Digital Whisper
Technologic Papers

תחום מפוספס - על אבטחת מידע בברקודים

מאת דניאל ליבר

מבוא

החודש חשבתי בכלל שאני אכתוב מאמר בנושא אחר, אבל אז קניתי כרטיס לאחד ממועדוני ההופעות הפופולריים בארץ וקיבלתי את הכרטיס במייל, להדפסה. ראיתי שהכרטיס מכיל ברקוד יחסית פשוט ומתחתיו מספר; תהיתי האם הברקוד שמודפס מכיל בדיוק את אותו המספר שכתוב תחתיו או לא (התברר שכן) ומפה לשם, הנחתי שאם יהיה בידיי מספר ברקוד בודד יהיה ניתן להדפיס כרטיסים מזויפים ללא בעיה (למען הסר ספק, מדובר במעשה בלתי חוקי ואין לראות במאמר זה המלצה לעבור על החוק). החלטתי לחקור באופן כללי מה עוד אפשר לעשות עם ברקודים וכך נולד המאמר.

מקור הברקוד

הרעיון הראשוני לשימוש בברקוד היה ב-1948 כאשר זוג סטודנטים באחד המכונים הטכנולוגיים בפילדלפיה שמע שיחה בין אחד הדיקנים במכון לבין בעלי רשת למוצרי מזון שהייתה קשורה ליצירת אוטומציה של תהליך ה-checkout בקופה על ידי קריאת מידע לגבי המוצר באמצעות תוויות. הנסיונות הראשונים כללו שימוש בדיו אולטרה-סגול (נכשל משום שהדיו התפוגג), ולאחר מכן בהשראת קוד מורס פותח הפטנט הראשון בתחום (התבנית הראשונה והמוכרת של ברקוד היא בעצם קוד מורס - קווים ונקודות - אשר 'זולגים' מטה ויוצרים פסים וקווים; בנוסף פותחה תבנית עגולה אשר איפשרה סריקה של הברקוד מכל כיוון).

לאחר מכן הפטנט התגלגל בין כמה חברות (IBM בתוכן) ולבסוף נקנה ע"י RCA. בינתיים, פיתוחים נוספים צצו מכיוונים אחרים; עובד לשעבר בחברת הרכבות בפנסילבניה עבד על פרויקט בשם KarTrak שעזר לזהות פסים מחזירי-אור שהוצמדו לקרונות (ברקוד ייצג את מספר החברה ומספר הקרון) בצבעי כחול ואדום, כאשר פיענוח הברקוד בוצע באמצעות מכפילור (מכפיל-אור) ומסננים לתדרים של אורך גל התואם לאדום וכחול.

הדחיפה האמיתית לברקוד הגיעה, כצפוי, מתחום המזון - ובאמצע שנות ה-1970 מספר חנויות מזון התנדבו לפיילוט לבדיקת טכנולוגיות שונות של יצירת ברקוד. בסופו של דבר, נבחרה ההצעה של IBM

(ברקוד פסים) לעומת ההצעה של RCA ברקוד עגול, בצורת Bullseye משום שמכונות ההדפסה היו מורחות את הדיו בכיוון ההדפסה. בתבנית מעגלית, פגם זה גרם לברקוד להפוך ללא קריא בעוד בברקוד פסים המריחה פשוט גרמה לברקוד להיות 'גבוה' יותר ולא פגמה ביכולת לקרוא אותו.

בשנת 1981 קיבל משרד ההגנה האמריקאי את השימוש ב-Code 39 (אחד מסוגי הברקודים החד מימדיים - פרטים בהמשך) כסטנדרט לסימון כל המוצרים שנמכרים לצבא האמריקני. המערכת, שנקראת LOGMARS (Logistics Applications of Automated Marketing and Reading Symbols) נמצאת עדיין בשימוש כיום.

סיווג וסימבולוגיה

יש מספר קטגוריות שונות אליהן ניתן לחלק את הברקודים (טבלה מפורטת ניתן למצוא כאן):

- **1D vs 2D** - כאשר מדברים על ברקודים ליניארים (1D), הכוונה היא לברקודים שבהם מדובר על אוסף פסים, כאשר אין שום חשיבות לאורך הפסים אלא לעובי הפסים ולמרווחים ביניהם. לעומת זאת בברקודי 2D יש חשיבות למידע גם במימד האורך וגם במימד הרוחב.

1D	2D
	

- **Character set** - כל ברקוד מייצג טווח תווים שונה. בין היתר ניתן למצוא אופציות נפוצות:
  - מספרים בלבד
  - אותיות 'גדולות' (Uppercase) + מספרים + תווים מיוחדים
  - תמיכה בכל תווי ה-ASCII
- **מגבלות גודל \ אורך** - רוב הברקודים הם בעלי אורך משתנה (או שטח משתנה, במקרה של 2D). עם זאת, יש מספר סוגים אשר בעלי אורך קבוע.
- **וידוא הברקוד** - ברקודי 1D לעתים מוסיפים ספרה או מספר ספרות על מנת לוודא את אמינות הקוד המקורי שקודד בברקוד. ברקודי 2D משתמשים ב-Error Correction על מנת לטפל בפגמים בברקוד (החל מגודל ריבוע ועד מריחות).

- **תקינה** - חלק מהברקודים נוצרו על ידי גופים לשימוש ספציפי (לדוגמא, הדואר האמריקאי) בעוד חלק מהברקודים האחרים נועדו לשמש כבסיס רחב למספר גופים (לדוגמא, EAN הוא חלק מסטנדרט אירופאי).

פענוח וקידוד

סורקי 1D ניידים (נקראים גם hand scanners) נחשבים לזולים למדי. באופן כללי מומלץ לא לקנות סורקים משוכללים במקרה ותחליטו להתעסק עם הנושא הזה. סורקי 2D היו יקרים בעשור הקודם אבל עם התקדמות הטכנולוגיה שלהם המחירים שלהם התחילו לרדת והיום הם במחיר סביר יחסית. כמו כן, כיום קיימים אתרים רבים שיכולים לפענח ברקודים, לדוגמא Inlite שמסוגל לפענח ברקוד על ידי העלאת התמונה שלו.

על מנת לקודד ברקוד, ניתן היום להשתמש במאות אתרים שונים שמסוגלים לקודד ברקודים מסוגים שונים. אם אתם מעוניינים לכתוב מקודד ברקודים משלכם, תצטרכו לשלם עבור מסמך המתאר את תהליך הקידוד המתבצע (בהתאם לסוג הברקוד שבחרתם). בעבר היה קושי להשיג מסמכים מהסוג הזה בעיקר כי הם ניתנו בעותק קשיח.

ברקוד ואבטחת מידע

הגדרות ואתחול (barcode configuration)

אחת הבעיות באופן כללי עם ברקודים הייתה הסורקים, משום שהם היו מקונפגים באמצעות ברקוד מיוחד שהיה מגיע עם הסורק ומכניס אותו למצב של אתחול. במצב כזה ניתן לשנות את ההגדרות של הסורק ולסרוק ברקוד נוסף שמעיד על סיום האתחול (או אתחול מחדש); מובן שמצב כזה מאפשר פתח לשינוי הגדרות ושיבוש פעולות הברקוד אפילו על ידי שינוי ה-encoding, שינוי תו ה-CRLF או שינוי של סוגי הברקודים הנתמכים במכשיר. לעתים היה ניתן גם לבצע עדכוני תוכנה בסורק באמצעות ברקודים מיוחדים. תסריט התקיפה כלל בדיקה באתר של ספק סורק הברקוד או היצרן, לעתים היו משתמשים גם ב-social engineering ומתקשרים אליהם מתוך מטרה לנסות להשיג את הברקודים הנ"ל.

העתקת \ החלפת ברקודים (barcode switching)

הניצול הכי ישן ומוכר בברקודים היה על ידי העתקת ברקודים. במקרה ואתם יודעים מה הברקוד שבידכם עושה, ניתן להעתיק אותו ולהשתמש בו בעיקר להונאות כספיות.

במקרה כזה כלים פשוט של מדפסת ביתי ומצלמה יספיקו לכם. מספר דוגמאות מעניינות לסוג הונאה כזו:

- גניבה שיטתית ב-3 מדינות שונות בסכום של כמיליון דולרים.
- גניבה של כ-70 אלף דולרים במוצרים על ידי יצירת ברקודים עם מחירים נמוכים והדבקתם על מוצרים שעלותם גבוהה יותר.
- בכיר בסאפ שגנב מוצרי לגו ומכר אותם ב-ebay.

רעיונות נוספים הם ברקודים אשר משמשים כהזדהות במקומות בהם ניתן לטעון כסף על החשבון - העתקת ברקודים עלולה לגרום לנזק ממשי ולגניבה של זהות מאדם אשר בעל סכום כסף משמעותי על הברקוד שלו. דוגמא נוספת היא מכונות שירות (מכונות כרטוס ברכבת, מכונות מחזור) אשר לעתים כללו כחלק מהברקוד את סכום הכסף ששילמת \ סכום הכסף שמגיע לך חזרה מהמכונה. במקרה כזה, מאוד קל לראות את ההשפעה הכספית של התקיפה.

אי-סנכרון (de-syncronization)

עקרון נוסף ששומש (בעיקר בגורם האנושי) היה עקרון אי הסנכרון: בעת הצגת כרטיס כלשהו, גורם הבקרה קורא את המספר שצמוד לברקוד בעוד הסורק מעביר למערכות הליבה את ערך הברקוד. במקרה ותוקף יוצר כרטיס אשר מכיל מספר וברקוד שאינם מסונכרנים (זאת אומרת, הערך המקודד בברקוד אינו המספר המוצג) אזי ניתן לבצע העלאת הרשאות: המספר מייצג את עובד א', ואילו הברקוד מייצג את עובד ב' (שיכול להיות בעל תפקיד רגיש ובעל כניסה לאיזורים נרחבים במשרד). במקרה והמערכת הליבה אינה מציגה לגורם הבקרה בחזרה פרטים המתקבלים כתוצאה מעיבוד ערך הברקוד, יש סיכוי גבוה לתקיפה כזו.

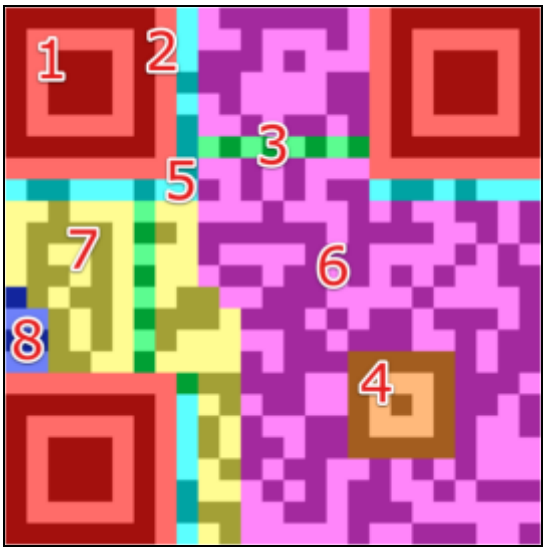
כמו כן, מקרה נוסף הוא לדוגמא במשרדים בהם משתמשים בסריקת הברקוד של המחשב הנייד (אשר מכיל גם את כתובת ה-MAC של המחשב) על מנת לאפשר כניסה לרשת התקשורת של המשרד רק למחשבים שמזוהים ע"י המערכת. במקרה ותשימו ברקוד שמכיל כתובת מסוג FF:FF:FF:FF:FF:FF, הדבר עלול לגרום למצב של broadcast ולשבש את כל הרשת.

הזרקות ברקוד (barcode injections)

לרוב שימוש בברקוד אמור להכיל מספרים, ולעתים גם אותיות. יש מספר סוגים של ברקודים אשר מכילים גם תווים מיוחדים (לדוגמא, Code128). במקרים כאלה ניתן גם להזריק תווים מיוחדים ולהשתמש בתוצאה על מנת לבצע הזרקות במערכות הליבה (back end) כדוגמת SQL\Separation string Injections או התקפות מסוג Format String. בברקודי 2D לרוב המצב אפילו מסוכן יותר שכן ניתן להכניס פנימה payloads שמכילים מספר רב יותר של תווים, וכבר ראינו בעבר כל מיני מקרים של התנהגות מוזרה בעת הכנסת תווים שאף אחד לא ציפה להם (סתם להמחשה - Poison null byte). מעבר לכך, ניתן לראות באופן כללי נסיונות של התקפות שאומנם מיועדות למערכות web אבל עדיין ניתן לנסות לתקוף גם באמצעות ברקודים (בהנחה והפלט מגיע למטרה שרגישה למתקפות מסוג זה כמו XSSאו SQLi).

QR Codes

QR הינו ברקוד מסוג 2D, כאשר הוא מורכב מהאיזורים הבאים:

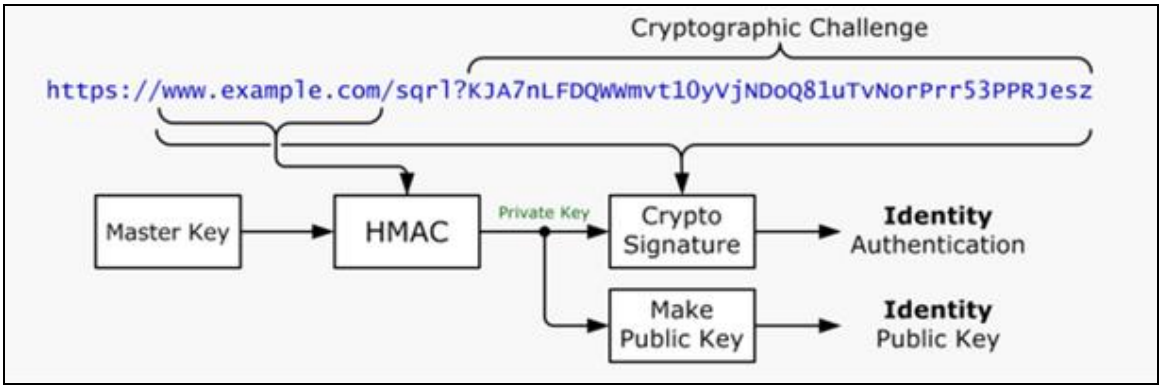


1. **Finder Pattern** - הריבועים ב-3 הפינות עוזרות לסורק להבין כי מדובר בקוד QR ובאיזה כיוון נסרק הקוד.
2. **Separators** - קו ברוחב פיקסל שמפריד את הריבועים מסעיף 1 על מנת להקל על הסורק לזהות שמדובר ב-QR.
3. **Timing Patterns** - מספר ריבועים שעוזרים לתוכנת הפענוח לקבוע את גודל מודול בודד.
4. **Alginment Pattern** - חלק שעוזר לתוכנת הפענוח להתמודד עם עיוותי תמונה.

5. **Format Information** - 15 ביטים שמכילים תיאור לגבי רמת ה-error correction של ה-QR.
6. **המידע**, מקודד ב-Bit Stream ומחולק למקטעים של 8 ביטים.
7. **Error Correction** - רמת תיקון השגיאות שה-QR דורש מתוכנת הפענוח.
8. **שארית**.

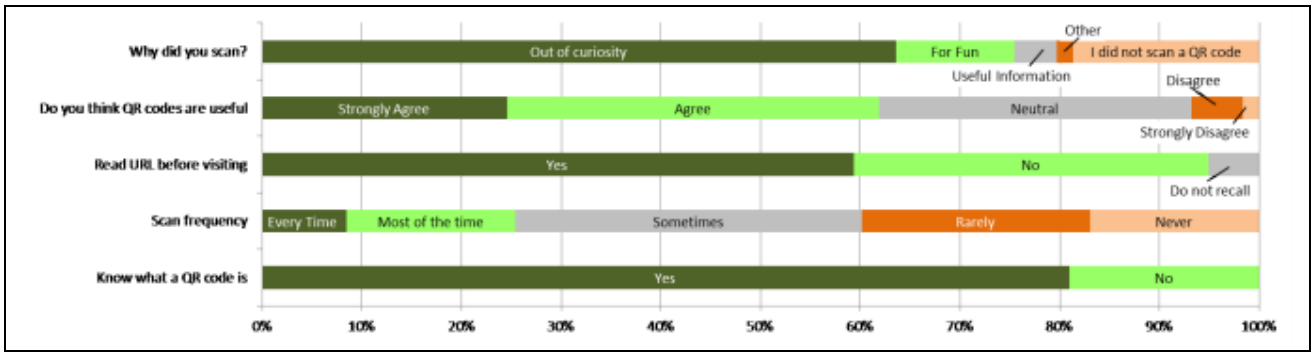
מה בעצם אפשר לעשות באמצעות QR? לרוב סביר להניח שה- QR יפנה את המכשיר שלכם לאתר שמשולב בו malware, בדרך כלל הוא יהיה JavaScript Tojan. הקלות שבה ניתן היום ליצור QR הופכת את התקיפה לקלה ביותר ביישום. אפילו במחיר של פרסומת בעיתון\לוח מודעות, ניתן לפרסם QR שכולו נועד למטרות תקיפה ולהשיג קהל רחב יעד. עוד דרך מעניינת שניתן לתקוף באמצעותה היא Stored XSS - בהנחה ואתם לא רוצים שיהיה לכם payload ששמור בתוך ה-DB (או כל מקום אחר), סביר להניח שתמונה נראית קצת יותר 'תמימה', במיוחד שכשפותחים אותה עדיין לא ברור לגמרי מה היא עושה.

בניגוד לפסקה הנ"ל שעלולה לשכנע אתכם ש- QR הוא המקור לכל הרוע בעולם, יש דווקא מספר מנגוני אבטחה שמנסים להסתמך על השימוש ב-QR. אחד מהם הוא ה-SQRL. איך זה עובד?



בהנחה ואתה מתקין על המכשיר שלך את ה-SQRL app, ברגע ההתקנה נוצר מפתח המיוחד למכשיר שלך באורך 256bits (נקרא גם - Master Key). בעת סריקת ה- QR באמצעות התוכנה, יחוללו מפתח פרטי וציבורי מהשילוב של ה-Master Key והדומיין שאליו אתה פונה. באמצעות HMAC. לאתר עצמו נשלחים 2 נתונים: המפתח הציבורי שלך (שמשמש גם בתור הזהות שלך) וכן Cryptograpphic challenge שמוצפן באמצעות המפתח הפרטי שלך. מכיוון שהאתר יודע מהו המפתח הציבורי שלך וה-challenge המקורי לפני שהוצפן עם המפתח הפרטי, הוא יוכל לוודא (בדומה לחתימה דיגיטלית) את מה שנשלח אליו מבלי שידע את המפתח הפרטי שלך. עם זאת, למנגנון יש חסרונות - העובדה שעל המכשיר ישב מפתח שאחראי על גזירת כל המפתחות האחרים לטובת ההזדהויות שלך, וכן שהמנגנון לא באמת פותח MITM או Replay attacks.

אם אתם חושבים לדוגמא שסריקת QR היא משהו שסביר להניח שלא יזכה לתפוצה רחבה, טעות בידכם. אם תתלו דף ברחוב בתור ניסוי, יש לכם טעות. מאמר שפורסם לפני כשנתיים מציג שמתוך 139 דפים שנתלו המכילים QR (בפורמטים שונים), כ-61% מתוכם נסרקו לפחות פעם אחת. הדף הכיל הפנייה לסקר ובו שאלות שונות לגבי הרגלי סריקת ה-QR של המשתמשים. ניתן לראות את התשובות בגרף בעמוד הבא.



מתוך הגרף ניתן לראות כי יותר מ-60% סרקו את ה-QR מתוך סקרנות, כאשר קיימים יותר מ-30% בסקר שאינם בודקים את ה-URL שאליו ה-QR מפנה.

הדפים שנתלו היו ב-4 פורמטים שונים:

1. QR בלבד.
2. QR עם הוראות טכניות.
3. QR עם הסברי לגבי הניסוי.
4. דפי תלישה אשר מכילים כתובת המקשרת לניסוי.

(a) *qrcode_only* (b) *qrcode_instructions* (c) *qrcode_SNS* (d) *ripoff_SNS*

ניתן לראות בבירור את ההתפלגות - ההעדפה ל- QR ברורה בקרב מכשירים סלולריים; עם זאת, הסיכוי שמשתמש יעבור תהליך מלא (במקרה הזה, יסיים למלא את הסקר) הולך וקטן ככל שמספקים פחות מידע בדף הפונה למשתמשים, כמו שניתן לראות בגרף בעמוד הבא.

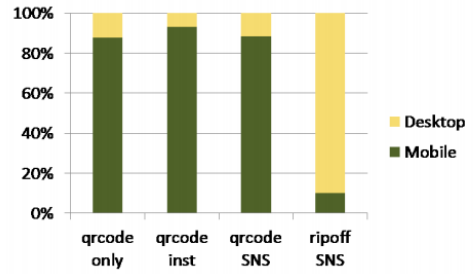


Figure 5. Mobile vs desktop users by condition.

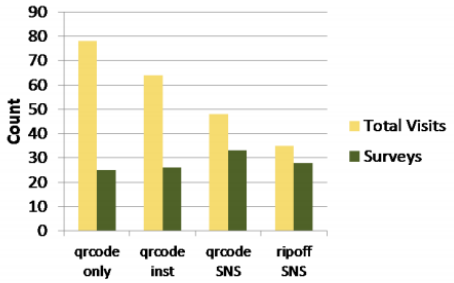


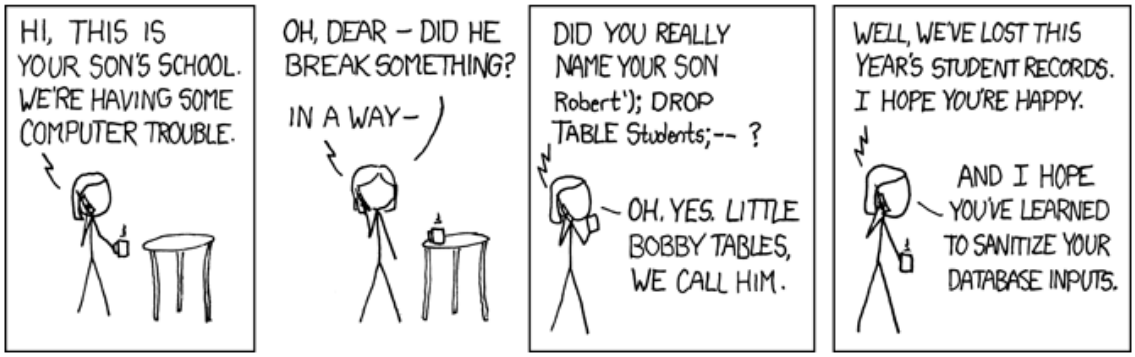
Figure 6. Visited URLs and Survey Completion by condition

עוד נתון מעניין היה שעל מנת לקבל תנועה אפקטיבית, סביר להניח שדווקא במקומות בהם אין למשתמשים מה לעשות, יש יותר סיכוי שינסו להפיג את השעמום באמצעות סריקת ה-QR.

סיכום

ניתן לראות כי למרות שעולם הברקודים הלך והשתכלל, עדיין מדובר ביעד אטרקטיבי לפורצים. אם בעבר היה מדובר בעיקר באבטחה פיזית (ברקודים של מוצרים), כיום מדובר על העולם הוירטואלי ואפשרות שבו ברקוד ישמש לתקיפה ולא רק להונאה או התגברות על בקרות אבטחה. כמו כן סוגי ההתקפות נהיו משוכללים וכוללים גם את ההתקפות הנפוצות ביותר (למי שמעוניין בקריאה מתקדמת יש מאמר הסוקר זאת).

נסיים בבדיחה מתוך XKCD, בתקווה שתזכרו תמיד לצפות לבלתי-צפוי:



הערה

מאמר זה נוצר בהשראה רבה לאחר ששמעתי את ההרצאה מתוך DefCon16 של Felix Lindner.