

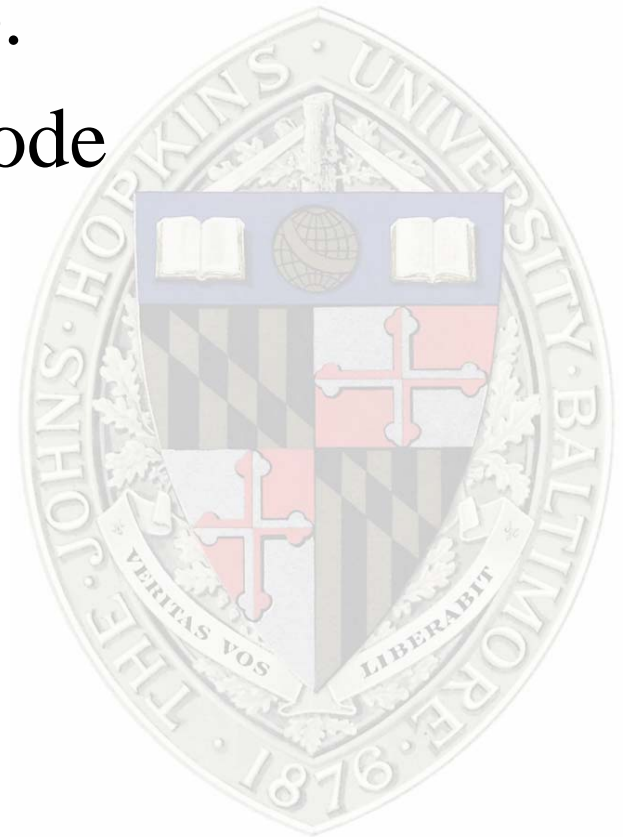
Watching the Watchers: Red Teaming The E-Voting Certification Process

Christopher Soghoian
Information Security Institute
Johns Hopkins University



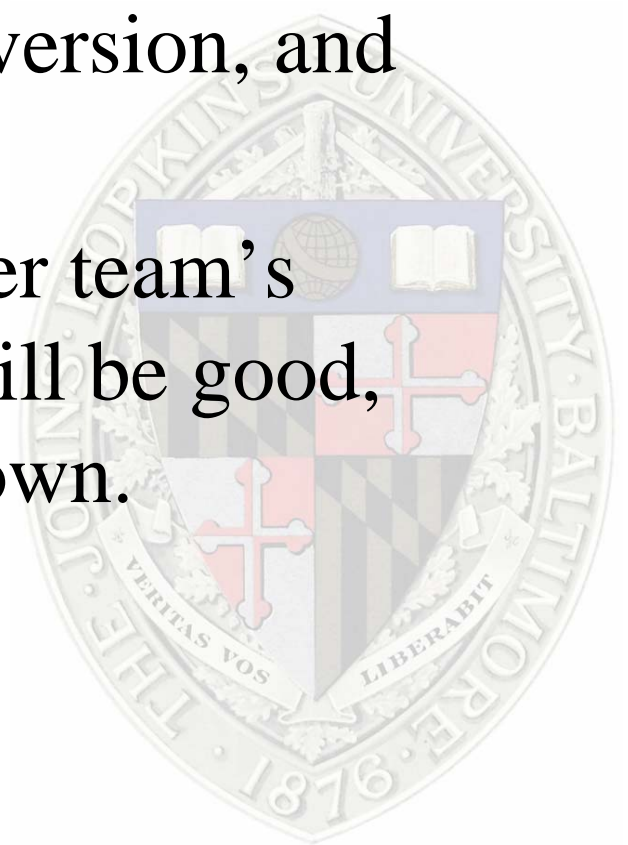
Personal Background

- Who am I?
- Previous research into electronic voting security by members of our lab.
- Avi Rubin & Diebold source code



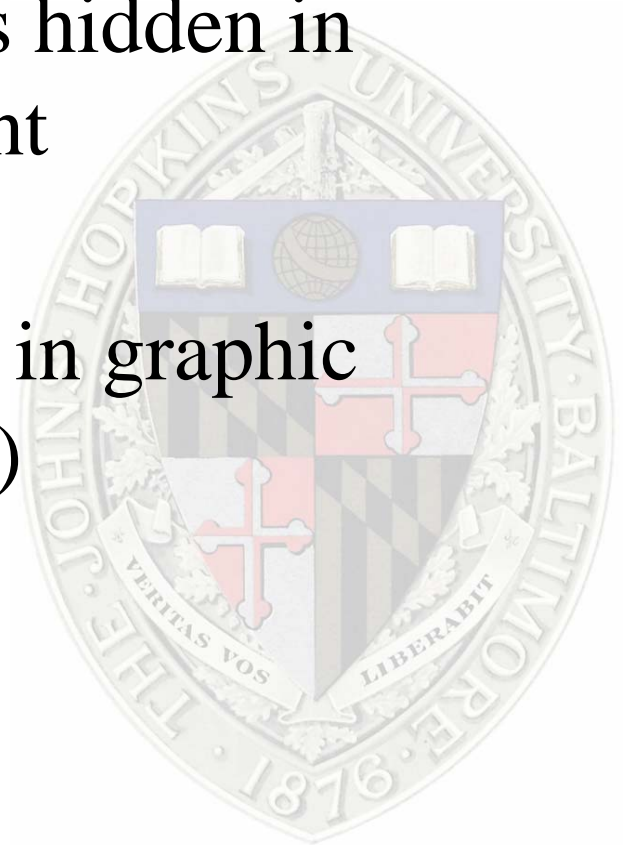
Our Recent Experiment

- Students split into groups of 1-5 people.
- Create a basic e-voting machine.
- Create two versions: a ‘clean’ version, and one with a backdoor.
- Each group is then given 3 other team’s projects. Only know that 1/3 will be good, 1/3 will be bad, with 1/3 unknown.



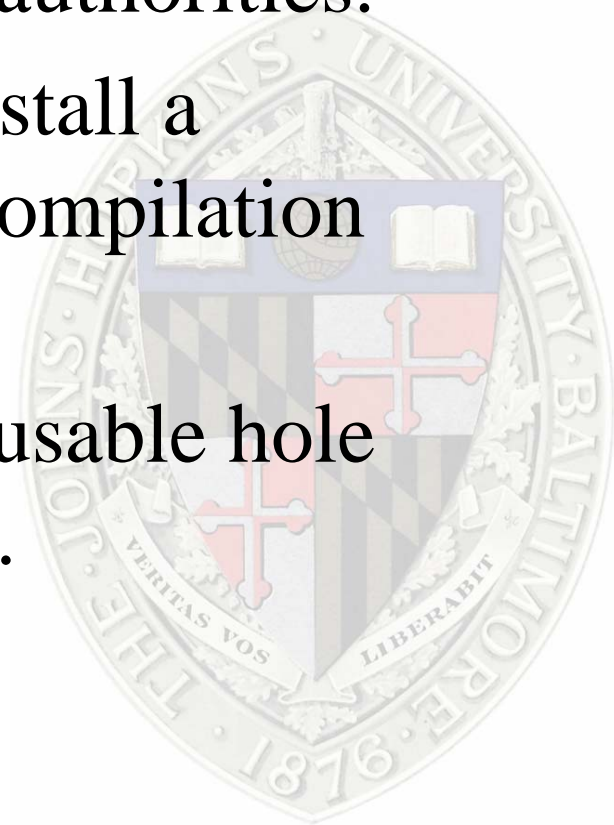
Variety of Backdoors

- A number of very sneaky techniques were used:
- The code for one backdoor was hidden in the whitespace of other innocent sourcecode.
- A couple groups hid their code in graphic files (that could still be viewed)



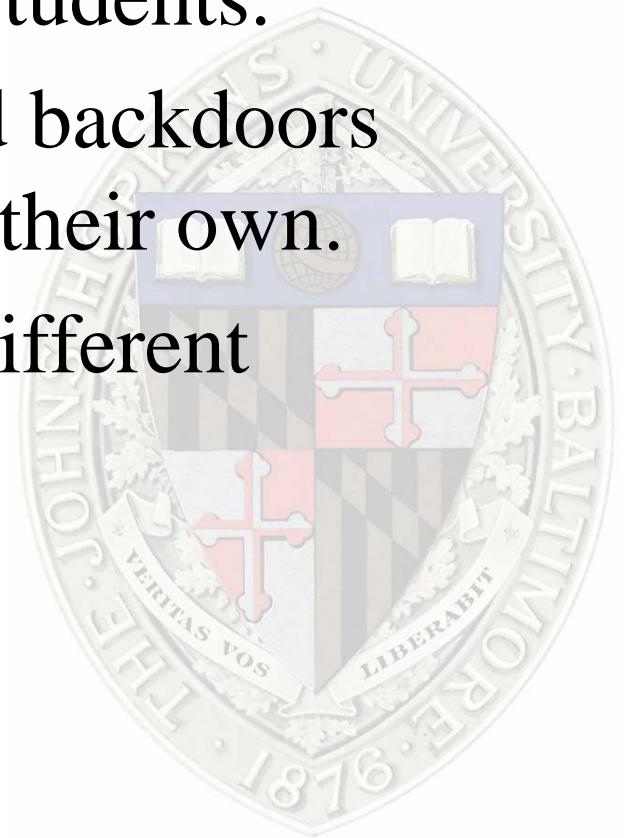
Variety of Backdoors (2)

- Buffer overflows – Even sneakier, as the backdoor didn't have to be in the source code submitted to the auditing authorities.
- One project used spyware to install a backdoor during the program compilation process.
- A group was able to find an abusable hole in another group's 'good' code.



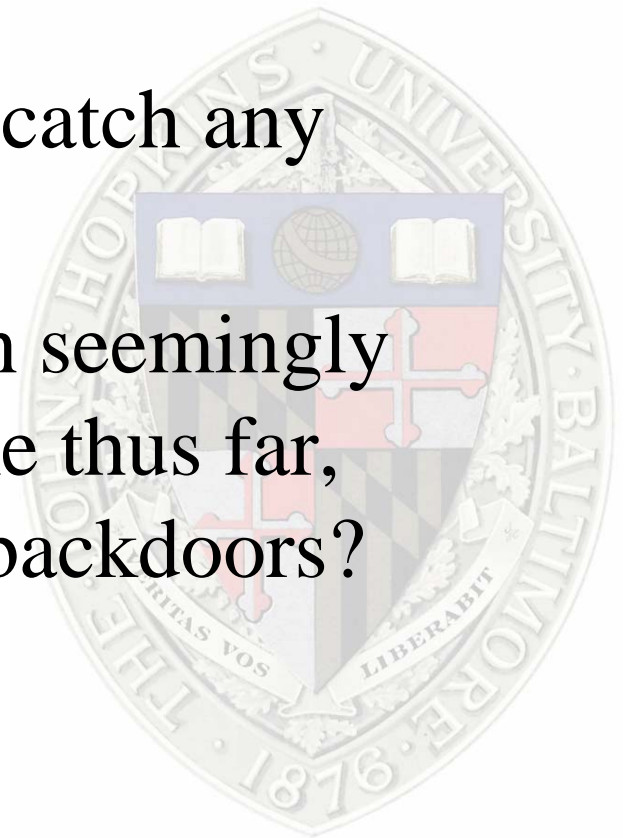
Results

- Groups that produced some of the best backdoors were unable to find backdoors made by other equally skilled students.
- Groups were able to easily find backdoors that used techniques similar to their own.
- Creating/Finding are perhaps different skillsets?



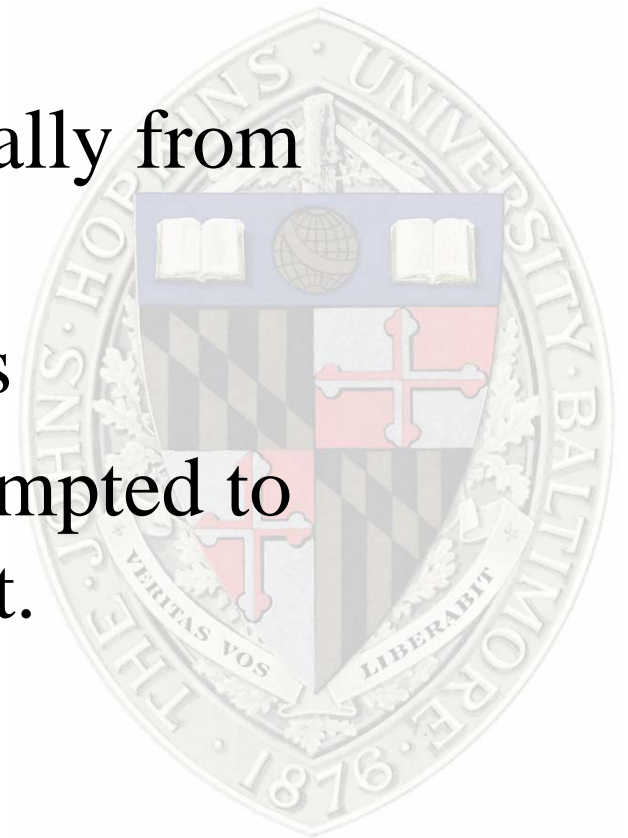
Who is looking for backdoors?

- In the US at least, the e-voting companies submit their code to the states for certification.
- It is the states responsibility to catch any dirty tricks.
- They have been unable to catch seemingly innocent mistakes ahead of time thus far, why do we think they'll catch backdoors?



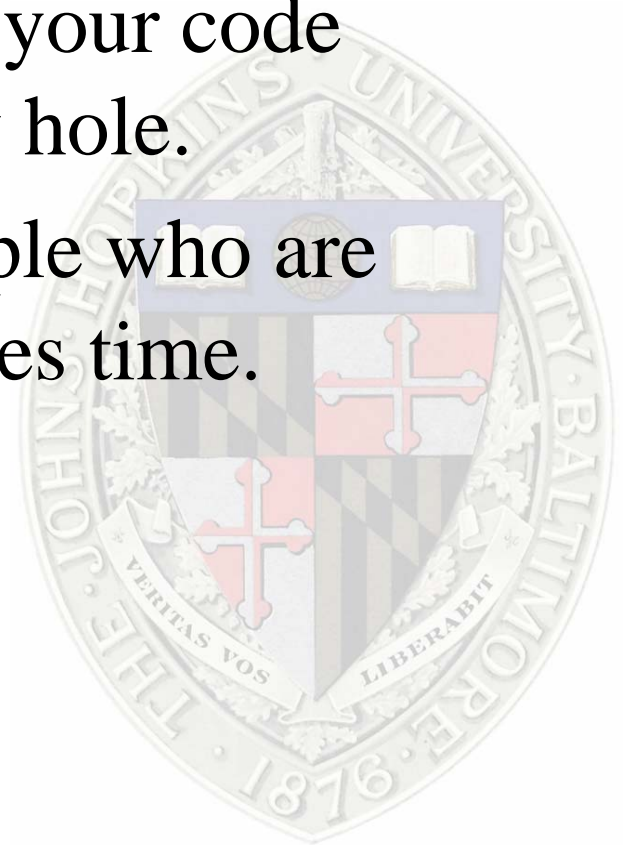
Who is going to install backdoors?

- Everyone has an incentive to cheat at voting.
- Political reasons
- Those who will benefit financially from their winner.
- Foreign governments/militaries
- - The CIA and others have attempted to manipulate elections in the past.



Open Source

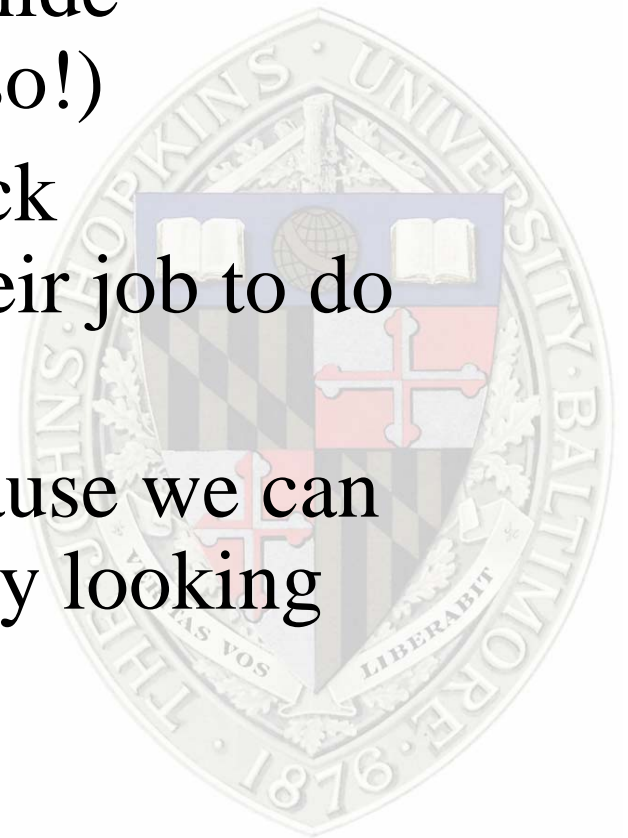
- Open Sourcing the code is a good start.
- However, as many Linux projects have shown – simply open sourcing your code doesn't automatically fix every hole.
- They have to be found, by people who are good at auditing code. This takes time.



Involve the spooks

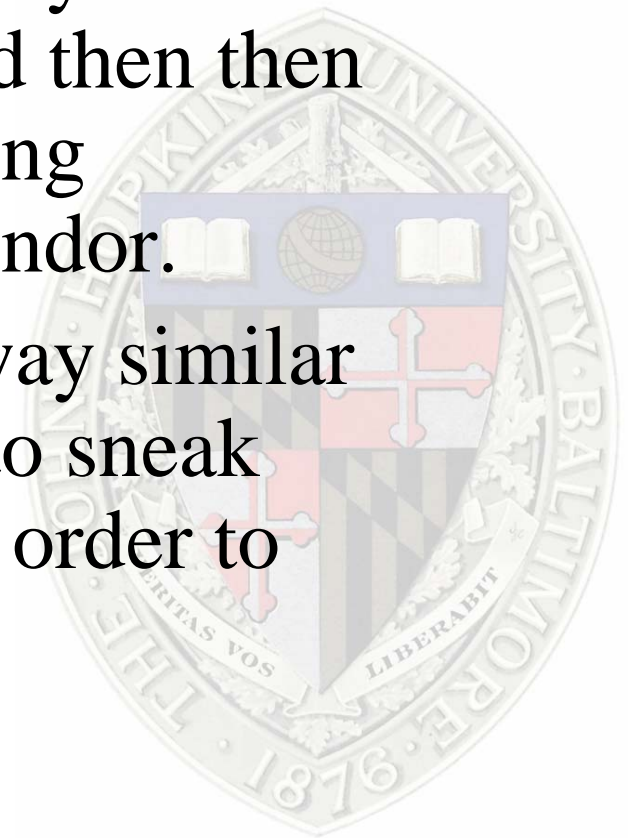
- Our respective spy organizations have the rights skills for the job.
- They know how to create and hide backdoors (it's their job to do so!)
- They know how to look for back doors/exploitable holes (it's their job to do that too).

Our spooks should help out, because we can be sure foreign spies are already looking



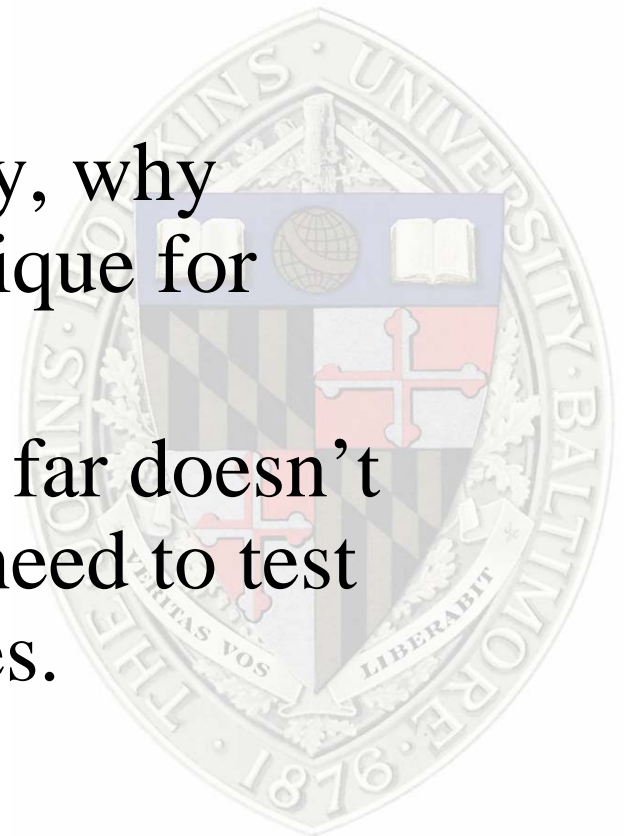
Avi Rubin's Challenge

- Avi Rubin would like to assemble a team, have them sign an NDA, be given a real vendor's source code, which they could then build a back door into, and then then submit to an Independent Testing Authority – on behalf of the vendor.
- Airport security is tested in a way similar to this. Federal employees try to sneak weapons through the airport in order to test the system.



Avi Rubin's Challenge (2)

- Airport security is tested in a way similar to this. Federal employees try to sneak weapons through the airport in order to test the system.
- If we do this for airport security, why aren't we using a similar technique for voting-machine security?
- The absence of backdoors thus far doesn't prove the testing process. We need to test it with real backdoored schemes.



Conclusion

- The security of e-voting machines is vitally important to society.
- We should be testing those who test our machines for us – otherwise, how can we be sure they'll spot backdoors placed by malicious players.
- Given the power that controlling an election can bring, e-voting security should be considered part of Homeland Security.

