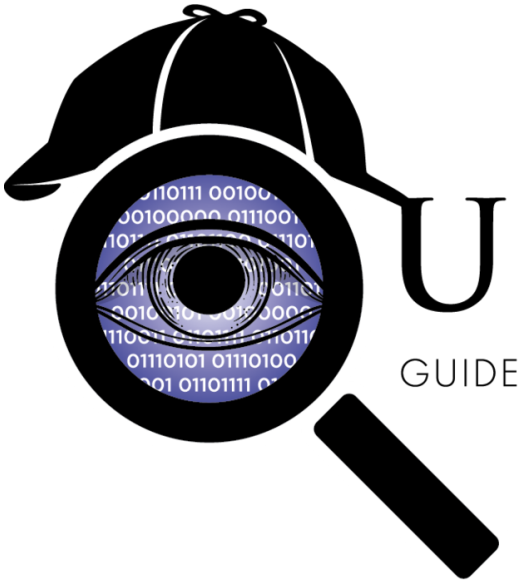


UNIT 221B

GUIDED BY INTEGRITY DISCREET BY DESIGN

SecretService

8th September 2021

OVERVIEW

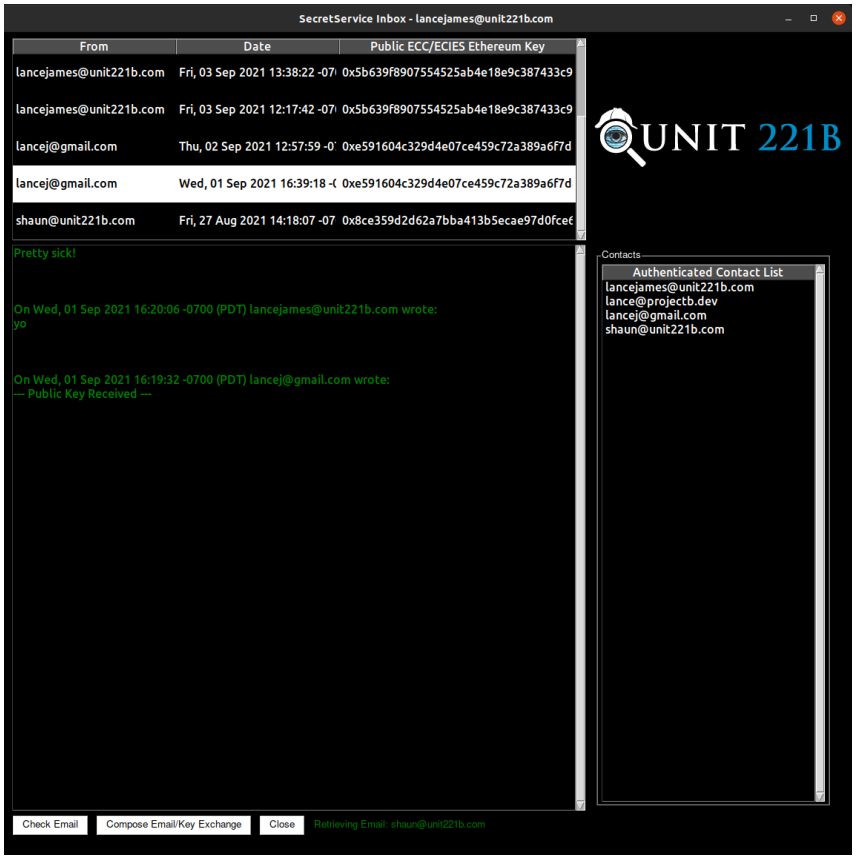
SecretService proposes to be a secure “office-like” tool that combines encryption and steganography together to exchange information via existing email and file-based cloud systems in a manner that hides the fact you are secretly communicating. Utilizing technologies such as ECC/ECIES (Elliptic Curve Cryptography) to exchange keys with a user and enables them to send secret messages and files back and forth, all the while generating decoy data to seem like normal office productivity is occurring. If an eavesdropper, attacker, or even IT Administrator were to see any part of the communication, the messages and communication indicators would appear benign, as the technology camouflages its activity through regularly seemingly innocuous public activity.

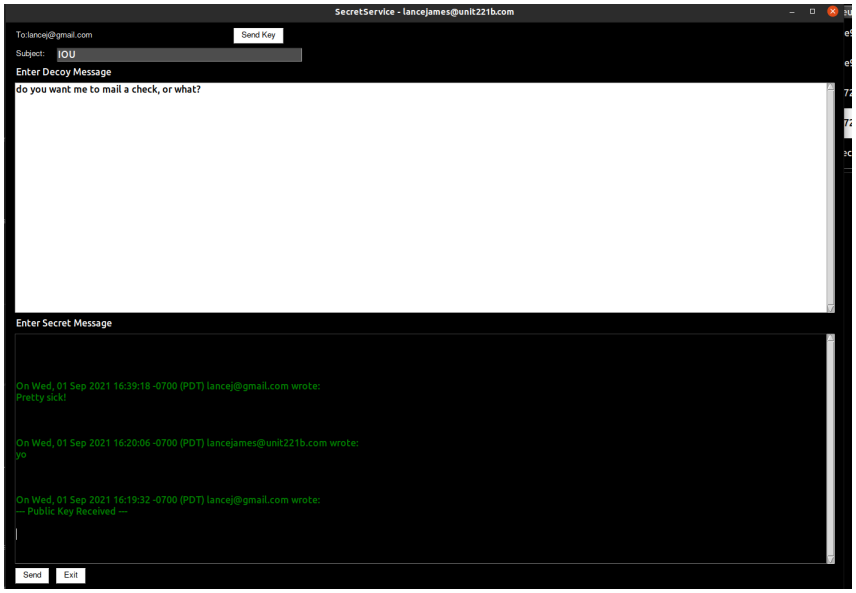
GOALS

1. To enable reasonable secure communications without detection[1]
2. To offer privacy protection within an environment without compromising the parties.
3. Portable, open-source and untraceable from beginning to end.
4. Cross-Platform use on Mac, Linux, and Windows

[1] We aren’t promising foreign dissident protection, nor are we overconfident in our means to create something like this. We have no means of testing against foreign governments like China, so we aren’t planning on lying to ourselves that we can.

Screenshots





Future Feature List

File Management

Portable Encrypted JSON-based Filesystem that can be used on any medium that supports reading a JSON file. Read/Write/Share/MFA capabilities.

Clandestine Chat

The ability to directly chat with users across hidden fields within the TCP/IP protocol. Unlike I2P and Tor where it's obvious you're using the protocol, this mechanism will safely encrypt your chat with zero installation requirements, anywhere in the world, embedding messages within existing protocols in use across the Internet.

Image-based Key Management

Key-Management can be a pain due to the centralization problem. Even a blockchain is a form of centralization in the fact that all users must share the same centralized ledger across the network (nothing wrong with that per se). We are proposing the ability to embed public keys within profile pictures in an undetectable way enabling easy lookup of public encryption keys of users across the Internet without the requirements of centralization or handling messy ASCII, binary, or paper key data that will likely get lost over time. The internet will serve as a backup system, and we will deploy secret sharing schemes to rescue private keys if needed simply by pulling a set of images that reside on the internet that are known only to the owner of the key. Put the keys together, and your key is recovered. The Internet is the perfect archive, let's use it that way.

FIDO2 Passwordless Authentication Compatibility

Where applicable, the integration of FIDO2 hardware security keys and WebAuthN will be supported. We want to move toward a passwordless future, where what is on your physical keychain is what is used online. This will include but is not limited to YubiKeys, FIDO2 compatible biometric security keys, and WebAuthN Public Key Cryptography capabilities.

Universal Cipher Suite Support

Albeit a big dream, we are making a goal to support all standard publicly peer-reviewed cipher suites commonly used today, allowing an interchange between OpenPGP, OpenSSL, OpenSSH, WebAuthN, SMIME, and coin-based public key encryption formats. The underlying encryption mechanisms are the same, so there is no reason to make yet another key pair.