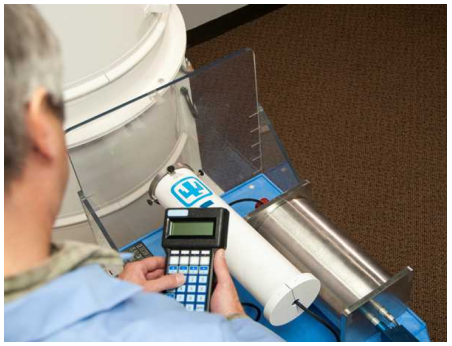
SAND2013-8425C

Exceptional service in the national interest

Sandia National Laboratories



Ephemeral Biometrics: What are they and what do they solve?

Peter S. Choi, Ph.D., CISSP, CSSLP

David Zage, Ph.D.

U.S. DEPARTMENT OF ENERGY | NNSA

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

What is Identity?

Sandia National Laboratories

"Identity: the qualities, beliefs, etc., that make a particular person different from others"

- What does it mean to me?
  - Self-awareness … "I think, therefore I am"
  - It exists only inside of your mind - "virtual" identity
  - This is what motivates us to get up every morning and live – "self preservation"
- What does it mean to others?
  - Sense of social acceptance…you want others to value you as much as you value yourself
  - This is the part of the identity that is assigned to you externally, - a "physical" identity
  - This physical identity is necessary for society to function properly

Cyber Identity

- Pervasive/Ubiquitous Computing
  - Embedded, connected computing device
- Cyber identity is essentially a long binary string, generated and managed by computing infrastructure
  - If operating system is compromised, digital identity can easily be created
  - It can be easily copied and retransmitted
  - Digital identity is virtual
- Cyber identity is largely anonymous
  - Crosses border, gender, time and space limitations
  - Cyber activity is done by someone or something but very hard to pin-down who is actually doing it

Cyber Identity ≠ Physical Identity

Sandia National Laboratories

- Authentication in cyber-world often defies the laws of physics
  - A person cannot be in two different places at the same time
  - There is a limit to how fast a person can move through space and time
  - A person's identity may not be inter-changed
- Cyber identity, as currently designed, has nothing that anchors it to the kinetic world
- What is wrong with having cyber-space "Avatar"?
  - Biggest bank heist – $45 million, ATM bank heist (Rakbank, Bank of Muscat: Feb 2013)
  - Stuxnet
  - Obama and Xi Jinping

Cost of Cyber Security?

Sandia National Laboratories

- 2012 survey of technology managers in the US *
  - Must increase current $5.3 billion to $46.6 billion to repel 95% of attacks
  - Estimation based on addressing 95% of currently **known threats** and **vulnerabilities**
- Cyberspace, full of anomalies, bugs, gaps and holes
  - Operating systems are massively complex
    - Windows NT 3.1 (~5 million SLOC)
    - Windows 200 (~29 million SLOC)
    - XP (~45 million SLOC)
    - Red Hat Linux 7.1 (~30 million SLOC)
  - Conservative
    - 4 to 11 errors per source lines of code (needs legitimate source quote like NIST)
    - Even for low 1 bug/1000 SLOC estimate, XP will have potential 45,000 bugs
  - Hackers can pick and choose from abundant source of vulnerabilities and weaknesses inherent in existing OS and software

*Ponemon Institute & Bloomberg 2012 Survey

Virtual Identity = Cyber Insecurity

Sandia National Laboratories

- Industry response (i.e., what you *know, have* and *are*)
  - Use multi-factor authentication
    - RSA Token
    - CAPTCHA
    - Text messaged, one time password
    - Fingerprint
    - Etc.
  - Unnatural for human beings to continuously authenticate
  - These are still all “virtual,” binary identification
  - Unsolved issues:
    - OS and software complexity issue ➔ insecure cyber-space, compromised identity
    - Stronger authentication ➔ Greater inconvenience to end users
    - Unable to replicate attributes of physical identity

Attributes of Physical Identity

Sandia National Laboratories

- It exists in kinetic world where identity obeys laws of physics
  - Can't be in multiple places simultaneously
  - Cannot travel at speed of light/wire ➔ China to US and US to Russia
  - In cyberspace, "There can be only one" mantra does not exist
- People will suffer the consequences of their actions
  - Crime must be committed in person
  - Can not hide behind cyber anonymity
  - Local laws, local rules matter
- Person's identity is captured in time and space
  - Your "spouse" – actively authenticates and no simultaneous existence
  - Abraham Lincoln -- historical context matters

"Where you are" as Fourth Factor Authentication (4th FA)

Sandia National Laboratories

- How do we build-in attributes of physical identity into cyber network?
  - Three Rules of Authentication
    - Does not interfere with operational modality
    - Continuous, active authentication
    - Obeys law of physics -"time dependency" and "space occupancy"
  - Indoor, Real-Time Location System (RTLS)
    - "Where you are" as 4th FA
    - Requires wearing electronic beacon or sensor ➔ Concept demonstration lab at SNL
    - Requires "ephemeral biometrics (EB)" technology for coupling electronic token ID to human identity
- RTLS + EB ➔ Creation of unique Human-Machine identity

Ephemeral Human-Machine Identity

Sandia National Laboratories

- Why not just use biometrics?
  - Physiological modality – intrusive and cumbersome
    - *Skyfall*, James Bond movie
  - High risk to institutions harvesting biometric data
  - Non-revocable, once compromised, permanently compromised
    - E.g., Apple's iPhone 5S fingerprint technology
- Then what?

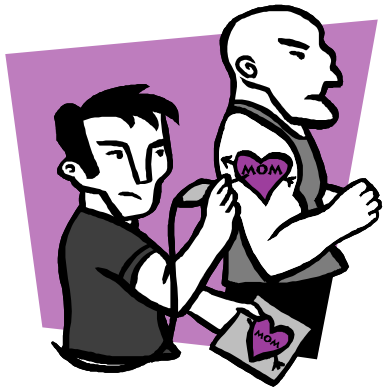
Ephemeral Biometrics: *defined as distinctive identifiers derived from merged traits of human factors (fingerprint, password, etc.) and the persistent live-state of the user.*

&

Ephemeral Biometric Identity: *defined as unique semiconductor identity merged with active EB measurements.*

EB Device Form Factors

- Device qualities:
  - Socially acceptable
  - Fashionably acceptable
  - Reusable
  - Easy to reissue
- Potential Devices:
  - **Watch**
  - Necklace
  - Tattoo
  - Google glass
  - Etc.



Potential Candidate for EB Watch

Sandia National Laboratories

Product/ Company	Modality	Heart Rate	Respiratory	Blood Oxygen	Emotion	Skin Temp	Perspiration level	Sleep	Blood Pressure
Tinke	Photoplethysmograph (PPG)	Yes	Yes	Yes	N/A	No	No	N/A	No
Jawbone UP	Accelerameter	No	No	No	No	No	No	Yes	No
Basis (or Pulse Tracer)	Photoplethysmograph (PPG)	Yes	No	No	No	Yes	Yes	Yes	No
Fitbit	Accelerometer	No	No	No	No	No	No	Yes	No
DirectLife	Accelerometer	No	No	No	No	No	No	Yes	No
BodyMedia	Accelerameter	No	No	No	No	No	No	Yes	No
Affectiva Q Sensor	Eletrodermograph (EDG)	No	No	No	Yes	Yes	No	N/A	No
Life Microscope	Accelerometer	No	No	No	No	No	No	Yes	No
Valencell	Photoplethysmograph (PPG)	Yes	No	Yes	No	No	No	No	No
Mio Alpha Heart Rate watch	Photoplethysmograph (PPG)	Yes	No	Yes	No	No	No	No	No
Xbox One	Photoplethysmograph (PPG)	Yes	No	No	No	No	No	No	No
STBL Medical Research AG	??	No	No	No	No	No	No	No	Yes

What Physiological Measurements?

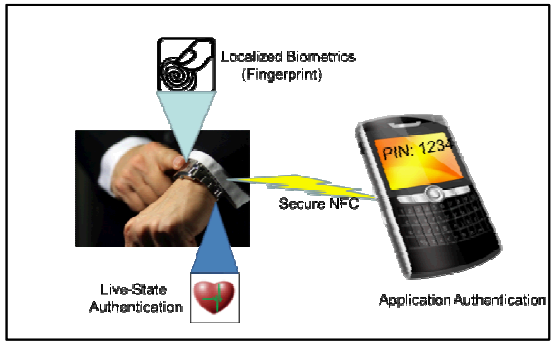
Sandia National Laboratories

- Electromyograph (EMG)
- Feedback thermometer
- Electrodermograph (EDG)
- Electroencephalograph (EEG)
- Photoplethysmograph (PPG)
- Electrocardiograph (ECG)
- Pneumograph
- Capnometer
- Rheoencephalograph (REG)
- Hemoencephalography (HEG)
- Magnetic field, blood flow interaction

Areas of Technical Innovations Needed

Sandia National Laboratories

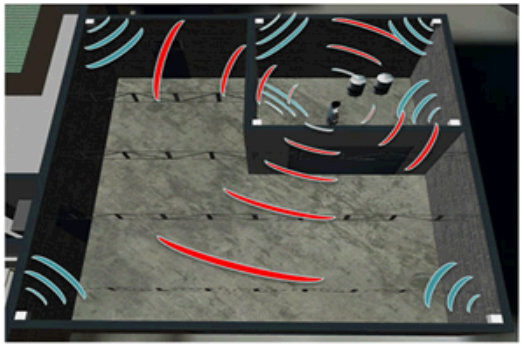
Ephemeral Biometrics



Human-Machine Identity

+

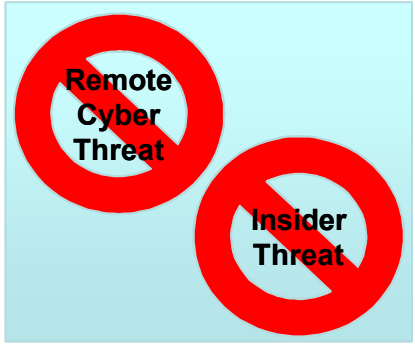
4th Factor Authentication



"Where You Are" as 4FA

=

Active/Persistent Identity



Persistent Identity

Human-Machine
Coupled state

Sensor vs Beacon, WiFi, UWB, GPS, Ultrasound, Sound, IMU, IR, RFID, mixture of solution

Integrated Safety & Security Application➔ 4FA Network protocol, Portability, scalability, Availability, integrity

R&D Efforts at SNL

Sandia National Laboratories

- Technology demonstration lab
  - 4th FA demonstration stage
  - Two patents related to EB
  - Looking for potential CRADA partnership
- EB+4th FA = Active/Persistent Identity
  - How does this address remote cyber threats?
  - How does this address insider threats?
  - Examples of “Active Authentication” Applications
    - Health and Safety
    - Finance
    - Computer/Network Access
    - Building Access
    - Gun control
    - Material Processing, Control & Accounting (MPC&A)

QUESTIONS