[1] The Nedap/Groenendaal ES3B electronic voting system, which is used in the Netherlands, portions of Germany, and France, has come under fire, particularly in Ireland, where its usage has been suspended. In this research, we investigate system vulnerabilities, raising concerns about the reliability of Direct Recording Electronic (DRE) voting devices.

Because of the widespread use of the Nedap ES3B in the Netherlands and its suspension in Ireland, it is crucial to evaluate the security and dependability of electronic voting systems. Realistic assaults on the Nedap ES3B are examined in this article, along with any potential vulnerabilities that might compromise the legitimacy of the election outcomes.

Among the attack possibilities described is the "Screen and Keyboard Man-in-the-Middle Attack," in which a tiny board is implanted inside the device's enclosure with the ability to intercept and manipulate data between the computer and the keyboard or display. This increases the likelihood of covert vote tampering with restricted access prior to elections. The ballot memory module's microcontroller, which permits manipulation after votes have been cast and compromises the voting process's integrity overall, is another cause for concern.

The article questions security techniques that restrict auditability and vehemently opposes the use of obscurity as a means of security. It focuses on the possible conflict between manufacturer-oriented security features and the goals of concerned voters. Moreover, the dependence on DRE systems and the neglect of any insider assaults are mentioned as significant issues.

The design issues that have been found make the Nedap ES3B system more susceptible to malicious actors taking advantage of it. While both hostile attackers and governments may be able to take advantage of the system's vulnerabilities, hostile attackers are more likely to succeed given the ease with which pre-election access can be obtained and the practicality of their attacks.

Ultimately, it is claimed that the Nedap ES3B lacks enough security to be used in elections. It has been said that the existing Dutch e-voting regulations place too much focus on security against different types of attacks. The paper [1] advocates for new legal requirements addressing basic computer security and independent verification to ensure election results are legitimate. This analysis broadens the scope of potential attacks beyond specific vulnerabilities in the Nedap ES3B to fundamental questions about the security, transparency, and verifiability of electronic voting systems, urging for a comprehensive approach to election protocols.

[2] The paper investigates the vulnerability of electronic voting (e-voting) systems to a new attack known as the "clash attack." This attack has the potential to jeopardize the integrity of the voting process, particularly in systems that use receipt verification mechanisms. It has been tested on four different e-voting systems, some of which have been used in actual elections. The paper emphasizes the potential risks posed by the clash attack and provides insights into its applicability across various e-voting configurations. The goal is to raise awareness about this threat, which will lead to the development and implementation of strong countermeasures or the explicit articulation of trust assumptions in future e-voting systems.

The Wombat voting system was utilised in a genuine college election in Israel. Voters use an ID card to enter the system, cast encrypted ballots, and then post the results on a public bulletin board. In the context of Wombat, where identical receipts are issued, enabling undetected manipulation, the collision attack is illustrated. The clash attack in Wombat focuses on producing duplicate receipts for voters with comparable selections. Countermeasures including pre-printing serial numbers on receipts and putting in place processes for clerks to recognise and handle duplicate receipts are suggested as ways to lessen the impact of this attack.

One popular electronic voting system that is available in multiple varieties is Helios. We discuss the original variation, variants with detachable names and versions with aliases. We describe the clash attack vulnerabilities of these variations. Rival browsers and message boards are exploited by the collision attack in Helios versions with detachable names, which publishes duplicate votes. When voters with similar choices are given the same alias, it could lead to a clash attack against the alias version. Modifications to random coin usage and alias issuance procedures are among the countermeasures.

The VAV (Vote, Audit, Verify) voting system—a variation on the Three-Ballot system—is presented in this paper. Voters are issued three ballots. Each ballot lists the candidates in a predetermined sequence, with one candidate designated as "A" and the rest as "V." Simple ballots' serial numbers are altered as part of the clash attack against ThreeBallot and VAV, allowing for manipulation. Verifiability is highlighted as being important, and a countermeasure with pre-printed serial numbers is proposed.

The research highlights differences in trust assumptions and attack techniques between the previously reported attack and the clash attack. A pre-printing of serial numbers countermeasure that complies with Wombat is suggested. The study adds to a deeper comprehension of the weaknesses and advantages of the electronic voting system, with a careful consideration of both verifiability and accountability.

[3] Dan S. Wallach's comprehensive approach evaluates the security and dependability of Webb County's ES&S voting system, focusing on the ES&S touchscreen systems used during the March 2006 Primary Election. The investigation included data collection via observations and data copying, which revealed potential vulnerabilities in the electronic voting infrastructure.

The initial step of the Threat Analysis report is to look into possible risks to the voting process. It highlights the vulnerabilities to malicious firmware installations and reverse engineering, as well as the dangers of software manipulation throughout the pre-election and election stages. It is advised to use stronger passwords and to install more security features.

During an election, the possibility of machine tampering and ballot stuffing increases. The paper discusses accessibility issues as well as the risk of sophisticated attacks. Concerns about poll worker-induced ballot stuffing are raised, emphasizing the importance of strong security measures to prevent fraudulent activities.

The Tabulation System may be subject to software and data tampering. The ES&S tabulation systems have centralized tampering risks, necessitating an "air gap" defence and strict physical access controls. The vulnerabilities also raise concerns about data corruption in event logs and voting logs, prompting recommendations for data protection measures such as system lockdown and digital signatures during transmission.

The report examines the mechanisms used to collect and transmit votes, highlighting the flaws in PEBs and CompactFlash cards. Procedural errors, such as incorrectly tabulating "test" votes, are discussed, as are suggestions such as incorporating sanity checks and rejecting votes cast after the election date has passed.

While both malicious attackers and governments could potentially exploit the vulnerabilities in Webb County's ES&S voting system, the practicality of attacks and the nature of identified vulnerabilities make it more likely that the system will be compromised by malicious attackers.

In conclusion, [3] the paper emphasizes the serious security flaws in Webb County's ES&S voting system. It makes useful recommendations to improve the voting infrastructure's security, transparency, and dependability. To maintain public trust and ensure the integrity of democratic processes, robust security measures and transparency in electronic voting systems are emphasized.

Critical Opinion:

We see a shared vulnerability in the overall security of the Nedap ES3B, contactless smartcard systems, and Webb County's ES&S voting system, which is the reliance on outdated security paradigms. Recent technologies, such as blockchain, are frequently viewed as election security saviors. Although blockchain holds promise, its widespread application to election protocols remains a contentious issue. The immediate need for strengthened legal requirements, independent verification, and transparency trumps the current industry hype surrounding specific technologies. To defend democratic processes and maintain their integrity, an all-inclusive commitment to modernizing election systems and improving security measures is required.

[4] In this paper, authors S. Park, M. Specter, N. Narula, and R. L. Rivest critically analyze the shift from internet voting to blockchain voting, examining whether blockchain technology alleviates or exacerbates existing vulnerabilities in electronic voting systems.

The paper first addresses challenges associated with internet voting, highlighting vulnerabilities to cyber attacks, concerns regarding voter anonymity, and potential threats to the integrity of elections. These challenges underscore the need for alternative solutions to ensure verifiable and secure voting outcomes.

As the focus turns to the transition to blockchain-based voting systems, the authors explore the promised benefits of blockchain, including decentralization and cryptographic security. The primary objective is to assess whether these features contribute to an overall improvement in the security of the voting process.

Contrary to optimistic views about blockchain's potential, the paper critically analyzes the risks associated with blockchain voting. It delves into issues such as unclear trust assumptions, potential attacks on consensus mechanisms, and challenges in ensuring transparency and auditability in blockchain-based voting systems.

In conclusion, the authors argue that transitioning from internet voting to blockchain voting does not necessarily enhance the security and reliability of electronic voting systems. They emphasize the importance of a nuanced understanding, robust security measures, transparent protocols, and clear trust assumptions in the design and implementation of electronic voting systems.

A critical opinion might further discuss the broader implications for cybersecurity and electronic voting, offering insights into the authors' perspective on the current state of internet and blockchain voting. This could include suggestions for future research directions or improvements in electronic voting systems.

[5] In this paper by K. M. Khan, J. Arshad, and M. M. Khan, the authors delve into the simulation of a transaction malleability attack specifically tailored for blockchain-based e-voting systems. The study focuses on understanding the vulnerabilities associated with transaction malleability in the context of electronic voting.

The paper commences by introducing the concept of transaction malleability and its potential implications on the security and integrity of blockchain transactions, particularly in the realm of e-voting. The authors aim to provide insights into how this type of attack could be simulated and its potential impact on the reliability of blockchain-based voting systems.

Throughout the simulation, the paper explores the feasibility of a transaction malleability attack in the context of e-voting, emphasizing the importance of robust security measures to safeguard against such manipulations. The authors also discuss the potential consequences of a successful attack, highlighting the need for proactive defenses.

In conclusion, the paper underscores significance of considering transaction malleability as a plausible threat in blockchain-based e-voting systems. The findings contribute to the current discourse on enhancing the security posture of electronic voting through a comprehensive understanding of potential vulnerabilities and the development of countermeasures.

A critical opinion might explore the implications of the simulated attack, evaluating its realism and potential real-world consequences. Additionally, it could discuss the broader implications for the adoption of blockchain in e-voting systems and the necessity of robust security measures to ensure the trustworthiness of the electoral process.

References:

[1] Gonggrijp, R., & Hengeveld, W. J. (2007). Studying the Nedap/Groenendaal ES3B voting computer.

[2] Kusters, R., Truderung, T., & Vogt, A. (2012, May). Clash attacks on the verifiability of e-voting systems. In 2012 IEEE Symposium on Security and Privacy (pp. 395-409). IEEE.

[3] Wallach, D. (2006). Security and Reliability of Webb County’s ES&S Voting System and the March 06 Primary Election. Expert Report in Flores v. Lopez.

[4] Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going from bad to worse: from internet voting to blockchain voting. Journal of Cybersecurity, 7(1), tyaa025.

[5] Khan, K. M., Arshad, J., & Khan, M. M. (2020). Simulation of transaction malleability attack for blockchain-based e-voting. Computers & Electrical Engineering, 83, 106583.