SAND2015-4481C

Exceptional service in the national interest

Sandia National Laboratories

Ephemeral Biometrics: Viable Active Authentication

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

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

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

Issues with Cyber 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"?
  - Identity based on "static information" is flawed
  - When "static ID" is converted to digital format, the authenticity of Identity becomes extremely fragile

Cybersecurity is Extremely Complex

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 2000 (~29 million SLOC)
    - XP (~45 million SLOC)
    - Red Hat Linux 7.1 (~30 million SLOC)
  - Conservative
    - Even for low error estimates of 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

Why do we need Solution like PUF?

Sandia National Laboratories

- Slew of digitized identity thefts
  - Target (40 Million Accounts)
  - Home Depot (56 Million Accounts)
  - JPMorgan Chase (76 Million Accounts)
  - Biggest bank heist – $45 million, ATM bank heist (Rakbank, Bank of Muscat: Feb 2013)
  - Stuxnet
- Cost of cybercrime and cyber espionage
  - $300 Billion to $1 Trillion (2013 MacAfee Report “Center for Strategic and International Studies”)
- Reliance on virtualized/digitized static ID
  - Cloneable, replicable static information
- Tokenized, non-replicable dynamic digital ID
  - True, two factor authentication
  - Solves the problem of scale (paradigm shift from one-to-many vs one-to-one attack model)

Cyber Identities are Hard to Manage

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.
  - 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
      - Unnatural for human beings to continuously authenticate
    - Cyber identity, unable to replicate attributes of physical identity

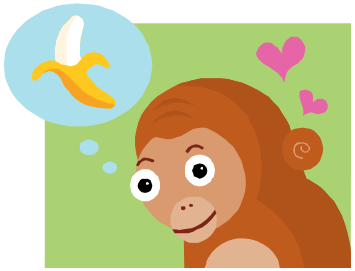
Attributes of Physical Identity

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

What is Authentication?

- Validating the identity (H➔M)
  - What you are
  - What you know
  - What you have
- Provides access privileges to people
  - Information
  - Assets



Authentication Factor One

- What you know (Knowledge)
  - People often forget
  - Limited complexity
  - Costly to maintain
  - Single-time mediation
  - People share their passwords

Authentication Factor Two

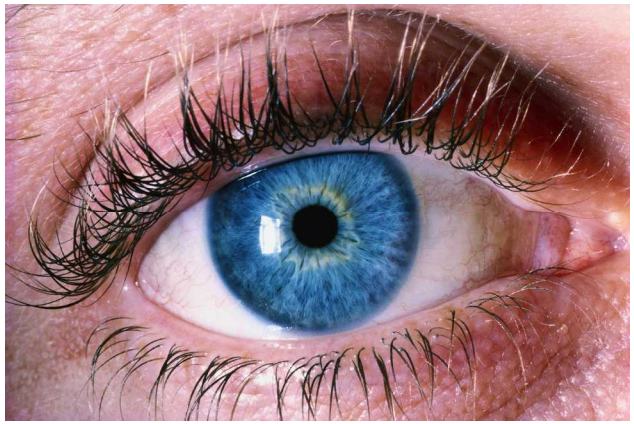
Sandia National Laboratories

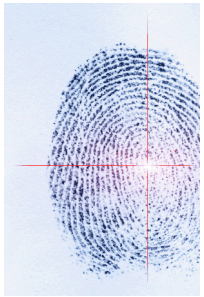
- What you have (Ownership)
  - Can be stolen or lost
  - Counterfeited
  - Mostly relies on human beings to check the validity
  - Single-time mediation
- Technological Innovation Opportunities here
  - Ephemeral Biometrics
  - Physically Unclonable Digital ID

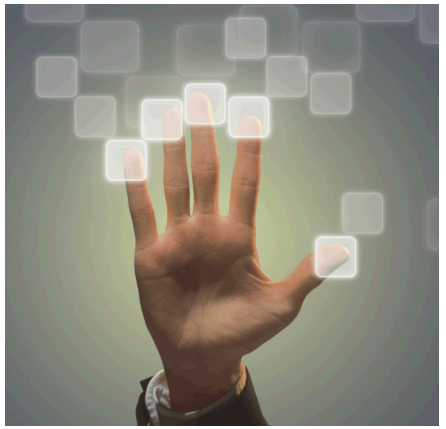
Authentication Factor Three

- What you are (Inherence)
  - Invasive properties of the biometrics
  - Once compromised, permanently compromised
  - Biometrics do not work on certain individuals
  - Poses potential risk to biometric owner
  - Can change over time
  - Single-time mediation

- Innovation Question:
  - "What does your device knows about your?"➔ Biometrics







Limitations of Traditional Three Factor Authentication Methods?

Sandia National Laboratories

- All 3 Factor Authentications (3-FA) suffer from

  - Single-time mediation ➔ Once an identity is authenticated, the insider is given complete and full unlimited access.
  - These 3 known factors can only be used sparsely in fear of annoying the end users if identity is requested too frequently.

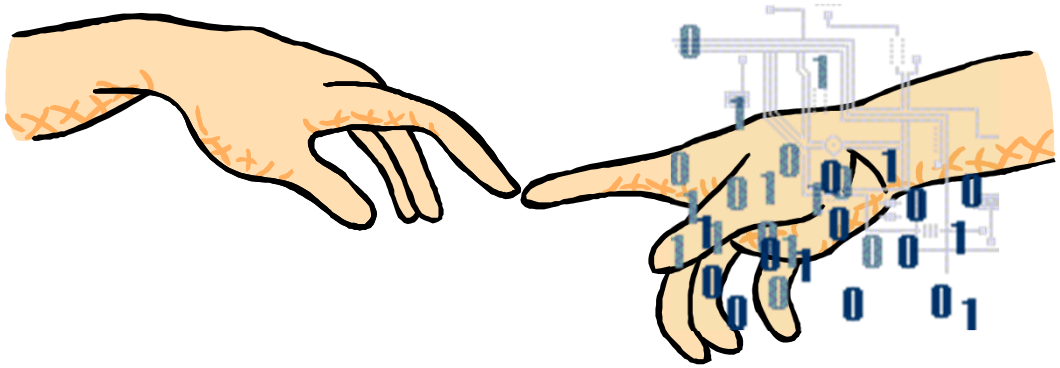
  - These 3-FA methods rely on virtual identity ➔ Susceptible to remote attack
    - Allow access to cyber assets from multiple places
    - Cyber identity does not account for the physical laws

SAND #2012-8776 C

What Makes Authentication Secure?

Sandia National Laboratories

- Interested in design principles/rules for human-machine authentication
- Created Three Rules for Authentication
  - Avoid “security by death”
  - Persistent identity
  - Obeys the laws of physics



Authentication Rule One (Avoid)

- Unless required by established security policies or safety rules, authentication may not hinder operational tasks at hand nor be cost prohibitive

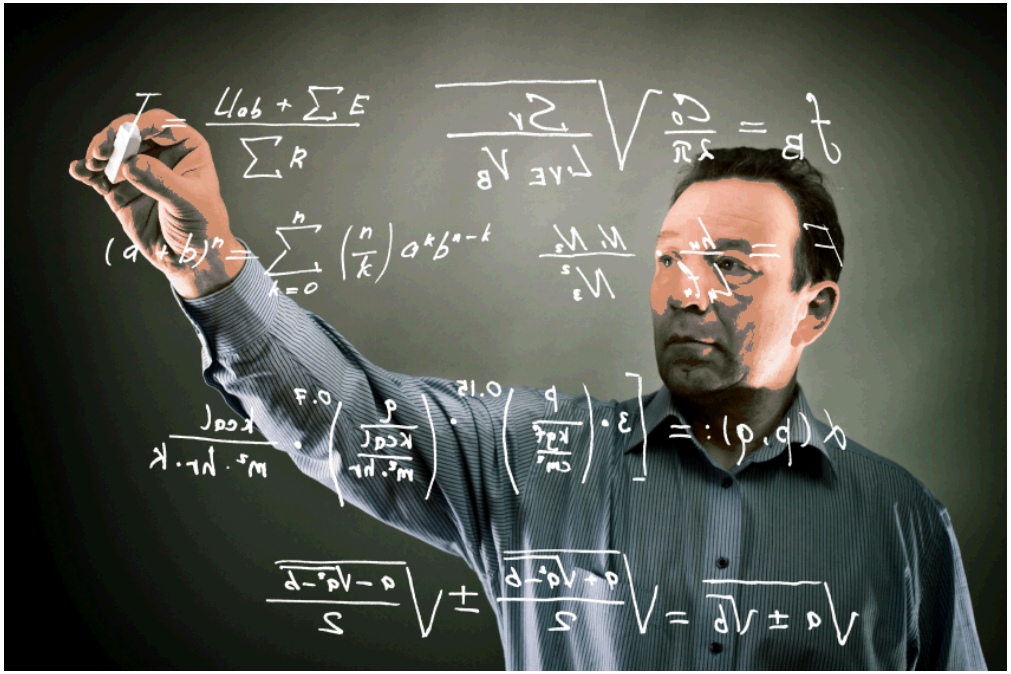
Authentication Rule Two (Persistent)

- Unless it violates the first rule, the integrity of authenticated data must be persistent and available throughout the authenticated state.

Authentication Rule Three (Obey)

Sandia National Laboratories

- Authentication may not violate 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



Ephemeral Human-Machine Identity

Sandia National Laboratories

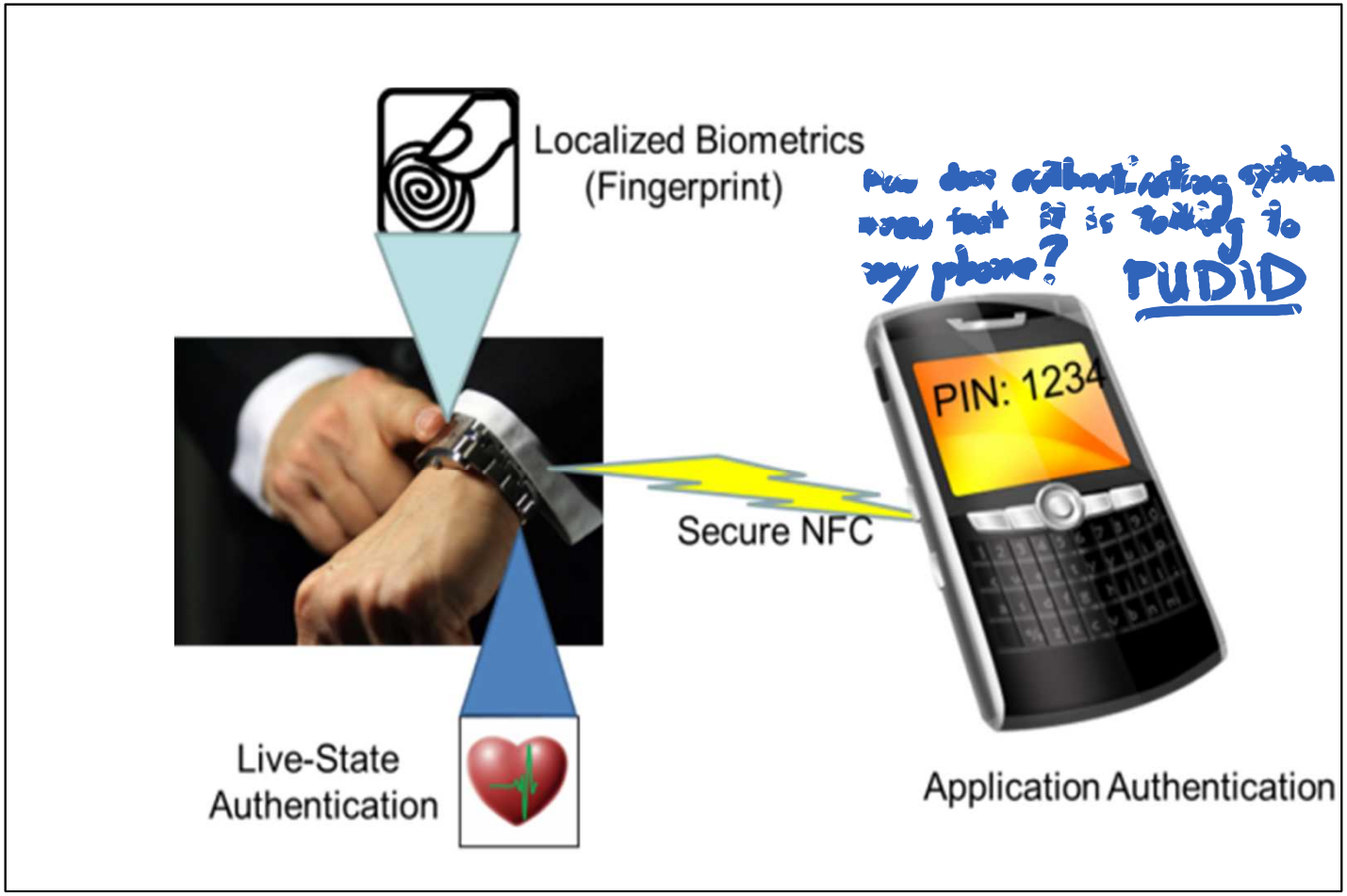
- Why not just use biometrics?
  - Physiological modality – intrusive and cumbersome
    - *Skyfall*, James Bond movie
  - High risk to institutions harvesting biometric data
  - Non-revocable, once compromised, permanently compromised
    - E.g., Apple's iPhone fingerprint technology
- Then what?

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.*

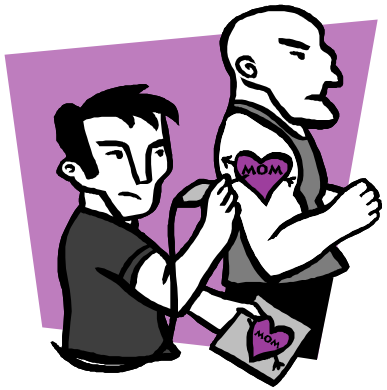
Ephemeral Biometrics



Human-Machine Identity

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	Accelerometer	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	Accelerometer	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

R&D Efforts at SNL

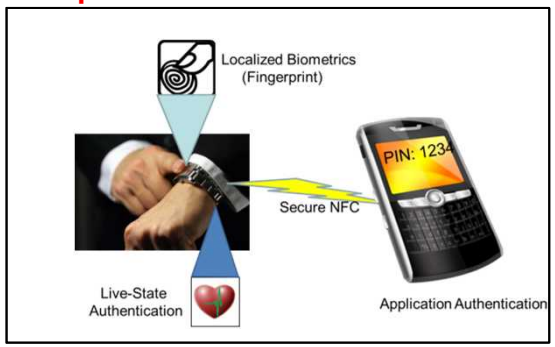
Sandia National Laboratories

- Technology demonstration lab
  - 4th FA demonstration stage
  - Two patents related to EB
  - Two more authentication patents in process of being filed
  - 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 (i.e., POS)
    - Computer/Network access
    - Building access
    - Secure drone control
    - Material Processing, Control & Accounting (MPC&A)

Areas of Technical Innovations Needed

Sandia National Laboratories

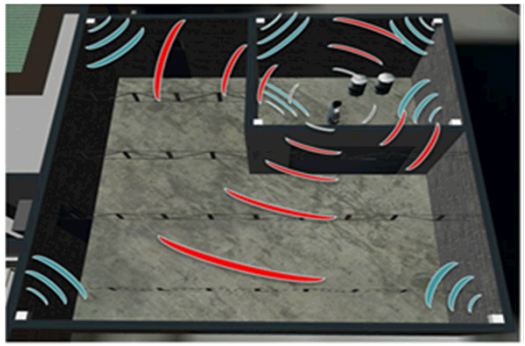
Ephemeral Biometrics



Human-Machine Identity

+

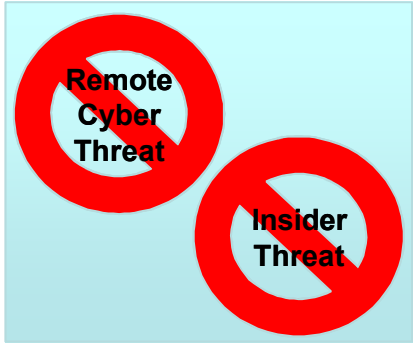
4th Factor Authentication



"Where You Are" as 4FA

=

Active/Persistent Identity



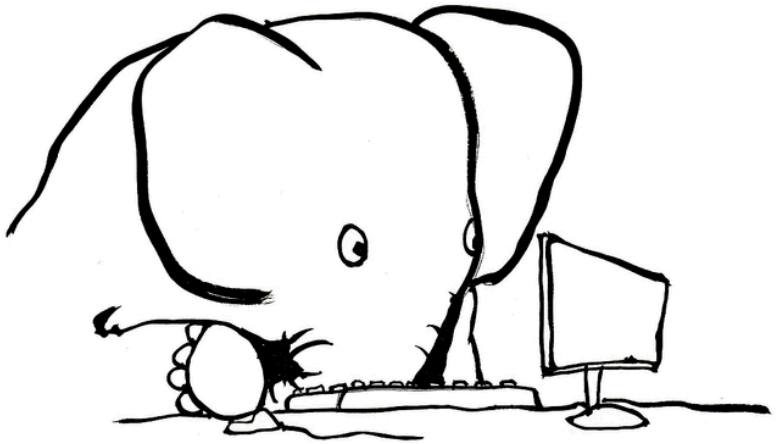
Persistent Identity

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

Parable of Mouse



- Verizon's 2013 Data Breach Investigation Report – An elephant in the room
  - 75% of all known network intrusions - weak or stolen credentials
- Parable of mouse: weakness inherent in cyber identity, a front door to entrance to cyber network resources

QUESTIONS