Real User

Personal Authentication

July 2003

Real User
Personal Authentication

Limitation of PKI

PK Crypto not good for online user authentication

“All the mathematics of cryptography cannot bridge the gap between me and my computer."

Bruce Schneier

The Need for Cognometrics

"The power of knowledge-based [*cognometric*] authentication is that it verifies a live human presence. This is distinct from a biometric approach (*something you are*) where physical characteristics cannot be changed or chosen, and is distinct from a stored-key approach (*something you have*) which can only verify the presence of a machine or device."

"If you're only using one factor, knowledge works. And when using stored-key or biometric systems, knowledge is still needed."

David Jablon

The Problem: Passwords

- **User authentication is fundamental to online security and access**

"Security is a challenge because the weakest link is always your problem. Today people use passwords to log in and people use passwords that are easy to guess. They write them down. So it's not sustainable…" *Bill Gates, Microsoft, May 17, 2002.*

- **Passwords are used for over 99% of online authentication today**

"Passwords are the oldest authentication method and, despite many vulnerabilities and overheads, are ubiquitous in IT." *Gartner, March 7, 2002.*

- **Current alternatives are not practical (scalable, manageable, reliable, useable, cost-effective)**

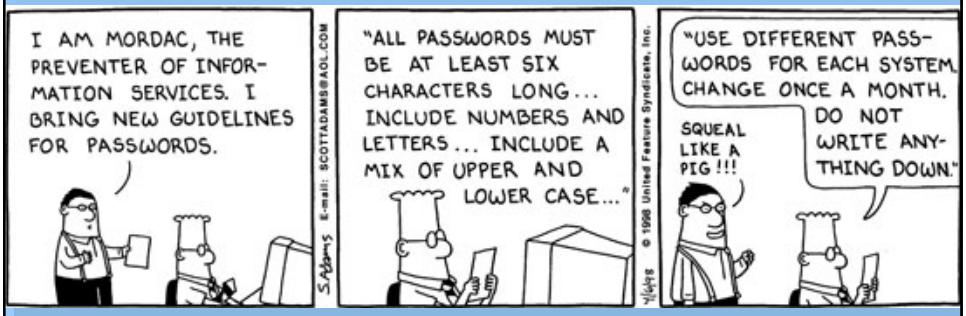
"Many technically more complex options (tokens, smart cards, certificates, biometrics) can offer greater security but a greater cost." *Gartner, March 7, 2002.*

- **Some technologies may not live up to their hype**

"Replace passwords with biometric technologies only when the chief goal is convenience and when security may be safely sacrificed." *Giga, June 24, 2002.*

Simple Solution?

"Giga believes most transactions require only a strong password that is not shared, written down or guessed." *Giga, June 24, 2002.*



"Passfaces™ provide a strong password that cannot be shared, written down or guessed – and users never forget them." *Real User Jun 25, 2002.*

Passfaces™ - easy as 1-2-3

- **Everyone can remember and recognize faces**
  - part of human brain dedicated to purpose
  - only 1 in 8 million have difficulty (prosopagnosia)

- **Your user secret is a set of (system-assigned) faces**

- **To enroll:** spend 3 to 5 minutes "familiarization" with your ***passfaces***

- **To authenticate yourself:**
  - pick each ***passface*** from N groups of 9 faces

Visit www.realuser.com ***to try it yourself***

Security and Privacy Benefits

Passfaces™ provide a authentication secret that cannot be shared, written down or guessed ….
… and users never forget them.

Passfaces™ overcome all(?) the security & privacy vulnerabilities associated with passwords:

- Providing predictable entropy
- Eliminating written-down passwords
- Inhibiting password sharing
- Preventing inadvertent password disclosure
- Cutting "social engineering" risks
- Reducing fallback to personal information Q&A
- By-passing key-stroke loggers
- Making current password cracking tools obsolete

System Benefits

- Thin network transaction
  - <200K bytes at enrollment
  - similar to password at logon time
  - easily supportable over low bandwidth connections
- Minimal additional processing required
  - authentication step is no more complicated than checking a password
  - several million users on a single low end server
- Minimal storage requirements
  - less than 100 bytes per user
- No additional system or user hardware
  - enables easy and cost effective scaling

Authentication Alternatives

Benefits/ Implications	Security	Privacy	Reliability	Usability	Cost - OOM	Easy Integration	Manageability
Passfaces	✓	✓	✓	✓	$5	✓	✓
Personal Info. Q&A	X	X	?	?	?	?	X
"Strong" Passwords	?	?	X	X	$50+	✓	X
Tokens	✓	✓	?	?	$50+	✓	X
Certificates (software)	?	?	?	X	$50+	X	X
Smartcards with PKI	✓	✓	?	✓	$50+	X	X
Biometrics	X	X	X	✓	$50+	X	X

Implementation Options

Passfaces™ can be implemented as a:

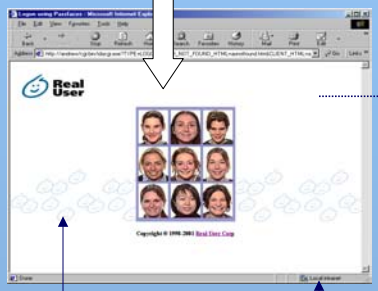
- Single/primary factor
- Second factor
- Part of a two-factor anonymous authentication scheme

And can be incorporated into any other password authentication protocol or scheme such as: Kerberos, SPEKE etc.

Single Factor

Passfaces Client:
ActiveX component
OR
Java applet

Toolkit CGI
OR
your server
application



Any
Network

Your
Web
Server

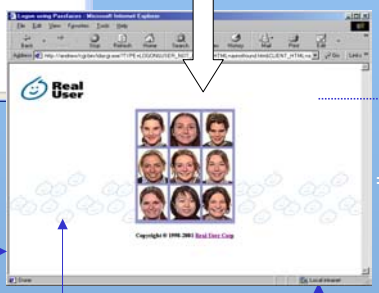
Example HTML
page from toolkit
OR your web page

User's Web Browser

Second Factor

Passfaces Client:
ActiveX component
OR
Java applet

Toolkit CGI
OR
your server
application



Any
Network

Password as
One Factor
+
Passfaces as
Second Factor

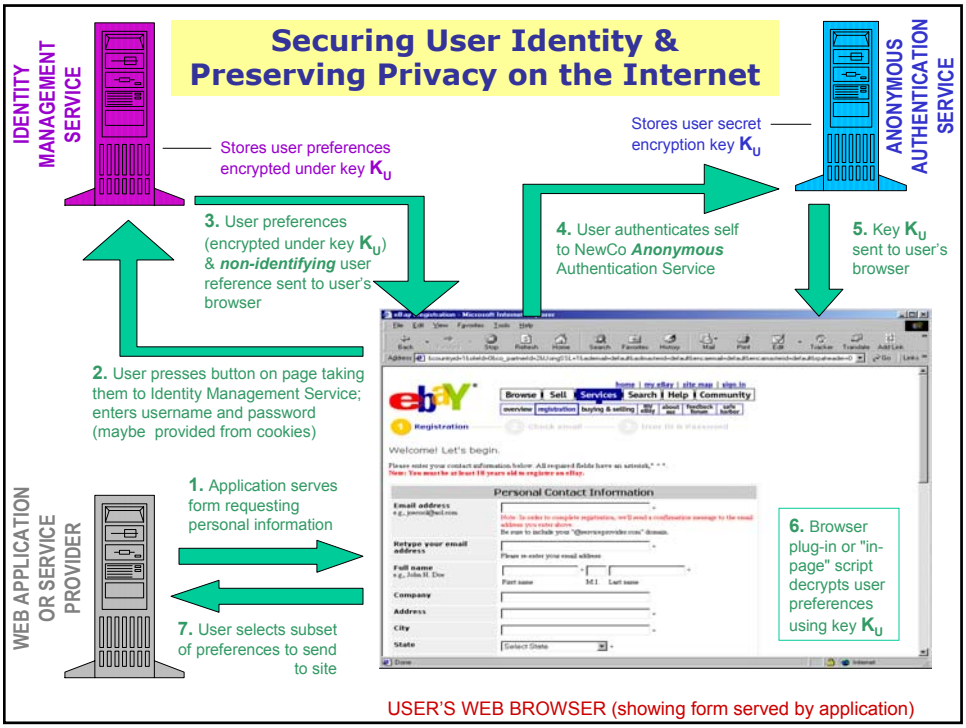
=

Composite
Passcode

Your Web
Server

Example HTML page
from toolkit OR your
web page

User's Web Browser



Real User
Personal Authentication

Passfaces: A New Paradigm

Passfaces™ can replace or augment passwords wherever there is a GUI.

The human brain's remarkable face recognition skill makes Passfaces – the ultimate cognometric

Passfaces™ intuitive usability and near 100% reliability make them a natural successor to the password and PIN for most applications.

Think: Passwords = command line (DOS)
Passfaces = GUI (Windows)

Products

Real User's enterprise security products provide a "strong" user authentication solution that can be deployed enterprise-wide, quickly and easily (often "out-of-the-box") – at an order-of-magnitude lower cost than any alternatives.

- ***Passfaces™ for Windows*** – an out-of-the-box solution to password security issues on Microsoft® networks. Installs in minutes and operates seamlessly with .NET/2000/NT4 servers and XP Pro/2000/NT4/98/95 clients.

- ***Passface™ Software Developers Program*** – provides the tools and support to enable OEMs, systems integrators and service providers to deploy Passfaces™ cognometric authentication in enterprise networks & applications.

For the Web – our technology is the only scalable password alternative that can ensure the security and privacy of all e-commerce, e-government and identity management applications.

Think … Out of the Box

Passfaces™ for Windows can be deployed network-wide in minutes:

1. Install administration application on server
2. Install on clients (from server or locally)
3. Set user security parameters
4. Initiate user 3 – 5 minute self-training

Strong authentication deployment complete

Passfaces™ for Windows:

the first out-of-the-box security solution since the introduction of anti-virus software

Passface™ Software Developers Program

- **Program includes**
  - A comprehensive range of Passface™ Software Developers Tools (SDKs)
  - An evaluation license allowing trials for (up to) 100 users
  - Access to the Passface™ software developer library
  - Expert support and consultancy from the Real User technology team
- **Passface™ Software Developers Toolkits (SDKs)**

  Contain Passface™ client software components, server integration code examples and full documentation.
  - **Passfaces™ for In/Extranets SDK**
  - **Passfaces™ for Windows Networks SDK**
  - **Passfaces™ Win32 Client SDK**
  - **Passfaces™ Windows CE Client SDK**
  - **Passfaces™ Palm SDK***
  - **Passfaces™ Authentication Server SDK***

Real User

Personal Authentication

Thank You !!