

Midterm Report: SecureChat Discord Plugin

Project Title: SecureChat Discord Plugin

Team Members:

- Daniel Willard
- Ethan Cha

1. Introduction:

Motivation: The motivation behind our project is to address the critical concern of communication security and privacy within online platforms. One such platform is the community server known as Discord. With the current lack of end-to-end encryption in Discord, users are vulnerable to various security threats such as eavesdropping, unauthorized access, and man in the middle attacks. Our project aims to develop the SecureChat Discord Plugin to provide robust end-to-end encryption for Discord chat messages. This will allow protection from attackers and allow the users to have privacy from discord and attackers, as well as prevent message leaks from the platform.

Objectives and Deliverables:

- Implementing end-to-end encryption to ensure direct message security.
- Designing a user-friendly interface. Ideally for seamless integration with Discord using better discord JavaScript Plugins.
- Developing methods to prevent man-in-the-middle attacks.
- Deliverables are install documentation and the program files.

Project Plan and Timeline:

1. Literature Review: Research existing encryption protocols.
2. Plugin Development: Ensure compatibility and minimal user impact.
3. User Interface Design: Create an intuitive interface for users.
4. Testing and Optimization: Conduct thorough testing to identify vulnerabilities.
5. Documentation: Prepare comprehensive guides for users and developers.

Timeline:

- Weeks 1-2: Plugin development and integration.
- Week 3: User interface design and initial testing.
- Week 4: Testing, optimization, and documentation.

2. Related Work: We have referenced various sources including the Discord developer documentation, support forums, and BetterDiscord plugin documentation.

3. Progress:

- Ethan faced challenges with the modified Discord library and the lack of documentation. He has also encountered difficulties with the UI and integration.
- Basic framework up.
- Daniel has focused on encryption functions, using AES for communication and considering RSA or Diffie-Hellman for authentication. He has also struggled with learning JavaScript, node integration, and library dependencies.
- Basic encryption functions made.

4. Lessons Learned:

- Challenges with documentation and modified libraries can impact progress.
- Discords ever updating system can make development difficult and unstable
- Reaching out to the developers of better discord has been a useful tool.
- Balancing security with usability is crucial for widespread adoption.
- Learning new languages and technologies requires dedicated effort and time management.
- Scalable projects help to allow flexibility to add if time allows but also allows for project slippage.

5. Action Plan:

- Ethan will continue working on library integration and UI improvements.
- Daniel will focus on encryption functions and minimizing library dependencies.
- Both will collaborate on testing, optimization, and documentation.

6. References:

- Discord Developer Documentation (<https://discord.com/developers/docs/intro>)
- Discord Support Forums (<https://support.discord.com/hc/en-us>)
- BetterDiscord Plugin Documentation (<https://docs.betterdiscord.app/plugins>)
- <https://nodejs.org/api/crypto.html>
- <https://developer.ibm.com/articles/secure-javascript-applications-with-web-crypto-api/>