$ הסיביות **הראשונות** שלו זהות לאלו של q, הביט ה- i שלו הוא 0, ושאר הביטים שלו הם 1.

נבחן שני מקרים אפשריים:

1. $q_i = 1$ - לכן, $g^{i,1} < q$. הטקסט הגלוי $g^{i,1}$ נשלח בתור המשתנה c לאלגוריתם 1 (שעבר שינוי), שבתוכו, הרדוקציה המודולרית בשורה 3 תחזיר c (כי $g^{i,1} < q$). מכאן, המבנה של c (מספר בעל 2048 ביטים ש- $i-1$ הסיביות **האחרונות** שלו שווה ל- 1) נשמר, ונשלח לשגרות הכפל בשורות 10 ו-12.

2. $q_i = 0$ - לכן, $g^{i,1} \geq q$. הטקסט הגלוי $g^{i,1}$ נשלח בתור המשתנה c לאלגוריתם 1 (שעבר שינוי), פעולת הרדוקציה המודולרית בשורה 3 תשנה את ערכו של c. מפני ש-c ו-q חולקים את אותם $2048-i$ ביטים **ראשונים**, מתקיים כי $g^{i,1} < 2q$ ולכן הרדוקציה שקולה ל: $c \leftarrow c-q$, שהוא מספר אקראי למראה בגודל $i-1$. ערך זה נשלח לשגרות הכפל בשורות 10 ו-12.

על פי המקרים המתוארים למעלה, בהתאם לערך q_i, האופרנד השני לשגרת הכפל יהיה באורך מלא והביטים האחרונים שלו יהיו 1, או באורך קצר יותר ואקראי למראה. וכפי שהחוקרים הצליחו לקבוע, ישנו הבדל משמעותי בהתנהגות שגרת הכפל בהינתן הערכים שתוארו. ובהתאמה דפוסי זליגה שונים שניתנים לזיהוי.

בחירת טקסט מוצפן עבור GnuPG סטנדרטי (ללא שינוי)

כפי שתואר למעלה, באלגוריתם 1 המקורי של GnuPG קיימת בדיקה שמונעת ביצוע חישובי מודולו מיותרים מה שמקטין את הזליגה הפוטנציאלית של המידע בכך שלא נוכל לבצע את האנליזה כפי שיכולנו באלגוריתם שעבר שינוי. למרות זאת, החוקרים גילו כי ניתן לעקוף מנגנון זה על ידי יצירת טקסטים מוצפנים שמכילים אפסים מובילים נוספים. ה-GnuPG יעביר את האפסים המובילים לחישוב, מה שמאלץ את האלגוריתם לבצע צעד חישוב נוסף של מודולו q, צעד שהתקיפה מתבססת עליו כדי לחלץ את הביטים של q אחד - אחד.

בנוסף, החוקרים מצאו דרך אחרת לאלץ את GnuPG לבצע את הצעד הזה, במקום לשלוח טקסט מוצפן בגודל זהה למודולוס q, הם שלחו טקסטים מוצפנים בגודל זהה למודולוס הציבורי n. מאחר ו-n הוא מכפלה של p ו- q, התוצאה היא שהאלגוריתם מבצע בהכרח חישוב מודולו q, מה שמאפשר את אותה זליגה אקוסטית שימושית:

$$g^{i,1} + n \bmod q = \left(g^{i,1} \bmod q\right) + (n \bmod q) = g^{i,1} \bmod q$$

חילוץ המפתח

החוקרים מתארים אלגוריתם לפענוח p ו-q של המפתח הסודי, הם מניחים כי השגרה DECRYPT_AND_ANALYZE_LEAKAGE_OF_Q(c) מבצעת הבחנה בין $q_i = 0$ לבין $q_i = 1$. השגרה מפעילה פענוח RSA של הטקסט המוצפן c בעזרת המפתח הפרטי (הלא ידוע) p ו- q על גבי המחשב המותקף, השגרה תמדוד את הזליגה האקוסטית ותיישם מסווג כלשהו (המסווג לפי הבדלי האותות האקוסטיים) כדי לזהות את ההבדל בין שני דפוסי הדליפה האפשריים (אשר נוצרים עקב פעולתה של שגרת הכפל)

האלגוריתם הבא מתאר הצגה של הלולאה החיצונית של התקפת *RSA* (מופשטת) על *GnuPG*:

Algorithm 2 Top loop of the (simplified) attack on GnuPG's RSA decryption.

Input: An RSA public key $\mathsf{pk} = (n, e)$ such that $n = pq$ where n is an m bit number.
Output: The factorization p, q of n.

```
1:  procedure SimplifiedAttack(pk)
2:      g ← 2^((m/2)−1)                          ▷ g is a m/2 bit number of the form g = 10···0
3:      for i ← m/2 − 1 downto 1 do
4:          g^(i,1) ← g + 2^(i−1) − 1            ▷ set all the bits of g starting from i − 1-th bit to be 1
5:          b ← DECRYPT_AND_ANALYZE_LEAKAGE_OF_Q(g^(i,1) + n)   ▷ obtain the i-th bit of q
6:          g ← g + 2^(i−1) · b                  ▷ update g with the newly obtained bit
7:      q ← g
8:      p ← n/q
9:      return (p, q)
10: end procedure
```

[אלגוריתם 2: הצגה של הלולאה החיצונית של התקפת RSA (מופשטת) על GnuPG]

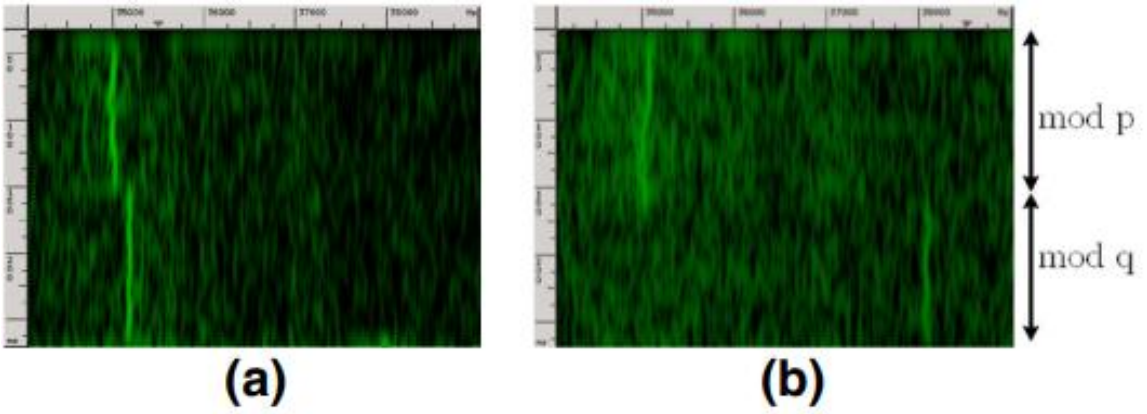
שלבי ההתקפה

1. שליחה אדפטיבית של טקסטים מוצפנים - התוקף בוחר טקסטים מוצפנים מיוחדים שנועדו להשפיע על תהליך הפענוח כך שהוא יאפשר זליגה אקוסטית ברורה שמקושרת לביטים הספציפיים של q.
2. ניתוח הדליפה האקוסטית - GnuPG משתמש באלגוריתם 1 על מנת לחשב העלאה בחזקה מודולרית, שבו קיימים הבדלים מדידים ברעש הנפלט מהמחשב כאשר הערך המחושב גדול מ- q לעומת המקרה שבו הוא קטן מ- q. הבדלים אלו מאפשרים להבחין בין שני מצבים:
   - כאשר הביט הנבדק של q הוא 1
   - כאשר הביט הנבדק של q הוא 0
3. שחזור המפתח הפרטי - התוקף מבצע את התהליך הזה באופן חוזר ונשנה עבור כל ביט של q, מהביט החשוב ביותר (*MSB*) אל הביט החשוב פחות (*LSB*). לאחר שהושלם השחזור של q, ניתן לחשב את p באמצעות חלוקה של n ב- q, ובכך לחשב את המפתח RSA הפרטי המלא.

למעשה, אם נחשוב על ההתקפה בצורה מופשטת, התוקף שולח רצף של הודעות מוצפנות לפענוח, כשכל אחת מהן נועדה לחשוף האם ביט מסוים (לפי אינדקס) הוא 0 או 1. כל הודעה מוצפנת שנשלחת זהה ל-$i-1$ הסיביות של ההודעה הקודמת. כך, מתחילים מהסיבית הראשונה (שידועה כשווה ל-1), מזהים את ערך הסיבית שאחריה, ולאחר קביעתה שולחים הודעה מוצפנת חדשה שבה שתי הסיביות שהתגלו כבר משובצות במקומן. בתום כל האיטרציות, ההודעה האחרונה שהתקבלה משקפת את הגורם q.

תוצאות ההתקפה

ניתן לראות בחלק a של האיור הבא, את ההקלטה האקוסטית שנעשתה בזמן ביצוע פעולת פענוח של RSA כאשר ערך הביט של q אותו תוקפים שווה ל-0, וניתן לראות באופן דומה בחלק b כאשר ערך הביט של q אותו תוקפים שווה ל-1.



[איור 4: זליגות אקוסטיות בזמן פענוח RSA. כאשר חלק a מייצג את הביט המותקף שווה ל-0 וחלק b מייצג את הביט המותקף שווה ל-0]

נוכל לראות באיור את המעבר מפעולת החלק הראשון של הפענוח המתאר את פעולת ההעלאה בחזקה מודולו p אל החלק השני המתאר את פעולת העלאה בחזקה מודולו q.

החוקרים מציינים כי בתחילת התהליך קל לזהות הבדלים בין ביטים, אך ככל שההתקפה מתקדמת, הזליגה נעשית פחות מובהקת. לכן, כדי לחשוף את כל 2048 הביטים של q, יש צורך בשיפור האלגוריתם הבסיסי והמשך אנליזה נוספת. לא נציג את שיפורים אלו, אך נזכיר כי הרעיון הכללי של הפענוח מתואר למעלה.

ההתקפה הזו מראה כי ניתן לבצע קריפטואנליזה אקוסטית של זליגות אקוסטיות שמקורן במעגלי המתח של המעבד, בכדי לפענח מפתחות הצפנה *RSA* סודיים ב-*GnuPG*.

ניסויים מוצלחים לחילוץ מפתח RSA סודי

החוקרים מסבירים כי התקיפה בוצעה במגוון תנאי מדידה, על מערכות שונות ותצורות תוכנה שונות. הצלחתה וזמן הריצה שלה (הנובע ממדידות חוזרות ופעולות תיקון) תלויים בפרמטרים פיזיים רבים, כגון:

- גיל ודגם המחשב
- חומרת קליטת האותות
- מיקום המיקרופון
- רעשי רקע ואקוסטיקת החדר
- טמפרטורה סביבתית (המשפיעה על פעילות המאוורר)

בנוסף, החוקרים מציינים כמה ניסויים מוצלחים לחילוץ המפתח הסודי:

תקיפת אולטרה סאונד - גרסת GnuPG 1.4.14, הרצה על Lenovo ThinkPad T61 בסביבת משרד טיפוסית. חילוץ 1024 הביטים הראשונים של q (ובכך את המפתח כולו) לקח כשעה אחת. מאחר שהאות השימושי של מחשב זה הוא סביב $35kHz$, ניתן להשתמש בציוד נייד עם מיקרופון Brüel&Kjær 4190 במקום ציוד מעבדה.

תקיפה בתדרים נמוכים - תדרים נמוכים מתפשטים באוויר ובעצמים טוב יותר מתדרים גבוהים. חלק מהמכשירים, כמו Lenovo ThinkPad X300 ו-ThinkPad T23, מאופיינים בזליגת מידע בתדרים $15 - 22\ kHz$ (בתוך טווח השמיעה האנושית). שימוש במיקרופון רגיש (Brüel&Kjær 4145) מאפשר לנצל את התפשטות הרחבה יותר של תדרים נמוכים ובכך להצליח לחלץ מפתחות RSA ממרחק בטווח של עד מטר אחד. יתרה מכך, מיקום מיקרופון Brüel&Kjær 4190 בתוך מחזיר פרבולי, מאפשר לחלץ מפתחות RSA ממרחק בטווח של עד ארבעה מטרים באופן אוטומטי, ועד כעשרה מטרים בעזרת עיבוד אותות ידני.

תקיפה באמצעות מכשיר טלפון נייד - הורדת תדרי הזליגה מאפשרת שימוש במיקרופונים פשוטים כגון אלו שבטלפונים חכמים. עקב יחס אות לרעש נמוך ותדרי תגובה מוגבלים, התקיפה מוגבלת לתדרים של $24kHz$ ולטווח של עד כשלושים סנטימטרים.

למרות זאת, עדיין ניתן לחלץ מפתח ממחשבים מסוימים על ידי הנחת הטלפון סמוך ליציאת האוויר של המאוורר בעת הרצת התקיפה. בשונה מדרישות קודמות, כאן נדרש רק להתקין אפליקציה מתאימה ולהניח את הטלפון קרוב למחשב המטרה, ללא צורך בציוד ייעודי נוסף.

אמצעי נגד התקפה אקוסטית

בחלק זה נציג בקצרה חלק מהאפשרויות שהציגו החוקרים במאמרם למניעת חילוץ מפתח RSA על ידי התקפות אקוסטיות.

מיגון אקוסטי

שימוש בבולמי קול ועטיפת מחשב המטרה במעטפת אטומה לרעש, יכולים להחליש את האותות שזולגים בזמן ביצוע פעולות קריפטוגרפיות. מה שיחייב את התוקף להשתמש בציוד יקר יותר, להציב את המיקרופון בעמדה מדויקת יותר או להקדיש זמן רב יותר לתקיפה.

לעומת זאת, מיגון כזה מעלה את עלויות התכנון והייצור, במיוחד בגלל הצורך באוורור לקירור ובפרט חורי האוורור של מאווררי הקירור במחשבים ניידים הם מקור משמעותי לדליפת קול ולא ניתן לאטום אותם בקלות. החוקרים הבחינו כי ספקי כוח חיצוניים של מחשבים ניידים עשויים לפלוט רעש הקשור לביצוע הפעולות הקריפטוגרפיות, מה שמצריך התייחסות הנדסית נוספת למיגון.

סביבה רועשת

ייתכן כי הצבת המחשב בסביבה רועשת תסכל את ההתקפה, חשוב לזכור כי רוב הרעש בסביבות רועשות (כגון בחוץ או בחדר מלא באנשים) מרוכז בתדרים נמוכים ומפני שזליגה אקוסטית לרוב מופיעה בתדרים גבוהים יותר, ניתן לסנן את הרעש הסביבתי באמצעות מסנן (High Pass Filter). אך מחולל רעש אקוסטי ייעודי, כזה המייצר רעש בתדרים גבוהים, יהיה פתרון אפשרי להסתרת הזליגה.

רנדומיזציה של המודולוס

טכניקת הרנדומיזציה של המודולוס (במקור: 'Modulus Randomization'), אומרת כי על מנת לחשב $m_q = c^{d_q} \bmod q$, יש קודם לבחור מספר טבעי באורך ממוצע - בינוני, t, ולחשב $m'_q = c^{d_q} \bmod tq$, לאחר מכן לבצע את הרדוקציה $m_q = m'_q \bmod q$.

דרך מתוחכמת יותר היא לשנות את המודולוס למכפילים שונים של q במהלך לולאה העלאה בחזקה המודולרית, מה שיקשה על התוקף לזהות את המבנה של q.

סיכום

כמו שציינתי, פגשתי את העבודה המרשימה הזו כשהייתי צריך לכתוב סמינר בקריפטוגרפיה. היו חלקים שלא לגמרי הבנתי או שהרגשתי שחסרים בהם נימוקים, ולכן החלטתי להרחיב ולסכם אותם בצורה הברורה ביותר. אני ממליץ בחום על צפייה בהרצאה קצרה מכנס קריפטו 2014[14].

משהו בהתקפות ערוץ צדדי מקסים בעיניי, במקום לחפש חולשות באלגוריתם עצמו, מחפשים חולשות במימוש. נניח שחבר קרוב סיפר שיש לו ארנק דיגיטלי עם כמות בדיונית של מטבעות מבוזרים בשווי עצום. במקום לנסות לפרוץ לארנק שלו ישירות, הרבה יותר יעיל לפרוץ לו לבית ולקחת את המפתח הדיגיטלי. הדוגמה אולי קיצונית, אבל היא ממחישה היטב את הרעיון שמאחורי התקפות מסוג זה: לנצל את הדרך שבה הקריפטוגרפיה מיושמת, ולא רק את התאוריה שמאחוריה.

על המחבר

בר טופליאן, סטודנט למדעי המחשב באוניברסיטה הפתוחה (לקראת סיום התואר ולפני תואר שני). בעל תשוקה לאבטחת מידע, למתמטיקה ומה שבניהם (להכין פיצה נאופוליטנית, משום מה...). משתדל לקרוא כמה שאפשר וללמוד, שואף לחקור סייבר.

LinkedIn: bar toplian, Instagram: bar_toplian, Email: bar.toplian@gmail.com

מקורות מידע

[1] https://digitalwhisper.co.il/files/Zines/0xAB/DW171-4-CryptoVideo.pdf

[2] Genkin, D., Shamir, A., & Tromer, E.

[3] Genkin, D., Shamir, A., & Tromer, E. (2017). Acoustic Cryptanalysis. *Journal of Cryptology*, *30*(2), 392-443. https://doi.org/10.1007/s00145-015-9224-2.

[4] Wikipedia contributors. (2025, January 1). GNU Privacy Guard. In *Wikipedia, The Free Encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=GNU_Privacy_Guard&oldid=1266666595.

[5] Daniel, M. P., Kumar, N. V., Swathi, K., & Subrahmanyam, V. (2023). Securing Your Smartphone: A Guide to Identifying and Avoiding Malicious Mobile Apps. *Technology*, *9*(11), 15-21.

[6] Ebert, Nico & Geppert, Tim & Knieps, Melanie & Zarouali, Brahim & Schaltegger, Thierry & Wiedemann, Anna & Ambuehl, Benjamin & Ch,. (2024). REFLECTIVE DATA SHARING ON TIKTOK: ENCOURAGING ADOLESCENTS TO ENGAGE WITH PRIVACY SETTINGS Completed Research Paper.

[7] Wikipedia contributors. (2024, December 30). Faraday cage. In *Wikipedia, The Free Encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Faraday_cage&oldid=1266194129.

[8] Wikipedia contributors. (2024, December 16). Air gap (networking). In *Wikipedia, The Free Encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Air_gap_(networking)&oldid=1263343824.

[9] Wikipedia contributors. (2024, December 25). Electronic filter. In *Wikipedia, The Free Encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Electronic_filter&oldid=1265230579.

[10] Wikipedia contributors. (2025, February 19). Loop unrolling. In *Wikipedia, The Free Encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Loop_unrolling&oldid=1276558448.

[11] Wikipedia contributors. (2025, January 15). Adaptive chosen-ciphertext attack. In *Wikipedia, The Free Encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Adaptive_chosen-ciphertext_attack&oldid=1269678232.

[12] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptol.10(4), 233-260 (1997).

[13] R.L. Rivest, A. Shamir, Efficient factoring based on partial information, in Eurocrypt 1985 (Springer, 1985), pp. 31-34.

[14] https://www.youtube.com/watch?v=DU-HruI7Q30&pp=ygUWYWNvdXN0aWMgY3J5cHRhbmFseXNpcw%3D%3D