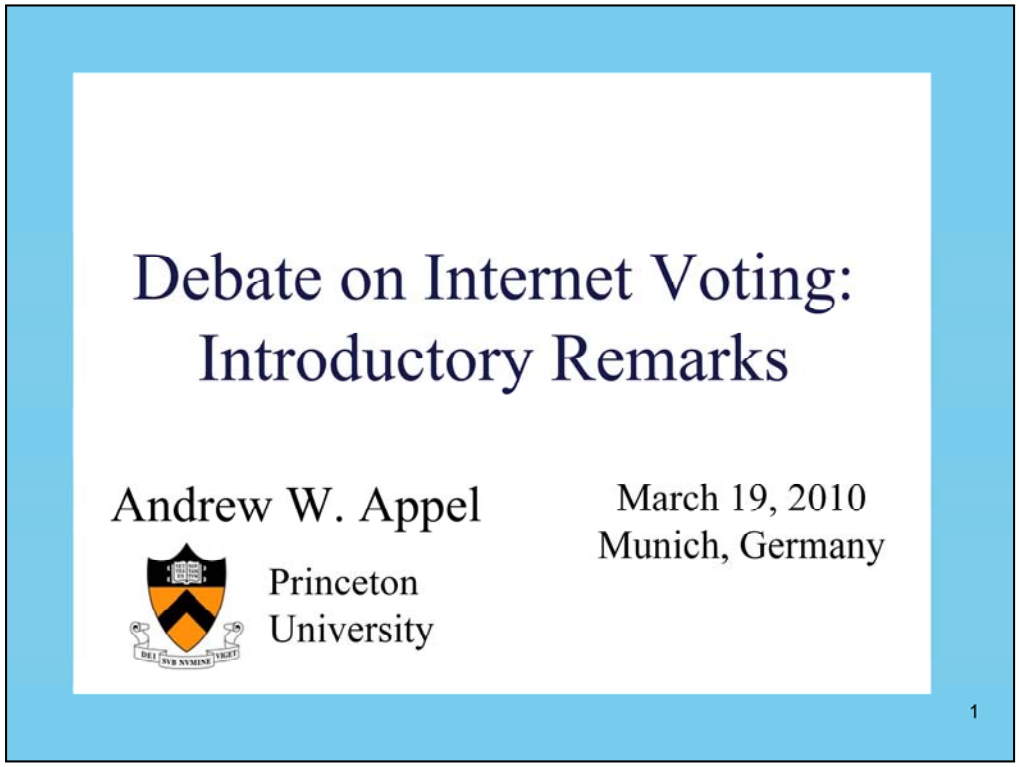


The Overseas Vote Foundation sponsored a debate on Internet Voting.

MODERATOR: Gregory Miller, Open-Source Digital Voting Foundation

INTRODUCTORY LECTURE: Andrew Appel, Professor of Computer Science, Princeton University

PROPONENTS:

Alexander Trechsel, Prof. of Political Science, European Univ. Institute, Florence

Christian Bull, Senior Advisor, Ministry of Local Government, Norway

Thad Hall, Associate Professor of Political Science, University of Utah

Tarvi Martens, Development Director at SK, Computer & Network Security, Estonia

OPPONENTS:

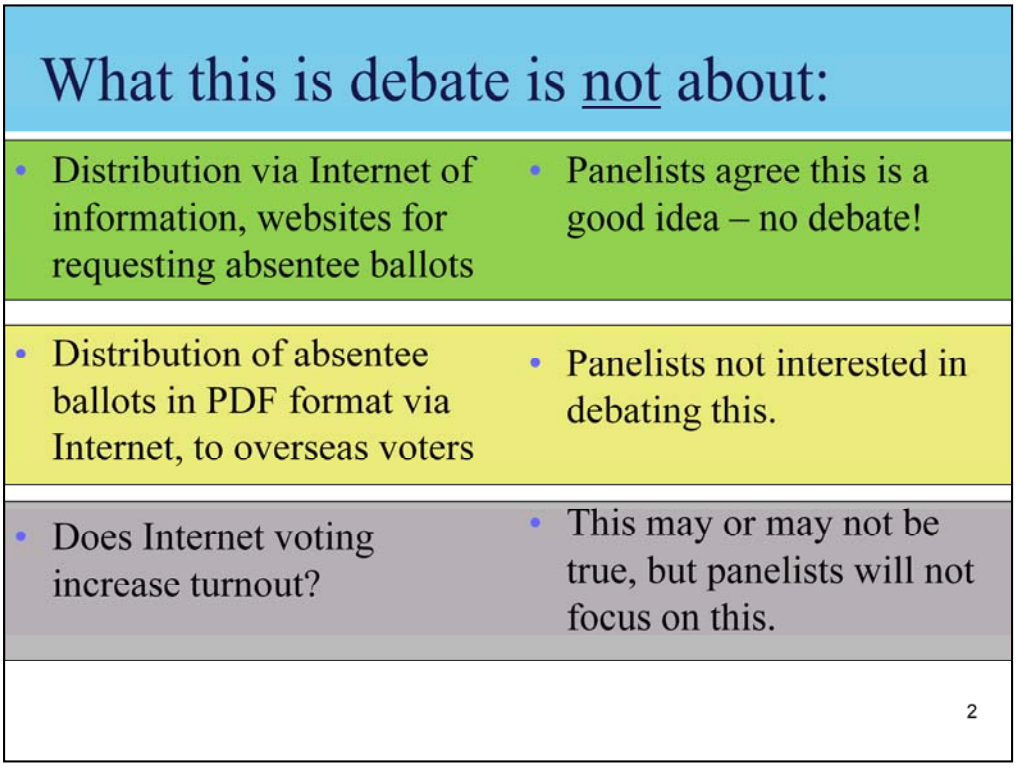
Harri Hursti, Expert on internet/computer/voting-machine security

Constanze Kurz, Engineer, Dipl. Inf., Humboldt University, Germany

Pamela Smith, President, Verified Voting

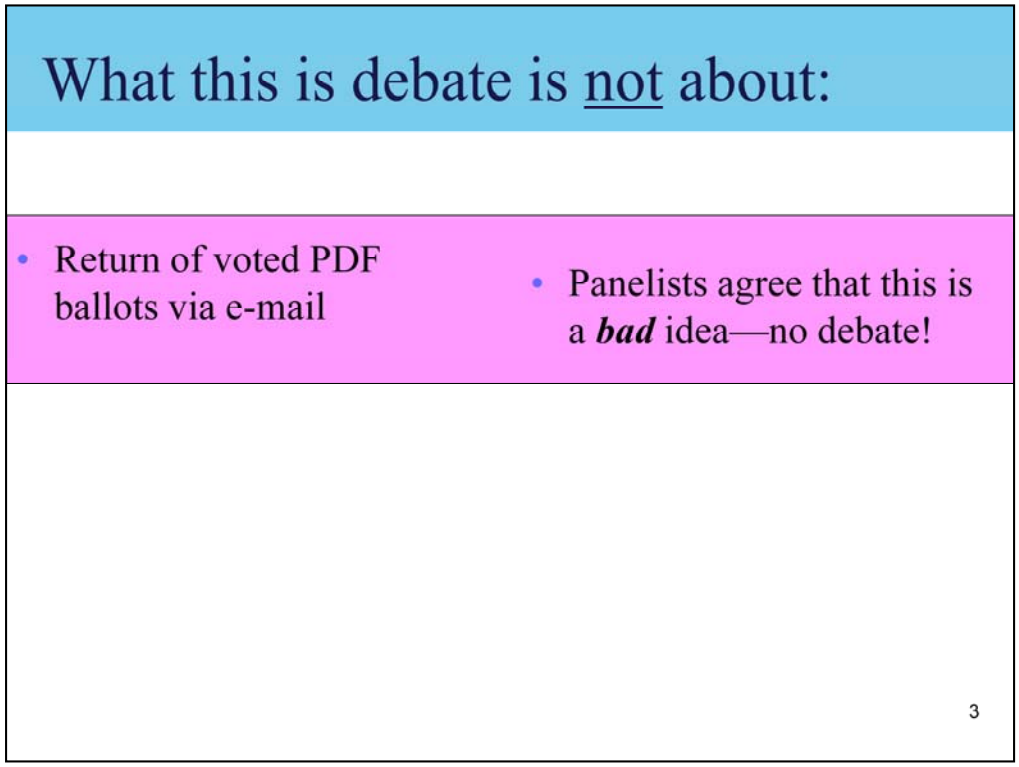
John Sebes, Open Source Digital Voting Foundation

CONCLUDING SPEAKER: Debra Bowen, Secretary of State, California



In the three weeks before this debate, Mr. Miller and I conducted a discussion by e-mail with all the panelists to find out where they agree and where they disagree, in order to focus the debate on the points of disagreement.

This debate is NOT about using the Internet to distribute information about how to vote, and how to register; all the panelists agree that this is a good idea. The debate is NOT about distribution of blank, unvoted ballets in PDF format to overseas voters; this may or may not be a good idea, but the panelists are not interested in debating it. The debate is NOT about whether Internet voting will increase turnout; there may be evidence that it does or does not, but the panelists will not focus on that topic.



Finally, all the panelists (proponents and opponents of Internet voting in this debate) agree that it is NOT a good idea for voters to return voted ballots to election officials in PDF format by ordinary e-mail. There is no debate here: this is NOT a desirable form of internet voting.

Why voting by e-mail is a bad idea

- **No privacy**— e-mail message is forwarded and reforwarded from one machine to another until it reaches its destination; any of these machines can read it.
- **No authentication**—Anyone can make up a set of "To/From" headers, there's no guarantee an e-mail is from the named sender
- **No integrity**—the contents of the e-mail may be modified at any of the "hops".

4

How did wood-and-paper-based voting achieve

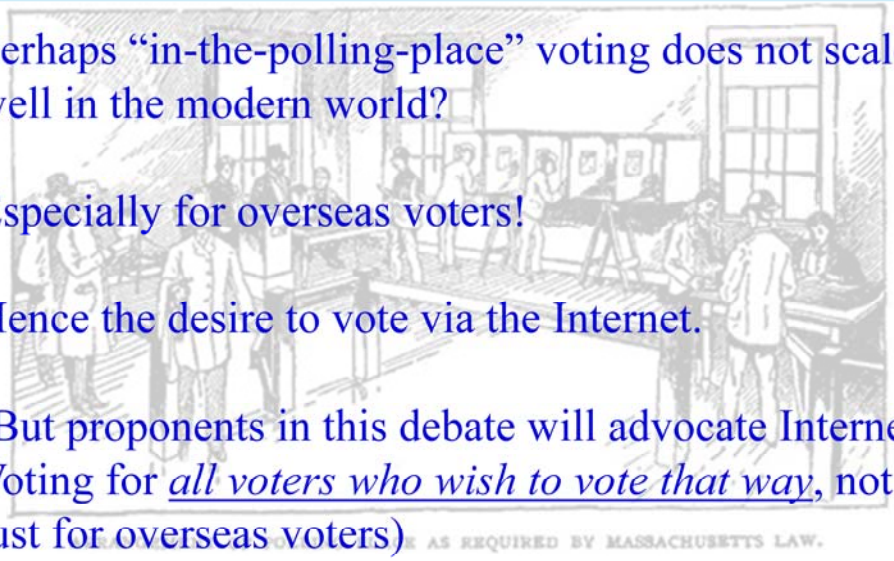
Authentication, Privacy, Integrity

ARRANGEMENT OF POLLING PLACE AS REQUIRED BY MASSACHUSETTS LAW.

From PETERMAN **1891** 5

Tradition "cellulose-based" voting technology, where all the components were made of wood and paper, achieved (or attempted to achieve) these desirable goals. Moving from right to left, we see AUTHENTICATION at the sign-in table where voters sign their name and receive their ballots; we see PRIVACY at the voting booths where they can mark their ballots without anyone looking on (the wooden guard rail helps with this too), and we can see INTEGRITY where the ballot box is being watched carefully by three different people, all day long. In actual practice, these three people watching the ballot box would be appointed by (respectively,) the two parties contesting the election and by the election officials, so they are watching each other as much as they are watching the ballot box.

Vote via Internet?



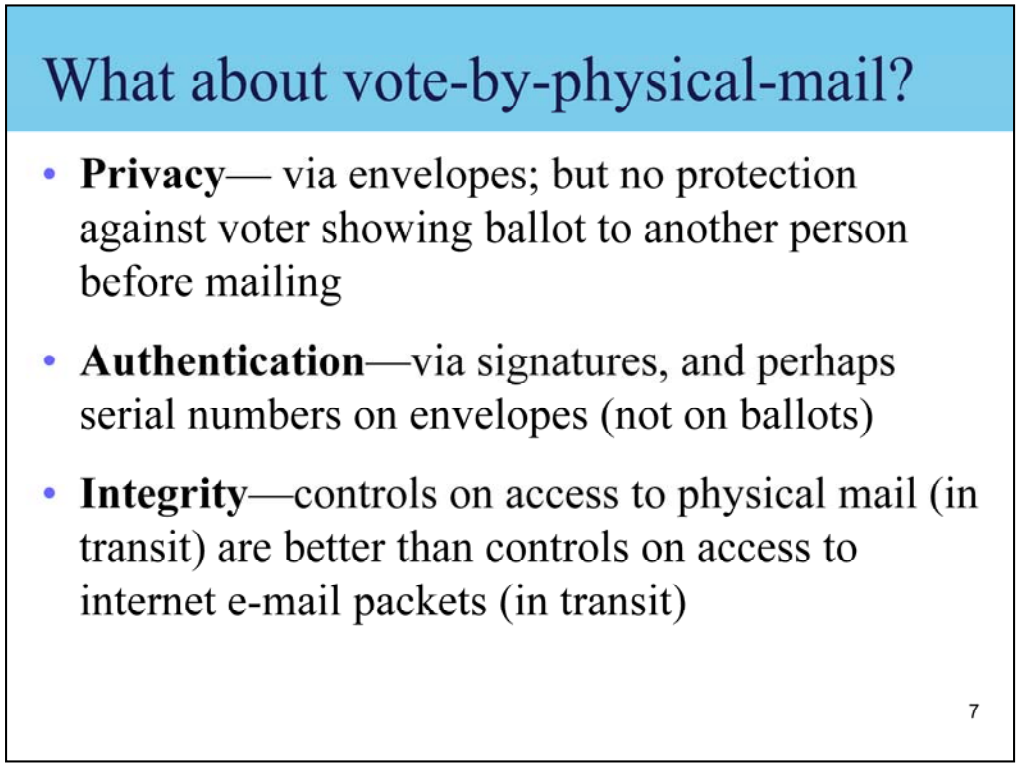
Perhaps "in-the-polling-place" voting does not scale well in the modern world?

Especially for overseas voters!

Hence the desire to vote via the Internet.

(But proponents in this debate will advocate Internet Voting for *all voters who wish to vote that way*, not just for overseas voters)

From PETERMAN **1891** 6



Paper absentee ballots cast by overseas voters have to go through the mail systems of at least two different countries. This is not perfectly secure, and may permit one or the other of those countries to tamper with the election. But it's significantly more secure than returning ballots through ordinary e-mail!

What about vote-by-physical-mail?

- **Priva**
  aga
  bef
- **Au**
  ser
- **Int**
  tra
  int

Absentee balloting via physical mail is not at all a perfect system. Some of the panelists have serious reservations about it; others do not.

However, all panelists have agreed that (for overseas voters) vote-by-mail is the most likely alternative to Internet Voting.

Panelists have agreed to exercise restraint in making objections to Internet Voting when those same objections would also apply to vote-by-mail with paper ballots and envelopes.

8

What this debate **is** about…

9

What this debate **is** about

"a client-server Web-based application that employs the public Internet to connect a server to a client,"

where the *client* is either

- HOME iVoting: "the voter's personal digital device (personal computer, cellphone, etc.)"

or

- KIOSK iVoting: "a dedicated system located and operated in a controlled public (nonresidential) environment"

10

What a voting protocol needs

- Allows each person to vote (just) once*
- Accurately records the votes
- Accurately counts the votes
- Voter can be sure his/her vote is counted, without trusting the other side's people
  - Even if the other side's people are election officials!
- Privacy
  - Can't learn how a person voted against his/her will
  - Can't learn how a person voted even with his/her cooperation!

11

One of the purposes of elections in democracies is to give the voters a chance to throw out "the Government". But election officials are appointed by, and part of, that very government that voters are voting for and against. Even if we know that election officials are people of the highest integrity, we must still design elections whose result can be trusted even without having to trust those election officials.

This is a difficult point to make without insulting the administrators of our elections. Of course no insult is intended, and in general these officials and government employees are dedicated, competent, hardworking, and fair. But the principle remains: we must be able to trust the elections without trusting any particular individual.

"Privacy" comes in two forms. "Weak privacy" means that you can't learn how the voted _without_ her cooperation. "Strong privacy" means that even with the voter's cooperation, the voter cannot prove to you how she voted. The reason we need BOTH forms of privacy is that otherwise, you could coerce or bribe a voter to cast her ballot a certain way.

*See slide 32 for an explanation that "Allow each person to vote just once" means, more precisely, "count just one ballot from each voter".

What a voting protocol needs

- Allows each person to vote (just) once
- Accurately records the votes
- Accurately counts the votes
- Voter can be sure his/her vote is count
  trusting the other side's people
  - Even if the other side's people are electio
- Privacy
  - Can't learn how a person voted against hi
  - Can't learn how a person voted even with his/her cooperation!

Designing a protocol that can achieve all of these at once is a ***difficult*** problem!

12

Cellulose-based voting protocol

attempts to achieve all these at once:

ARRANGEMENT OF POLLING PLACE AS REQUIRED BY MASSACHUSETTS LAW.

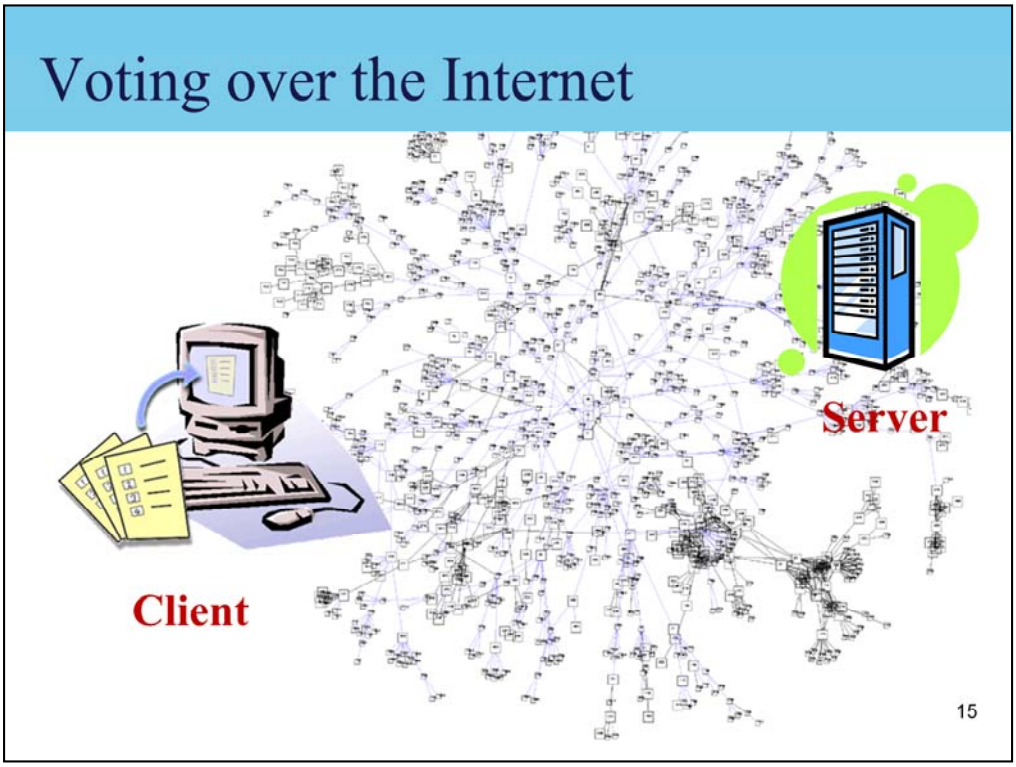
From PETERMAN **1891** 13

Different components of the traditional polling place are there to achieve these different goals. In particular, each political party has a person at the sign-in desk checking who's allowed to vote, and each party has a person watching that ballot box! Those "pollwatchers" or "challengers" will also want to make sure that the ballot box is empty before the first vote is cast, and will witness the count of the paper ballots.

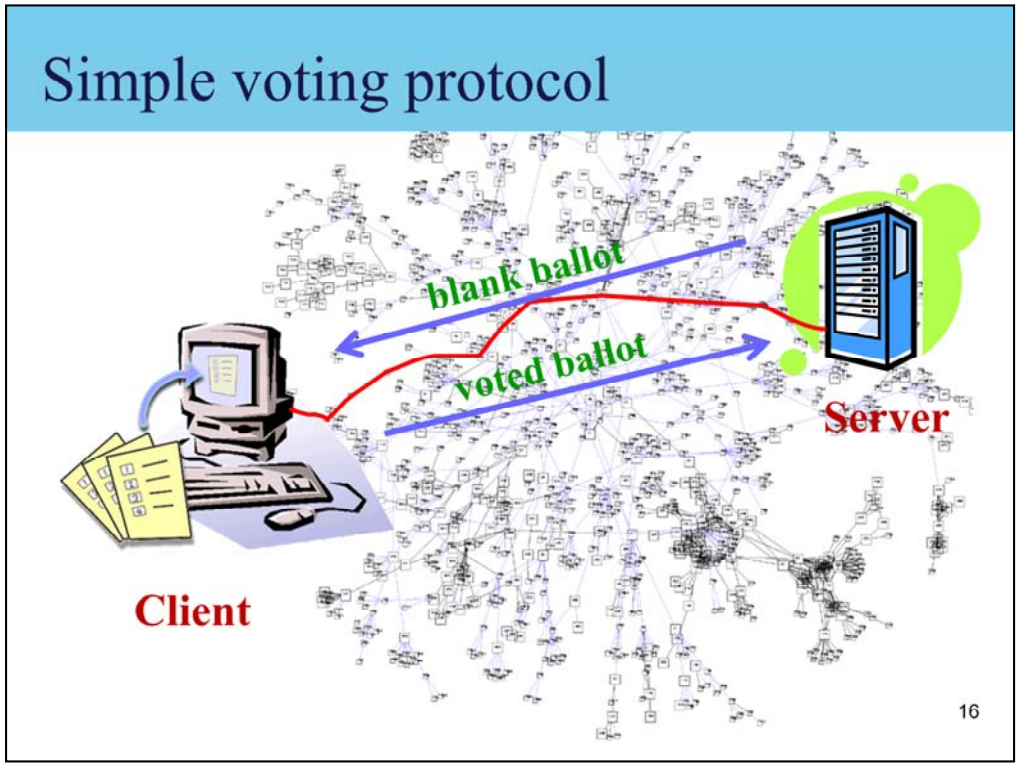
In the rest of my talk:

I will explain some technical challenges for the trustworthiness of Internet Voting. The panelists can debate whether these challenges can be addressed successfully; they will also debate other issues posed by the moderator.

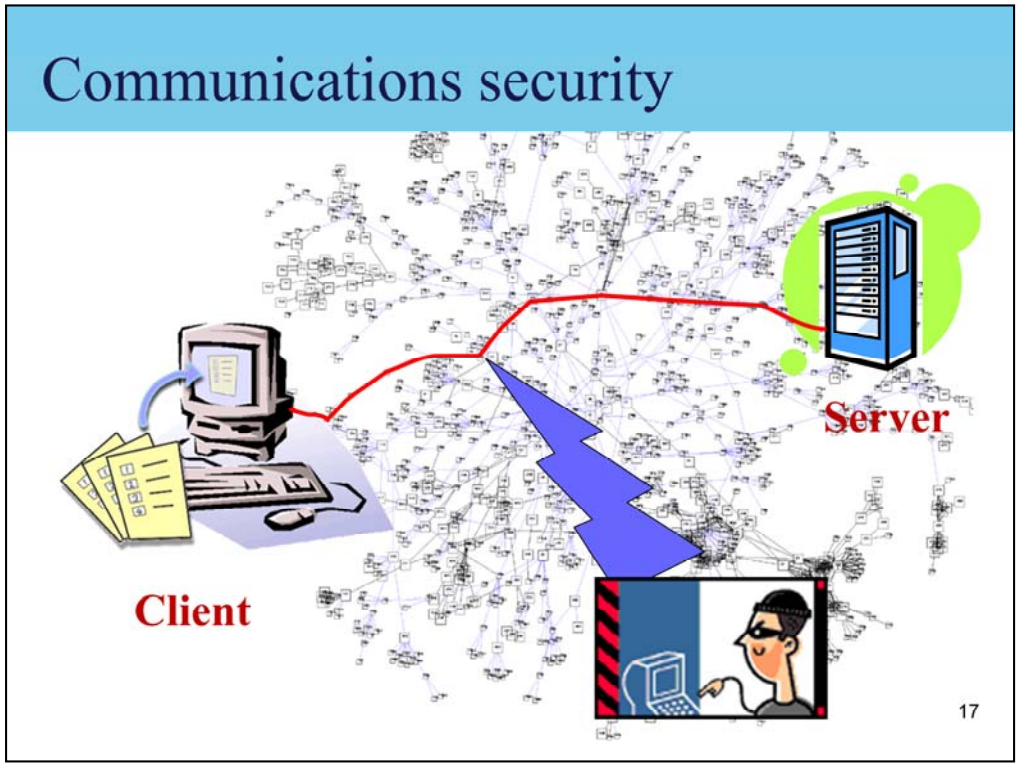
14



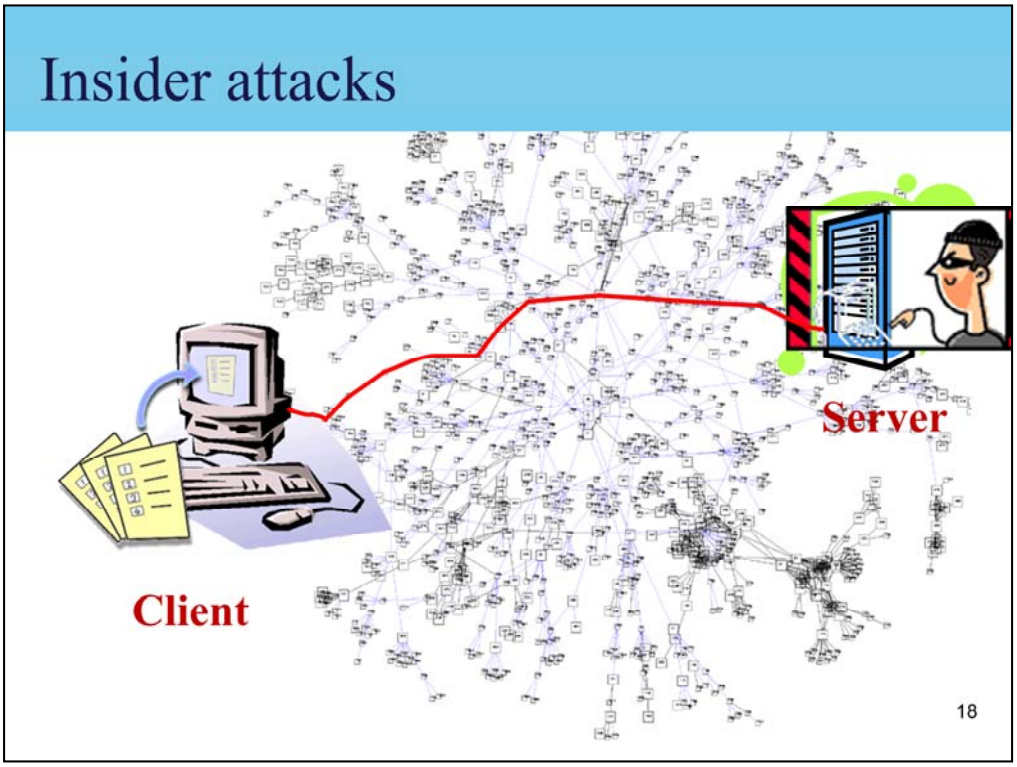
Client and server computers communicate over the internet by sending “packets” of information that hop from one Internet host to another.



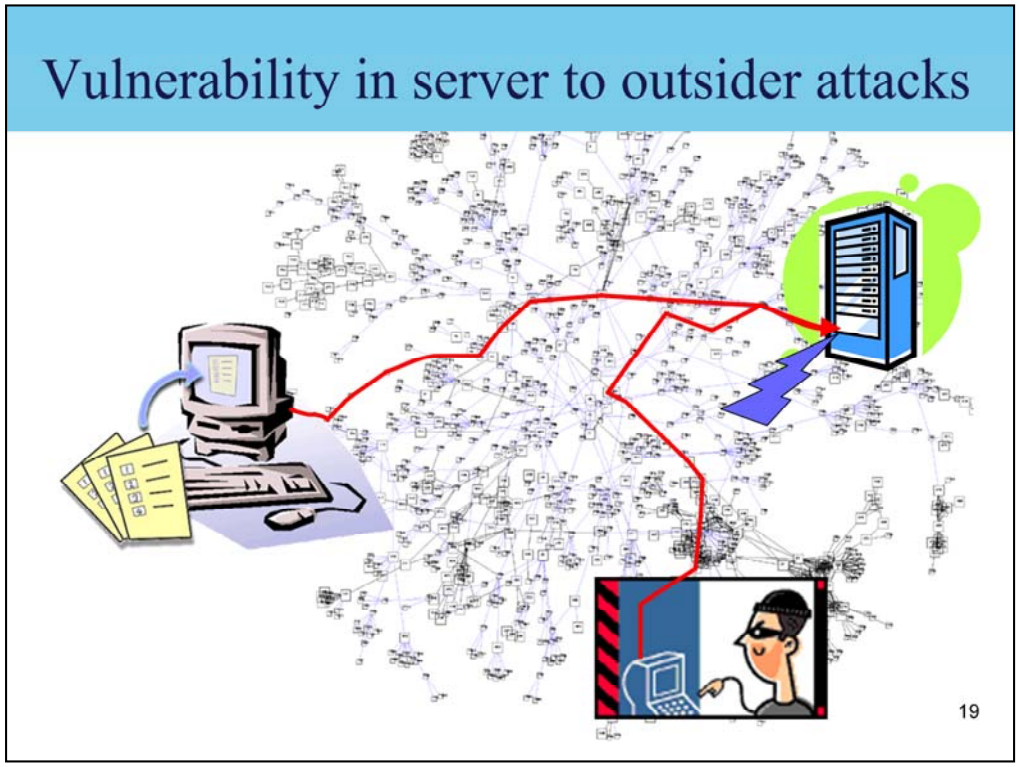
In this vastly simplified depiction of an Internet Voting protocol, the blank ballot (listing the candidates in an election) is sent from the Server to the Client, then the voted ballot is sent from the Client to the Server.



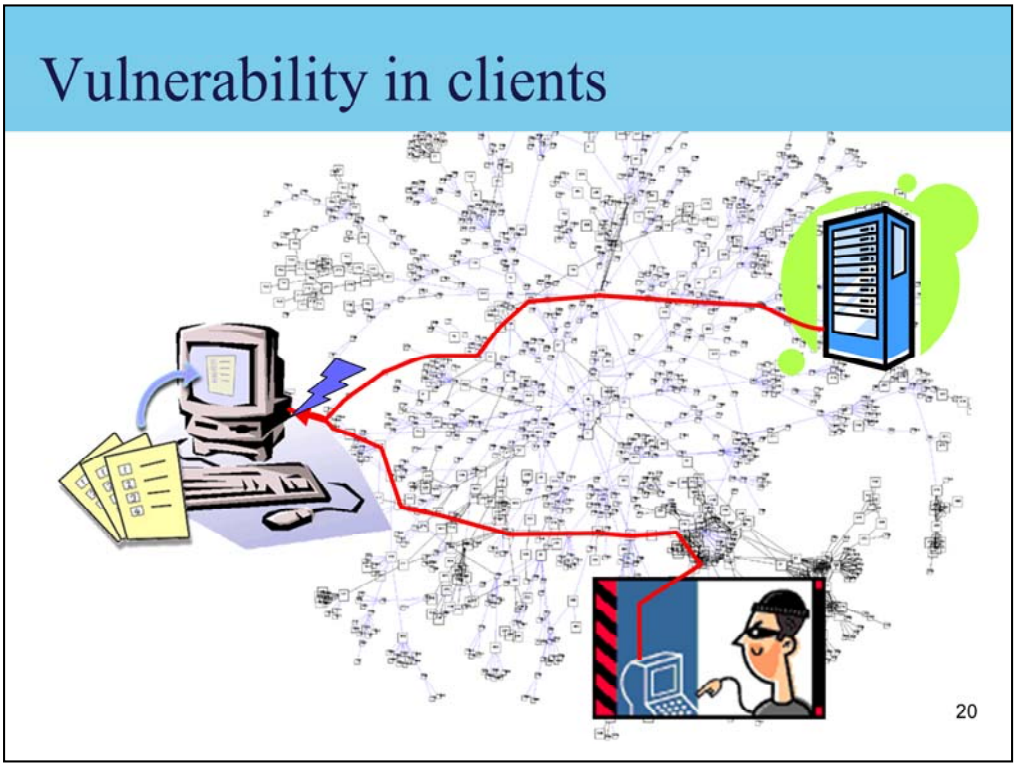
Since the packets pass through many computers on their way from Client to Server, we might wonder whether somebody can tamper with the ballots along the way. (Or write a computer program that tampers with the ballots as they go by.)



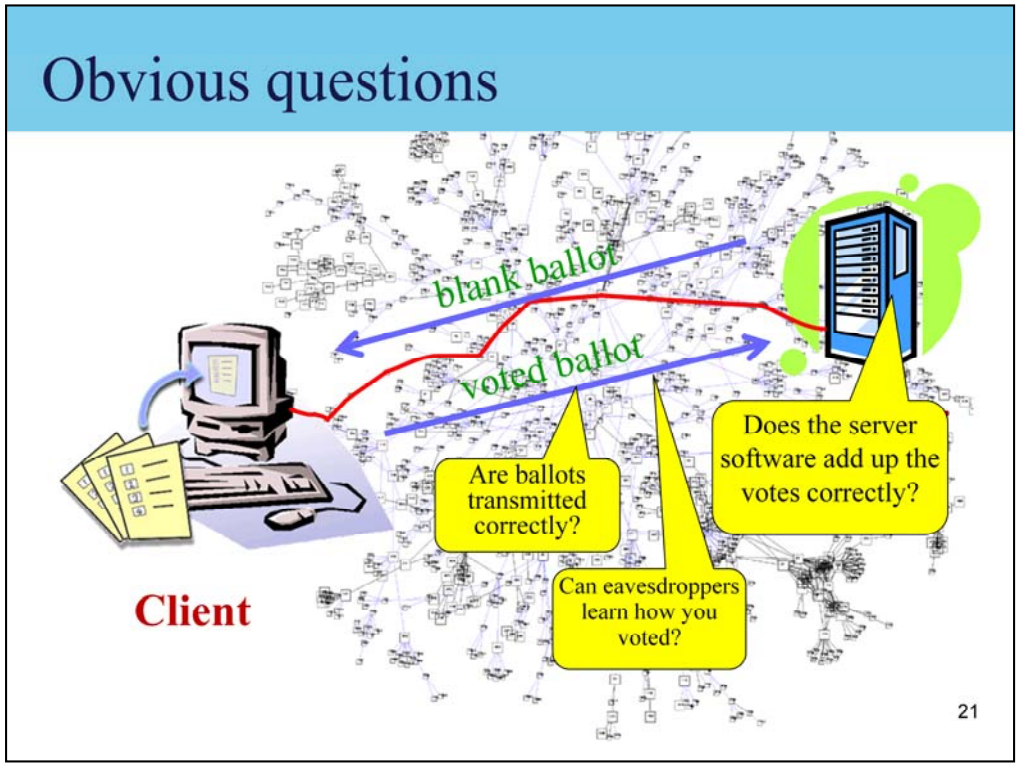
Inside the server computer, there is a computer program that receives the ballots and adds up the votes. We might wonder, “who installed that program?” “Can someone install a program that pretends to add up the votes, but instead manipulates the results?”



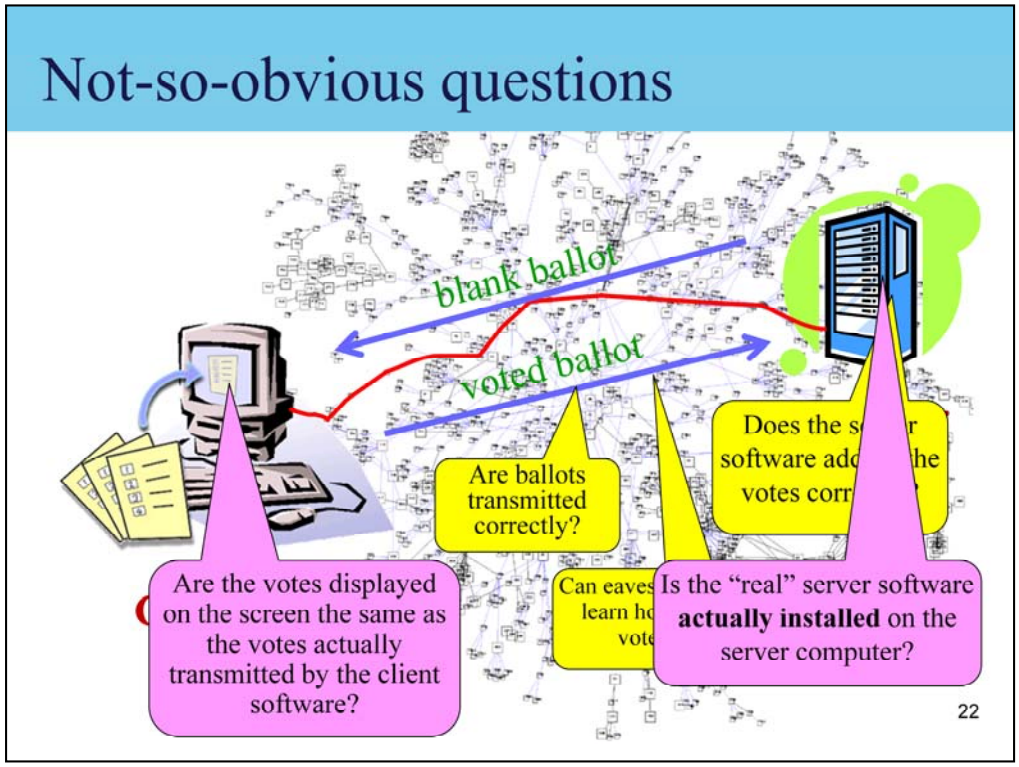
Since the server computer communicates on the Internet, we can ask whether it is vulnerable to hackers from the outside that can gain enough access to be able to fraudulently modify the software inside the server (and thus manipulate the results of the election).



We know that thousands of computers across the Internet have been plagued by computer viruses. Estimates are that more than 10% of computers around the world have been infected, and are part of “botnets” that (unbekownst to the owners of these computers) are using them for fraudulent purposes such as forwarding Spam e-mail.

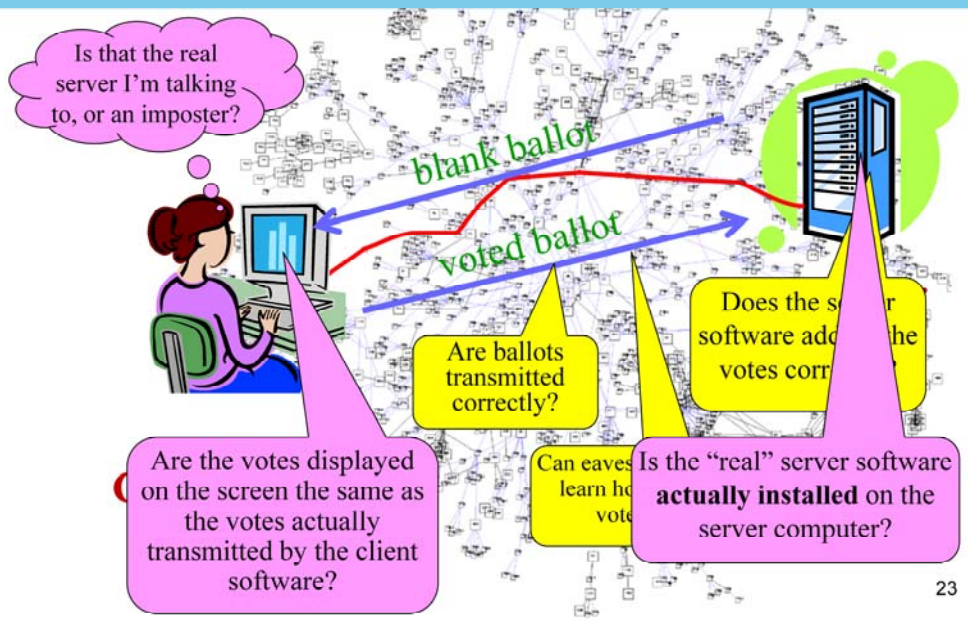


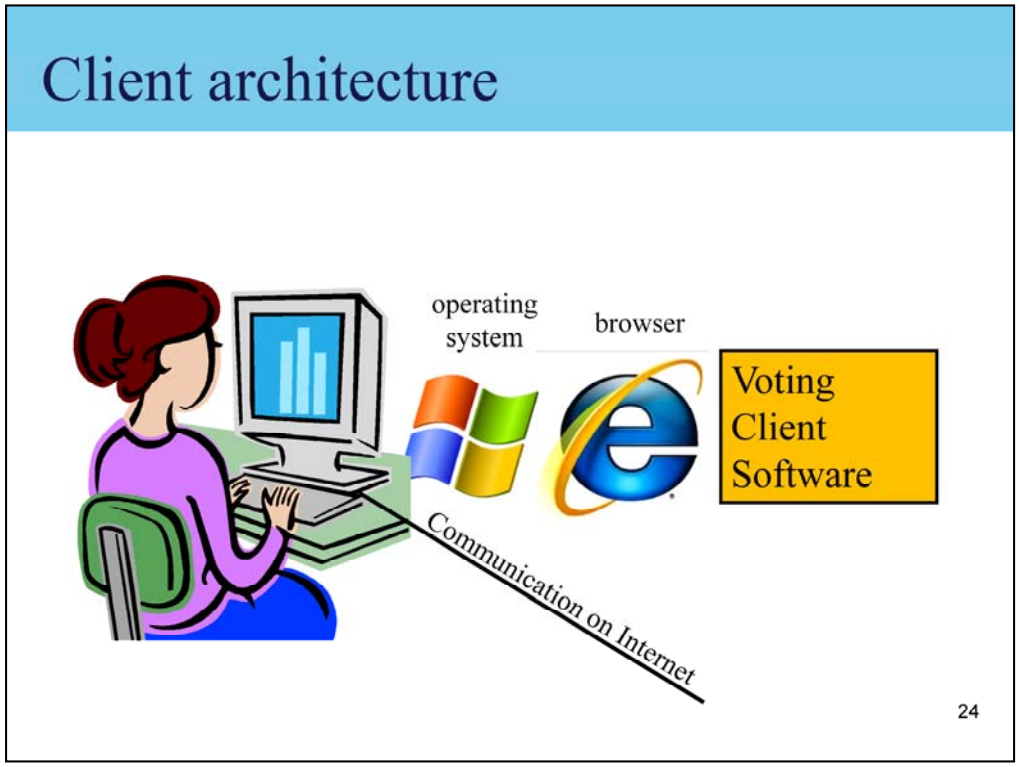
So, these are some of the questions that the panelists in today's debate might want to address.



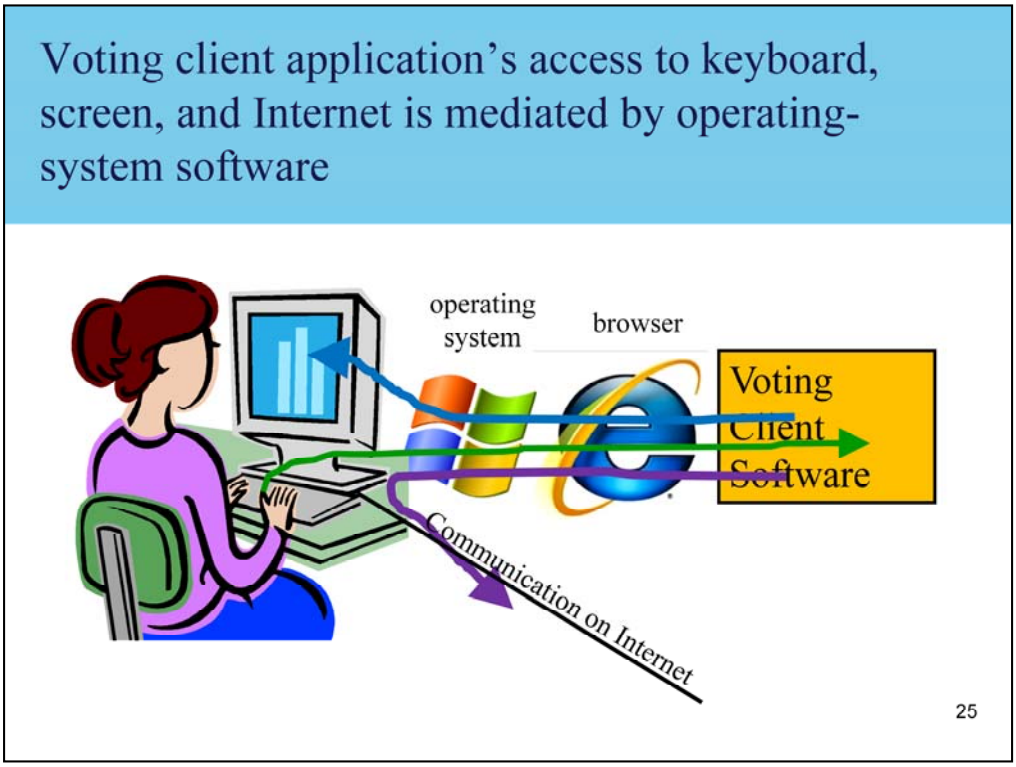
But after the "obvious" questions, there are these "not so obvious" questions that are just as important!

Not-so-obvious questions





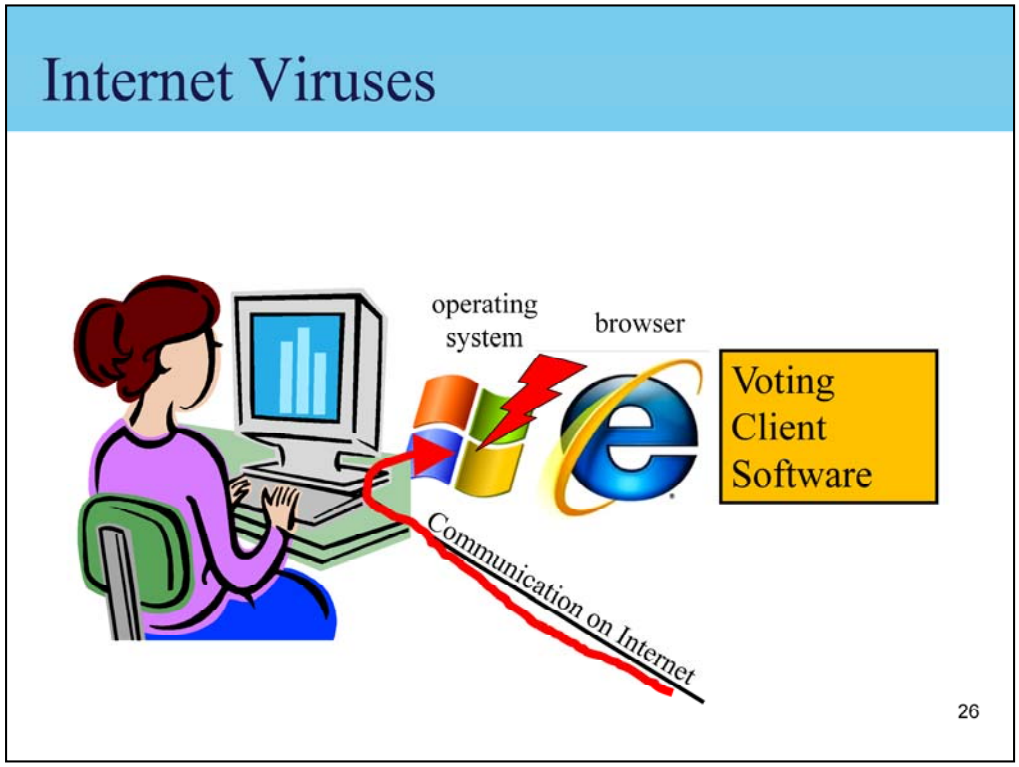
Because the question of “client computer security” is so important, I will take a few minutes to explain the internal architecture of the client. The “Voting Client Software” on your computer runs (typically) inside your internet browser, which runs on top of the operating system (such as Microsoft Windows, MacOS, or Linux).



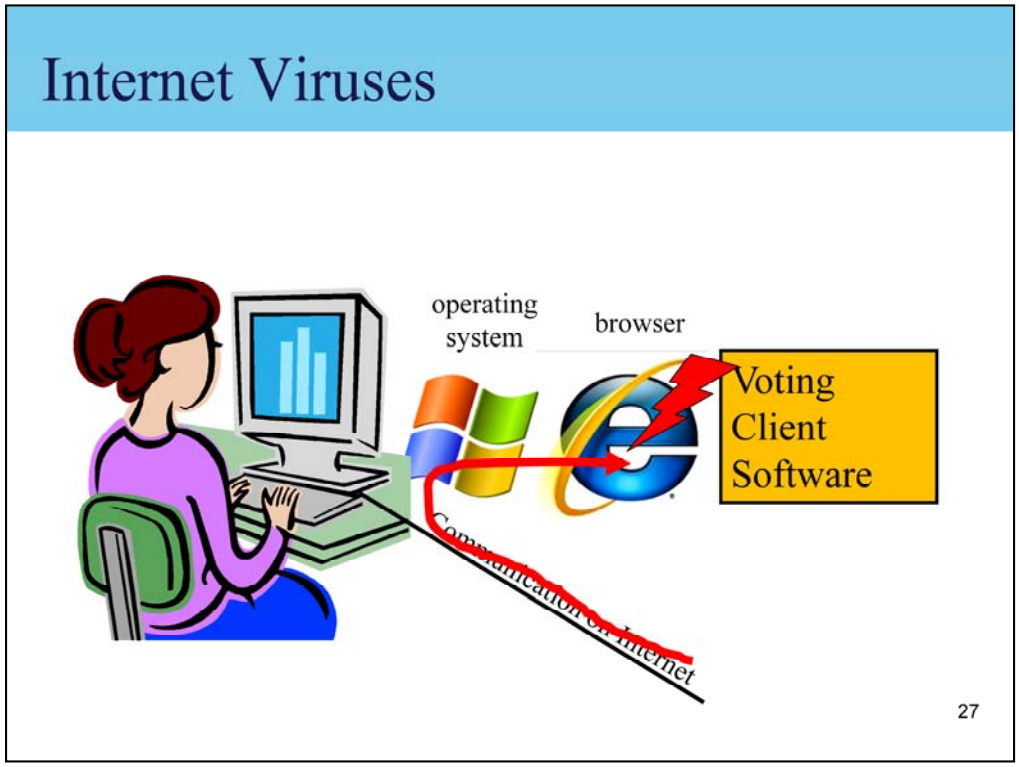
When you press a key on the keyboard or click the mouse, the application software (Voting Client Software) can't see that directly. Instead, the operating system controls the keyboard and mouse, and passes the information on to the browser, which passes it on to the Voting Client Software.

Similarly, when the Client Software wants to indicate a mark on your ballot, it can't paint onto the screen directly. It must pass its request through the browser, which passes it on to the operating system, which paints the screen.

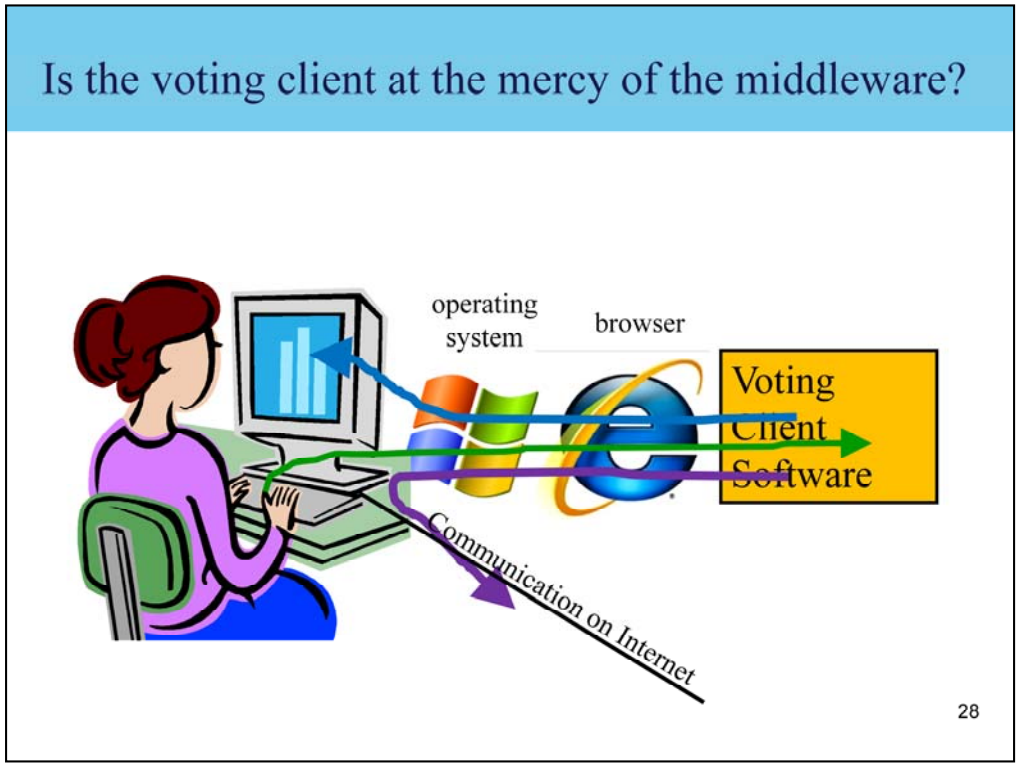
Finally, when the Voting Client Software wants to transmit your ballot over the Internet to the Server, it must do that through the browser and through the operating system, as well.



Frequently, people discover security vulnerabilities in the operating system that allow hackers on the internet to install fraudulent software inside your computer, just by sending Internet packets to the operating system. The operating-systems makers respond by fixing their operating systems to remove those particular vulnerabilities, and sending the improved version of the operating system to your computer. But in the meantime, its common for computers to be in a "hacked" state without their owners knowing it.



The same kind of vulnerabilities also exist in Web browsers.



The fact that every step of the operation of the Voting Client Software is mediated by (possibly hacked) operating systems and browsers means that: it's possible that the votes that you click on, and that are indicated on your computer screen, are not the same as the votes that are packaged up and sent over the Internet to the Server.

Insecurity of home PCs leads to consideration of "kiosk" iVoting

- "a client-server Web-based application that employs the public Internet to connect a server to a client,"

where the *client* is either

- "the voter's personal digital device (personal computer, cellphone, etc.)"

or

- "a dedicated system located and operated in a controlled public (nonresidential) environment"

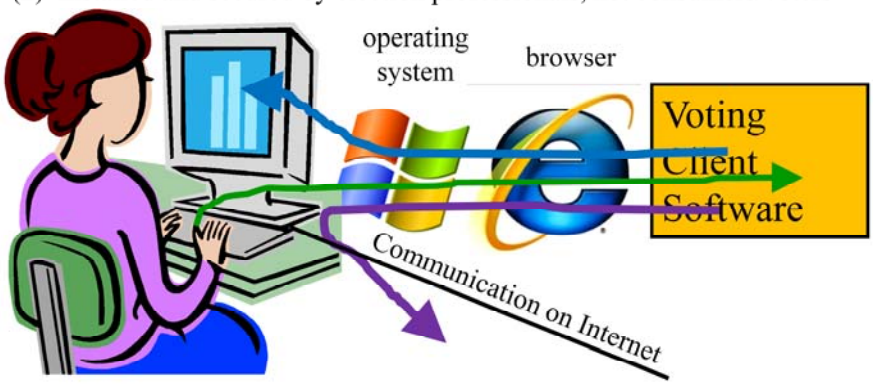
29

"Kiosk" has same architecture as client!

Subject to same attacks on operating system; but more secure because:

(1) Not used for promiscuous Web-surfing and personal e-mail

(2) Installed and secured by election professionals, not consumers/voters

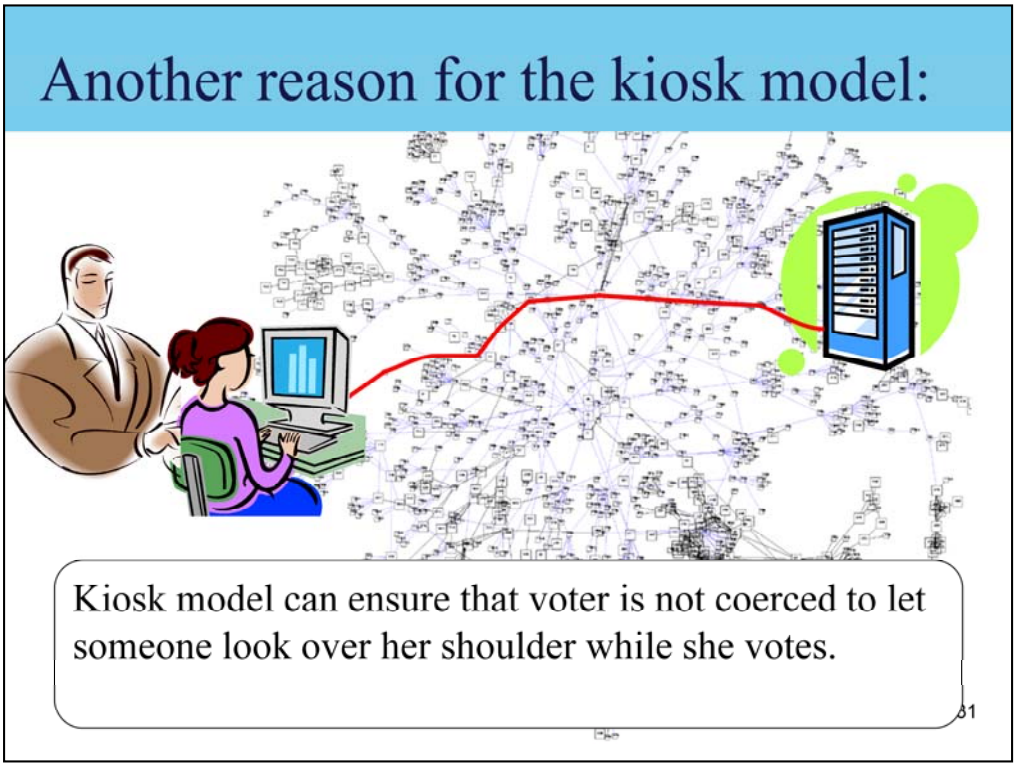


Is the Kiosk adequately secure for elections?

We'll let the panelists debate this!

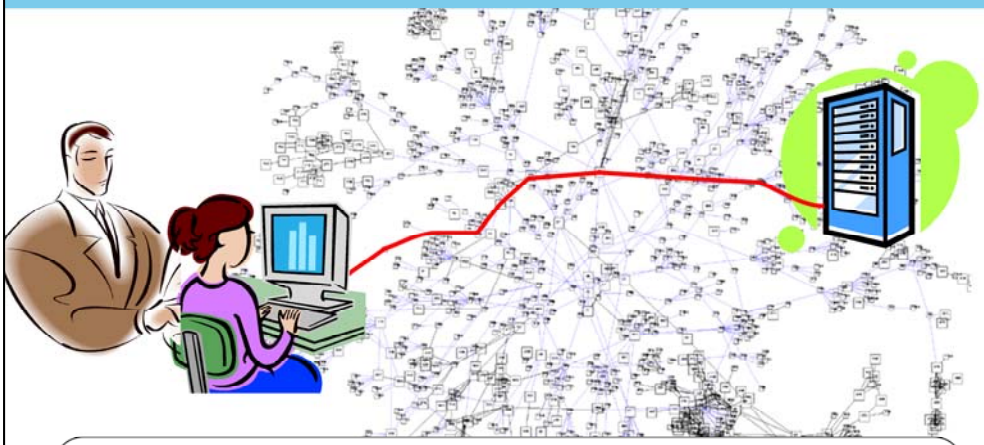
30

I'll remark here that the two "PROPONENT" panelists who actually deploy Internet Voting for their own countries (Mr. Martens of Estonia and Mr. Bull of Norway) are both deploying HOME iVoting solutions. Neither of them is in favor of the Kiosk model.



Since the Kiosk is in a public place controlled by election officials, they have the opportunity to arrange that place so that no one can look over your shoulder.

An idea for privacy in HOME iVoting



Let the voter cast her ballot as many times as she wants; only the last time counts.
Is this effective? We'll let the panelists debate it.

The ballot box

ARRANGEMENT OF POLLING PLACE AS REQUIRED BY MASSACHUSETTS LAW.

From PETERMAN **1891** 33

In the traditional voting solution, the ballot box is not very complex. The witnesses to the election (representing the contesting political parties) can see for themselves that it is empty at the beginning of the day, that each voter deposits just one ballot, and that the votes counted at the end of the day actually came out of the ballot box.

Transparency

Witnesses to an election need to be able to see that:

Ballot box is initially empty
Each voter deposits 1 vote
Only legitimate voters cast a ballot
Ballots counted are the ones cast
The votes are counted accurately

"Witnesses" include:
Election officials, Party representatives,
Candidate representatives, members of the public.

34

In France, the ballot box is literally transparent, so that anyone in the room can see that it's empty at the beginning and that each voter deposits just one envelope.

Opacity

Can one (election officials, the public) really know what software is really installed and running in the server computer?

We'll let the panelists debate this!

35

In my opinion, this is one of the most important questions to address in this debate.

End-to-end protocols

- Can we avoid the need to fully trust the client and server computers?
- Idea: Let each voter (digitally) sign her ballot, and post every ballot on a public (Internet) bulletin board.

Accurate and trustworthy: Each voter can verify that her ballot is present; any member of the public can add up all the posted votes and reconfirm election results.

Complete loss of voter privacy!

36

Cryptographic end-to-end protocols

- Idea: Let each voter (digitally) sign her ballot, and post every ballot on a public (Internet) bulletin board. **But use special-purpose encryption protocols to avoid loss of voter privacy**

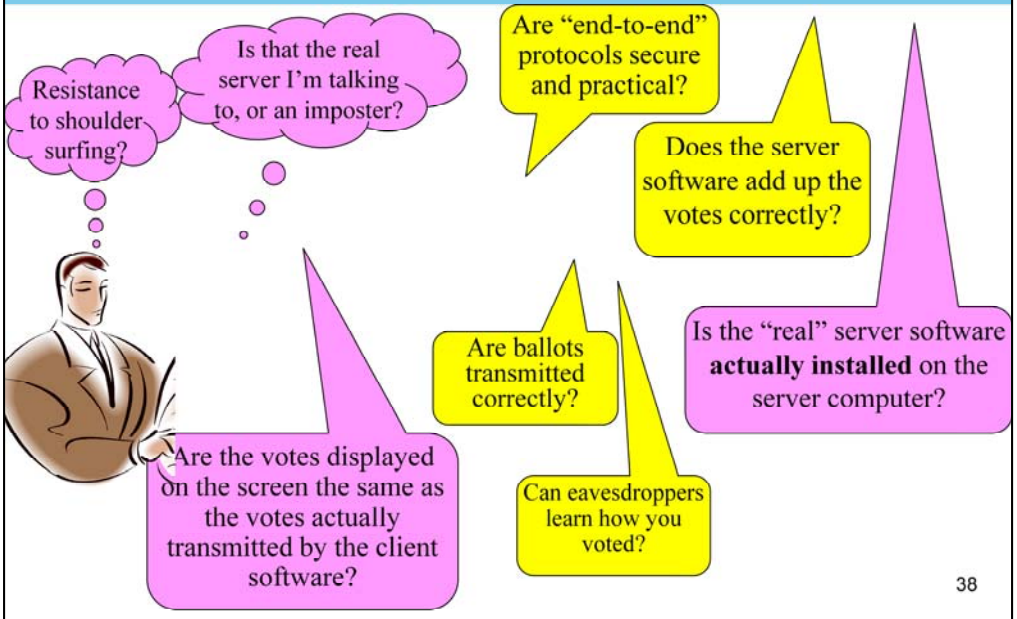
Each voter can verify (probabilistically) that her ballot is (very likely) present; any member of the public can add up all the posted votes (probabilistically) and reconfirm election results.

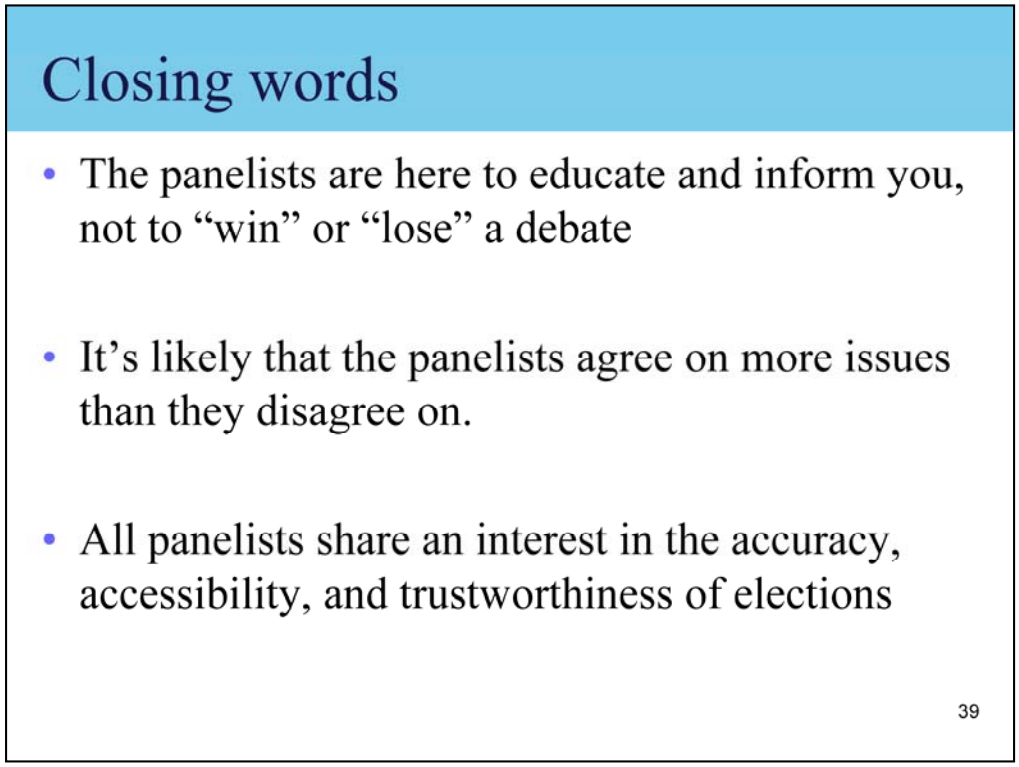
Do these protocols actually work? Can they be explained to voters and policymakers? Are policymakers able to evaluate these protocols? Are there hidden vulnerabilities?

The panelists may debate these issues. But the panelists recognize that complicated technical issues cannot be covered very well in today's debate format.

37

Questions for debate





All of the panelists (PROPONENTS and OPPONENTS) were given a copy of these slides several days in advance of the debate. The panelists agreed that these slides laid out the important questions. During the debate itself, of course, they disagreed about the answers to some of these questions (and to other questions posed by the debate moderator, Mr. Miller).