**Overview, Key Words, and Subtopic Name:**

This endeavor aims to bring enhanced two-factor authentication to personal workstations, eventually impacting how the log-in process is handled on smartphones, tablets, and numerous other consumer electronics. Firmly situated within the Information Technology & Cybersecurity topics, this system will use voice recognition and keystroke dynamics analysis to introduce a confidence measure for each login attempt, enabling systems to admit users with limited permissions as necessary, or notify users via SMS that their account has been accessed.

**Intellectual Merit:**

This Small Business Innovation Research Phase I project strives to improve the authentication procedure for desktop operating systems, preventing unauthorized access even from actors with the login password. The most significant technical hurdle will be supplementing the existing login process with biometric signatures that are tuned to adequately balance security (unforgeability) with clemency (“forgiveness”).

**Broader/Commercial Impact:**

This project aspires to become a SaaS product for institutions like banks to further secure online portals, and for sensitive information enterprises like EHR to quantify their confidence that they’re showing information to the right people. This, in turn, provides companies with another tool in the information assurance tool belt, protecting them from legal exposure in the event of a data breach, and ultimately lowering their costs for cyber insurance.

**Overview, Key Words, and Subtopic Name:**

This endeavor aims to bring enhanced two-factor authentication to personal workstations, eventually impacting how the log-in process is handled on smartphones, tablets, and numerous other consumer electronics. Firmly situated within the Information Technology & Cybersecurity topics, this system will use voice recognition and keystroke dynamics analysis to introduce a confidence measure for each login attempt. This confidence measure enables systems to admit users with limited permissions as necessary, or notify users via SMS that their account has been accessed.

**Intellectual Merit:**

This Small Business Innovation Research Phase I project strives to improve the authentication procedure for desktop operating systems, preventing unauthorized access even from actors with the login password. The most significant technical hurdle will be supplementing the existing login process with biometric signatures that are tuned to adequately balance security (unforgeability) with clemency (“forgiveness”). This means that users need not deliberately practice their typing rhythm to perfection, as small deviations will be filtered out in favor of more-significant typing characteristics; worry not about an “off-day” preventing you from accessing your machine.

Beyond improving the login procedure, the project aims to spark a conversation about unobtrusive mechanisms for securing information, and to change the nature of the relationship between enterprises, consumers, and the cyber-liability insurance industry.

**Broader/Commercial Impact:**

This project aspires to become a Software-as-a-Service product for institutions like banks to further secure online portals, and for sensitive information enterprises like Electronic Health Records to quantify their confidence that they are showing information to the right people. This confidence, in turn, provides companies with another tool in the information assurance tool belt, protecting them from legal exposure in the event of a data breach, and ultimately lowering their costs for cyber insurance.

**The Customer:**

Forbes, the NYTimes, and MIT’s Sloan Review all agree that, in this modern digital landscape, every company is a tech company. Industries dealing with sensitive information depend on their information assurance infrastructure to prevent catastrophe from affecting the bottom line. Cyber liability insurance premiums totalled $2 billion in 2015, and, according to [InsuranceJournal.com](http://www.insurancejournal.com/magazines/features/2016/04/04/403439.htm), are slated for a ten-fold increase over the next ten years. Legal costs and liability expenses from a data breach can hamstring businesses focused on rapid growth, like many modern Silicon Valley unicorns.

**The Value Proposition:**

Simple username/password combinations are no longer sufficient to protect a user’s data, and organizations that fail to implement modern security measures like two-factor authentication are paying the price. But even these new measures are flawed in some regard; for example, two-factor authentication depends on the user having a mobile phone available whenever they wish to access their account.

**The Innovation:**

This project aims to provide the benefits of multi-factor authentication without making too many assumptions about the user’s access to a charged mobile phone with an active phone number. Leveraging technologies already available in modern consumer PCs, this project will supplement the traditional password login with additional verification stages as needed.

Keystroke dynamics & typing rhythm are analyzed as a user enters their password, returning a confidence level that the user is in fact authorized. Returning a confidence level beneath an organization’s predetermined threshold prompts the user to perform additional voice recognition tasks to complete the login process. Acoustic metrics like pitch, intensity and timbre combine to provide a robust authentication mechanism, guaranteeing only authorized users gain access to a machine, network or web portal.