Democracy and The New Frontiers of Mobile Security

IN PARTNERSHIP WITH:

eclypses

FEATURED EXPERTS

David Schoenberger, Chief Innovation Officer**, Eclypses**

Nimit Sawhney, Co-Founder & CEO**, Voatz**

A conversation about mobile application security in a democracy has become especially important amid evolving threats and unprecedented expansion of the surface of attacks. The concerns of custodians of democratic institutions are immediate, with an eye on the future. This conversation preempts and precedes the current focus on security. For democracy to function fully, we need to prepare for threats as we expand the use of technology to make our democracy more inclusive. Eclypses and Voatz participated recently in a webinar to discuss the future of mobile, election, and infrastructure security.

Nimit Sawhney suggests adopting a "layered approach" to improving election security by conducting a risk assessment for each component of voting infrastructure, as well as different methods and scenarios for voting.

- It's important to do this because no technology solution is 100% secure, and that extends to voting technology. **Sawhney** notes that "there is no magic bullet for security of our election infrastructure."
- **Sawhney** points out that there is an inherent skepticism within our society surrounding advances and changes with technology, particularly with mobile applications and online services. He and **David Schoenberger** agree that societal trust plays a large role in accepting these changes.

Schoenberger says that, unfortunately, current practices focus more on user experience than they do data integrity, and shifting the focus to securing the data itself will build trust.

- He notes that users have no issue sharing data with apps, but oftentimes don't think about how that data is secured. Hackers are seeking that data for malicious reasons, and using our own infrastructure to launch cyber-attacks. Instead of safeguarding the actual data, we try to protect against the hackers by preventing access.
- **Schoenberger** indicates that if the focus shifts to securing the data, then trust will follow, particularly as it pertains to voting through a mobile application. He says, "with the advance of security, we can actually secure the data, secure the vote and actually bring trust back into these applications. Because the data itself cannot be compromised, it can be delivered to the receiving endpoint without compromise, we can trust this more than a paper process."

Remotely proofing the identity of a voter is another concern surrounding mobile voting, but Sawhney notes that, with the inclusion of NIST standard 800-63, that risk is significantly reduced, allowing for assurances that a user is who they say they are when submitting a voting ballot through an app

- NIST 800-63 is widely used within the financial industry for compliance purposes to truly, remotely identify an individual. Schoenberger agrees that untethered hacks on smartphones and tablets are something to worry about, but adds that by following best practices, and adopting a data security mechanism, these hacks can be reduced.

ABOUT THE EXPERTS

David Schoenberger, Chief Innovation Officer, Eclypses

David Schoenberger is the Chief Innovation Officer of the cybersecurity software company Eclypses. Schoenberger has been in tech startups since the late 90s, having founded several tech companies in payment processing, cybersecurity, and predictive intelligence. Schoenberger also started a non-profit research laboratory that experiments with simulating mono-polaric magnetic behavior and the effect on moving electrons efficiently.

Schoenberger has assisted clients in protecting data communication between any connected devices or end-points – including private information on a web browser in an unsecure network, command communication to an autonomous device, and data communication supporting critical infrastructure.

Nimit Sawhney, Co-Founder & CEO, Voatz

Nimit Sawhney is the Co-Founder, CEO of Voatz - a mobile elections platform that is changing the way the world votes. Backed by cutting-edge security, biometrics and a blockchain-backed infrastructure, Voatz enables smartphone voting to increase accessibility and security in elections. Since 2016, Voatz has successfully served more than 1.8 million voters across 76 elections with several governments, major political parties, universities and non-profits. In 2018, Voatz ran the first mobile vote in US Federal Election history, and, in 2020, Voatz became the first smartphone app to be used for voting in the US Presidential Elections. Nimit has 20+ years experience in digital security and mobile security software development, previously serving as Director of R&D at Oberthur Technologies (now IDEMIA), and prior to that, as Director of R&D at MoreMagic Solutions where he deployed some of the world's first mobile payment solutions.

Nimit holds a graduate degree from Carnegie Mellon University in Computer Science, Electrical Engineering and Business Management and is an alumnus of the Harvard Business School's YALP (Young American Leaders Program) Class of 2019.

ABOUT ECLYPSES

The Eclypses' patented cyber technology, MicroToken Exchange® (MTE) is redefining data security and addresses vulnerabilities immediately to ensure data integrity, immutability and trust. Eclypses was founded in 2017 with the primary focus of developing the MTE cyber technology to be the most innovative and disruptive data security solution for all connected devices, including mobile applications. Eclypses helps organizations stay ahead of the evolving landscape by adopting a mindset that vulnerabilities are real, and a compromise is inevitable.

We don't make the things you use. We make the things you use more secure.

ABOUT RANE

RANE (Risk Assistance Network + Exchange) is networked-based risk intelligence company that connects business leaders to critical risk insights and expertise, enabling risk and security professionals to more efficiently address their most pressing challenges and drive better risk management outcomes. RANE clients receive access to a global network of credentialed risk experts, curated network intelligence, risk news monitoring, in-house analysts and subject matter experts, and collaborative knowledge-sharing events.