RFID Jamming and Attacks on Israeli e-Voting

Yossef Oren, Dvir Schirman, and Avishai Wool
{ yos@eng | dvirschi@post | yash@eng } .tau.ac.il
School of Electrical Engineering, Tel-Aviv University, Ramat Aviv 69978, ISRAEL

Abstract

The next generation of Israeli elections is proposed to run on an e-voting system which uses near-field RFID tags instead of plain paper ballots. In 2010 we investigated the system and identified several potential attacks which can be launched against the proposed system. In this work we report on the actual implementation of two of these attacks – zapping and jamming. These attacks have a critical effect on the security of the proposed system.

1 Introduction

The Interior Ministry of Israel is preparing to transition from a traditional paper ballot system to an e-voting system. During 2007 the scheme was passed through country-wide pilot testing in several municipal elections in Israel[16]. The system is also in the final stages of legal ratification[6]. The scheme is officially described in a patent claim recently granted to the Government of Israel by the World International Property Organization [17, 2], as well as by the public tender to contractors implementing the scheme[5] and by the Israeli law governing the election process[24]. The novelty of the system is that instead of using paper ballots, the votes in the proposed system are cast on contactless smartcards. To cast their votes, the voters use a computer terminal to write their choice into a contactless smartcard, and then physically deposit this smartcard into a ballot box. By encrypting the ballot as it is cast, the system aims to protect the privacy and authenticity of the votes, while still allowing the votes to be counted manually. The designers of the Israeli e-voting scheme chose near-field contactless readers instead of traditional smartcards for non-security-related reasons. First and most important is the issue of cost and reliability – since a contactless smartcard reader has no mechanical interface and no moving parts (in contrast to a traditional smart card or magnetic-stripe reader), it can survive many more repeated uses with a reduced opportunity for damage or deliberate vandalism. In addition, as observed in [7], contactless smartcards are easier to use than magnetic stripe cards or traditional smart cards since they work regardless of the way the card is oriented with respect to the reader. Cost saving is also reportedly the reason why the system has absolutely no paper trail – the designers wished to save on the cost of maintaining and supplying paper to thousands of printers on election day. The cards chosen for use in the Israeli scheme are Global Platform Java cards conforming to the ISO/IEC 14443[9] standard family.

In [19] we reported on a series of potential vulnerabilities of the proposed system. Some of these attacks were of the general category of relay attacks[11], which use a pair of specially-located transceivers to arbitrarily extend the interrogation range of RFID tags beyond their nominal range. Another set of attacks, which we focus on in this report, work on a more fundamental level and do not require a full relay system to be built. On the basis of these attacks we argued that the proposed e-voting system was insecure and unusable.

We made a preliminary version of our report available to the Israeli Government in early 2010. On April 8, 2010 the government issued a formal response to our report [15]. The Interior Ministry noted that our attacks were only theoretical in nature and could not succeed in practice, mostly due to the differences between the common RFID tags attacked by previous works in the field and the high-security cards used in the proposed system. In this work we dismiss this claim by reporting on the actual implementation of two of these attacks: zapping and jamming'. We report on the range at which the attacks are possible in practice – we successfully implemented a jamming attack from more than 2m away, using power that can be supplied by a car battery.

1.1 Description of the proposed Israeli e-voting system

The components of a voting station are illustrated in figure 1. Each voting station consists of a **voting and counting terminal** (a computer with a contactless smartcard reader), which the voter uses to cast his vote, a read-only **verification terminal** (another computer with a contactless smartcard reader), where the voter can optionally place his written ballot and make sure his vote was correctly cast, and a set of **blank ballots**, taking the form of secure contactless smart cards which are cryptographically paired with this specific instance of voting and verification terminals (see [19, ¶II.c]). The voting and counting terminals are located behind a cardboard divider to guarantee the privacy of the voting process. After casting his vote, the voter takes his cast ballot (written contactless smartcard) and physically deposits it into a **ballot box,** where all votes are held until

the end of the day. Many instances of this voting station will be set up on election day in public schools, government offices and so on.
At the end of the elections day, the local elections committee manually counts all votes found inside the ballot box by passing them one by one through the verification terminal. This hand-count forms the final result of the election. Preliminary results can also immediately be read from the voting terminal as soon as elections conclude, but these figures serve only for verification and do not determine the final results.

1.2 Security Features of the Scheme

The Israeli e-Voting Scheme was designed with a certain emphasis on security. The Global Platform Java cards used by the system conform to Common Criteria EAL 4+ [1] and are used in other high-security applications such as e-commerce and access control. The voting and verification terminals are cryptographically paired with the blank ballots used in each specific station, meaning that (at least as designed) a ballot cannot be read from or written to outside its specific voting terminal[1]. This means an attacker cannot steal a voting terminal from one voting station and use it to his advantage in another station. The voting terminals have no online connection either – the identity of the voter is only verified by using the population register terminal used by the voting committee and is not recorded on the ballots.
The redundancy in the vote counting process offers another degree of security, since the voting tallies which are written to the secure smart card inside the voting terminal must match the count of votes in the ballot box. Thus, an attacker would theoretically need to subvert both locations before compromising the election results.

1.3 Attacks on the proposed voting system

In [19] we described several attacks on the proposed system. If the attacker is in possession of a **relay device**[11], he can mount a **ballot sniffing attack** (which allows him to learn at any time which votes were already cast into the ballot box), a **single dissident attack** (which can undetectably suppress the votes or any amount of voters), and finally a **ballot stuffing attack** (which gives the adversary complete control over previously cast votes). If the attacker does not use a relay he can mount a **zapping attack** (which can quickly and easily disqualify an entire ballot box), a **jamming attack** (which can disrupt the operation of the voting station at a distance), or a **fault attack** (which can cause the voting station to enter an unpredictable state and thus disqualify it).
In the rest of this paper we report on actual implementations of two of the above attacks: the **zapping attack** and the **jamming attack**.

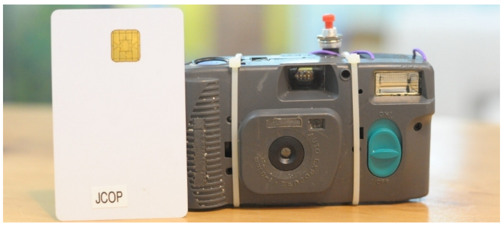

Figure 2 The Zapper, shown next to an Israeli e-voting card

2 RFID zapping

2.1 Description

RFID zapping is a well known attack, having previously been demonstrated in several places, including the 25th Chaos Computing Convention[21]. As stated in [22], the RFID zapper attack is built to attack the RF front-end of RFID tags. To carry out this attack, the adversary sends a short high-power pulse through an antenna placed next to the tag under attack. Because of the coupling between the zapper and tag antenna, this causes a high-power pulse to flow through the tag's antenna. This pulse causes the RF power harvesting system of the tag to be overwhelmed, permanently disabling the tag. This attack is particularly effective against passively-powered tags, since their only power source is the RF power harvester. The overall energy used in the attack is not very large if the high-power pulse is made short enough, allowing this attack to be carried out using inexpensive and portable components – one particularly common configuration is to reuse a disposable film camera, replacing the flash bulb with an appropriate antenna and pressing the camera shutter to activate the attack.

2.2 Attack setup

The attack setup is illustrated in Figure 2. For our attack we followed the recommendation of [22] and purchased a disposable film camera with built-in flash. The total price of the attack was 40 NIS (about 8 Euros) for 3 cameras. We removed the flash bulb and replaced it with a handmade PCB antenna, with the same size and geometry as the RFID tag under attack. The camera is powered by a single 1.5 battery, which is used to charge a 68 μF electrolytic capacitor to a voltage of approximately 250V. This battery can supply enough power for dozens of flash activations.
We used this zapper to attack a high-security ISO/IEC 14443[9] tag provided to us by a contractor of the Israeli Ministry of the Interior. To carry out the attack, we first verified that the tag works properly by placing it on a standard ACR122 NFC reader[12] connected to a PC. We then placed the tag next to the zapper and activated the zapper once. Next, we placed the zapper tag on the reader to verify that it cannot be read any more. A video demonstration of the attack can be found online[18].

[1] According to the proposed design, even the government's "master key" is incapable of rewriting a ballot. It can only format the contactless smart card to a blank state

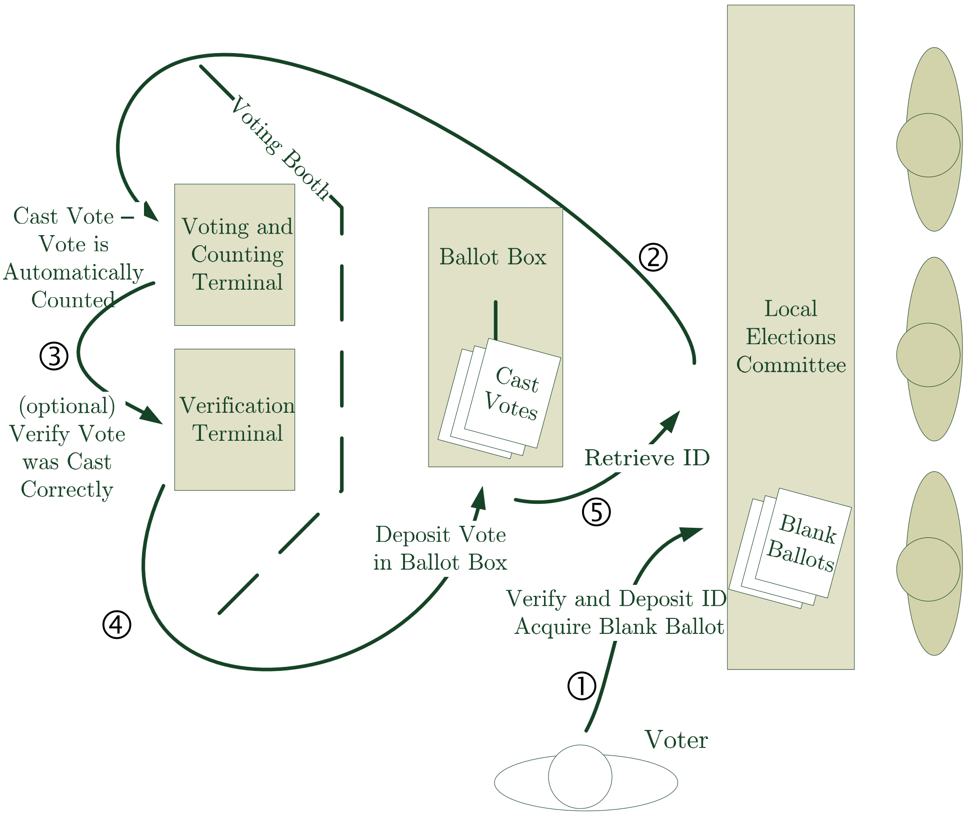
Voting Booth
Cast Vote – Vote is Automatically Counted
Voting and Counting Terminal
③
(optional) Verify Vote was Cast Correctly
Verification Terminal
④
Ballot Box
Cast Votes
②
Local Elections Committee
Retrieve ID
⑤
Deposit Vote in Ballot Box
Verify and Deposit ID Acquire Blank Ballot
Blank Ballots
①
Voter

Figure 1 The proposed Israeli e-voting scheme in action. Illustrated from left to right are the voting booth, the cast ballot box and the local election committee's desk area. The arrows show the path followed by a voter through the three areas of the voting station.

2.3 Results and Discussion

As our video demonstration shows, the zapper attack was completely capable of disabling the high-security tag in the proposed system. Evidently, the increased ESD protection and other countermeasures which exist in the high-cost EAL 4+ cards used in the system was not sufficient to prevent the zapping attack from being carried out. We note that it is quite simple to build zappers which are even more powerful than the one we constructed, for example by replacing the camera's built-in capacitor with a higher-capacity element.

3 RFID jamming

3.1 Description

An adversary who wishes to disturb the normal course of the elections in a certain ballot station can synthesize a jamming signal, thus preventing the RFID reader from communicating with the tag and recording the votes. The signal can be transmitted from outside the room, and can be turned on and off at the adversary demand. This way the attacker can create a denial of service attack at will, depending on the people currently entering to vote.

In order to block the communication between the reader and the tag there is a need to transmit a signal which mimics the load modulation of a tag, thus preventing the reader from receiving the tag's reflected signal. In [10] and [20] the authors implemented RFID blockers by building an active tag emulator which transmitted a fake UID in order to interfere with the anti-collision algorithm of ISO14443. We suggest a more straightforward method of transmitting a powerful signal on the sub-carrier used for the tag load modulation.

An ISO14443 tag transmits its response using load modulation on a sub-carrier of the reader's carrier signal (13.56 MHz). The sub-carrier frequency $\frac{f_c}{16}$ = 848 kHz produces side bands at 12.712 MHz and 14.408 MHz. The two sidebands function both as carriers for the tag's data, and are basically the same. According to [4] a typical ISO14443 compliant reader evaluates only the upper side band. Therefore, in order to block the signal from the tag it suffices to transmit a powerful signal on the upper side band (14.408 MHz).

Blocking of the signal can be performed either by transmitting a powerful carrier signal that will interfere with the the legitimate tag's signal at the receiver, or by transmitting a modulated signal similar to ISO14443 load modulation. In the first step of our research we examined the performance of each of these methods.

In [4] Finkenzeller et al, demonstrate an extension of RFID transmission range by using an active load modulation, and a large loop antenna. As mentioned above, in order to block the tag's signal we need to produce a modulated signal on the upper side band, hence, the challenge of jamming is similar to range extension using active load modulation. However in the case of jamming there is no concern about bit errors – which should allow the jamming range to be higher than the communication range.

3.2 Using a monopole antenna

As part of the attack we investigated the possibility of transmitting the jamming signal using an HF monopole antenna rather than a loop antenna. RFID communication is based on magnetic coupling between two loop antennas. As explained in [4] an effort to increase the range of an active transmitting signal requires either increasing the current injected to the antenna, or increasing the area of the loop. An alternative approach is to use the field generated by an HF monopole antenna. Monopole antennas are designed for the electric field, or plane wave, transmission rather than magnetic coupling. However, the antenna still produces a magnetic field in the near field region. Moreover, there may be a coupling between the electric field produced by the monopole antenna to the reader's circuit, which will also contribute to the jamming.

There are a few advantages of using a monopole antenna for this attack. First, since it usually looks like a simple pole it is easier to hide. Second, there is a variety of commercial antennas in the radio amateurs market which are designed for the desired frequency range. And third, we hypothesize that the jamming range will be longer, and the power consumption will be reduced in comparison to the loop antenna.

According to [23] the magnetic field at the near-field region around a monopole antenna (assuming an infinitely thin wire) as derived from Stratton [25] is given by:

$$H_{\phi}\left(\rho, z\right) =$$

$$\frac{jI_0}{4\pi \cdot \rho \cdot sin\left(kh\right)}[e^{-jkr_0} - cos(kh) \cdot e^{-jkr} - \frac{jz}{r} \cdot sin(kh) \cdot e^{-jkr}]$$

where ρ is the distance from the antenna, k is the wave number given by $k = \frac{2\pi}{\lambda}$, z is th height above ground, h is the length of th antenna, and:

$$r = \sqrt{\rho^2 + h^2}$$

$$r_0 = \sqrt{\rho^2 + (z - h)^2}$$

We compare the predictions for the magnetic field produced by a $\lambda/4$ monopole antenna, with the predictions of the magnetic field produced by a 39 cm loop antenna. According to [4] the magnetic field produced by a loop antenna is given by:

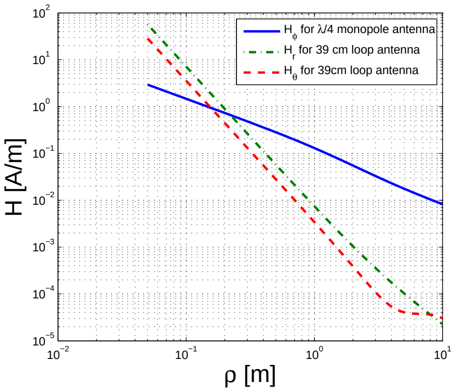

Figure 3 Magnetic field of a $\lambda\backslash 4$ monopole, and a 39 cm loop antenna, for a current of 1A as a function of the distance from the antenna.

$$H_{\rho}\left(\rho, \theta\right) = \frac{jka^2 I_0 cos\theta}{2\rho^2}\left(1 + \frac{1}{jk\rho}\right)e^{-jk\rho} \qquad (1)$$

$$H_{\theta}\left(\rho, \theta\right) = -\frac{\left(ka\right)^2 I_0 sin\theta}{4\rho}\left(1 + \frac{1}{jk\rho} - \frac{1}{\left(k\rho\right)^2}\right)e^{-jk\rho} \qquad (2)$$

Figure 3 presents the magnetic field as a function of distance from the antenna for: (a) An ideal monopole antenna ($h = \frac{\lambda}{4} \approx 5m$) applied with $I_0 = 1A$ measured at a height of $z = \frac{h}{4} \approx 1.3m$. (b, c) A magnetic loop antenna with a diameter of 39 cm and $I_0 = 1A$ (both H_r and H_θ) [26, §5-3]. We note that for $\rho > 20cm$ the field produced by the monopole antenna exceeds the field produced by the loop antenna. Based on the above, we predict that using an HF vertical antenna will result in a better jamming range.

4 Experiments

4.1 Jamming technique

Before checking the jamming distance we wanted to choose the preferred jamming technique. We examined two techniques: (a) Transmitting a continuous wave at the upper sub-carrier frequency of 14.408 MHz that would interfere with the legitimate load modulation signal at the reader's receiver. (b) Producing a clock signal at 212 kHz, which is the bandwidth of the Manchester coded bit stream the tag transmits (according to ISO14443a [9]), and modulating it using ASK modulation on the upper sub-carrier frequency. We compared between the two techniques in the lab, measuring the jamming distance achieved using a 39 cm copper tube loop antenna. For the second technique, the 212 kHz clock signal was produced by a pattern generator (Agilent 81110a).

Figure 4 presents the jamming range achieved for each of the techniques for different input powers. One can notice that there is hardly any difference between the performance of the two techniques. Therefore, the attack setup

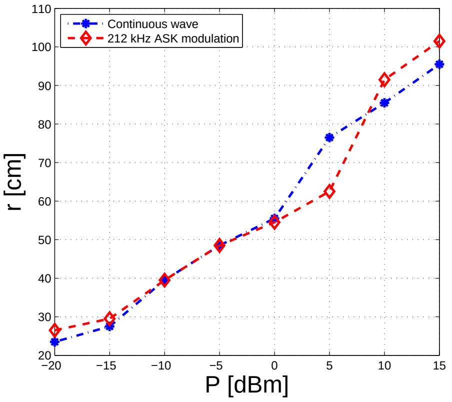

Figure 4 Comparing the two jamming techniques, as a function of transmitted power.

described next uses the first technique only, since it requires less equipment from the attacker.

4.2 Attack setup

The setup for the jamming attack includes a RF signal source, an amplifier, and an antenna. As mentioned above, the ideal monopole antenna for the desired frequency is over 5m long, and requires a large metal surface for a ground plane. This antenna is undesirable in the attack setup, which should be mobile, and look innocent to the average eye. Therefore, for our attack setup we used two kinds of mobile HF antenna which are about 1.5m long. In these antennas the lack of height, which results in a capacitive load, is compensated by a large coil.

We examined two kinds of antennas: (a) A radio amateur's antenna. (b) A military broadband helically wound antenna. According to [26, §6-37] a helically wound antenna with a height of $\lambda/20$ is similar in performance to a $\lambda/4$ monopole.

Figure 5 illustrates the setup we used for the jamming attack. The setup includes the following equipment:

- RF Signal Generator - to produce the 14.408 MHz sub-carrier signal. We used an Agilent E4438C[27].
- Power Supply - In our experiment we used a lab power supply. The power consumption from the power supply was at most 15W, thus an attacker can also use a car's battery.
- Amplifier - In our experiment we used a Mini-Circuits ZHL-32A[13] amplifier.
- Antenna - We examined two mobile HF antenna (both of them about 1.5m long):
  - (a) New-Tronics Hustler: MO-4 (mast) + RM-20-S (resonator), which is designed for the 14–14.35MHz ham radio band. – estimated cost: $125 [14] (See [26, §6-29]
  - (b) Broadband vertical helically wound antenna: NVIS-HF1-BC – estimated cost: $1500 (See Figure 6 and [26, §6-37])

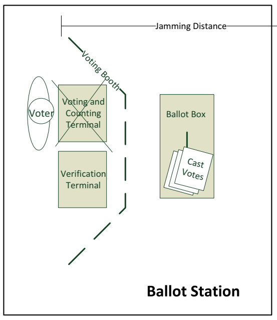

Figure 5 Jamming attack setup

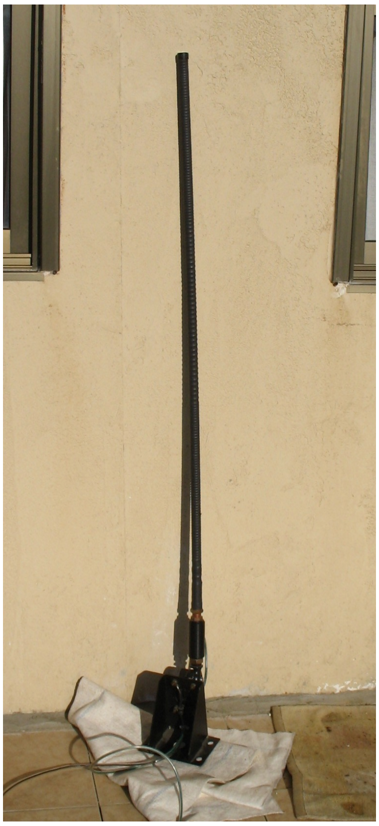

Figure 6 NVIS-HF1-BC antenna. The antenna height is 1.5m.

The jamming signal was produced by the RF generator with an output power of 15 dBm, then amplified by 25 dB using the amplifier, and transmitted through the antenna. Note that for a smaller and more mobile setup the adversary can use a 14.408 oscillator and a pre-amp instead of the RF generator, and he can supply power for all the setup from a car battery instead of the power grid.

4.2.1 Coupling effects

During our initial expirements we observed a surprisingly long jamming range of about 10m using the helical antenna. Although we carefully sepertated the reader from our jamming setup, we later noticed, thanks to an observation by K.Finkenzeller [3], that the coax cable connecting the amplifier and the antenna was passing close to the reader. As observed by [28], cables, power wires, and even wall framings act as very good antenna relays at HF frequencies. Therefore, the surprisingly long distance was a result of the coupling from the coax cable.

4.3 Results and Discussion

The maximum jamming range was measured for the two mobile HF antenna, and a 39 cm copper tube loop antenna. Jamming was identified using a ISO14443A compliant tag placed next to TI MF S4100 Reader [8]. Using TI's demo software the computer beeps every time a tag is recognized. When placing a tag on top of the reader frequent beeps are heard (about 5-10 beeps per second). We distinguish between two jamming types: full jamming is defined when no beep is heard from the reader for 10 seconds, while partial jamming is defined when 1-2 beeps per second are heard, but still significantly less beeps than with no jamming signal at all.

The maximum jamming ranges for each jamming type, and each antenna are summarized in Table 1. We notice that using the helically wound antenna we achieve a significant improvement over the loop antenna.

In addition, we wanted to check the effect of the distance between the tag and the reader on the jamming distance. Therfore, we repeated the expirement with the helical antenna, this time with the tag seperated from the reader by 3 cm producing about 20 beeps per minute. In this setup we managed to get an improvement of 30 cm, producing a jamming distance of 2.3 m.

The jamming attack described above can be easily mounted on a car by replacing the RF signal generator with a circuit containing oscillator and a pre-amp. Since in our setup the generator produced a signal with only 15 dBm $\approx$30 mW, this circuit can be powered by a battery. Most of the power demands of setup comes from the amplifier which in our experiment consumed a current of about 0.5 A, at a voltage of 24 V. Thus, the power consumed by the entire setup is about 12 W, an amount which can be supplied from a regular car battery.

Antenna	Full jamming range [m]	Partial jamming range [m]
39 cm loop	0.95	1.25
Hustler	1.1	1.65
Helical	2	2.3

Table 1 Jamming distance using different antennas

4.4 Future Work

For better results the HF antennas should be placed over a large ground plane. Our experiments were conducted with a 50x30 cm metal plate we had available in the lab as a ground plane.

Furthermore, our amplifier could produce power up to 10 W, using a small HF power amplifier (a variety of these are available in the radio amateurs' market. Increasing the transmission power this way will increase the jamming distance while maintaining the ability to mount the setup on a car, and using the car battery for power supply.

5 Discussion

In this work we reported on the physical implementation of two proposed attacks on the Israeli e-Voting System – the zapping attack and the jamming attack. We showed that even high-cost EAL 4+ smart cards are vulnerable to these attacks, and not only the low-cost cards tested in previous works. It is no longer possible to dismiss these attacks as existing only in the realm of theory.

Our results indicate that using a mobile HF antenna and some affordable RF equipment that can be easily mounted on a car, one can block the communication of a RFID reader from a distance of few meters. This effectively means that the attacker can place his setup right outside the wall of the ballot station's room and still be able to prevent the voting terminal from working at his command.

The jamming attack is a selective denial of service attack, since it is easy to apply selectively only to a certain subset of voters at the discretion of the attacker. Thus, the attacker can consult any apriori information he has on a voter entering the voter booth (i.e. age, skin color, etc) to decide "on the fly" whether or not to disallow voting for this particular voter. The attack is very difficult to prevent, unless electromagnetic shielding is applied to the walls, doors and windows of every voting station (and not just the ballot box itself) – a very difficult undertaking.

6 References

[1] Common Criteria Recognition Agreement. Common criteria for information technology security evaluation part 2: Security functional components. Online, July 2009.

[2] Boaz Dolev. Laying the groundwork for electronic elections in Israel (in Hebrew). Invited Talk, CPIIS IDC/TAU Workshop on Electronic Voting, May 2009.

[3] Klaus Finkenzeller. Personal communication.

[4] Klaus Finkenzeller, Florian Pfeiffer, and Erwin Biebl. Range Extension of an ISO / IEC 14443 type A RFID System with Actively Emulating Load Modulation. In *7th European Workshop on Smart Objects: Systems, Technologies and Applications (RFID SysTech)*, May 2011.

[5] Government of Israel, Ministry of the Interior. Public tender 16-2008 for the establishment and operation of a computerized election system, August 2008.

[6] Government of Israel, Prime Minister's Office. Decisions of the ministerial committee on legislation (in hebrew). Online, August 2009. http://www.pmo.gov.il/PMO/vadot/hakika/2008-2012/08-2009/des663.htm.

[7] Gerhard P. Hancke, Keith Mayes, and Konstantinos Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers & Security*, 28(7):615–627, 2009.

[8] Texas Instruments. Multi function reader series 4000. Online, March 2005. http://www.ti.com/rfid/docs/manuals/pdfSpecs/RF-MFR-RNLK-00.pdf.

[9] International Organization for Standardization, Geneva. *ISO/IEC 14443-2 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface*, 2001.

[10] Ari Juels, Ronald L. Rivest, and Michael Szydlo. The blocker tag: selective blocking of RFID tags for consumer privacy. In *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, pages 103–111. ACM Press, 2003.

[11] Ziv Kfir and Avishai Wool. Picking virtual pockets using relay attacks on contactless smartcards. In *International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pages 47–58, Los Alamitos, CA, USA, 2005. IEEE Computer Society.

[12] Advanced Card Systems Ltd. ACR122U NFC contactless smart card reader. Online, August 2008. http://www.acs.com.hk/index.php?pid=product&prod_sections=0&id=ACR122U.

[13] Mini-Circuits. ZHL-32A coaxial amplifier. Online, August 2009. http://www.minicircuits.com/pdfs/ZHL-32A.pdf.

[14] New-Tronics. mobile HF hustler antenna. Online, October 2008. http://www.new-tronics.com/main/html/mobile__hf.html.

[15] Ministry of Finance Spokesman Unit. Comments on the Haaretz article about computerized elections (in Hebrew). Online, April 2010. http://www.eng.tau.ac.il/~yash/RFID/tehila-response.pdf.

[16] Ministry of the Interior Spokesman Unit. Pilot of computerized elections for regional councils (in hebrew). Online, November 2007. http://www.israel.gov.il/FirstGov/Templates/NewsItem.aspx?NRNODEGUID={6CA2D671-1427-46A1-91D7-9C8957E733EB}.

[17] Yoram Abraham Oren, Pinchas Rosenblum, Ofer Margoninsky, Ilan Yom-Tov, and Boaz Dolev. (wo/2010/010564) electronic voting system. Online, January 2010. http://www.wipo.int/patentscope/search/en/WO2010010564.

[18] Yossef Oren and Avishai Wool. Israeli e-voting RFID card zapper. Online, April 11 2010. http://youtu.be/wxd3-YodOmM.

[19] Yossef Oren and Avishai Wool. RFID-Based electronic voting: What could possibly go wrong? In *International IEEE Conference on RFID*, pages 118–125, Orlando, USA, 4 2010.

[20] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. Keep on blockin' in the free world: personal access control for low-cost RFID tags. In *Proceedings of the 13th international conference on Security protocols*, pages 51–59, Berlin, Heidelberg, 2007. Springer-Verlag.

[21] Tilman Runge. 22nd chaos communication congress lightning talks, day 1. Online, December 2005. youtu.be/uXEJ1_I49MQ#t=18m58s.

[22] Tilman Runge. Schriftliche arbeit jugend forscht: Der RFID-Zapper (in German). Online, February 2007. http://rfidzapper.dyndns.org/RFID-ZAPPER.pdf.

[23] Omer Al Saraereh, Abdul Karem, A Al Sbeeh, Ahmad H Zaid, and Ibrahim M Hruob. Monopole Antenna. *Computer Engineering*, pages 2–29, 2007.

[24] Meir Shitrit. Local authorities bill (elections) (amendment - election systems) (in hebrew). Online, May 2009. http://www.knesset.gov.il/privatelaw/data/18/1180.rtf.

[25] J.A. Stratton. *Electromagnetic theory*, volume 33. Wiley-IEEE Press, 2007.

[26] R.D. Straw. *The ARRL antenna book: The Ultimate Reference for Amateur Radio Antennas*. Amer Radio Relay League, 2003.

[27] Agilent Technologies. E4438C ESG vector signal generator. Online, May 2008. http://www.home.agilent.com/agilent/product.jspx?nid=-536902340.536880956.

[28] P.H. Thevenon, O. Savry, S. Tedjini, and R. Malherbi-Martins. Attacks on the HF physical layer of contactless and RFID systems. In Cornel Turcu, editor, *Current Trends and Challenges in RFID*, chapter 21. InTech, July 2011.

About the authors

Yossef Oren received a B.Sc. (Cum Laude) in Communications Systems Engineering from Ben-Gurion University in the Negev, Beer-Sheva, Israel, in 2003. He received an M.Sc. in Computer Science from the Weizmann Institute of Science, Rehovot, Israel in 2006. He is currently studying towards his Ph.D. at the School of Electrical Engineering at Tel-Aviv university, Tel-Aviv, Israel. His research interests include power analysis attacks and countermeasures, low-resource cryptographic constructions for lightweight computers, and cryptography in the real world.

Dvir Schirman received a B.A. in Physics and a B.Sc. in Electrical Engineering from the Israel Institute of Technology, Haifa, Israel, in 2006. He is currently studying towards his M.Sc. at the School of Electrical Engineering at Tel-Aviv university, Tel-Aviv, Israel. His main research area is information security in RFID.

Avishai Wool received a B.Sc. (Cum Laude) in Mathematics and Computer Science from Tel Aviv University, Israel, in 1989. He received an M.Sc. and Ph.D. in Computer Science from the Weizmann Institute of Science, Israel, in 1993 and 1997, respectively. He then spent four years as a Member of Technical Staff at Bell Laboratories, Murray Hill, NJ, USA. In 2000 he co-founded AlgoSec Systems (formerly Lumeta), a network security company. He is currently an Associate Professor at the School of Electrical Engineering, Tel Aviv University, where he has been since 2002.

Prof. Wool is the creator of the AlgoSec Firewall Analyzer. He has served on the program committees of the leading IEEE and ACM conferences on computer and network security. He is a senior member of IEEE, and a member the ACM and USENIX. His research interests include firewall technology, computer, network, and wireless security, smartcard and RFID systems, and side-channel cryptanalysis.