#339: Machine politics: Electronic voting and the persistent doubts about its integrity

VOICEOVER
This is Up Close, the research talk show from the University of Melbourne, Australia.

ELISABETH LOPEZ
I'm Elisabeth Lopez. Thanks for joining us. It's hard these days to find an area of our lives that doesn't depend on digital technologies, whether it's banking, how we entertain ourselves, keep in touch with friends or meet a life partner, so much of our lives is now conducted online. It's no surprise, then, that the machinery of democracy is part of this online revolution. In recent years countries like the United States, Norway, the Netherlands and Australia have been experimenting with internet voting, but there are serious challenges when it comes to privacy, reliability and security, and electronic democracy is looming as a new arena for cyber warfare. The British playwright Tom Stoppard wrote in 1972, 'it's not the voting that's democracy, it's the counting?'. According to our guests on Up Close today, that quote holds true four decades later. Today any internet voting system must grapple with encryption and fend off viruses, hackers and other cyber threats. How can regular voters put their trust in this brave new ballot world? J. Alex Halderman is an expert on electronic voting security and is Assistant Professor of Computer Science and Engineering at the University of Michigan. He studied online voting in Estonia and four years ago led a team of researchers from the University of Michigan in hacking Washington DC's internet voting system. Welcome, Alex.

J. ALEX HALDERMAN
Hi, great to be here.

ELISABETH LOPEZ
Dr Vanessa Teague is a Research Fellow in the Department of Computing and Information Systems as the University of Melbourne. She is an expert in cryptographic protocols for verifiable elections and she's been following the progress of the iVote system in Australia, which is being watched around the world in what is one of the biggest trials of internet voting. Hello, Vanessa.
VANESSA TEAGUE
Hi, Liz.

ELISABETH LOPEZ
How far have we come in developing watertight systems? Vanessa, you have been scrutinising what's happening in New South Wales, the eastern seaboard state in Australia, its most populous one. What is happening there with their iVote system?

VANESSA TEAGUE
Well, watertight is not a word that I would use. iVote, like any internet voting system, is struggling to achieve three different really important security requirements. One is making sure that only eligible voters are actually able to vote and authenticating those voters at the time of their vote. Two is making sure they vote in private, both in the sense that they're protected from people leaning over their shoulder and that they're protected from insiders at the Electoral Commission and that they're protected from eavesdropping on the channel over which they vote. And it's struggling with the question of trying to make sure that voters get some evidence that they can verify that their vote was cast in the way that they intended, and they're struggling with trying to provide to the scrutineers or to the public some kind of evidence that all of the votes that have been received are properly dealt with and properly entered into an accurate count.

ELISABETH LOPEZ
And this system has been around for some time. I guess a lay person might think well, surely it's just a question of ironing out a few bugs, what's the problem? We release our credit card details online, we do all sorts of stuff online; why can't we get this right?

VANESSA TEAGUE
This is really hard because you expect your vote to be private, from the Electoral Commission, from the other people in your household, from people who try to buy information about how you voted from you, but you don't expect your banking details or your credit card purchases to be private from the people you're doing that transaction with. In fact, if you think about banking or online commerce, not only do the people at the other end know exactly who you are and what you're doing but they usually give you some kind of receipt or evidence that tells you exactly what you did.

ELISABETH LOPEZ
Alex, one of the very thorny questions that has come up in your research is that the vulnerability of systems like this to things like viruses and cyber-attacks can mean things like you can see that you've voted, it all looks fine but actually what's running in the background is something quite different, and it might never be detected.

J. ALEX HALDERMAN
Yes, so internet voting and computer voting in general are particularly difficult security problems to solve and it's for some of the same reasons that Vanessa just mentioned. When you are trying to vote electronically you have to simultaneously be
providing strong integrity and very strong confidentiality of the ballots, so the security solutions we use for other things like e-commerce and online banking just don't apply since we can't use receipts and double ledger accounting and so forth. As a result of that, because the security problems involved are so hard, almost every electronic voting and internet voting system that I've studied in my research has turned out to have very severe vulnerabilities, problems that would allow attackers potentially from anywhere in the world to hack into the system and change votes, or that would allow people to find out how voters actually voted and thereby violate their privacy. Solving these problems is an immense open research challenge that people in our academic community around the world are working very, very hard to solve, but it's going to be a long time I think before we have all the answers.

ELISABETH LOPEZ
You've made the point elsewhere that people developing internet voting systems need to anticipate just about every vulnerability that is known or unknown yet a hacker only needs to find one weak point.

J. ALEX HALDERMAN
That's right, and that's the asymmetry of computer security, that to defend a system you have to close all of the different doors and to attack it you just have to find one that hasn't been properly locked. That is an especially difficult problem for voting because once again, you read every week in the newspaper these days about big companies or government agencies or even the Pentagon being hacked, but in many cases we can recover from this kind of hacking incident by taking down the site or the service for a while, making repairs, restoring data from backup and so on and so forth. With an election, that election is scheduled for one day or one period; at the end we all expect to know who will lead, and if that is disrupted by hacking it can be catastrophic. We don't have the same ability to just hit pause, to just declare oh, we're going to re-do the entire election again next month after this hacker attack stops. That would be chaos.

ELISABETH LOPEZ
Especially a Presidential election.

J. ALEX HALDERMAN
That's right.

ELISABETH LOPEZ
I suppose there are systems of checks and balances to audit elections but they haven't necessarily caught up with the technology. What are your observations on how equipped courts or judges might be to really get their heads across the technical side of this, if something is suspected to have gone wrong? Vanessa.

VANESSA TEAGUE
I've been working for the best part of a decade on fancy cryptographic protocols for electronic election verification, and they're really complicated. And we recently finished a project here in Victoria to introduce a small-scale polling place version of a
voting system that gave some electronic opportunity for voters to verify that their vote was cast as they intended in the privacy of the polling place and that it was accurately included in the proper list of accepted votes, which they could check up online afterwards. Now, there are a few things about this kind of method. First of all, it's pretty complicated and it's very hard to get it right. Secondly, they're called end-to-end verifiable election systems; they introduce a degree of hard work for voters and the poll workers.

ELISABETH LOPEZ
So presumably lots of steps. Can you go into some of those?

VANESSA TEAGUE
Well, the most important step is the step in the polling place where you're trying to make sure that the electronic vote that's been recorded on your behalf actually matches your intention. In other words, you're trying to defend against the case where there's some malware or just a bug on the machine that you're using in the polling place that would miss-record your vote if you didn't check it. There are a few different techniques. For processes that you can use to challenge the machine and challenge what it has produced for you and demand some evidence that it's done the right thing. It works great for organisations like the International Association of Cryptologic Research, but when we're talking about using it for ordinary voters, I think there's a real challenge for our research community in getting it to work more easily so that people can understand it.

ELISABETH LOPEZ
Presumably cryptological researchers know exactly what to do but people overseeing elections just are bamboozled, perhaps?

VANESSA TEAGUE
Bamboozled might be putting it a bit strongly but I certainly think there's pressure to make it simple enough that it's easy enough for them to understand. Now, the iVote system, which is the New South Wales system that's running as we speak, has its own homemade verification mechanism, which as far as I know is not available for peer review in any way. There's no publicly available source code.

ELISABETH LOPEZ
Is that a bad thing? I mean wouldn't it make sense for the developers of a system to close it off from the outside world so that they can better fend off any compromises to its integrity?

VANESSA TEAGUE
That's a good question as well, but for the moment I'm talking about understanding just whether that verification mechanism really does consistently detect any attempts to manipulate it, and it's pretty hard to say that with confidence when there's been no opportunity to understand how it works. I think we could discuss at length whether making something public makes it more secure or not, that's perhaps debatable, but it's pretty much unquestioned that keeping the detail secret does not make it more
J. ALEX HALDERMAN
And in this case, the intent of that verification system is to prove to the public, to establish to the public's satisfaction that the outcome is correct, and if we don't know how it works, if nobody knows how it works except the insiders at the election office, there's no way it can actually instil confidence. So it's self-defeating to keep it secret.

ELISABETH LOPEZ
Alex, you're from the United States, 50 states dealing with a plethora of technologies. Would the Holy Grail be to have one system covering the entire country or is it better to have a patchwork of different systems?

J. ALEX HALDERMAN
Yes, in the US each state and in some cases, individual counties within states, determines its own election technology. So there are states that use paper ballots, there are states that use computer voting machines and a range of other technologies as well. I think this system that we have with so many different technologies has some advantages and some disadvantages. On the bright side, it gives us the ability to actually test many different variations on how voting gets conducted and in different states there may be indeed different requirements and constraints on the technology. On the other hand it is a very complicated patchwork of different kinds of systems. As someone who likes to study the technology and maybe point out whether there are problems with particular systems, it's just too many different places and variations on the theme to study all of them in depth. I think there may be security advantages though to having diversity here; the larger your voting system and the more homogenous the technology maybe the less work it is for attackers to just target it once, develop some way to break it and then apply that on a wide scale. In a sense it's like firewalling off state-to-state to make sure they're completely different systems.

ELISABETH LOPEZ
But we have seen instances, haven't we, where one state has abandoned a technology because of some pretty serious vulnerabilities and then another state has gone, yeah, we'll use that. It's as if they haven't learnt from each other.

J. ALEX HALDERMAN
Yes, it is a little bit of an uphill battle to try to reform problems with the technology because you have to take up that battle again in each and every state. But we have seen a lot of progress over the last decade or so in terms of security in polling places in the States. About 15 years ago, after the Bush versus Gore election debacle where we didn't know who was President for almost a month because of problems counting ballots in Florida, Congress gave the states a huge pile of money, more than a billion dollars, to implement new election technology. Unfortunately, the technology that they implemented was touchscreen computer voting machines that
actually were not adequately tested or designed for security and in many cases were extremely vulnerable to hacking.

But after years of work by technologists, by activists in this state and by progressive election officials, now the majority of US states have gotten rid of that technology again and imposed requirements that every voter should have access to a paper record of their vote, whether that's something the machine prints out that goes in a ballot box or whether the voter is just filling out a paper ballot in the first place. It's one of the great ironies of this entire debate that old-fashioned paper seems to provide much better security and privacy than any of our most recent, most modern computer technology.

ELISABETH LOPEZ
We'll get back to that point, Alex. You're listening to Up Close. I'm Elisabeth Lopez and I'm talking to J. Alex Halderman and Vanessa Teague, electronic voting experts, about the challenges of internet and electronic voting. So Vanessa, going back to New South Wales, this 2015 election, there have been a few articles in the media talking about possible scenarios that are quite scary, for instance state-sponsored attacks or attacks by activist groups, lobby groups, in order to further their political ends. It seems like this is an arena in which paranoia probably really pays off?

VANESSA TEAGUE
Well, I think it's important to think clearly about what the threats really are. I think the state-sponsored threat to electronic security and electoral integrity is serious, but I also think that old-fashioned unglamorous threats of electoral manipulation are probably a lot more serious. I'd be a lot more worried about system administrators, people on the ground in the place where the servers are stored, people associated with politicians or political candidates themselves, ordinary voters who'd like to cast two or three votes. Oh, and not to mention just ordinary electronic errors, and we've already seen one in the case of iVote in which the boxes for selecting some of the candidates were just accidentally left off the electronic ballot. All those kinds of unglamorous but potentially more common attacks are what I would really be most worried about.

ELISABETH LOPEZ
And some of this unglamorous stuff, Alex, you looked at in your review of California's internet voting system, in particular things like very basic lessons in password protection that you would assume companies involved in this space would know. Can you take us through some of the things you found?

J. ALEX HALDERMAN
Well, in California in 2007 the Secretary of State ordered a state-wide review of all of the computer election technology that they used and this was in response to problems that researchers had found in touchscreen polling place voting machines in other parts of the US. This was the first US-based intensive study of the security of voting machines. In that study it wasn't actually internet voting, it was polling place electronic voting. But I was part of a team of academics from around the country who were given access to the source code and the machines for systems from three
different manufacturers that supplied all of the equipment for California. We looked at that code - and for one thing, if people who have ever programmed a computer know that the complexity of your program goes up astronomically as the size of the code increases, that it's very, very difficult to make large and complex programs that are correct and are free of security vulnerabilities. Well, in California each of the voting systems had in the order of a million lines of source code; this is what we were given to review. Just because of that length, that complexity, if these programs were completely secure they might be the first programs of that complexity ever produced by mankind that were secure; there was just no way they were going to be able to get everything right with an engineered system of that complexity. But what we found, we found a very wide range of severe vulnerabilities, everything from bad password practices?

ELISABETH LOPEZ
Okay, how bad?

J. ALEX HALDERMAN
How bad? Well, the Diebold voting system, one internal password that was used was actually Diebold, the name of the company. That's pretty bad. But we also found problems that would allow, say, dishonest election officials to figure out how everyone voted by reverse engineering the very poorly encrypted data that was stored by the system, or just completely unencrypted in some cases. Also, the most severe thing we found was that an attacker could take advantage of the benefits of computerisation in the same way we hope to for the economy of scale and efficiency. The computer provides advantages to the attacker too. In this case, that advantage is the ability to make self-replicating code that can spread through the networked environment of the polling place or from machine to machine as data is loaded on and off of them. We engineered voting machine viruses as a proof-of-concept and these are vote-stealing code that just sets the outcome of the election to be whatever you want but that can be injected into one machine with just a few second of access to it and then spread to an entire state. That's one of the scariest things about computerised voting to me is that the attacker can take advantage of the power of computation to potentially commit wide-scale fraud.

ELISABETH LOPEZ
How simple or complex is it for someone to install that sort of code?

J. ALEX HALDERMAN
Well, it's very simple to install. In the case of the Diebold machine the only thing that is stopping you, even as a voter, from installing that code is a flimsy little lock on the side of the machine. You pop that open and you put in a memory card and in about five seconds you can load on malicious code. But that lock, it turns out, is maybe a good analogy for the security of the entire system. So we looked at the lock in the laboratory for a little while until we realised that every machine ever produced by Diebold used the same key. If you stole one of these keys you could open all of the machines. Not only that, even if you don't have the key the lock is really easy to
pick. I've taught students to do it with a paper clip in about 30 seconds. So we're not talking about something that's high-grade security, we're talking about something that's essentially checklist security. There was a requirement that there be a lock and so they put on a lock on it. Not much thought went into making sure that that lock was actually secure.

ELISABETH LOPEZ
There is a slight irony here in that I'm sitting with two engineers, computer scientists, warning that this is possibly never going to be got right. If the companies themselves have these massive gaps in their security, what hope is there for someone in government overseeing the implementation of electronic voting?

J. ALEX HALDERMAN
Well, securing electronic voting is going to take more than just contracting it out to the lowest bidder. It's going to take research, it's going to take new innovations from people, including in our community people like Vanessa who are working on cryptographic protocols that someday may be used to do secure internet voting, but we have a lot of security challenges standing between us and them. I think the thing that most people don't realise is that this is a harder problem. As we've talked about, it's a harder problem than banking and e-commerce; it's a totally different shape of problem. It may seem like an irony that the technologists are among the people who are saying wait, wait, we're not ready to vote online, but the more we've studied the technology, the closer we've gotten to it, I think the more obstacles we've realised are standing in the way.

ELISABETH LOPEZ
I'm Elisabeth Lopez and you're listening to Up Close where we're talking to two electronic voting experts, J. Alex Halderman and Vanessa Teague. Where internationally have we found that internet voting hasn't worked but is still being carried on?

J. ALEX HALDERMAN
Well, one of the largest users of internet voting anywhere in the world actually, and the oldest user, is the nation of Estonia in northern Europe. Estonia is a very interesting case because they were behind the Iron Curtain for many years and after emerging have had a rapid modernisation and actually become a leader in e-government. Estonia introduced internet voting in 2005 and over the decade since have used internet voting in large-scale elections eight times. In the most recent election almost a third of all votes nationally were cast online. There's no other country in the world that comes anywhere close to that.

In 2014 I completed a study that was the first detailed security review of their internet voting system, and what we found in Estonia was really shocking. We approached the question from the perspective of: could a foreign state that wanted to disrupt their electoral results use the internet voting system to do that? Thanks to Edward Snowden we now know all about the hacking capabilities of national governments, so we could adopt a pretty realistic model of the things they can do in terms of compromising hardware as it's being delivered, in terms of using unpatched, what
are known as zero-day vulnerabilities. What we found in Estonia was that a state-level attacker could very easily hack the system, despite many different kinds of protections that were in place, and either disrupt the election, undermine the secret ballot or even completely change the outcome. The Estonian system administrators, the election officials running the system, just didn't have anywhere near the level of operational security that would be required to defend against that sort of attacker. They released videos of the election configuration process that as a transparency measure they just published to YouTube during the vote. Well, in these videos you could see things like the root passwords to the servers. You could see that they were building the internet voting software for people to use on just what looks like somebody's personal laptop that probably already had malware on it. So just many different ways that someone could get in there and change the election outcome. It was extremely disturbing.

ELISABETH LOPEZ
So they were unwittingly giving away information that was just incredibly sensitive?

J. ALEX HALDERMAN
Unwittingly giving away the keys to the kingdom. Everyone makes mistake; you can understand that, its human nature, but security and especially security for voting is very unforgiving of those mistakes. One little mistake can have the consequence of letting someone get in and completely change the election results.

ELISABETH LOPEZ
What has Estonia learned from this investigation into its voting system?

J. ALEX HALDERMAN
Well, our recommendation was that Estonia should discontinue the internet voting system until there's been fundamental technical progress in security. But as to what they're actually going to do, there seems to be a lot of dispute between the major parties about that. One party wants to continue using the system because they think it's the best thing since sliced bread; the other is saying that internet voting is a tool of the devil. I'm not sure how they're going to work out that disagreement.

ELISABETH LOPEZ
Ultimately it's not a decision that's in the hands or engineers or computer scientists or other experts, it is going to be political, presumably.

J. ALEX HALDERMAN
Ultimately the decision whether to vote by any particular process is up to the citizens of a country, and I think that's a large part of why Vanessa and I not only do the research here but also try very hard to communicate to the public some sense of what the relevant security questions and challenges are. And as countries become more educated about the security problems we've often seen good progress on security. The US instituting requirements for paper trails or even more recently, the Supreme Court of India passed a requirement that voters be given some kind of paper record of their votes. So it's an educational process but ultimately I think it's
up to the people.

ELISABETH LOPEZ
Even though you're advising caution, extreme caution in developing internet voting systems, we're not likely to see a return to exclusively paper-based systems because there are all sorts of groups that would miss out, like military personnel serving overseas, expatriates and people with disabilities. What is a good way to handle the needs of these voters and to use technology to do that without delivering something inherently compromised?

J. ALEX HALDERMAN
Technology can do a lot to help all of those groups. The argument isn't that using technology in elections is bad, you just have to use it really intelligently rather than simply because we want to do the latest new thing. For instance, to help voters living overseas. This is something that Washington DC in the United States tried to build an internet voting system to accomplish, they were going to let overseas military and expat voters vote online. They held a public trial of that system and in the public trial there was a mock election before the real election when they invited just anyone in the public who wanted to, to try to break in and show it was vulnerable. My students and I took part in that test and within 48 hours of it going live we had changed all the votes in the mock election.

So Washington DC after that failure did something very sensible; they set up their system so that the voters overseas could download their ballots online, which has relatively few security concerns, and then just mail them back, which avoids the problem of a central hacker changing all the votes. So that's one instance. That way you cut in half the time it takes for an overseas voter to participate. For voters who have accessibility needs, for instance, we have things called ballot marking devices and machines that can present an interface to the voter that's audio or even tactile. And using these machines the voter can complete a paper ballot that's counted with all of the other ones, with the same strong integrity guarantees that are provided. Or even the work that Vanessa and many of her colleagues do on cryptographic voting protocols can be applied to paper ballots to add another level of integrity protection. These are all ways to use technology smarter rather than just more of it, and I think they have a huge potential to help.

ELISABETH LOPEZ
Would it be desirable to have an international standard on all of this? We've got international standards in engineering and accounting. Wouldn't it be so easy for governments to be able to go okay, yep, we can tick items off a list when we're developing electronic or internet voting?

J. ALEX HALDERMAN
Well, there are two problems with that. One is that security generally doesn't work that way; you can't just have a checklist that says if you check off all of these boxes then your system will be secure. You're facing attackers who are just other clever people and they'll find a way around it if all you've done is checked off the box. The other problem is that democracy around the world is surprisingly diverse. The way
elections work, the requirements on them, Australia has this very, very complicated, in my opinion, method of voting where you have to rank all of the candidates in the order of preference that you want.

ELISABETH LOPEZ
Yeah. We have a situation where when you're voting in Senate elections, if you vote below the line so that you don't fall in with the major parties' preferences, you could be numbering 160 candidates.

J. ALEX HALDERMAN
Wow. Some countries just have one question on the ballot and just maybe a handful of choices. Some countries privacy is the most important requirement, even above integrity. Other places privacy is just an important security protection. Because of all of this diversity it's hard to have a one-size-fits-all solution. Also, I'm not sure that any country really feels like it would be comfortable outsourcing the design or requirements for this fundamental foundation of its democracy and self-rule to the international community or others abroad. This is something where having this domestic capacity to engineer a system to your particular needs seems especially important.

ELISABETH LOPEZ
So what do ordinary people without necessarily a great deal of technical knowledge or expertise need to know? What can they do to hold their governments to account in order for us to reach a climate where there is a fair amount of trust in a voting system in their country?

VANESSA TEAGUE
Well, I think the principles that have always applied to voting apply exactly the same to electronic voting. I think transparent electoral processes, keeping the votes private and giving voters and scrutineers or observers the opportunity to verify the outcome are the fundamental rules against which these electronic voting systems should be judged, just like they are for paper systems. And I think everywhere in the world is still figuring out exactly how to reinterpret those fundamental principles to apply to this new technology. I think the right approach is scepticism at this stage. I think voters should be asking for the evidence as to why they should trust a particular electronic system. Some systems do a good job of preserving privacy and giving verifiable evidence of their integrity and others don't.

ELISABETH LOPEZ
What does the future hold?

J. ALEX HALDERMAN
I think people will always have this desire to apply modern technology to the complicated problems of elections. I hope that the future for voting is one where we can wait long enough before we adopt large-scale internet voting until some of the really, really difficult security problems are solved. We need advances in fundamental security questions like how to keep people from hacking into servers,
how to keep users' home computers free of malware, how to provide something better than just passwords that can be easily stolen. I think eventually we may be able to overcome these problems and provide secure online systems, but in my view it's going to be decades, if ever, before we're able to accomplish that.

ELISABETH LOPEZ
Vanessa Teague and Alex Halderman, thank you so much for coming in.

VANESSA TEAGUE
Thank you, Liz.

J. ALEX HALDERMAN
Thanks.

ELISABETH LOPEZ
We've been talking on Up Close about the challenges of internet voting and whether it will ever be possible to stay one step ahead of the hackers with Assistant Professor J. Alex Halderman of the University of Michigan and Dr Vanessa Teague of the University of Melbourne. Up Close is a production of the University of Melbourne, Australia, created by Eric van Bemmel and Kelvin Param. This episode was recorded on 19 March 2015 and was produced by Eric van Bemmel with audio engineering by Gavin Nebauer. I'm Elisabeth Lopez, thanks for listening and I hope you can join us again soon.

VOICEOVER
You've been listening to Up Close. For more information, visit upclose.unimelb.edu.au. You can also find us on Twitter and Facebook. Copyright 2015, The University of Melbourne.

© The University of Melbourne, 2015. All Rights Reserved.