



משרד האוצר דוברות והסברה

כ"ד בניסן התש"ע
8 באפריל 2010
דב. 2010-656

לכבוד,

אסף שטול-טראורנינג
"הארץ"

הנדון: תגובות לכתבה של עיתון הארץ בנוגע לבחירות ממוחשבות

אסף שלום, מדובר בנושא מורכב ביותר. אנו מתייחסים כאן בפירוט לטענות השונות תוך ניסיון להסביר את הסוגיות המורכבות. במאמר עולות מספר טענות, נתייחס לכולן.

1. שיבוש באמצעות חסימה

הטענה היא שניתן לשבש מרחוק את התקשורת בין הכרטיסים לקוראי הכרטיסים המותקנים בעמדות ההצבעה. תקשורת זו נעשית באמצעות שדה אלקטרומגנטי המיוצר על ידי הקורא. שדה זה משמש הן לאספקת אנרגיה לכרטיס החכם (שאינו לו סוללה עצמאית) והן לתקשורת בין הכרטיס לקורא. לא נלאה אתכם בהסברים מורכבים אבל נאמר רק שהרכיב המשמעותי בתקשורת זו הוא הרכיב המגנטי ולא הרכיב החשמלי.

כדי לשבש תקשורת כזו נדרשים שלושה תנאים:

- א. עיקר האנרגיה בקרינה של החוסם היא מגנטית.
 - ב. אנטנת החוסם צריכה להיות במצב מרחבי מוגדר מול אנטנת הקורא. אם תנאי זה לא מתקיים נדרשת אנרגיה עצומה לצורך שיבוש התקשורת.
 - ג. גם במצב אידיאלי של האנטנה החוסמת מול הקורא נדרשת אנרגיה חזקה מאד כדי לשבש בפועל. שדה מגנטי נחלש במהירות רבה מאד כשהמרחק עולה (חזקה שלישית של המרחק).
- שיבוש כזה חזקה עליו שיתגלה מיד והוא משול לניסיון לשבש את הבחירות באמצעות הצתת הקלפי, כלומר הוא לא יוכל להיות חשאי כפי שעולה במרומז מהמאמר.

שבבים דומים מאד משמשים כיום לדרכונים אלקטרוניים, המונפקים כיום על ידי יותר ממאה מדינות. ארגון התעופה האזרחית הבינלאומי (ICAO) שהוא גוף התקינה לדרכונים ביצע ניסיונות של שיבוש קוראי RFID בשדות תעופה. הארגון הגיע למסקנה שזה איננו

מעשי. ראשית נדרש מרחק זעום בין החוסס לקורא כדי להצליח בשיבוש ושנית נדרשת אנרגיה עצומה.

2. הריסת כרטיסים מרחוק

ככל הידוע לנו החוקרים המכובדים לא טענו שהם ביצעו זאת בפועל, אלא נסמכו על פרסומים של האקרים גרמניים שטענו שהצליחו להשבית תגי RFID במרכולים בצורה כזו. כאשר מדובר על תגי RFID חשוב לזכור שלא מדובר בסוג יחיד. ניתן בהחלט להשבית תגים מסוימים, המשמשים לסימון מוצרים בעולם הקמעונאות, בצורה המתוארת במאמר. מאידך הכרטיסים עליהם מדובר הם משהו שונה לגמרי. כל כרטיס כזה עמיד בפולסים של אלפי וולטים באמצעות הגנות הבנויות לתוך חומרת השבב שבתוכו. כדי לגרום לפולס בעוצמה שתפגע בכרטיס לא די במכשיר פשוט כמו זה המתואר במאמר (מכשיר המבוסס על מבזק של מצלמה). גם כאן נדרשת האנטנה של אותו מכשיר להיות קרובה מאד לכרטיס ובמצב מרחבי מאד מסוים יחסית אליו, אחרת לא ניתן לבצע הריסה כזו. ההגנה של אותם שבבים נובעת מצורך פרקטי אחר לגמרי – הגנה מפני חשמל סטאטי. כולנו מכירים את התופעה של התחשמלות בעת נגיעה ברכב, במיוחד בימים יבשים. הצורך להחזיק את הכרטיס החכם ביד ולהכניסו לקורא מחייב לתכנן אותו מראש כנגד פריקה של חשמל סטאטי, ומכאן הצורך בהגנה. אם החוקרים המוזכרים במאמר אכן הצליחו לגרום להרס כרטיס מסוג דומה לזה שמשמש את מערכת הבחירות נשמח לדעת על כך ולקבל את כל הפרטים. אם לא בוצעה הדגמה כזו בפועל – ראוי לומר זאת בצורה מפורשת, למען היושר האינטלקטואלי.

3. relay attack ("חוט מאריד")

תקיפה זו מתבססת על ציוד שיכול לדמות כרטיס מצד אחד וקורא מצידו השני. הטענה היא שבאמצעות ציוד כזה ניתן לקשר בין כרטיס שכבר הוכנס לתיבת הקלפי ובין עמדות ההצבעה, ואז לשנות את ההצבעה הרשומה בו. לכאורה הדבר אפשרי אך בפועל המציאות היא שונה לגמרי. הגורם העיקרי המונע בצורה מוחלטת תקיפה כזו הוא תכונה שהוכנסה מראש למערכת. תכונה זו מונעת מכרטיס שכבר נרשמה עליו הצבעה לשנות את תוכנו לאחר שעזב את עמדת ההצבעה. תכונה זו כנראה לא הייתה מוכרת לחוקרים ולכן סברו בטעות שניתן לעשות תקיפה כזו. יתרה על כך, גם ללא תכונה זו אין זה מעשי לבצע תקיפה כזו. כאשר יש בתיבת הקלפי מספר כרטיסים לא ניתן לבדוד כרטיס מסוים ולתקשר רק איתו. למעשה לא ניתן לתקשר עם הכרטיסים כלל כאשר מספרם עולה על ארבעה.

כאן נכנס גורם נוסף למשוואה. בניגוד לשיבוש באמצעות חסימה כאן נדרשת תקשורת תקינה בין הכרטיס לקורא התוקף. כדי להפעיל כרטיס מטווח של 35 ס"מ נדרש הספק אדיר (לפחות כמה מאות וואטים), ובעיקר נדרשת אנטנה גדולה, הנמצאת במצב מקביל לכרטיס. קשה לדמיין מצב בו תוקף כלשהו יכול לבצע זאת במציאות.

4. paper trail ("עקבות נייר")

לגבי השימוש ב"עקבות נייר" התקיימו דיונים רבים במהלך פיתוח המערכת, הן דיונים פנימיים והן דיונים עם משרד המשפטים שהיה שותף מלא לתהליך. המסקנה החד משמעית מאותם דיונים הייתה שמדובר בהחלט בעיקרון יפה ברמה התיאורטית אך אין כרגע דרך מעשית לממש זאת, תוך התחשבות בכלל העקרונות המנחים את פיתוח המערכת, ובפרט בעיקרון חשאיות הבחירות. חשוב להדגיש שאיננו שוללים "עקבות נייר" אך אנו טוענים שמימוש סביר של "עקבות נייר" מחייב הקרבה של תחומים אחרים, כגון חשאיות. שילוב של "עקבות נייר" רק יוסיף עומס לוגיסטי לא סביר ויפתח פתח למניפולציות על מערכת ההצבעה. רק לצורך הדוגמה, אם יש מדפסת נייר רציף הרי שסדר ההדפסות מסגיר את מה שהצביע כל אזרח, ודי לרשום את סדר ההגעה של האזרחים לקלפי כדי לחסל לחלוטין את החשאיות. האמינות הנמוכה של המדפסות יוצרת גם את הצורך בתחזוקה. בהתאם לכך יש צורך בגישה של אנשי התחזוקה למדפסות במהלך יום הבחירות, דבר המעלה את הסיכון של תקיפת המערכת. הויכוח על הצורך ב"עקבות נייר" במערכות בחירות הוא ויכוח ישן, וקשה להסביר את הדעות השונות מבלי להיכנס לדיון ארוך מאד על מערכות כאלה. בדרך כלל מביאים כדוגמה את הבחירות בארה"ב אך חשוב לזכור שמדובר בבחירות אחרות לגמרי, שלא ניתן להקיש מהן לגבי הבחירות בישראל. בארה"ב בוחרים בעלי תפקידים רבים (שריף, שופטים, תובע מחוזי, מושל ועוד), ושם משמש הנייר המודפס כחלק מהליך הבחירה, ומחוסר ברירה. נזכיר גם שבמדינות אחרות (כדוגמת בלגיה והודו) משתמשים בבחירות ממוחשבות כבר זמן ממושך, וללא עקבות נייר. קוריוז מעניין: בבלגיה משתמשים בבחירות ממוחשבות כבר משנת 1991. ב-2003 שולב במערכת הממוחשבת של בלגיה מנגנון של "עקבות נייר" אך זה הוסר ב-2004 לאחר שהם הגיעו למסקנה שאיננו נחוץ ומייצר יותר בעיות מהתועלת שבו.

5. עלות המערכת

הרגישות לעלות המערכת הייתה אחד משיקולי התכנון העיקריים שלה. בשלבי הפיתוח נבחר אמנם כרטיס חכם יקר יחסית, אך כזה שיש לו גמישות רבה. כרטיס כזה טוב לתקופת הפיתוח, כאשר חוסר הודאות הוא גבוה. למערכת הסופית ניתן

להשתמש בכרטיס חכם זול מאד, שניתן למחזר אותו למערכות הבחירות שלאחר מכן, ללא תוספת עלות ובעיקר ללא סיכון של חשיפת ההצבעה הקודמת שבו. נושא זה נלקח כאמור בחשבון בעת הפיתוח וכל מנגנוני הצופן שנבחרו הם כאלה שלא יחייבו שימוש בכרטיסים חכמים יקרים, החל מאותו שלב שבו יש ודאות לגבי התכונות והתפקוד הנדרש מהכרטיסים.

6. האם יישום החוק מובטח לפרויקט ממשל זמין או שהוא צפוי לעמוד למכרז?

ממשל זמין, לפי בקשת משרד הפנים ובתיאום עם משרד המשפטים, הקים את הפתרון והיה מוכן להפעלת פיילוט בבחירות לרשויות המקומיות בתחילת שנת 2009. פיילוט זה, כזכור, לא התקיים עקב עיכובים בתהליכי החקיקה. בעקבות הפיילוט תוכנן תהליך ארוך ויסודי של הפקת לקחים. כחלק מתהליך הפקת הלקחים הייתה אמורה להיבחן שאלת ההפעלה, כולל האפשרות להפעיל את מערך הבחירות באמצעות זכיינים שייבחרו במכרז.