Trust and security: e-voting as a special case

Tallinn, 19 June 2002

Neil Mitchison
Institute for the Protection and the Security of the Citizen
Joint Research Centre, Ispra (Va) 21020 Italy

Neil.Mitchison@jrc.it

Structure of this presentation

This paper presents the challenge of analysis of the risks involved in Internet voting; it does not try to develop a system.

- Top-level risk categorisation
- How to do a threat analysis
- The problem with e-voting: verification
- A threat analysis matrix
- Some threats, in increasing order of severity
- An – entirely personal – conclusion

e-voting – risk assessment

Risks are of three types:

- intrinsic defects of e-voting

These are broadly similar to those of postal or proxy voting systems, plus added concerns about selective disenfranchisement

These can be evaluated and a political decision taken.

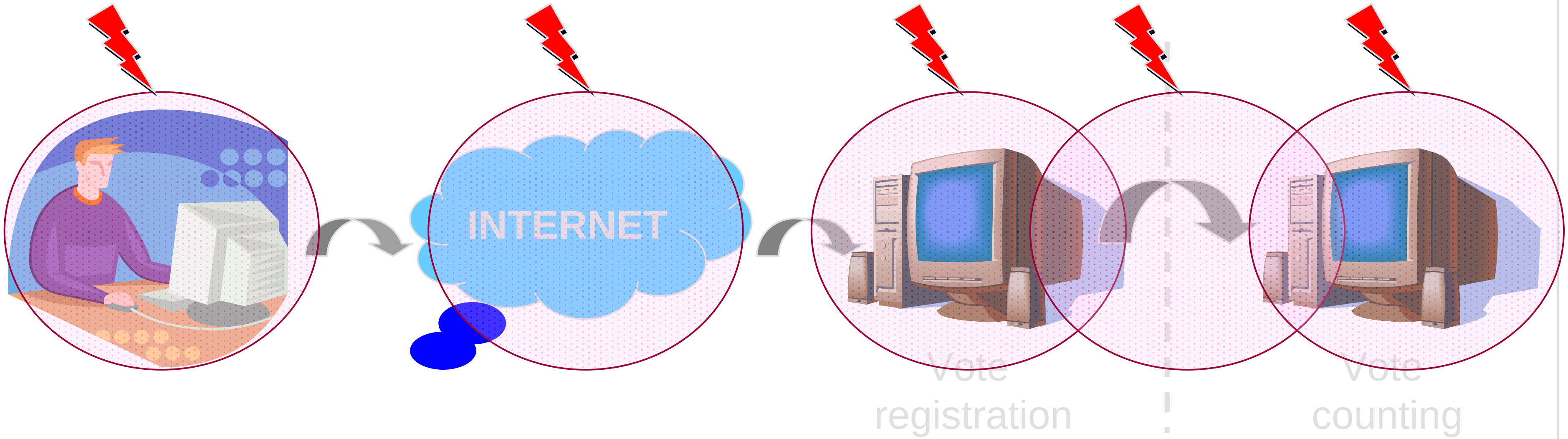
- accidental malfunctions

These include software bugs, hardware or network failures, leakage of confidential information

These are a significant challenge, but with care can be addressed.

- deliberate attacks, intended to disrupt or distort

An Internet voting architecture



e-voting attacks

It is assumed that we are dealing with remote Internet voting.

- Threats can be evaluated on the basis of:

  Motivation *(depends on importance of election? Remember “disruption”)*

  Ease of implementation *(given the precautions defined)*

  Preventability *(by technical or organisational means)*

  Detectability *(bearing in mind the constraints of the voting process)*

  Technical Recoverability

  Possibility of legal response *(=> deterrence)*

  Analogy with postal voting *(= how easy for non-technicians to evaluate)*

  Seriousness of consequences *(wrong results; cancellation; public image)*

  => overall evaluation of acceptability

The special case of voting

- Normal response:

Defence in depth:
- we validate system development ✓
- we test our systems ✓
- we verify a random subset of the results ✗
Anonymity of the ballot!

Usually:

1) the voter must not have documentary proof how he voted
2) no-one else must know how he voted

=> Straightforward verification is impossible

Threats: examples

Threat	Easy?	Prevent	Detect	Recovery	Response
Impersonating voters	Easy	Moderately difficult	Difficult	Yes	Sometimes possible
MITM attack between voter and central machine	Tricky	Moderately Difficult	Difficult	Yes	Possible
Hacking into central machine	Moderately difficult	Possible	Fairly easy	Probably possible	Very difficult
Corruption of central software	Internal cooperation	Difficult	Very difficult	Extremely difficult	Possible
Corruption of voters' software	V. difficult: preparation	Extremely difficult	Difficult	Probably impossible	Probably impossible
Attack on voters' machines ("Trojan")	Difficult	Virtually impossible	Very difficult	Probably impossible	Probably impossible

Key concepts for severe threats

1) Single point of vulnerability

2) Technological magnification

Threat: disruption by DDOS

Threat: I decide to disrupt the election by a DDOS attack

Ease of implementation: Not difficult, but probably needs long preparation

Prevention: Redundancy, and over-dimensioning servers

Detection: Trivial

Response: Legal deterrence probably ineffective

Analogy with postal voting: none

Seriousness of consequences: could be embarassing, but no worse, if the possibility has been taken into account initially

Evaluation: acceptable?

Threat: impersonation 1

Threat: I pretend to be a voter, without any special connection

Ease of implementation: Easy, but difficult to avoid detection

Prevention: identifying codes

Detection: some cases should be detected anyway; also random checking of voters by telephone

Analogy with postal voting: limited: we tend to assume that postal votes will get to the right house

Seriousness of consequences: very limited

Threat: impersonation 2

Threat: I pretend to be a voter, but am in fact his brother, etc.

Ease of implementation: Very easy

Prevention: Very difficult

Detection: Difficult

Analogy with postal voting: very close

Seriousness of consequences: probably limited

Evaluation: political decision to accept?

Threat: MITM/spoofing attack

Threat: My computer picks up the message from the voter to the central machine, and reads/suppresses/modifies it

Ease of implementation: difficult; requires special access and/or knowledge

Prevention: Encryption; DNS refreshing ...

Detection: For central system, difficult; for voter???

Analogy with postal voting: postal workers opening votes?

Seriousness of consequences: unless it can be executed on a large scale, limited

Evaluation: acceptable?

Threat: Hacking into central machine

Threat: I can remotely install software on the voting machine

Ease of implementation: Hacking happens every day

Prevention: With due attention (e.g. special-purpose operating systems with built-in firewalls) can probably be prevented

Detection: Can be detected with sufficient care

Analogy with postal voting: not really

Seriousness of consequences: unlimited

Evaluation: Must be prevented.

Threat: corruption of central software

Threat: A party worker works on the voting software…

Prevention: Social engineering, internal checks.

Detection: Examination of code, with integrity tests? Test runs? ... *may depend on complexity of system*

Response: Legal deterrence may be effective

Analogy with postal voting: Bribing the vote counters?

Seriousness of consequences: unlimited

Evaluation: Must be prevented.

Threat: corruption of voters’ software

Threat: A party worker works at Microsoft, and the screen routines have been “tweaked” to give us 3% advantage

Ease of implementation: Extremely difficult, with long preparation needed

Prevention: Virtually impossible if voters use proprietary software

Detection: Test runs; may be possible, but hard to be sure

Response: Legal deterrence ineffective

Analogy with postal voting: None

Evaluation: Ultimately political: “worthwhile for this election?”

Threat: attack on voters’ machines

Threat: I can remotely install software on the voters’ machines which will invisibly change their vote.

Ease of implementation: Not easy, but can probably be done. Difficult to predict success rate. The Trojan could delete itself afterwards.

Prevention: Boot voters’ computers off clean CD-ROMs. But is that acceptable? Otherwise hard to prevent.

Detection: Some well-informed voter might find it. Or could “honeypot” voters be set up to identify such an attack?

Response: Legal deterrence very difficult

Analogy with postal voting: brainwashing?

Evaluation: ???

A personal conclusion

- Without convincing mechanisms to cover against the most severe attacks, it will be hard to proceed to full-scale deployment of remote Internet voting at national or international level.
- These mechanisms could address either prevention or detection. It seems likely that ‘detection’ means ‘verification’.
- The mechanisms must be secure; they must also be useable. It would help enormously if they were comprehensible.

=>

Further work needed!