SECURING THE HUMAN PROTECT SURFACE

Applying Secure Cognitive Architecture to Military Base Security

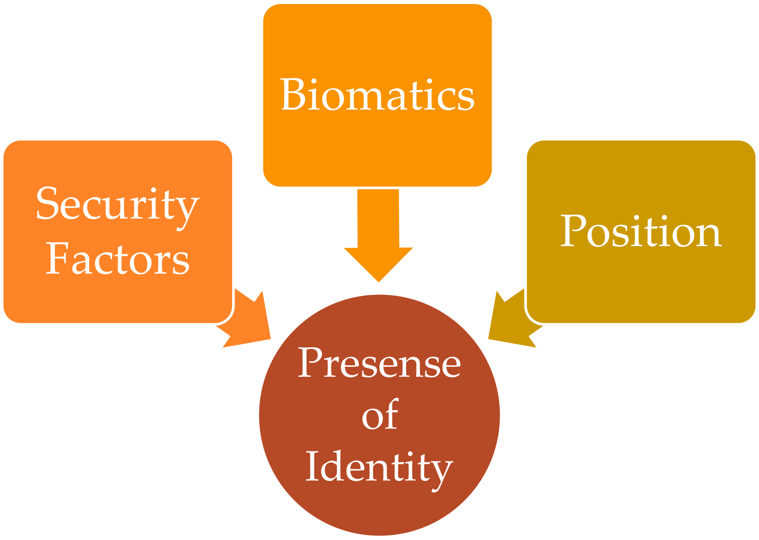
Jason L. Lind, USAF (Sep.)
Coalition Lead / MultiPlex.studio
lind@multiplex.studio

11 September 2020

Historically base security has had a focus of maintaining a tight perimeter with additional perimeters configured at, and within building sites. Ostensibly this would be a proper application of Zero-Trust Architecture (ZTA) however this strategy is missing a key component: continuous evaluation of the protect surface.

The primary goals are to achieve the following:

- Real-Time tracking of authorized members on the military GPS and milCloud infrastructure
  - Identify COTS or develop custom Android based Health Watch
- Vitals monitoring to realize enhanced biomatics in addition to increased health monitoring
  - Deep Learning models to differentiate wearers of uniquely identified wearables as individuals – when coupled with a HUF (Hardware-Unique-Factor) enabled device this would provide constant presence of identity
  - Analyze a combination of temperature, blood pressure, and pulse-ox to identify potential COVID-19 infections and aid in contact tracing
  - Provide real-time health statistics to prioritize rescue/evacuation



- For at least select members: mixed/augmented reality goggles with heads-up-display (HUD) capabilities for interacting with both the environment and other members
  - Base directions
  - Enhanced signage based on Multi-Level-Security
  - Visual Authentication of individuals by Security Forces
  - Visualize social distancing requirements

When interacting with devices, humans secured in such a manner plug into the Secure Cognitive Architecture.

ACHIEVING A BASE BEYOND THE BASE

Extending the Physical Protect Surface into Cyberspace

By many predictions, the sudden uptick in telework among DoD service members and civilian staff as a result of COVID-19 is only going to accelerate. However for many to perform their work they must have access to highly secured networks (e.g. SIPR) and their information which is currently only available on a physical base.

This is primarily for two reasons:

1. Physical access security to the base is viewed as an enhanced vector to better assert the identity of those accessing classified systems
2. Secure access often utilizes physically separated classified and non-classified networks

For (1) we contend that a perimeter based physical security model - even one that continuously bounds the protect surface by securing movement within and within each new perimeter - is only a possible factor and a proper "presence of identity" factor can augment, if not replace, physical security when accessing cyberspace systems.

As to (2) we agree that maximum security involves separate networks however realistically in our new world we contend that this is not an option – all military activity comes with risk analysis, and we must mitigate security risks as much as possible while providing operational functionality. Bottom line if we live in a world where many personnel find themselves primarily working off-physical base we need to build a "virtual base" around them.

By reading and analyzing real-time biometric data and combining that with military GPS data that gives near exact position resolution we can have a greater "verification proposition" for determining the true identity of the person access a device at their location. This could include 1st party secured devices such as cell phones or laptops that have additional military grade factor readers – including: fingerprint, iris and smartcard readers – or even 3rd party devices such as public kiosks with only username/password verification.

Based on the number of factors, and a confidence score of those factors, access to SIPR and other secure network resources could be partially or fully allowed forming a "base beyond the base."

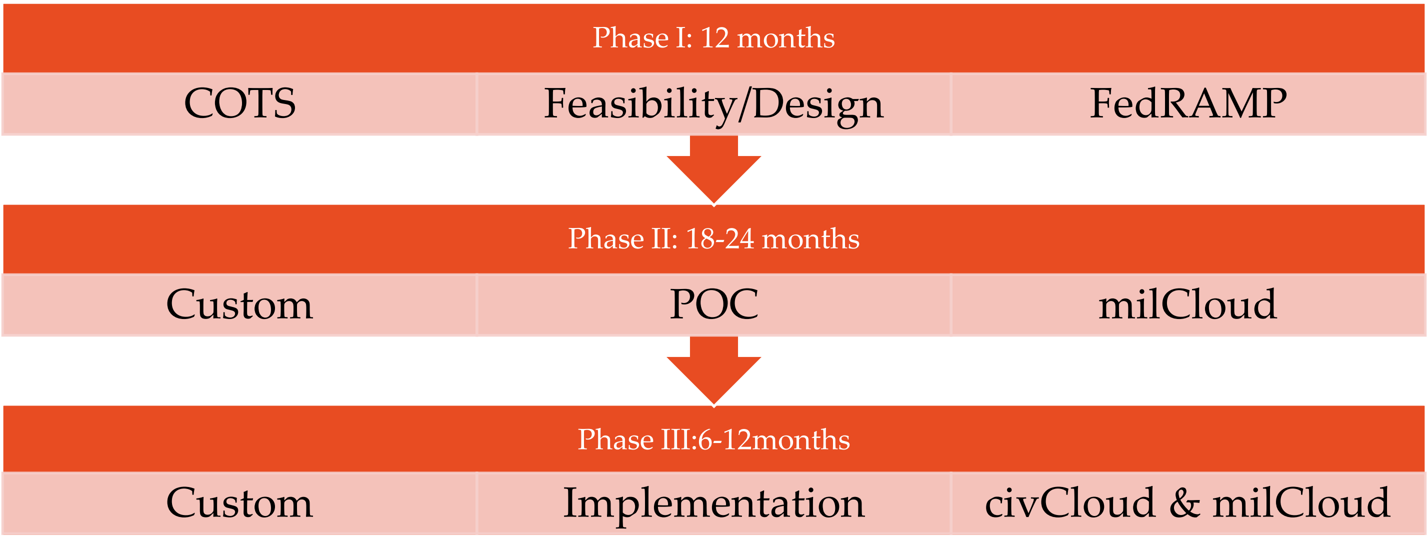
http://wwidew.net/mil.api.fit.pdf

http://wwidew.net/CSH.pdf

SBIR Phase I Definition

MultiPlex.studio proposes a feasibility study to develop a biomatics identification scheme and determine just how fuzzy it is – that is the amount of identity collusions based on the biomatics alone, answering the question: does biomatic identification produce not only statistically meaningful results but enough of a result to justify a claim of increased security.

While Phase II will involve developing new hardware to provide an integrated – convenient and secure – package, Phase I will focus on using COTS (Commercial off the Shelf) products such as fitness trackers, watches and temporary subdermal implants. Phase I should be developed under FedRAMP specifications whereas Phase II would be under milCloud as there may not be alternative COTS devices to those that are not milCloud ready.



Phase I: 12 months

COTS	Feasibility/Design	FedRAMP

Phase II: 18-24 months

Custom	POC	milCloud

Phase III:6-12months

Custom	Implementation	civCloud & milCloud

Addressing the "Gattaca" Problem

Whenever one deals with enhancing the collection of biomatic data, particularly at this scale, one must be mindful of ethical considerations. Specifically:

- An obligation to go beyond the call of duty when protecting individual's HIPPA rights

The Supreme Court has ruled there is a right to privacy in the Constitution of the United States and as such healthcare information must be protected – if not our service members could face discrimination in future employment by the civilian sector. It is important to note that these sensors can and should be used to identify service members whose health precludes them from duty.

However this must be applied in context of US Law and the UCMJ – careful not to extend these definitions using this new technology, for example: it would probably be a bad idea to perform deep learning to disseminate on potential risks versus actual real-time symptoms. As such the architecture must only enable real-time alerts on health issues instead of a full history – and even if the raw data was able to be collected over long periods of time, once trained the model should only have aggregated, non-identifiable data.