|  |  |
| --- | --- |
| Pegasus%20-%20Black%20on%20White | Department of Electrical Engineering & Computer Science, CS DivisionCollege of Engineering & Computer ScienceUniversity of Central Florida |
| *Return Form to*: Dr. Mark Heinrich, heinrich@cs.ucf.edu |
| **COP 4934: Computer Science Senior Design** |
| **Proposed Project Description Form\*** |
| (Sponsors who are willing and able are asked to provide a Team Donation of $1500 or more for supplies and the running of the CS Senior Design Program) |
| Will support: X Cannot support: |
|   |
| Sponsoring Organization: | DigiThinkIT, Inc. |
|  |
| Mailing Address: | 37 N. Orange Ave., Suite 616, Orlando, FL 32801 |
|  |
| Project Contact: | Eric B. Delisle | Position: | CEO |
|  |
| Contact Phone: | 407-442-0876 | Fax: | 321-206-8697 |
|  |
| Contact E-mail: | eric@digithinkit.com |
|  |
| Project Title *(working)*: | End user verification solution of  |

*Please feel free to use as much space as needed for each of the sections below.*

|  |
| --- |
| **Background of Company/Organization**(Provide a brief overview of the company/organization and the specific project location here) |
| DigiThinkIT, Inc. is a custom software development company which has developed a privacy and anonymity brand called ICLOAK™. The first product we have built is ICLOAK™ Stik, a USB drive with a hardened live Linux OS and other tools to help the non-tech user browse online securely and anonymously.The vision of ICLOAK is to provide a trusted branded set of tools for individuals to use when they want to protect their privacy. In concert with this vision we plan to release a new information sharing client that allows for the anonymous, secure and private transfer of messages and other information (docs, etc.) through a peer-to-peer over Tor (and other anonymizing networks) facility. |
| **Statement and Scope of the Problem(s)**(Provide the problem statement here; Please be as specific as possible to help us understand the scope of the problem, and thus the scope of the project, specifically the design content) |
| The problem is sending and receiving information between 2 or more people when they want privacy and/or anonymity in both short form (sms/im) messages and long form (email/files) messages is complex and setting up a safe environment to do it within is also complex. Our goal is to simplify this process by deploying a solution that is robust and user friendly while adhering to best practices in protecting privacy and anonymity. |
| **Overall Project Goal(s)**(Describe the overall goals of the project in this space) |
| The overall goal of this project to research, explore, and create at least prototype systems for secure, private and anonymous messaging between contacts. |
| **Project Objectives**(Enter the project objectives that will help achieve the goals of the project; Please be as specific as possible) |
| The project will provide a client application which will handle information sharing between anonymous participants in a GUI that resembles a hybrid between Instant Messaging (between 2 or more contacts) where the message is threaded in the display in the order of communication. Additionally, the “mail mode” is for longer form messages that are not intended to be responded to in real time or even at all. Additional functionality would allow for the transfer of files (images, zip files, docs, etc.).One of the key features is the ability for users to be connected to each other only through anonymous networks like I2P, Tor, and Freenet. Each time 2 or more parties want to communicate the messages would be delivered through anonymous relay nodes creating an anonymous circuit between the participants. Additionally, for purposes of robustness, the ideal protocol would use distributed data stores as a “buffer” for the encrypted messages that would allow the recipient a period of time before the message “self destructs” to be picked up.Through the use of Distributed Hash Tables, the locations of the various messages can be stored briefly, allowing them to be “picked up” without a direct p2p connection, thereby separating the participants for additional security. Longer lived messages (similar to email) could have a longer persistence on the network.Another key feature of the client will be a robust way of managing contacts and their associated public keys for encrypted communication. A solution that provides for a simplified way of having people expand their “web of trust” gradually as they self promote contacts through levels of trust from NOT TRUSTED > SOME TRUST > MOSTLY TRUSTED > VERIFIED. These trust levels should play a role in a built in “alert system” that only notifies the user in cases of sending information to contacts whose trust profile is less than the threshold set by the user. |
| **Expected Project Deliverables**(Enter the expected project deliverables including, if possible, proposed project tasks; Please be as specific as possible)* Develop feature set and scope of the client and the messaging protocol
* Research, analyze and choose the technology “stack” to build on
* Create UI Moqups™ of the Client Application
* Create a messaging client with a “normal” database with a clearly defined abstraction layer to replace the database with a distributed data store to allow for early usability testing
* Develop and test the distributed data store and distributed hash tables for moving information data through it
* Create a method of notifying clients for “presence” when a contact becomes available
* Develop simplified key exchange and verification between contacts
 |
| * Work with ICLOAK team to develop a suitable application interface that hides complexity for the end user and focuses on usability in messaging/information sharing
* Develop a distributed storage system that works with existing networks and distributed data stores like the Bitcoin Blockchain, or the Freenet data stores and/or a base of ICLOAK run hidden services
* Develop an easy to deploy anonymous relay and data store for users to run on their regular systems (Windows and Mac) to help improve the network and its robustness
 |
| **Desired Core Competencies and Experience of Team**(Please list the desired competencies/experience/knowledge needed by the project team members that you feel will facilitate successful project execution; Examples: specific programming language experience, familiarity or expertise in certain web technologies, databases, mobile SDKs, prior classes in certain subject areas, a love of computational complexity and efficient algorithms etc.) |
| * Linux OS knowledge
* Python, C/C++, JavaScript, HTML, CSS3 are the most likely languages which will be used
* Networking knowledge including concepts like Distributed Hash Tables and Distributed Data Stores are very important
* Knowledge of the Blockchain (like the Bitcoin blockchain) and its uses for storing transaction data
* Encryption and Cryptography
* UI/UX Design Understanding is also helpful
* Networking protocols, and understanding of packet routing and automated route optimizations also helpful
* A strong desire to give average people the tools they deserve to protect their own privacy!
 |
| **Other Special Considerations and Project Requirements**(Please provide any special circumstances, constraints, and requirements needed by the project team members; **Examples**:* University participants must be US Citizens or Permanent Residents,
* All work is to be performed off-campus at a specific site,
* *Interdisciplinary project*: You would like to see CS students teamed with engineering students from one or more of: Computer Engineering, Electrical Engineering, Mechanical Engineering, Industrial Engineering, Civil and Environmental Engineering (please specify)
* All team members and the professor must submit to background checks,
* All team members and the professor must sign non-disclosure agreements
 |
|  |
| **Project Mentor(s), if different than who is listed above**(Please provide the contact information and title/position for the project mentor(s), who will advise the student team) |
|  |

*\*IMPORTANT NOTE: Proposed projects may not be chosen by student groups. In any one semester the number of potential industry-sponsored, faculty-proposed, or student-funded projects may exceed the number of student teams. If this project proposal is approved by Dr. Heinrich as a potential CS Senior Design project, you or an appropriate representative will be asked to come to class and give a 15-minute project pitch to the students. Keep in mind this is your chance to convince the students why they should pick your proposed project. Think about what is in it for them, what technologies they will get exposed to, what are the broader, enduring, and social impacts of the work, etc. If your project is chosen, you will be notified typically by the 4th week of the semester. If your project is not chosen, you will be notified in the same timeframe and if it makes sense for your timeline, we would love to offer the same project in the next semester.*