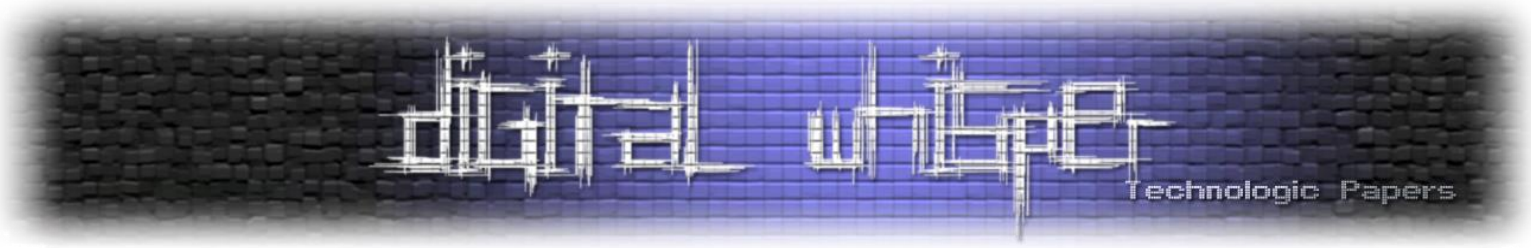

RFID Hacking

מאת אפיק קסטיאל (cp77fk4r)

הקדמה

היום נדבר על טכנולוגיה "חדשה" יחסית שנמצאת כרגע עוד בתחילת דרכה: RFID. RFID זהו קיצור של Radio Frequency Identification, שזה אומר "זיהוי אלקטרוני על גבי רדיו". בפועל מדובר על מעין התקן קטן (כמו מדבקה קטנה) שמצמידים לאותו חפץ שאותו רוצים לזהות. הרעיון המעניין מאחורי מדבקה זו הוא עניין הרדיו - המדבקה משדרת את הזיהוי שלה באופן אלחוטי על גבי גלי הרדיו לקורא הרלוונטי.

למה כתבתי את המילה "חדשה" במרכאות? כי הטכנולוגיה קיימת כבר הרבה זמן - היא הומצאה לפני כמעט מאה שנה, אך עקב העלויות, הגודל והתיפקוד- הנושא לא היה רלוונטי לשוק הכללי, ורק לאחרונה, כמה שנים בודדות אחרי שנת 2000, החל הרעיון לצבור תאוצה, עלות הפיתוח ירדה, וכמו כל דבר- המדע הצליח למזער אותה עוד ועוד עד שלאט לאט התחילו לפתח את זה לשוק הכללי.

קצת מידע כללי

בערך לפני שנתיים שלוש, (קצת לפני תחילת 2007) משרד התקשורת אישר שימוש אזרחי של RFID בארץ (אושרו התדרים 915-917MHz) והשוק התחיל לפרוח.

כל המערכת מחולקת לשני חלקים עיקריים:

- **Transponders** - ("תגי קרבה" - המשדר) - מדובר בתג קטן אשר מסוגל לשדר את המידע המאוחסן עליו באופן אלחוטי, כל תג כזה מורכב משני חלקים עיקריים, משבב קטן המאחסן את המידע, ומאנטנה פנימית/חיצונית שתפקידה לשדר את המידע המאוחסן על השבב, לרוב התג לא יהיה מחובר לשום מקור אנרגיה, והוא ישתמש באנרגיה שהוא מקבל מהשדה האלקטרו-מגנטי שמפיץ קורא הכרטיסים- אך הדבר אינו מחייב.

בכל תג מותקנים אחד משני סוגי צ'יפים, צ'יפים לקריאה בלבד, וצ'יפים גם לקריאה וגם לכתיבה, שטח של כ-2MB, אך לכל צ'יפ הניתן לכתיבה יש סקטור שבו מאוחסן הקוד היחודי של השבב שעליו אפשרות הכתיבה מוגבלת.

- **Interrogator** - ("קוראי קרבה" - הקולט) - מקלט, מחובר לאנטנה פנימית או חיצונית (לפעמים המקלט יהיה מחובר למספר מרובה של אנטנות בכדי לשפר את יעילותו), המקלט גם מפיץ שדה אלקטרו-מגנטי בתדר ספציפי קטן יחסית אך בסדר גודל המספיק בכדי לשמש כמקור האנרגיה לתגי הקרבה הנמצאים בסביבתו. הקורא יהיה עצמו מחובר בדרך כלל למחשב, בצורה חוטית, או בצורה אל-חוטית על גבי תשדורת Wi-Fi או Blue-Tooth וכד' אשר מספקת את השרת שמנהל את הנתונים.

קיימים מספר סוגים של תגי RFID:

- Passive TAG - תגית RFID ללא שום מקור אנרגיה, זאת אומרת שבמצב רגיל היא לא משדרת שום דבר, ורק לאחר שהוא נכנס לשדה האלקטרו-מגנטי של קורא הכרטיסים הוא נטען על-ידו ומשדר את המידע.
- Active TAG - תגית RFID המחוברת למקור אנרגיה, וכך היא יכולה לשדר את המידע שלה בכל זמן נתון גם במצב שבו היא ממוקמת רחוק מכל שדה מגנטי.
- "Semi Active TAG" - תגית RFID אשר משתמשת בסוללה קטנה יחסית אבל את שידור המידע היא מבצעת באמצעות אנרגיה חיצונית (כגון השדה המגנטי של קורא הכרטיסים).

כיום תגי ה-RFID משתמשים בארבעה אורכי-גל שונים, כל אורך-גל משדר למרחק שונה, ומאופיין ביכולות שונות ולכן משמש לצרכים שונים.

- **125 KHz** - מיוחס כ-Low Frequency, התדר הנמוך ביותר בשימוש כיום (גם בארץ), משדר למרחק של עד שלושים סנטימטר בקירוב, ואינו מסוגל להתמודד עם יותר מקריאה של תגית אחת בכל פעם, משמש בעיקר למערכת בקרת כניסה שונות - כמו למשל כמפתח כניסה לדלת, שעוני נוכחות, כרטיסי אשראי וכו'.

- **13.56 MHz** - מיוחס כ-High Frequency, משדר למרחקים של קצת יותר ממטר, משתמשים בו בעיקר לניהול לוגיסטי של מכולות, מעקב אחרי מוצרים בזמן פיתוח המוצר וכו' - קיים בארץ.

- **UHF** - מיוחס כ-Ultra High Frequency, משדר למרחקים של קצת פחות משבעה מטרים. משתמשים בו בעיקר לניהול מחסנים שלמים. השימוש בו אושר בארץ אך עם הגבלות מרובות ולכן כמעט ולא תמצאו אותו בשימוש.
- **2.45 GHz - מיוחס כ-**Microwave**, הוא התדר הגבוה ביותר שנמצא בשימוש כיום והוא משדר למרחקים עצומים, השימוש העיקרי שנעשה בו הוא למעקב אחרי מכוניות. בעיקר נגד גנבות ומעקב אחרי פס ייצור. לא קיים בארץ.**

- **Ultrasound** - כמעט ולא נמצא בשימוש, אך עדיין כדאי להזכיר אותו - משדר למרחק של עד 5 מטר, משתמש לזיהוי מרחבי, נקרא גם RTLS, קיצור של "Real Time Location System". לא קיים בארץ.

המתקפה

הרעיון הכללי

איך כל מתודת השימוש ב-RFID עובדת:

- שלב ראשון - תג RFID מוצמד לאובייקט כלשהו. התג מכיל קוד ייחודי לו אשר מאפשר לקורא התגים לזהותו.
- אם מדובר ב-Active-Tag, התג משדר את הקוד ללא הפסקה. אם מדובר בPassive/Semi-Tag, התג אינו משדר את הקוד אך בהגיעו לשדה אלקטרו-מגנטי (שלרב מופץ על-ידי קורא התגים) משתמש התג באנרגיה שבשדה ומשדר את הקוד הייחודי לו בתדר קבוע מראש.
- קורא התגים מוגדר להאזין באותו התדר עליו משדר תג ה-RFID וקולט את המידע ששידר אותו התג.
- קורא הכרטיסים מעביר את הנתונים שקיבל מתג ה-RFID אל מערכת הבקרה הכללית- מחשב אשר תפקידו לנהל/להשתמש במידע (אם מדובר במערכת בנק או מעקב כניסה/יציאה בעבודה, מוצרים בעגלת מכולת וכו').

חולשות מתודת השימוש ב-RFID

קיימות מספר חולשות בסכמה זו, נגע בשתיים מהן:

- **Unencrypted Storage** - כיום כמעט ולא נמצא בשימוש שום תקן אשר תפקידו לקבוע הצפנה או שימוש בהצפנה כל-שהיא בעת אחסון הנתונים על גבי תג ה-RFID עקב עלויות השימוש בתג זה. הנתונים המאוכסנים על גבי זכרון הצ'יפ נשמרים כמעט תמיד כמו שהם (Clear Text) ולא בשום צורת הצפנה/עירבול/גיבוב, לא בעת השידור לקורא התגים, ולא בעת העברת המידע למערכת המיחשוב האחראית לניהול המידע. **התקנים אשר כן נמצאים בשימוש חשופים לחולשות רבות וניתן לפרוץ אותם באופן פשוט עד כדי מגוחך** (מדובר בשני מנגנוני הצפנה, הראשון הוא DST אשר פותח בידי חברת Texas Instruments, אשר תומך במפתחות עד 40-bit, המנגנון נפרץ ע"י JHU-RSA כשנה לאחר תחילת השימושו בו בשנת 2005. השני הוא NXP אשר נפרץ ב-2008 ע"י קבוצת האקרים הגרמנית הידועה "The Chaos Computer Club".
- **None Authorization System** - תג ה-RFID מוגדר לשדר את המידע שהוא מאחסן כל עוד הוא מחובר למקור אנרגיה, אם פנימי ואם חיצוני ללא שום מערכת אשר קובעת כי אכן מדובר בקורא תגים מהימן. בנוסף, למשדר ה-RFID אין שום בקרה כי גם אם אכן מדובר בקורא מהימן אין שום יישות אשר מאזינה לאותו שדר.

בעזרת שילוב של שתי החולשות שראינו, נוכל לבצע התקפה אשר בעזרתה נוכל לגנוב את המידע הקיים על הכרטיס.

קורבנות פוטנציאלים

בארץ הנושא עוד לא הגיע לשיאו, אך בחו"ל (ארה"ב/אירופה) נושא פריצת ה-RFID מפותח מאוד ונמצא בשימוש נרחב. בין הקורבנות פוטנציאלים אפשר למצוא:

- כרטיסי אשראי (בינהם Visa Card, Master Card, American Express ועוד).
- כרטיסי גישה למקומות מוגבלים (נקראים גם "כרטיסי גישה חכמים").
- כרטיסי חניה (גם בארץ ניתן למצוא כאלה).
- כרטיסי תחבורה ציבורית המופעלים בעזרת RFID.
- מפתחות רכבים המופעלים בעזרת מפתחות RFID.

- כל מערכת המבוססת על RFID בלבד כמנגנון זיהוי.

מימוש המתקפה

כדי לממש את המתקפה יש צורך במספר כלים. הכלים אינם כלים ביתיים, אך הם עדיין זולים (באופן מפחיד) וחוקיים לחלוטין.

- RFID Reader/Writer - כגון: Point-RX, S300, XR-400, J168. (עולים כ-95 דולר ב-EBay).

- RFID Cable - כגון: SM8836, SM8837, SM8838 (יש מ-PVC ויש מ-Nylon-66, שניהם מספקים עבודה טובה) עולה כ-25 דולר ב-EBay.

יציאת SM8836 - כניסת USB למחשב.

- Driver מתאים - הנפוץ ביותר (ל-Win32) הוא ISC.MR101, אך התקנים שונים צורכים דרייברים שונים, ולכן אם מזמינים חובה לבדוק האם מגיע דרייבר מתאים.

- כלי לפיצוח ההצפנה (במקרה וקיימת), מדובר ב-Key-Search מבוסס Brute-Force פשוט.

בכדי לפצח את מפתח ההצפנה (40bit) לוקח (במקרה הגרוע ביותר) קצת יותר משבועיים, ולכן במקרים כאלה יש אפשרות ליעל את המנגנון (עד לתזמון של 10 שעות!) ע"י שילוב התוכנה על גבי לוח עיבוד הניתן לתיכנות (FPGA - ראשי תיבות של Field Programmable Gate Array). הנפוץ ביותר לשימוש כיום הוא "Cyclone II", והוא מגיע עם ערכת פיתוח מוכנה מראש.

מהלך המתקפה:

שלב ראשון - השגת המידע:

החלק הקשה במהלך הפריצה הוא להגיע לקרבה פיזית לתג, אך בגלל שמדובר בגלי רדיו אין בעיה לזהות את הזליגה גם מעבר לבדים או ארנקי עור לדוגמא (במצב שה-RFID הוצמד לכרטיס חכם אשר נמצא בארנק בתוך כיס אחורי או תיק של מישהו). מפני שהתג המשדר את המידע על גבי הצ'יפ משדר אותו ללא הבחנה, אין בעיה להשתמש בכל קורא ואין חובה להשתמש דווקא בקורא הייעודי לאותו כרטיס.

שלב שני - פיענוח המידע:

לאחר שהשגנו את המידע הנמצא על הכרטיס המצב הוא- או שהמידע מפוענח, כך שאין בעיה, או שהמידע הוצפן בעזרת אחד מהאלגוריתמים, בכדי לפענח את המידע יש צורך בהרצת ה-Brute-Force, בעזרת הכלים הנכונים, גם במצב הגרוע ביותר ייקח לא יותר מעשר שעות.

כמו שכבר ציינו, אחד האלגוריתמים השמישים ביותר להצפנת המידע הנמצא בכרטיסים אלו נקרא "Crypto-1", והוא הומצא ע"י חברה בשם NXP Semiconductors. החבר'ה שהצליחו לפרוץ את האלגוריתם, יצרו ספריה ב-C, המשמשת לבצע מספר התקפות על המידע המוצפן בעזרת האלגוריתם, שמה הוא Crapto1 (בדיחה על השם המקורי של האלגוריתם).

הספריה מכילה מספר פונקציות שמנצלות חולשות במנגנון האימות של ה-Crypto-1.

את הספריה אפשר להוריד מכאן:

http://crapto1.googlecode.com/files/crapto1-v2.4.tar.gz

מאמר המנתח לעומק את החולשות הקיימות באלגוריתם של NXP, ודרך ניצולם כמתקפה אפשר למצוא פה:

http://www.sos.cs.ru.nl/applications/rfid/2008-esorics.pdf

שלב שלישי - הנפקת הכרטיס

- אם מדובר בכרטיסי אשראי, המתקפה נגמרת פה - כל המידע על הכרטיס נמצא אצלנו, מספר הכרטיס ופרטיו האישיים של בעליו (שם/תעודת זהות וכו').
- אם מדובר בכרטיס חכם המאפשר גישה למקום מסויים - או כל כרטיס הצורך שימוש פיזי במידע שיש עליו, יש צורך גם בהנפקת כרטיס חדש עם הפרטים שהשגנו, ולכן אנחנו צריכים להשיג גם RFID Writer. כיום קיימים לא מעט התקנים אשר קוראים מידע וגם מסוגלים לכתוב מידע חדש על הכרטיס. הפעולה פשוטה, ובעזרת התוכנה המגיעה עם הכותב אין שום בעיה לבצעה.

בכדי לבצע פעולה זאת ישנה אפשרות להשתמש בכלים כגון "RFDump" שמסוגל להציג באופן מסודר את כל המידע "יבש" (Meta Information) כגון Tag ID, Tag Type, יצרן וכו', בנוסף הכלי מסוגל גם להציג ולערוך את המידע הקיים על הכרטיס (במידה וההתקן מאפשר זאת). התוכנה הנ"ל מאפשרת לייצא/לייבא את המידע מפורמט XML.

מפני שישנם הרבה סוגי כרטיסים וישנם מספר דרכי יישום לשמירת המידע, התוכנות משתנות בין חומרה לחומרה, התוכנה RFDump, למשל, מסוגלת לבצע את הפעולות רק מהתקנים שתואמים לרכיבי "ACG Multi-Tag" (תגים התומכים בתדרים 125 kHz ו- 134.2 kHz).

אפשר להשיג אותה בכתובת:

http://www.rfdump.org/dl/rfdump-1.3.tar.gz

במצבים בהם המידע המאוחסן על הכרטיס מוצפן יש להצפין את המידע לפני האחסון (בכדי לא ליצור אי-תאימות קריאה בזמן פיענוח המידע ע"י קורא הכרטיסים), אך זה לא מהווה בעיה, אלגוריתם ההצפנה מוכר לנו ואת מפתח ההצפנה השגנו כבר בשלב השני.

שלב רביעי - שימוש

מפני שרב המערכות משתמשות בתג ה-RFID כאמצעי היחיד לזיהוי המשתמש, אין בעיה לבצע את השימוש, למשל- כאשר מעבירים כרטיס עובד בדלת-חכמה אין צורך בהצגת תעודה מזהה, התעודה המזהה היא התעודה בעלת תג ה-RFID.

התגוננות

מה אפשר לעשות בכדי להתגונן? נכון לכתיבת שורות אלה, ההמלצה הטובה ביותר היא להמנע משימוש ב-RFID. מספר פתרונות אחרים:

- שימוש בתגי RFID מבוססי מפתחות הצפנה של 128-bit ויותר. (כגון BUSlink).
- שימוש בתגי RFID מבוססי מנגנון הזדהות חכם אשר ממוקם לפני שידור המידע כגון התגים של CryptoRF.
- שימוש בתגי RFID אשר מממשים את עקרון ה-RSA וכך בעצם מונעים מגורמים זרים להגיע למידע המוצפן עליהם.
- תגים התומכים בהעברת מידע על-גבי SSL או TLS.
- שימוש בתגי RFID מבוססי Token.

כאן תוכלו לקרוא מאמר מעניין מאוד של VeriSign על עקרונות אבטחת ה-RFID:

http://www.verisign.com/static/028573.pdf

סיכום + קישורים

נושא האבטחה בענף ה-RFID לא נמצא במודעות החברות או האירגונים הגדולים - לא בעולם ובמיוחד לא בארץ. המודעות לאבטחה בנושא נמצאת בעליה בשנה-שנתיים האחרונות, אך עדיין יש הרבה מאוד מה לשפר. אני מקווה שמאמר זה העשיר את הידע שלכם על הנושא ועל סכנות השימוש ב-RFID.

<u>מספר קישורים רלוונטיים:</u>

- ההסבר של JHU-RSA על פריצת ה-DST: http://www.rfidjournal.com/article/print/1415
- קישור (וידאו) להרצאה של CCC על פיצוח ה-XNP:
/http://www.videogold.de/iw/chaos-communication-camp-2007-24c3-mifare-security
- מידע על ה-FPGA:
http://www.altera.com/products/devkits/altera/kit-cyc2-2C20N.html
- קישור (וידאו) להסבר על מימוש הפריצה ב-Boing-Boing TV:
http://tv.boingboing.net/2008/03/19/how-to-hack-an-rfide.html
- מקור מידע מעניין עם כלים, תוכנות ומאמרים על הנושא: http://rfidiot.org/