



Final Project (MIT Course 6.868)

An investigation relating a sub-Field of AI with event driven security architecture and ideas from *The Emotion Machine*

This project proposal provides the overall scope, software and technical requirements for the stated invention.

Prepared For

Dr. Marvin Minsky
Dustin Smith, Teaching Assistant
Bo Morgan, Teaching Assistant

Prepared By

Ralph A. Rodriguez

Date

May 14, 2008

Registered trademarks and trademarked names are referred to throughout this document. Rather than put a registered trademark (®) or trademark (™) symbol after every occurrence of such names, we state that we are using the names for the benefit of the trademarked owner, with no intention of infringement.

Non-disclosure, Copyright and Confidentiality

© 2008 Ralph A. Rodriguez. All rights reserved.

This document proposal is provided under non-disclosure, confidentiality and proprietary information and has been provided by Ralph A. Rodriguez for the purpose of a final class project for MIT course 6.868. No part of this document may be copied, reproduced, disclosed, or transferred by any means without prior written consent of Ralph A. Rodriguez.

Notice

Ralph A. Rodriguez reserves the right to make updates to the information in this document without prior notice or approval from others. Please consult the author (prepared by) of this document to ensure that you have the latest revision.

Responsibility and Authority

Template

FM-000-0000-01 Rev A

Ralph A. Rodriguez reserves the right to make updates to the template for this document without prior notice or approval from others. Please consult the author of this document to ensure that you have the latest revision.

Prepared For.....	1
Prepared By.....	1
Date	1
Non-disclosure, Copyright and Confidentiality	2
Notice.....	2
Responsibility and Authority	2
Template.....	2
INTRODUCTION.....	4
Using AI concepts with event driven security architectures and ideas from	
<i>The Emotion Machine</i>.....	4
AI-BASED EVENT-DRIVEN ARCHITECTURES (EDA) AND SECURITY ...	5
Using Trouble-Detecting Critics for Security Access.....	6
COMBINING AN AI-BASED SECURITY SYSTEM WITH EXISTING	
SECURITY MODELS.....	7
The Bell-LaPadula security model	7
The Biba Integrity Model	8
The Clark-Wilson integrity model	8
Incorporating Model Sixbased AI ideas with Traditional Security Models.....	9
Model Six Ideas	10
AI-BASED SECURITY COMPLIANCE SYSTEM	10
Current problems with two-factor authentication (T-FA) for system security ...	11
Adaptive Biometric System: Sense – Decide – Respond.....	13
Combining Business Intelligence (BI) and AI-based models	19
USPTO PATENTS, PUBLISHED APPLICATIONS AND REFERENCES: 20	
United States Patents.....	20
United States Published Patent Applications.....	21
Other Reference Material	21
Significance: Novel and Non-Obvious Contribution to the Art	22

Introduction

Using AI concepts with event driven security architectures and ideas from *The Emotion Machine*

The biggest top of mind security issues for 2008 and beyond can best be described by Forrester Research's Big Idea on "The Natural Order of Security¹." By this we mean that security issues are both maturing and recycling continuously; from authentication and authorization to administration and audit. This continual cycle has companies looking back into their organizations to try and validate security decisions made coupled with measuring the increasing needs of the enterprise for major issues such as enterprise single sign-on (E-SSO), identity management, fraud and authentication. In each critical area there are a host of players, both new and old that is leading the way to address these problems. Add compliance, governmental directives and ease of use requirements into the mix and you'll quickly become engulfed in a security management quagmire.

To address this complex mix of issues for businesses there is an opportunity to demonstrate an identity theft and fraud detection system for applications using key artificial intelligence concepts from *The Emotion Machine*. This system will address two key areas; authentication and authorization. The system will attempt to overcome previous learning schemes such as statistical and logical based only to overcome problems mentioned in *The Emotion Machine* like these:

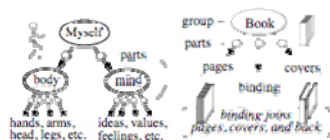
The Optimization Paradox: The better a system already works, the more likely each change will make it worse.

The Parallel Processing Paradox: The more that the parts of a system interact, the more likely each change will have serious side effects.

In other words, as a system gets better it may find that it is increasingly harder to find more ways to improve itself. As Marvin Minsky states in *Emotion Machine* "evolution is often described as selecting good changes—but it actually does far more work at rejecting changes with bad effects. This is one reason why so many species evolve to occupy narrow, specialized niches that are bounded by all sorts of hazards and traps. Humans have come to escape from this by evolving features that most animals lack—such as ways to tell their descendants about the experiences of their ancestors."²

Starting in the mid 1990's, Internet browser-based authentication and authorization were used as simple methods to validate a user's access to a system and its database via an often simple username and password. It did not address whether the user's password had been stolen or borrowed nor did it make any intelligent decisions as to where this user could go beyond what access and privileges were originally set up. Additionally, as enterprise applications get ported to the world-wide-web over mobile communications, smart phones and PDA's the ability to track and trace an individual user becomes more difficult and inherently prone to identity theft and potential fraud.

In 2008 and beyond we need to address authentication and authorization in a whole new paradigm. This new paradigm will address authentication as "are you who you say you are?" to detect identity theft, based on the system's unique statistical tracking method and algorithm, coupled with AI based concepts like **Semantic Networks**³ it will decide your authorization as "are you who you say you are?", "where will I allow you to go?" and "what level of system access will I give you?" to prevent fraudulent activity, in **real-time**, before it happens not after a breach or theft has occurred.



Semantic Networks for 'Person' and 'Book'

¹ July 9, 2004, Forrester's Big Idea called *The Natural Order of Security Yields The Greatest Benefits*

² From Marvin Minsky, *The Emotion Machine* page 16, Chapter VI, July 28, 2005

³ From Marvin Minsky, *The Emotion Machine* page 22, Chapter VII, July 28, 2005

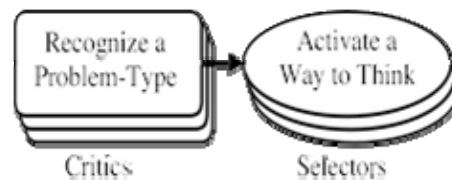
AI-based Event-Driven Architectures (EDA) and Security

Event driven architecture is about creating workflow efficiency as organizations are moving towards an application environment focused on individual “triggered” events and looking for correlation between events that are meaningful. The challenge with systems such as security architectures is that these triggers are logic based only and don’t account for many of the concepts in *The Emotion Machine*. Given the unpredictable, asynchronous nature of today’s business world, seamless business processes are predicated upon an architecture that can respond to discrete events in real-time without imposing a significant processing burden or causing major workflow disruption. In a recent report on event driven architectures⁴ findings confirm this trend toward event driven software by revealing that more than a third (39%) of top performing companies rated Event-Driven Architectures (EDA) as the most important feature of an integration solution.

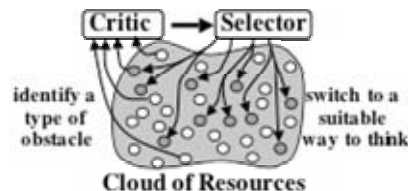
Event driven software in its most basic form has been around for many years, but the formal incorporation of this technology into existing software applications such as security systems and tools is relatively new. In another report on (EDA)⁵ it further demonstrates momentum in the direction of event-driven software by revealing that top performing companies were more than three times as likely to support event-driven business process management (BPM).

Current research data shows a significant push in the direction of event processing solutions with large portion of organizations are planning to implement this technology. However, while there is an unmistakable need for technology that allows for the real-time sensing of, and response to key business events, market deployment of event processing (EP) solutions is still quite immature and could use improvement by incorporating AI based concepts that could put context into a given “triggered” based event to find the particular “pattern” and “analogy”.

Using key AI concepts from Marvin Minsky’s books titled *The Emotion Machine* suggests a Model of Mind based on reacting to ‘cognitive obstacles.’ Minsky calls this the **CRITIC-SELECTOR** model:⁶



On the left are resources called **CRITICS**, each of which can recognize a certain species of “Problem-Type.” When a Critic sees enough evidence that you now are facing its type of problem, then that Critic will try to activate a “Way to Think” that may be useful in this situation.



The goal would be to incorporate this *Critic-Selector* model into a security system to give the system a sense of “Self” and the ability to recognize a problem-type and to activate a way for the system to “think” that utilizes AI based concepts from *The Emotion Machine*. This would increase system performance and create a high-level form of system protection and authentication.

⁴ Aberdeen Group report called [Enterprise Information Integration: The Foundation for Business Success and Transformation](#), January 31, 2008

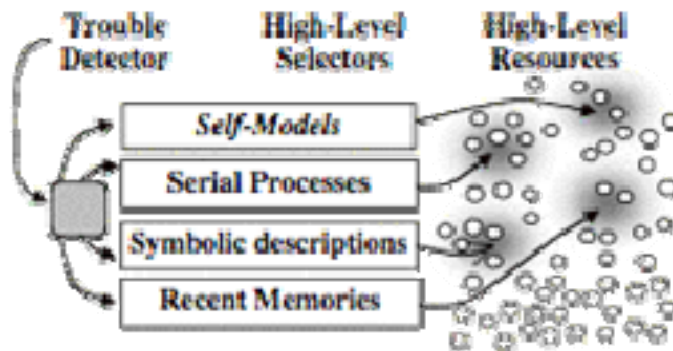
⁵ Aberdeen Group report called [BPM Convergence: Workflow and Integration Meet in the Middle](#), September 30, 2007

⁶ From Marvin Minsky, [The Emotion Machine](#) page 7, Chapter VII, July 28, 2005

Using Trouble-Detecting Critics for Security Access

A Trouble-Detecting Critic assumes the system contains one or more special “trouble-detectors” that start to react when the usual systems don’t achieve some desired goal such as access and authentication verification. Then such a resource could go on to activate other, higher-level processes, such as the ones in Figure 1. This would begin to create self-aware security systems which has several systems and sub-layers with goals to look beyond classical numerical, statistical and heuristic based algorithms only to incorporate multiple critic models, each with their own singular purpose to detect an individual’s access and authentication behavior.

Figure 1: Trouble-Detecting Critics



- **Self-Models** – The system would create predefined representations of the users various goals based on typical conscious system access and behavioral patterns such as navigation and user actions:
 - The system could predict representations of various conscience goals such as type of access needed based on what was selected and sub-conscience goals such as usual pattern of access needed to render specific screens together.
 - This self-model critic would run as a layer to increase system security by locking off other databases and data types and increase system performance because of the segmented type of access and system usage saving memory and open system links.
- **Serial Processes** – The system monitors behavioral aspects of typical pattern based sequential actions and data access:
 - The system would setup serial based processes and workflows that enable the user to start a task of access to specific data and dynamically rendering an end state such as a submit button or other graphical user based rendering for completion of a task or tasks before allowing the user to start a new process or to alert the user or other parts of the system or “critics” of the anomaly in behavior patterns.
- **Symbolic Descriptions** - The system creates a Semantic Network, which uses multiple links to indicate that different components of the end user’s behavioral access create different kinds of relationships and higher level “symbolic representations” (rather than simple connections or links) to help solve more complex problems of detection:
 - User accessing a system to perform a specific functional task
 - User accessing a system to read specific data
 - User accessing a system to change or modify specific data

These linked relationships could be combined to create a symbolic user package and stored as a group in the database to create a behavioral description and combined with other like groups. These groups would be added to the access schema to further determine the confidence level of system access validity.

- **Recent Memories** – The systems takes some amount of time for any particular part of the system to find out what other parts of the system have recently done or detected in order to react to signals from other parts to react to prior events:
 - The system would combine multiple higher-level “symbolic representations” to perhaps create a state of security awareness by having multiple patterns compared and contrasted against its own databases to quickly search for anomalies or uncharacteristic representations.

Each one of these trouble detecting critics would be self contained with its own dedicated memory, CPU and specific task handling to solve a goal related to access and authentication.

Combining an AI-based Security System with Existing Security Models

The identity and fraud detection system uses multiple methods to measure identity theft and fraud. The basic premise is to create a real-time application and database usage profile using a complex validation algorithm which captures a user’s rate of accessing a system, their password attempts, typing speed and entry style, time of day, time zone, internal data accessed, session info, environment and IP or GPS based location. The key measurements are to capture this information in real-time and at the sub-millisecond rate or better today and the nanosecond rate in the future for fraud detection and monitoring.

If the system detects fraud, the unique AI-based workflow process begins. This workflow can process multiple methods of security. The system can prompt a user for an “n-tiered security profile” of data which the user setup initially. This tier security model uses multiple standard models.

The Bell-LaPadula security model

The Bell-LaPadula security model was developed to formalize the U.S. Department of Defense multi-level security policy. The model is a formal state transition model of computer security policy that describes a set of access control rules by the use of security labels on objects, from the most sensitive to the least sensitive, and clearances for subjects:

- Top Secret
- Secret
- Confidential
- Unclassified

The Bell-LaPadula model focuses on the confidentiality of classified information. The system will use this model to demote a user’s authorization data access should any initial identity theft or user fraud be detected.



- **IF** fraud detected **DEMOTE** security level from Top Secret (highest) to N-level (lowest) below based on suspected rating of fraud detection:
 - Top Secret = Level 4
 - Secret = Level 3
 - Confidential = Level 2
 - Unclassified = Level 1

The Bell-LaPadula model is built on the concept of a state machine with a set of allowable states in a system. The transition from one state to another state is defined by transition functions.

A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy. To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object to determine if the subject is authorized for the specific access mode. The clearance/classification scheme is expressed in terms of a

lattice. The model defines two mandatory access control rules and one discretionary access control rule with three security properties:

- The Simple Security Property states that a subject at a given level of confidentiality may not read an object at a higher confidentiality level (no read-up).
- The * (star) Security Property states that a subject at a given level of confidentiality must not write to any object at a lower level of confidentiality (no write-down).
- The Discretionary Security Property uses an access matrix to specify discretionary access control.
- The transfer of information from a low-sensitivity paragraph to a higher-sensitivity document may happen in the Bell-LaPadula model via the concept of Trusted Subjects. A Trusted Subject can violate the * property if the intent of the policy is not violated.

This security model is directed toward confidentiality (rather than data integrity) and is characterized by the phrase: "no read up, no write down"

With Bell-LaPadula, users can only create content at or above their own security level (secret researchers can create secret or top-secret files but may not create public files). Conversely, users can only view content at or below their own security level (secret researchers can view public or secret files, but may not view top-secret files).

The Bell-LaPadula model has some weaknesses, including:

The model considers normal channels of information exchange not covert channels.
The model does not specify how to work with file sharing and servers in modern distributed systems.
The model does not explicitly define what a secure state transition is.
The model is based on multi-level security policy and does not address other secure policies that an organization might require.

Based on these weaknesses you could create a “**Semantic Network**” which combines higher level “symbolic representations” (rather than simple connections or links) to help solve more complex problems of detection by incorporating multiple models together and connecting them based on the nature of those relationships.

The Biba Integrity Model

The Biba Integrity Model describes rules for the protection of information integrity⁷. In this formal model, the entities in an information system are divided into subjects and objects. The notion of a secure state is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby “**Inductively**” proving that the system is secure.

Using the “**Critic-Selector**” model I will implement a system whereby the demotion of a user’s rights and access immediately flags this user to not be able to gain applicable access to like kind states.



- **IF** fraud detected **DEMOTE** user and **FLAG** user and **PREVENT** access to like kind states.

The Clark-Wilson integrity model

The Clark-Wilson integrity model is based on transactions.⁸

⁷ Wikipedia – Online Encyclopedia - http://en.wikipedia.org/wiki/Bell-LaPadula_model

⁸ TCSEC85 National Computer Security Center, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, December 1985. Sections 2.1.1, 2.2.1, 3.1.1, 3.2.1, 3.3.1, and 4.1.1, contain the security policy requirements. Sections 3.1.3.2.2, 3.2.3.2.2, 3.3.3.2.2, and 4.1.3.2.2 contain the security policy model requirements, which are summarized on pages 98-99.

A well-formed transaction is a series of operations that transition a system from one consistent state to another consistent state. In this model the integrity policy addresses the integrity of the transactions. The principle of separation of duty requires that the certifier of a transaction and the implementer are different entities. Specifically, in the Clark-Wilson Model there are Integrity Verification Procedures (IVP), Transformation Procedures (TP), Constrained Data Items (CDI) and Unconstrained Data Items (UDI). The only transactions that can apply to data items are IVPs and TPs.

Again, based on these weaknesses you could create a “**Semantic Network**” which combines higher level “symbolic representations” (rather than simple connections or links) to help solve more complex problems of detection by incorporating multiple models together and connecting them based on the nature of those relationships.



IF Clark-Wilson Model fails **COMBINE** or **COMPARE** Bell-LaPadula and **COMBINE** or **COMPARE** Biba Integrity Model to create representation of all three groups.

Incorporating Model Six⁹based AI ideas with Traditional Security Models

An abstract example on how a system might incorporate **Model Six** ideas into the security model would be the following:

1. User A attempted to login with the wrong password (Confidence level 50%)
 - a. The system would trigger an event to assume you have simply just made an error and provide you with another try because it assumes no foul play but would check how other current users were interacting with the system. (*Self-Conscious Reflection*)
2. User A logged in with the correct password 2nd Attempt (Confidence level 60%)
 - a. The system would consider the recent access attempt and log the change in password state to reflect what access variables might have changed and look for ways to avoid system changes or try another method based on simple login errors to create the ideal access state. (*Self-Reflective Thinking*)
3. User A typing signature is “very similar” (Confidence level 70%)
 - a. The system would assume a commonsense state whereby its confidence level would be trending directionally higher based on the prior trial and error access states yet continue to monitor its “diagnostician” reasoning. (*Reflective Thinking*)
4. User A typing from known host (Confidence level 80%)
 - a. The system would consider several alternatives for an increase in confidence level and tries to decide which would be best based on comparing other relationships. (*Deliberative Thinking*)
5. User A login is during their normal working hours (Confidence level 90%)
 - a. The system learned from prior data states stored that when the user reaches this level of confidence it quickly promotes its confidence level. (*Learned Reactions*)
6. User A given “Secret” level authority
 - a. The system quickly assigns the appropriate security level based on its confidence level of the user. (*Instinctive Reactions*)

INTERP94 National Computer Security Center, The Interpreted TCSEC Requirements, (quarterly).

Gasser, M., Building a Secure Computer System, Van Nostrand Reinhold Co., N.Y., 1988.

⁹ From Marvin Minsky, The Emotion Machine page 15, Chapter V, July 28, 2005

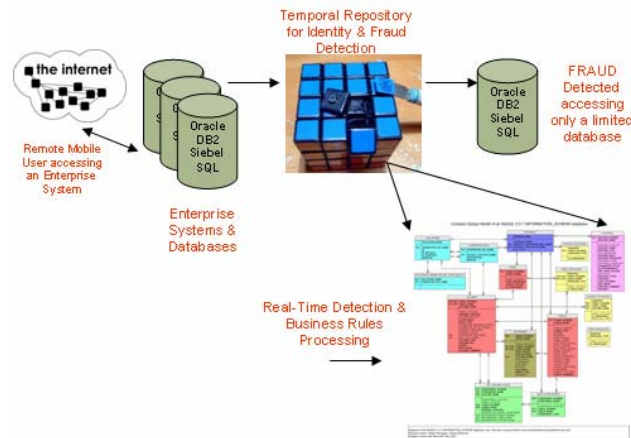
Model Six Ideas



AI-based Security Compliance System

The notion of an AI-based system using ideas from *The Emotion Machine* combining existing security models and patterned based biometric detection is the next paradigm in creating a security compliance system (Figure 2) capable of using multiple Critic-Selectors to “Sense, Decide and Respond” in order to identity theft of fraudulent activity of a system or systems. Creating a program we’ll call authentication manager (AM) will enable the capture of a user’s keyboard, mobile device or PDA entry screen(s) using pattern or an “electronic heartbeat” signature that has logged onto a system with an enterprise single sign on (e-SSO) authentication schema (E.g. AOL/MSN/Brower-based Password messenger lightweight client side application) to capture information about the user environment, heart-beat, IP address, IP subnet, default gateway and then communicate this information to an (AM) in an encrypted form via a secure communication channel (SSL).

Figure 2: Global View of System Architecture



This electronic heartbeat would provide the system with a series of parameters that can be compared against “Known configuration” variations from the known configuration and would trigger security warning if any Critic-Selector flags an event. The manual interaction block in (AM) allows procedures to be paused at the sub-second rate and wait for some additional user interaction. This would allow the “Ask me another question” aspect of verifying a user is who he/she says they are.

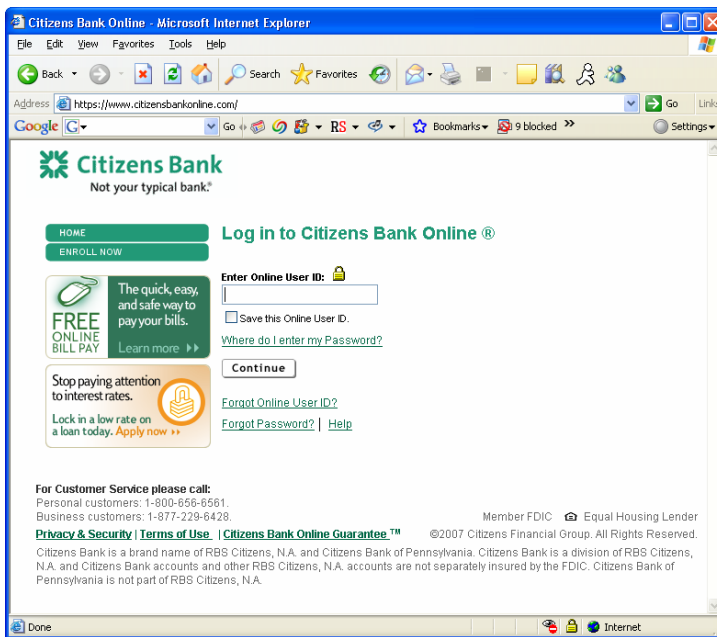


Example: **IF** initial login fails **PAUSE** and **ASK** a follow on authentication question.

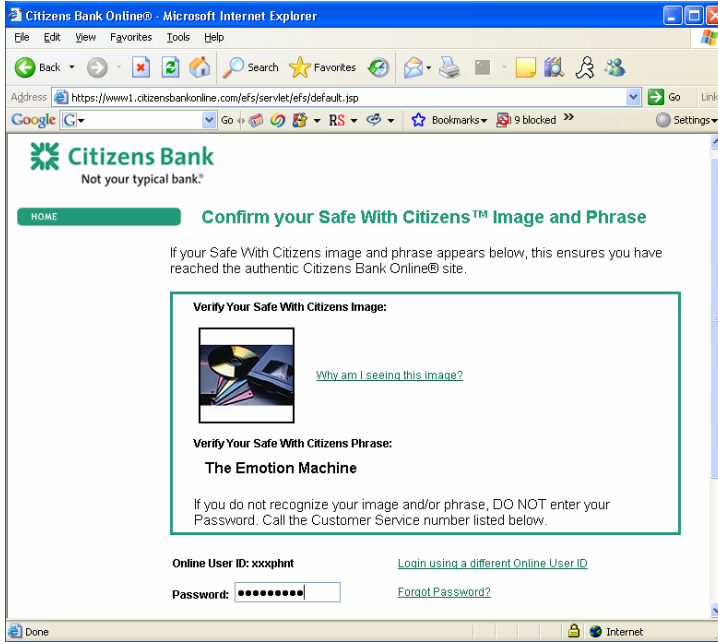
Knowing the correct information would not be enough. Spoofing the information would also not be enough as you will need to understand so much more about the user and their pattern characteristics to thwart the next generation fraud detection and security system.

Current problems with two-factor authentication (T-FA) for system security

The challenge with online password protected systems such as “online banking” surrounds the current implementation of protecting an end user or customer because of the information and process used to authenticate or verify a person's identity for security purposes is based on two-factor authentication (T-FA), which is a system wherein two different methods are used to authenticate your identity. Using two factors as opposed to one is supposed to deliver a higher level of authentication assurance. Using more than one factor is sometimes called strong authentication. The problem with the current usage of “strong authentication” is that it’s based on static information which does not change or have any inherent intelligence to protect the authenticity or access protection of an end-user.

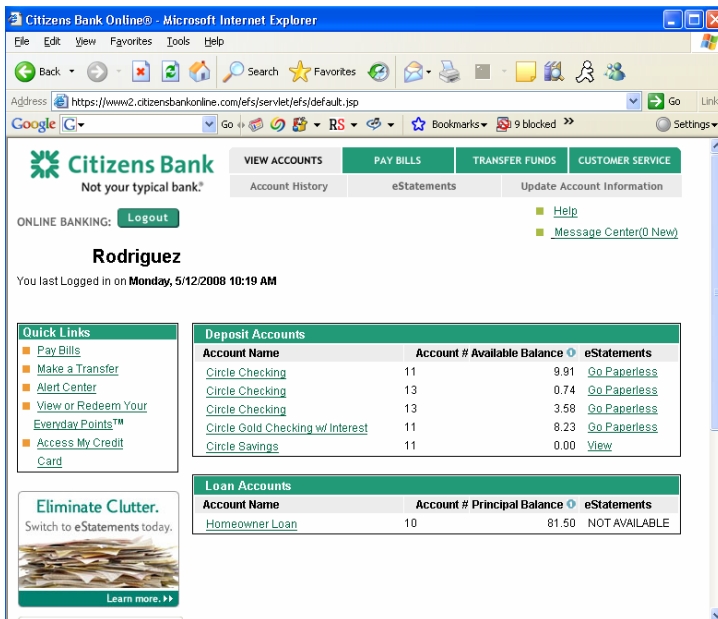


With current two-factor authentication implemented an end-user would see the following upon entering a correct username and password:



As you will see above the implementation of two-factor authentication is based on a user's correct username and password coupled with the usage of an "image" previously chosen upon initial account setup as well as a "pass phrase" also chosen during account setup.

At this point in conventional banking systems a correct combination of username and password will enable anyone to both login into the system (authentication assurance) and gain full access to every end-user capability and system functionality such as payments and money transfers irrespective of whether the real user has logged into the system or whether it is identity theft or fraud.



The opportunity for an AI-based implementation of system security based on an intelligent event driven architecture with key concepts and ideas from *The Emotion Machine* creates the next paradigm in intelligence based systems with adaptable biometrics.

Adaptive Biometric System: Sense – Decide – Respond

A conceptual design implementation and usage of an AI-based security system would be the following:

Imagine you log into a banking system looking to gain access. In this new system you would provide your username and password. The system however doesn't know it's really you, so the system begins to first look at your environment information in this initial security layer. It sees that you've logged in from the same IP address before and compares a variety of other environment data in its database such as:

- IP Address – IP address of the host system from where the user logs in
- Host Name – NetBIOS name of the system from where the users logs in
- Monitor Resolution – Resolution of the monitor from where the users logs in
- Browser Type – The type of browser the user normally uses
- OS – The type of OS the browser is installed.
- Ctrl C, V usage – The habit of using Ctrl C, V.
- GPS / Location - Could be country or coordinates where machine is located
- Time - Machine usage time and duration
- Time Zone - Machine time zone

Based on this simple rule the system's confidence that "You are who you say you are" begins to rise or fall based on these parameters and rates your initial access with a degree (%) of confidence.

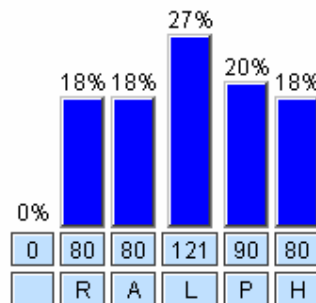


Examples:

- IF** environment collection equals prior environment **PROMOTE** confidence level x (%)
- IF** environment collection does not equal the prior environment **DEMOTE** confidence level x (%)
- IF** environment collection does not equal the prior environment **DEMOTE** confidence level x (%) and **SELECT** another way to access or **SUB-DIVIDE** environmental data sets using "Reflective Critics"

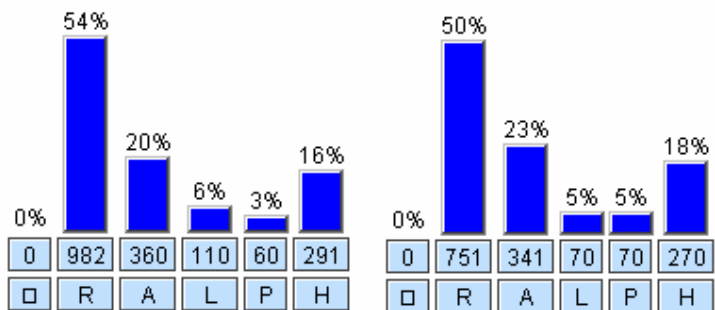
The next challenge surrounds how the system can determine whether the person entering the username and password data didn't steal or acquire the information fraudulently. In this new adaptive biometric system the system captures the user's "electronic heartbeat" signature which has the ability to capture the following measurement characteristics:

- **Per Key Time:** The time difference in milliseconds between press and release of a key in the keyboard or device pad.

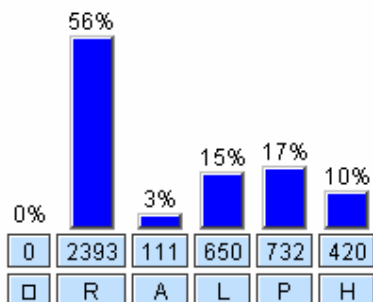


In this second layer the system could try another series of methods, such as matching related environment variables should the **Per Key Time** biometric fail or rate the confidence level based on the prior mean value of matching environment variables using the "diagnostician critic."

- **Pattern Gap:** The time delay between two consecutive key strokes.



*** Similar patterns (CURRENT and PRIOR) in both charts above indicating a high confidence level



In this third layer the system could apply another “diagnostician critic” to undo the confidence level rating should the pattern not match (ABOVE) the correct user data due to false positive issues such as an injured hand or different state of mental awareness (inebriation).

- **Reflective Time:** The difference between the time a question was asked and the time user started to enter the first character in the answer.

Powered by **Adaptive Biometric Compliance System™**

Time (Control Entered into text box):Sun May 11 13:36:30 EDT 2008

Time (Control out of text box):Sun May 11 13:36:36 EDT 2008

Entered Characters	Time interval between Characters (milliseconds)	Time interval between Key Press & Release (milliseconds)
0	0	110
R	1582	60
A	301	80
L	90	120
P	60	90
H	270	60

If the initial sign-on password fails or is suspect based on past environment variables or patterns, the Critic-Selector workflow flags the confidence level of the password as “low” and will ask another question. The workflow picks a random question based on the user’s initial validated session.

A good workflow example would be the following:

User A (who has top secret clearance) logs into a system and they get the password wrong the first time. If this is a bank/government your suddenly very interested. You don't want the user to be aware you're interested you want to see what they will do. The AM workflow fires an event which email/pages your security manager. They go to their terminal and look at their screen. On their screen is information from the security system.

- A security warning issue has been raised (User A)

The security manager then clicks on this and drill down into the issue

- This gives an audit trail of what user A is doing
7. User A attempted to login with the wrong password (Confidence level 50%)
 8. User A logged in with the correct password 2nd Attempt (Confidence level 60%)
 9. User A typing signature is "very similar" (Confidence level 70%)
 10. User A typing from known host (Confidence level 80%)
 11. User A login is during their normal working hours (Confidence level (90%)
 12. User A given "Secret" level authority
 13. User A will be asked additional question when attempting to view "Top Secret" areas

However this story could go another way

1. User A attempted to login with the wrong password (Confidence level 50%)
2. User A attempted to login with the wrong password 2nd Attempt (Confidence level 25%)
3. User A logged in with the correct password 3rd Attempt (Confidence level 35%)
4. User A typing signature is very "dissimilar" (Confidence level 25%)
5. User A typing from unknown host (Confidence level 15%)
6. User A typing outside their normal working hours (Confidence level 10%)
7. User A typing from unknown IP address (Confidence level 5%)
8. User A (trace route) finds user in Non normal continent (5%)
9. User A asked second question
10. User A get answer correct (Confidence level 10%)
11. User A typing signature is very "dissimilar" (Confidence level 8%)
12. User A given "Unclassified" level authority
13. User A will be asked multiple additional questions when attempting to view "Classified and above" areas

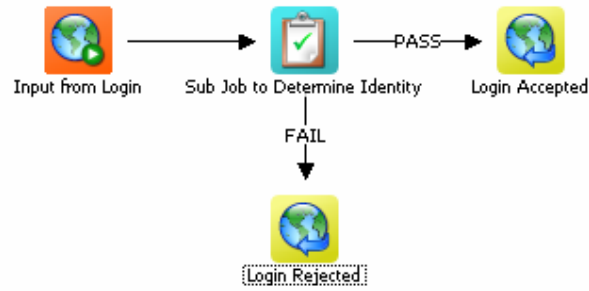
At this point the security manager could use this real time data to make a decision about this user, perhaps call their cell phone and check they are trying access the system. Perhaps they would just automatically kick them out of the system and have them call the help desk

In the second example User A may well be User A from the first example; you don't want to kick him out of the system he may be trying to log into. He may just be a very tired businessman on a trip to another continent. However the system can adapt to this by initiating various "critics" thereby relaxing the users' security clearance until they have answered enough questions to raise the confidence level. This could also include some form of direct call to confirm the user's identity.

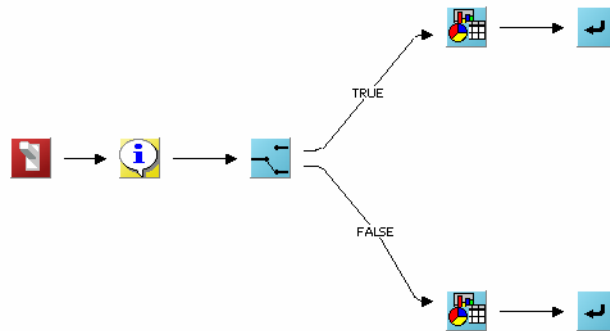
A graphical view of the model would look like the following:



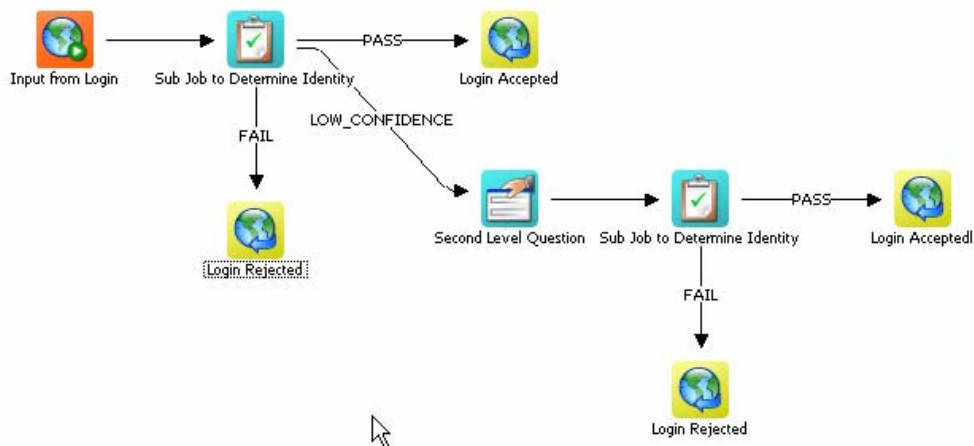
IF user credential fails **PROMPT** session to initiate another question in the workflow



Question: “Welcome Ralph, what city and state were you born in?”



The user has to know the correct answer and must give it quickly otherwise the reflective time will not be able to match the pattern time. The authentication manager (AM) will ask the sign on application which will host the login question how long does the user take to answer the question irrespective of whether this info is in the public domain, what is known, the heartbeat of the answer will give us a further confidence level. If the confidence level drops then the authentication manager (AM) can trigger events without the user even knowing.

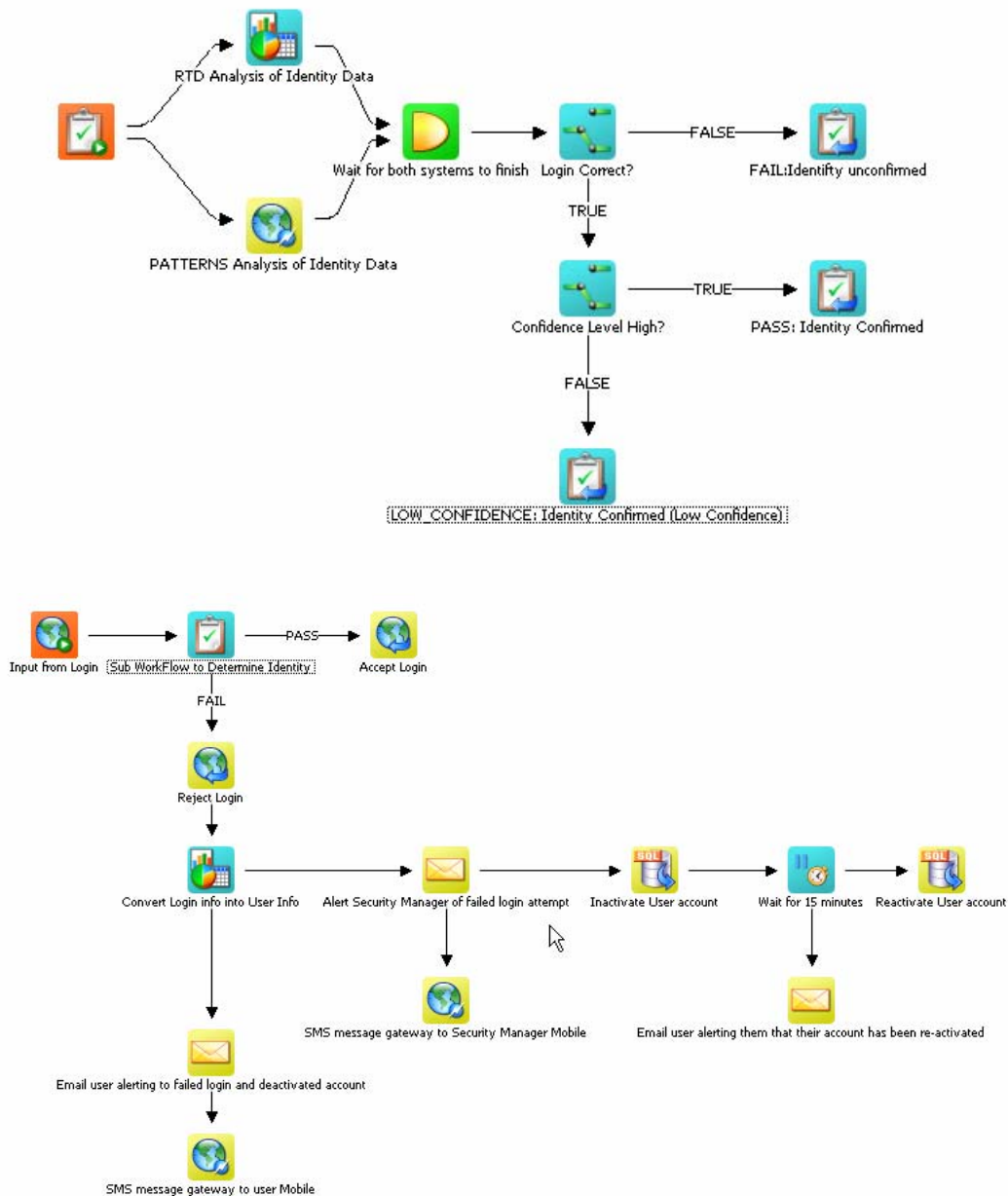


The authentication manager (AM) exposes jobs as web services to an external hacker this would simply look like a web service that is going to validate the sign on. This unique checking disguises itself as a simple web service known throughout the Internet yet is in reality a “Honey Pot.” This information is

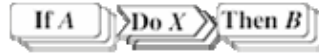
passed to the (AM) would then be used to feed a workflow which would be used to determine are you who you say you are.

The beauty of the workflow is that irrespective of whether the user knows it or not certain security actions such as (recording your access, tracing all future communication, locking down parts of the system, informing a security manager of a security violation) could be done without the user even knowing that they have caused a breach of security. An example would be (Figure 3) whereby you would alert both a user and security manager via both email and SMS text message, plus deactivate user account for 15 minutes emailing user on reactivation or determine the identity sub-job with confidence level checking.

Figure 3: Combining multiple Decision Flows

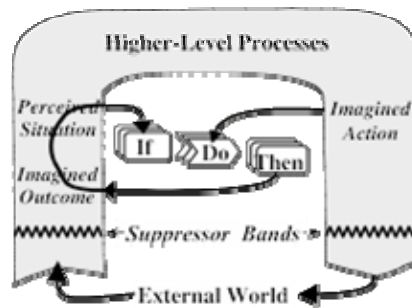


How would we analyze the heart-beat signature, is actually a **Neural Network** more than anything but will require a lot of training to get things right. One approach is to store previous login information that could be used to come up with a statistical confidence level. Decisions about what to do would be based on confidence levels could be user defined depending on the workflow but you could also design the system that does that same sort of thing, by predicting the outcomes of various actions. Let's assume that it has some rules like these.



We would give the system a way to replace what it currently registers as a low confidence level (situation A) by the prediction described by this rule. Then when system is again in situation A, and then considers doing action X, this will cause the system to 'imagine' that it is now in a situation like B so that it could combine multiple situations as described by Minsky in *The Emotion Machine*¹⁰ (Figure 4).

Figure 4: Prediction Capabilities of System



How would you first acquire the environment data? This would need to be part of an initial data collection activity (much like a speech recognition systems work, this could be performed by the AM) but also successful logins should also be used to feed the data model improving the detection capabilities. Like in voice recognition software, (AM) could be trained overtime to capture the heartbeat of a user based on the security model needed and the level of access required. The higher level of access or validation the longer the algorithm needs to statistically recognize your electronic heartbeat. This combination of software tools combined together would enable a novel implementation of a security paradigm.

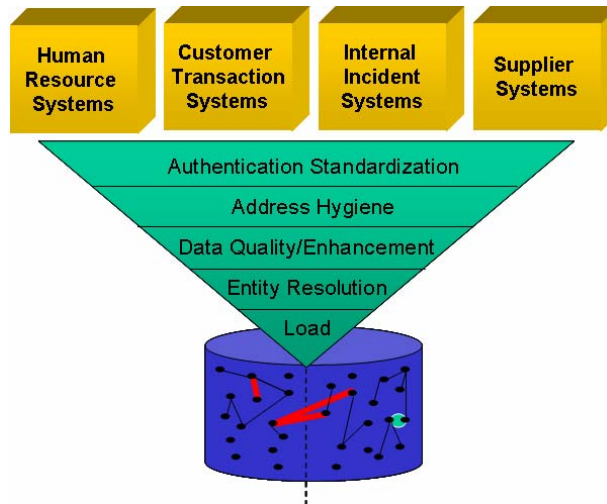
The user defined workflow should decide what confidence level is needed by creating a series of serial based steps:

1. Sign in programs parses data along
2. Environment data (session data, IP local time, etc.)
3. Authentication Manager (AM) analyzes this session data
4. AI of System "Do I trust you?"
5. Back to sign in, second level
6. Random question
7. Statistical analysis typing signature
8. Credentials back with token (pass)
9. View workflow using different security levels outside working environment

¹⁰ From Marvin Minsky, *The Emotion Machine* §5-9. Prediction Machines, Chapter V, July 28, 2005

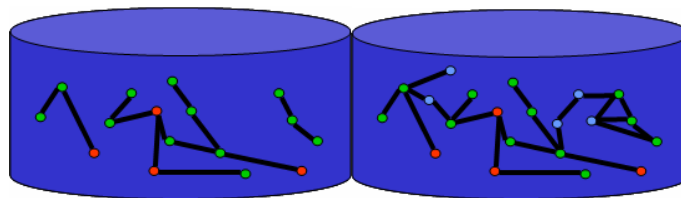
Combining Business Intelligence (BI) and AI-based models

Combining business intelligence and analytical dashboards with an AI-based model to render “real-time” data feeds could give a continuous live display of security breaches in enterprise systems by reporting on changing confidence levels as they occur using a dashboard based business intelligence system that looks for various correlation or relationship matching stored in complex databases incorporating a *Critic-Selector* model.

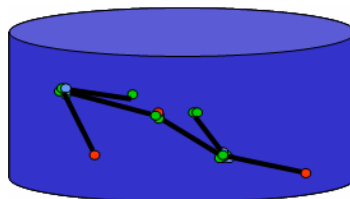


For example, a *Critic-Selector* security model could embody a set of ‘rules’ like these:

- If** the correlation seems familiar, try reasoning by Analogy.
- If** the correlation seems unfamiliar, change how you’re describing it.
- If** the correlation still seems too difficult, divide it into several parts.
- If** the correlation seems too complex, replace it by a simpler one.



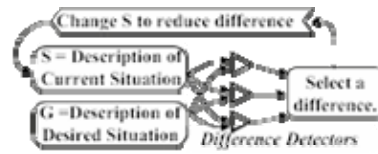
For example, using traditional methods, both databases (above) show no distinct correlation or match



For example, using a *Critic-Selector* security model (above) could potentially find the correct match

A lot has changed in fifty years since the AI-based Difference-Engine. As with the key ideas and concepts from *The Emotion Machine* “No machine had clearly displayed those three traits of *Aim*, *Persistence*, and *Resourcefulness*—until 1957, when Allen Newell, Clifford Shaw and Herbert

Simon developed a computer program called the “*General Problem Solver*.” Here is a simplified version of how it worked; we’ll call this version a Difference-Engine.



At every step, this program compares its descriptions of the present and that future situation, and this produces a list of differences between them. Then it focuses on the most serious difference and applies some technique that has been designed to reduce this particular type of difference. If this succeeds, the program then tries to reduce what *now* seems to be the most serious difference. However, whenever such a step makes things worse, the system goes back and tries a different technique.”¹¹

The foundation of these prior ideas from decades ago, coupled with new AI-based concepts it is my goal to be able to demonstrate a new way beyond 2-factor authentication currently being employed in the enterprise to one whereby the enterprise can utilize key AI ideas from *The Emotion Machine* and *The Society of Mind* to create intelligent security systems.

USPTO Patents, Published Applications and References:

United States Patents

United States Patent	6,151,593
Cho , et al.	November 21, 2000

Apparatus for authenticating an individual based on a typing pattern by using a neural network system

Abstract

A user authentication apparatus for use in controlling access to a system inputs an owner's login name and password and then extracts the owner's timing vectors from keystroke characteristics with which the owner repeatedly types the owner's password to thereby form a training set. A neural network is trained by using each of the owner's timing vectors in the training set as an input. Thereafter, when a user inputs the owner's login name and password, it is checked if the user's password is identical to the owner's password. The user's timing vector is extracted from a keystroke characteristic to type the user's password if the checked result is affirmative, and the user is prohibited from accessing the system if otherwise. The user's timing vector is applied to the trained neural network as an input and a difference between the input and an output of the neural network is compared with a predetermined threshold. The user will be permitted to access the system if the difference is not greater than the threshold and prohibited from accessing the system if otherwise.

¹¹ From Marvin Minsky, *The Emotion Machine* page 22, Chapter VI, July 28, 2005

Method and apparatus for verifying an individual's identity

Abstract

A device and method for verifying the identity of an individual based on keystroke dynamics comprising a keyboard for the inputting of data in the form of alphanumeric characters by keystrokes, a timing encoder coupled to the keyboard for timing periods between keystrokes, a CPU coupled to RAM and to the timing encoder for generating a template for the individual, the template comprising a first plurality of features based upon a first set of time periods between keystrokes from a first set of keystrokes of the individual and the CPU determining a plurality of extracted features based upon a second set of time periods from a second set of keystrokes, and comparing the template to the plurality of extracted features such that the identity of the individual may be verified.

United States Published Patent Applications

PUB. APP. NO.	Title
1	20070250920 Security Systems for Protecting an Asset
2	20070245151 System and method for classifying regions of keystroke density with a neural network
3	20070234056 Method and apparatus for multi-distant weighted scoring system
4	20070233667 Method and apparatus for sample categorization
5	20070198712 Method and apparatus for biometric security over a distributed network
6	20070150747 Method and apparatus for multi-model hybrid comparison system
7	20040187037 Method for providing computer-based authentication utilizing biometrics
8	20020188854 Biometric rights management system

Other Reference Material

Mohammad S. Obaidat, David T. Macchiarolo; "An On-line Neural Network System for Computer Access Security"; IEEE Transactions on industrial electronics, vol. 40, No. 2; pp. 235-242, Apr. 1993. .
M. S. Obaidat, Balquies Sadoun; "Verification of Computer Users Using Keystroke Dynamics"; IEEE Transactions on systems, man, and cybernetics-Part B: Cybernetics, vol. 27, No. 2; pp. 261-269, Apr. 1997.
Umphress, D. et al., "Identity Verification Through Keyboard Characteristics", Int'l Journal of Man-Machine Studies, 23(3): 263-273, 1985 (Umphress).
Leggett et al., "Verifying Identity via Keystroke Characteristics", Int'l Journal of Man-Machine Studies, 28(1): 67-76, 1988 (Leggett).
M. Brown et al., "User Identification via Keystroke Characteristics of Typed Names using Neural Networks", Int'l Journal of Man-Machine Studies, 39(6): 399-1014, 1993 (Brown).
Monrose et al., "Authentication via Keystroke Dynamics", Proc. of the ACM Workshop, pp. 48-56, 1997 (Monrose).
Robinson et al., Bleha et al., "Computer-Access Security Systems Using Keystroke Dynamics", IEEE Transactions on Pattern Analysis and Machine Intelligence, PAMI-12(12): 1217-1222, December 1990 (Bleha) have developed methods based on keystroke dynamics for verification of users with successful results.
Gaines et al., "Authentication by Keystroke Timing: Some Preliminary Results", Rand Report R-256-NSF, Rand Corporation, 1980 (Gaines).

Significance: Novel and Non-Obvious Contribution to the Art

The significance of this invention will be to help solve single sign-on (E-SSO) password vulnerabilities for mobile users who access enterprise systems globally and to decrease password authentication ineffectiveness. The prior art suggest solving biometric issues using neural networks, distributed networks, HTTP protocols, JAVA language and computer based systems only. With the global adoption of mobile users and ubiquitous Internet access a new protection mechanism is needed which uses elements of the prior art coupled with mobile capabilities, protocols and technologies. Lastly, incorporating AI-based ideas from *The Emotion Machine*, using critic and selector models, to initiate an “artificial self reasoning model” of system access, control and future strong authentication will be the keys to future true security.