Pass a Note, Peek a Note

AES Encrypted Messaging and Hacking Simulator

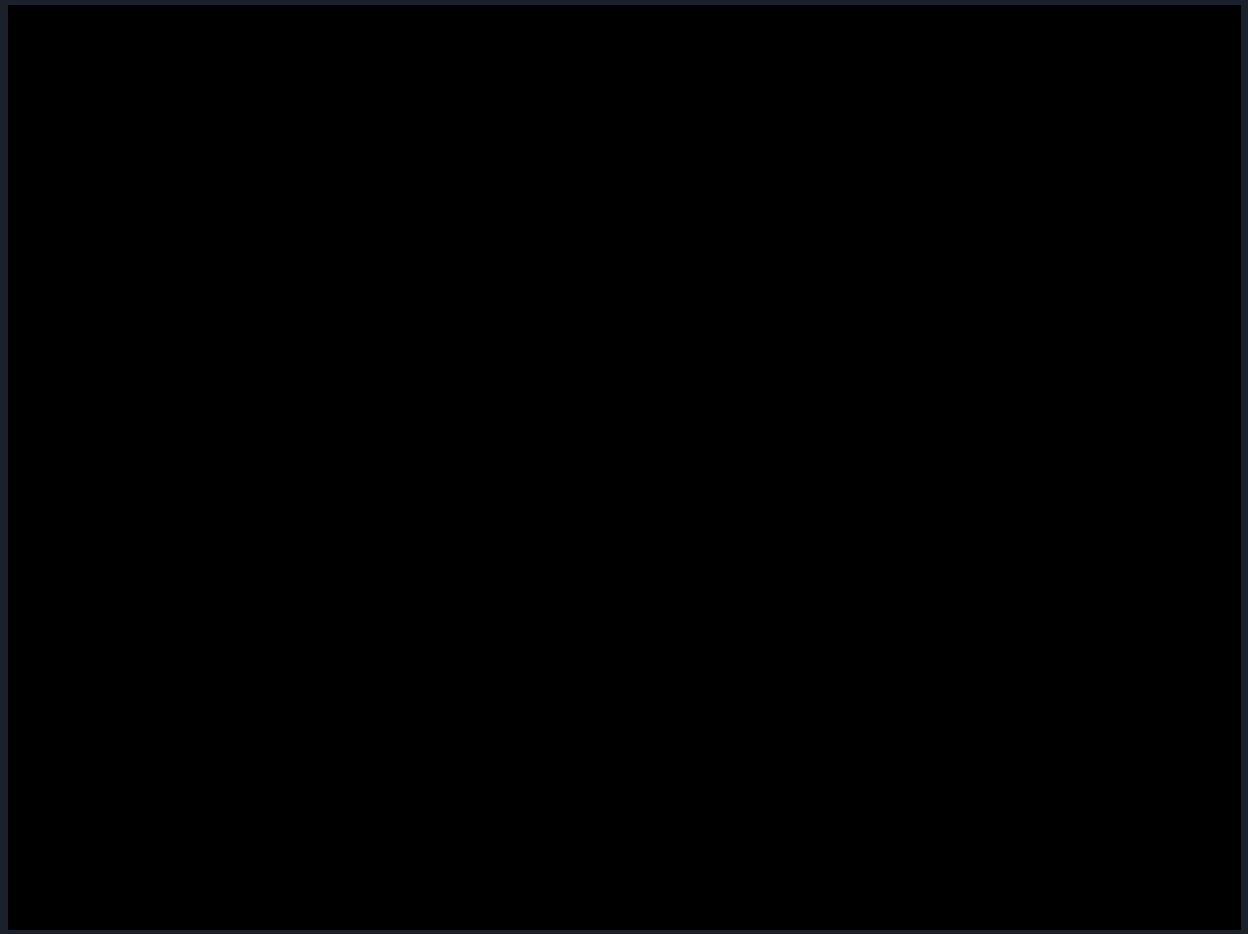
Brandon Litwin

Background

- Based on the simple idea of Alice and Bob who want to pass notes to each other
- A hacker (Eve) will try to peek at the note
- A security system is only as strong as its weakest link
- Although the messages are AES encrypted, PaNPaN has a security vulnerability
  - The decryption key can be revealed by cracking a simple password
  - Hacker can guess password by reading user's profile page
  - Password is a group of words from the profile like **baseballhikingfour**
- Password generation is based on idea that people pick really simple passwords

Methodology

- Flask web page where users create a profile and send messages to each other
- Messages encrypted using Pycryptodome's AES library
- Password to unlock decryption key is generated based on user's profile
- Users choose another user to hack
- Users are notified when they are hacked, and must generate a new password after changing their profile
- Top Hackers and Victims are displayed on the Hall of Shame



Conclusion

- Teaches users to complicate their passwords
- Demonstrates how password cracking can be simple
- Even if you have AES encryption, another system vulnerability can weaken the security