Ethical Researchers & Penetration Testing:

Ensuring Confidence in the Voting System

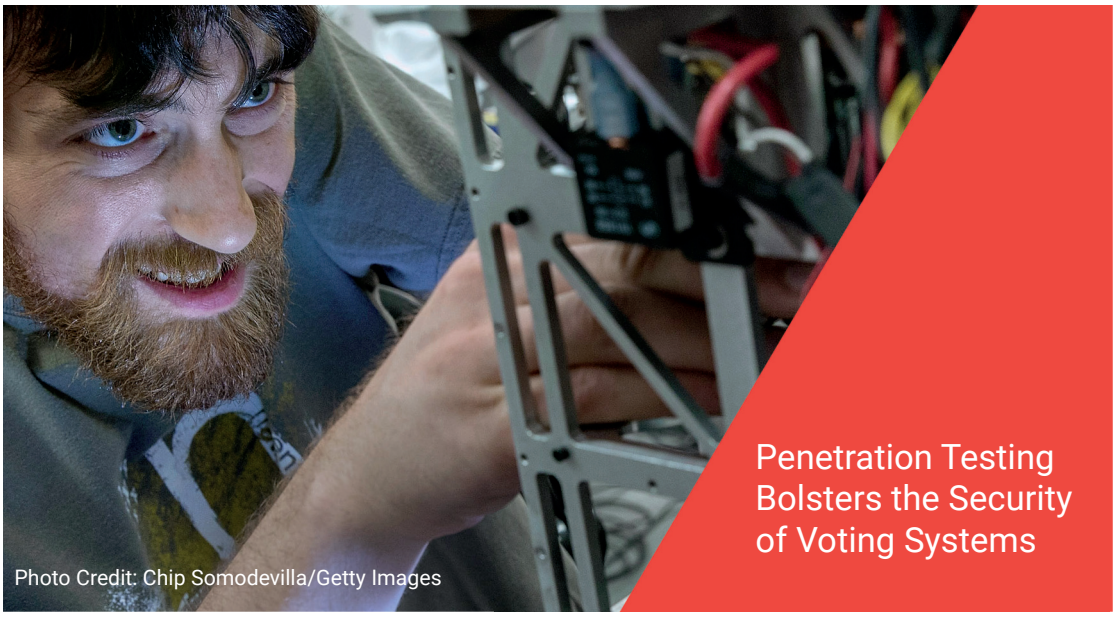
Voting technology manufacturers must keep pace with changing security threats and attack vectors. This paper explores the importance of leveraging coordinated, industry wide penetration testing involving ethical researchers focused on modern U.S. voting technology.

HART intercivic™

Ethical Researchers & Penetration Testing: Ensuring Confidence in the Voting System

In a democratic society, fair and credible elections rely on secure and dependable voting systems. Today, the increasing spread of misinformation, disinformation, and malinformation (MDM)[1] regarding hacking attempts, unauthorized access and other system vulnerabilities present growing challenges for Election Officials.

Many voting technology companies are committed to partnering with Election Officials to safeguard and protect electoral processes. To ensure the reliability, accuracy, and safety of their equipment, voting technology manufacturers must keep pace with changing security threats and attack vectors. This vigilance is necessary to validate their equipment, thereby preempting any potential negative public perception that could undermine the credibility of electoral outcomes.



This paper explores the importance of leveraging coordinated, industry wide penetration testing involving ethical researchers focused on modern U.S. voting technology. The objective of penetration testing for voting technology is to reveal potential issues for remediation before equipment is deployed for public use. While this process may make manufacturers feel exposed, those who choose to participate and engage in this form of testing value the transparency and security this type of stress testing can provide. By offering their voting equipment for participation, manufacturers aim to surface any vulnerabilities that need to be addressed, which can contribute to establishing trust – not only with Election Officials but also with the general public. Penetration testing helps ensure that voting technology utilized in our country is secure and trustworthy, leading to higher levels of confidence.

1 www.cisa.gov/resources-tools/resources/stop-disinformation-products

Voting Technology Systems and Security

Election Officials are expected by the voting public to guarantee both the security and accuracy of voting technology systems today. The spread of MDM and the increasing sophistication of hacking techniques have made it essential for Election Officials to have confidence in their voting solutions and trust in the manufacturers that make the voting technology they utilize on Election Day. The role of Election Officials has matured beyond the logistics of running an election; executing successful elections now demands a comprehensive understanding spanning cybersecurity, changing election laws, physical security, voter communications, and evolving technologies.

As a best practice, the Cybersecurity & Infrastructure Security Agency (CISA) promotes a Secure By Design[2] approach for manufacturers of voting technology. This Secure by Design strategy prioritizes making the security of voting equipment and relevant election systems a fundamental requirement throughout product design and development. The top leaders of the voting manufactures community are committed to continuously reviewing tactics and protocols to guard against security threats.

The role of Election Officials has matured beyond the logistics of running an election; executing successful elections now demands a comprehensive understanding spanning cybersecurity, changing election laws, physical security, voter communications, and evolving technologies.

They do this by combining Secure by Design methodologies with Defense in Depth[3] (DiD) principles, which weaves people, processes and procedures with technology and operations to establish variable defense barriers across multiple layers of their organizations. At the product level, Defense in Depth and Secure By Design principles instill security controls at every product entry point.

All voting devices, no matter who the manufacturer is, must go through rigorous evaluations conducted by government-accredited testing labs[4] to earn required certification at the federal and state levels. While Secure by Design and DiD methodologies provide a strong foundation for voting systems, penetration testing[5] adds another layer of security. This kind of testing is not required but the manufacturers who choose to participate feel passionate about the benefits it offers from an election industry standpoint, and because it serves the greater good of our voting democracy.

2 www.cisa.gov/securebydesign

3 www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-defense-in-depth-did

4 www.cisa.gov/resources-tools/resources/voting-system-standards-testing-and-certification

5 www.hartintercivic.com/wp-content/uploads/2022/06/TestingBeforeTheVote.pdf

Manufacturers Come Together to Drive Ethical Research

In penetration testing, ethical researchers pose an attack on software, hardware or infrastructure to flesh out potential vulnerabilities for fortification within a reasonable and specified timeframe. By leveraging specific expertise (e.g. BIOS, networking, hardware, etc.) ethical researchers do their best to uncover potential threat vectors to provide recommendations for remediation and to improve security and resilience. The goal of penetration in this arena is to help election technology manufacturers ensure their systems are as secure as possible, lending peace of mind to Election Officials and to more readily foster trust in our electoral systems.

After five years of groundwork, the Elections Industry Special Interest Group (EI-SIG), and the Election Security Research Forum (ESRF) came together in the fall of 2023. For this cross-functional initiative, three leading US election technology manufacturers were hosted by the Information Technology - Information Analysis Center[6] (IT-ISAC) at MITRE Corporation[7]. Attended by security researchers, security companies, nonprofits, and former state and local Election Officials, ESRF provided a platform for election technology manufacturers to subject newly developed, unreleased technology to robust penetration testing by trusted ethical researchers.

The integration of systemic penetration testing delivers advantages for voting systems – allowing for the identification and remediation of vulnerabilities, reinforcing systems against various threats, and bolstering security and resilience.

These three leading US election technology manufacturers collectively offered up current election technologies, including digital scanners, ballot marking devices, electronic poll books and other equipment that voters encounter today at polling sites for testing. This event required collaborative and coordinated efforts among a diverse array of stakeholders, including government agencies, Election Officials and voting manufacturers. The participation of ethical researchers and the transparent testing environment of ESRF aims to identify potential vulnerabilities for resolution and to enhance the overall security of voting technologies.

6 www.it-isac.org

7 www.mitre.org

Cross-Industry Efforts and Disclosures

The integration of systemic penetration testing delivers advantages for voting systems – allowing for the identification and remediation of vulnerabilities, reinforcing systems against various threats, and bolstering security and resilience. By pursuing comprehensive security measures, including collaborative penetration testing across industry stakeholders, the US voting systems can be collectively verified and assured. Insights gained from testing events can establish best practices and produce industry guidelines based on real-world findings. These guidelines can serve as an invaluable resource for all voting industry system providers and government agencies alike.

Such organized ethical testing events like ESRF provide voting technology manufacturers the opportunity to be transparent about the security of their systems, foster improved voter confidence by mitigating the MDM claims and progress the industry toward Coordinated Vulnerability Disclosures[8].

Key Takeaways

Penetration testing is a cross functional effort that is voluntary for voting manufacturers. This is just one more way voting manufacturers can help increase confidence in voting technology and support the democratic principles upon which our government is founded.

The integration of systemic penetration testing stands to deliver advantages for all voting systems in the industry.

This proactive approach identifies potential vulnerabilities, reinforcing systems against many types of threats, thereby bolstering security and resilience.

Insights gained from penetration testing can establish best practices and produce guidelines based on real-world findings that can serve as insightful industry resources as the sector innovates.

As voting technology manufacturers take extra steps to ensure election results are secure and accurate, the responsibility of elections moves to state and local elections offices. In addition to physical storage and the conservation of election equipment, providing election staff with necessary tools, processes, and training is critical for making revised and informed security decisions. Continuous collaboration between voting technology companies and Election Officials can strengthen the overall security posture and instill confidence in the electoral processes.

8 www.cisa.gov/coordinated-vulnerability-disclosure-process

Our Commitment to Secure Elections

Leading voting technology manufacturers believe that penetration testing with ethical researchers and collaboration with industry stakeholders are crucial to enhancing the efficacy of voting systems and foster better public confidence in the electoral process. The proactive approach of identifying vulnerabilities and reinforcing systems against various threats not only strengthens the security and resilience of voting technology but also serves as a trust validator for Election Officials and voters alike.

The success of ESRF demonstrates the power of cross-functional and collaborative voting industry efforts. By bringing together government agencies, Election Officials, several major U.S. voting manufacturers, security researchers and other stakeholders, we can collectively verify and assure the security of voting systems. This approach not only addresses immediate concerns but establishes a foundation for continued improvement and innovation across the industry.

We understand that secure elections require a multi-faceted approach. While we are committed to implementing robust security measures in our voting technology, we also recognize the importance of supporting state and local election offices. By acting as partners to Election Officials, we strive to strengthen the entire electoral ecosystem. Based on the thank you notes already received and the support for penetration testing events like ESRF, we are doing just that.

HART intercivic™

About Hart - Election Integrity starts with Hart.
Hart's end-to-end election solutions and services enables you to conduct elections with confidence and deliver accurate results with ease. Only Hart provides the secure and certified voting systems you expect plus the tools, services and support you need before, during and after election day. With Hart, you get a partner who is committed to your success and delivers a full suite of programs tailored to your unique needs. The result? You can have confidence in us so your voters can have confidence in you.

www.hartintercivic.com | info@hartic.com | 800.223.HART