Customer Use Case

How Eclypses MTE Technology Secured Voatz Mobile Application

Voatz

eclypses®

Table of Contents

eclypses®

Introduction

Eclypses was founded in 2017 with the mission of developing the MTE cyber technology to be the most innovative and disruptive data security solution for all mobile application technologies and websites.

MTE Technology Highlights

Generates instantly obsolete, meaningless **random streams of values**. These values replace any form of data transmitted between endpoints OR generated as single use encryption keys.

Provides a necessary – low latency – added layer of security complementing existing cyber protocols with real-time speeds.

Highly scalable solution offering ease of implementation into existing systems with user-friendly API's and SDK's.

Voatz + eclypses

Customer Challenges

Voatz is a mobile election voting application. Their mission is to "make voting not only more accessible and secure, but also more transparent, auditable and accountable."

Network communication can be intercepted by man in the middle attacks to manipulate data, run replay attacks, determine sensitive data, inject code into the transmission to compromise the application server, or simply prevent any communication from ever reaching the intended endpoint.

Jailbroken/Rooted devices pose a great security threat to any company that has an application installed on that device. Such devices can easily contain malware that can intercept communication or tamper with data, gain access to potentially sensitive information, or create fraudulent transactions from the users compromised device.

Voatz + eclypses®

Customer Challenges

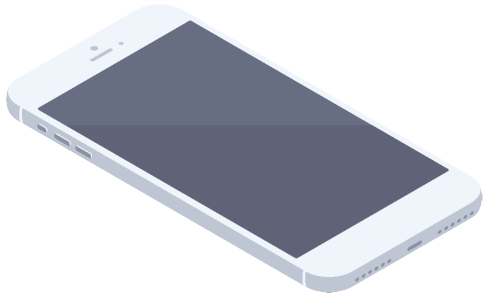
Before MTE, Voatz had a wide variety of security standards, including: TLS/HTTPS, Certificate pinning, Additional AES-GCM, New handshake for initial launch, Encrypted database, OS secured storage, Malware detection and Obfuscated source code

Massachusetts Institute of Technology (MIT) tested the security of the Voatz system with the intent of discovering how well votes were secured and if any manipulation was possible given any of the three conditions below are true.

- Attacker has control of user's device
- Attacker can intercept all network activity but with no key material or access to the voter's and Voatz's systems
- Attacker has control over Voatz's API server

Voatz + eclypses®

Customer Challenges



MIT was able to create a test environment based on their own specific assumptions and attack vectors.

During this study, MIT was able to attack the simulated Voatz system to achieve a number of potential malicious activities and corrupt a fictitious election. Through this re-engineering in the test environment, MIT was capable of achieving the threats listed below.

- Suppress voter ballot
- Identify who the user voted for
- Alter the ballot
- Learn the user's identity
- Learn the user's IP

Voatz + eclypses®

MTE Implementation

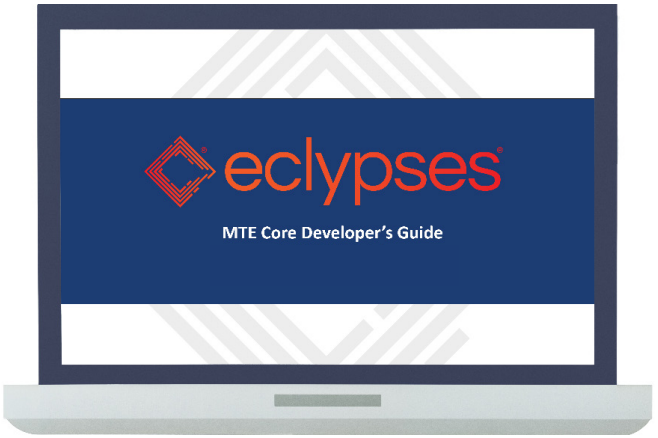
Adding the MTE technology didn't require any major changes to the Voatz app while adding better jailbreak/root detection and a higher level of data protection.

WEEK 1

Initial training of the Voatz team on MTE Technology.

WEEK 2

Voatz has MTE linked into their existing application and is successfully using it within a week.



Voatz + eclypses

Outcome

"Our MTE cyber technology is uniquely positioned for all mobile apps to create an advanced security strategy that enhances any existing security measures in place. We are thrilled about our partnership with Voatz, as they continue to pioneer through the mobile app sector and provide accessibility for people to participate in democracy." - Bryan Champagne, Eclypses CEO

The standard security measures that Voatz implemented were deemed sufficient in protecting against either network or device intrusion. However, MIT testing proved that vulnerabilities still existed and additional measures would be required to protect the integrity of their asset class data...the casted vote.

The Eclypses MTE solution (MTE Mobile & MTE Web) was added to create an advanced security strategy that enhanced the existing security measures that are in place today.

Mobile Threat Protection provides greater security over the network.
Mobile Threat Detection creates better security against Rooted/Jailbroken devices.
Web Browser Protection offers an additional layer of security that protects individual fields of sensitive data on a web page, for when exposure cannot be tolerated.

Voatz + eclypses

“Security is a persistent work in progress and Voatz has always been at the forefront of pushing the boundaries. We are excited to partner with the Eclypses team to further this exciting exploration of how a modern election system can function seamlessly in the presence of anticipated future threats and provide an accessible method of voting to citizens around the world.”

- Nimit Sawhney, CEO of Voatz

MTE Mobile & Web Threat Detection

Eclypses provides Mobile and Web Threat Protection through MTE technology. MTE technology creates a unique pair between the endpoints providing network obfuscation between the app and server. MTE technology generates instantly obsolete, meaningless random streams of values. These values replace any form of data transmitted between endpoints OR generated as single use encryption keys.

In the MIT testing environment, MTE technology would have prevented several of the attacker's capabilities:

- Prevent ballot suppression
- Prevent secret vote from being discovered or discernable
- Prevent any alteration of the ballot
- Prevent collection of personal information about user

Voatz + eclypses

MTE Technology Advantages

Random streams of values generated from MTE technology are safeguarded with several layers of security measures to prevent tampering with the network communication. Everything works within any current security to create an added layer of protection. Attackers cannot even extract anything useful from RAM because it is only using these random values to process data.

Voatz + eclypses

MTE Technology Advantages

Radomly generated
values ensure that there is no pattern recognition or way to extract the original data by anything other than the paired decoder.

Unique pairing
will reject anything that is invalid and will prevent any injection or packet tampering.

Sequencing
gives the ability to recover from missed packets and gives indication that a packet could have been suppressed.

Instantly obsolete
values are meaningless once used preventing any replay attacks.

Timestamps
are included for a higher level of packet validation.

Voatz + eclypses®

MTE Technology Advantages

Eclypses utilizes a specialized method for incorporating checks into the instantiation of MTE there by intentionally corrupting communication to the server if a device is compromised.

Additionally, detection of compromised devices ultimately resides with the server for a more robust solution. There is nothing that can be done from the app side to resurrect the communication to the server. No matter what is tried on the compromised device the server simply won't understand anything being received from such a device.

Voatz + eclypses

Eclypses Enhanced Mobile & Web Browser Security

With the threat from mobile device and web browser vulnerabilities constantly on the rise, Eclypses' MTE Mobile can alleviate risk related to mobile application deployment on a jailbroken/rooted device or operation on unsecure networks. MTE Web can protect the data that will be transmitted over unsecured Wi-Fi and provides the ability to secure single web browsing sessions with low latency.

MTE technology security solution can be implemented alongside your current safety measures to enhance the overall security profile of your mobile applications and infrastructure to protect your business and your customers.

Voatz + eclypses

We don't make the *things* you use; we make the *things* you use more secure.™

contact@eclypses.com
www.eclypses.com

Voatz

eclypses®