Ballot printer – performance of eavesdropping protection –radio-frequency emissions

1 Introduction and scope

This specification aims to define the level of eavesdropping protection expected from a ballot printer. A ballot printer is a device (typically a desktop unit) that can be configured with a ballot configuration file *C*. This file defines and names the n choices $\{c_1, c_2, \ldots, c_n\}$ that a voter can make during the election process. A typical configuration file *C* may contain a list of political parties and/or candidates, or a list of options for a referendum, along with associated names, logos, portrait photographs, or accompanying descriptive text that the ballot printer displays to assist the voter in making their choice, or prints onto the resulting ballot paper. A voter can use the ballot printer to make one choice *X* out of the available *n* options defined by the configuration file, and the device then records that choice by printing out a ballot paper that the voter can fold and take away to the ballot box. The choice made by the voter has to remain confidential, and must not become known to anyone else until the ballot box is opened and the ballot paper is unfolded during the counting process, at which point the ballot paper should no longer be linkable to the voter.

One security concern in the design of such a ballot printer is that electromagnetic signals that are unintentionally emitted by its circuitry can give away the voter's choice to a nearby eavesdropper with suitable antennas, radio receiver and signal-processing equipment.[1] Whether such an eavesdropping attack is feasible or not depends on a number of factors, such as at what distance can the eavesdropper use what type of antenna, what is the background noise level in the environment, and how detailed and accurate must the eavesdropped information about the voter's choice be to count as a successful attack. It is not practical to shield devices completely against every imaginable form of an electromagnetic eavesdropping attack, for a number of reasons. While electric fields can be shielded relatively easily using a metallic enclosure (Faraday cage), shielding magnetic fields is far more difficult. Very close to the device (in the *near field*), magnetic fields can be the dominant form of emissions, but will also drop off rapidly with increasing distance. It may not be difficult to demonstrate a successful eavesdropping attack that estimates the choice of the voter with slightly better chances than random guessing, using large antennas placed centimetres from the surface of the device, with both the device and the antenna located in a shielded chamber that eliminates environmental background noise.

[1] Acoustic or optical eavesdropping attacks (using microphones, or sensors for diffusely reflected light) are also a potential threat, but outside the scope of this document. However, Section 5 offers some related informal notes.

However, such an attack would be easy to spot, and would therefore hardly constitute a realistic threat. It may also be very difficult and costly to prevent. It is therefore useful to agree on some constraints for, and expectations of, what can be considered a successful and realistic eavesdropping attack, in order to give device designers, evaluators and users a common understanding of the expected threat level.

The specification of such an attack scenario is proposed in this document. It defines the rules of a game to be played between a *challenger* (e.g. a representative of the designer of the ballot printer), whose intent is to demonstrate the security of the device, and an *adversary* (e.g., a representative of an evaluation laboratory or an independent security researcher), whose intent is to demonstrate an eavesdropping vulnerability.[2]

2 Setup

1) Choose two ballot printers at random out of a manufacturing batch of printers of identical construction. Both printers must contain the same types and versions of internal components and may differ only in continuous parameters within the specified manufacturing tolerances.
2) The adversary is given access to one of these two sample printers, for laboratory tests and reverse engineering.
3) The other sample printer remains intact and will be used as the *target of evaluation (TOE)* in the following experiment.
4) The adversary provides a valid configuration file C, which a referee loads into the TOE ballot printer. The file must pass all the acceptance tests implemented by the printer and must cause the printer to offer the voter a ballot with at least two choices. If the configuration file requires inclusion of an authentication code or digital signature before it can be loaded into the TOE printer, then the referee or challenger will provide that code.
5) Repeat the following steps k times:
   a) Prepare the TOE printer for the next vote.
   b) The adversary sets up or adjusts their eavesdropping equipment, within the constraints set out in the next section.
   c) The adversary choses two of the ballot choices available in that configuration file, which we will call c^0 and c^1, and hands these to the challenger.
   d) The challenger picks a random bit b (e.g. by tossing a coin) and instructs a neutral voter to use the TOE ballot printer (like a regular voter would) in order to print out a ballot paper recording a vote for option c^b, that is either c^0 or c^1, as chosen by the random bit b, which is not yet revealed to the adversary.

[2] The rules of the game proposed here is somewhat inspired by security definitions used in modern cryptography, such as *ciphertext indistinguishability under chosen-plaintext attack* (IND-CPA).

e) The adversary is verbally informed when the voter starts to use the TOE device and when the printout has finished and the device has reset itself for use by the next voter. The adversary observes the ballot printer through their eavesdropping equipment while the voter makes their choice and prints their ballot paper.
f) The adversary now examines any data received and then announces their best guess b' for the value of the secret bit b chosen by the challenger.
g) The challenger/voter now reveal their secret bit b. If $b = b'$, then the adversary has guessed the vote correctly and won this round, and the win counter w is increased by one.

The TOE printer has failed the test if the adversary can demonstrate that they can guess the random bit b correctly $w \geq 45$ times in $k = 60$ trials.[3]

3 Eavesdropping setup

The eavesdropper's equipment must comply with the following restrictions:

R1 At least 8 metres horizontal distance between the outer surfaces of the TOE and any eavesdropping equipment
R2 All radio antennas used (excluding tripod/mast legs used for positioning) must together fit into a cuboid of width 1.0 m, height 0.9 m and length 1.2 m
R3 May include voltage-probe and current-clamp access to the power-supply cable of the TOE (again at 8 m distance)

Alternatively, the adversary may choose the following conditions for a very compact eavesdropping system:

C1 At least 4 metres horizontal distance between the outer surfaces of the TOE and any eavesdropping equipment
C2 All equipment (antennas, receivers, processors) fits comfortably inside a typical 20-litre backpack (such that the backpack remains externally indistinguishable from one filled with books or clothes)
C3 Weighs not more than 8 kg
C4 Does not require any access to a power line (or other external wired connection)
C5 Includes a power supply (battery) for three hours
C6 Does not require any on-site adjustment other than crude one-off placement and orientation

[3] The "45 out of 60 trials" threshold ensures that if an adversary merely picks b' uniformly at random, the ballot printer will pass the test with probability greater than 0.999, whereas if the adversary is able to guess b correctly with probability 0.9, the TOE will fail the challenge with probability greater than 0.999. The number of trials $k = 60$ should allow completing the test within an hour.

In neither scenario may the eavesdropping equipment include a radio transmitter that violates European Union spectrum-licencing requirements or that would require a radio amateur licence.

In both scenarios, the experiment can be conducted at any in-door site that is not especially shielded against environmental radio-frequency noise. In case of doubt, a spectrum analyser can be used to verify that the antenna noise levels at the receiver inputs are matching at least the minimum radio noise levels given in ITU-T Recommendation P.372 (solid line in figures 1–3), adjusted for the gain and antenna factor of the type of antenna used.

In case the adversary requests a more controlled radio environment (for example because a nearby transmitter overshadows a particularly useful signal), the test can alternatively also be conducted inside a shielded, semi-anechoic chamber. In this case, the eavesdropper's receiver system has to be modified to ensure that simulated Gaussian noise of amplitude equivalent to the minimum radio noise levels given in P.372 is added to the received signal band. Detailed geometric arrangements (e.g. TOE on a wooden table above a ground plane, antenna positioning and distance to chamber walls, etc.) should be adopted from the requirements of either NATO SDIP 27 or CISPR 22.

If the available semi-anechoic chamber is not large enough to achieve the required eavesdropping distances (8 m or 4 m), then the eavesdropping equipment can also be set up at a closer distance, down to 1 meter. In this case, the signal has to be attenuated (after the antenna but before simulated noise is added) to the signal level that is to be expected at the required eavesdropping distance. To calculate the required signal attenuation for an electric-field eavesdropping antenna, the TOE can be modelled as a short (compared to the wavelength) Hertzian dipole transmission antenna, and for a magnetic-field eavesdropping antenna, the TOE can be modelled as a small loop transmission antenna. In both cases, the model transmission antenna should be assumed to be oriented such that its direction of maximum emission is pointing towards the eavesdropper's antenna. In this case, the signal voltage received by the eavesdropper will drop approximately with the cube of the distance in the near field, and linearly with the distance in the far field. This drop of field strength with distance for the model transmission antenna should then be used to calculate the required attenuation to be applied to the eavesdropping system, to correct for its distance, before noise is added. This way, a realistic best-case signal-to-noise ratio at 4 m or 8 m can be simulated, even if the eavesdropping antenna is actually positioned much closer due to space constrains.

4 Rationale

The following considerations went into the design of this specification:

- We do not ask the adversary to completely identify the voter's choice, but merely to extract one bit of information about each vote made, and even give them control over which bit of information they have to extract, that

is between which two voter's choices they have to distinguish. This is not only in line with commonly used security definitions in modern cryptography (e.g., IND-CPA), but is also what adversaries in the past found sufficient to damage public trust in previous electronic voting equipment. (The attack on a previously used voting machine that was withdrawn in 2007 revealed only the number of non-ASCII characters in the displayed party name, in practice just one bit of information, and not the complete voter choice!)

- We allow the adversary to design the configuration file of the test ballot, in order to ensure that weaknesses that show up only in certain ballot configurations can be exploited. In the real world, the adversary may be one of the political parties, and they have control over some of the supplied configuration information, such as how names are spelled or the content of portrait photos or logos, which could be optimized for distinguishability via radio emissions. (In the case of a previously used voting machine that was withdrawn in 2007 candidates could in theory have varied the number of non-ASCII characters in the spelling of their names.)
- We allow the adversary to calibrate their equipment and software on a type-identical model, but not on the actual target of evaluation. Any on-site calibration needed will have to be done during actual voting rounds performed as part of the test, such that initial votes lost due to incomplete calibration of the eavesdropping equipment do affect the test outcome.
- The eavesdropping distance of 8 m is mainly inspired by the commission's choice of NATO SDIP-27 Level A as one of the applicable protection requirements. This is likely a realistic distance of eavesdropping attacks from outside a building, such as from an adjacent parking space. As 8 m seems quite a long distance for an attack with very compact equipment that can easily be disguised, we offer a second alternative setup at 4 m distance, to simulate a small backpack placed in an adjacent room.
- The 8 m attack setup limits the antenna dimension to a volume of roughly one cubic meter, which could be installed in a vehicle or adjacent building. The actual dimensions deviate slightly from a cuboid with 1 m side length merely in order to accommodate some commonly used types of measurement antenna (log-periodic) and directional antenna (Yagi-Uda).
- The size constraint of the 4 m attack setup is meant to exclude the use of highly directional and carefully aligned antennas.

5 Some notes on optical and acoustical side channels

The test setup specified in the preceding sections could, in a future revision of this document, also be extended beyond radio-frequency and power-line emissions, to cover other types of leakage channels, such as

- visible or near-visible light emitted by the display, after it was diffusely reflected by nearby white surfaces (i.e., no direct line of sight to the display surface),

- visible light or near-visible light emitted by the display after specular reflection from the user's glasses or eyeballs,
- acoustic emissions from the voice-prompt interface for visually-impaired users,
- acoustic, ultrasound or infrasound emissions from mechanical components, such as buttons or the print engine, as well as from power-supply filter components, such as capacitors and inductors, which can leak power-supply signals through piezo-electric or magnetic-force effects.

This section outlines a few related, preliminary considerations.

One challenge in adapting the protection-performance requirement to these other channels is to define realistic levels of background noise. In the case of optical leakage, an attacker might use a photo detector or spectroscope to spot minor colour and brightness variations in the light emitted by the display. A high-frequency noise source will be "shot noise", which is determined by the level of background illumination. A slower source of light variability will be changes in the surrounding scenery (e.g. people moving around), but this is difficult to quantify. An attacker could attenuate such noise sources using time-domain band-pass filters. Spectral composition also matters. In some voting stations, background illumination will come from fluorescent lights that emit a characteristic, non-uniform line spectrum. An attacker could use a spectroscope or a set of optical filters to separate such interfering light sources from the signal of interest. Therefore, in the absence of more detailed data, a starting point would be to specify for the eavesdropping challenge a level of background illumination from a spectrally more uniform source (e.g. a halogen lamp, colour temperature about 3000 K), but at least one order of magnitude darker than what would be considered acceptable at a real voting station, for example 1–5 lux from above and all horizontal directions.

In the case of acoustic emissions, a quiet office room (e.g. 20–30 dB_{SPL}) would seem a suitable starting point for the test environment. One particular difficulty with assessing the eavesdropping risk of the headphone voice interface is that voters will have control over the audio volume. Therefore, this should be set to the volume of a quiet conversation (e.g. 50–60 dBA) as measured in a standard ear simulator on which the headphone is mounted.

For optical eavesdropping attempts, the test user should wear bright clothing (e.g. a white shirt) and glasses without anti-reflective coating, or be replaced with an equally dressed head-and-torso simulator with glass eyes, arranged in a typical operator position.