**Abstract**
April 27, 2014
Akhilesh Tyagi
Iowa State University
Sponsor: DHS

**Status:**
- New [x]
- Renewal [ ]
- Status Report [ ]

**Description:**
Traditional integrated circuits (ICs) based physical unclonable functions are passive and do not involve human user in the loop. In mobile systems, many authentication scenarios exist where the identities of both the mobile device and the user need to be established. IC based PUFs cannot generate signatures unique to both the user and device.

**Related Work Elsewhere:**
Physical unclonable functions have been developed for silicon bio-identity. They are based on ring oscillators, arbiters, and memory. For mobile devices, signatures based on accelerometers have been developed.

**How Our Work is Different:**
The response entangles both the device and the user. A device in Alice’s possession can have access to a different set of services than when it is in Bob’s possession.

**Milestones:**
A challenge path generated by the authentication layer will be traced by the user. The pressure values reported in the MotionEvents will be used to generate a binary response. This response needs to have enough variability over different challenges, different devices and different users. However, it should be reproducible for the same user, same device, and same challenge scenario.

**Deliverables:**
2. Statistical characterization of a pseudorandom generator based on this PUF.
3. Integrating a secure Android layer for PUF challenge-response based authentication mechanism based on ARM TrustZone
4. An application framework development using this authentication mechanism.

**Related Work in S²ERC:**
None.

**Affiliate Support:**

**Potential Benefits:**
Layered, differentiated services can be provided for mobile devices that are also user based.

Stronger cryptographic blocks that compose a software based implementation with the physical unclonable functions are feasible. We will illustrate that with a pseudorandom number generator.