[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.

The broad usage of the Nedap ES3B in the Netherlands, combined with its suspension in Ireland, emphasizes the importance of assessing the security and dependability of electronic voting systems. This article investigates realistic attacks on the Nedap ES3B, disclosing all probable flaws that could jeopardize the validity of the election results.

The "Screen and Keyboard Man-in-the-Middle Attack" is one of the attack scenarios outlined, in which a small board is installed inside the device's enclosure and can intercept and modify data between the computer and the display or keyboard. This raises the possibility of undetectable vote manipulation with limited access before elections. Another source of worry is the inclusion of a microcontroller in the ballot memory module, which allows for manipulation after votes have been cast, jeopardizing the entire integrity of the voting process.

The paper strongly opposes the reliance on obscurity for security and calls into question security methods that limit auditability. It focuses on the potential clash between the objectives of concerned voters and manufacturer-oriented security features. Furthermore, the failure to examine potential insider attacks and reliance on DRE systems are cited as major problems.

Because of the observed design flaws, the Nedap ES3B system is more vulnerable to exploitation by malevolent actors. While both attackers and governments might possibly exploit its weaknesses, the practicality of attacks and the type of vulnerabilities make hostile attackers more likely to compromise the system, particularly given quick pre-election access.

In conclusion, the Nedap ES3B is said to be insufficiently secure for use in elections. The current Dutch e-voting requirements have been criticized for putting too much emphasis on security against various 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.

In an actual election scenario at an Israeli college, the Wombat voting system was used. The system works by voters presenting ID cards, casting encrypted ballots, and then publishing these ballots on a public bulletin board. The clash attack is demonstrated in the context of Wombat, in which identical receipts are issued, allowing for undetected manipulation. In Wombat, the clash attack revolves around the creation of duplicated receipts for voters who make similar choices. To mitigate this attack, countermeasures such as pre-printing serial numbers on receipts and implementing procedures for clerks to identify and address duplicate receipts are proposed.

Helios is a widely used e-voting system that comes in a variety of flavors. The original variant, as well as versions with aliases and detached names, are discussed. These variants' vulnerabilities to clash attacks are described. The clash attack in Helios variants with detached names takes advantage of dishonest browsers and bulletin boards, resulting in the publication of identical ballots. The alias version is vulnerable to a clash attack in which the same alias is issued to voters with similar choices. Modifications to random coin usage and alias issuance procedures are among the countermeasures.

The paper introduces the VAV (Vote, Audit, Verify) voting system, a ThreeBallot variant in which voters are given three ballots. Candidates are listed in a fixed order on each ballot, with one marked as 'A' and the others as 'V.' The clash attack on ThreeBallot and VAV involves changing the serial numbers on simple ballots, which allows for manipulation. The significance of verifiability is emphasized, and a countermeasure involving pre-printed serial numbers is suggested.

The paper compares the clash attack to another previously presented attack, highlighting differences in trust assumptions and attack strategies. A Wombat-compliant countermeasure involving pre-printing serial numbers is proposed. The paper contributes to a broader understanding of e-voting system vulnerabilities and strengths, with a nuanced focus on 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 Threat Analysis report starts by investigating potential threats to the voting system. It emphasizes the risks of software tampering during both the pre-election and election phases, as well as the vulnerability to reverse engineering and malicious firmware installations. Passwords are recommended to be strengthened, and enhanced security features are implemented.

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 a "air gap" defense 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.

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.