The multilayered biometric security system serves the purpose of enhancing the security measures taken today. In today's society, hackers and individuals with malicious intent, continue to run rampant, constantly scheming new methods to gain access to information that does not belong to them. This product would serve the purpose of providing an additional wall of defense against unwanted intrusions. The product would be composed of multiple biometric systems that work together to increase an entity, or system's, security defenses. Some of these biometrics include, but may not be limited to, voice recognition, oral password matching, fingerprint scanning, and typing rhythm. When these biometrics are combined, they provide layers of defense that make it less likely for an intruder to gain unauthorized access. It would do so by conducting these security checks, in random order, to ensure that the person requesting access is authorized. Otherwise, it will deny the user. The subtopic is adapting different means of protection to strengthen a system's defenses.

This Small Business Innovation Research Phase I project will provide a great deal of technical challenges and difficulties in order to make it an effectively working system. Some of the technical hurdles include attaining the correct, physical biometric systems for the project, correctly coding the system to recognize different voice frequencies, utilizing a dictionary and other word sources to cross-check voiced words, brainstorming a way to differentiate the different keystroke rhythms people possess, and one of the biggest challenges, combining them all to work together seamlessly. If these challenges are met and overcome, the result will be a product that provides a high level of security and protection to whatever it is implemented on. In addition to the security functions, it alleviates some of the stress on both internal and external stakeholders, as the system works to increase security measures, and reduce the possibilities of intrusion. In order to reach these goals, an extensive search for the necessary parts will need to be conducted, a great deal of research will need to be executed to find the right code and implement it, and a significant amount of trial-and-error to combine the pieces.

Not only could this security system improve and increase the number of defenses utilized today, it would also help ensure the safety of sensitive information that should not fall into the wrong hands. The purpose of security is to protect, and many systems now are susceptible to attacks and infiltrations due to the lack of security that is implemented. This has been a consistent problem throughout history that has only gotten harder to manage. Attackers become more creative in their methodology of attempting to gain access to information that does not belong to them, and there needs to be countermeasures in place for whatever may happen. No security system is perfect, but this security systems provides a great deal of protection as it implements numerous methods of security seen today, but in a more efficient manner. Different methods of intrusion, such as cryptanalytic and brute-force attacks, have been successful in some cases, but with the process used in this system, getting past one line of defense is not enough. This security system would help meet company needs for protection, improve the service provided to customers, save a great deal of revenue for the company that would be spent on recovering from a cyber attack, and much more.

Revision - Due: 09/25/2016

Leslie Ogu

CSCI 4243: Senior Project - Project Summary

09/24/2016

The multilayered biometric security system serves the purpose of enhancing the security measures taken today. It will act as a defense against the unwanted additional wall of defense against unwanted intrusions of hackers and attackers with malicious intent. The product would be composed of multiple biometric systems that work together to increase an entity, or system's, security defenses. Some of these biometrics include, but may not be limited to, voice recognition, oral password matching, fingerprint scanning, and typing rhythm. When these biometrics are combined, they provide layers of defense that make it less likely for an intruder to gain unauthorized access. It would do so by conducting these security checks, in random order, to ensure that the person requesting access is authorized. Otherwise, it will deny the user. The subtopic is adapting different means of protection to strengthen a system's defenses. A couple of keywords that describe the technical area this product relates to are cyber security, biometrics, machine learning, security breach, security infrastructure, databases, and intrusion defense.

This Small Business Innovation Research Phase I project will provide a great deal of technical challenges and difficulties in order to make it an effectively working system. Some of the technical hurdles include attaining the correct, physical biometric systems for the project, correctly coding the system to recognize different voice frequencies, utilizing a dictionary and other word sources to cross-check voiced words, brainstorming a way to differentiate the different keystroke rhythms people possess, and one of the biggest challenges, combining them all to work together seamlessly. If these challenges are met and overcome, the result will be a product that provides a high level of security and protection to whatever it is implemented on. In addition to the security functions, it alleviates some of the stress on both internal and external stakeholders, as the system works to increase security measures, and reduce the possibilities of intrusion. In order to reach these goals, it is crucial to search for the necessary parts, carry out a great deal of research to find the right code and implement it, and conduct trials to determine the best combination for the various pieces.

Not only could this security system improve and increase the number of defenses utilized today, it would also help ensure the safety of sensitive information that should not fall into the wrong hands. No security system is perfect, but this security systems provides a great deal of protection as it implements numerous methods of security seen today, but in a more efficient manner. It would create a much more genuine sense of safety for people, as they would have additional layers of security surrounding their personal and sensitive information. This security system would help meet company needs for protection, improve the service provided

to customers, and most importantly, save a great deal of revenue for the company that would be spent on recovering from a cyber attack. These benefits would translate to companies being able to utilize their saved funds to provide more for their customers, including additional security packages, more efficient features for the service they provide, and investments in additional services that could be extremely rewarding to customers. The overall gain would lead to an increase in stocks, and a more successful company. No longer will they have to fear their business being the next on the news for a security breach. Rather, it will be praise for the dominance they would now have in the market.

Elevator Pitch

Have you heard the news of the different entities experiencing security breaches, that have ultimately led to a critical financial loss? Did you know that each of them believed that they were completely protected since they had passed the security check, which, in reality, is just checking off a box that says they have some form of security? Do you want to be next? This multilayered biometric security system is just the tool you need to avoid being the next headliner of the Washington Post.

The product is meant for organizations, companies, and businesses - public, private, nonprofit, and more - to be able to provide more secure, efficient, and reliable security measures to its customers. Typical systems tend to have one line of defense that has yet to be truly tested for security holes and/or isn't as extensive as it should be. This system will significantly increase your company's security hygiene, and ensure you are much less likely to get breached. With all the incidents being announced on various forms of social media in regards to cyber security, people are hesitant and unsure of who to trust. If you adopt, and implement this system, you can guarantee your customer's safety, which in turn, will build trust.

When you encounter a customer, one of the many concerns they will vocalize is how secure your systems are, and what security measures have you taken to ensure their information is not susceptible to falling into the wrong hands. The more security-conscious individuals will take it a step further, and ask how often your security is updated, or checked. If this system is one you have added to your arsenal, you will be able to do more than just address these concerns. You will be able to show them exactly the kinds of dangers that are out there, and how your system will have no problem maintaining the security of their information. In fact, you could show them a short demo of how it works, and why they wouldn't need to be worried.

The defining factors that differentiate this product from others is the fact that it is a multilayered system that implements biometrics, in addition to other security measures such as password matching, that is constantly monitored, and updates itself each month. This way, if there are things that need to change, such as removing a fired or retired employee from the system, security is not compromised. The best part is the amount of funding that would be saved as a result that is usually spent on purchasing numerous security systems that are not always the most reliable. It's a package deal that keeps customers safe and happy, and keeps the company from having its image tainted. Everybody wins!

Now you might ask, "How exactly does this system work?" Well, as I stated before, the product is a biometric system, and it would be composed of multiple biometric security checks that work together to increase an entity, or system's, security defenses. Some of these biometrics include, but may not be limited to, voice recognition, oral password matching, fingerprint scanning, and typing rhythm. Since biometrics are being utilized, it is the kind of security that makes it extremely difficult for someone to attack remotely, and even internally. This is a transformation of the basic security system used by most companies because it introduces a new form of security that combines different ideas into one unique defense mechanism. In time, the hope is to introduce additional security aspects to the system because one can never be too secure. If you want to ensure your company can deliver when they ensure customer safety, then this system is something you should adopt. The sooner you have it in your infrastructure, the better.

If you want more details, we could set up a meeting about additional logistics, and more reasons why you need this product.

Covert Ops - Commercial Opportunity and Social Impact (Writing Assignment 3)

One of the biggest faults we have as human beings is not seeing something as a major issue until it personally affects us. Think back to the event of the OPM breach, and how millions of members of society had their personal information compromised. In the same vein, people do not see cyber security as a major topic of concern until events such as the breach, as well as the influx of cyber attacks recently targeted at health entities, occur. Imagine how much information about and belonging to us is on the internet, in the systems of our places of employment, in our educational institutions, and any other place in which at some point in our lives, we have shared some kind of information about ourselves. Numerous entities are entrusted with protecting our information on a daily basis, but just how safe are they? How safe is our personal data? If our personal information is something very precious, and something we don't want in the wrong hands, why isn't its protection our top priority? Our society is in need of more efficient and reliable security measures. The multilayered biometric security system, Covert Ops, will address the problem and help bridge the gap between a more secure cyber world and the entities maintaining our information. Why wait until the next company or industry to fall victim to a cyber attack before taking action?

Despite there being a rise in the attention given to cyber security, there are still not as many industries investing into it. For example, less than a decade ago, Deloitte began focusing its efforts on the cyber world, and how many people and companies are at risk. Companies like Cisco, IBM, Dell, FIreEye, and RSA, and government agencies such the NSA, and the Department of Homeland Security, are at the forefront of the market of cyber security with their technologies such as SecureWorks and traffic monitoring, which have been successful in hindering breaches and hacks. They invest millions of dollars each year to improve the efforts they have, enhance the products they have developed to fight cyber crime, and create new, innovative ways to combat cyber risk. One could see them as the ones who set the standard of how cyber security should be handled, and what it means to properly invest in it. The market is, in a sense, pretty scarce in terms of how many companies are making significant impacts in the cyber realm and/or are investing the necessary funding into the field. Covert Ops is a huge necessity. The addressable market for it product would be any market really - health, education, entrepreneurship, etc. The reason being is every field in some way needs security of information belonging to its customers, or the company itself. If they can't keep it secure, or are not placing as much effort into their security, then they lose their integrity, and the trust of others. Every market needs to invest in some way in their security hygiene. The market of cyber security needs more innovative and reliable methods to combat the hackers and individuals with malicious intent. Covert Ops would not only be cost efficient, but save millions of dollars in possible damage from a successful cyber attack. In regards to the business economics, as mentioned earlier, a significant amount of money is used to drive and address the field. Microsoft is aiming to eventually invest trillions into the field because it is extremely important. Although it may sound like a lot of money for one to spend, it is worth it. You are paying to maintain your company's image and companies using rudimentary security policies and standards in place in order to pass things like audits, or to meet company standards, are the ones more susceptible to be attacked andor breached. Security costs money and to put it to

figures, investing over a million dollars into it has become the standard. The money goes to research, development of products, monitoring of systems, and addressing cyber risks, such as malware, botnets, and DDoS attacks, as they come. It is not necessarily a competition of who is investing the most into the field because it is costly, but rather doing whatever it takes to keep customer information safe and secure.

The validation of Covert Ops on the market is the successfulness of its infrastructure used today. Adding additional layers of security into a system makes it more difficult for any person with malicious intent to gain access to things they are either unauthorized to see, or does not belong to them. Throughout history even, the combination of different methods of encryption and protecting information has made it more of a challenge to hack into any system. For example, there is the Vigenère cipher, which incorporates the Caesar cipher and certain aspects of AES encryption. In addition, biometrics has been proven to be an extremely effective method of protecting information as it is used in agencies such as the FBI and CIA. By combining different methods of security, any system would be extremely secure. Therefore, by investing in Covert Ops, any company would be providing their customers with an additional assurance of their information being protected. Many products and services, such as Deloitte's Secure.Vigilant.Resilient initiative, have been successful in addressing security vulnerabilities before they happen, after they become a serious problem, and constantly monitoring systems to ensure nothing suspicious is occurring. However, even though the available services seem to address the problem in different capacities and at different stages, they are still, for the most part, one-sided. Covert Ops takes it a step further by ensuring certain incidents should not occur. For example, an attacker shouldn't be able to get into a system because they would need to be an actual authorized individual due to the biometrics incorporated into the product, such as voice recognition and typing rhythm. Covert Ops is necessary because the security products on the market now only address the problems to a certain extent, and can only do so much. Not only would it help alleviate some of the risks arising from overlooked possibilities for one to get into a system, it would greatly improve the market by influencing the providers of the current products to make them more effective in combatting potential intrusions.

The customers for Covert Ops, as I mentioned earlier, would be any company with information they want to keep safe. Since it is a means hindering unwanted access of information, any company would be able to incorporate it into their infrastructure. The product would be advertised to companies looking to protect their information using a more efficient method. The creation of the product would be handled by the software engineers of my company, as well as a team of security professionals who would play a role as well to ensure each product is secure. Only certain individuals would aid in its creation, and only authorized developers would be given access to it once it is complete. There would be a chain of command in place to ensure the product isn't handled incorrectly, and help guarantee everyone isn't able to tamper with it, as well as assist with problems a customer may have. The funding for the product would come from the revenue my company accumulates, external stakeholders, customers who are paying for the product, and any business investments the company has made. For a company to pay for the product, they would pay installments each month, or a lump sum per year, for as long as they intend to use it. Revenue would come from the sales of each

product, donations made by different entities, and the external stakeholders who would help fund operations in the company.

The competition in the cyber security market is pretty strong due to many companies having a well-established name and tenure. They include, but are not limited to, Cisco's products such as network security monitoring, cloud security, and Advanced Malware Protection (AMP); Deloitte's Secure.Vigilant.Resilient services; and FireEye's Malware Protection service. All of their products follow the model of providing customers with protection against unauthorized access, monitoring of their systems to ensure they aren't getting attacked, and recovery services in the case they are successfully breached. Their method addresses the problems a company would typically have. I expect the landscape of competition will change a great deal in the future and by the time Covert Ops enters the market as more companies are beginning to invest in cyber security. Pretty soon, most of them will have some kind of product on the market aimed at addressing security risks and concerns. The increase in individuals interested in the cyber security market will make it harder for companies to get their product to sell, and for customers to make a choice of which service or product to purchase.

One of the key risks to bringing Covert Ops to the market is it lacks the experience of being implemented on a company and it would be a brand new product. The reasoning behind the risks is a customer may be less likely to trust a product not implemented in companies, and proven successful. In addition, if they have a product they are using now, they may want to avoid the risk of trying something new with the potential to fail, and cause long-term damage. The two aforementioned risks contributes to a third risk - the product does not work properly and does more harm than good to a customer. The risks will be difficult to address in the beginning, but not impossible to overcome. It would take strong efforts in gaining the trust of a customer, building a good relationship with them, and convincing them of the potential Covert Ops has to guide them in the right direction.

Most of the finances needed will be for the development and management of the product, consistent updates on a daily basis to ensure it is able to address security risks as they arise, and avoidance of possible intrusions on the product itself. Assuming Covert Ops is able to sell on the market to numerous customers, and my company is able to build strong, long-lasting relationships with different entities, revenue projections could start from 30-50 thousand dollars, and increase to the 10-30 million dollar range. It has the potential to grow and be given additional features to make it more attractive to customers, as well as provide more services. As mentioned earlier, the economic impact would be astounding as it would help save millions of dollars. The millions saved may have ended up being used for damage control in the case a company is breached. The savings would allow the company to use their funding in other areas of need, and save them a great deal of revenue each year. In fact, it could help improve the company's standing in the market compared to its competitors, as they would be seen as more secure and reliable. However, one can not put a price on the trust and integrity Covert Ops would help preserve.

If Covert Ops were used widely, it could help address the concerns many companies have - is my company really safe? The answer would be yes, and in turn, Covert Ops would help society as a whole because the information people have entrusted to different companies will be safe. They can have peace of mind knowing their information is in good hands, and they

won’t fall victim to another scare such as the OPM breach. There aren’t specific groups Covert Ops would impact because it would affect everyone. We all have our personal information in the hands of some entity for different reasons, such as our taxes we submit to our schools, and we would not want our information to be handled or given to just anyone. People want to feel safe. We all have enough stress to deal with on a daily basis, and adding your information being in the hands of someone with malicious intent would not improve our lives in the least bit.

There are no environmental or health issues associated with Covert Ops. It is still being determined if the product will be a program or a physical product. Regardless of the fact, it wouldn’t necessarily be appropriate for children, as there is really no reason they should be using it. It will need constant regulation to ensure it is running properly and up-to-date on any new security risks. The management of the system would be handled by the security and technology team responsible for its development and surveillance. It does have the potential to be used for the wrong purposes if the system itself was hacked and used to keep authorized users, as well as the company itself, out of the company’s system and database. The chances of a hack on Covert Ops are extremely low as the product will be managed on a consistent basis to ensure it passes security checks, and is as secure as possible.

Covert Ops does have the potential to have a global impact if it is bought, used, and/or has its methodologies used by foreign entities. The product is not necessarily country-specific, as it serves the same purpose in whatever system infrastructure it is apart of. Therefore, it is also not limited to solving problems only in the US. It could help improve security overall as it would provide safety assurance for customers wherever they are in the world. Cyber security could be enhanced and improved on a global scale as the number of breaches would reduce, and the chances of people having their personal information compromised would decrease significantly.

Covert Ops could potentially be used for unethical purposes. One example could be a case of certain people managing the system deciding to keep other individuals within the company out for personal reasoning, or gain. In addition, if the company decided the product should be charged for a higher rate than necessary, or hindering certain features from being used in an attempt to receive more payment from customers, their act would be unethical as well. The product should only be used for the purpose it was made for, and not manipulated for the gain of certain individuals, or for the exploitation of its users. To combat the potential danger, employees would be required to go through ethical training, among others, to ensure they understand how the product who is to be handled, which individuals manage the system, how to report if there is a belief the system is being misused, and ensuring the company practices are legitimate. The trainings would help to make people less likely to use the system incorrectly, and show customers their information is safe from both internal and external attacks.