Argentina: don’t criminalize security research in e-voting - Access Now

Javier Pallero@javierpallero View all posts by Javier Pallero →

Argentina is reforming its election system and moving to adopt electronic voting machines, but the proposed laws on “tampering” could put security research at risk

Argentina moves toward electronic voting

Argentina’s ruling party has recently introduced a bill to reform the election system (PDF). The objective of the bill is to tackle several issues in the current system, addressing problems such as candidates running for multiple offices, and making improvements including introducing mandatory presidential debates and strengthening controls for how political parties are financed. But the biggest issue for digital rights is the proposed adoption of an electronic voting system. If the system is not implemented correctly, the digital security, transparency, and accountability of Argentina’s national elections will be put in jeopardy.

A version of the system that the bill proposes for Argentina’s national elections is already in use in some local jurisdictions, like the province of Salta and the city of Buenos Aires. It consists of an e-voting terminal with a touch screen that records the voter’s choice in an RFID-equipped paper ballot that is then physically printed out. The voter reads the choice to verify it, folds and casts the paper ballot in a ballot box. At the end of election day, the ballot boxes are opened and the same voting machine is used to read the RFID votes and record/print a ticket with the totals, which are then transmitted to a central data center.

Seems pretty straightforward, right? But there's a problem, and it has to do with how these kinds of systems are tested.

An election system security researcher prosecuted

Last summer, when Buenos Aires held local elections, security researcher Joaquin Sorianello discovered that the SSL certificates that authenticate communications between computers at voting venues and the central data center had been leaked online due to a mis-configuration of the servers. Joaquin immediately reported the incident to Magic Software Argentina, the private company that had been hired to provide the machines and transmit the results. Since he accessed the server to create a file and show that the vulnerability was real, the company pressed charges against him for unauthorized access to a computer system and damage to property. The company did this even though Joaquin was informing them of a serious security problem.

It took a year of effort in a costly, uneven legal battle between Joaquin and Magic Software Argentina before the prosecutor dropped the charges, recognizing that Joaquin's intentions were positive. He wanted to warn people against using an "easily vulnerable system." Joaquin's exoneration is good news, but the decision only goes so far. The new government proposal for reforming national elections would facilitate just this type of prosecution. It would include prison penalties for people like Joaquin who research the security of election systems.

How the election reform bill threatens digital security

The election reform bill creates new felonies to discourage "tampering" with the voting system, using language that fails to account for or protect the activities of security researchers like Joaquin. Many researchers have found vulnerabilities in computer systems by doing exactly the things the new bill would penalize, such as accessing computer or "cryptographic systems" without authorization, and using RFID paper ballots for purposes other than casting a vote on election day. The bill would even punish broad, vaguely defined behaviors like "[flaunting] knowledge about information systems to induce election authorities to confusion" with prison time.

These provisions pose a serious threat to digital security and limit the ability to audit election mechanisms. The law would make any *independent* audits of the system extremely difficult, hampering accountability.

What Argentina should do — support, not criminalize, security research

If lawmakers in Argentina want elections that are secure and trustworthy, they need to make sure that security researchers have the freedom to conduct research and report vulnerabilities without risking fines, lawsuits, and incarceration. When it comes to systems that underlie democracy, there is no more important issue than digital security. Criminal laws must be written — or amended — so that they do not infringe on essential security research. Discovering and reporting a security breach should not be a crime.

No computer system is flawless. We all depend on independent security researchers — or "hackers" — because they help ensure accountability and transparency in our increasingly technologically complex societies. That is why companies and even some governments have begun to recognize the value of independent security research, and are working to encourage it.

More countries globally are using technology in public administration, so in the future, there will be more opportunity for bad actors or other governments to secretly exploit vulnerabilities in these systems for their own purposes. Lawmakers in Argentina need to recognize that “hackers” like Joaquin that find and report bugs in these systems may be their best defense against disasters like a privacy breach or a stolen election.

The Argentine government needs to rethink the criminal provisions in the election reform bill and take a hard look at its criminal justice system as a whole, to ensure that public policy supports rather than criminalizes security research. Only then will the people of Argentina benefit from the inclusion of technology in their daily lives, including the proposed “updates” to the election systems.