Capstone Abstract

Upon researching what issues exist today with technological implementations in security, two of the most prominent implementations are: keypads and IoT/smart homes. With those implementations came their respective complaints and issues amongst consumers.

With keypads, the continuous pressing of buttons would progressively create wear out the hardware, and customers would consistently experience malfunction with their machines. These malfunctions would create inconveniences for consumers, where they would have to wait for repairs [of the keypad] in order to gain access to the property using the keypad.

Currently (since this concept is relatively new) with smart home security systems, there is a fear of allowing a security system to be governed by internet, being that malicious attacks are always an option for malware authors when IoT is involved. For a user, a home is literally the LAST place/thing in the world that one would have uneasiness about, so this IoT component is worrisome for security purposes.

So, what type of system is as easy to use as a keypad, but as comprehensive and structured as a smart home security system? That’s where the proposed “Visual Security”, security system comes in. Visual Security would use computer vision and machine learning in order to allow users to submit a sequence of fingers gestures, as a password, into the camera of a device, in order to gain access into a property. How does this address the issues of keypads and smart homes?

When compared to keypads, Visual Systems will NOT use any technologies that will be susceptible to rapid mechanical or hardware issues, because the only way the user will be interacting with the system is the camera. "What about the wearing down of the device, that comes from the system being on being on all day waiting for the user to input a password?" That will not necessarily be the case with Visual Security; Visual Security will be implemented with proximity sensors to ensure that the device will ONLY be on when it’s time for the user to input their password. This means that the device will be on for a couple seconds of the day, and the device will never have to be touched by the user.

Compared with smart home security, the answer is simple: this system will not require any networking or internet access. Visual Security will ONLY depend its own internal software and stored information, which will only consist of the code used in its development, as well as the correct password required for access granted.

“What about security concerns that could come from such simplicity that comes from mere finger gestures?” With Visual Security, as long as there’s no carelessness involved, there shouldn’t be simple breaches from unwanted visitors. This is so because the device will be designed to ONLY take in the input when the user is certain “closeness” to the system, reducing the probability of “over-the-shoulder” password thievery. So someone stealing the password from the user, over the shoulder, would have the same likelihood here, as the probability of someone seeing a user enter a password into
a smart phone, which all boils down to the user. Therefore, if the user isn’t careless with how they use their phone, then a user of such responsibility will not experience such concern with this security system.

No technology is perfect. Being that there is a high dependency on the computer vision/machine learning aspect of the system, there will also be bugs that develop over time. The solution will be to provide the device with updates for these bugs, where the updates will be implemented the same way firmware updates are performed, since Visual Systems will not include any wireless networking. This approach of fixing bug development is no different from how smart phones produce updates for bugs that develop through their artificial intelligence.

The design approach of this project will be discussed in future reports, but the purpose of this abstract is to provide users with a deeper look into what Visual Systems is, and what the idea is about.