Side-channels and eVoting machine security

Identifying vulnerabilities and defining requirements

Richard Frankland, Denise Demirel, Jurlind Budurushi, Melanie Volkamer
TU Darmstadt/CASED
Mornewegstraße 32
64293 Darmstadt, Germany
{richard.frankland, denise.demirel, jurlind.budurushi, melanie.volkamer}@cased.de

***Abstract*—Election systems making use of eVoting machines are becoming more prevalent. However, security issues do exist within current products and proposed systems. One of these issues is the occurrence of implementation-specific information leakage, otherwise known as side-channel leakage. These have serious implications for voter secrecy. An attack based on electromagnetic leakage from Nedap voting machines has demonstrated that this type of leakage is a relevant issue within eVoting. Therefore, in this paper we present an analysis showing how common components of eVoting machines may be vulnerable to side-channel attacks. As side-channel leakage is also not sufficiently addressed in the many available requirement documents for eVoting systems, we also define requirements for side-channels within the scope of eVoting machine security. Our proposal involves the application of the Common Criteria method. These requirements can be integrated into existing or future Protection Profiles and Security Targets for eVoting systems.**

***Index Terms*—electronic voting; security requirements; vote secrecy**

I. Introduction

The use of eVoting machines for legally binding elections has been increasing worldwide, with eVoting machines currently in use in many countries such as Russia, Venezuela, Brazil, and the US. Their purpose is to enhance the speed and accuracy at which votes are counted and also to facilitate the voting process for users. However, many questions have been raised over security issues with the use of eVoting machines, with some common makes and models having been criticised and withdrawn from use, for instance in the Netherlands, Germany, Ireland and some parts of the US.

One interesting security issue with eVoting machines has been the exploitation of electromagnetic emanations from the machine itself. This was demonstrated against Nedap and SDU Direct Recording Electronic (DRE) voting machines in the Netherlands [1], where signals caused by the machine display would allow an attacker to determine if a specific party was voted for, just by using basic radio receiver equipment.

The attack exploited an implementation-specific type of information leakage, or "side-channel", occurring during operation of the eVoting machine. The goal of these types of attacks is to break voter confidentiality, which has the effect of disrupting a fundamental right of voters; the right to a secret vote. By breaking secrecy of the vote, attackers can coerce voters, damaging the democratic process.

However, vulnerabilities which allow these attacks to take place are not taken into account in most design or evaluation stages of eVoting machines. This is no surprise since they are hardly addressed in requirements documents for eVoting. Although general security requirements for eVoting have been defined, for example in the Council of Europe Recommendations [2], which state that the eVoting system shall maintain individual privacy, these have essentially been blanket recommendations, and do not possess the necessary detail for the consideration of side-channel vulnerabilities.

The goal of this paper is to demonstrate the relevance of side-channel leakage for eVoting systems, concentrating on security vulnerabilities of polling station eVoting machines, and to make recommendations for the mitigation of security issues that would lead to vote confidentiality being compromised. Such systems represent a special use-case and link to passive plaintext information leakage, taking place during normal machine operation, through the fact that human-system interaction must be conducted in the clear, and using technologies that make vote selection as accessible as possible. By taking common forms of eVoting machines and finding ways that published side-channel attacks can be applied to them, we highlight the possible existence of serious vulnerabilities that need to be taken into account for the development and implementation of secure eVoting systems. We also make recommendations for the definition of security requirements and the evaluation of eVoting machines so that their security might be held to an open, accessible standard. Our main recommendation takes the form of following the Common Criteria methodology for defining requirements within the scope of assumptions, threats and objectives, and then matching these to predefined Security Functional Requirements. In this paper this is achieved by demonstrating how information on practical side-channel attacks can be taken from the available literature and used to formulate requirements with an example outlining a Security Functional Requirement for machine display leakage and attacker distance within a controlled environment. Such a requirement could form part of a Protection Profile or Security Target for an eVoting machine, and satisfy our requirement for openness and accessibility.

In Section II, previous publications addressing the issue of side-channels in eVoting will be discussed in relation to our own contribution with this paper. In Section III, a short overview of the development of side-channel cryptanalysis

This work has been published in the International Workshop on Requirements Engineering for Electronic Voting Systems (REVOTE), 2011. ISBN 978-1-4577-0951-7 DOI: http://dx.doi.org/10.1109/REVOTE.2011.6045914

will be given, going through the principles of attacks. After this, a highly relevant class of side-channel will be discussed; compromising emanations, which take the form of plaintext information leakage. In Section IV the relevance of these different types of side-channel attacks to different types of eVoting systems will be covered. In Section V, we will provide an overview of the requirements for a successful attack exploiting compromising emanations and examine countermeasures. In Section VI, we will outline how security requirements addressing side-channel vulnerabilities can be semi-formally defined through the use of the Common Criteria methodology, presenting an example requirement using the same methodology. Finally, in Section VII, our contributions will be summarised and suggestions for future work will be given.

II. Related work

In this section we discuss related work both regarding existing requirement documents as well as regarding previously performed side-channel evaluations of existing eVoting systems.

A. Requirement documents

The Voluntary Voting System Guidelines - Volume 1 [3], designed to act as a best practice guide for the design and implementation of eVoting systems after the Help America Vote Act, makes some small mention, in Section 3.2.3.1, of information leakage from headphones that are too loud, which are used to relay sight-disabled voters' choices back to them. Also mentioned, in Section 4.1.2.9, is the requirement for machines not to give out electromagnetic emanations, in accordance with the FCC's Rules and Regulations; Part 15, for Class B devices. However, this was primarily designed to prevent electronic devices from giving out electromagnetic interference that might disturb other electronic equipment, or interfere with the correct operation of the device itself, and does not take into account the possibility of the signals containing leaked information. Note, this type of requirement is also mentioned in other requirement catalogues like in [4]. While the second section, 4.1.2.9, does not address side-channels that might break the secrecy of the vote, the first section, 3.2.3.1, does and will be taken into account when identifying potential sources of information leakage.

There has also been a general mention of side-channel resistance in security requirements for eVoting machines [5], which defines a threat to eVoting machine secrecy during the vote casting stage as an "intruder in or close by the polling station sees, hears or measures information provided by the voting process in order to compromise secrecy of the vote". The corresponding security objective requires that the eVoting machine shall not leak any information about the voting process, apart from that needed for other necessary functions, and that the eVoting machine "shall prevent any emissions which might endanger the secrecy of the vote", including acoustic and radio emissions, and power analysis. While the author provides some examples, this list is not complete nor very detailed regarding which components of the eVoting system might cause the emission.

B. Side-channel evaluations of eVoting systems

Emission tests of the Digital Voting Pen, proposed for use in the Hamburg city elections, has been executed by Cambridge University [6]. The test found that while some signals were emitted, one of these being characteristic of a video signal, no distinct information-bearing signal could be found. The author mentions in his report that the emissions test was not conclusive and that within 30 centimetres there is the potential for a compromising emanation to be found. This shows that distance is a relevant parameter when defining security requirements, which will be taken into account in our considerations. While the analysis of the Digital Voting Pen only looked at the pen itself, not taking into account other aspects of its implementation, such as being used with the docking station and connected via USB connection to a PC, both aspects of how it was actually used, we recommend in our requirement definition to take any component of an eVoting system into account.

The Nedap voting machines previously used in Germany underwent an emissions test carried out by the Physikalisch-Technische Bundesanstalt (PTB) [7]. The authors of this paper mention that besides distance being a factor, the quality of the equipment and environmental factors (e.g. radiation and reflection free test environments which might not be realistic in polling stations) are also important. Furthermore, the fact that the PTB executed their test again after the problems in the Netherlands were published leads to the question of how often these tests need to be repeated. An example of one of these aspects, distance, will be taken into account in Section VI where we define requirements. The other factors can be considered as important future work.

III. Side-channels

The term "side-channel" refers to an implementation-specific form of information leakage, usually from an implementation of a cryptographic algorithm, in a manner not considered in the data flow model of the implementation [8]. This leakage can allow the determination of the secret key and reconstruction of plaintext data. It is important to note that a successful side-channel attack does not equate to a successful break of the cryptographic algorithm, only demonstrating that the method of implementation, which can be in software or hardware, is not secure.

A. Side-channel cryptanalysis

There are three primary types of side-channel cryptanalysis: timing analysis, power analysis and electromagnetic analysis, which will be introduced in the following three subsections.

1) Timing analysis: Timing analysis first came into prominence with Kocher's work on public key algorithms that relied on modular exponentiation [9]. The general attack relies on the ability of an attacker to eavesdrop on the known cryptographic protocol and collect time measurements of exponent

operations on several known plaintexts, the exponent being the secret key. Individual bits of this secret key can be guessed with high probability through comparison of time variations that arise due to differences in the speed of modular exponentiation calculations.

Symmetric algorithms have also been the target of timing attacks, focussing on discrepancies in time taken for specific operations. Bad implementations of AES have been shown to be vulnerable to timing attacks, where certain operations do not run in constant time, and also across networks in certain versions of OpenSSL, where key bits were found to be recoverable over the network itself using timing information from the computer performing the encryption operations.

2) Power analysis: Power analysis attacks evolved from the work done on timing attacks, with a greater emphasis on attacking hardware implementations, especially smart cards. Differences in power consumption during encryption operations, measured over time using power probes in conjunction with oscilloscopes, are utilised to determine information about the secret key [10].

Two main types of power analysis have been developed; SPA, simple power analysis, and DPA, differential power analysis. SPA of DES, for instance, produces a power trace that can elucidate the information about a single encryption operation, while DPA of DES can make use of multiple traces to determine individual key bits by multiple guesses. Implementations of AES have also been successfully attacked.

3) Electromagnetic analysis: Electromagnetic analysis of cryptographic implementations derives from the techniques used in power analysis attacks, with SEMA, simple electromagnetic analysis, and DEMA, differential electromagnetic analysis, existing as electromagnetic counterparts to the different types of power analysis. The main difference between electromagnetic analysis and power analysis is that in an electromagnetic attack power consumption is measured through the detection of electromagnetic currents caused by electric activity in the target device over time. Such an attack has been demonstrated against implementations of DES and RSA in smart cards [11].

B. Compromising emanations

There is one ubiquitous aspect of cryptographic implementations providing confidentiality between two users; the data being protected must at some point be human readable. Whether it is at the input stage, or when the plaintext is presented on a computer display or some other readable format, sensitive data is vulnerable to eavesdropping before the encryption process and after the decryption process. In effect, attacks focussing on recovering this information are circumventing the protection offered by any cryptography in place.

Here, surveillance style attacks can be directed against common methods of data input and display. By targeting devices such as computer keyboards and monitors it is possible for an attacker to recover information through remote, passive, observation. The most obvious way of doing so would be by visual monitoring, performed by an attacker and standard optical or imaging equipment, such as a telescope or a camera. However, by investigating and exploiting device-specific information leakage, there are other ways to recover sensitive data.

The source of this leakage must come from what can be considered ”side-channel” information, which is given out by the target device. This information can be thought of as a ”compromising emanation”. These emanations can take the form of any distinct signal containing leaked information from a device, but in academic literature three distinct types are the most published on; electromagnetic emanations, optical emanations and acoustic emanations.

1) Electromagnetic emanations: Popularly known under the name ”TEMPEST” or ”Tempest”; electromagnetic emanations, which can occur from various electronic devices, leak information as radio frequency emissions.

Beginning in the eighties with work demonstrating the eavesdropping capabilities of radio receivers picking up emanations from cathode ray tube (CRT) monitors [12], allowing display reconstruction, and later from RS-232 serial data cables, allowing binary data capture [13], electromagnetic emanations have repeatedly been shown to be exploitable and capable of breaking confidentiality of displayed and transmitted plaintext data. Further development has resulted in more advanced technique in radio signal processing being applied to liquid crystal display (LCD) technology [14] and touch screens [15], again allowing display reconstruction, and PS/2 and USB keyboards, allowing remote and autonomous keystroke logging [16].

2) Optical emanations: Attacks based on visual information have been known as security issues for quite some time, with ”shoulder surfing” being a common attack against password or PIN entry. However, more powerful attacks are possible with special equipment.

It is possible to reconstruct screen content from low resolution CRT displays by measuring diffuse light emanations using photomultiplier tubes, without the need for line-of-sight access [17]. Using similar equipment, it is also possible to reconstruct data from flashing status LEDs on various types of computer hardware, including those from an older Federal Standard-rated cryptographic module, in plaintext [18]. Additionally, the capture of screen content through distance imaging of reflected images in common everyday objects such as eyeglasses, teapots, and even the human cornea has demonstrated that in certain circumstances even blocking line-of-sight access to a display may not be enough to stop sensitive information leakage [19]. Optical eavesdropping of keyboard input has also been demonstrated, using a consumer-grade video capture device to relay keystrokes and using image analysis techniques to determine the original data [20].

3) Acoustic emanations: Sound carries information in the form of frequency, wavelength and amplitude which can be measured by audio capturing equipment such as microphones. Acoustic emanations cause information leakage that can be exploited with such equipment. The most powerful attacks

presented academically have been against keyboard input, and demonstrate the potential application of such an attack for capturing login details and other secret information recovery.

The first attack method dealing with acoustic recognition of keystrokes was capable of differentiating between keystrokes through labelled acoustic signatures, and that telephone and ATM keypads were as vulnerable to this method as computer keyboards [21]. Further development on the idea of autonomous keystroke detection came with the application of a hidden Markov model in combination with statistical processes based on English grammar to create an attack methodology capable of real-time keystroke detection after short period of training [22]. The latest methodology allowing the reconstruction of plaintext data from acoustic emanations involves using statistical analysis, based on estimated distance between keys on a "QWERTY"-layout keyboard and assumption of the use of English words, of keystrokes to determine the most likely words being typed, in real time with no prior training or program preparation required [23]. However, keyboards are not the only target of acoustic attacks. Recently it has been demonstrated that dot-matrix printers are also capable of leaking data through noise emitted during regular operation [24]. This data allows the reconstruction of the original printout.

IV. Relevance to eVoting

In this section we examine how the above attacks could be applied against eVoting machines. In general, one can say, that attacks taking advantage of plaintext leakage are especially relevant to eVoting systems because for a voter to make a selection they must be able to accurately cast and check their own vote, meaning that these processes must be human readable. Furthermore, the parameters of vote selection mean that voter input is constricted to a limited set of choices which would manifest themselves as distinct signals within the leaked information.

As the analyses presented in this section are intended to identify potential vulnerabilities, and concrete attacks would depend on an in-depth technical evaluation of a specific implementation, we present the following ideas to highlight potential targets for attack. We analyse which components might be the most vulnerable, and present demonstrated and published attacks to underline the extent of their applicability.

The eVoting systems chosen here represent the majority of proposed and implemented technologies. Direct Recording Electronic (DRE) voting machines and additional components that offer voter verifiable paper audit trails (VVPATs) are first analysed, followed by systems that make use of optical scanners to interpret marked ballot papers. Finally, the use of cryptography in eVoting systems is considered.

It should be noted that the papers referenced here, with the exception of the VVSG guidelines [3], have demonstrated these attacks on the same type of equipment as used in eVoting machines, not against them specifically.

A. DRE voting machine with VVPATs

Let us consider a typical type of eVoting machine at a polling station. It is not connected to any network, is capable of only direct recording of votes through a simple interface, such as buttons or a touch-screen, and uses a display to provide voters with feedback of their selections. It may also have a printer attached to it for the purposes of providing a paper audit trail in the form of voter receipts. For sight-disabled voters, headphones may also be attached to allow the playing back of voter options and selections.

The application of side-channel cryptanalysis to such a device would not be required, since it does in general not make use of any cryptographic processes. However, the exploitation of plaintext compromising emanations would be extremely attractive to an attacker, since it affords a method of passively and remotely breaking voter secrecy.

Table I gives an overview of how the three types of compromising emanations can be directed to the most common components of Direct Recording Electronic voting machines. These types are explained in more detail in the following paragraphs.

Electromagnetic emanations can come from the DRE voting machine display, which may be cathode ray tube (CRT) or liquid crystal display (LCD) [14]. Some implemented DREs use touch screens for providing both display of candidates and means to select them. These have also been demonstrated to be vulnerable to exploitation [15]. Since displays are used to provided voters with feedback on their selections, successful capture of this information would provide an attacker with confidential vote data. Electromagnetic emanations may also come from additional selection tools such as buttons or keyboards, against which there exist demonstrated attacks [16]. Additionally, if the printer is connected to the machine with an RS-232 serial cable, ballot information can also be leaked [13].

Optical emanations can be exploited from CRT screens, using indirect diffuse light, such as that reflected from a wall or through opaque material, to reconstruct an image of the screen [17]. Screen capture can also be achieved through the imaging of reflections in voters' eyeglasses and other reflective objects in the immediate surroundings [19]. Autonomous reconstruction of keyboard input [20] can also be applied against voter interaction with DRE machine keypads.

Acoustic emanations can come from voter input with selection tools. Keyboards, keypads and buttons have all been shown to create identifiable acoustic signatures that allow the reconstruction of input information [21]–[23], and these attacks can be directed towards the selection tools provided by DRE voting machines. Additionally, dot-matrix printers have demonstrated susceptibility to acoustic eavesdropping, allowing reconstruction of the printed data [24]. This could be used to reconstruct printed ballots. Additionally, the headphones used by sight-disabled voters may leak information if set at too high a volume [3].

TABLE I
COMPONENTS OF DRE VOTING MACHINES WITH VVPATS THAT ARE POTENTIALLY VULNERABLE TO EXPLOITATION OF COMPROMISING EMANATIONS

	Potentially Vulnerable Machine Component			
Compromising Emanation	Visual Display Unit	Selection Peripheral	Ballot Printer	Headphones
Electromagnetic	Yes [12], [14], [15]	Yes [15], [16]	Yes [13]	-[a]
Optical	Yes [17], [19]	Yes [20]	-	-
Acoustic	-	Yes [21]–[23]	Yes [24]	Yes [3]

[a](-) denotes no examples to be found in the available literature.

TABLE II
COMPONENTS OF OPTICAL SCANNER BASED SYSTEMS THAT ARE POTENTIALLY VULNERABLE TO EXPLOITATION OF COMPROMISING EMANATIONS

	Potentially Vulnerable System Component		
Compromising Emanation	Scanner-PC Cable	LEDs on Network Port	Paper Ballot at Scanner
Electromagnetic	Yes [13]	-[a]	-
Optical	-	Yes [18]	Yes [19]

[a](-) denotes no examples to be found in the available literature.

B. Optical scanner based systems

With eVoting systems based on optically scanned ballot papers, other potential vulnerabilities may exist. There are many methods for implementing optical scanner based systems, including approaches where the scanning is performed during the tallying phase, or where the scanner stores the vote in an integrated internal electronic storage medium. Here we consider a simple and generic system where voters are required to scan in their completed ballot papers at the polling station, using an optical scanner which then transfers their selections to a computer and interprets the marks on the ballot. Typically such systems do not employ any cryptography, but some possibilities exist for attacks exploiting plaintext information leakage. Table II gives an overview of potential vulnerabilities of optical scanner based systems.

Electromagnetic emanation leakage may be present from the connection between the scanner and the PC to which ballot images are saved, if this connection is made with an RS-232 serial cable [13]. This would allow recovery of each ballot image as it is scanned and saved. Regarding optical emanation leakage, the ballot paper may be inadvertently visible when placed into the scanner from being transported from the private polling booth with long distance imaging techniques, and non-direct imaging techniques [19], being used to recover ballot information. One other possibility is that one or more scanners may be connected to a computer with network cables. Here, status light emitting diodes (LEDs) on an ethernet port could leak the ballot image while being scanned and sent back to the PC, provided that the LED can be defined as a Class III LED as described in [18].

Although it is possible that the actual scanning components of commercially available optical scanners give out exploitable electromagnetic emanations, no published work is available on this topic, and an attack against the scanner itself must be considered as speculation.

C. eVoting systems that use cryptography

In addition to the threat of compromising emanations mentioned above which are applicable to display, selection, printing or scanning devices, attacks using side-channel cryptanalysis must be considered for cryptographic implementations in eVoting systems. However, it should be noted that the existence of vulnerabilities would depend on the concrete implementation of the system. Therefore, we only focus on one example: the Bingo Voting system, where cryptography can be used to generate random numbers, used for vote secrecy and verifiability [25].

In Bingo Voting, a system that makes use of random numbers generated at the polling booth in secret to allow only the voter to determine their selected candidate among other pre-generated random numbers, which act as ”dummy” votes, on a ballot receipt [25]. This allows the voter to verify that their vote has been interpreted by the system correctly by checking the receipt on a public bulletin board. Since knowledge of the poll booth random number allows the finding of the selected candidate on the voters' receipt, any leakage of this number reveals their selection and breaks vote secrecy. In this case, the implementation of the random number generator would determine vulnerability to attack and the application of side-channel cryptanalysis might be relevant. Here, key recovery from a cryptographically based pseudorandom number generator would allow the determination of each following number, allowing an attacker to gain knowledge of each secret random number for all following voters. However, the existence of these vulnerabilities completely depends on the specifics of the implementation, and none of the above suggestions are intended to cast doubt on the security of the proposed protocols, but are only intended to highlight how

vulnerabilities in the implementation of eVoting machines in an eVoting system might affect election security as a whole.

V. Feasibility of attacks and countermeasures

In this section we discuss the general feasibility of the most relevant side-channel attacks against eVoting machines; those that exploit compromising emanations. We also discuss the, to be assumed, attacker potential and countermeasures proposed in literature.

A. General feasibility

We concentrate on attacks exploiting compromising emanations because they can be applied to common components of many eVoting systems. For all the attacks presented, it is necessary to match the captured ballot information to each voter. This requires the ability to link each voter to the time of their cast vote, but this kind of "traffic analysis" can be carried out by observing voting booth entry and exit, and creating an association between voters and their votes in this way should be considered trivial.

Regarding the exploitation of electromagnetic emanations, demonstrated distances of successful information retrieval can range from 50 metres for CRT displays in plastic casings and 10 metres for CRT displays in metal casings [12], 10 metres for LCD displays [14], 5 metres for keyboards [16], 7 metres for RS-232 cables [13] and 1 metre for touch screens [15]. All these attacks are achievable using widely available radio receiver technology.

Attacks based on exploiting optical emanations, in the form of shoulder-surfing, are generally taken into account already with the designed privacy of polling booths mitigating most of optical based threats. However, the suggested vulnerability of status LEDs on scanners, practical at a distance of 10 metres [18], and the possible exploitation of light emanations from CRT displays, which can be realised at a distance of 50 metres without line-of-sight access and in the right light conditions [17], is something which is not dealt with in any security standards. Furthermore, attacks based on exploiting reflected images containing 10 pt font can take place from a distance of 5 metres [19].

Acoustic emanations are a novel source of information leakage from data input devices and dot matrix printers. Keypad input can be reconstructed from a distance of 15 metres with a parabolic microphone, but the best results were achieved with a microphone being placed close to the target device [21]. For the attack against the printer, the microphone must be within 10 centimetres of the printer [24]. However, the current level of sophistication and miniaturisation for remotely operated audio bugs can be used to greatly increase the range of a practical attack.

In the future, developments in technology specific to these emanations could increase the power of these attacks. If autonomous collection of ballot information where possible, the application of these attacks on a large scale would be feasible.

B. Attacker motivation and power

Attacker motivation must also be considered. There exist a multitude of groups opposed to the implementation of eVoting for legally binding elections, and each will no doubt attempt to discover vulnerabilities in any proposed system. Some members of such groups also possess a high degree of technical expertise and knowledge, this coupled with a strong desire to find security holes in eVoting systems means that systems that have not undergone a thorough and open security analysis prior to deployment are guaranteed to be given a trial by fire. This reinforces our motivation and suggestion for formalised security requirements, which would do away with the principle of security through obscurity.

While there is some potential for such attacks to be deployed en masse against implementations of eVoting systems, the real power and practicality of these attacks stems from their remote and passive properties. The surveillance capabilities of these attacks open up avenues that are hard to predict when designing a theoretically secure system. For instance, in countries that are made up of an amalgamation of distinct ethnic and political groups, and where these groups make up the majority of distinct localities within the country, the breaking of voter confidentiality can cause reprisals against voters for minority groups, or provide a means of inducing future voter coercion. Another scenario might involve targeting polling stations where high-profile individuals, who do not wish to disclose their political preference, are known to vote at.

Overall, the attacks presented here should be considered feasible as we have good reasons to assume the existence of determined and competent attackers. Note, large scale attacks are only possible by a group of people as it is required to observe the polling booths to know who cast a vote on which machine when.

C. Countermeasures

Electromagnetic emanations are taken into account by manufacturers of electronic devices due to the need to comply with emission standards for the reduction of electromagnetic interference, published by the International Electrotechnical Commission through CISPR standards [26], but these do not address the existence of information leakage. Countermeasures have been suggested and implemented, such as software font design to reduce legible image reconstruction [27].

The techniques described above that exploit optical emanations can be directed against eVoting machines in a way that would not seem obvious when setting up a polling station to prevent shoulder-surfing type attacks. As such, designing countermeasures to combat this form of leakage creates a link between information and physical security. While it would appear to be common sense to block all line-of-sight access to sensitive data that an attacker might possess, further thought is required to adequately defend against methods using the more novel forms of attack. This could include covering status lights of auxiliary equipment [18] and using completely enclosed poll booths to prevent reflection based attacks.

With regards to preventing acoustic emanations, the source of such emanations from keyboards and keypads lies in their design; the supporting plate on which all keys rest acts as a drum, resonating with each keystroke. It has been suggested that using a keyboard that does not rely on this, such as a projected keyboard or touch screen would solve this issue [21]. The most effective countermeasure for preventing leakage from the printer was acoustic shielding. However, other countermeasures might include changing printer technology to inkjet or laser printers, which were not found to be vulnerable to the same attack [24], or implementing greater physical security measures around the target device, preventing the attacker from using covert audio recording equipment.

By putting forward the above countermeasures along with the discovery of each attack, it becomes obvious that it is possible to protect electronic voting systems against side-channels but it is necessary to take this type of attack into account and apply these countermeasures.

VI. Side-channel requirements for eVoting

As a crucial component of the overall security of an eVoting system, side-channel security for the guarantee of confidentiality must be formalised and integrated in existing requirement documents. Therefore, we first analyse existing security evaluation standards' applicability for this purpose. After having shown that the Common Criteria fits best we provide a short introduction to the Common Criteria and define afterwards our requirements in the Common Criteria language.

A. Existing standards

Here we present the two relevant security evaluation standards, namely FIPS and Common Criteria, and analyse if they can be used to define security requirements for side-channels in eVoting machines.

a) FIPS 140-3: The draft of FIPS 140-3, the Federal Information Processing Standard 140-3 [28] which standardises security for cryptographic modules, mentions the forms of side-channel cryptanalysis presented in Section III-A. FIPS 140-3 is essentially the first step towards formal security requirements for protection against side-channel attacks. Developed by NIST, the National Institute for Standards and Testing, the standard represents the work of a central body beginning to define security requirements for side-channel cryptanalysis and providing a framework for evaluation and certification.

Out of 4 levels of security, assurance ascending with number, side-channel resistance is required for levels 3 and 4. The actual requirements in the document specify that the validating authority, in other words the organisation that performs the evaluation, shall determine that the device's security is not compromised by timing analysis, power analysis and electromagnetic analysis. Furthermore, it requires that documentation of the countermeasures and their effectiveness are provided. Finally, the effectiveness of the countermeasures will be specified by the validating authority.

FIPS 140-2 [29] Level 3 has already been applied to the system T-DRE for the purposes of implementing countermeasures for protecting against physical manipulation. The system was developed and implemented in Brazil for the 2010 presidential elections [30]. The machine makes use of trusted platform modules and corresponding cryptographic analysis to provide extra assurance for machine and election integrity.

b) Common Criteria: The purpose of Common Criteria is to define a method for the semi-formal definition of evaluation criteria for IT security [31]. In its most basic form, a designer or vendor of the TOE (Target of Evaluation) produces documentation in the form of a Security Target (ST). This addresses threats, assumptions and security objectives. Furthermore, predefined requirements, published in the Common Criteria Security Functionality Requirements Catalogue, are matched to the defined threats, assumptions and security objectives. These are called Security Functional Requirements (SFRs), which specify secure functionality of the TOE. Generally, SFRs have dependencies, where one or more defined SFR are required to be met for the purposes of another SFR. As a complete document, the Security Target is then used by the evaluating authority to ensure that the TOE performs as stated.

There exists an extension of the Common Criteria Security Functional Requirements catalogue that takes into account emanations that cause information leakage; FTP_EMSEC [32]. FTP here denotes these requirements falling under the area of Trusted Paths/Channels. This provides a basis for formalising requirements based on side-channel cryptanalysis and compromising emanations within the Common Criteria methodology.

The details of the FPT_EMSEC.1 requirement family are given here, and there are no dependencies for the two requirements.

FPT_EMSEC.1.1

The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMSEC.1.2

The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

It constitutes two parts, the first part requiring that the TOE, which in our case would be an eVoting machine, does not create emanations that leak information that is wished to be protected. The second part requires that the TSF (TOE Security Functions), which would be all countermeasures deployed, adequately prevents the leakage of sensitive information.

c) Comparison: The FIPS standard only provides definitions relevant to side-channel cryptanalysis. For the specific forms of compromising emanations discussed in Section III-B,

which are even more relevant to eVoting than side-channel cryptanalysis, the Common Criteria can be used to address both side-channel cryptanalysis, as has been demonstrated for power analysis [32], and compromising emanations with the use of the FTP_EMSEC.1 requirement family, an extension to the Security Functional Requirement Catalogue. A further benefit is that the use of Common Criteria for the purposes of eVoting machine evaluation has already occurred, as the Digital Pen Voting system has been analysed according to the Common Criteria[1]. Correspondingly, there already exists some familiarity with the application of the Common Criteria to eVoting. Therefore, we have decided to apply the Common Criteria method for the definition of security requirements.

B. Defining requirements with Common Criteria

In the following subsections, we give an overview of the procedure for defining security requirements with Common Criteria.

The first step is to formulate assumptions and threats that deal with the specific vulnerabilities that should be taken into consideration. In the case of defining these components to address side-channels, it is necessary to look at the specifics of each published attack for each vulnerability. We can draw assumptions and threats from such details, as effective distances for successful attacks and type of equipment needed. With these details, objectives can then be formulated for that specific type of attack.

In the next step, security objectives are deduced from these threats and assumptions. Predefined Security Functional Requirements, published and openly available on the Common Criteria website as Common Criteria Part 2: Security Functional Requirements [31], are then chosen and included along with the security objectives.

One difficulty with this is that in the main requirements catalogue, there exist no mention of emanations or emissions. However, extensions to the catalogue exist, and one of these, the FPT_EMSEC.1 Family, addresses the existence of side-channels. This extension has been used in Security Targets for products and devices where side-channels are an important consideration, such as smart cards [32].

A Protection Profile is a user generated set of security requirements. It allows third-parties to formalise security requirements to be taken into consideration by designers for incorporation into a Security Target. Since these requirements can be made in an implementation-independent manner, it is preferable to define a Protection Profile in sensible contexts like eVoting machines first and later base an evaluation of a concrete product on such a Protection Profile.

C. Example requirements

Here we define an example set of assumption, threat, security objective, and corresponding Security Functional Requirements, denoted as A, T, O and SFR respectively. These definitions are intended to act as a demonstration of how published attack methodologies can be used to formulate security requirements. As we only provide examples, more work needs to done to formalise security requirements that comprehensively cover side-channels in relation to eVoting. Other requirements can be defined in the same way, i.e. taking available information from published attacks and using it to identify attack capabilities. For now, there exists the one SFR extension described above, so each assumption, threat and objective would be defined in the same way as the following example, for the formulation of actual security functional requirements.

Note, the requirements we propose do not intend any defined requirements to form their own Protection Profile. Instead, we suggest that these requirements form part of more comprehensive Protection Profiles like the existing one for the Digital Election Pen [33], that would look at security for one type of eVoting machine. The proposed requirements could also easily be integrated in existing Security Targets.

The examples for the operational environment are as follows:

A.ElectromagneticEmanations.AttackerDistance
The eVoting machine, TOE, is secure from physical manipulation, and is operated by voters in an environment that can be kept secure, i.e an attacker cannot initiate an attack without being detected, to a distance of 10 metres around the machine.

Application Note. The distance of 10 metres, the maximum range demonstrated in the literature for an attack on LCD monitors or CRT monitors in metal casings, takes into account a reasonably sized polling station. Note, whatever distance is selected, it needs to be ensured that the placement of the machine within the station allows a secure environment to be maintained.

T.ElectromagneticEmanations.DisplayLeakage
Display technologies (CRTs and LCDs), used to display voters' selections back to them during the vote casting process, leak electromagnetic emanations in the radio frequency spectrum. The emanations are eavesdropped by an attacker, breaking vote confidentiality. The attacker is able to link votes to each voter by having additional information about who cast their vote when, i.e. timing information from observation.

Correspondingly, the example security objective is:

O.ElectromagneticEmanations.DisplayLeakage
The eVoting machine, TOE, shall not leak electromagnetic emanations, containing information that can be used to the deduce the cast vote, that can be received from 10 metres away or more.

Based on this security objective the following Security

[1]Note, side-channels have not been addressed in this Common Criteria evaluation.

Functional Requirement can be deduced:

FPT_EMSEC.1.1
The TOE shall not emit [*electromagnetic emanations*] in excess of [*a distance of 10 metres*] enabling access to [*ballot information, generated by the machine*]

FPT_EMSEC.1.2
The TSF shall ensure [*attackers*] are unable to use the following interface [*emanations in the radio frequency spectrum received with radio receiver technology*] to gain access to [*ballot information*]

Rationale
The SFRs chosen here address all aspects of the security objective above. The security objective addresses the assumption and the threat defined above.

With this example, we demonstrate how threats and assumptions found in the available literature can be used as the basis for formulating security objectives, and can be met by predefined SFRs. This needs to be extended for the other types of side-channels mentioned above.

VII. Summary and Future work

We have seen how implementation-specific attacks can defeat certain types of cryptographic and physical security measures. Indeed, some of the attacks discussed here are especially relevant to the simple, plaintext, data input and output of vote casting present in many eVoting systems.

We have shown how potential avenues exist for information leakage and that electromagnetic, optical and acoustic emanation exploitation attacks are applicable against current eVoting system technologies. All these attacks have been demonstrated in the available literature as functional and practical. They have shown that the use of consumer-grade equipment, such as displays, keypads, printers and scanners, enables attacks exploiting compromising emanations, and also allows the applicability of such attacks across distinct eVoting systems that make use of those same types of equipment. Attacks exploiting electromagnetic emanations having already been successfully directed against DRE voting machines, and with this in mind, we have called for an improvement of this situation through the formalisation of the security threats that these types of attacks present.

The clearest direction for future work lies in the need for defining a complete list of security requirements for addressing side-channel vulnerabilities of eVoting machines. For example, assumptions taking other aspects of feasibility, such as the size of required attack equipment need to be defined. To ensure that the list is exhaustive, we will use techniques such as attack trees, which would allow the methodical development of a complete list of threats.

Furthermore, once work on defining requirements for poll booth eVoting machines has been completed, there may be interesting future work in seeing how these security requirements could be extended to cover remote eVoting systems. In such systems such as internet voting, leakage might occur from a voter's PC or at the voting server, environments that would require different security requirements to be enforced.

Acknowledgment

This paper is developed within the project "VerkonWa - Verfassungskonforme Umsetzung von elektronischen Wahlen" which is funded by the German Science Foundation (DFG).

References

[1] W. Pieters, "Combatting Electoral Traces: The Dutch Tempest Discussion and Beyond," in *E-Voting and Identity*, ser. Lecture Notes in Computer Science, P. Y. Ryan and B. Schoenmakers, Eds. Springer Berlin / Heidelberg, 2009, vol. 5767, pp. 172–190.

[2] *Recommendation Rec(2004)11 and explanatory memorandum - Legal, operational and technical standards for e-voting*, Council of Europe, 2004.

[3] EAC, "Voluntary Voting System Guidelines 1.1 - Volume 1," The U.S. Election Assistance Commission, Tech. Rep., 2009. [Online]. Available: http://www.eac.gov/assets/1/workflow_staging/Page/124.PDF

[4] V. Hartmann, N. Meissner, and D. Richter, "Online Voting Systems for Non-parliamentary Elections - Catalogue of Requirements," Physikalisch-Technische Bundesanstalt Braunscheig und Berlin, Laborbericht PTB-8.5-2004-1, 2004. [Online]. Available: http://ib.ptb.de/8/85/LB8_5_2004_1AnfKat.pdf

[5] M. Volkamer, "Requirements for electronic voting machines," in *Evaluation of Electronic Voting*, ser. Lecture Notes in Business Information Processing, W. van der Aalst, J. Mylopoulos, N. M. Sadeh, M. J. Shaw, and C. Szyperski, Eds. Springer Berlin / Heidelberg, 2009, vol. 30, ch. 5, pp. 73–91.

[6] M. Kuhn, "Bericht über eine Kurzuntersuchung zur Einschätzung des Risikos kompromittierender RF Abstrahlungen eines digitalen Wahlstifts," November 2007, [German] Emissions report and correspondence to Willi Bei, Behörde für Inneres, Hamburg.

[7] H. Schrepf, N. Greif, and D. Richter, "Wahlgerärte in Deutschland," *Datenschutz und Datensicherheit - DuD*, vol. 33, pp. 88–91, 2009, [German].

[8] P. Rohatgi, "Side-Channel Attacks," in *Handbook of Information Security*, H. Bidgoli, Ed. Wiley, 2006, vol. II.

[9] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in *Advances in Cryptology CRYPTO 96*, ser. Lecture Notes in Computer Science, N. Koblitz, Ed. Springer Berlin / Heidelberg, 1996, vol. 1109, pp. 104–113.

[10] P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Advances in Cryptology CRYPTO 99*, ser. Lecture Notes in Computer Science, M. Wiener, Ed. Springer Berlin / Heidelberg, 1999, vol. 1666, pp. 388–397.

[11] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic Analysis: Concrete Results," in *Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, ser. CHES '01. London, UK: Springer-Verlag, 2001, pp. 251–261.

[12] W. van Eck, "Electromagnetic radiation from video display units: an eavesdropping risk?" *Computer Security*, vol. 4, no. 4, pp. 269–286, December 1985.

[13] P. Smulders, "The threat of information theft by reception of electromagnetic radiation from RS-232 cables," *Computer Security*, vol. 9, no. 1, pp. 53–58, February 1990.

[14] M. Kuhn, "Electromagnetic Eavesdropping Risks of Flat-Panel Displays," in *Privacy Enhancing Technologies*, ser. Lecture Notes in Computer Science, D. Martin and A. Serjantov, Eds. Springer Berlin / Heidelberg, 2005, vol. 3424, pp. 88–107.

[15] H. Sekiguchi, "Information leakage of input operation on touch screen monitors caused by electromagnetic noise," in *Proceedings of the 2010 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, Fort Lauderdale, FL, USA, 2010, pp. 127–131.

[16] M. Vuagnoux and S. Pasini, "Compromising electromagnetic emanations of wired and wireless keyboards," in *Proceedings of the 18th conference on USENIX security symposium*. Montréal, Canada: USENIX Association, 2009, pp. 1–16.

[17] M. Kuhn, "Optical Time-Domain Eavesdropping Risks of CRT Displays," in *Proceedings of the 2002 IEEE Symposium on Security and Privacy*. Berkeley, CA, USA: IEEE Computer Society, 2002, pp. 3–18.

[18] J. Loughry and D. A. Umphress, "Information Leakage from Optical Emanations," *ACM Transactions on Information and System Security*, vol. 5, no. 3, pp. 262–289, August 2002.

[19] M. Backes, T. Chen, M. Dürmuth, H. P. Lensch, and M. Welk, "Tempest in a Teapot: Compromising Reflections Revisited," in *Proceedings of the 30th IEEE Symposium on Security and Privacy (S&P 2009)*. Oakland, CA,USA: IEEE Computer Society, 2009, pp. 315–327.

[20] D. Balzarotti, M. Cova, and G. Vigna, "ClearShot: Eavesdropping on Keyboard Input from Video," in *Proceedings of the 2008 IEEE Symposium on Security and Privacy (S&P 2008)*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 170–183.

[21] D. Asonov and R. Agrawal, "Keyboard Acoustic Emanations," in *Proceedings of 2004 IEEE Symposium on Security and Privacy (S&P'04)*. Berkeley, CA, USA: IEEE Computer Society, 2004, pp. 3–11.

[22] L. Zhuang, F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," in *Proceedings of the 12th ACM conference on Computer and Communications Security*. Alexandria, VA, USA: ACM, 2005, pp. 373–382.

[23] Y. Berger, A. Wool, and A. Yeredor, "Dictionary attacks using keyboard acoustic emanations," in *Proceedings of the 13th ACM conference on Computer and Communications Security*, ser. CCS '06. New York, NY, USA: ACM, 2006, pp. 245–254.

[24] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder, "Acoustic side-channel attacks on printers," in *Proceedings of the 19th USENIX conference on Security*, ser. USENIX Security'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 307–322.

[25] J. Bohli, J. Müller-Quade, and S. Röhrich, "Bingo Voting: Secure and Coercion-Free Voting Using a Trusted Random Number Generator," in *E-Voting and Identity*, ser. Lecture Notes in Computer Science, A. Alkassar and M. Volkamer, Eds. Springer Berlin / Heidelberg, 2007, vol. 4896, pp. 111–124.

[26] CISPR, "CISPR 22:2008 - Information technology equipment Radio disturbance characteristics Limits and methods of measurement," 2008.

[27] M. Kuhn and R. Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," in *Information Hiding*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 1998, vol. 1525, pp. 124–142.

[28] "FIPS PUB 140-3 (Revised DRAFT 09/11/09) - SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES," National Institute of Standards and Technology.

[29] "FIPS PUB 140-2 (CHANGE NOTICES (12-03-2002) - SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES," National Institute of Standards and Technology.

[30] R. Gallo, H. Kawakami, R. Dahab, R. Azevedo, S. Lima, and G. Araujo, "T-DRE: a hardware trusted computing base for direct recording electronic vote machines," in *Proceedings of the 26th Annual Computer Security Applications Conference, ACSAC '10*, C. Gates, M. Franz, and J. P. McDermott, Eds. ACM, 2010, pp. 191–198.

[31] "Common Criteria for Information Technology Security Evaluation," Version 3.1, Revision 3, Final, July 2009, available at: http://www.commoncriteriaportal.org/cc/ Retrieved: 07.06.2011.

[32] Giesecke&DevrientGmbH, "Security Target Lite - STARCOS 3.4 Health - AHC C1," Final Version, December 2009.

[33] M. Volkamer and R. Vogt, "Digitales wahlstift-system. Common Criteria Protection Profile BSI-PP-0031," Bundesamt für Sicherheit in der Informationstechnik, Tech. Rep., 2006, [German].