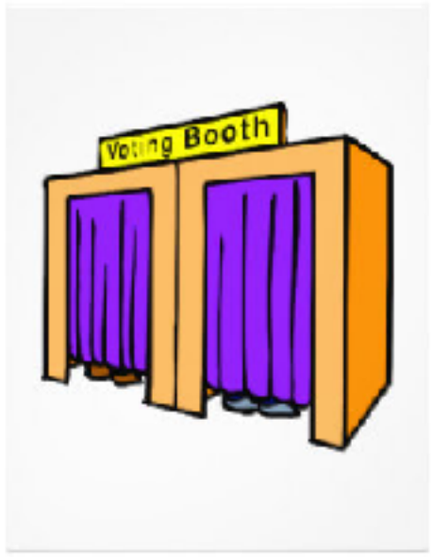
General Challenges of e-Voting

Aggelos Kiayias
University of Edinburgh

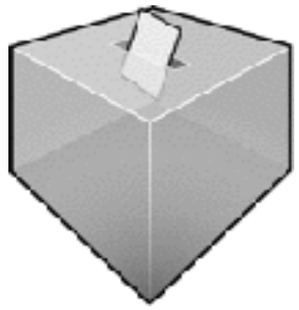
29 November 2017

Scottish Government and University of Edinburgh, School of Informatics Workshop

“Traditional” Voting



casting



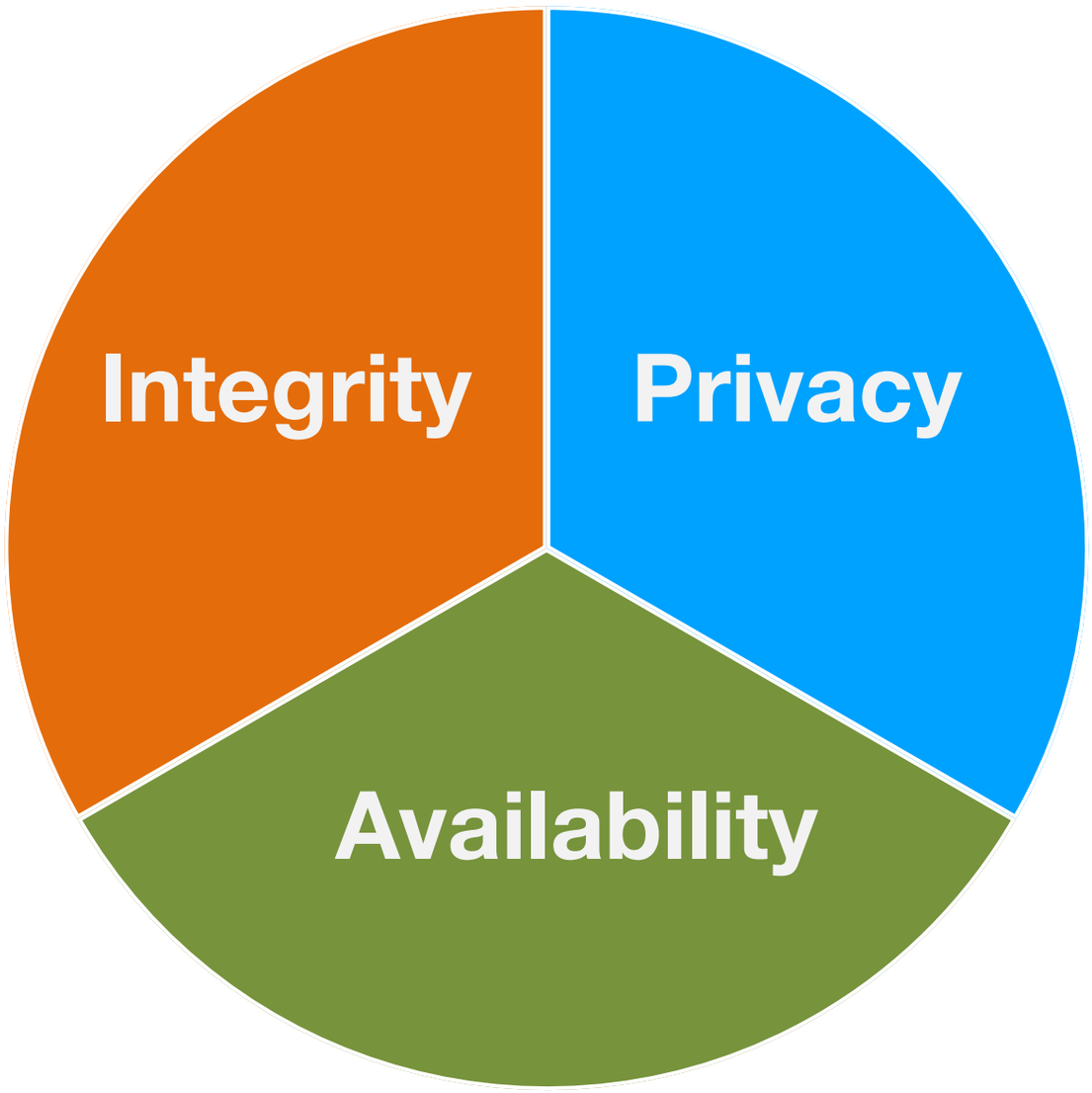
announcement

counting

auditing

identification

Fundamental Requirements of Voting



Traditional Voting & Requirements

- **Privacy** is guaranteed via physical means: (e.g., private booth, ballot box, opaque envelopes).

- **Integrity** is guaranteed via reliance on continuous oversight, (e.g., presence of accredited observers).

- **Availability** is guaranteed via procedural means: (e.g., announcing the election day ahead of time and allowing sufficient time to vote, ability of presiding officer to call the police).

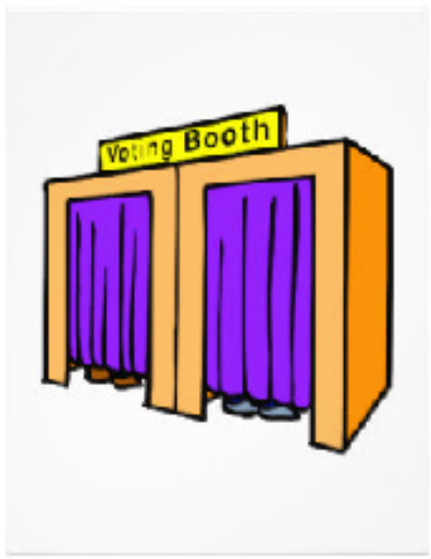
E-Voting

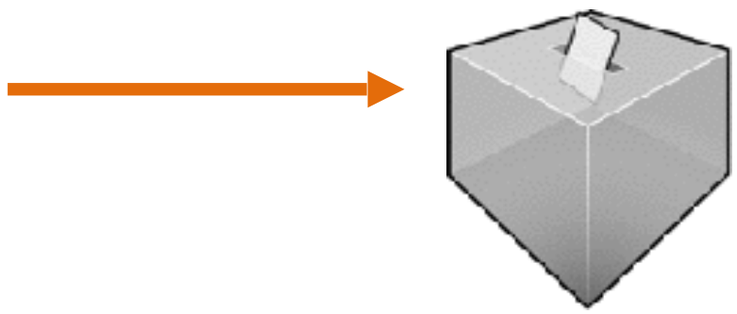
E-voting : using computers in at least one of the following three voting processes:

- Identification of voters
- Casting the vote
- Counting the vote
  - ~~(announcing / auditing)~~

Source: https://www.e-voting.cc/en/it-elections/definitions/

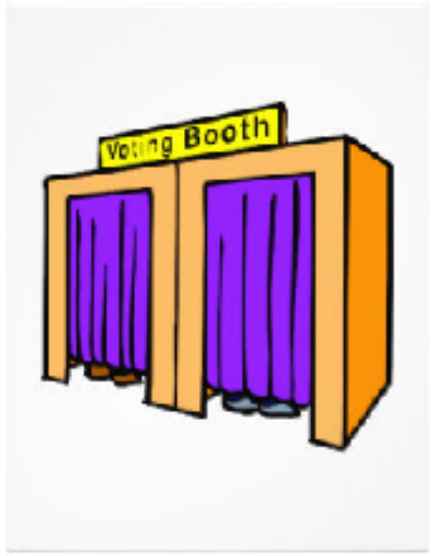
From Traditional Voting to E-voting

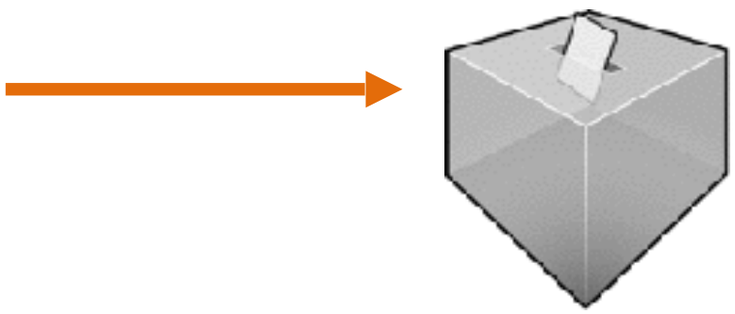




From Traditional Voting to E-voting

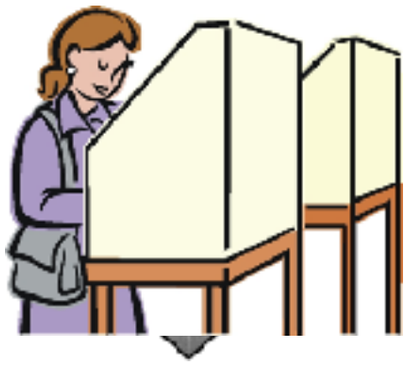
e-counting





From Traditional Voting to E-voting

ballot scanning / direct recording electronic



From Traditional Voting to E-voting

online voting

The benefits of e-voting

- Increase the participation of social groups that face considerable physical barriers.

- Increase the efficiency of the preparation of the election and the calculation of the final results.

- Reduce the financial cost of the elections (in long term).

The risks of e-voting

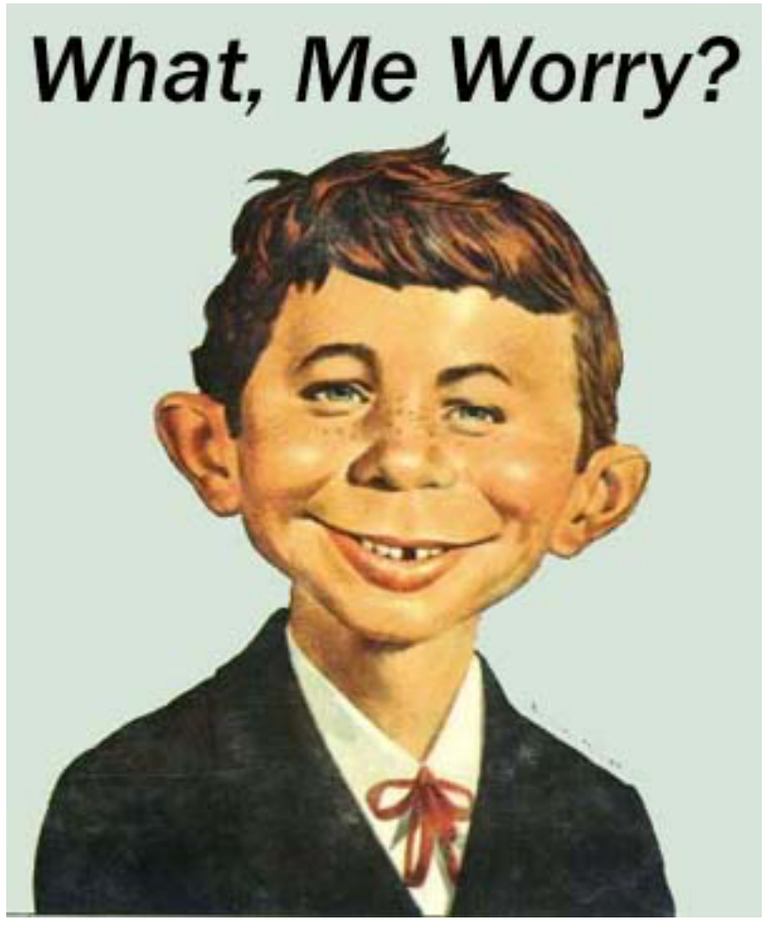
- Software vulnerabilities and/or the availability of digital transcripts may lead to privacy leaks. (~~privacy~~)

- Protocol and software vulnerabilities may lead to large-scale manipulation by a small group of insiders. (~~integrity~~)

- Interference (via electronic means) may cause denial of service & selective disenfranchisement. (~~availability~~)

- Auditing may require substantial technical expertise.

Is it really that bad?



we fly planes “by wire” so how come it’s hard to vote “by wire”?

Yes, it is!

- The adversary in voting can be **immensely more sophisticated** than in other settings.

- You may **never** know the system was hacked!

Is there a way forward?

…There is a way forward

- Modern cryptography provides a thorough methodology for designing and **formally establishing** the security of voting systems.

- Use it in order to extract and standardise the **proper specifications** of e-voting systems.

- Impose a **rigorous compliance regime** to the e-voting systems that are adopted.