

11/4/2010

לכב' אסף שטול-טראורינג

"הארץ"

**הנדון: תגובת "ממשל זמין" לכתבה של עיתון הארץ בנוגע לבחירות ממוחשבות**

תגובות "ממשל זמין" למחקרנו חוזרות על הערות שקיבלנו מהם בעבר, ויש בהן אי דיוקים משמעותיים. להלן תגובותינו לטענות אחת לאחת:

1. **שיבוש באמצעות חסימה:** כבר ביצענו חסימה בפועל של תקשורת כרטיס-קורא ממרחק של כ-

2 מטר. אנחנו מבצעים עוד ניסויים והטווח עוד יגדל.

פירוט טכני של ההתקפה: בינתיים השתמשנו בהספק שידור של 1 וואט, עם אנטנה ניידת בקוטר 40 ס"מ עשויה מצינור נחושת של גז בישול. הספק זעיר שכזה אפשר לקבל גם מחיבור ה-USB של מחשב נייד. מודלים ממוחשבים מדויקים חוזים אפשרות לשיבוש גם ממרחק של 20-50 מטר עם אנטנה גדולה יותר והספק של וואטים בודדים (זמין ממצבר של רכב).

הסבר מדעי: הטיעון כי שיבוש חייב להיות מבוסס על שדה מגנטי חזק (ולכן יכול לפעול רק מטווח קצר ומצריך אנרגיה מרובה) – שגוי. שדה מגנטי חזק נחוץ רק כדי להפעיל את מעגלי הכרטיס – זה לא רלוונטי לצורך חסימה שפועלת כנגד הקורא. המשבש שלנו משדר אות רדיו (RF) בתדר של אונת הצד העליונה של איפנון ה-load modulation (14.4075MHz) וחוסם בזאת את מעגל הקליטה בקורא. תדרי רדיו כאלה בתחום הת"ג (תדר גבוה) משמשים גם חובבי רדיו וטווח השידור מגיע למאות או אלפי קילומטרים.

2. **"ICAO גוף התקינה לדרכונים ... הגיע למסקנה שזה איננו מעשי":** (א) ההתקפה מעשית

לגמרי ובוצעה בפועל – ראה 1. (ב) בכריכת דרכונים אמריקאיים משולב סיכוך חשמלי (סיבים מתכתיים) להגנה בפני התקפות, בין היתר בזכות מחקר קודם של קבוצתי. דרכונים אירופאיים ללא סיכוך הודגמו כחשופים מאד להתקפה בכנס USENIX האחרון.

3. **הריסת כרטיסים:**

(א) בהחלט בנינו זאפר ואף הרסנו באמצעותו כרטיס JCOP מהסוג המתוכנן לבחירות בישראל – והסרטנו את התהליך.

(ב) בימים הקרובים נעלה סרטון וידאו כחול-לבן המדגים איך אנחנו הורסים את הכרטיס.

(ג) הזאפר שלנו, וגם אלה של האקרים בעולם, עובד היטב נגד Contactless Smartcards ממשפחת ISO14443 (ולא נגד תגי UHF במרכולים כפי שנטען). ראה סרטון יוטיוב בלינק

המצורף.

4. **התקפת חוט מאריך:** "תכונה שהוכנסה מראש למערכת ... מונעת מכרטיס שכבר נרשמה עליו הצבעה לשנות את תוכנו":
- (א) חוק הבחירות ואיפיון המערכת מאפשר למצביע לשנות את הצבעתו מספר בלתי מוגבל של פעמים והמערכת אמורה לתמוך בכך.
- (ב) התכונה המדוברת לא מוזכרת במסמך האיפיון. לכן לא ברור מה היא בדיוק חוסמת ואיך היא בדיוק פועלת.
- (ג) היות והתכונה איננה במסמך האיפיון, לא ברור כלל אם היא תופיע במימוש הסופי של החברה הזכיינית.
- (ד) בהחלט יתכן שמנגנון הגנה שכזה, באם הוא אכן קיים, יכול לשמש בעצמו לשיבוש וחסימה (למשל ע"י התעיית המערכת לחשוב כי כבר נרשמה הצבעה)
- (ה) אם "תהילה" יעמידו לרשותנו אבטיפוס של מערכת הצבעה נוכל לנסות ולחוות דעה.
5. **התקפת חוט מאריך:** "כאשר יש בתיבת הקלפי מספר כרטיסים לא ניתן לבודד כרטיס מסוים ... כאשר מספרם עולה על ארבעה". זו כנראה מגבלה הנדסית של הציוד של תהיל"ה. מנגנון anticollision של תקן ISO1443-2 כן מאפשר לבודד כרטיס אחד, גם מתוך מאות – כלומר הכרטיסים יגיבו. ציוד חתרני שנבנה כדי לממש התקפת חוט מאריך לא יהיה כבול למגבלות ההנדסיות של ציוד הלגיטימי.
6. **התקפת חוט מאריך:** "כדי להפעיל כרטיס מטווח של 35 ס"מ נדרש הספק אדיר (לפחות כמה מאות וואטים)" – לא נכון. תלמידי אילן קירשנבאום בנה בציוד חובבים אנטנה, והפעיל כרטיס תקני מטווח של 25 ס"מ בהספק של וואט אחד. המערכת הופעלה ע"י סוללת 12 וולט של מערכת אזעקה ביתית. ראה קישור למאמר וקישור לצילומי האנטנה.
7. **עלות המערכת:** אין לנו מידע אמיתי לא על עלות הבחירות כיום (ב"טכנולוגיית" פתקים ומעטפות) וגם לא של המערכת המוצעת. אבל חשבון גס מאד שכולל את מחיר הכרטיסים (כ-\$10 לכרטיס) כפול כמה מיליוני בעלי זכות בחירה, עלות הציוד הקורא (נניה \$5000 לעמדת קלפי) כפול כמה אלפי קלפיות, בתוספת עלות הפיתוח ורווח לחברה הזכיינית, מצריך בקלות תקציב של חמישים עד מאה מליון דולר. הכסף הזה מחליף רק את עלות הפתקים והמעטפות – ולא את עלות התפעול של יום הבחירות. במאה מליון דולר אפשר לקנות פתקים להרבה מאד מערכות בחירות!

לינקים:

- סרטון ההריסה שלנו (כחול לבן), התקפת חוט מאריך, צילום אנטנת צינור הגז, ומכתבים לממשל האמריקאי שהשפיעו על תכנון הדרכונים האלקטרוניים:  
<http://www.eng.tau.ac.il/~yash/RFID>
- סרטון יוטיוב (גרמני) המדגים בנית זאפר ממצלמה חד פעמית והריסת כרטיסי Contactless Smartcard :  
<http://www.youtube.com/watch?v=c0vZigwn09I&NR=1>
- המאמר של קירשנבאום-וול How to build a low-cost, extended-range RFID skimmer :  
<http://www.eng.tau.ac.il/~yash/kw-usenix06/index.html>

בכבוד רב,

Avichai Wool

פרופ' אבישי וול