digital whisper
Technologic Papers

מבוא לקריפטואנליזה מבוססת וידאו

מאת בר טופליאן

הקדמה

ראשית, חשוב לי לציין כי המאמר מבוסס על העבודה הנהדרת של קבוצת החוקרים[1] מהמחלקה להנדסת מערכות תוכנה ומידע באוניברסיטת בן-גוריון שבנגב, שפורסמה בשנת 2023, תחת הכותרת "Video-Based Cryptanalysis" (קריפטואנליזה מבוססת וידאו). מבין המחקרים הרבים בתחום, ובפרט אלו שפורסמו על ידי מעבדות המחקר באוניברסיטת בן-גוריון שבנגב, המאמר שסייג לעצמו חשיבות רבה, ושבמהרה צבר תהודה בקרב ענף אבטחת המידע וזכה לכבוד הראוי לו, הוא המאמר העוסק בקריפטואנליזה מבוססת וידאו[2]. המאמר מתאר שיטה חדשה, המאפשרת חילוץ מפתחות קריפטוגרפיים, מתוך ניתוח סרטוני וידאו של נורית LED ממכשירים ניידים, אשר משקפים שינויים זעירים בעוצמת האור כתוצאה מחישובים קריפטוגרפיים.

רקע

אבטחת מידע הוא תחום הניצב בקדמת החזית הטכנולוגית, 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 לפענח אותו. 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?

מצלמות וידאו כיום הן נחלת הכלל, כמעט כל אדם מחזיק מכשיר בעל מצלמה בכיס של המכנס. מצלמות וידאו, שללא ספק הפכו לסוג החיישנים הנפוץ ביותר בעת הזו, משולבות במגוון מערכות ומכשירים (מכשירים ניידים, רכבים, רחפנים, מכונות משקאות, כספומטים, מערכות אבטחה ועוד אין ספור נוספים), ואף משולבות בסביבות השונות (למשל, תחבורה ציבורית, בתים, משרדים, עסקים וכבישים). השימוש הנרחב במצלמות וידאו, והטמעתן בכל מקום בסביבתנו היומיומית, גרם לכך שכמעט לא ניתן לברוח לחלוטין מאמצעי או סביבה בה יש מצלמת וידאו משקיפה.

למצלמות וידאו יש שימושים ויתרונות, בין אם לכידת רגע משפחתי ובין תיעוד נהג המתפרע בכביש. אך למצלמות וידאו ורוחב פריסתן יש חסרון מהותי, והוא סיכון. במקרים מסוימים אפילו איבוד הפרטיות. מצלמות וידאו מאפשרות ריגול, תפיסת אדם במעשה, תיעוד מצבים רגישים ומסמכים סודיים, ולמעשה מאפשרות גישה למצבים, מקומות ואנשים, בצורה דיסקרטית.

בעוד שקיימים מחקרים, וישנה מודעות לניצול שימוש במצלמות וידאו לטובת ריגול, תיעוד והקלטה, והדיון בנושא שימוש במצלמות על מנת זיהוי פנים כבר חדר לתודעה הציבורית ורב העיסוק בו, מעטים, אם בכלל מספר המחקרים המציגים את הסיכונים שהמצלמות מהוות עבור סודיות המידע בעולם הדיגיטאלי, וסיכון הפרטיות. סיכון זה לאו דווקא נובע ממרכז התמונה והאובייקט שנתפס, אלא בפרטים ברקע התמונה, כאלו שעין אנושית לא יכולה לנצל.

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 הרחבה 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. 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

במחקרם, החוקרים מראים כי חישובים קריפטוגרפיים המבוצעים על ידי מעבד המכשיר משנה את צריכת החשמל של המכשיר, מה שמשפיע על בהירות נורת ה-LED שלו. החוקרים, בהתבסס על הבחנה זו, מציגים כיצד תוקפים יכולים לנצל מצלמות וידאו מסחריות (למשל, מצלמת iPhone 13 או מצלמת אבטחה מחוברת לרשת), כדי לחלץ מפתחות סודיים ממכשירים.

החוקרים מציינים כי ניצול אפקט הצַמְצַם (rolling shutter), מאפשרת הגדלה של שיעור הדגימה פי שלושה סדרי גודל מקצב התְּמוּנִית לשנייה (Frames Per Second), מ-60 ל- 60,000, עבור מכשיר מדגם iPhone 13 Pro Max.

החוקרים מספקים שתי דוגמאות ליישום קריפטואנליזה מבוססת וידאו:

- חילוץ מפתח ECDSA באורך 256 סיביות מכרטיס חכם, על ידי ניתוח צילומי וידאו של נורית ה-LED של קורא הכרטיסים החכם, שהושג באמצעות השתלטות (hijacking) על מצלמת אבטחה המחוברת לרשת, הממוקמת כשישה עשר מטרים מהקורא החכם.
- חילוץ מפתח (SIKE Supersingular isogeny Diffie-Hellman key exchange), באורך 378 סיביות, ממכשיר Samsung Galaxy S8, על ידי ניתוח צילומי וידאו במכשיר iPhone 13 Pro Max, של נורית ה-LED ברמקולי ה-Logitech Z120 USB, שהיו מחוברים לרכזת (USB hub), בה השתמשו לטעינת מכשיר הנייד.

מודל ההתקפה, דגימה וקצב דגימת המידע

בקריפטואנליזה מבוססת וידאו, התוקף מחלץ מפתח הצפנה סודי ממכשיר המטרה, באמצעות שימוש בצילום וידאו של נורית ה-LED של מכשיר המטרה. ניתן לעשות זאת באמצעות התקפה ישירה (בה נורית ה-LED ממוקמת פיזית על מכשיר המטרה), או התקפה עקיפה (בה נורית ה-LED אינה ממוקמת פיזית על מכשיר המטרה אך מושפעת משינוי צריכת המתח של המכשיר).

התוקף מנצל קשר בין פעילות המכשיר לבין אור הנורית שלו. כאשר המכשיר מבצע פעולות קריפטוגרפיות, צריכת החשמל שלו משתנה. במכשירים רבים, נורית ה-LED (למשל, נורית ההפעלה) מחוברת ישירות למעגל החשמלי של המכשיר. ללא הגנה מספקת, שינויים בצריכת החשמל עשויים להשפיע על בהירות הנורית.

התוקף יכול לנתח את השינויים הזעירים בצבע ובבהירות של הנורית (באמצעות ניתוח ערכי RGB), ולהסיק מהם מידע על הפעולות הקריפטוגרפיות המתבצעות במכשיר. זוהי צורה של 'דליפת מידע צדדית' שמאפשרת לתוקף לבצע קריפטואנליזה, כלומר לפענח את המידע המוצפן, בלי גישה ישירה למכשיר עצמו."

מכשיר התקיפה

מתבצעת ההנחה כי מכשיר המטרה (מעתה נפנה עליו רק כ-המכשיר), מבצע פעולות קריפטוגרפיות. מקור הפעולות הקריפטוגרפיות יכול להיות מכמה יזמים:

- **משתמש המכשיר** - על ידי שימוש ב-TLS session (פרוטוקול שמטרתו לאבטח הודעות העוברות בין צד שרת/לקוח), לצורך גישה לאתר מאובטח (HTTPS), או בעת שימוש ברשת פרטית וירטואלית (VPN).
- **התוקף** - על ידי שליחת הודעות למכשיר, כך שהן יבצעו פעולות חתימה אוטומטיות (על מנת לבסס אמיתות מקור ההודעה).

בנוסף, מניחים כי המכשיר מכיל נורית חיווי, או מחובר למכשיר נוסף/ ציוד היקפי בו יש נורית כזו. נורית החיווי יכולה להיות שייכת לכמה מטרות ובהתאם צבעה ופעילותה:

- **הדלקה/ כיבוי** - סוג הנורית הנפוץ ביותר במכשירים, צבע הנורית בדרך כלל אינו משתנה והנורית מאירה רק בעת שהמכשיר דלוק.
- **נורית התראה** - נפוצה יותר בקוראים חכמים דיגיטליים, צבעה משתנה בהתאם לפעולות קריפטוגרפיות.

התוקף

ישות זדונית בעלת מניע לחלץ את מפתח ההצפנה הסודי של המטרה, בכדי לפענח מידע מוצפן קודם ועתידי, שהצליח ליירט, שמקורו (או יעדו) הוא המכשיר.

השגת הווידאו

מתבצעת ההנחה כי התוקף יכול לשים את ידו על צילומי וידאו המכילים את נורית ה-LED של המכשיר בזמן פעילות קריפטוגרפית. החוקרים מתייחסים לשני מודלים להשגת צילומי הוידאו:

- **השגת הוידאו דרך גישה מקומית פיזית** - התוקף משתמש במצלמת המכשיר החכם שברשותו, על מנת לצלם את נורית המכשיר בעת פעילות קריפטוגרפית. כלומר, התוקף כנראה ימצא באותו החדר עם המטרה, או בקרבה מספקת לשימוש.
- **השגת הוידאו על ידי הרשת** - התוקף ישיג גישה לצילומי הוידאו דרך פריצה למצלמת אבטחה המחוברת לרשת. החוקרים מניחים כי המצלמה ממוקדת על המכשיר, או שמצלמת האבטחה יכולה להסתובב כ-360 מעלות, מצוידת בזום אופטי וממוקמת עד כ-16 מטרים מהיעד. בנוסף, החוקרים מניחים כי התוקף בעל שליטה בפעולות ותזוזות המצלמה, ויכול לייצא את תצלומי הוידאו.

השגת הוידאו דרך מצלמת רשת פרוצה היא הנחה סבירה, והחוקרים מציינים כי ישנם מחקרים רבים לעניות רמת אבטחתן של המצלמות כנגד התקפות אבטחה.

חשיבות המודל

החוקרים מציינים כי מודל תקיפה זה הוא אינו פולשני. כלומר, הוא אינו דורש חיבור/ גישה פיזית למכשיר המטרה, ומסתמך רק על ציוד שגרתי ושאינו מעורר חשד (אינו מסגיר את ייחודיו כמו אמצעים אחרים ובולטים בסביבה הציבורית).

הגדלת קצב דגימת נתוני המצלמה

החוקרים מציינים כי במרבית המכשירים הניידים המסחריים, וברוב מצלמות האבטחה, קצב ה-FPS הנתמך הוא כ-60 ל- 120. קצב הדגימה הנפוץ אינו מספיק עבור ביצוע קריפטואנליזה (עקב מהירות שינוי הנורית בעת ביצוע חישובים קריפטוגרפיים), ולכן, בכדי להגביר את קצב הדגימה, על מנת להגיע לקצב דגימה המאפשר ביצוע של קריפטואנליזה, התוקף יכול לנצל את אפקט הצַמְצַם.

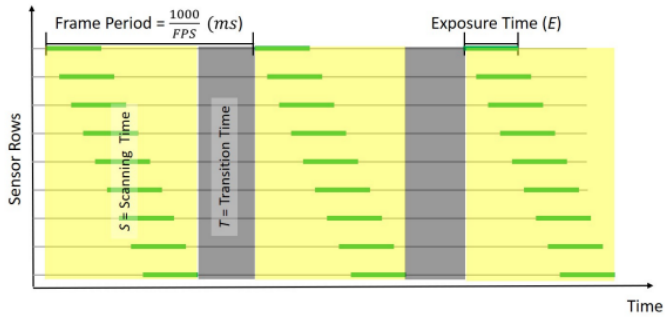
אפקט הצַמְצַם

שיטה ללכידת תמונה, כך שפריים של צילום וידאו נלכד על ידי סריקה של מרחב הצילום אנכית/ אופקית. כאשר שיטה זו בשימוש, פריים אינו מורכב מצילום בודד של הסצנה ברגע נתון, אלא ממספר צילומים של חלקים אנכיים/ אופקיים של הסצנה בזמנים שונים.

דוגמא לתהליך זה מופיע באיור 1- פיקסלים של החיישן נחשפים ונקראים שורה אחרי שורה בזמנים שונים מלמעלה למטה (או משמאל לימין), בהתאם למהירות סגר שניתן להגדיר (E), הקובעת את משך הזמן שבו החיישן חשוף לאור. כיוון שכל שורה (או קבוצת שורות סמוכות) במצב זה נלכדת בזמן שונה, התוקף יכול למעשה להגדיל את קצב הדגימה מקצב הדגימה של המכשיר (FPS 60-120) אל הקצב בו השורות נקלטות.

בקריפטואנליזה מבוססת וידאו, תוקף יכול לנצל אפקט זה על ידי צילום נורית ה-LED בשילוב תיעוד הנורית, כך שהמצלמה מתמקדת בנורית, הכי קרוב שניתן (באמצעות זום אופטי), באופן שהנורית תמלא את כל מרחב התמונה, והגדרת קצב הדגימה במכשיר להיות הגבוה ביותר שניתן. באופן זה הצליחו החוקרים להגדיל את קצב דגימת התמונה (וכך למעשה ללכוד את שינוי הנורית בזמן הפעולות הקריפטוגרפיות), מקצב FPS 60-120, עד כדי FPS 60,000, תוך שימוש במכשיר מסוג iPhone 13 Pro Max.

החוקרים מציינים, כי אפקט הצַמְצַם אינו מבטיח קצב דגימה אחיד לגמרי, אך מספק קצב דגימה אחיד למדי שמספק את הדרישות לביצוע הקריפטואנליזה.



[איור 1: אפקט הצַמְצַם במצלמת וידאו. בכל מחזור פריים מתבצעת סריקה של אובייקט הצילום אנכית לזמן חשיפה קצר (E). הזמן הכולל עבור הפריים מסומן ב-(S). בין שני פריימים עוקבים יש זמן מעבר, בו האובייקט לא נלכד בשום פריים כלל, זמן זן מסומן ב-(T).]

אנליזה

פונקציות חישוב האות

החוקרים הבחינו כי בהתאם לסוג נורית ה-LED על המכשיר, ישנם גורמים המשפיעים על איכות האות, לכן הם השתמשו בשתי פונקציות שונות על מנת לייצר אות מערוץ RGB נתון:

- **Rows - Average** - יוצרת אות (סדרת זמן) מערכי שורות הפריימים של הוידאו, על ידי חישוב ערכי ה-RGB הממוצעים בכל שורה בפריים. פונקציה זו, בעיקר מתאימה לסוג השני של נורית ה-LED.
- **Average - Frames** - יוצרת אות (סדרת זמן) מערכי הפריימים של הוידאו, על ידי חישוב ערכי ה-RGB הממוצעים עבור הפריים במלואו. פונקציה זו, בעיקר מתאימה לסוג הראשון של נורית ה-LED.

החוקרים מציינים כי הצורך להשתמש בשתי פונקציות שונות הוא עקב הרעש המתווסף לפריים. בכל פריים, רעש נמצא בפיקסלים אינדיבידואלים. כאשר האות חלש, הרעש בפריים יכול להאפיל על האות. כדי לפתור בעיה זו, משתמשים בפונקציה Average - Frames, אשר מפחיתה את הרעש, ומשפרת את יחס אות לרעש (SNR Signal-to-Noise Ratio).

לעומת זאת, כאשר האות חזק, חישוב ממוצע לפי שורה (שימוש ב-Average - Rows) משמר את הדקויות ואת השינויים הקטנים והמהירים, וכך מספק איכות טובה יותר לנתונים.

גורמי ההשפעה על קריפטואנליזה מבוססת וידאו

בחלק זה החוקרים מציגים את הגורמים המשפיעים על קריפטואנליזה מבוססת וידאו. לצורך כך, השתמשו החוקרים בשתי פונקציות על מנת לייצר אות מערוץ (RGB) נתון:

רוחב הפס

החוקרים בוחנים מספר מצלמות וידאו, כולן בעלות רוחב פס שונה כתגובה לשינויים בעוצמת הנורית.

למעשה, החוקרים בוחנים מצלמות הנבדלות ברגישות וזמן תגובה לשינויים.

החוקרים חיברו רכזת USB אל מחולל אותות, בו השתמשו כדי לחולל אותות (26 גלי סינוס במרווחים של 1000 Hz) בתדירויות של 200 - 25,200 הרץ (Hz). בניסוי שערכו בשימוש עם:

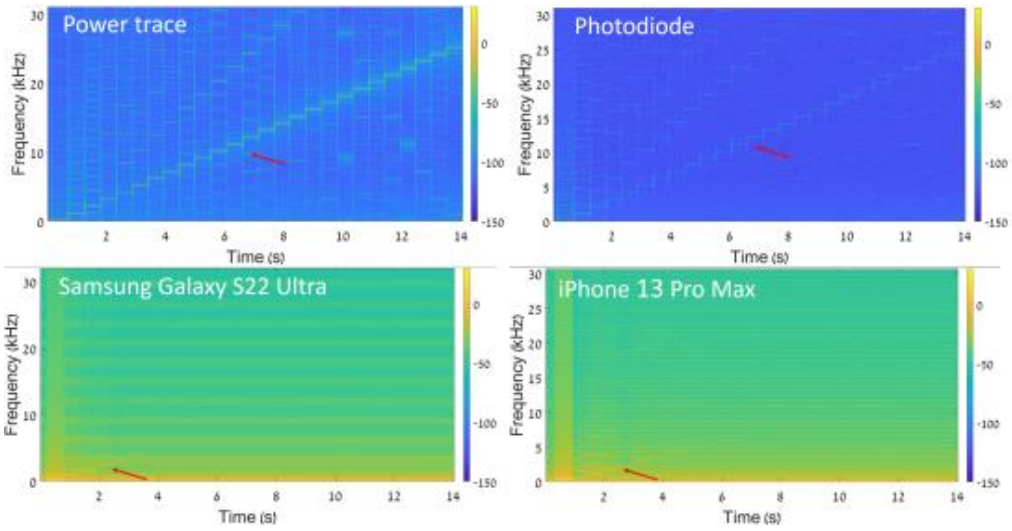
- iPhone 13 Pro Max, resolution: 1920x1080, FPS: 120, rolling shutter speed: $\frac{1}{61400}$
- Samsung Galaxy S22 Ultra, resolution: 1920x1080, FPS: 120, rolling shutter speed: $\frac{1}{12000}$

כאשר שני המכשירים מוגדרים למהירות הצַמְצַם המרבית הניתנת. כל אחד מהם משקיף על נורית ה-LED של רכזת USB, ומצלמותיהם צילמו את הנוריות על פי המתואר מעלה. בנוסף, החוקרים ערכו ניסוי דומה באמצעות דיודה רגישה לאור (photodiode), על מנת לקרוא שינוים בעוצמת הנורית הממוקמת על כרטיס NI-9223 ADC. הדיודה הוצבה כ-2 סנטימטרים מנורית המתח של הכרטיס, וקצב דגימה של כ-1000 KHz.

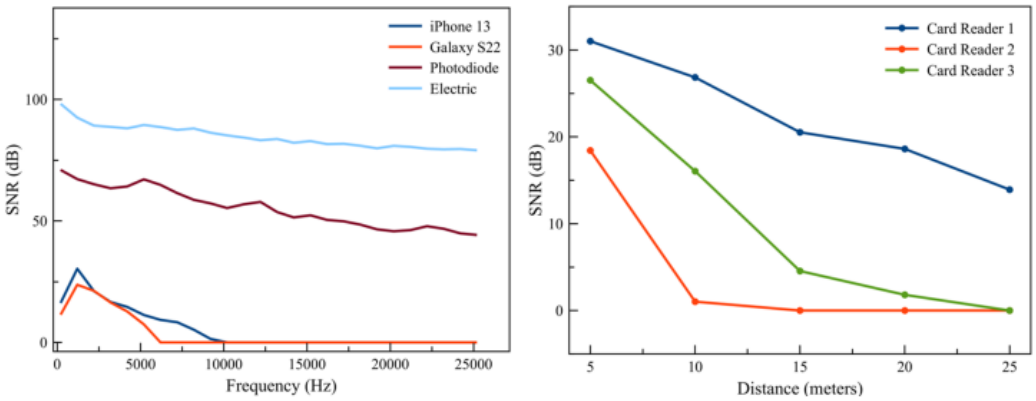
לאחר מכן, הפרידו החוקרים את האות לחלוקתו בייצוג RGB, ובחנו את טווח התדירויות המיטבי (בו המכשירים הצליחו לקרוא הכי טוב את האות), תוך כדי שהמשיכו להשוות את יחס האות לרעש (SNR). זאת על מנת לקבוע את רוחב הפס הכדאי. כך למעשה, החוקרים הראו כי סדר רוחב הפס של המכשירים שונה, ולא כולם תפקדו באופן זהה:

1. Photodiode (25 KHz).
2. iPhone 13 Pro Max (Maximum 10 KHz).
3. Samsung Galaxy S22 Ultra (Maximum 6 KHz).

את תוצאות ניסוי קריאת האותות לצד אות הבקרה, ניתן לראות באיור 2. את תוצאות SNR של המכשירים ביחס לתדירויות, ניתן לראות באיור 3:



[איור 2]



[איור 3]

ספריות קריפטוגרפיות ומקור הנורית

החוקרים ערכו ניסוי כדי לבחון את איכות האות ביחס לרעש (SNR - Signal-to-Noise Ratio) בתרחישים שונים. הם בדקו כיצד השימוש בספריות קריפטוגרפיות שונות משפיע על היכולת לבצע קריפטואנליזה מבוססת וידאו. הניסוי התמקד בשני סוגי נוריות LED:

נוריות המחוברות ישירות למעגל החשמלי של המכשיר. נוריות של אביזרים היקפיים, המושפעות באופן עקיף. החוקרים השתמשו בשלוש ספריות קריפטוגרפיות שונות ובדקו את פעולות החישוב הבאות:

- Libgcrypt 1.8.4 (ECDSA sign operation).
- GnuPG 1.4.13 (RSA decrypt operation).
- PQCrypto-SIDH 3.4 (SIKE operation).

באופן דומה לניסוי הקודם, בצעו את המדידות באמצעות מכשירים בעלי נורית LED, ומכשירים בהם הנורית שייכת לאמצעי היקפי. החוקרים הגיעו לתובנות כי יחס SNR הגבוה ביותר נמדד על ידי שימוש בספריית PQCrypto-SIDH 3.4, וביצוע פעולת SIK. ערכו נע בין 17.4-22.4 dB. היחס הנמוך ביותר, נמדד על ידי שימוש בספריית Libgcrypt 1.8.4 המבצעת (13.2-15.2 dB ECDSA sign operation).

החוקרים מצאו כי לקריאת הנורית בצורה עקיפה יש התנהגות לא מוחלטת (יכולה להגדיל או להפחית את רמת ה-SNR). אך המסקנה החשובה ביותר היא, שגם מכשירים בהם אין נורית LED באופן ישיר, יכולים להיות פגיעים לקריפטואנליזה מבוססת וידאו (בהינתן נורית LED המחוברת בצורה עקיפה ולא מבודדת). התוצאות לכך, באיור הבאה:

	Directly	Indirectly	
	Raspberry Pi 3b+	Connected USB Hub	Connected Speakers
Libgcrypt 1.8.4	15.2 dB	16.4 dB	13.2 dB
GnuPG 1.4.13	16.5 dB	17.6 dB	14.5 dB
PQCrypto-SIDH 3.4	18.1 dB	22.4 dB	17.4 dB

[איור 4]

מרחק

במחקרם, החוקרים בודקים את השפעת המרחק בין נורית ה-LED במכשיר המטרה, לבין מקור הצילום, וכן את השפעת הקשר בניהם על רמת ה-SNR. על ידי שימוש בשלושה כרטיסים חכמים, מצאו כי ניתן לבצע קריפטואנליזה מבוססת וידאו ממרחק של עד 25 מטרים (בתנאים מסוימים), והראו כי כרטיסים חכמים בעלי נוריות LED מהסוג השני, היו רגישות יותר, ומכך, פגיעות יותר לזיהוי השינויים. לעומת זאת, החוקרים גילו כי כרטיסים בעלי נוריות LED מהסוג הראשון, חשופים לפגיעה ממרחק של עד מטר אחד, ולפיכך, הם לא פגיעים לקריפטואנליזה מבוססת וידאו ממרחק.

תאורת הסביבה

אחרי בדיקה וניסוי של ביצוע קריפטואנליזה מבוססת וידאו בסביבות בעלי מאפייני תאורה שונים (אור/חושך/תאורת חדר), החוקרים הבחינו כי במידה ומרחק המצלמה קצר, אזי ההשפעה בין מצבי התאורה כמעט לא קיימת. זאת בניגוד להשפעה כאשר מרחק המצלמה גדול יותר, כך שתאורת הסביבה מעטה, כלומר, בסביבה חשוכה יותר, רמת ה-SNR גבוהה יותר, לכן, האות נקלט בצורה טובה יותר. ניתן לראות זאת בטבלה הבאה:

	Ambient Light		
	Darkness	Room Lighting (Fluorescent)	Sunlight
Data Acquisition	0 Lux	300 Lux	3000 Lux
Close via a smartphone (2 cm)	26.8 dB	14.6 dB	0 dB
Remote via a security camera (10 meters)	16.9 dB	17.2 dB	16.6 dB

[איור 5]

חילוץ מפתחות ECDSA

אלגוריתם ECDSA

בשמו המלא, Elliptic Curve Digital Signature Algorithm, הינו אלגוריתם קריפטוגרפי המבוסס על קריפטוגרפית עקומות אליפטיות על מנת ליצור חתימה דיגיטלית. האלגוריתם, מאפשר דרך לאמת את מקוריות המסר ושלמותו, ובכך לספק ודאות שהמסמך או הודעה לא שונו במהלך העברתם, ושהם מגיעים מהגורם המתאים.

האלגוריתם עושה שימוש במבנה מתמטי של עקומות אליפטיות, המאפשר רמת אבטחה גבוהה עם גדלי מפתח קטנים יותר, בהשוואה לאלגוריתמים מסורתיים, כמו RSA. תכונה זו הופכת אותו ליעיל במיוחד במכשירים בעלי משאבים מוגבלים.

במאמר, החוקרים מתארים את התקפת מינרווה (Minerva Attack)[3]. הם עושים בה שימוש על מנת להדגים שחזור של מפתח הצפנה ECDSA פרטי באורך 256 סיביות מקורא כרטיסים חכם, באמצעות קריפטואנליזה מבוססת וידאו. המחקר התבצע על צילומי וידאו של נורית המתח (סוג ראשון) של הכרטיס החכם, ממרחק של כ-5 מטרים, אשר הושגו מפריצה למצלמת אבטחה המחוברת לרשת.

ספריות קריפטוגרפיות נפוצות משתמשות בשיטה לייעול אלגוריתם ה-ECDSA על ידי הסרת אפסים מובילים במספרים מסוימים, אך שיטה זו יוצרת פגיעות, מכיוון שהייעול גורם למספר משתנה של פעולות חוזרות בתהליך החישוב. לכן זמן הריצה של התהליך משתנה, בהתאם למספר האפסים המובילים, במספר חד-פעמי שנוצר אקראית. תוקף יכול לנצל זאת על ידי מדידת זמן החתימה, ובכך להעריך כמה אפסים מובילים היו במספר החד-פעמי. מידע זה מאפשר לתוקף להשתמש בשיטות מתקדמות של קריפטוגרפיה מבוססת סריג, ליצור 'בעיית מספר מוסתר' ולפתור אותה באמצעות טכניקות של רדוקציית סריג. פתרון זה מוביל

לבעיית הווקטור הקצר ביותר, שפתרונה עשוי לחשוף את מפתח ההצפנה הפרטי. בסופו של דבר, ייעול שנועד לשפר ביצועים יוצר למעשה פתח לתקיפה שעלולה לחשוף את המפתח הפרטי.

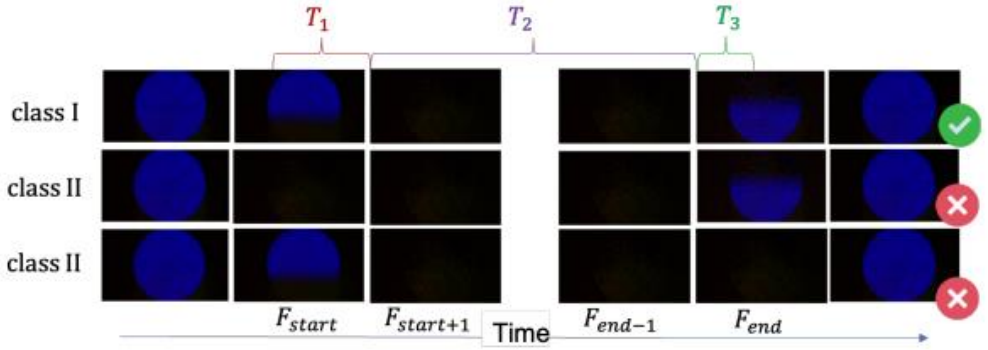
זיהוי פעולות ECDSA ממספר קוראי כרטיסים חכמים

במחקרם, החוקרים בחנו שמונה קוראי כרטיסים חכמים מסחריים שנרכשו באמצעות אתר Amazon. כל הקוראים הללו היו מצוידים בנורית חיווי מהסוג השני, כלומר נורית שאינה מחוברת ישירות למעגל החשמלי הראשי. החוקרים גילו כי נוריות החיווי בכל שמונת המכשירים מדליפות מידע לא מכוון. הדליפה התבטאה בשינויים בצבע הנורית, אשר הגיבה לפעולות שונות שבוצעו על ידי המחשב הנייד המחובר לקורא הכרטיסים. באופן ספציפי, החוקרים הצליחו לזהות שינויים בנורית שהתרחשו בתגובה לזמן הביצוע של חתימת ECDSA. ממצא זה מדגים כיצד אפילו רכיבים שנראים תמימים, כמו נורית חיווי, עלולים לשמש כערוץ צדדי לדליפת מידע רגיש על פעולות קריפטוגרפיות.

בוצעו חמישה ניסויים, בהם הכרטיסים החכמים מחוברים למחשב נייד דרך כבל USB, ודרך השקפה ממצלמה בעלת רזולוציה של MP5, וזום אופטי של X25. ממרחק של כעשרים סנטימטרים מנורית הקורא החכם, צולמו הכרטיסים החכמים מבצעים כשש פעולות חתימת ECDSA (מרווחים במרווחי זמן של ms200). החוקרים הראו כי עבור כל אות (שנוצר על ידי צילום וידאו מתאים), ניתן היה לראות את כל ששת פעולות ה-ECDSA.

שחזור מפתחות ECDSA ממרחק של כשישה עשר מטרים

באופן דומה לניסוי הקודם, הפעם ממרחק של כשישה עשר מטרים. החוקרים מיקדו את המצלמה כך שנורית ה-LED ממלאת את כל מרחב הצילום. הפעם, בסביבה חשוכה, הוקלטו כ-10,500 פעולות חתימת ECDSA שונות שביצע הכרטיס החכם (מרווחים במרווחי זמן של ms200). זמן ההקלטה של כל 10,500 הפעולות ארך כ-65 דקות, ומחולק לכ-35 הקלטות וידאו שונות (כל הקלטה ארכה כדקה וחמישים שניות), המכילות כ-300 פעולות חתימת ECDSA.



[איור 6]

כעת, בוצע לכל פריים פונקציה לקביעה האם הפריים משויך למצב בו הכרטיס החכם ביצע פעולת חתימת ECDSA, או למצב בו הכרטיס היה בהמתנה (idle). החוקרים הצליחו לזהות 10,500 פעולות ECDSA עוקבות,

המרווחות בניהן בפעולות המתנה. כמו כן, הם מיפו את הפריימים אל הפעולה המיוחסת להם. לאחר מכן, כל חתימה סווגה לאחת מבין שתי מחלקות (אלו ניתן לראות באיור 6:

- **מחלקה ראשונה** - סדרת פריימים של פעולת חתימת ECDSA, שהתחילו והסתיימו בזמן הסריקה. ניתן לזהות פעולות אלו על סמך ההחלפת צבע הנורית מכחול ושחור.

- **מחלקה שנייה** - סדרת פריימים של פעולת חתימת ECDSA, שהתחילו או הסתיימו בזמן הסריקה. ניתן לזהות פעולות אלו על ידי צבע שחור מלא בתחילת או בסיום הסדרה.

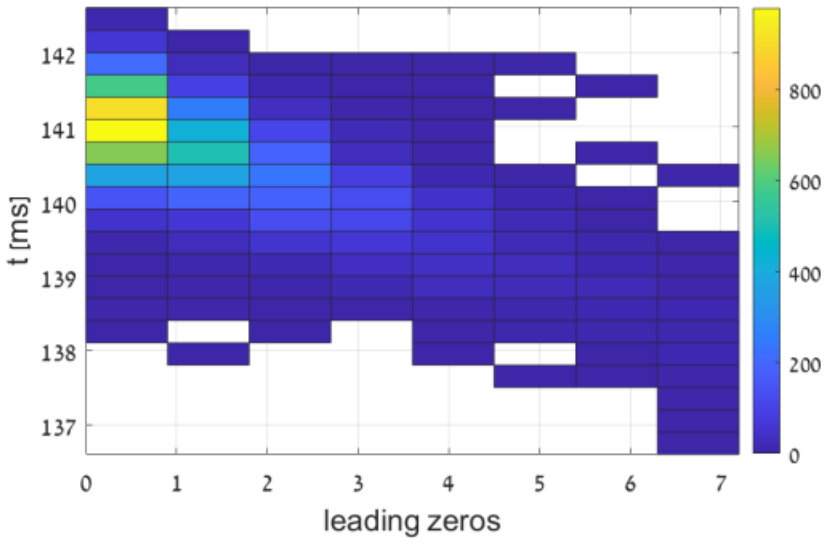
במהלך המחקר, החוקרים נתקלו באתגר משמעותי. הם גילו שלא ניתן לחשב במדויק את פעולת חתימת ECDSA עבור חלק מהמקרים - אלו שהתחילו או הסתיימו בדיוק בזמן הסריקה של המצלמה. מקרים אלו, שסווגו כ'מחלקה השנייה', היו בעייתיים מכיוון שחסר בהם מידע חיוני. ניסיון לכלול מקרים אלו בניתוח היה מוביל להכנסת שגיאות לתהליך החישוב. מכיוון שתהליך רדוקציית הסריג, שהוא חיוני לפענוח, רגיש מאוד לשגיאות, החוקרים החליטו לנקוט בגישה זהירה. הם בחרו להסיר לחלוטין מהניתוח את כל 2,674 החתימות שסווגו למחלקה השנייה. החלטה זו נועדה להבטיח את דיוק התוצאות ואמינות המחקר.

הערכת זמן חתימת ECDSA לפי סדרת הפריימים

החוקרים מתארים כיצד הצליחו לחשב את זמן המעבר (T) וזמן הסריקה (S), ואז לחשב את זמן ריצת כל סדרת פריימים עבור יתר 7826 החתימות מהמחלקה הראשונה.

לבסוף, הצליחו החוקרים לקבוע את זמן חתימת כל אחת מ-7826 חתימות ה- ECDSA שסווגו למחלקה הראשונה, ועליה לבצע את התקפת מינרווה. כך הצליחו לשחזר את מפתח ECDSA הפרטי באורך כ-256 סיביות, בפרק זמן של שתי דקות בלבד.

מפת חום המייצגת את הזמן המשוער לחישוב 7826 פעולות ECDSA, כפונקציה של מספר ה-0-ים המובילים:



חילוץ מפתחות SIKE

אלגוריתם SIKE

בשמו המלא, Supersingular isogeny Diffie-Hellman key exchange, הוא אלגוריתם פוסט-קוונטי לא בטוח (הוכח כי אינו בטוח בשנת 2022). אלגוריתם זה מאפשר לשני משתתפים שלא נפגשו מעולם, ואינם חולקים ביניהם מפתח סודי משותף כלשהו מראש, להעביר אחד לשני מעל גבי ערוץ פתוח מפתח פרטי, באופן דומה לפרוטוקול החלפת המפתחות של דיפי-הלמן (Diffie-Hellman key exchange).

אלגוריתם זה מבוסס על "הליכות" (walks) בגרף איזוגני סופר סינגולארי[4], ועוצב כך שיוכל לעמוד בפני התקפות קריפטאנליטיות מצד יריב עם מחשב קוונטי. לפני שנפרץ[5] ביולי 2022, היה נחשב האלגוריתם לבעל אורך המפתחות הקטנים ביותר מכל פרוטוקולי החלפת המפתחות הפוסט-קוונטים. אורך המפתח היה כ-2688 סיביות, ברמת אבטחה של 128 סיביות כנגד התקפות קוונטיות.

במאמר מתואר חילוץ מפתח ה-SIKE הפרטי, (מימוש של SIKE-751) באורך 378 סיביות. חילוץ המפתח התבצע באמצעות הספרייה הקריפטוגרפית PQCrypto-SIDH, על ידי שימוש בהתקפת הרצבליד [6] (Hertzbleed), נגד מכשיר Samsung Galaxy S8. חילוץ מפתח זה הודגם באמצעות קריפטואנליזה מבוססת וידאו, עבור הקלטת נורית ה-LED של רמקולי USB, המחוברים לרכזת USB, אליה מחובר גם מכשיר המטרה ממצלמת וידאו של iPhone 13 Pro Max.

התקפת Hertzbleed

מימוש אלגוריתם SIKE על ידי ספריית PQCrypto-SIDH, משקפת מידע בנוגע לסיביות המפתח, עקב מנגנון ה-DVFS של אינטל (dynamic voltage and frequency scaling). מנגנון זה מאפשר לתוקף לזהות חריגות בתדירות המעבד, באמצעות העמסת יתר על המעבד, כדי ליצור שינויים בתדר המעבד עם מספר רב של חישובים במקביל. פעולה זו יוצרת הבדלים בזמני הריצה בהתאם לנתונים המעובדים, והבדלים אלה, יכולים להיות מוגברים לרמת הבחנה של מילישניות. התקפה זו מופעלת על מנת לחלץ את המפתח הפרטי על ידי הערכת זמן הריצה של מספר פעולות די-אינקפסולציה (decapsulation) של SIKE. יתרת תיאור המנגנון מפורט במאמר ולא יובא כאן מפרט מורכבות חישובית וכלים מתמטיים מתקדמים.

מניעת יכולת חילוץ מפתחות באמצעות קריפטואנליזה מבוססת וידאו

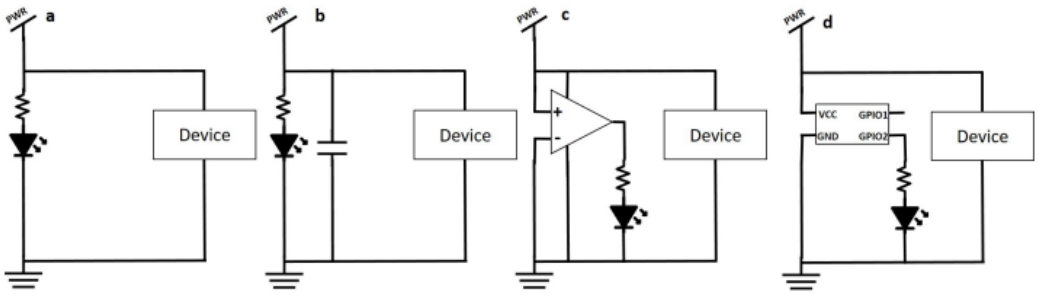
מניעת היכולת הזו רצויה לאור תגליתם של החוקרים, והקלות היחסית שניתן לחלץ מפתחות קריפטוגרפים פרטיים בשימוש ברעיון זה. החוקרים מציינים כי הדרך הטובה יותר למניעת היכולות הזו על ידי תוקף אפשרי, היא כמובן לוודא כי הספריות הקריפטוגרפיות בהן משתמש המכשיר על מנת לבצע חישובים ופעולות קריפטוגרפיות, אינן משקפות או משפיעות בצורה בלתי רצויה על גורמים שניתן לזהות ולנטר אותם. בפרט, השפעה על רכיבי חומרה שניתן לבצע קריפטואנליזה מבוססת וידאו על ידי צילומם. יתרה על כך, מובאות דוגמאות לפעולות שיכולים היצרנים והמשתמשים לבצע בעצמם, בכדי להסיר את הפגיעות המדוברת.

מניעת קריפטואנליזה מבוססת וידאו מצד היצרן

החוקרים מציעים ליצרנים להמנע כלל משימוש בנוריות מהסוג השני במכשירים שהם מייצרים, זאת מפני רגישותן הגדולה לפעולות הקריפטוגרפיות. למעשה, רמת הפריצות שלהן גבוהה, ומאפשרת קריפטואנליזה מבוססת וידאו ממרחק ובתנאי תאורה שונים.

עבור נוריות הסוג הראשון, שבדרך כלל מחוברות ישירות לאותם קווי המתח של המעגל החשמלי האחראי על העיבוד ועל ביצוע הפעולות הקריפטוגרפיות (איור a8), מומלץ השימוש בקבל (capacitor). זאת על מנת שישמש כמסנן תדרים (low-pass filter, איור b8). הוספת קבל היא פתרון יחסית זול להפחתת התנודות הנראות בשינויי המתח. עם זאת, עבור מכשירים שצורכים הרבה חשמל, יש צורך בקבל בעל קיבולת גדולה כדי לתמוך בצריכת המתח הגבוהה. קבל כזה עשוי להיות יקר יותר.

בנוסף, מוצעת האפשרות להשתמש במגבר-שרת (operational amplifier, OPAMP), שימצא בין קווי המתח ולבין נורית ה-LED (איור c8). לבסוף, ישנה האפשרות להשתמש בקווי יציאת וכניסת נתונים (general-purpose input/output, GPIO) של בקר השליטה המוטמע (לא בהכרח בכל מכשיר יש GPIO פנויים לשימוש), על מנת לספק מתח לנורית ה-LED.



=

מניעת קריפטואנליזה מבוססת וידאו מצד המשתמש

שיטה זו יכולה להיות פשוטה ופרימיטבית, כמו הדבקת רצועת דבק אטומה (בפרט בצבע שחור) על נוריות המתח של המכשיר. למרות הפגיעה החזותית בנראות המכשיר, שיטה זו פשוטה ביותר יכולה למנוע השגת מפתחות קריפטוגרפיים ממכשירים פגיעים.

סיכום

המאמר שסיכמתי מציג בצורה יפיפייה ואלגנטית התקפת ערוץ - צדדי שרובנו לא היינו בכלל משערים שאפשרית. הקסם של התקפות מסוג זה הוא שהן לא "גלויות" או מסמלות התקפות במובן הקונבנציונאלי ואפילו במובן הפופולארי.

את המאמר הזה פגשתי כחלק מהקורס "מבוא לקריפטוגרפיה". ניתנה לנו האפשרות להגיש סיכום על נושא מעניין בקריפטוגרפיה ומיד ידעתי איזה מאמר אבחר. הסיבה היחידה שהייתי מודע למאמר הזה, היא בגלל החדשנות שלו שגרמה לו להתפרסם לא רק במקומות הפרסום הטריוואליים. אני במקור פגשתי את הנושא הזה דרך סרטון[7] ברשת (מומלץ מאוד).

על המחבר

בר טופליאן, סטודנט למדעי המחשב באוניברסיטה הפתוחה. 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] Ben Nassi, Etay Iluz, Or Cohen, Ofek Vayner, Dudi Nassi, Boris Zadov, Yuval Elovici.

[2] Nassi, B., Iluz, E., Cohen, O., Vayner, O., Nassi, D., Zadov, B. & Elovici, Y., Video-Based Cryptanalysis: Extracting Cryptographic Keys from Video Footage of a Device's Power LED Captured by Standard Video Cameras, 1 Jan 2024, Proceedings - 45th IEEE Symposium on Security and Privacy, SP 2024. Institute of Electrical and Electronics Engineers, p. 2422-2440 19 p. (Proceedings - IEEE Symposium on Security and Privacy).

[3] J. Jancar, V. Sedlacek, P. Svenda, and M. Sys, "Minerva: The curse of ECDSA nonces (systematic analysis of lattice attacks on noisy leakage of bit-length of ECDSA nonces)," IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2020, no. 4, pp. 281-308, 2020.

[4] https://en.wikipedia.org/wiki/Supersingular_isogeny_graph.

[5] Wouter Castryck and Thomas Decru. 2023. An Efficient Key Recovery Attack on SIDH. In Advances in Cryptology - EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V. Springer-Verlag, Berlin, Heidelberg, 423-447. https://doi.org/10.1007/978-3-031-30589-4_15

[6] Y. Wang, R. Paccagnella, E. T. He, H. Shacham, C. W. Fletcher, and D. Kohlbrenner, "Hertzbleed: Turning power {Side-Channel} attacks into remote timing attacks on x86," in 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 679-697.

[7] https://youtu.be/vXe8pe18MNk?si=TM6fmkUJXKms7O80.