THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

FedEx INSTITUTE OF TECHNOLOGY
THE UNIVERSITY OF MEMPHIS

GA-Based User Identity Management System

Prof. Dipankar Dasgupta, IEEE Fellow

Director: Center for Information Assurance

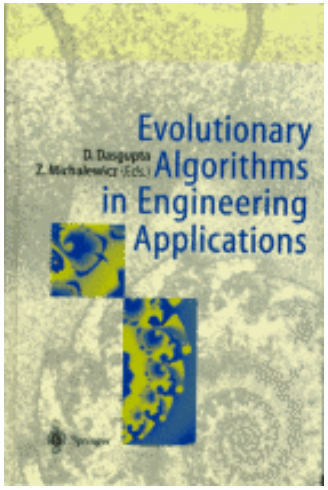
Center website: cfia.memphis.edu

Dipankar Dasgupta's Ph.D Thesis

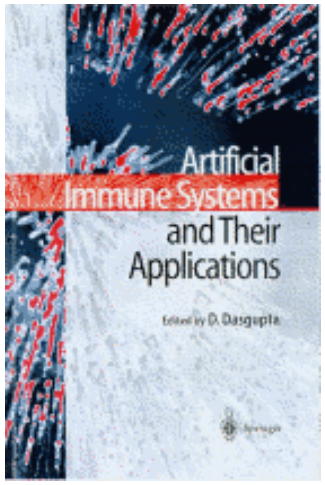
Structured Genetic Algorithms in Search & Optimization, 1993

BOOKS PUBLISHED

1997

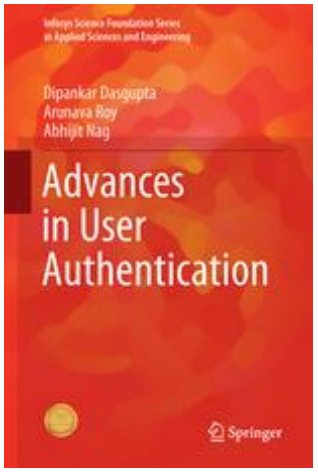


1998

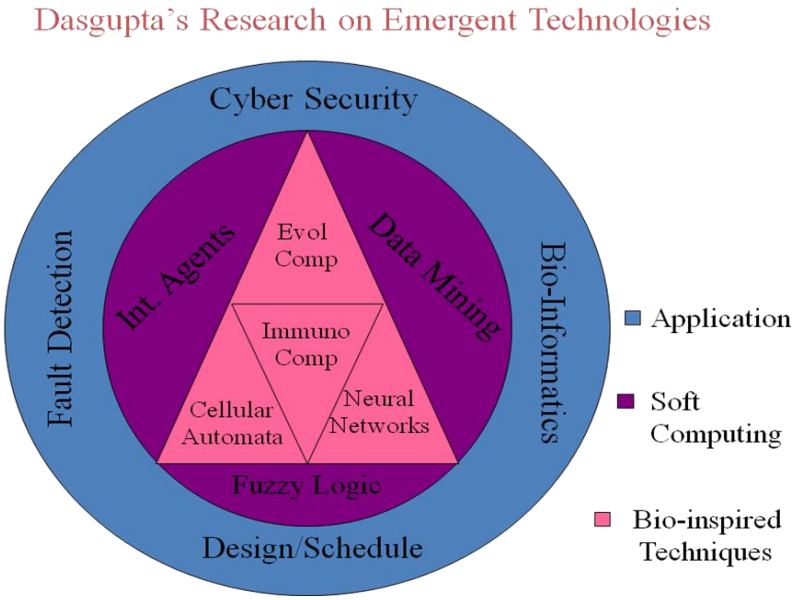


2008

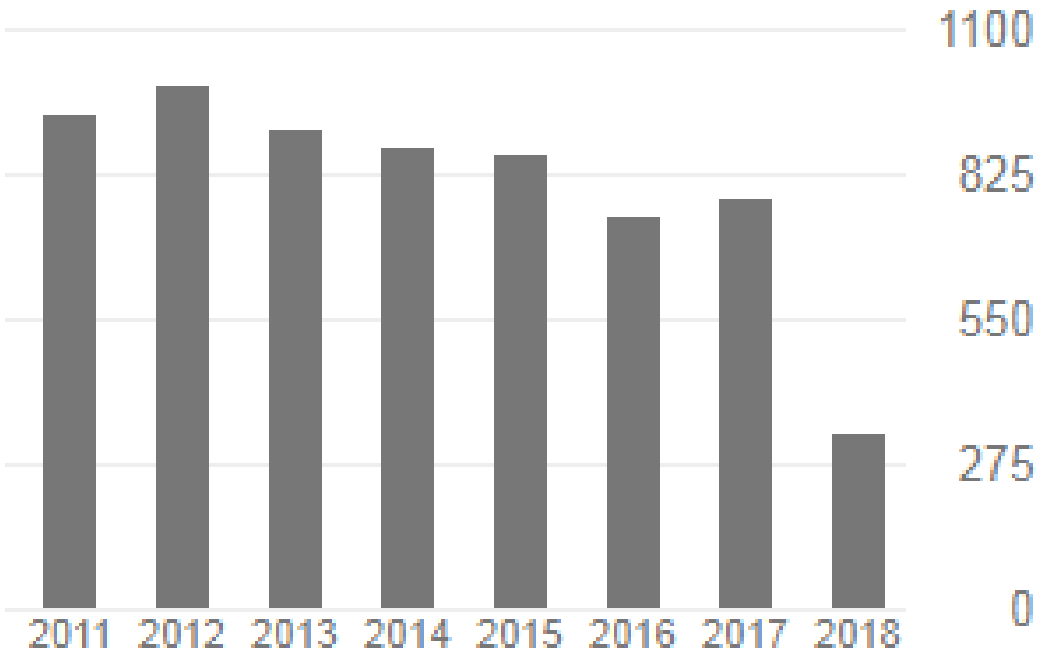
2017



My Research Publications



250+ Publications	All	Since 2013
Citations	15105	4515
h-index	57	31
i10-index	125	75



Conducting multidisciplinary/ collaborative research

Dasgupta's research citation statistics as shown in Google Scholar (accessed on July 7, 2018).

Agenda

- User Identity Verification: Authentication
- Multi-Factor Authentication (MFA)
- Active/Continuous Authentication
- Adaptive Multi-Factor (A-MFA)
  - Overview: Goal & Objectives
  - Design of A-MFA Framework
  - A-MFA Prototype System
  - Use Cases for A-MFA
- Cyber Identity Ecosystem
- Summary

Authentication

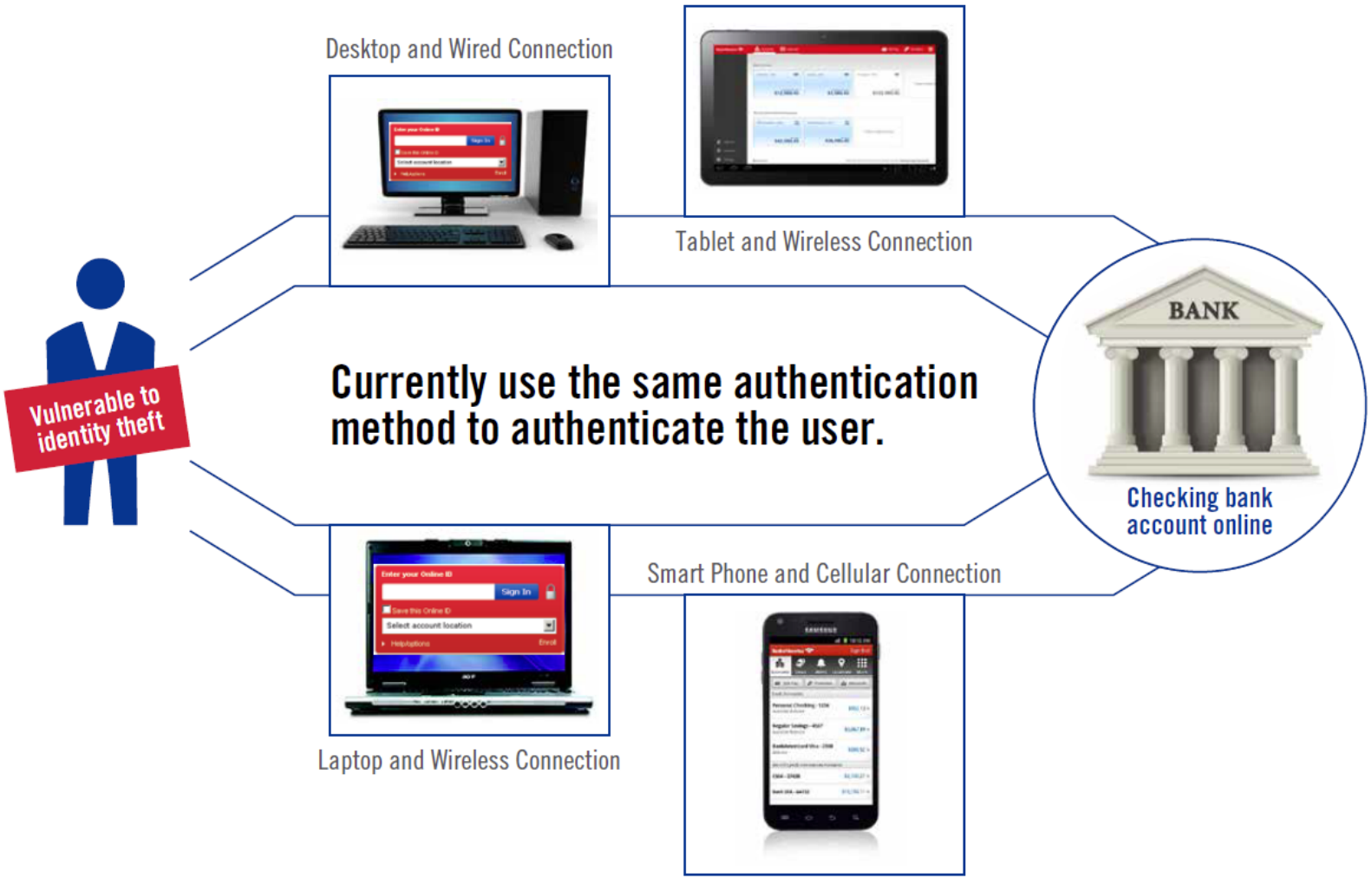
- Authentication is the critical safe guards against illegal access to computing systems.
  - the process of giving individuals access to system objects based on their identity.
- Ensures that the individual is who he or she claims to be.
  - But says nothing about the access rights of the individual.
- Challenges
  - Correctly identify authorized users in particular Operational Settings.
  - Take appropriate action on demand basis to prevent un-authorized access.

Password-Based Authentication

- Single-factor
  - Username-password. (most widely used as of now!)

- Issues
  - Mostly targeted by the attackers
  - If this single channel is compromised, the users are denied of the service until it is restored
  - Recent advancement of computer processing power, makes to check all possible cases in a short amount of time
  - Difficult to remember for a wide variety of websites

Need for Multi-Factor: Sample Scenario



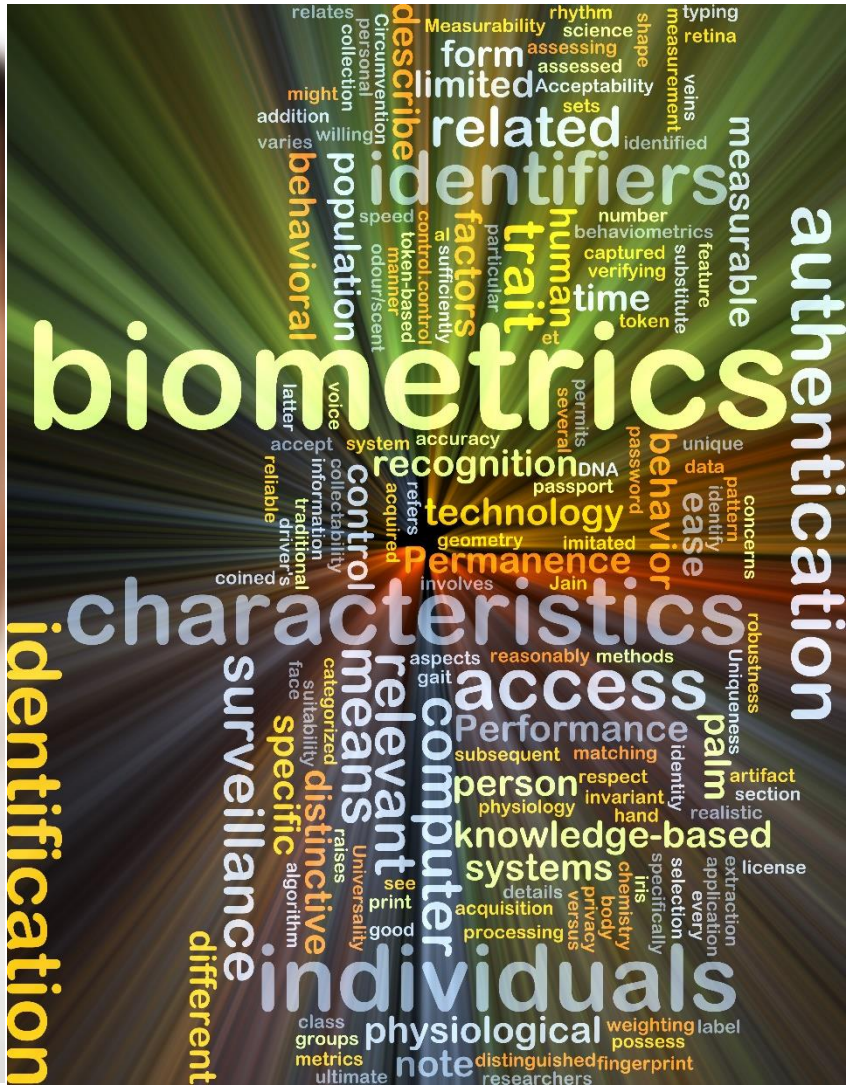
Perspective for Multi-factor Authentication

- What the User knows
  - Password, PIN, pass phrases
- What the User has
  - Smart card, digital certificate, driver's license
- Who the User is
  - Fingerprint, iris scan, voice recognition
- Where the User is
  - GPS, IP address of user

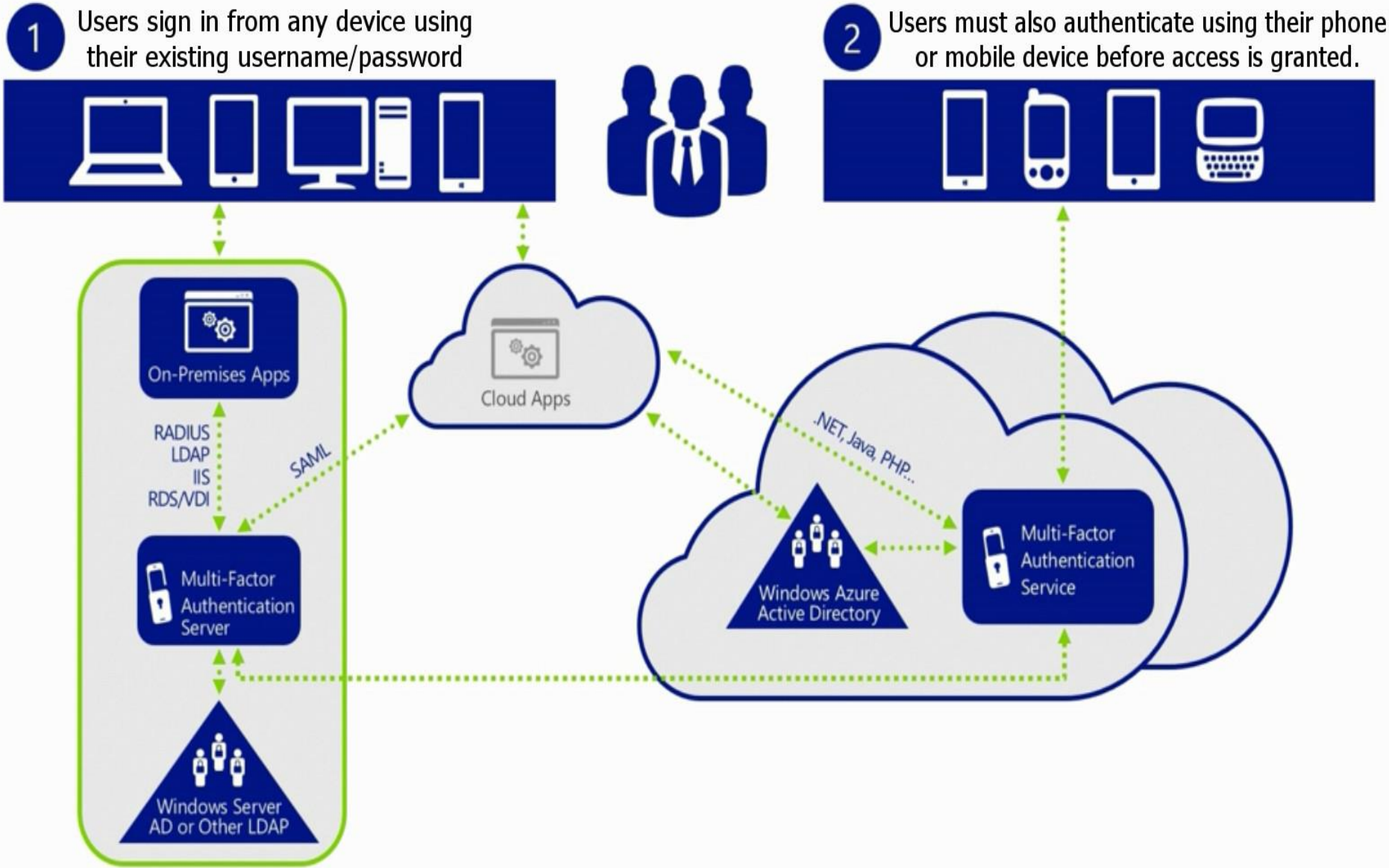
Two Factor

- Generally Password along with SMS for verification code

Authentication Types



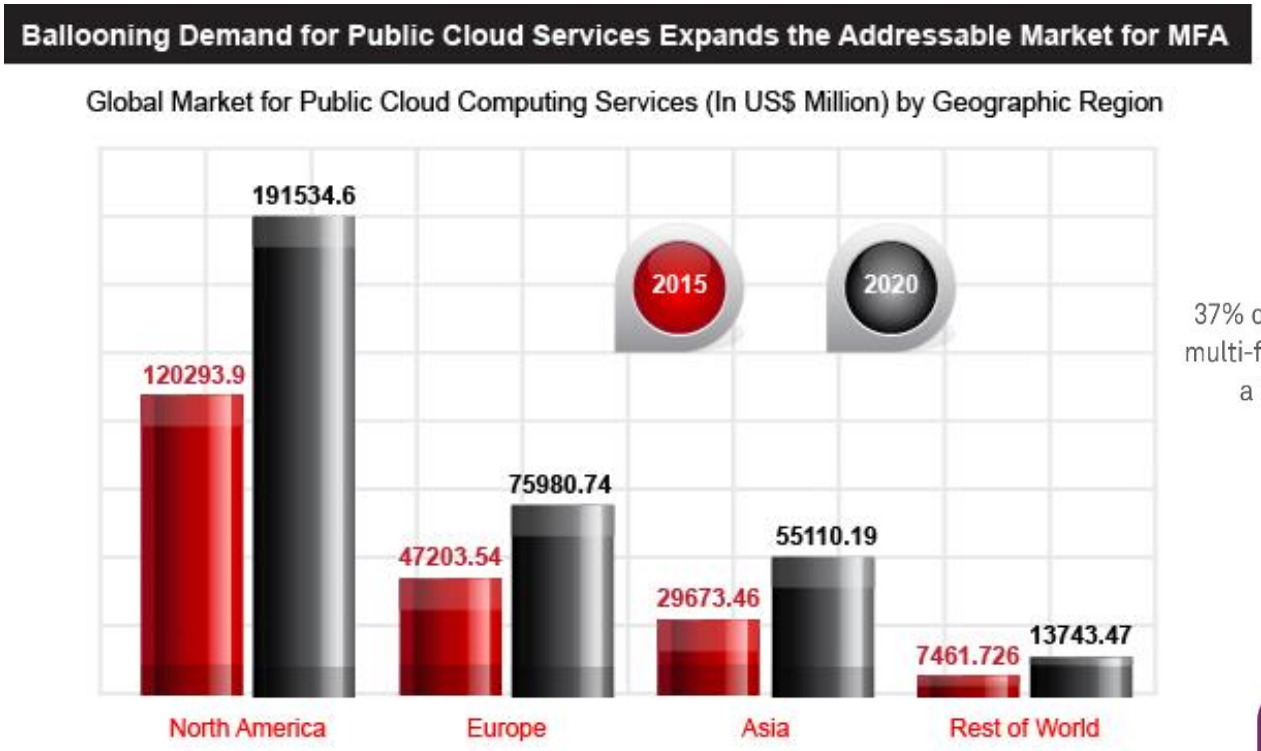
Product- Microsoft Azure



Different MFA products in Market Today

Product Name	Vendor	Factors	Features	Source (Website)
SecureAuth IdP	SecureAuth	Two factors and SSO (out of 20)	Mobile, cloud, web or VPN	www.secureauth.com
RSA SecureID	RSA	Two factors	Software (smartphones, tablets and PC) and hardware authenticators	http://www.emc.com/security/rsa-securid.htm
Safenet	SafeNet	Two factors	Cloud, Password + SMS/Hardware Token	www.safenet-inc.com/multi-factor-authentication/?tabnum=2
SecurEnvoy	SecurEnvoy	Two Factor	Tokenless (One-swipe, SMS Preload, Soft Token, Voice Call, Email Preload)	www.securenvoy.com/
Symantec O3	Symantec	Cloud identity and access control (Two Factor authentication)	Cloud applications (set policies for groups, persons, devices) [security control point]	www.symantec.com/page.jsp?id=O3
Microsoft Azure	Microsoft	Multi factor (Phone call, SMS and Password)	On premises and cloud authenticationsMobile Device + user-id and password	azure.microsoft.com/en-us/services/multi-factor-authentication/
Deepnet DualShield	Deepnet Security	Two factors out of 10 different methods	SMS, Voice, Mobile App, Face, Keystroke, Smart Cards	www.deepnetsecurity.com/products/dualshield/
Swivel Secure	Swivel Secure	SSO + two factor	Mobile App, SMS, tokens, Telephony, Browser	www.swivelsecure.com/
miniOrange Strong Authenticati	miniOrange	SSO + two factor	14 different authentication types	miniorange.com/strong_auth

Current MFA trends



- **Effectiveness of MFA as a potent tool to tackle BYOD security complexity benefits the market.**
- **Rise in smartphone thefts spurs use of MFA on mobile devices.**
- **Cloud services need MFA to establish customer trust and increase cloud adoptability.**

- Amazon, Google, Yahoo, Dropbox, Facebook, LinkedIn, Twitter, Microsoft uses two factors to access their online services for authentication.

http://www.strategyr.com/MarketResearch/Multi_Factor_Authentication_MFA_Market_Trends.asp

Why we should care?

Aside from the fact that all companies should take their customer data security seriously, not having adequate authentication mechanisms in place increases the potential of corporate PII breach risks including:

Legal Liability

- Government Enforcement Action
- Class Actions
- Individual Actions

Reputational Exposure

Business Consequences

Typical Breach Costs

- Outside Counsel
- Credit Monitoring
- Security & Technology upgrades
- Defence costs
- Fines
- Settlements

Sec/Shareholder Issues

Employee/Customer Issues

Use of Multi-factor Authentication (MFA)

- Provide different choices to the user during authentication to verify their identity.
  - However, all the factors may not be available in all operating conditions.
- Come with a fail-safe feature in case of any authentication factor gets compromised
  - users should be authenticated utilizing the other non-compromised modalities.

- **Concerns:**

- **How to choose a better set of authentication factors out of all possible choices in any given operating environment.**

- **The choice of an appropriate set of authentication factor determines the performance of the MFA**

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

How to select Modalities in MFA?

- The selection procedure should not follow (having bias towards) any pattern that can be used by the attackers.
- The process should make the consideration of previous selection of the authentication factors to avoid repetitive use of the same factors.

Modes of Auth. Factor Selection		Illustration
Static		**A predefined set of modalities for any given environment.**
Dynamic		**A set of modalities chosen dynamically at different time triggering event for authentication.**
Dynamic	***Random***	**Modalities are chosen in any random order at the time of authentication.**
✔	***Adaptive***	**Modalities are chosen based on current system settings and previously selected modalities.**

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Adaptive Multi-Factor Authentication (A-MFA)

- This greatly enhances security without changing the user experience.
- However, when an unauthorized user attempts to gain access with stolen credentials and the additional factors and behaviours normally seen don't line up, the login is prevented and challenged.
- The selection of multiple authentication factors are conducted adaptively considering

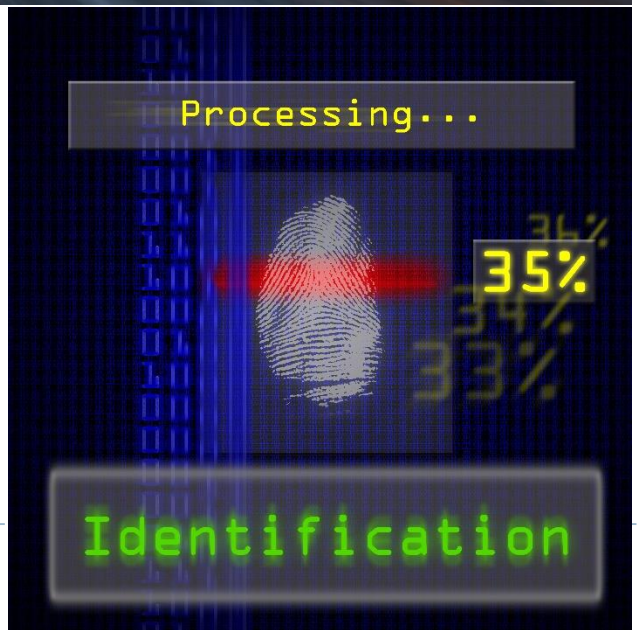
Operating devices

Connected Media

Surrounding Conditions/Environment

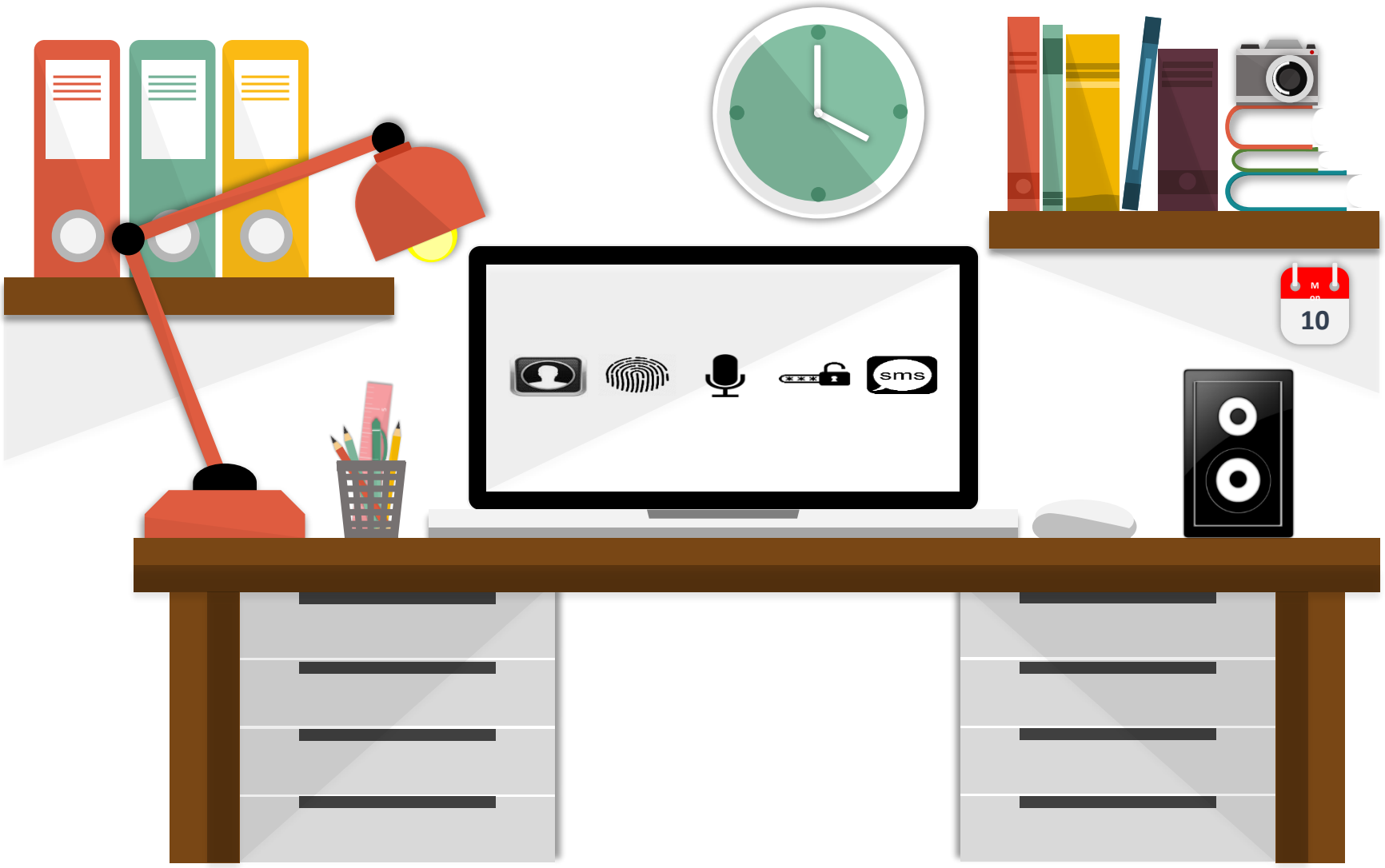
THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

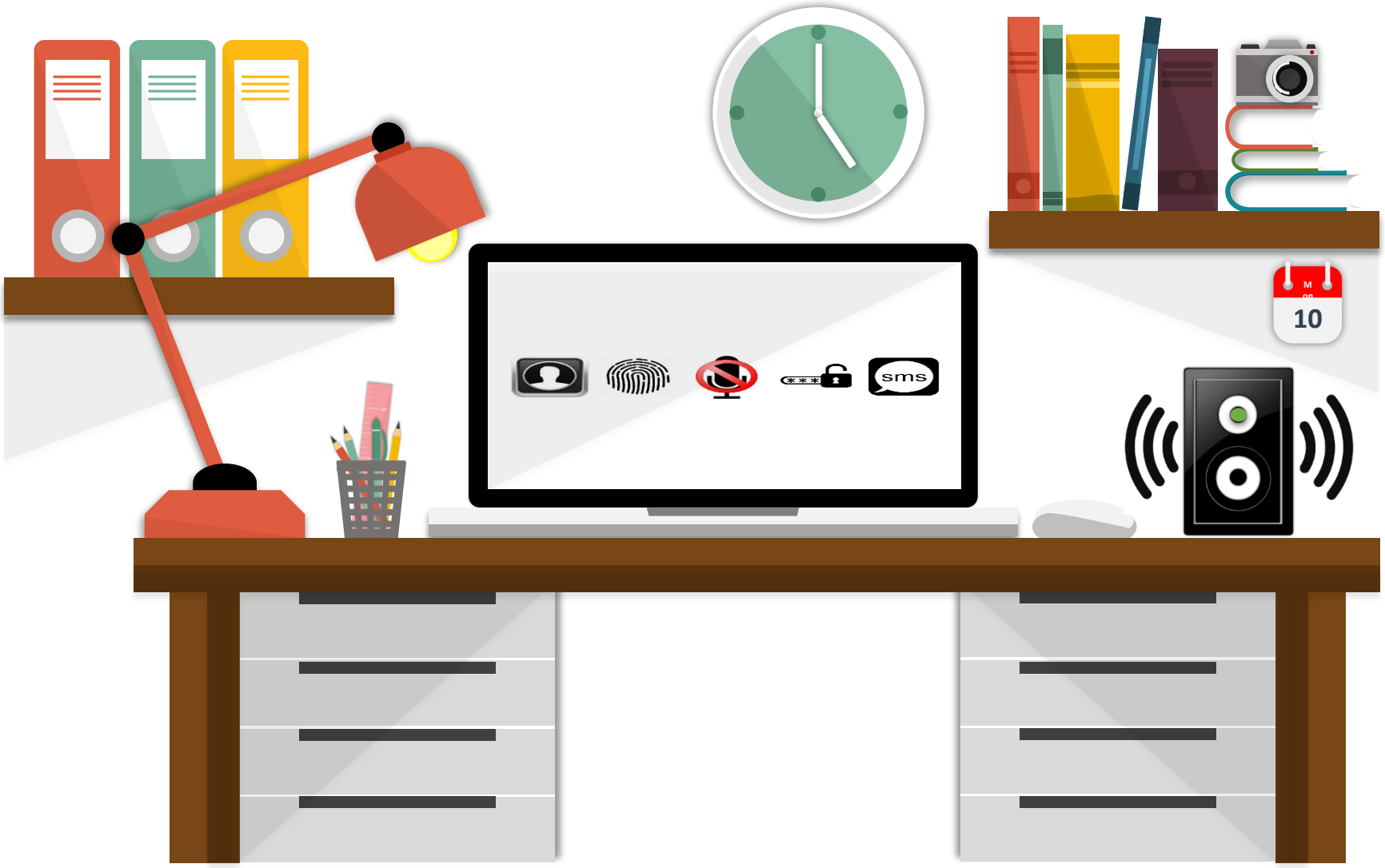
Biometric Presentation Attacks



THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Public Place with shared wifi

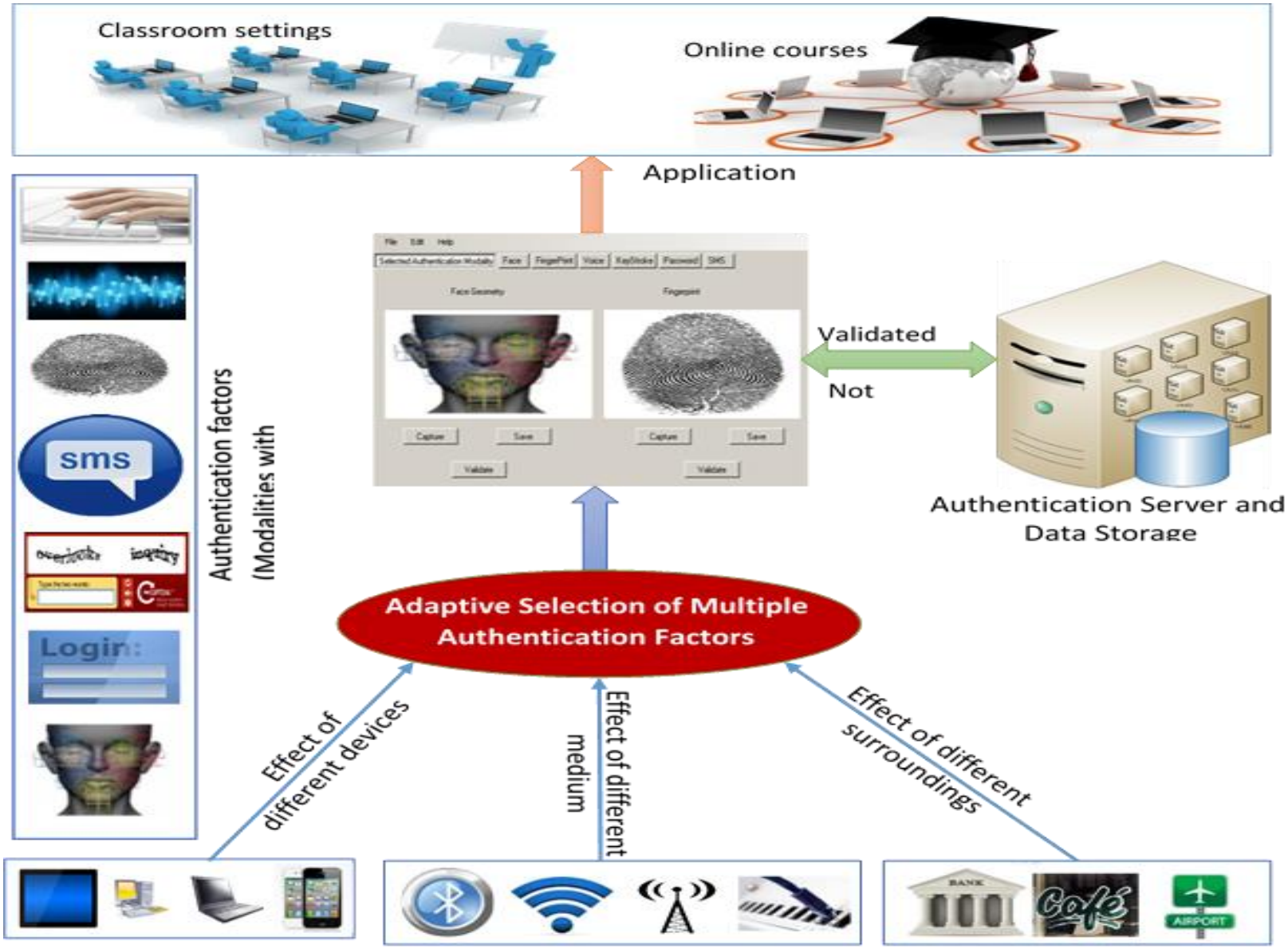

sms
10


sms
10

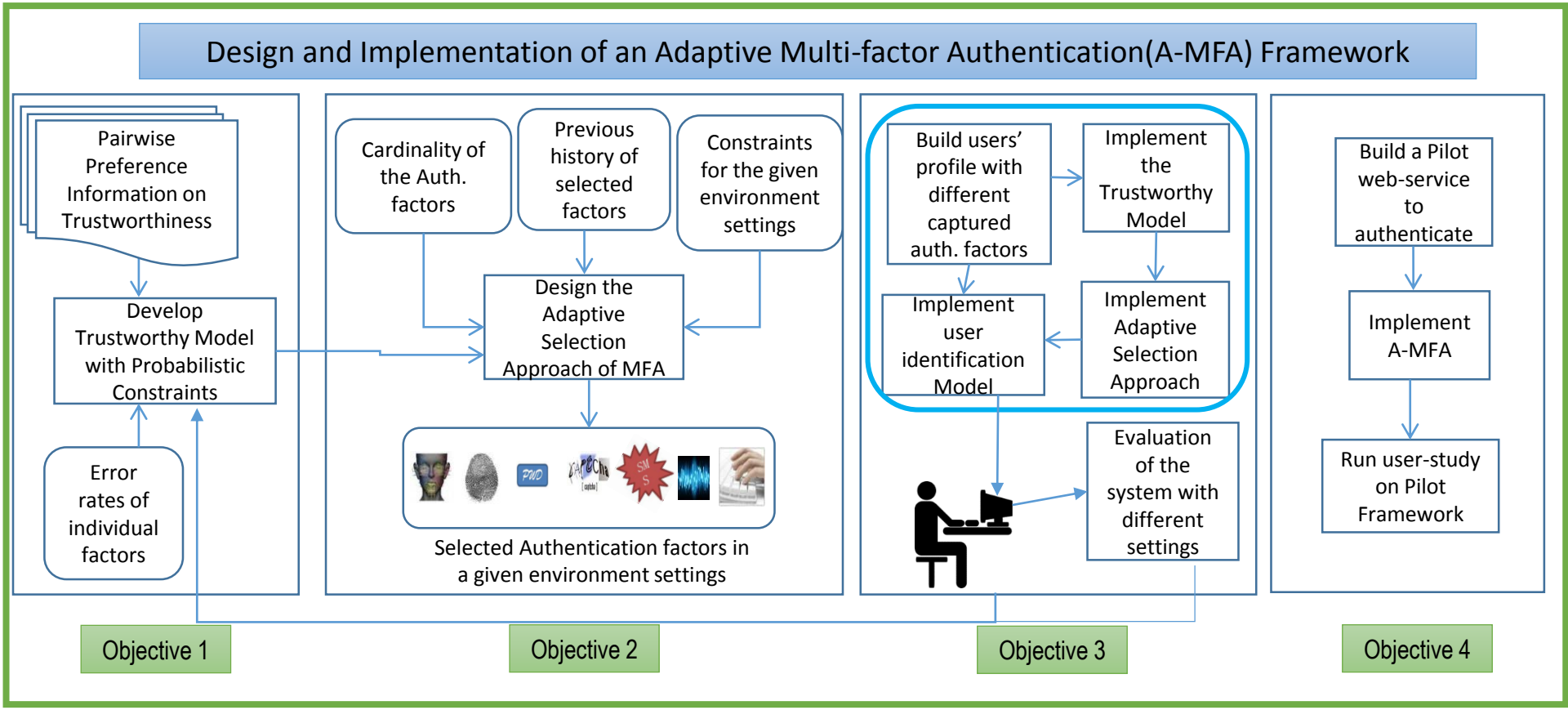

sms
10


sms
10

Overall Concept of A-MFA

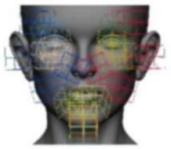


A-MFA: Overall Goal and Objectives



THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Popular A-MFA Modalities & their features



M1: **Face Recognition**

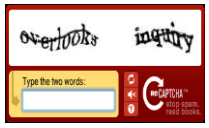
It is computed through face geometry features. Features include different points in Lips, eyes, brow and cheek, Crows-feet wrinkles nasal root wrinkles.

M2: **Finger Print**

Three level of features are used for this modality. Level 1 features show macro details of the ridge flow shape, Level 2 features (minutiae point) are discriminative enough for recognition, and Level 3 features (pores) complement the uniqueness of Level 2 features.

M3: **Password**

Password is the most common modality. It can be stored in hashed form and matched with the input by hashing the given password as string matching. Password can be made with alpha-numeric characters along with some special characters.



M4: **CAPTCHA**

It is used to prevent automated software to perform actions and can discriminate between human and bots. a CAPTCHA features an image file of slightly distorted alphanumeric characters. It also has read out feature for users with visually impaired.

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Modalities & their features

M5: SMS

SMS feature is used to send the pass-code to any phone number and that code is valid for a short period of time. The phone number should be registered to the system a-priori basis.

M6: Voice recognition

It uses pitch and different formant features (F1, F2 and F3). The pitch of the speech signal contains crucial information about the intonation pattern. The formants represent the articulators of the speech signal where the resonant frequencies are generated.

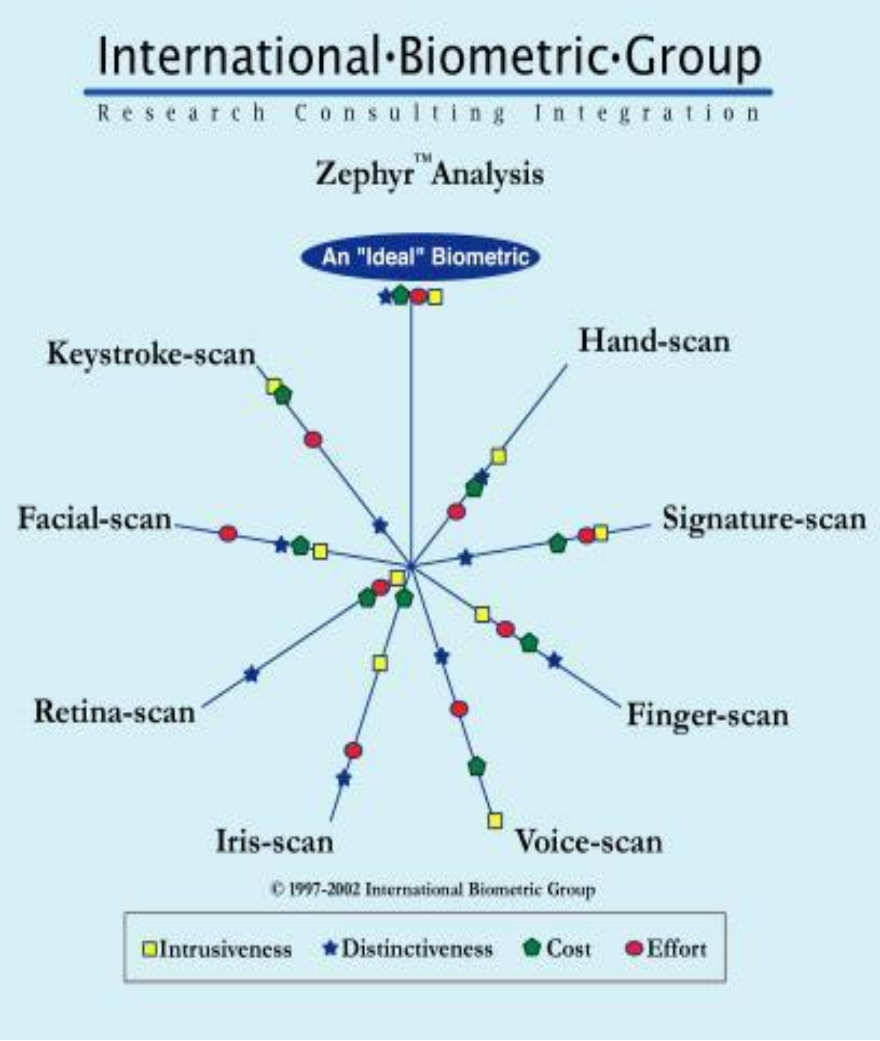
M7: Keystroke pattern

This modality detects the pattern of the keystrokes. The features used for this techniques are : mean latency and standard deviation of digraphs [A combination of two letters representing one sound], mean duration and standard deviation of keystrokes.

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Using Biometric Characteristics

- ✓In this chart the further away the characteristic is from the center, the better is the biometric technique.
- ✓So for instance keystroke scan and signature scan are low cost, require very little effort, and are not intrusive at all, however they are not distinctive.
- ✓On the other end of the spectrum, retina scan and iris scan, provide very high distinctiveness, however they are both expensive, and intrusive



THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Authentication Factors

In this work, an authentication factor is defined as

(i) Single feature of an authentication modality;

(ii) Any combination of features of an authentication modality;

(iii) Combination of multiple features of different authentication modalities.

Key Term

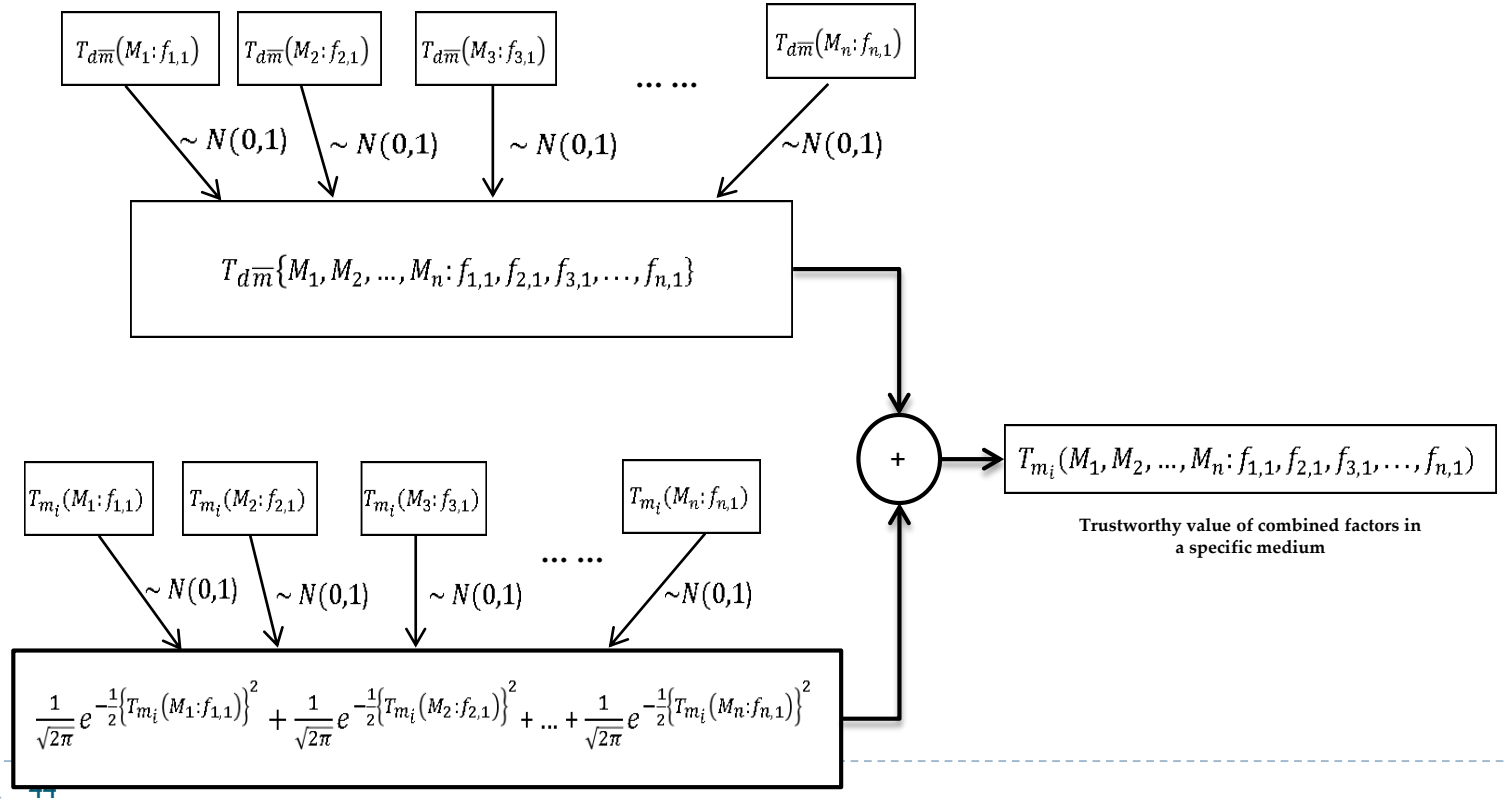
- $\mathrm{M}_k (k \in \mathbb{Z}^+)$ be the k^{th} authentication modality and $\{\mathrm{M}_k : f_{k,i}\}$ be its i^{th} feature.
- $\left\{\{\mathrm{M}_k\} : \{f_{k,i}\}_{i \in \mathbb{Z}^+}\right\}_{k \in \mathbb{Z}^+}$:
  - i^{th} features of different combinations of $\{\mathrm{M}_k\}_{k \in \mathbb{Z}^+}$.

Authentication Factors

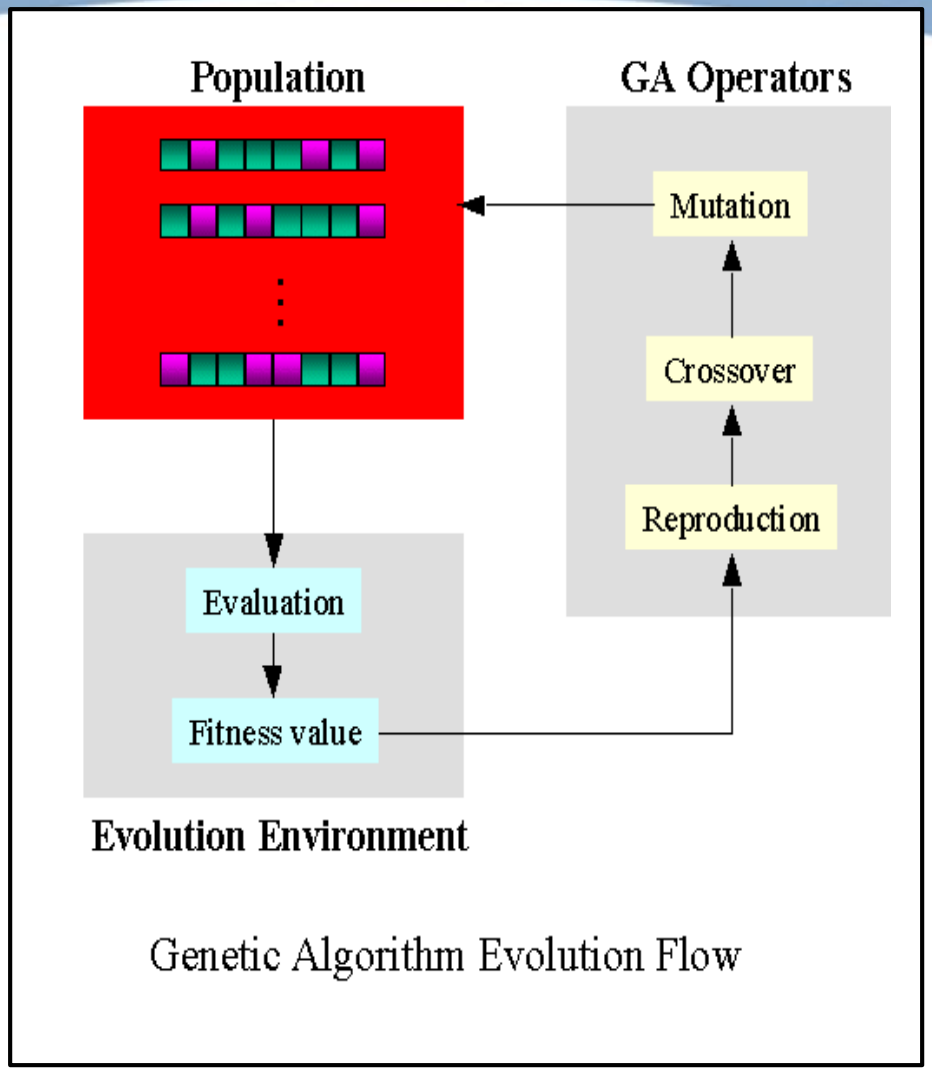
- The first features of M_1 and M_2: $\{M_1: f_{1,1}\}$ and $\{M_2: f_{2,1}\}$.
  - They are considered as two authentication factors (according to (i))
- $\{M_1: f_{1,1}, f_{1,2}\}$ is one authentication factor (according to (ii))
  - combinations of $\{M_1: f_{1,1}\}$ and $\{M_1: f_{1,2}\}$
- $\{M_1, M_2: f_{1,1}, f_{2,1}\}$ is considered as one authentication factor (according to (iii))
  - combination of $\{M_1: f_{1,1}\}$ and $\{M_2: f_{2,1}\}$.

Trustworthy Value of Combined Factors

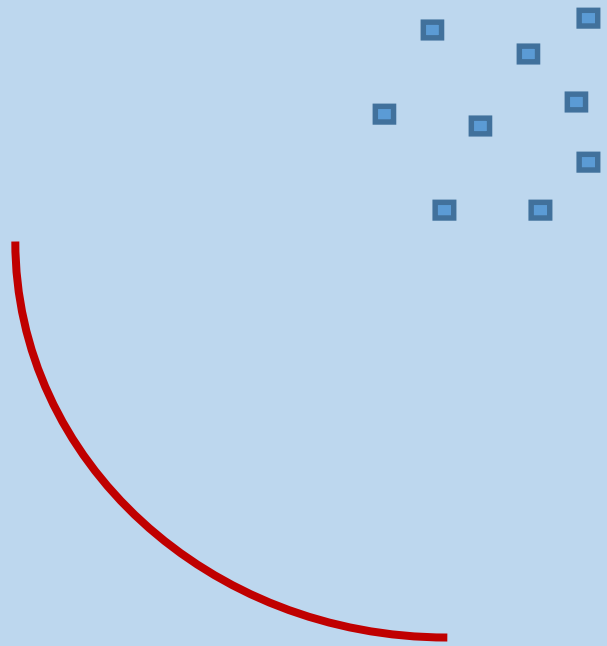
- Calculation of trustworthy values of combined factor from individual trustworthy values illustrated.



Machine Learning Algorithm



Genetic Pareto-Optimization



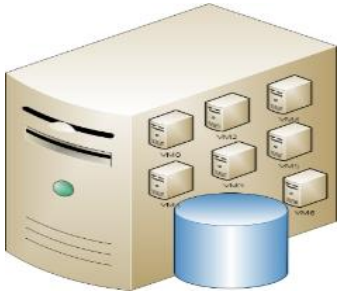
A Framework for A-MFA System

Application Environment

UI

Validated Users

Not Validated



VMs stores different authentication factors of users

Authentication factors (Modalities with features)

Adaptive Selection of multiple authentication factors

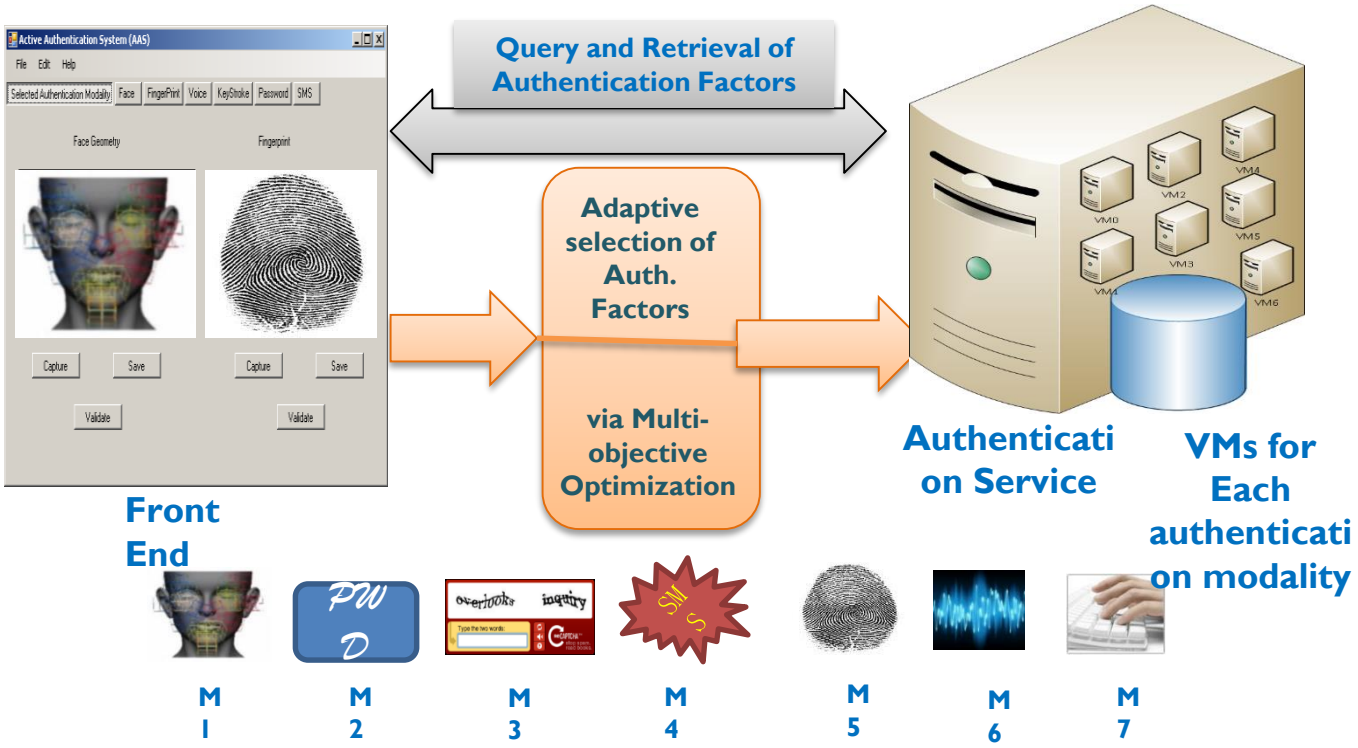
Effect of different devices

Effect of different medium

Effect of different surroundings

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Some Details of A-MFA



THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Auth Modality Activation Pattern

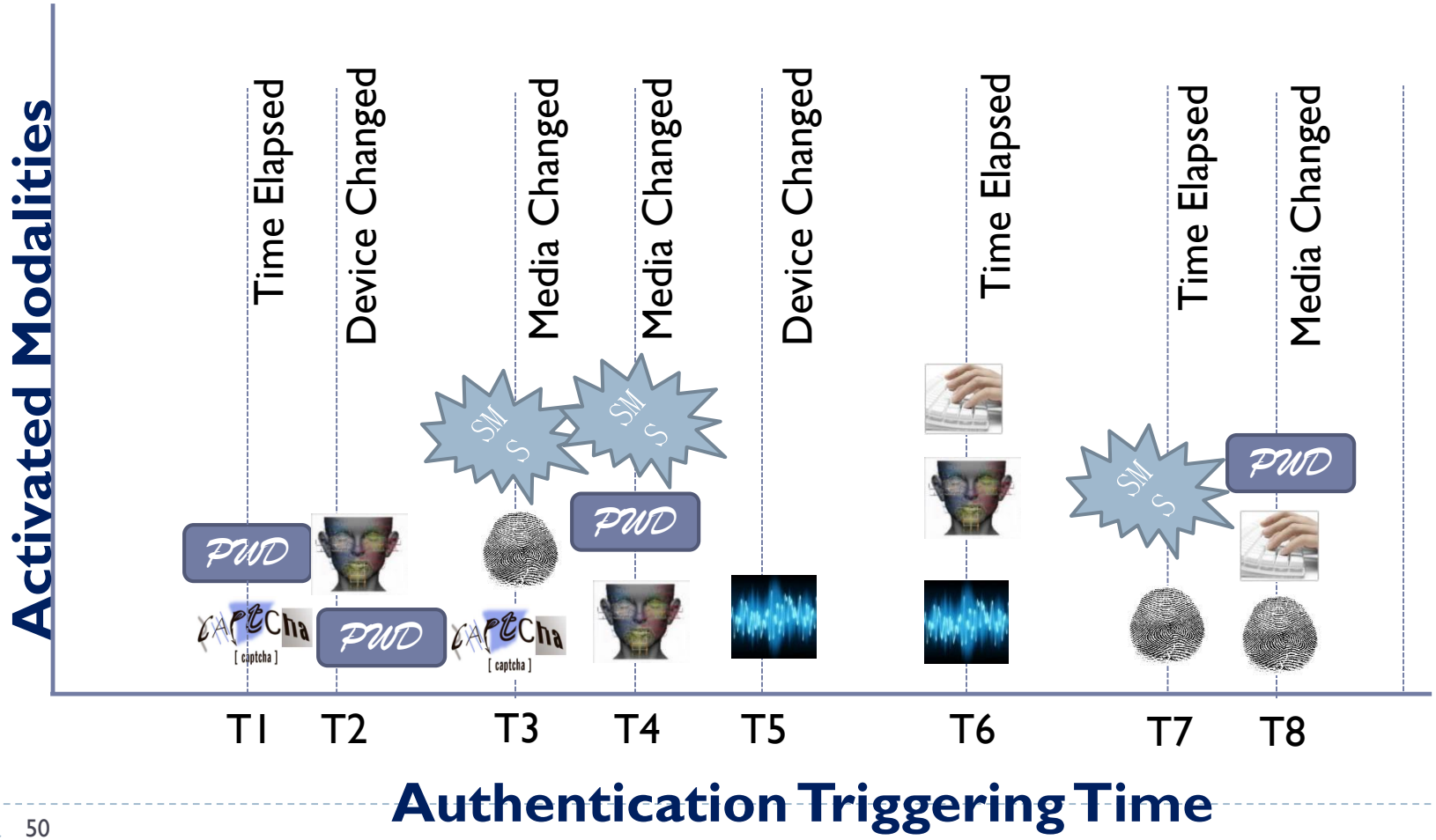
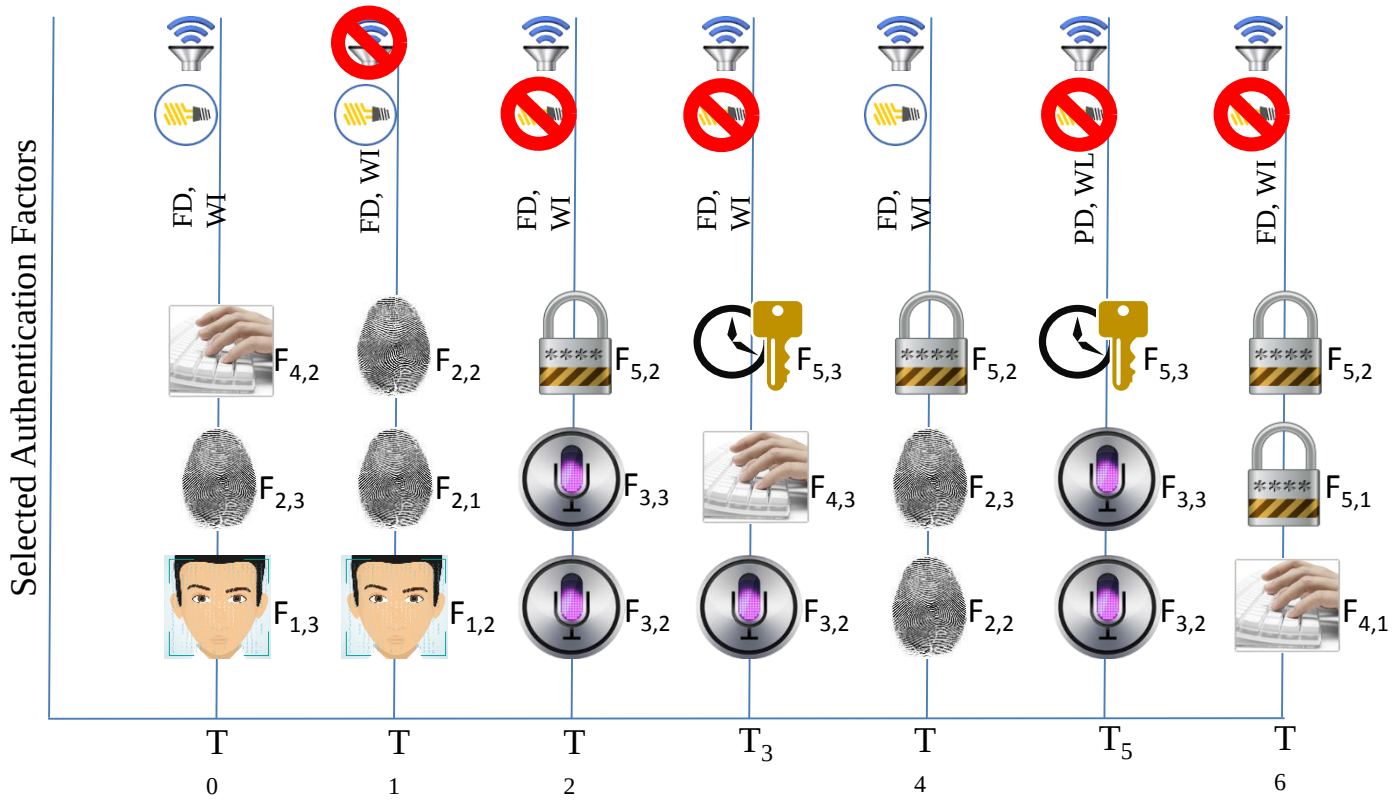


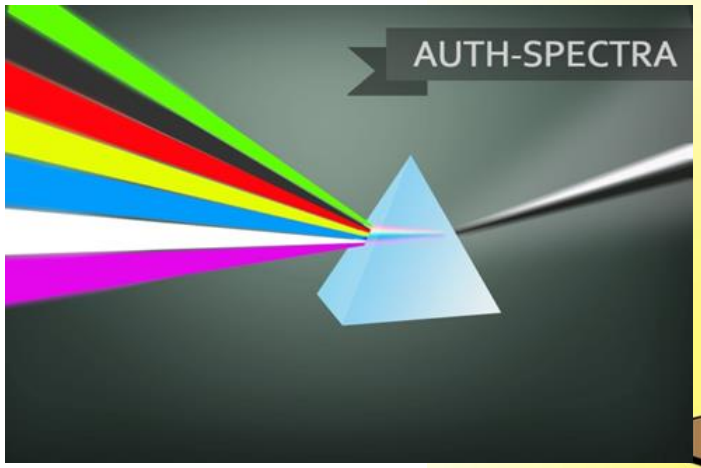
Illustration of Adaptive Selection Algorithm



Initial Experiments

- Dataset is created for 50 users as a test-bed for Adaptive-MFA System
  - **Face Dataset**:
    - 10 images for registration and 3~5 images for authentication purpose.
    - Faces94, faces95 dataset [1] are used
  - **Fingerprint Dataset**:
    - 3 images for registration and 2 images for authentication purpose.
    - CASIA Fingerprint Image Database Version 5.0 [2]
  - **Voice Dataset**:
    - 3 voice samples for registration and 1 voice sample for authentication.
  - **Keystroke Dataset**:
    - 5 keystroke samples for registration and 3 or more keystroke samples for authentication.
    - CMU dataset [3] is used.
  - Non-biometric data are generated programmatically.
  - Passwords and pass-phrases are hashed using SHA-512 in client side and B-Crypt [4] in the server side (data-at-rest).
  - The communication between client and server are done through https protocol which is basically an end-to-end encrypted communication while data-in-motion.

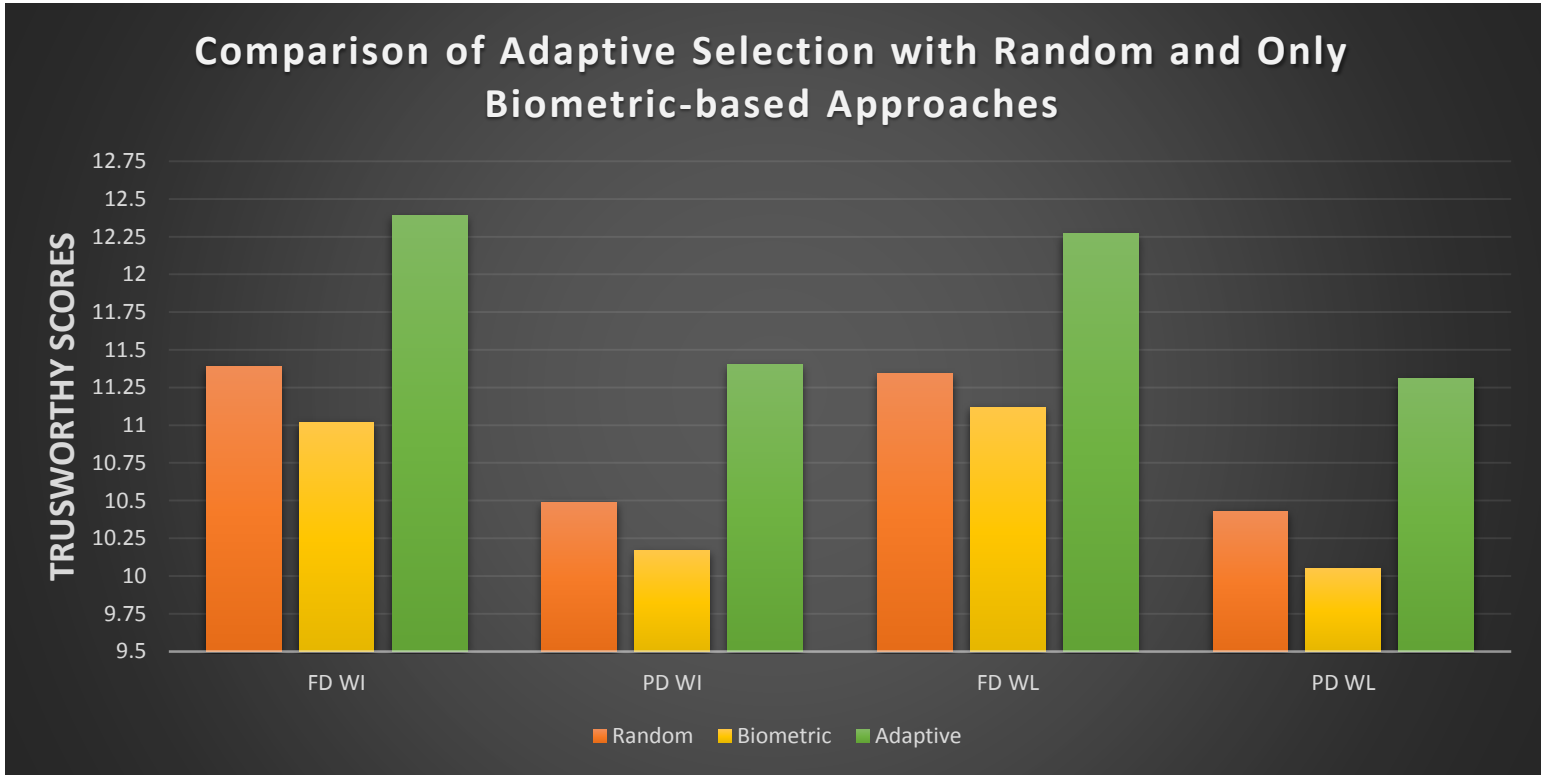
1. Faces 94. The University of Essex. Face Recognition Data Set, Libor Spacek. Url: http://cswww.essex.ac.uk/mv/allfaces/faces94.html
2. Casia-FingerprintV5, Url: http://biometrics.idealtest.org/
3. CMU dataset, Url: http://www.cs.cmu.edu/~keystroke/
4. 4. Bcrypt Generator. Date accessed: September 1, 2016. Url:https://www.bcrypt-generator.com/


AUTH-SPECTRA


XYZ BANK
ACOUNTS HOME
>PASSWORD
Multiple Factors
varified
"Access granted"

Authentication modalities incorporated in A-MFA System

Knowledge-Based Modalities	Possession-Based Modalities	Biometric Modalities	Location-Based Modalities
Password Pass-phrase Security Challenge Questions	SMS Code TOTP Code	Face Recognition Fingerprint Recognition Voice Recognition Keystroke Recognition	GPS IP address MAC Address Wi-Fi Triangulation Cellular Triangulation



- The selection procedure should not follow (having bias towards) any pattern that can be used by the attackers.
- The process should make the consideration of previous selection of the authentication factors to avoid repetitive use of the same factors.

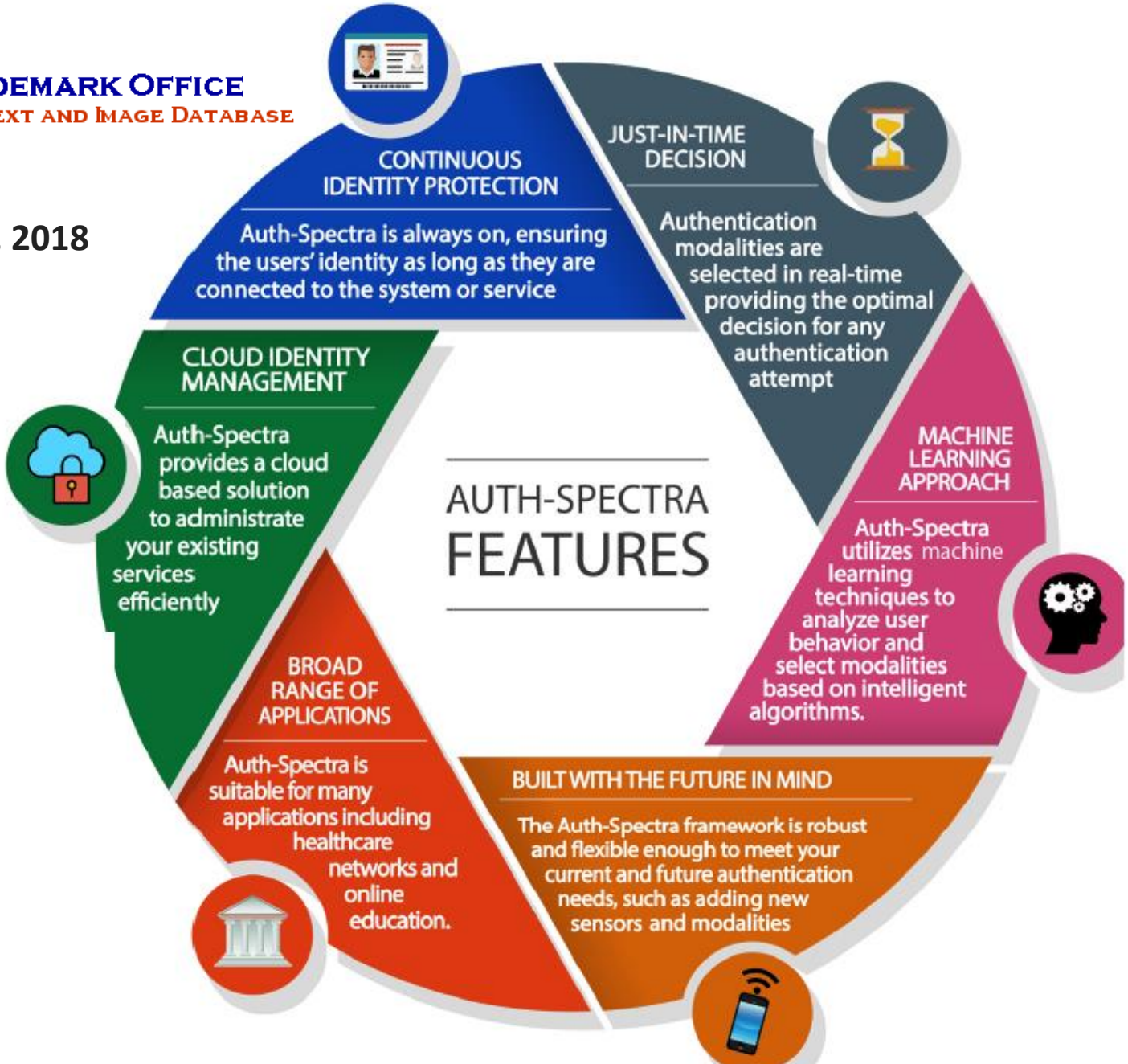
Stress Test: System accuracy given valid and imposter data and varying light and noise conditions

Surrounding Conditions	Two-factor based Authentication		Three-factor based Authentication	
	Valid Data	Imposter Data	Valid Data	Imposter Data
	92%	0%	92%	0%
	98%	0%	96%	0%
	94%	0%	92%	0%
	79%	8%	76%	0%

Auth-Spectra: Important Features

US PATENT & TRADEMARK OFFICE
PATENT APPLICATION FULL TEXT AND IMAGE DATABASE

Patent # 9,912,657
Issue Date: March 6, 2018



Video of A-MFA Prototype Demo

A company using a similar Technology:
https://www.okta.com/learn/Adaptive-MFA

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

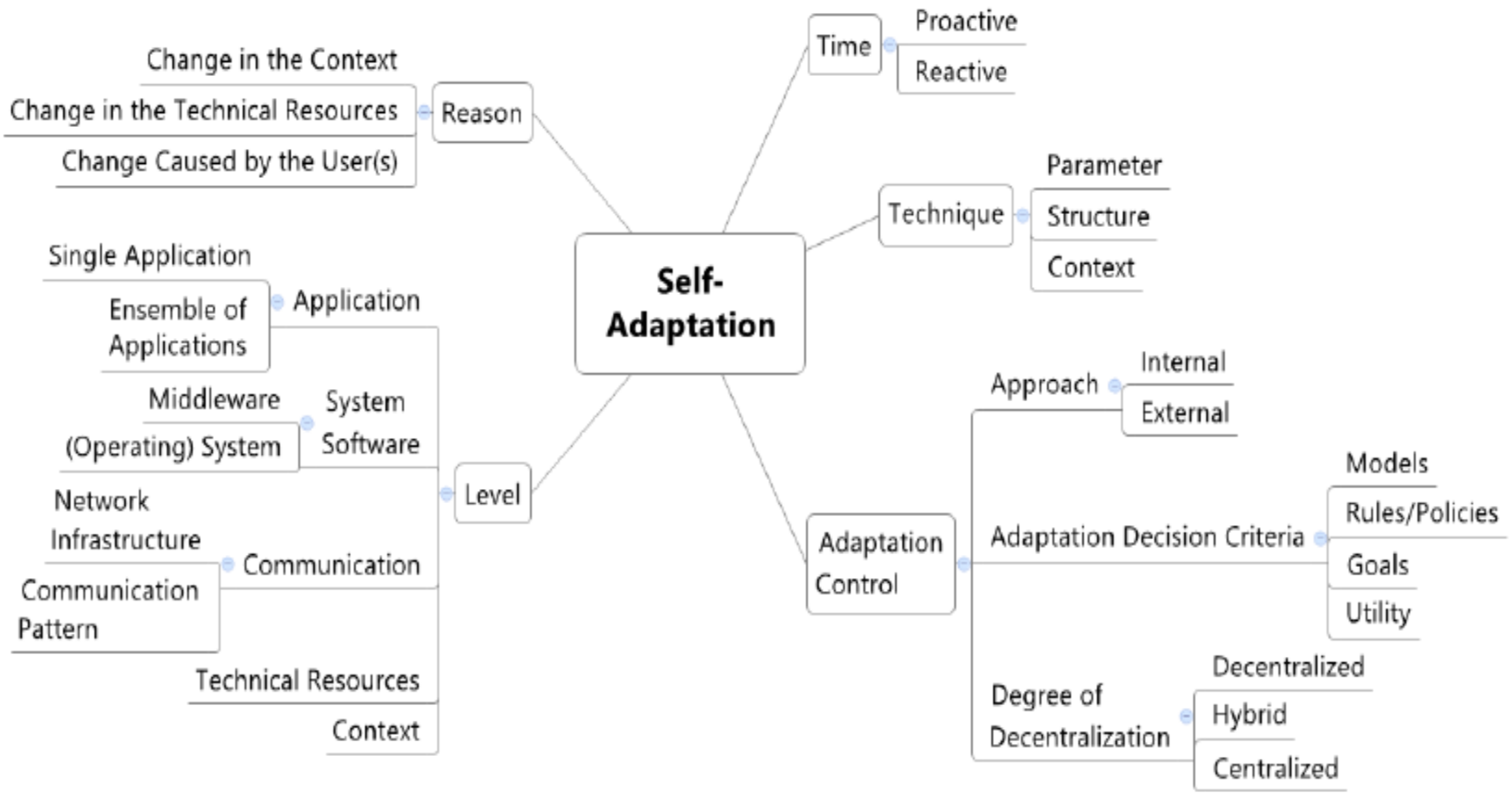
Version 2: A-MFA using additional factors

- A-MFA invisibly can integrate hundreds of auth factors.

- Including behaviours, as an extra set of "factors"
- Evaluates if there is enough of a match with a user's known profile to allow the user to access a site or service without requiring the user to enter any additional factors.

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Adaptation at Different Levels



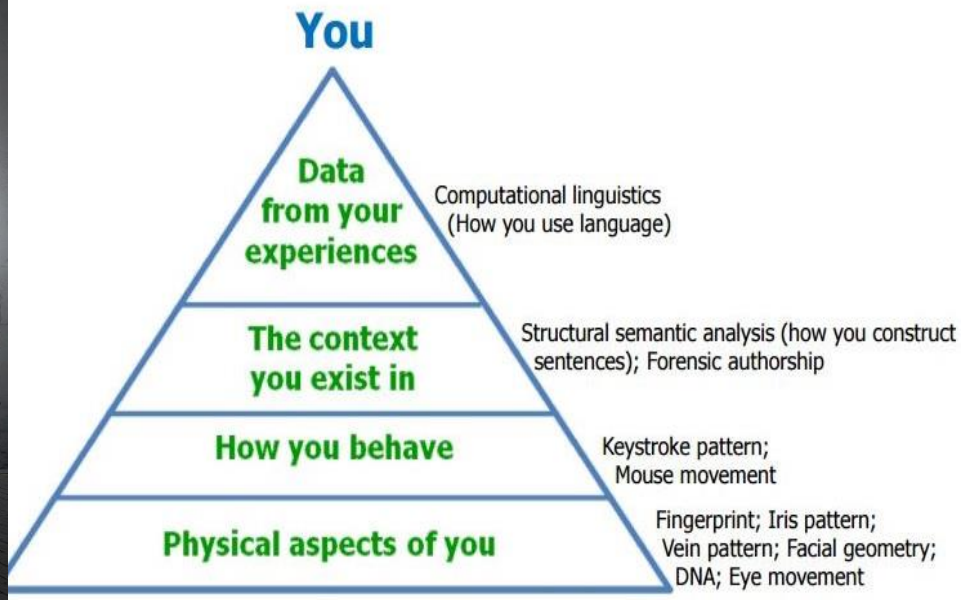
Salehie and Tahvildari (February, 2018) introduce the questions for eliciting adaptation requirements: When to adapt? Why do we have to adapt? Where do we have to implement change? What kind of change is needed? Who has to perform the adaptation? How is the adaptation performed?

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

Identity Eco-System: Continuous Authentication

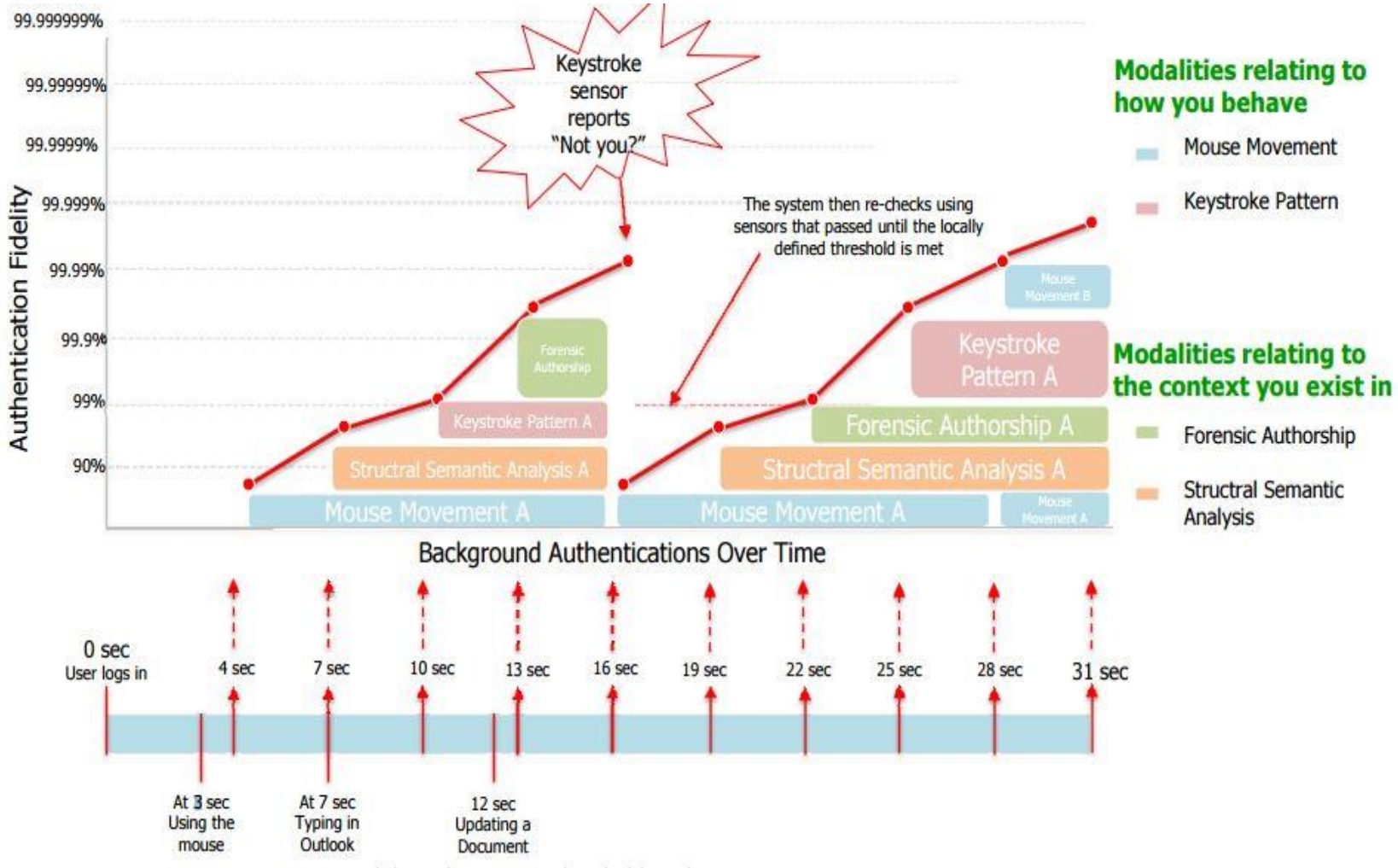
A person be authenticated on a regular interval through

- Physical aspects (example: fingerprint, face geometry, etc.)
- Interaction with the system (example: keystroke pattern, mouse movement, etc.)
- Existing context of the user (example: structural semantic analysis, forensic authorship, etc.)
- Experienced data usage (example: computational linguistics)



THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

User Identity Profiling for Continuous Authentication



Identity Ecosystem Steering Group (IDESG)

IDESG Members

- More than 350 members and 65 universities over 12 countries

- Private sector group that works under the National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative toward the goal of creating a trust framework that can replace passwords, allow individuals to prove online that they are who they claim to be, and enhance privacy [3].
- Identity Ecosystem Framework
  - A set of three core documents that describe the Identity Ecosystem and requirements, best practices, and approved standards needed to be considered in compliance with it.

[3] NSTIC. (2015). About NSTIC. http://www.nist.gov/nstic/about-nstic.html

A-MFA Applications:

- Continuous, high-confidence, identity authentication for:
- Banking, including online funds transfer
- Online testing in education and training settings
- Secure access to Electronic Medical Records
- Access to Sensitive sites by government employees and others.
- Internet of Things (IoT) sensory data access.
- Use in Blockchain Technology for access verification to Hyper ledger.
- Specific web services such as PayPal, Netflix and other paid services.

Deployable at different levels of Internet Computing:

- Application level (financial applications, email/business/personal applications, social applications)
- User level (root user, administrators, guest user)
- Document level (pdf containing application form, document containing proprietary information, image/video containing confidential and sensitive footage)

2018 IEEE Symposium on Computational Intelligence in Cyber Security (CICS 2018)

at

2018 IEEE SYMPOSIUM SERIES ON COMPUTATIONAL INTELLIGENCE (IEEE SSCI 2018)

November 18- November 21, 2018, Bengaluru, India.

URL: http://ieee-ssci2018.org/cics.html/

DEADLINES:

- ~~**Special Track/Session Proposal: April 5, 2018**~~
- **Paper Submission: July 23, 2018**

Symposium Chair: Dipankar Dasgupta, IEEE Fellow, The University of Memphis, USA

Co-Chair: Marco Carvalho, Florida Institute of Technology, USA

Co-Chair: Shamik Sural, Indian Institute of Technology, Kharagpur, India

THANK YOU!