Journal of the Nigerian Association of Mathematical Physics
Volume **18 (May, 2011), pp 395 – 400**

Enhancing Authentication Models Characteristic Metrics via Probability Modeling

[1]Onibere Emmanuel A. and [2]Egwali Annie. O.
[1, 2]Department of Computer Science
Faculty of Physical Sciences
University of Benin P.M.B 1154,
Benin City, Nigeria.

Abstract

Many choices exist for authenticating users into secure computing systems, yet users continue to lose confidence in the services of online and offline systems because of the increasing activities of identity attackers to circumvent in-built authentication models. Researchers and security experts are becoming uncertain in their opinion of what actually constitute the characteristic metrics that should be evident in invulnerable authentication models. In this work, we derive the universal characteristic metrics set for authentication models based on security, usability and design issues. We then compute the probability of the occurrence of each characteristic metrics in some single factor and multifactor authentication models in order to determine the effectiveness of these models. Our result show that single factor models do not have enough strength to counter identity attacks., for our findings revealed that textual passwords had efficiency of 30.0%, graphical passwords (63.3%), tokens (43.3%) and biometric systems (90.0%). Conversely, multifactor models proved to be more efficient and offer a more robust characteristic metric and by adding two unique characteristic metrics: reusability and randomization, we proffer an authentication solution, HUn_3^1, which is 6.7% more effective. Using Bayes' theorem, we verify that authenticating users with HUn_3^1 reduces the chances of false positivity by 0.7%.

1. Introduction:

Authentication in computer security is the process of attempting to verify the digital identity of the sender of a communication such as a request to log in. The sender or principal being authenticated may be a user operating a computer, a computer itself or a computer program. Security practitioners and researchers have made strides in protecting systems; and correspondingly user identities or credentials by postulating several techniques to counter identity attacks. Current authentication techniques can be divided into three main areas: *knowledge-based authentication techniques* i.e. something the user knows, which include textual passwords, pass phrase, mnemonic password, personal identification number (PIN) and graphical passwords; *token-based authentication techniques* i.e. something the user have, which include cards and tokens; and *biometric-based authentication techniques* i.e. something the user is, which include voice, fingerprints, gait and keystroke. The aforementioned techniques can be based on *single factor models* i.e. passwords, *two-factor models* i.e. passwords and tokens or *multifactor models* i.e. textual passwords, graphical passwords and tokens.

Several securities, usability and design challenges emanate from the deployment of authentication models (AM) and hence a number of characteristics metrics have been used to evaluate the capabilities of AM. In analyzing design and implementation issues, credentials reusability and decoupling was submitted by [1]. Ian et al [2] asserted that usability and the memorability ability which affect the efficiency of inputs are two key human factors criteria from which graphical passwords can be analysed, that is, how the user chooses and encodes the password and what task the user does when retrieving the password. Suo et al [3] proposed five measuring metrics, security, usability, reliability, storage and communication. Monrose et al [4] postulated security, key generation and usability. Brostoff and Sasse [5] affirm to the fact that apart from security, graphical password development has partly been geared towards memorability. This idea was also supported by [6,7]. Norman [8] posited that user satisfaction should also be a measuring metrics. Jain et al [9] proposed nine metrics, which are performance, acceptability, circumvention resistance, cost-effectiveness, universality, uniqueness, permanence, collectability and distinctiveness. Scheuermann et al [10] and Biometric Technology [11] affirmed unanimously that a practical biometric system should meet the specified recognition accuracy and speed, and should be harmless to the users and be sufficiently robust to various fraudulent methods and attacks to the system.

To evaluate an AM performance probability with a high level of accuracy, we ascertain what actually constitute the universal characteristic metrics that should act as a benchmark for determining the effectiveness of AM against identity attackers. The fact is that an AM with a robust characteristic metric database will offer a better and an all-end solution to identity attacks [12]. The benefit is that the efficiency rate of AM can be determined before deployment and the ratio of accuracy rates to false positives can be analyzed before adoption.

[2]Corresponding authors: Egwali Annie. O A: E-mail: egwali@yahoo.com; Tel. 07033247730

2.0 Authentication Models Characteristics Metrics

Most authentication models designed to counter identity attacks fails because these models depend on a subset of the entire characteristics metrics affecting AM deployment. For example, textual passwords *T* under knowledge-based authentication techniques is tilted more towards design issues for it positively addresses the following characteristics metrics: efficiency (E_{CY}^{T}), simple training (T_S^{T}), easy to create (E_C^{T}), collectability (C^{T}), performance (P_F^{T}), acceptability (A_{CC}^{T}), cost effectiveness (C_E^{T}), portability (P_Y^{T}) and scalability (S^{T}).

Mathematically, *T* can be defined as the function of nine characteristics metrics, which can be represented as:

$$T = f(E_{CY}^{T}, T_S^{T}, E_C^{T}, C^{T}, P_F^{T}, A_{CC}^{T}, C_E^{T}, P_Y^{T}, S^{T}) \quad (1)$$

From initial analysis on graphical password [13, 14, 15, 16**]**, it is evident that graphical passwords strength depends on its usability characteristics, which also include good memorability features. Graphical passwords *G* addresses: Brute Force Attack Resistance (R_{BF}), Dictionary Attack Resistance (R_{DA}), Nice Interface (N_I), Easy to Memoralize (E_M), Meaningful (M), Training Simple (T_S), Easy to Use (E_U), Easy to Create (E_C), Easy to Learn (E_L), Conveyable Image (C_I), Effectiveness (E_{FF}), Replay Resistance (R_R), Efficiency (E_{CY}), Collectability (C), Performance (P_F), Acceptability(A_{CC}), Cost Effectiveness (C_E), Portability (P_Y) and Scalability (S). These nineteen characteristic metrics are mathematically represented as:

$$G = f(R_{BF}, R_{DA}, N_I, E_M, M, T_S, E_U, E_C, E_L, C_I, E_{FF}, R_R, E_{CY}, C, P_F, A_{CC}, C_E, P_Y, S) \quad (2)$$

Token-based authentication techniques have the capabilities to tackle efficiently the following thirteen characteristics: Acceptability (A_{CC}^{TS}), Cost Effectiveness (C_E^{TS}), Performance (P_F^{TS}), Meaningful (M^{TS}), Training Simple (T_S^{TS}), Easy to Use (E_U^{TS}), Easy to Create (E_C^{TS}), Collectability (C^{TS}), Easy to Learn (E_L^{TS}), Challenge Response (C_R^{TS}), Effectiveness (E_{FF}^{TS}), Efficiency (E_{CY}^{TS}) and Scalability (S^{TS}) [17, 18]). Token-based systems *TS* can be defined as (3):

$$TS = f(A_{CC}^{TS}, C_E^{TS}, P_F^{TS}, M^{TS}, T_S^{TS}, E_U^{TS}, E_C^{TS}, C^{TS}, E_L^{TS}, C_R^{TS}, E_{FF}^{TS}, E_{CY}^{TS}, S^{TS})$$

The strength of Biometric-based Systems depends on their ability to address effectively security, usability and design issues [19, 20]. This makes biometric models *B* a function of the following twenty-seven characteristics metrics: Brute Force Attack Resistance (R_{BF}), Dictionary Attack Resistance (R_{DA}), Shoulder Surfing Resistance (R_{SS}), Spyware Resistance (R_S), Guessibility Resistance (G), Social Engineering Resistance (R_{SE}), Nice Interface (N_I), Easy to Memoralize (E_M), Meaningful (M), Training Simple (T_S), Easy to Use (E_U), Easy to Create (E_C), Easy to Learn (E_L), Challenge Response (C_R), Conveyable Image (C_I), Effectiveness (E_{FF}), Efficiency (E_{CY}), Universality (U), Uniqueness (U_Q), Permanence (P), Collectability (C), Performance (P_F), Acceptability(A_{CC}), Cost Effectiveness (C_E), Distinctiveness (D), Portability (P_Y) and Scalability (S). Therefore biometric systems are a function of the following:

$$B = f(R_{BF}^{B}, R_{DA}^{B}, R_{SS}^{B}, R_S^{B}, G^{B}, R_{SE}^{B}, N_I^{B}, E_M^{B}, M^{B}, T_S^{B}, E_U^{B}, E_C^{B}, E_L^{B}, C_R^{B}, C_I^{B}, E_{FF}^{B}, E_{CY}^{B}, U^{B}, U_Q^{B}, P^{B}, C^{B}, P_F^{B}, A_{CC}^{B}, C_E^{B}, D^{B}, P_Y^{B}, S^{B}) \quad (4)$$

To establish the best choice of authentication factors to employ that will prolifically and inclusively counter identity attackers' techniques; we assemble the inclusive characteristics metrics C_{set} of *T*, *G*, *TS*, and *B* via union derivative based on the security, usability and design analysis. This yields the following collective sixty-eight characteristic metrics:

$$C_{set} = T \cup G \cup TS \cup B = f(E_{CY}^{T}, T_S^{T}, E_C^{T}, C^{T}, P_F^{T}, A_{CC}^{T}, C_E^{T}, P_Y^{T}, S^{T}, R_{BF}, R_{DA}, N_I, E_M, M, T_S, E_U, E_C, E_L, C_I, E_{FF}, R_R, E_{CY}, C, P_F, A_{CC}, C_E, P_Y, S, A_{CC}^{TS}, C_E^{TS}, P_F^{TS}, M^{TS}, T_S^{TS}, E_U^{TS}, E_C^{TS}, C^{TS}, E_L^{TS}, C_R^{TS}, E_{FF}^{TS}, E_{CY}^{TS}, S^{TS}, R_{BF}^{B}, R_{DA}^{B}, R_{SS}^{B}, R_S^{B}, G^{B}, R_{SE}^{B}, N_I^{B}, E_M^{B}, M^{B}, T_S^{B}, E_U^{B}, E_C^{B}, E_L^{B}, C_R^{B}, C_I^{B}, E_{FF}^{B}, E_{CY}^{B}, U^{B}, U_Q^{B}, P^{B}, C^{B}, P_F^{B}, A_{CC}^{B}, C_E^{B}, D^{B}, P_Y^{B}, S^{B}) \quad (5)$$

3.0 Concept of Exclusivity

The concept of exclusivity represented as *Ex* in this context denotes that characteristic metrics are not redefined in every cases of occurrence. For example by applying the concept of exclusivity in which characteristics metrics are not repeated to equation 5, we derive the following twenty-eight characteristics set of equation 6, defined as:

$$Exclusivity\ of\ C_{set} = Ex(C_{set}) = f(R_{SS}^{B}, R_S^{B}, R_{SE}^{B}, U^{B}, U_Q^{B}, P^{B}\ D^{B}, G^{B}, R_R, E_U, E_L, M, N_I, E_{CY}, E_C, T_S, C_I, A_{CC}, E_{FF}, C, P_F, R_{BF}, C_E, S, P_Y, E_M, R_{DA}, C_R^{B}) \quad (6)$$

Where exclusivity *Ex* is with the inference that in all cases of the four models: *T*, *G*, *TS*, and *B*, $E_U \equiv E_U^{B} \equiv E_U^{TS}$, $E_L \equiv E_L^{B} \equiv E_L^{TS}$, $M \equiv M^{B} \equiv M^{TS}$, $N_I \equiv N_I^{B}$, $E_{CY} \equiv E_{CY}^{T} \equiv E_{CY}^{B} \equiv E_{CY}^{TS}$, $E_C \equiv E_C^{T} \equiv E_C^{B} \equiv E_C^{TS}$, $T_S \equiv T_S^{T} \equiv T_S^{B} \equiv T_S^{TS}$, $C_I \equiv C_I^{B}$, $A_{CC} \equiv A_{CC}^{T} \equiv A_{CC}^{B} \equiv A_{CC}^{TS}$, $E_{FF} \equiv E_{FF}^{B} \equiv E_{FF}^{TS}$, $C \equiv C^{B} \equiv C^{T} \equiv C^{TS}$, $P_F \equiv P_F^{T} \equiv P_F^{B} \equiv P_F^{TS}$, $R_{BF} \equiv R_{BF}^{B}$, $C_E \equiv C_E^{B} \equiv C_E^{T} \equiv C_E^{TS}$, $S \equiv S^{T} \equiv S^{B} \equiv S^{TS}$, $P_Y \equiv P_Y^{T} \equiv P_Y^{B}$, $E_M \equiv E_M^{B}$, $R_{DA} \equiv R_{DA}^{B}$ and $C_R^{B} \equiv C_R^{TS}$

Despite the comprehensive nature of $Ex(C_{set})$, it is deficient of two unique characteristics metrics that should also add as a measure for an effective authentication model, these are reusability (R_{USE}) and randomization (R_M). We therefore introduce a more inclusive nature of ExC_{set} by introducing IN_{set}, which includes R_{USE} and R_M, defined thus:

$$IN_{set} = f(R_{SS}^{B}, R_S^{B}, R_{SE}^{B}, U^{B}, U_Q^{B}, P^{B}\, D^{B}, G^{B}, R_R, E_U, E_L, M, N_I, E_{CY}, E_C, T_S, C_I, A_{CC}, E_{FF}, C, P_F, R_{BF}, C_E, S, P_Y, E_M, R_{DA}, C_R^{B}, R_{USE}, R_M) \quad (7)$$

Using probability semantics, we next determine the level of efficiency of the individual authentication models under consideration.

Probability of *T* is defined as:

$$P(T) = \frac{\text{number of metrics set in T}}{\text{Total metrics set in IN}_{set}} = \frac{9}{30} = 0.3, \text{ with efficiency result of 30.0\%} \quad (8)$$

Similarly,

$$P(G) = 0.633, \text{ with efficiency result 63.3\%} \quad (9)$$

$$P(TS) = 4.33, \text{ with efficiency result 43.3\%} \quad (10)$$

$$P(B) = 0.9, \text{ with efficiency result 90.0\%} \quad (11)$$

The exclusive characteristic metric E_X of *T*, *G*, *TS*, and *B* via intersection derivative is expressed as:

$$E_X = T \cap G \cap TS \cap B = f(E_{CY}, T_S, E_C, C, P_F, A_{CC}, C_E, P_Y, S) \quad (12)$$

Where $E_{CY} \equiv E_{CY}^{T} \equiv E_{CY}^{G} \equiv E_{CY}^{B}$, $T_S \equiv T_S^{T} \equiv T_S^{G} \equiv T_S^{B}$, $E_C \equiv E_C^{T} \equiv E_C^{G} \equiv E_C^{B}$, $C \equiv C^{T} \equiv C^{G} \equiv C^{B}$, $P_F \equiv P_F^{T} \equiv P_F^{G} \equiv P_F^{B}$, $A_{CC} \equiv A_{CC}^{T} \equiv A_{CC}^{G} \equiv A_{CC}^{B}$, $C_E \equiv C_E^{T} \equiv C_E^{G} \equiv C_E^{B}$ and $S \equiv S^{T} \equiv S^{G} \equiv S^{B}$.

Equation 12 contains the principal characteristic metrics that should be evident in any authentication model. The drive then is to design more robust models that build on these principal characteristics. To increase efficiency level further, we must employ multifactor authentication models, which will increase the verify mode, performance, circumvention resistance and the reliability of decisions made by the systems [21]. We thus derive the effectiveness of the following classes of unions and their corresponding unions based on the exclusivity inference (see equations 13 – 32).

$$Un_1 = (T \cup G) = f(E_{CY}^{T}, T_S^{T}, E_C^{T}, C^{T}, P_F^{T}, A_{CC}^{T}, C_E^{T}, P_Y^{T}, S^{T}, R_{BF}^{G}, R_{DA}^{G}, R_R^{G}, N_I^{G}, E_M^{G}, M^{G}, T_S^{G}, E_U^{G}, E_C^{G}, E_L^{G}, C_I^{G}, E_{FF}^{G}, E_{CY}^{G}, C^{G}, P_F^{G}, A_{CC}^{G}, C_E^{G}, P_Y^{G}, S^{G}) \quad (13)$$

$$Ex(Un_1) = f(E_{CY}, T_S, E_C, C, P_F, A_{CC}, C_E, P_Y, S, R_{BF}, R_{DA}, R_R, N_I, E_M, M, E_U, E_L, C_I, E_{FF}) \quad (14)$$

Probability of $Ex(Un_1)$ is defined as: $P(ExUn_1)$=0.633, with efficiency result of 63.3%

Similarly, for $Un_2 = (T \cup TS) = f(E_{CY}^{T}, T_S^{T}, E_C^{T}, C^{T}, P_F^{T}, A_{CC}^{T}, C_E^{T}, P_Y^{T}, S^{T}, A_{CC}^{TS}, C_E^{TS}, P_F^{TS}, M^{TS}, T_S^{TS}, E_U^{TS}, E_C^{TS}, C^{TS}, E_L^{TS}, C_R^{TS}, E_{FF}^{TS}, E_{CY}^{TS}, S^{TS})$ (15)

$$Ex(Un_2) = f(E_{CY}, T_S, E_C, C, P_F, A_{CC}, C_E, P_Y, S, M, E_U, E_L, C_R, E_{FF}) \quad (16)$$

$P(ExUn_2) = 0.467$, with efficiency result of 46.7%

$$Un_3 = (T \cup B) = f(E_{CY}^{T}, T_S^{T}, E_C^{T}, C^{T}, P_F^{T}, A_{CC}^{T}, C_E^{T}, P_Y^{T}, S^{T}, R_{BF}^{B}, R_{DA}^{B}, R_{SS}^{B}, R_S^{B}, G^{B}, R_{SE}^{B}, N_I^{B}, E_M^{B}, M^{B}, T_S^{B}, E_U^{B}, E_C^{B}, E_L^{B}, C_R^{B}, C_I^{B}, E_{FF}^{B}, E_{CY}^{B}, U^{B}, U_Q^{B}, P^{B}, C^{B}, P_F^{B}, A_{CC}^{B}, C_E^{B}, D^{B}, P_Y^{B}, S^{B}) \quad (17)$$

$$ExUn_3 = f(E_{CY}, T_S, E_C, C, P_F, A_{CC}, C_E, P_Y, S, R_{BF}, R_{DA}, R_{SS}^{B}, R_S^{B}, G^{B}, R_{SE}^{B}, N_I, E_M, M, E_U, E_L, C_R, C_I, E_{FF}, U^{B}, U_Q^{B}, P^{B}, D^{B}) \quad (18)$$

$P(ExUn_3) = 0.9$, with efficiency result of 90.0%

$$Un_4 = (G \cup TS) = f(R_{BF}, R_{DA}, R_R, N_I, E_M, M, T_S, E_U, E_C, E_L, C_I, E_{FF}, E_{CY}, C, P_F, A_{CC}, C_E, P_Y, S, A_{CC}^{TS}, C_E^{TS}, P_F^{TS}, M^{TS}, T_S^{TS}, E_U^{TS}, E_C^{TS}, C^{TS}, E_L^{TS}, C_R^{TS}, E_{FF}^{TS}, E_{CY}^{TS}, S^{TS}) \quad (19)$$

$$ExUn_4 = f(R_{BF}, R_{DA}, R_R, N_I, E_M, M, T_S, E_U, E_C, E_L, C_I, E_{FF}, E_{CY}, C, P_F, A_{CC}, C_E, P_Y, S, C_R^{TS}) \quad (20)$$

$P(ExUn_4) = 0.667$, with efficiency result of 66.7%

$$Un_5 = (G \cup B) = f(R_{BF}, R_{DA}, R_R, N_I, E_M, M, T_S, E_U, E_C, E_L, C_I, E_{FF}, E_{CY}, C, P_F, A_{CC}, C_E, P_Y, S, R_{BF}^{B}, R_{DA}^{B}, R_{SS}^{B}, R_S^{B}, G^{B}, R_{SE}^{B}, N_I^{B}, E_M^{B}, M^{B}, T_S^{B}, E_U^{B}, E_C^{B}, E_L^{B}, C_R^{B}, C_I^{B}, E_{FF}^{B}, E_{CY}^{B}, U^{B}, U_Q^{B}, P^{B}, C^{B}, P_F^{B}, A_{CC}^{B}, C_E^{B}, D^{B}, P_Y^{B}, S^{B}) \quad (21)$$

$$ExUn_5 = (G \cup B) = f(R_{BF}, R_{DA}, R_R, N_I, E_M, M, T_S, E_U, E_C, E_L, C_I, E_{FF}, E_{CY}, C, P_F, A_{CC}, C_E, P_Y, S, R_{SS}^{B}, R_S^{B}, G^{B}, R_{SE}^{B}, C_R^{B}, U^{B}, U_Q^{B}, P^{B}, D^{B}) \quad (22)$$

$P(ExUn_5) = 0.933$, with efficiency result of 93.3%

Un_6 = (TS U B) = $f(A_{CC}^{TS}, C_E^{TS}, P_F^{TS}, M^{TS}, T_S^{TS}, E_U^{TS}, E_C^{TS}, C^{TS}, E_L^{TS}, C_R^{TS}, E_{FF}^{TS}, E_{CY}^{TS}, S^{TS}, R_{BF}^{B}, R_{DA}^{B}, R_{SS}^{B}, R_S^{B}, G^B, R_{SE}^{B}, N_I^B, E_M^B, M^B, T_S^B, E_U^B, E_C^B, E_L^B, C_R^B, C_I^B, E_{FF}^B, E_{CY}^B, U^B, U_Q^B, P^B, C^B, P_F^B, A_{CC}^B, C_E^B, D^B, P_Y^B, S^B)$ (23)

$ExUn_6 = f(A_{CC}, C_E, P_F, M, T_S, E_U, E_C, C, E_L, C_R, E_{FF}, E_{CY}, S, R_{BF}, R_{DA}, R_{SS}^B, R_S^B, G^B, R_{SE}^B, N_I^B, E_M^B, C_I, U^B, U_Q^B, P^B, D^B, P_Y)$ (24)

P($ExUn_6$) = 0.9, with efficiency result of 90.0%

Un_7 = (T U TS U G) = $f(E_{CY}^T, T_S^T, E_C^T, C^T, P_F^T, A_{CC}^T, C_E^T, P_Y^T, S^T, A_{CC}^{TS}, C_E^{TS}, P_F^{TS}, M^{TS}, T_S^{TS}, E_U^{TS}, E_C^{TS}, C^{TS}, E_L^{TS}, C_R^{TS}, E_{FF}^{TS}, E_{CY}^{TS}, S^{TS}, R_{BF}, R_{DA}, R_R, N_I, E_M, M, T_S, E_U, E_C, E_L, C_I, E_{FF}, E_{CY}, C, P_F, A_{CC}, C_E, P_Y, S)$ (25)

$ExUn_7 = f(A_{CC}, E_{CY}, C_E, P_Y, C, C_R^T, E_{FF}, R_{BF}, R_{DA}, R_R, N_I, E_M, M, T_S, E_U, E_C, E_L, C_I, P_F, S)$ (26)

P($ExUn_7$) = 0.667, with efficiency result of 66.7%

Un_8 = (T U TS U B) = $f(E_{CY}^T, T_S^T, E_C^T, C^T, P_F^T, A_{CC}^T, C_E^T, P_Y^T, S^T, A_{CC}^{TS}, C_E^{TS}, P_F^{TS}, M^{TS}, T_S^{TS}, E_U^{TS}, E_C^{TS}, C^{TS}, E_L^{TS}, C_R^{TS}, E_{FF}^{TS}, E_{CY}^{TS}, S^{TS}, R_{BF}^B, R_{DA}^B, R_{SS}^B, R_S^B, G^B, R_{SE}^B, N_I^B, E_M^B, M^B, T_S^B, E_U^B, E_C^B, E_L^B, C_R^B, C_I^B, E_{FF}^B, E_{CY}^B, U^B, U_Q^B, P^B, C^B, P_F^B, A_{CC}^B, C_E^B, D^B, P_Y^B, S^B)$ (27)

$ExUn_8 = f(E_{CY}, T_S, E_C, C, P_F, A_{CC}, C_E, P_Y, S, M, E_U, E_L, R_{BF}, R_{DA}, R_{SS}^B, R_S^B, G^B, R_{SE}^B, N_I, E_M, C_I, E_{FF}, U^B, U_Q^B, P^B, D^B)$ (28)

P($ExUn_8$) = 0.867, with efficiency result of 86.7%

Un_9 = (B U TS U G) = $f(R_{BF}^B, R_{DA}^B, R_{SS}^B, R_S^B, G^B, R_{SE}^B, N_I^B, E_M^B, M^B, T_S^B, E_U^B, E_C^B, E_L^B, C_R^B, C_I^B, E_{FF}^B, E_{CY}^B, U^B, U_Q^B, P^B, C^B, P_F^B, A_{CC}^B, C_E^B, D^B, P_Y^B, S^B, A_{CC}^{TS}, C_E^{TS}, P_F^{TS}, M^{TS}, T_S^{TS}, E_U^{TS}, E_C^{TS}, C^{TS}, E_L^{TS}, C_R^{TS}, E_{FF}^{TS}, E_{CY}^{TS}, S^{TS}, R_{BF}, R_{DA}, R_R, N_I, E_M, M, T_S, E_U, E_C, E_L, C_I, E_{FF}, E_{CY}, C, P_F, A_{CC}, C_E, P_Y, S)$ (29)

$ExUn_9 = f(R_{BF}, R_{DA}, R_R, N_I, E_M, M, T_S, E_U, E_C, E_L, C_I, E_{FF}, E_{CY}, C, P_F, A_{CC}, C_E, P_Y, S, R_{SS}^B, R_S^B, G^B, R_{SE}^B, C_R^B, U^B, U_Q^B, P^B, D^B)$ (30)

P($ExUn_9$) = 0.933, with efficiency result of 93.3%

Un_{10} = (B U T U G) = $f(R_{BF}^B, R_{DA}^B, R_{SS}^B, R_S^B, G^B, R_{SE}^B, N_I^B, E_M^B, M^B, T_S^B, E_U^B, E_C^B, E_L^B, C_R^B, C_I^B, E_{FF}^B, E_{CY}^B, U^B, U_Q^B, P^B, C^B, P_F^B, A_{CC}^B, C_E^B, D^B, P_Y^B, S^B, E_{CY}^T, T_S^T, E_C^T, C^T, P_F^T, A_{CC}^T, C_E^T, P_Y^T, S^T, R_{BF}, R_{DA}, R_R, N_I, E_M, M, T_S, E_U, E_C, E_L, C_I, E_{FF}, E_{CY}, C, P_F, A_{CC}, C_E, P_Y, S)$ (31)

$ExUn_{10} = f(R_{SS}^B, R_S^B, G^B, R_{SE}^B, C_R^B, U^B, U_Q^B, P^B, D^B, R_{BF}, R_{DA}, R_R, N_I, E_M, M, T_S, E_U, E_C, E_L, C_I, E_{FF}, E_{CY}, C, P_F, A_{CC}, C_E, P_Y, S)$ (32)

P($ExUn_{10}$) = 0.933, with efficiency result of 93.3%

Table 1: Summary of Efficiency Level

Models	IN_{set}	No of Metrics in Models	Probability	% of Efficiency
T	30	9	0.3	30.0%
G	30	19	0.633	63.3%
TS	30	13	4.33	43.3%
B	30	27	0.9	90.0%
$ExUn_1$	30	19	0.633	63.3%
$ExUn_2$	30	14	0.467	46.7%
$ExUn_3$	30	27	0.9	90.0%
$ExUn_4$	30	20	0.667	66.7%
$ExUn_5$	30	28	0.933	93.3%
$ExUn_6$	30	27	0.9	90.0%
$ExUn_7$	30	20	0.667	66.7%
$ExUn_8$	30	26	0.867	86.7%
$ExUn_9$	30	28	0.933	93.3%
$ExUn_{10}$	30	28	0.933	93.3%
HUn_3^I	30	30	100%	100%

From table 1, it is evident that models $ExUn_5$, $ExUn_9$, and $ExUn_{10}$, yielded the same optimum results at countering identity attacks. However, employing model $ExUn_9$ will make the system very cumbersome, because it defies usability, from a practical perspective since users will be forced to use multiple devices for authentication (i.e. biometric systems and tokens), which is similar to merging all four single factor models. Model $ExUn_5$ makes a better choice than $ExUn_{10}$ because it employs just two authenticating factors, and still maintains robustness.

Nonetheless, $ExUn_5$ does not satisfy all the required characteristic metrics as postulated in the literature. For example Reusability (R_{USE}) and Randomization (R_M) are not incorporated. Since we want a 100% efficient model over existing multifactor models of graphical password and biometric systems, we must integrate R_{USE} and $R_{M.}$. Our proposed hybrid model is therefore defined as:

$$HUn_3^I = ExUn_5 \cup R_{USE} \cup R_M = f(R_{BF}, R_{DA}, R_R, N_I, E_M, M, T_S, E_U, E_C, E_L, C_I, E_{FF}, E_{CY}, C, P_F, A_{CC}, C_E, P_Y, S, R_{SS}^B, R_S^B, G^B, R_{SE}^B, C_R^B, U^B, U_Q^B, P^B, D^B, R_{USE}, R_M) \quad (33)$$

$P(HUn_3^I) = 1.00$, with efficiency result of 100.0%

The probability of effectiveness of HUn_3^I is therefore a 6.7% improvement over $ExUn_5$.

4.0 False positives

To establish further the strength of HUn_3^I over $ExUn_5$, we used Bayes' theorem to determine the probability that a user authenticated as legitimate by $ExUn_5$ is in fact a false positive. This is established by computing the probability that a model's capability to exhibit a characteristic trait is false positive. Where:

X represents the condition, in which a model incorporates R_{USE} and R_M,

Y represents the evidence of a positive authentication result.

$P(X)$ = Probability of the models population having R_{USE} and $R_M = 0.067$

$P(Y/X)$ = Probability of the Model with R_{USE} and $R_M = P(HUn_3^I) = 1.00$

$P(Y/not\ X)$ = Probability of the Model without R_{USE} and $R_M = P(ExUn_5) = 0.933$

The probability that a positive result is a false positive is obtained by computing:

$$P(X/Y) = \frac{P(Y/X)\,P(X)}{P(Y/X)\,P(X) + P(Y/not\ X)\,P(not\ X)}$$

$$= \frac{1.00 \times 0.067}{1.00 \times 0.067 + 0.933 \times 0.933} = \frac{0.067}{0.067 + 0.870489} = 0.07$$

Hence the probability that a user authenticated by $ExUn_5$ is a legitimate user is about $1 - 0.07 = 0.93$, or 93%, while 7% of authenticated users will be false positive.

5.0 Conclusion

To design effective authentication models, researchers and security technologists concentrate on authentication factors that incorporate just a subset of the universal set of security characteristics. The probabilistic semantics of the different authentication model characteristic metrics, specifically, the likelihoods, naturally lead to the definitions of key authentication characteristic metrics that would enable AM to authenticate legitimate or illegitimate user's probability with a superlative degree of precision. By means of Bayes' probabilistic semantics we were able to provide evidence that the absence of a characteristic metric can affect the efficiency of an authentication model's resistance to identity thefts and the probability that there will be some chances for illegitimate users to be authenticated as legitimate users. The authentication model parameterized with these characteristics can thus be used for making authentication decision by applying Bayesian inference. Our effort is aimed at increasing the resources available to security analysts. Policy makers will have enhanced information when developing identity counterattack measures.

References

[1]. Jansen W, Gavrila, S., Korolev, V., Ayers, R., and Swanstrom, R. Picture Password: A Visual Login Technique for Mobile Device. (2003). Available at: http://csrc.nist.gov/publications/nistir/nistir-7030.pdf.

[2]. Ian J., Alain M., Fabian M., Michael R., and Aviel R. The Design and Analysis of Graphic Passwords. In Proceedings of the 8th Annual USENIX Security Symposium. (1999).

[3]. Suo X., Zhu Y. and Owen G.S. "Graphical passwords: A survey", 21st Annual Computer Security Applications Conference (ACSAC'05). (2005). p 463-472. Available at: http://www.acsac.org/2005/papers/89.pdf

[4]. Monrose F. and Reiter M. Reiter, "Graphical passwords," in Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Eds. O'Reilly Media, ch. 9. (2005). p 157–174.

[5]. Brostoff S. and Sasse. M. Are Passfaces more usable than passwords? A Field trial investigation. In British Human-Computer Interaction Conference (HCI), September (2000).

[6]. Dhamija, R., Perrig, A. Dej`a Vu: A User Study Using Images for Authentication. University of California Berkeley. (2000). Available at: http://sparrow.ece.cmu.edu/~adrian/projects/usenix2000/usenix.pdf.

[7]. Wiedenbeck, S. Waters, J. Birget, J. Brodskiy C. A. and Memon N. "PassPoints: Design and longitudinal evaluation of a graphical password system", International J. of Human-Computer Studies 63. (2005). p 102-127.
Norman. D. The Design of Everyday Things. Basic Books. (1988).

[8]. Jain, A. K.; Ross, A. and Prabhakar, S. "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology 14th (1). (2004). 4 – 20.

[9]. Scheuermann, D.,m Schwiderski-Grosche, S. and Struif, B. Usability of Bometrics in Relation to Electronic Signature. EU-Study 502533/8, Darmstadt. (2002). Available at: http://www.sit.fraunhofer.de/english/SICA/sica_projects/project_pdfs/eubiosig.pdf

[10]. Biometric Technology. Biometric Technical Assessment. Biometrics: Personal Identification in Networked Society, Boston/Dortrecht/London. (2002). p 1- 41. Available at: http://bio-tech-inc.com/Bio_Tech_Assessment.html

[11]. Ross, A. and Jain, A. Information Fusion in Biometrics. In Proceedings AVBPA, Halmstad, Sweden, June, (2001). p 354-359.

[12]. Blonder G. E. "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, United States Patent 5559961. (1996). Available at: http://www.usenix.org/events/upsec08/tech/full_papers/chiasson/chiasson_html/#Blonder

[13]. Davis, D. Monrose, F. and Reiter, M.K. On user choice in graphical password models. In Thirteenth Usenix Security Symposium. San Diego, CA, USA. (2004). Available at:http://www.usenix.org/events/sec04/tech/davis.html.

[14]. Dhamija R. and Perrig A. "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium., Denver, CO. (2000) p 45–58. Available at: http://www.usenix.org/publications/library/proceedings/sec2000/dhamija.html.

[15]. Suo X., Zhu Y. and Owen G.S. "Graphical passwords: A survey", 21st Annual Computer Security Applications Conference (ACSAC'05). (2005). p 463-472. Available at: http://www.acsac.org/2005/papers/89.pdf

[16]. Hurley, E. Experts: Smart cards have their advantages over passwords. (2002).. Available at: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci865191,0 0.html**.**

[17]. FDIC. FFIEC guidance: Authentication in an online banking environment. Available at:
(2005). Http://www.tricerion.com/files/76_FFIEC_strong_authentication_guidance.pdf).

[18]. Pankanti, S., Prabhakar, S. and Jain. A. K. On the individuality of fingerprints. Transactions on PAMI, 24(8). (2002). p 1010–1025.

[19]. Matyas, V and Riha, Z. "Toward reliable user authentication through biometrics," Security & Privacy Magazine, IEEE, Volume: 1, Issue: 3. (2003).

[20]. Ross, A. and Jain, A., Information Fusion in Biometrics. In Proceedings AVBPA, Halmstad, Sweden, June (2001). p 354-359.