Secure Electronic Voting with Encryption

Janae Hoyle

December 14, 2016

Mentor: Ming Chow

Abstract

A representative democracy depends on a universally trusted voting system for the election of representatives; voters need to believe that their vote count, and all parties need to be convinced that the winner and loser of the election were declared legitimately. Even though America has moved towards electronic voting, there is still need for a paper trail. In addition, there is the lack of ability to verify ones vote. There is no way to know if your vote was counted, or if it was counted correctly. Using a Paillier Homomorphic Encryption scheme can provide security to the voting system.

Introduction

Ballot stuffing, recounts, miscounts, hacking, and coercion are just some of the keywords heard surround controversial elections and this election season was no different. The 2016 presidential election has been a whirlwind. The DNC was hacked and there has been constant worry that state-sponsored hackers are having influence in the election. This year the FBI uncovered evidence that foreign hackers penetrated two state election databases prompting them to warn election officials across the country to take new steps to enhance the security of their computer systems. It is clear that technology is evolving but the technology of voting is struggling to keep up. It is important that there is a strong encryption scheme to protect the electronic voting system. Homomorphic encryption is an encryption scheme that allows operations on cipher text without knowing any information about your key or password. Therefore, generating an encrypting result which when decrypted produces the same result if the same set of operations were performed.

To the Community: Why care about voting?

The right to vote is the foundation of a democracy. Electing leaders or voting on referendums affects every citizen. Therefore, it is important that citizens have the belief that their vote will matter. The integrity of the system that people use to vote is vital in preserving democracy. Although the 2016 presidential election brought fears of ballot tampering, this is not new to the United States. In the presidential election of 1876, both candidates, Hayes and Tilden, both declared victory. Tilden had been declared the winner of three southern states when Democratic votes were disqualified for a "misleading illustrated ballot". A committee of 15 people decided the outcome of the election with the Compromise of 1877. This continued in the 2000 presidential election when the margin of victory in Florida was so small that Al Gore demanded a recount by hand rather than machine. However, the Supreme Court declared the hand recount unconstitutional. Following that election, Congress passed the Help America Vote Act that "help improve state and local administration of federal elections and authorized funding for state and local governments to expand their use of electronic voting systems (Gao 1). In 2007, California Secretary of State Debra Bowen commissioned a "top-to-bottom" review of all electronic voting systems in the state. The security experts found significant security flaws in all of the manufactures' voting systems including flaws that could allow a single non-expert to compromise an entire election ("Top to Bottom Review"). Without knowing the source code of the software, the experts were able to gain root access and manipulate every setting on every device in the network ("Top to Bottom Review").

As technology becomes more advanced so will attacks. It is clear that the electronic voting systems in the United States are antiquated and vulnerable which in part makes our democracy untrustworthy.

Ideal Voting System

Neumann proposed ideal electronic voting-criteria would include:

1. System integrity – The computer systems (in hardware and system software) must be tamperproof. Ideally, system changes must be prohibited throughout the active stages of the election process.
2. Data Integrity and Reliability – All data involved in entering and tabulating votes must be tamperproof. Votes must be recorded correctly.
3. Voter Anonymity and Data Confidentiality – The voting counts must be protected from external reading during the voting process. The association between recorded votes and the identity of the voter must be completely unknown within the voting systems.
4. Operator Authentication – All people authorized to administer an election must gain access with nontrivial authentication mechanisms. Fixed passwords are generally not adequate.
5. System accountability – All internal operations must be monitored, without violating voter confidentiality. Monitoring must include votes recorded and votes tabulated, and all system programming and administrative operations such as pre and post-election testing. All attempted and successful changes to configuration status must be noted.

6. System disclosability, availability, and reliability – The system software, hardware, and any custom circuitry must be open for random inspection at any time. The system must be protected against both accidental and malicious denials of service, and must be available for use whenever it is expected to be operational. Additionally, system development should attempt to minimize the likelihood of accidental system bugs and malicious code.
7. Interface usability – Systems must be amenable to easy use by local election officials, and not necessitate the online control of external personnel. The interface to the system should be inherently fail-safe, foolproof, and overly cautious in defending against accidental and intentional misuse.
8. Documentation and assurance – The design, implementation, development practice, operational procedures, and testing procedures must all be unambiguously and consistently documented.

These criteria, first proposed in 1993, set the standard for what an electronic voting system should have to be secure. Yet, 23 years later many of these standards have not been met.

Problems with current voting systems

There are many problems with current electronic voting systems. In 2010, a group of computer scientists from the University of Michigan effectively hacked into the District of Columbia online voting system and changed all the ballots to a different candidate (Wheaton). This voting system was scheduled to run later that year to military voters and overseas citizens, many of whom vote electronically. It only took the group 36 hours to find the list of the government's passwords and break into the system. In 2015, problems at polling stations in Hamilton County, Ohio caused delays. Voters and poll workers in several polling locations stated that they struggled with the technology. In some places, the problem was troublesome enough that the workers restored to old paper poll books. Some poll workers reported they did not know how to operate the new electronic system and others stated that the technology did not appear to work in some instances because it could not connect to the Internet (Butts). These problems should not be happening. Referring back to Neumann's criteria for an ideal electronic voting system, the most pressing issues are the following:

1. Data Integrity and Reliability
2. Interface usability
3. Voter Anonymity and Data Confidentiality
4. Operation Authentication

Application: Encryption in Electronic Voting

Homomorphic encryption

Fully Homomorphic encryption should allow anyone (not just the key holder) to output a cipher text that encrypts for any desired function as long as that function can be efficiently computed. No information or any intermediate plaintext values should leak. The inputs, outputs, and intermediate values are always encrypted (Gentry 5). While no system has been implemented using full homomorphic encryption, partial homomorphic encryption has many uses. Partial homomorphic encryption allows some computation to be carried out on chipper text like addition, multiplication, etc. (Sharma 14)

Homomorphic encryption has a variety of uses. It is used in watermarking and fingerprint schemes, oblivious transfer, and lottery protocols (Sen 13). For electronic voting, homomorphic encryption provides a tool to obtain the tally given the encrypted votes without decrypting the individual votes.

Paillier Cryptosystem

The Paillier cryptosystem gives the homomorphic property we want for voting. The Paillier cryptosystem, invented by French researcher Pascal Paillier, is an algorithm for public key cryptography. Public key cryptography is the use of asymmetric key algorithms where the key used to encrypt the message is not the same as the key used to decrypt it. Each user has a public and private key. The private key is kept secret while the public key may be widely distributed. Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key. The cryptosystem works as follows:

Step 1: Key Generation

1. Choose two large prime numbers p and q randomly and independently of each other such that gcd(pq, (p-1)(q-1)) = 1
2. Calculate n = ab and k(n)=lcm(p-1, q-1) where k(n) is the Carmichael function
3. Select generator g where $g \in Z^{*}{}_{n}{}^{2}$
4. Calculate the modular multiplicative inverse $\mu = (L(g^{\lambda} \bmod n^{2}))^{-1} \bmod n$. The multiplicative inverse exists if and only if a valid generator was selected in the previous step.

The public (encryption) key is (n,g).

The private (decryption) key is (λ,μ).

Step 2: Encryption

1. Let m be a message to be encrypted where $m \in Z_n$
2. Select a random r where $r \in Z^*_{n.}$
3. Computer ciphertext as $c = g^m \cdot r^n \bmod n^2$

Step 4: Decryption

1. Let c be ciphertext such that $c \in Z^*_n{}^2$
2. Compute message $m = (L(c^\lambda \bmod n^2)) \cdot \mu \bmod n$

The homomorphic properties of the Paillier cryptosystem are a defining feature. The encryption function is homomorphic; therefore it can be described as the homomorphic addition of plaintexts. This is partial and not full homomorphic encryption. The product of two ciphertexts will decrypt to the sum of their corresponding plaintexts (Choinyambuu 3).

$$D(E(m_1, r_1) \cdot (E(m_2, r_2) \bmod n^2) = m_1 + m_2 \bmod n$$

Choinyambuu explains that using homomorphic properties can be reduced to a simple binary (1-for and 0-against). Let *m* voters cast a vote of either 1 or 0. Each voter would encrypt their choice before casting their ballot. The election official would then take the product of the *m* encrypted votes and decrypt the result and obtain *n* – the sum of all the votes. It can now be verified that *n* people voted for and *m-n* people voted against.

Having a random *r* ensures that two equivalent votes will encrypt to the same value ensuring voter privacy.

End-to-end auditable voting systems

End-to-end voting systems employ cryptographic methods to craft receipts that allow voters to verify that their votes were counted as cast, without revealing which candidates were voted for. With this voting system we are guaranteed voter auditing in which any voter can check that their vote counted. We are also guaranteed universal verifiability in which anyone can determine that all ballots in have been correctly counted.

Helios is a web-based open-audit voting system that was first proposed in 2008 (Adida 1). Helios uses a protocol, which is closely related to Benaloh's Simple Verifiable Voting Protocol (Adida 2) and Sako-Kilian's mixnet. To provide vote verification, Helios, makes use of a publicly visible bulletin board where each cipher vote is displayed, making it easier to track back to the voter. For auditing purposes, Helios provides two verification programs - One for verifying a single encrypted vote produced by the ballot preparation system and another for verifying the shuffling, decryption, and tallying of an entire election.

Limitations of using bulletin boards

Using a bulletin board, as a means to check weather a vote was casted is not secure. The organization with access to the private key can view how individuals voted. This does not guarantee voter anonymity, which is one of Neumann's criteria for a secure electronic voting system. There needs to be security measures in place so an attacker could not access the data on the bulletin board.

Conclusion

Encrypted electronic voting is the future. If the 2016 presidential election season taught us anything, it is that we need a system we can be confident in. Voters should be confident that their vote was cast without tampering. Candidates should be confident that they won the election fairly. An ideal voting system should be private, accurate, and accurate. Homomorphic cryptographic properties can be used by secure electronic voting systems. End-to-end auditable systems are a way that secure voting can be implemented. While there are flaws with some implementation methods, overall the system is better than the one we use today. In the future, we could have the computational power to implement electronic voting with full homomorphic encryption and therefor not need a private key ensuring that all the data is always encrypted and secure.

Works Cited

1. Adida, B. Helios: Web-based open-audit voting. In Proc. USENIX Security, Aug. 2008.
2. Butts, Rebecca and Dan Horn. "Problems, Delays at 10 Polling Stations." Cincinnati.com. N.p., 03 Nov. 2015. Web.
3. Choinyambuu, Sansar. "Homomorphic Tallying with Paillier Cryptosystem." Homomorphic Tallying with Paillier Cryptosystem (n.d.): 1- HSR Hochschule Für Technik Rapperswil, 6 Dec. 2009. Web.
4. Government Accountability Office (GAO). N.p., Sept. 2005. Web.
5. Sen, Jaydip. "Homomorphic Encryption: Theory and Applications." Theory and Practice of Cryptography and Network Security Protocols and Technologies. N.p.: n.p., n.d. 1-31. Print.
6. Sharma, Tannishk. "E-Voting Using Homomorphic Encryption Scheme." International Journal of Computer Applications 141.13 (2016): 14-16. Web.
7. “Top-to-Bottom Review." Top-to-Bottom Review | California Secretary of State. N.p., n.d. Web.
8. Wheaton, Sarah. "Voting Test Falls Victim to Hackers". The New York Times. Web.