Ceci n'est pas une urne:

On the Internet vote for the *Assemblée des Français de l'étranger*

Andrew W. Appel*

June 14, 2006, Rocquencourt, France

Executive Summary

On Monday, June 5, 2006, I attended a training session for *assesseurs* (poll watchers) of the world-wide Internet election for the *Assemblée des Français de l'étranger*. This *Assemblée* will in turn elect 12 members of the French Senate, so the legitimacy of this election is important even to citizens residing in France. I observed many things about the process of the election that will make it impossible for the *assesseurs* to certify with any confidence that the election is conducted accurately and without fraud.

In a normal French polling place *(bureau de vote)*, there are many safeguards, and every safeguard is there because in the past, without the safeguard, there was cheating in elections. Many countries around the world—not just France—have experienced cheating in elections, and many countries have very similar safeguards. Therefore, it is important that the *(assesseurs)* can see with their own eyes that the ballot box *(urne)* is empty at the beginning of the day—because there was ballot-box stuffing in the past. They can see with their own eyes that the voter enters the voting booth *(isoloir)* alone—because in the past there was vote-selling and coercion of voters. The *assesseurs* can see that the voter deposits just one ballot in the ballot box—in fact, the ballot box is even transparent to make it easier to monitor—because in the past there was cheating. The *assesseurs* can hear that no one except a voter deposits a ballot, because a bell rings every time the slot is opened. They can see that the votes are counted accurately at the end of the day—votes are counted in public because there was cheating otherwise—and what is counted are physical paper ballots that everyone can understand and everyone can see. Therefore, when the poll workers and *assesseurs* report results

*About the author: Andrew W. Appel is Professor of Computer Science at Princeton University in New Jersey, USA. From July 2005 to July 2006 he is a visiting professor at the *Institut National de Recherche en Informatique et en Automatique*, the French national computer-science research laboratory, at Rocquencourt, France. Professor Appel does research and teaching on computer security and has taught a course at Princeton on the history and technology of voting.

at the end of the day, these results are accepted as legitimate because everyone can see and understand every part of the process. There are many safeguards in this process, every safeguard is there because without it there was cheating in the past, and every safeguard is one in which the *assesseur* participates directly.

In contrast, the process of an Internet election—this Internet election for the *Assemblée*—has no safeguards that the *assesseurs* can assess directly. The election is conducted on machines built by EADS and operated by Experian in a room in Aix-en-Provence, and monitored remotely by the *assesseurs* in a room in Paris. From Paris the *assesseurs* see a video image, purportedly from a camera in Aix, showing an *urne*—but not a physical *urne*, but a room full of computers. They see also a web browser in Paris purporting to show data from the computers in Aix: the number of votes already in the virtual *urne* database, the number of voters who are registered, the number of voters who have already voted.

Computers can be programmed to simulate almost any phenomenon. A computer program can conduct an accurate election or a fraudulent one. Every ballot cast on the Internet is received and processed by a computer program on a web server in Aix. **It is very easy to write a computer program that will receive a voter's ballot for candidate A and deposit in the *urne* a vote for candidate B.** The *assesseurs* have no way of knowing what program is installed on the computers in Aix that run the election, because EADS guards that program as a trade secret and will not show it to the *assesseurs*. Even if EADS showed them the program, the *assesseurs* have no way of knowing whether the program showed to them is the same one that is installed on the computers in Aix.

In 2003 the U.S. military commissioned the development of an Internet voting system to allow soldiers away from home to vote in the 2004 Presidential election. Before the election, the military assembled a commission of experts to assess the system before using it. These experts produced a report, the "SERVE Report" (www.servesecurityreport.org) concluding that there are too many problems with Internet voting—in particular, the vulnerability of client machines to vote-hijacking by viruses, the vulnerability of server machines to hacking, and the general impossibility for the assessors of the election to know what the software is doing. On the basis of the SERVE report, the United States decided to abandon Internet voting. As an expert in computer security and in voting technology, I believe that this was a wise decision.

When the election concludes on June 18, 2006, the French people and the *assesseurs* that represent them will have no way to be confident that the election was conducted accurately and without fraud. Internet elections are not possible to conduct in a way that ensures legitimacy.

Introduction

On Monday, June 5, 2006, I attended a training session in Paris at the French ministry of foreign affairs, quite close to the Arc de Triomphe. The purpose of the meeting was to train the official *assesseurs* of the central *bureau de vote* of an election conducted by Internet. Between June 6 and June 18 the citizens of France living abroad (in Europe, Asia, and the Middle East) are voting for their representatives *(conseillers)* to an Assembly of 155. Representatives from Africa and the Americas were elected in 2003 and will be again in 2009.

The Assembly represents the interests of French citizens abroad to the French government, and it also elects 12 senators to the French Senate which has power over the laws and government of France.

How normal elections work in France

As in most democracies, France has specific laws governing the operation of polling places (*bureaux de vote*). There are *assesseurs* (which in different American states would be called pollworkers or election judges) who are physically present at the polling place during the entire election day and supervise the election to make sure that it is conducted lawfully with no cheating.

Most French elections are conducted with paper ballots. Unlike in the U.S., where voters mark a single preprinted ballot form with a pencil, French voters are given a choice of several preprinted ballot forms, one prepared by each political party. The voter takes at least two of these into the voting booth (*isoloir*), puts just one into the official envelope, exits the voting booth, and deposits the envelope containing the ballot (*bulletin*) into the ballot box (*urne*). The French word *urne* is derived from the Latin *urna* "jar, vessel." The Romans voted by dropping small balls into earthen vessels. Now in France the *urne* is a lockable box with a slot on the top.

The voter makes no pencil marks on the ballot, and in fact any such marks will, by law, cause the ballot to be invalid. This may surprise an American voter: How can the French voter vote for President, Representative, Senator, Mayor, Governor, Sheriff, and Dogcatcher all at once with this system? But France does not have a Federal system the way the U.S. does, and they vote only for one thing at a time: there is one election for President, a different election for Parliament, and another election for city council. When there's only one race on the ballot, the method of selecting one paper from one of the several piles of preprinted ballots works just fine.

Pencil marks on a ballot could be used by a voter to identify himself, proving to a (hypothetically) corrupt local political boss how he voted. Presumably, France

Ceci n'est pas une urne

(like the U.S.) had problems in its history with vote-buying and coercion, and has instituted procedures to prevent this: the secret ballot, where no one else can see how you voted and you can't even prove to them how you voted even if you wanted to.

As in any well-conducted election with paper ballots, the *assesseurs* watch the ballot box all day to make sure nobody puts any ballots in when they're not supposed to. At the beginning of the day they verify that the ballot box is empty. In most countries this is done by opening up the ballot box, but in France the ballot box is transparent! This example of transparency in election procedures is very striking: the assesseurs can monitor the contents of the ballot box from beginning to end. Clearly this is in reponse to the fact that France (like the U.S.) must have had problems in the past with ballot-box stuffing and other similar forms of cheating. (Americans may wonder, "but can't the election judges see what's marked on the ballots in a transparent ballot box?" but remember, the voter puts his ballot in an envelope before depositing it.)

At the end of an election day, the votes are counted. This is done by citizens in full view of the *assesseurs*, who are representatives of the political parties. A colleague of mine in France (this year I am a visiting scientist at INRIA, the French national computer-science research lab) says that one time, when he was voting late in the day, he was invited to stay and help count the votes. The ballot box is opened up and its contents dumped onto the table, the envelopes are opened up one by one, and the ballots are counted. Those elections are easy to count by hand, too, since there's only one race on the ballot. I would not recommend this method for an American election with many races on the ballot—I believe that optical-scan paper ballots with hand recounts of randomly selected precincts are the best method there—but when there's only one race to count it can work fine.

This counting of the votes with representatives present from all the parties is just like the way that hand recounts are done in the U.S. Clearly France (like the U.S.) in the past had problems with corruption in the vote-counting.

Unlike the U.S., France does not permit absentee ballots (*vote par correspondance*) in a normal election. Apparently in the past absentee ballots were associated with problems with cheating (or vote-selling, or coercion).

At the end of the election day, the *assesseurs* write and sign a *procès-verbal*, that is, a written statement of the results of the election at this *bureau de vote* and of their personal observation whether or not the election was conducted without fraud and according to procedure.

I have gone into this long digression about the method by which *normal* elections are conducted in France just to illustrate that French law has very many specific rules about how paper-ballot elections are conducted and exactly how assesseurs must do their job. But the meeting I attended Monday was for the *assesseurs* of an election conducted by Internet to learn how to do their jobs. As you might imagine, the procedures are a bit different.

Internet vote for the Assemblée

There are over 500,000 eligible voters in this election. In the 2006 election of the *Assemblée*, each citizen is given the option to vote in person at a French consulate abroad, or by physical mail, or by Internet. As of June 6, about 28,000 voters had chosen to vote by Internet, which is about one-third of the typical turnout for the election. Each country or region of the world has its own representatives; for example, French voters from the Scandinavian countries will choose one from several slates of candidates specific to that set of countries.

As in any election, the job of the *assesseurs* is to supervise the election and to make sure, with their own eyes, that each voter is legitimate, each legitimate voter has the opportunity to vote, that each voter deposits one vote—and no more than one—in the ballot box, that the ballot box is empty at the beginning of the election, that there is no tampering with the ballot box during the election, and that the contents of the ballot box are accurately counted at the end of the election. On June 5, the day before the election started, there was a training session for the *assesseurs*. The instructors at this session were three engineers from EADS, the company that produced the software and built the system to run the election, and one from Experian, the company contracted to actually run the election. EADS is a large European military and aerospace manufacturer; Experian is an "information solutions" subsidiary of a large British company.

I attended the training session as an observer, not in any official capacity. At the training session several things were explained: How voters had already regis-

tered for Internet voting; how voters would interact with the system; the general architecture of the installation at Aix-en-Provence (in the south of France); and the user interface by which the *assesseurs* in Paris could monitor the election taking place on the installation at Aix. In fact, the primary purpose of the meeting was to explain the user interface, on a series of PowerPoint slides.

As it was explained to us, before the election each voter visits a web site to download a Java applet that will be the user-interface for voting. At this time, the compatibility of the user's machine, operating system, and Java virtual machine is tested. The user may be advised to download the Java virtual machine, or may be advised that his or her system is not compatible and that he should either find another computer to vote on or revert to one of the other two methods (in person or by physical mail) to vote.

A Java applet is used, instead of just ordinary HTTP, so that the vote can be encrypted and then signed before it is sent over an SHTTP channel. Encrypting the ballot and signing it on the client machine is supposed to ensure the secrecy and authenticity of the ballot. I will explain below why it is not possible for the *assesseurs* to assess whether the Java applet actually provides secrecy and authenticity.

The Java applet running on the voter's computer transmits the ballot to a web server running in Aix-en-Provence. There are several such servers running in parallel, all in the same secure room. Also in that room are a computer with a database of the list of eligible voters (the *Liste* computer), another computer with a database containing the votes already cast (the *Urne* computer), and a third computer containing software to manage the election and perform queries on the two databases (the *Supervision* computer).

In a room 760 kilometers away, in a building of the *Ministère des Affaires Etrangères* in very nice neighborhood of Paris, are several more machines. This is the room used by the *assesseurs*. One of these machines is connected by a VPN (virtual private network) to the Supervision machine in Aix, and thus all the PCs in this room in Paris are networked (with various routers and firewalls) to the machines in Aix.

The training session took place in the same room that the *assesseurs* would actually use, so I could see for myself the machines and cables in Paris. I did not see the room in Aix, but I was told about it by the engineers from EADS and Experian. There were about eight *assesseurs* at the training session on Monday; most of them did not seem to be experts in technology. They were invited to visit the room in Aix but it was pretty clear that none of them was going to do so.

There is a browser-based user interface, running on Microsoft Internet Explorer on the PCs in Paris, purporting to show data transmitted from the Supervision machine in Aix. I write "purporting" because, as the *assesseurs* and I sit in a room in Paris, it's impossible for us to know what is the source of the numbers displayed

on the screen. All we have is the assurances of the four engineers running the training session.

Just as I have no way to be sure that the data comes from Aix-en-Provence, I have no basis to suspect that it does *not* come from Aix. I will continue to write "purport" to indicate that "this is what we were told."

Since the *assesseurs* are required to sign a *procès-verbal* stating that they saw the empty ballot-box, one of the screens available through the user interface purports to show the number of ballots recorded in the *Urne* database. At the beginning of the election period, the *assesseurs* are supposed to verify that the ballot box is empty; thus they are interested in seeing that this screen of the interface reports 0 votes in the *Urne*. There is also a video camera purporting to show the room in Aix on a screen in Paris, because one of the things the *assesseurs* are required to verify is, "who has access to the ballot-box?"

The purpose of several other screens on the web browser user-interface was explained to us. The *assesseurs* have the opportunity to query the database of eligible voters, to see which voters have voted and which have not, to see which voters are planning to vote by Internet. They can also see the format of the ballots presented to the voters in each voting district (each country or region).

There is also a screen called *Supervision* that can "check the sound progression of the election" *(contrôler le bon déroulement de l'élection)*. Apparently this includes consistency checks on the *Liste* database, consistency checks on the *Urne* database, coherence between the list of voters who have formally presented their votes *(émargement)* and the number of votes in the *Urne*, and so on. This screen, like the others, purports to show the operation of computer programs in Aix.

It seems "obvious" that the web-server computer in Aix has the job of "opening the envelopes" and "depositing the votes in the *Urne* database." Computers do whatever they are programmed to do: a computer program, written by an employee of EADS and running on the web-server computer, has the job of decrypting the messages received from voters' machines and, in turn, transmitting messages to the *Urne* computer. The message transmitted to the *Urne* may or may not correspond to the vote received from the voter—it depends on how the program is written. Does this program do an accurate and faithful job of interpreting the ballots? One cannot tell just by running tests before the election, because it's easy to write computer programs that behave one way before the 12th of June and another way after.

One might think that examining the computer program would be useful in assuring that it accurately interprets the votes. But the *assesseurs* are not given the opportunity to examine these computer programs, on the grounds that they are trade secrets. Even if they could examine the programs, it can be extremely difficult to understand what a computer program does under any possible circumstance: in particular, whether it contains inadvertant bugs or deliberate fraud that will alter

the votes received over the Internet from the Java applet running on the voters' computers.

Even if the *assesseurs* could examine the programs and understand them, it is extremely difficult to know whether that is the program actually running on the *Urne* computer. If you have a computer sitting right in front of you, you can ask it to print out the programs installed its hard drive—but you are asking a computer program installed on the machine to read the hard drive, and you don't know whether that computer program is telling the truth. You can open up the machine and remove the hard drive, to read it from another computer that you trust—that way you know what's on the hard drive, but you don't know whether the software in the BIOS of the computer (which is elsewhere in the box than the hard drive) is actually running the program from the hard drive, or is running another program entirely. And needless to say, the *assesseurs* are not invited to come to Aix with a screwdriver and dismount the hard drive of the *Urne* computer to examine it.

All the same is true for the Java applet running on the voter's machine. The *assesseurs* were not shown the source code to this program. The *assesseurs* have no direct way of knowing that this program actually runs on the voter's machine. In fact, even the engineers at EADS and Experian don't know what's running on the voter's machine. At most they can know what Java program is sent to the voter. But they cannot know whether the Java Virtual Machine (the computer program in the voter's browser that interprets the Java program) is corrupted by a computer virus. Any security holes in the voter's operating system or web browser—that is, any viruses and spyware that may have infected the voter's machine—can alter the behavior of the Java applet. This would mean that the voter would see on his or her screen that the boxes are checked for a particular slate of candidates, but the actual vote sent could be quite different.

The *assesseurs* cannot see the voter enter an *isoloir* (voting booth) because there is no *isoloir*. In fact, the voter can easily sell his vote—or be coerced—because another person can see him perform the act of voting.

In fact, in 2003 the U.S. military commissioned the development of an Internet voting system, the "Secure Electronic Registration and Voting Experiment (SERVE)," to allow U.S. soldiers away from their home states to vote in the 2004 Presidential election. Before the election, the military assembled a commission of experts to assess the system before using it. These experts produced a report, the "SERVE Report" (www.servesecurityreport.org) concluding that there are too many problems with Internet voting—in particular, the vulnerability of client machines to vote-hijacking by viruses, the vulnerability of server machines, and the general impossibility for the assessors of the election to know what the software is doing. On the basis of the SERVE report, the U.S. military decided to abandon Internet voting, and did not use the SERVE system in the 2004 Presidential election.

As an expert in computer security and in voting technology, I believe that this was a wise decision.

Cultured French people understand the difference between the thing and the image of the thing, as demonstrated by the famous painting by the Belgian artiste René Magritte, *The Treachery of Images*. It is a realistic painting of a tobacco pipe, with the words in script on the canvas, *Ceci n'est pas une pipe* (this is not a pipe). The representation of the thing is not the thing—or perhaps he meant, the names we choose for things are arbitrary.

The *assesseurs* of a normal French election see a physical ballot-box with their own eyes. They can touch it with their own hands to make sure it's not a mirage. They can see and hear each voter approach the ballot box and deposit one envelope. The picture of a French *urne* that I have displayed is, I am told, what the ballot-box really looks like. But the picture is not the thing.

When the *assesseurs* of the *Election des Conseillers à l'Assemblée des Français de l'Étranger* see a computer screen in Paris saying "0 votes in the ballot-box", they are not seeing a ballot-box. They are seeing a representation, in Paris, that purports to be a communication from a Supervision machine in Aix, that purports in turn to be connected to an *Urne* machine in Aix, that purports in turn to be running certain software. The *assesseurs* do not even see a representation or image of that software, since it is held as a trade secret. The *assesseurs* do not see the voter approach the ballot box; in fact, there is no particular way to know that the vote recorded by the voter is actually transmitted to the web server in Aix, or that the web server in Aix accurately transmits the vote to the *Urne*.

The clear consensus of computer-science experts around the world who have studied these issues is that Internet elections cannot be trusted, for all the reasons that I have explained: the voters and political parties cannot audit the operation of the software and hardware that serves as the real *bureau de vote*. Therefore it is not clear to me how the *assesseurs* can sign anything but a surrealist image of a true *procès-verbal*.