I. Introduction

The purpose of context aware authentication is to protect against unauthorized access to a system in the event that an attacker gets ahold of a user's credentials. Regardless if the credentials were obtained through social engineering or compromising the system at a technical level, context aware authentication will make it extremely difficult for an impersonator to log into the system by checking the "context" of the surrounding Internet of Things (IoT) devices and determining if the intended user is the person attempting to log into the system at a given location.

Currently, this is only practical for highly secure and localized systems where the user has to login on-premises because the sensor actuator network promised by IoT has not been fully realized. However, once IoT networks are common place and ubiquitous computing becomes a reality, location based access control could potentially become viable for a variety of everyday applications such as webmail, credit card transactions, and accessing property. The authentication backend of the proposed context aware authentication system put forward in this document will be referred to by its working name, PinPoint.

II. Security

A. General Security Concerns

In any authentication system security is a major concern as authentication is usually one of the major attack vectors that are explored when attackers are attempting to compromise a system. The need for well thought out security measures is only increased in the case of context aware authentication systems because the process for authenticating a user becomes distributed. Now, instead of trying to guess a password or crack a weak password hash, attackers may attempt to impersonate devices or use a man in the middle attack to make it appear that the user is in fact present for login attempt. Furthermore, once context aware authentication systems become widely distributed, a perception that the extra security provided by the system is enough to prevent attacks could potentially cause users to become more careless in choosing strong passwords.

B. General Security Concerns

The idea of context aware security to gather the "context" of the current login attempt from a variety of devices. These devices could include almost any type of sensor including card scanners, thermometers, motion sensors, and microphones. Using the context provided by these devices, PinPoint would then attempt to determine wheter or not the person attempting to log into the system is indeed the person they are claiming to be.