Maximum Security Online: Best Practices for Designing the Ultimate Online Security Strategy

Contents

Executive Summary

This paper is intended for chief security officers and risk management executives tasked with forming the enterprise strategy to combat online fraud. It is also intended to lay a common language for all C-Level executives who need to familiarize themselves with the threat environment, as well as the available solutions and their associated ramifications.

While a layered approach to online security helps balance the needs and desires of users (to transact conveniently), with the enterprise needs to reduce the risk of fraudulent activity, it is the view of the author that no single technology can effectively meet the nuanced needs of users and online enterprises. While regulations have focused on "user authentication," recent FFIEC guidance and real-world applications call for a layered approach to security that deploys overt, Real-Time methods, agent-less client device identification (CDI), forensic analysis and data masking.

Both Real-Time and Time-Delayed fraud detection systems have a role in combating Internet fraud, but how can they be used in concert with one another for even greater lift in detection and prevention? This paper discusses how organizations should best employ Real-Time and Time-Delayed systems, in addition to human intelligence, to achieve maximum security online.

While this paper does not directly focus on the critically important process of account registration or enrollment, it is important to understand that these processes are vulnerable. Since anyone can acquire the necessary personal identification needed to assume a false identity (i.e. birth certificate, fake driver license/ID card, credit report), it is very difficult to establish the true identity of the end user, thus rendering the global context of security and authentication inherently problematic. Often people think there "must be" some easy and definitive way to authenticate the user's identity, yet anything a user knows and presents as credentials can be obtained fraudulently or under duress.

Since true identities of the users simply cannot be discerned online with total certainty, this paper addresses a realistic blueprint for a security schema that brings together an array of risk management methodologies, best practices and technology. This schema helps produce a security environment that offers a convenient user experience, while providing accurate risk assessment during the login, throughout the session and prior to the execution of transactions.

Many businesses that operate today "On Demand" and in Real-Time are limiting their ability to detect, prevent and recover their fraud losses. This paper may trigger a change in the very business model of such enterprises, helping to maximize profits, protect the customer experience with convenience and privacy, and extend the life-time-value of every user, while minimizing fraud and operational losses as well as customer inconvenience and attrition.

Best practices for online security are outlined as a four-tier strategy:

1) Overt authentication on the front-end,
2) Agent-less client device identification (CDI) and surveillance that allows for monitoring of fraudsters presenting credentials as well as their site navigation,

3) Covert transaction risk monitoring, and

4) Overt data masking to obscure/hide sensitive customer information.

Given the enemy (the fraudster) is ingenious in devising penetration strategies and nefarious schemes, it can be argued that maximum security online must include a healthy dose of expert human intelligence. Fortunately, the majority of the technologies needed to establish maximum security online are now commercially available in the market; although an amazingly small percentage of enterprises have deployed the full spectrum of necessary capabilities.

Definitions

Authentication

The term "authentication" is used in many ways. In its simplest form, the word 'authentic' relates to something being real, true and genuine. In an anonymous medium such as the Internet, the only real authentication can come from *credential presentment*. In other words, the credentials presented do not necessarily mean that the authentic user is on the other end. Only by process of association is it deduced that the user is the person who is presenting the credentials.

Likewise, the same concept extends to hardware tokens. For example, if a hotel maid finds and uses a hotel guest's login credentials (user name, password and possibly even a one time password token) to access that guest's account, permission will be granted even though the rightful account owner is not presenting the credentials.

This concept also applies to registration and enrollment. Since it is possible to fraudulently obtain someone's personal documentation (i.e. birth certificate, driver license/ID, credit report), it is very difficult to establish the true identity of the user during such processes.

Open vs. Closed Communities

Before determining the optimal security strategy, it is important to first clarify whether the community is open or closed. Closed communities are those that can limit users to certain hardware or software configurations. Typical closed communities include corporate networks and some gambling sites. As a closed community, corporations can provide employees with one time password (OTP) hardware tokens as a required security measure for network login. Likewise, they can also employ software tokens that generate a new password at each login.

Very few online sites are considered closed communities, as the Internet is designed for open and anonymous communication. Hence, some high-risk businesses can operate as 'closed communities' and force their users to go through any number of prerequisites before granting access to the site. For example, requiring users to install software that helps identify their PC every time they attempt to login to the site.

Hence, the challenge for most enterprises transacting on the Internet is truly "authenticating" users in an open community.

The Threat Environment

Knowing that all it takes is the right credential presentment, fraudsters have been devising methods to obtain this information. In effect, they are practicing the age-old art of impersonation in new, electronic forms using techniques such as:

- **Phishing** – Sending fraudulent e-mails that appear to be from the user's financial institution or a merchant to lure victims to provide their credentials.
- **Pharming** – Poisoning the DNS cache on the user's PC so it appears to access the correct URL, when in reality it is redirecting the browser to a spoofed site; this can also be done to a DNS server which poisons an entire region.
- **Spoofed Site** – Presenting a link to a fake site that looks and feels like the original financial institution or merchant site.
- **Duress** – Using e-mail or calling the user with a threat of shutting down the account if they fail to respond and provide their user credentials.
- **Malware** – Installing malicious software on the user's PC to collect information through keyboard logging, screenshots and file searches.
- **Man-In-The-Middle (MITM)** – Passing a user's PC through a proxy that is privy to all traffic between the user and the website, including the user's credentials.
- **Session Hijacking** – Using an authenticated session (after the user authenticated) to mimic a new session and conduct transactions from the compromised account.
- **IVR Spoofing** – Faking Interactive Voice Response (IVR) systems that call on users to dial and provide their account information and/or credentials.
- **Cookie Theft** – Theft of software cookies that are used to assume the victim's digital identity.
- **Shoulder Surfing** – Viewing of sensitive information behind the shoulder of an authenticated user (i.e. if a user views check images online or at a physical ATM / teller location).

This list is far from complete, yet the point remains: given the human ingenuity of the fraudsters, they will always find a way to glean information from unsuspecting users,.

Since we can never be sure that credentials have not been compromised, it is imperative that compromised credentials do not turn into compromised accounts.

We're Fighting Humans, Not Machines

Before the security issue can be solved, it is critical to understand the kind of issues the online industry faces. One cannot assume that the problem can be solved through technology alone.

Take for instance, the anti-virus world where hackers write malicious code used to infect the host. By design, anti-virus detection software is blind to new attacks and is invariably one attack behind the latest scheme. After a new virus is detected, usually by humans, it is inspected down to its "DNA" and a detection algorithm is devised to alert when this exact code is executed again.

At this point, every replica of the same virus will exhibit the same code execution, thereby allowing a digital guard to search for it and quarantine it upon engagement. Why then can't the same digital guard find the next virus, inspect its "DNA" and write the inoculation code?

The reason is very simple – the fight is against humans, not machines. While some heuristics allow anti-virus mutations to be detected even if the exact code was not executed, the true problem lies with new attacks that have never been seen before. The same question can be asked about anti-SPAM solutions. Every network that installs a SPAM filter still gets some SPAM because the latest attacks have not yet been detected. Far worse, some good e-mails are trapped and never reach the intended recipients.

The main challenge in defending against online fraud attacks is the ingenuity of the humans behind them and the fact that enterprises most often try to counter them solely with machine intelligence.

False Positives and False Negatives - A Necessary Evil

In the end, a site must be built to conduct business. Otherwise, it will be incredibly secure, yet provide little or no profit. Any security measure deployed to millions must be easy and convenient to use, which in most cases, also makes it easy to foil.
For that reason alone, there must be some measures of balance between convenience, security and privacy, in the form of False Positives and False Negatives, which are defined as:

False Positive: A good user transaction declined under the suspicion of being fraudulent

False Negative: A fraudulent user transaction approved while not sounding the alarm

In a classic case of False-Positive detection, a credit card company calls a customer to verify charges that were made legitimately. Had the purchase been declined in Real-Time (at the store), the card company would have an angry customer who was denied a legitimate purchase. However, a risky transaction that passed through, yet later confirmed as fraudulent, is a False-Negative. Such occurrences end up hurting the company as well as the customer, particularly if the customer is then required to change his/her accounts.

The Market Environment

Security Based on the User is Only as Secure as the User

Thus far, we have examined the anonymity of the Internet and how it is leveraged in fraud attacks. This problem is exacerbated exponentially when the security credentials are distributed among millions of users who are not security experts. Regardless of how often customers are educated about online security, (i.e. "Our Company employees will NEVER ask you for your user name and password"), they will always be susceptible to Phishing attacks. Therefore, a security solution based on users inherently casts users as the weakest link.

Conditioning the Users

One method of conditioning is to train users to "expect" certain visual measures when they act in a certain way. While this provides a positive reassurance to valid users ('consumer confidence'), it tells the fraudster when they have tripped the alarm, hence, helping them to reverse engineer the system.

This is the equivalent of 'Tipping Your Hand' in a poker game, or revealing your cards to the opponent.

Tipping one's hand to the fraudster is one issue, but conditioning users to expect challenge questions is another matter. Should the online site consider taking away those challenge questions one day, it will create a new set of issues. For example, when a user travels and logs into his/her account from a different computer and does not receive the challenge questions, it can quickly cause the user to believe that the site is no longer secure – or worse, that it is not the authentic site.

For instance, consider a watermark that users view as the site's seal of authenticity. Once users associate this seal with their security, there could be a time when a browser will not load the seal due to technical reasons and will show an error placeholder in its place.

Now, consider an attack that will show this red "X" instead of trying to mimic the site's seal. Most savvy – and novice users – will think there is a browser technical issue rather than suspect fraud.

Internet communication is a two-way street, and just as the sites do not know who is presenting the credentials, the users do not know if they landed on the authentic webpage.

As the lifeblood of online business, a positive customer experience is critical to a holistic security strategy. Changing the behavior of millions of customers is no small feat given the time and expense needed to educate them – both of which are often vastly underestimated.

Changing user behavior even once is difficult; changing it time and again to stay ahead of new fraud schemes becomes nearly impossible. More often, the security methods appear deficient or worse yet, are tuned out altogether.

The Conflicting PR Objective

One of the objectives for having strong online security is to make users feel protected. Users learn about a site's security system not only from what they see and do online, but also from company correspondence, such as e-mail, phone calls, letters, etc. When a credit card company calls to verify a transaction, the customer knows the company is monitoring his/her account. Even in the case where a customer receives a call that ends up being a false-positive, the consumer is made aware that someone is watching over the account. This typically has a positive and lasting effect on the consumer's perception of the site's security.

Unfortunately, PR and security often are on a collision course. While it is important for the consumers to know their account is protected, the real security mechanism must remain covert and not be revealed to the fraudsters.

Balancing Convenience, Security and Privacy

One approach is to simply give up and assume that true security cannot be achieved. Yet, the implications associated with this line of thinking are extreme, and not likely to keep users from transacting online. It is important to recognize that giving users "some" credentials – a way of

identifying themselves online – increases their sense of security and trust with a website.

Credentials need to be user-friendly, as opposed to providing an account ID and password that are secure, yet difficult to remember and therefore only artificially secure. After all, users are not machines.

To illustrate this point, study the following account ID and password for two minutes, then look away and try to recall them both.

- Account ID = a3GH67db889Ikl
- Password = 6yGtrf44sedw67

As you can see, this is nearly impossible. While a long and case-sensitive password may achieve security, the inability to remember it will cause great frustration and inconvenience. Furthermore, for large user bases, complex passwords will ultimately result in locked-out users and thousands of expensive call center requests to reset passwords. Some enterprises opt to allow password reset online, which then opens another door for the fraudster. How does the enterprise know who just initiated this password reset?

Humans are wired a certain way and are pre-disposed to remember shorter length, meaningful passwords. Hence, sites should allow users to select passwords they can relate to and memorize. However, solely depending on users who are susceptible to Phishing attacks for your security strategy to succeed is unrealistic; additional layers of security are needed to achieve the necessary balance.

Effective security must be both easy and secure.

The Online Security Environment

Security Options: Authentication is Not a Silver Bullet

A common misconception is that with stronger authentication, the security issue is solved. In light of the growing sophistication and complexity of fraud schemes, we know this to be far from true. Just as the police employ both overt and covert agents, so should any security system. Here are some examples of how overt and covert methods complement each other in life:

- Police: Street Cop and Undercover Detective
- Army: Infantry and Special Forces
- Air Force: F-16 Fighter Jet and Stealth Bomber
- Navy: Marines and Navy Seals
- Casino: Pit Boss and Backroom Operations
- Credit Cards: Overt Holograms and Black Light Features
- Currency: Watermarks and Special Inks
- Airport: TSA Agents and Air Marshalls

Together, a synergy is created that allows for maximum security away from the eyes of customers, and offers two safety nets of protection from any catastrophic failure by each individual component.

Pros and Cons of Available Authentication Methods

	Definition	Pros	Cons
User Name & Password	User defined credentials	Convenient, user driven	Can be compromised/phished; users may forget
Images	User selected image from database	Easier to remember than password	Easily compromised, hard to authenticate, multiple account holders may not know image selected
Secret Questions / KBA	User selected challenge question & answer	Easier to remember than password	Easily compromised; multiple account holders may not know answers
Toolbars	User downloads / installs custom security toolbar	Simple and relatively convenient	Requires user adoption and consistent use; can be compromised by virus or malware
Alerts & Email Notifications	Rules-based triggers that send notification of suspect activity	Customizable and timely	Rules quickly outdated with each new attack; requires continual system tuning
Cookies / Flash Objects	Data/objects web servers deliver to first time users for future ID	Easily distributed to many users / devices	Easily deleted or stolen from many users; not designed for true security
Document Image Masking	Blurring sensitive information in scanned online documents	No user action or storage required	Cannot verify digital signatures to authenticate if fraud is suspected
Hardware Tokens (OTP)	Physical device that delivers changing one-time password	Relatively secure	Users must carry device; can be lost or stolen; requires timely response; expensive to deploy
Hardware Tokens USB (Dongle)	Physical device that stores user credentials external to PC	Relatively secure	Users must carry device; can be lost or stolen; requires timely response; expensive to deploy
Software Tokens	Stores user credentials on the device / PC	Relatively secure, easy to distribute to many users	Requires download; may not be compatible with all machine types
Digital Certificates	Electronic "credit card" that stores and delivers user credentials	Convenient for repeat visitors	Can be deleted or compromised by virus or malware
Biometrics	Hardware device that captures unique physical traits	Relatively complex to spoof	Users must adopt / use; expensive to deploy
IP Address / HTTP Header Data	Internet protocol or HTTP data used to identify devices	Easily collected from any online transaction	Easily spoofed; no way to identify same device using multiple IPs; can change often
Printable OTP (Bingo Cards)	Randomly generated one-time passwords from pre-defined grid of passwords	Easily printed / used by visitors	Spoof websites lure users to submit credentials
Virtual Keyboard	Virtual control extension of physical keyboard	Does not require additional device	"Back door thief" virus can send captured images of user screens
Out of Band (Phone Call)	Customer support contacts user to verify authenticity	Cost effective, can be automated	VoIP reliability; outdated contact data; no answer
Overt Device Identification (Download)	Software download / installation to detect / authenticate device configuration	Relatively secure	Requires download and user opt-in; fraudster will not adopt and therefore escape detection
Agent-less Client Device Identification	Covert device configuration recognition / authentication	Highly accurate, detects any type device, no user downloads, enrollment, registration or adoption	No targeted PR / Marketing message to build customer confidence

The table above outlines a number of industry-adopted authentication and security measures, their definitions, and the pros and cons of employing each in a financial services, e-commerce or other online business environment where the identity of the end users is critical to the safety of the business.

KBA: A Catch 22?

To foster the additional authentication of "suspicious" transactions, a growing industry practice is the use of Knowledge Based Authentication (KBA). With KBA, the user is prompted to answer additional questions that only he/she should be able to answer. For example, a user who has successfully logged in, browsed the site, and then decided to wire money is prompted with additional questions to establish a higher level of "authentication" before completing the transaction. The assumption is that the KBA will provide a clear answer as to who is on the other end.

However, such assumptions can be dangerous. Should the additional KBA be answered by the fraudster, no other line of defense exists before the transaction is completed, resulting in a false sense of security. For instance, the KBA could be answered by a perpetrator who gained initial access and gleaned information from the account. Alternatively, should the valid user fail to answer the KBA, the transaction will decline and result in a negative customer experience. There are many reasons why a valid user would fail a KBA challenge, namely: a spouse who was not privy to the original answer ("House Holding Effect"), misspelling of the correct answer ("Saint John High School" versus "St. John High School"), or simply forgetting it after a few months.

Should one still consider the use of KBA, it is critical to determine when to invoke the questions in order to retain any value. If challenge questions are posed only when risky transactions are requested (towards the end of the session), one must ask, "Why weren't the questions posed ahead of time to prevent an unauthorized user from even getting into the account?" Furthermore, it begs the question: *who has been wandering around the account thus far?*

On the other hand, if the KBA is part of the initial login process and the user cannot answer correctly, he/she will be denied access. If the question is answered correctly, the user is granted full access to the account. Either way, the risks are the same. If the valid user is denied all access, the customer will be further inconvenienced which will also lead to increased call center volume. Worse still, if the account is compromised, the fraudster has full access to the account without any further inspection.

When KBA is used in conjunction with other security measures, such as device recognition technology, a philosophical security conundrum emerges. If the device recognition technology detects an unauthorized PC attempting to access an account, the user will be prompted with a KBA in an attempt to salvage the login. This KBA prompt, as already established, can be easily defeated by a fraudster and therefore defeats the purpose. It is the equivalent of presenting a fraudster with an easier lock to pick if they failed to open the stronger one.

No News is NOT Good News

If customer interaction is part of the authentication process, one must consider all options: getting the correct answer, getting the wrong answer, and getting no answer. Certain security strategies include sending SMS messages to the cell phone on record when a user attempts to conduct a risky transaction. However, it is important to establish a procedure should the user not respond. Perhaps this is a legitimate user whose cell phone battery is dead or not with them. However, it may be a fraudster who did not receive the SMS message and, therefore, did not respond. Either way, if no response is received, the institution must take action.

If a valid user fails to receive and respond to the message, he/she will be locked out of the account. If the customer is not contacted, the risk of attrition is elevated. If it is a fraudster who fails to receive and respond to the message, he/she, too, will be locked out of the account. The customer must be contacted to avoid the risk of overlooking an early warning of a fraudulent attack. To illustrate, imagine that a teller is approached by a person with a key to a Safe Deposit Box. When asked for further identification, the person simply turns around and runs out… should the teller just go back to normal operations and address the next customer?

If your security strategy includes customer interaction, failure to handle such exceptions will not yield maximum online security.

Online Security Best Practices: Authentication and Beyond

Thus far, we have addressed the following:

- True online authentication is not feasible, as the Internet is not designed for it.
- The ultimate fight is against humans, not machines.
- Users should play a role in your security strategy, yet should not solely be relied upon. Users are not secure by design.

Given these conditions, the following strategies for enterprise security should be considered:

1. Real-Time Security at the Front-End – Provides ironclad doors at the front-end based on strong authentication.
2. Time-Delayed Security on the Back-End – Provides ironclad doors at the back-end which do not let

any transaction execute until exhaustive analysis is performed.

3. Combination of Real-Time and Time-Delayed Security – Decisions are based on what is possible and best to perform at each juncture of the transaction's lifecycle and involve human intelligence, in addition to sensitive data masking.

There are a number of schemes that would not be detected with only Real-Time systems, namely:

Detecting one PC logging into multiple accounts – this is impossible to detect based on analyzing one login at a time. Due to transaction latency and database seek-time, this type of detection is not conducive to Real-Time analysis.

Detecting device manipulations, cookie theft, or session hijacking – this is impossible to detect based on analyzing one login at a time. Due to transaction latency and database seek-time, this type of detection is not conducive to Real-Time analysis.

Detecting offline fraud that results from fraudulent account access (wires or counterfeit checks) – it is impossible to detect the link between these events and fraudulent online access because they occur out of sequence and in different channels with long delays between the occurrences.

The Secuity Trinity: Three Critical Questions

At the core, three primary questions must be addressed by the risk manager when a user attempts to login, view and potentially transact online:

1. Should the site allow the user to login to the account? (Authentication)

2. Should the site monitor if one device is accessing multiple user accounts even without transacting? (Account Surveillance)

3. Should the site allow the transaction(s) to execute and money to leave the account? (Transaction Risk Monitoring)

The first question lends itself to a Real-Time check, in which the user is either authenticated or not, with a simple "yes" or "no" answer. The user then receives an approval or rejection page.

The second question relates to transaction authorization and is not required to be answered in Real-Time or during the session. Rather, it can, and should be determined post-session. This question should be answered with "shades of gray" (vs. "yes" or "no") and if necessary, prompt human intervention for final verification. This aspect of maximum security should require a re-evaluation of Real-Time fulfillment of transactions that involve the transfer of funds or goods.

The third question reveals if a perpetrator is lurking and waiting to see when accounts have high balances, or alternatively, if they are gleaning sensitive customer information from online document images to commit offline fraud such as check counterfeit or siphoning accounts via ACH. For that reason, it is critical to mask sensitive customer and account data in addition to quickly detecting and containing such attacks.

Don't Tip Your Hand

Just as card players do not show their hands to competitors, the same strategy applies in risk management. When fraudsters attempt to login and conduct transactions, they can be detected in a variety of ways: at login, during the session, or after the session is closed. By detecting and stopping them at the

door, it lets the fraudsters know; "with these credentials, we know you are bad." Both good customers and fraudsters will be stopped at the door if the credentials are incorrect. For a good customer, it is an inconvenience, yet for the fraudsters, this becomes important information that tips them off.

The strategy should not focus on stopping fraudsters at login since it quickly reveals what not to do. It gives the perpetrator the tools and information needed to reverse engineer the security measure and provides a map for planning their counter-move.

Negative Lists

No matter how rich the negative list is, when a fraudulent user receives the error message, they know they did something they should not have. There is a diminishing marginal utility to a negative list since the bad guy was just told what not to do. Remember we are fighting humans and not machines, so the perpetrators are likely to try again with a different set of credentials that are not (yet) on the negative list.

Naturally, after a fraud case is confirmed, the fraud investigators can and should update the front door negative list to try and prevent these credentials from coming in again. This effort is both Sisyphean[1] in nature and reactive.

Of course, this is not to imply a company should not attempt to stop known fraudsters at the door. Rather, anticipating future moves by invisibly monitoring behavior is equally important. In every successful fraud attack, the perpetrator slipped through the front gates and any back-end fraud detection processes that were in place. Adding layered security to the transaction lifecycle provides more interception points.

The Element of Surprise

In Sun Tzu's *Art of War*, the "Skilled General" is described as:

- A master of concealing his true dispositions and ultimate intent
- When capable, he feigns incapacity; when near, he makes it appear that he is far away
- His spies and agents are active everywhere, gathering information
- Moving as intangibly as a ghost in the starlight, he is obscure, inaudible
- His warfare is based on deception

A parallel exists between SunTzu's doctrines and the art of fraud detection and prevention: remain covert and mask your true disposition. It is critical to continually gather new information, to adjust the course, and deceive the enemy as much as possible to prevent counter-moves. The most important of which is to maintain the element of surprise to prevent the enemy from detecting the enterprise's online strategy.

Imagine a hunter who with precise aim lines his quarry into the crosshairs. Then, mistakenly, his laser marker turns on, revealing a visible beam of red light which marks the animal's forehead. The animal is immediately alerted to the shot and escapes. The element of surprise is completely lost, as well as the covert approach.

Masking Visible Sensitive Customer Information

To determine the usability and security of a site, a detailed security audit must be performed. It should include all sensitive customer information and scanned documents that contain potential points of vulnerability, such as online checks, statements and previous transactions details. Some of this data

is presented in text format, thus, it can be partially masked. Account information should be truncated. For example, if the full account number is 123456789, the visible information shown would be xxxxx6789.

However, the same account number that is partially covered on the textual form is left completely viewable on a scanned check image. In fact, other customer data such as address, signature and potentially driver's license or SSN, are also shown on online check images – none of which are masked. Given the anonymity of the Internet, all sensitive customer information should be completely or partially masked. Most legitimate users do not need to view their own sensitive information. Yet, by leaving the information viewable, it provides everything a perpetrator needs to counterfeit a check or siphon the account.

Even if an enterprise could authenticate who is logging in with 100 percent certainty, masking a portion of the account would still be necessary and prudent to prevent "shoulder-surfing" and to achieve maximum online security.

Let Humans Do What They Do Best and Machines Do What They Do Best

We have established that Real-Time systems cannot and should not detect all possible fraudulent scenarios, thus, separation of duties must be determined. It is not feasible for the front-end to conduct back-end investigations. As evident in the hotel and casino industries, when a guest registers at the hotel, the front desk staff will ask for a valid ID. If the name matches a negative list entry, security staff will be alerted. While front desk employees are not part of the investigation team that adds names to this negative list, they do fulfill their role in the ecosystem of security.

The back-end, inherently, has additional time and human intelligence. Therefore, it should feed the negative lists that serve as the first line of defense. This approach also helps when a wrong value is placed in a negative list, which can wreak havoc in Real-Time, such as blocking an IP address from a popular Internet Service Provider. While an attack coming from a popular IP Address may be mathematically "right" to place in the negative list, the overall implications would be disastrous.

The Medium Is the Message

Part of setting up any security perimeter includes limiting multiple login attempts originating from the same source. If the wrong password is provided three times on an account, the account should be frozen until direct support from the company is obtained. Alternatively, multiple successful logins originating from the same source into different accounts are equally suspect and must be monitored as well.

The velocity needs to be monitored on multiple vectors, such as IP address, Login ID and Device ID. All of which require database seek time and CPU processing cycles that can consequently delay the customer experience.

When one point of origin is linked to many accounts, the medium is the message. When one source is attempting, or has actually gained access to multiple accounts, there is good reason to suspect it as fraud.

What is the Best Recipe for Success?

If each login was guaranteed to originate from the account holder, there would be no false-positives. However, the Internet has no such guarantees. Sound strategy, sophisticated technology and advanced human detection skills are required beyond the basic credential presentment and authentication process.

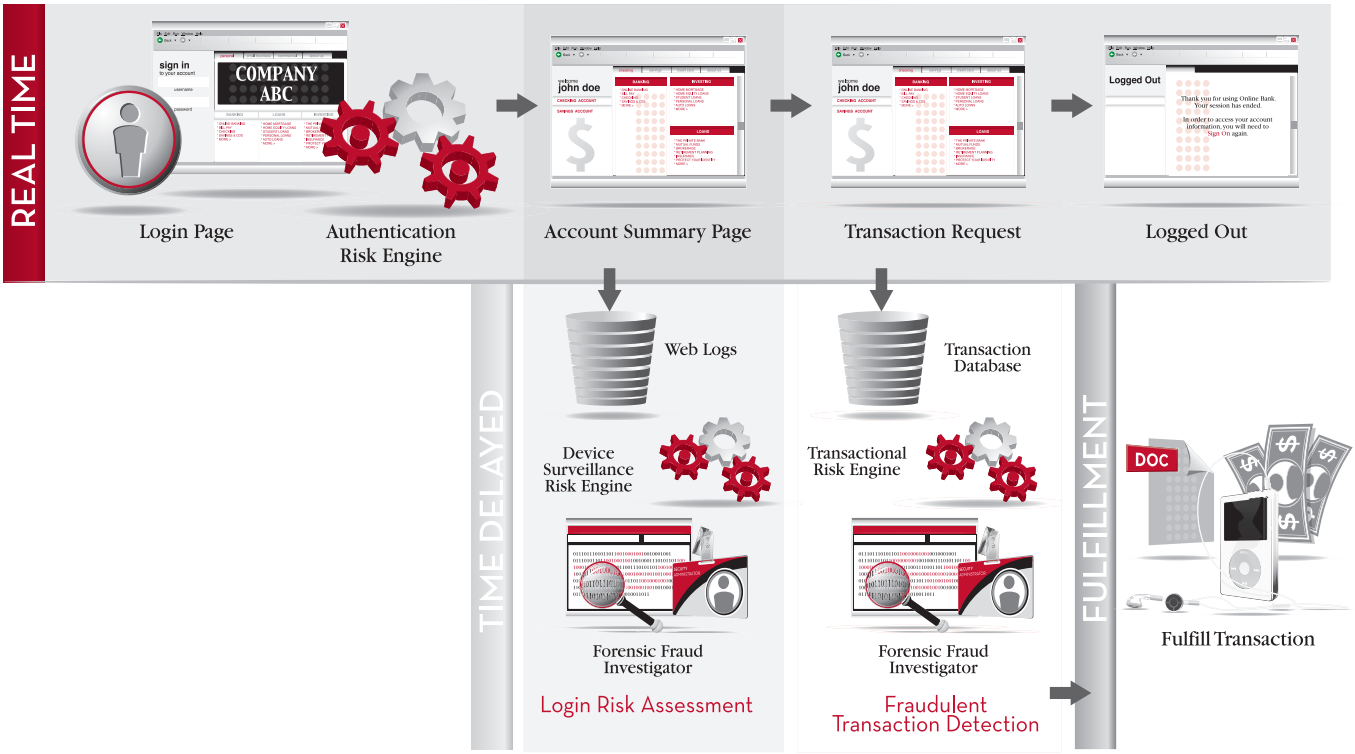
Proposed Best Practices

Best practice employs user name and password authentication, and adds a check into a negative list based on intrinsic values (such as Device ID, account ID or high-risk countries). The error message in case of a "hit" should be as 'vanilla-flavored' as possible, as to not tell the potential crook why they are being denied. For example, "our website is currently experiencing heavy traffic, please try again later." It is then recommended that the business contact the account holder to validate this activity for customer service reasons, as well as proactive fraud detection.

Best practice calls for minimal interaction with the user and minimal checks in Real-Time, all the while garnering as much insight as possible from the user and his/her device for further review prior to executing transactions.

A holistic strategy combining Real-Time with Time-Delayed security methods results in maximum security online with minimal inconvenience to users and minimal exposure of an institution's security strategy to the crooks. The best practices, once again, should focus on the following core activities:

- Overt authentication on the front-end,
- Agent-less client device identification (CDI) and surveillance that allows for monitoring of fraudsters presenting credentials as well as their site navigation,
- Covert transaction risk monitoring, and
- Overt data masking to obscure/hide sensitive customer information.



The Blueprint

The total blueprint of the transaction flow and steps above illustrate the three primary questions that must be addressed:

Should the site allow the user to login to the account? (Authentication)

Should the site monitor if one device is accessing multiple user accounts even without transacting? (Device Identification and Account Surveillance)

Should the site allow the transaction(s) to execute and money to leave the account? (Transaction Risk Monitoring)

Real-Time Steps

Step 1: Customer Browser hits the Login Page

Step 2: After filling in the User ID and Password, a login request is initiated

Step 3: User's password is matched against a password database, as well as a Thin check against the risk engine to verify if the transaction violates critical business rules

Step 4: Login is granted into the system (with sensitive customer information masked) <User is wandering around and may attempt to transact or glean information>

Step 5: Transaction is requested, (i.e. new payee, change of address, wire transfer, etc.) <No additional prompting of the user in Real-Time>

Time-Delayed Steps

Step 6: Risk Engine analyzes the session to assign risk score and recommend action

Step 7: If need be, a human investigator will asses the risk and can choose to invoke an automated verification or personal call (i.e. for high-end clients)

Step 8: Transactions that clear will be fulfilled

Not only does this security process and transaction flow help answer the fundamental three questions and also achieves the following business objectives:

- Maximize good users' throughput
- Maximize fraudulent declines
- Maximize good users' experience (convenience)
- Minimize good users' false positives (declines)
- Minimize fraudulent false negatives (approves)
- Minimize 'tipping of one's hand' and instant gratification that enables reverse engineering

Final Thoughts

A holistic security framework consists of three areas of risk focus: authentication at login, transaction monitoring, and account and session surveillance. Each area is chartered with one mission and does not rely on the others. By applying these three together, you achieve a sum that is greater than the value of each area on its own. In effect, you have emulated the very environment we have always trusted, namely one that relies on complex assessment of both initial recognition and subsequent behavior to determine whether authenticated activity should be intercepted.

Today, we understand more than ever before that online authentication is not feasible since the Internet is not designed for true user authentication. Given that the ultimate fight is against humans, not machines, we must prepare for an ongoing 'arms race' in the war against Internet fraud and identity theft. Combining Real-Time and Time-Delayed security with intervention from company investigators allows an organization to let users take part in the security ecosystem, without hinging the strategy upon them. Real-Time plus Time-Delayed security delivers maximum security online.

41st Parameter
17851 N. 85th Street
Suite 250
Scottsdale, Arizona 85255
(888) 843-4178 (Toll Free)
(480) 776-5500
(480) 776-5504 (Fax)