

MBA Panel on Process Procedures in Security

– 27th March 2007 –

Beyond Passwords

Paul Barrett

CEO, Passfaces Corporation

Strong Authentication Drivers

- Compliance
 - FFIEC, GLB, SOX etc.
- Fraud Protection / Risk Reduction
 - Increasing remote access
 - Expansion of network access to 3rd parties
 - Increased volume of attacks
 - Increased sophistication of attacks
- Protection of Reputation
 - Breaches are bad for business
- User Reassurance / Trust
 - Insecure users don't use or will stop using Web
- Competitive Advantage
 - E.g. CitiBank
- **Passwords Are Broken!**

Passwords Are Broken

“Passwords are the weakest of weakest links” – Bill Gates at RSA2007

- They can be guessed or “cracked”
 - 3.8% of MySpace users’ passwords are single dictionary word
 - 8% are single dictionary word plus the number “1”
 - 23% could be cracked in 30 minutes
- They are written down by users
- People use the same one everywhere
- They are never changed
- They can be phished
- People will give them up for a bar of chocolate!

Authentication Challenge

- Users are the weakest link
 - They are responsible for most password problems
 - You cannot expect them to follow instructions
 - If it is possible for them to get it wrong, some definitely will
 - If they don't like it, they will find a way round it
- Most authentication technology developed for enterprise
 - Users were not a primary consideration
- Consumers are even more challenging
 - Most will not read instructions as a matter of principle
 - Some will deliberately get it wrong
 - Cost of help-desk support is mostly not justifiable
 - If they don't like it, they will walk
 - To a more costly service channel or to a competitor

Authentication Requirements

1. **Higher Security** – *than passwords*
2. **Usability** – *no complex pass codes or procedures*
3. **Non-Intrusive** – *users are adverse to change and reluctant to do more*
4. **Visibility** – *users want to see that companies are increasing security*
5. **Mobility** – *users log on using different PCs in different locations*
6. **Consistency** – *of user experience*
7. **Reliability** – *no false rejection, no system errors, no user errors*
8. **Bidirectional** – *verify the User to the Site AND the Site to the User*
9. **Flexibility** – *for varying risk levels and customer choice*
10. **Easy Integration** – *with current systems and procedures*
11. **Low Cost** – *Procurement, deployment and ongoing maintenance*

Authentication Requirements

1. **Higher Security** – *than passwords*
2. **Usability** – *no complex pass codes or procedures*
3. **Non-Intrusive** – *users are adverse to change and reluctant to do more*
4. **Visibility** – *users want to see that companies are increasing security*
5. **Mobility** – *users log on using different PCs in different locations*
6. **Consistency** – *of user experience*
7. **Reliability** – *no false rejection, no system errors, no user errors*
8. **Bidirectional** – *verify the User to the Site AND the Site to the User*
9. **Flexibility** – *for varying risk levels and customer choice*
10. **Easy Integration** – *with current systems and procedures*
11. **Low Cost** – *Procurement, deployment and ongoing maintenance*

Process Procedures in Security Beyond Passwords

What Are the Alternatives?



Biometrics



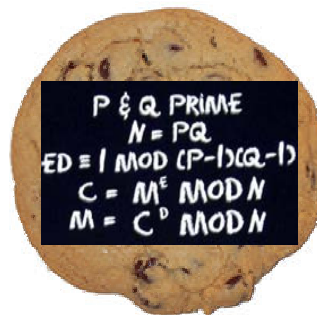
Tokens



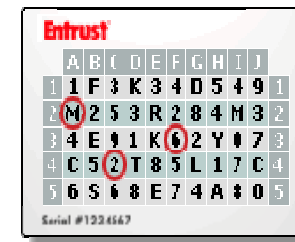
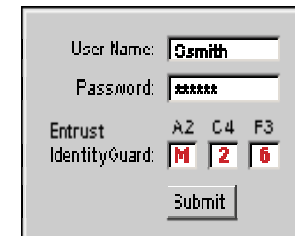
Smart Cards



Keypad Scrambler



Crypto Cookie



Code Cards

Process Procedures in Security Beyond Passwords

... and more

SwivelPIN™ (stays the same) **2 4 6 8**

New Security String™
1 2 3 4 5 6 7 8 9 0 **8107432956**

New One-Time-Code **1 7 3 9**

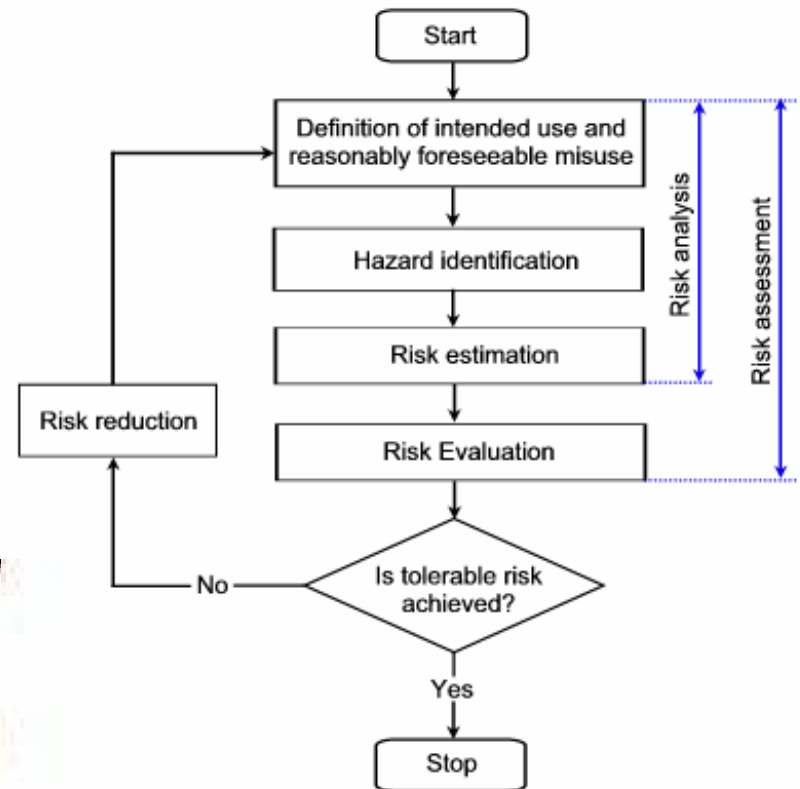
One-Time PIN



Code Wheel



Out-of-Band



**Risk assessment /
fraud detection**

Visibility vs. Unobtrusiveness

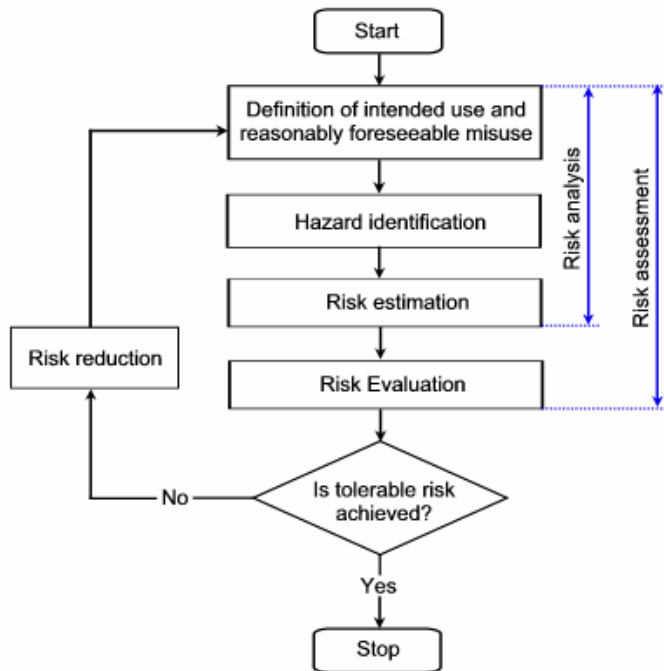
- Cookies **can't** be seen
- Risk assessment and fraud detection **can't** be seen



- But you can't reject users
 - if they fail by 1%
 - or if cookie is missing
- So what then?
 - mother's maiden name?
 - favorite restaurant?

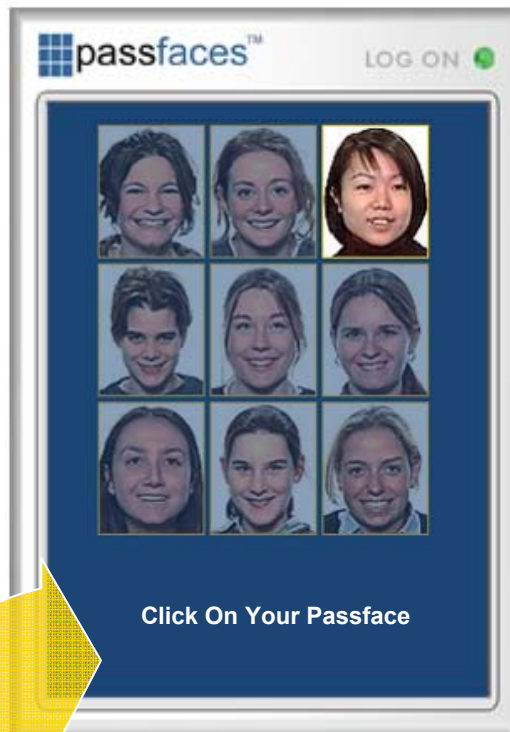
- **Inevitable obtrusion**

- Site-to-user authentication **must** be seen



- Will users notice if image is not there?
 - “the emperor’s new security indicators” (MIT/Harvard)
- Does it matter?
 - “users are reassured anyway” (RSA)

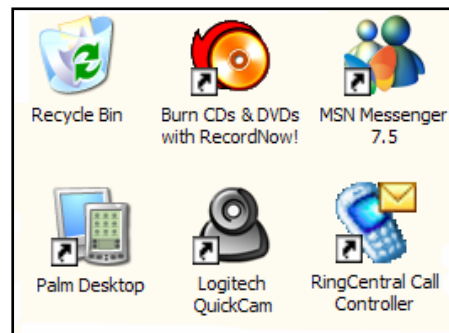
Passfaces Simply Put



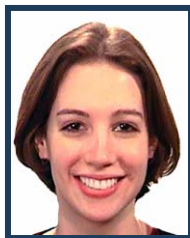
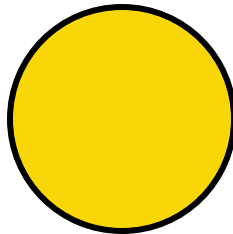
- Passfaces are used as an **enhancement**, or as a **replacement** for, passwords
- When used with passwords, users are typically assigned 3 “secret” passfaces
- To log on, users pick out one of their passfaces from a “challenge” grid of 9 faces
- Each challenge grid contains 1 passface and 8 “decoy” faces
- The process is repeated for each of the passfaces
- The **site is authenticated** because it presents the correct faces to the user
- The **user is authenticated** because they identify their passfaces
- Site authentication **does not rely on users paying attention!**

Patented Cognometric Technology

Graphics and images are among the simplest and most effective means to communicate and interact with people



But, like a password, you still need to *recall* a graphic or image

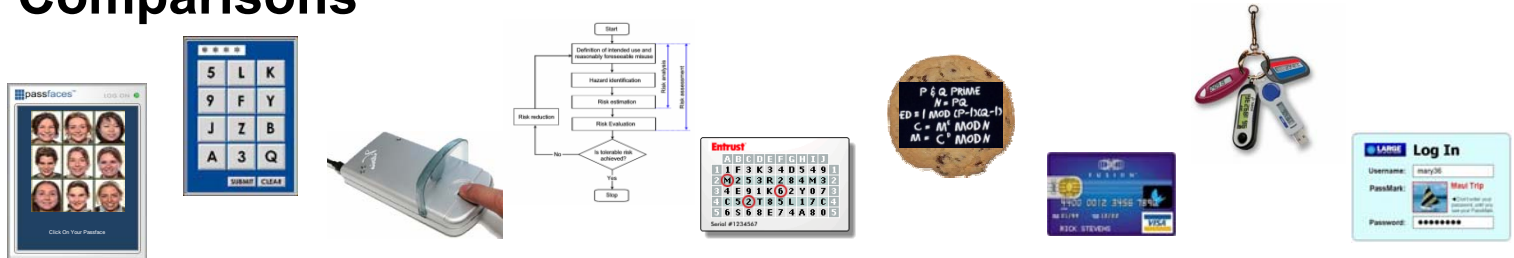


Faces are Different

- The brain uses a dedicated process to “learn” and remember faces.
- The brain *recognizes*, not recalls, faces.
- This most powerful form of memory is unique to human faces and does not apply to other images.
- Face recognition is a universal skill – independent of age, language or education.

Process Procedures in Security Beyond Passwords

Technology Comparisons

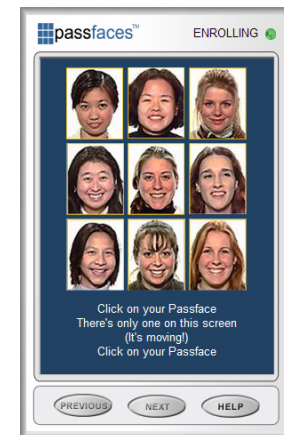


	Passfaces	Virtual Keypad	Biometrics	Risk Analysis	Code Cards	Crypto Cookies	Smart Cards	Tokens	Personal Pictures
Higher Security	Green	Green	Green	Green	Green	Green	Green	Green	Red
Bidirectional	Green	Yellow	Red	Red	Red	Red	Green	Yellow	Yellow
Intrusiveness	Yellow	Red	Red	Green	Red	Green	Red	Red	Green
Visibility	Green	Green	Green	Red	Green	Red	Green	Green	Green
Usability	Green	Green	Green	Green	Red	Green	Red	Red	Green
Mobility	Green	Green	Red	Red	Green	Red	Red	Green	Green
Management	Green	Yellow	Yellow	Yellow	Red	Green	Yellow	Red	Green
Integration	Green	Green	Green	Green	Green	Green	Green	Green	Green
Rollout	Green	Yellow	Red	Green	Yellow	Green	Yellow	Red	Green
Cost	Green	Green	Green	Green	Green	Green	Red	Red	Green

Passfaces Products



Integrates Passfaces with web access applications. Features a Software Developers Kit (SDK) with a server-side Java Class Package, Passfaces Library (database of faces), and “zero-footprint”, browser-based client (java, ActiveX and javascript).

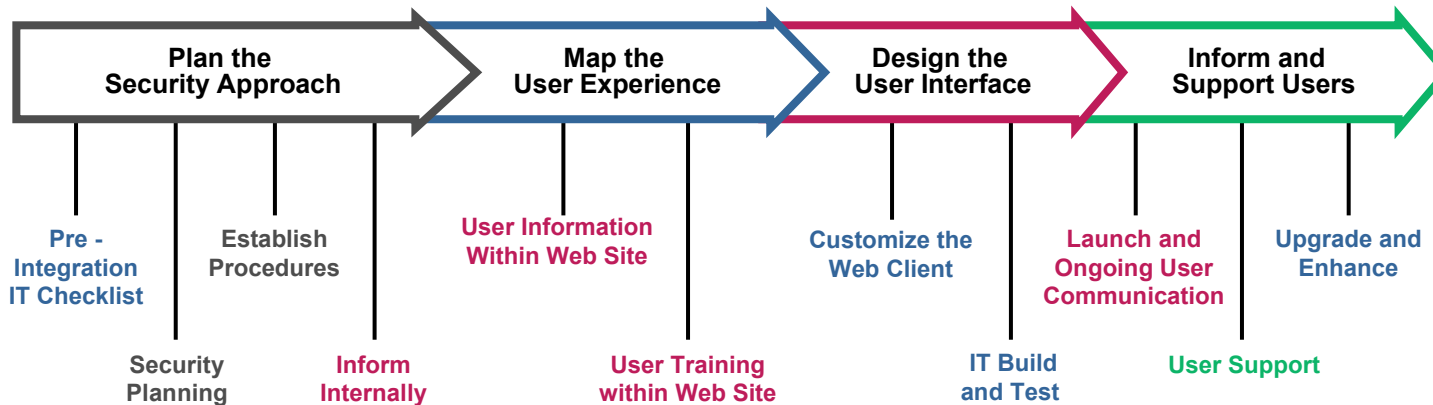


Out-of-the-box bidirectional authentication for Windows networks, Microsoft® IIS based intranets, extranets and enterprise Web Services



Process Procedures in Security Beyond Passwords

Users are Key to Successful Authentication Deployment



*You must Communicate, Educate and **Motivate** them*

Nation's Money Announces Improved Security

Nation's Money is adding Passfaces, an enhanced logon procedure, to our online services. The new process places an additional security lock to existing Online IDs and passwords. We are taking this step to provide the best protection possible for your online account information.



Action
Click on your passface to logon

Users are required to enable Passfaces over the next thirty days. You will be prompted to enable Passfaces each time you login. We recommend you enhance your login security as soon as possible. The process takes from 3 to 5 minutes. We also recommend you [View the Demo](#) before starting the process.

Stronger Authentication to Protect Your Information

The Nation's Money is changing the way you log into your account to better protect your information and prevent others from attempting to access your account. We are making these changes because security is of the utmost importance to Nation's Money. Federal regulations require that all financial institutions strengthen security by the end of 2006.

Just 4 Easy Steps to Stronger Security

- 1 Review** - Review the demo to learn how Passfaces sign up and log on works. Pick a convenient time to sign up and allow 5 to 10 minutes.
- 2 Sign Up** - Once you complete sign up information, your Passfaces are assigned. Go through the familiarization process and follow all steps to assure effective results.
- 3 Log In** - Once you have completed the sign up process, log on using Passfaces.
- 4 Return to the Site** - Reinforce your recollection of Passfaces by returning to the site within a week of signing up.



Welcome to the Passfaces Sign-up and Logon Demonstration.

Click on "Next" Below to Begin and Advance through the Demonstration.

<< Back Next >>

Introduction

Leave the Demo

MBA Panel on Process Procedures in Security

– 27th March 2007 –

Thank You!

Paul Barrett

Passfaces Corporation

paul.barrett@passfaces.com

+1 202 580 8582