Real User
Personal Authentication

TECHNOLOGY AND PRODUCTS

In the online world, the reliance on passwords – the weakest link in IT security – as the primary means of personal authentication and the absence of a reliable and cost-effective "second-factor" authenticator, not only leaves systems vulnerable to potentially crippling breaches of security, but also costs business, government and consumers, billions of dollars annually in fraud, support costs and productivity losses.

Real User Corporation has developed a new class of authentication technology – *cognometrics* – that enables simple, reliable, and secure on-line personal authentication for everyone, everywhere. Our *Passface™ Enterprise Secure* products provide businesses and government agencies with a practical and instantly scalable means to reinforce or replace passwords; and, for the World Wide Web, we are developing an *anonymous authentication* solution that will help ensure the security and privacy of all e-commerce, e-government and identity management applications.

PERSONAL AUTHENTICATION: THE CHALLENGE

Personal authentication is a fundamental requirement for most human interaction. In the real world, individuals can recognize each other's faces or voices when they meet or communicate by phone; they can authenticate themselves to banks or retailers with a card and a signature; and they can use badges, IDs and other documents or credentials to gain access to restricted locations. Online, in the absence of any practical alternative, we are forced to rely almost exclusively on passwords – with all their well-documented shortcomings – as the basic means of personal authentication. As a consequence, enterprises everywhere (including businesses, government agencies and other organizations) are facing a number of serious challenges:

- ***System Insecurity*** **–** Passwords are widely acknowledged as being the weakest link in the cyber-security chain: they are written down, shared and exposed on multiple systems by users and they can be guessed or "socially engineered" by hackers.
- ***Poor Usability and Reliability*** – Faced with an increasing number of business systems and applications requiring passwords, users typically adopt one or more of three basic strategies to avoid forgetting them: they write them down, they choose them to be easy to remember and they make them all the same. Despite this, forgotten passwords remain the number one cause of help-desk calls.
- ***Management Costs*** – The Gartner Group reports that password management is one of the most labor-intensive and risk-prone IT functions, and costs enterprises up to $300 per user each year. This estimate excludes productivity losses due to failed access by legitimate users.

And on the Web, in addition to the above issues, users and service providers must contend with:

- ***Credit Card Fraud*** – According to Visa International, the level of credit card fraud online is 19 times higher than in the real world and, in the absence of any practical means of verifying card ownership, the total losses from fraud are forecast to exceed $10 billion in 2005.
- ***Loss of Privacy and Identity Theft*** – The Federal Trade Commission has declared identity theft as the fastest growing crime today with an estimated 700,000 victims in 2002. Increasingly, users' personal information (e.g. address, bank details, mother's maiden name and social security number) is being used as a means of identity verification; this not only engenders an implicit loss of privacy, but also raises the likelihood of fraud and identity theft by both exposing the data and providing the opportunity to (ab)use it.

These problems are compounded by the exponential increase in interactions and transactions enabled online. Moreover, they are undermining trust in the Internet and preventing enterprises and users from enjoying the full benefits of their technology investments. And the conventional, "hard technology" approach to solving these problems (using smartcards, cryptography, biometrics, etc.) shows no indication of delivering a solution that is either affordable or practicable for any but a small minority of on-line system users.

REAL USER'S COGNOMETRIC SOLUTION

Real User's Passface™ system is a ***cognometric*** method of personal authentication - based on the measurement of an innate cognitive function (of the human brain), specifically: its ability to recognize familiar faces. As with passwords and PINs (knowledge-factor authenticators), with Passfaces™ there is a shared secret between the user and the system. However, instead of relying on users to memorize and recall strings of characters and/or numbers, it employs [photographs of] faces as its "alphabet" and requires only familiarization and recognition on the part of the user. The system works as follows:

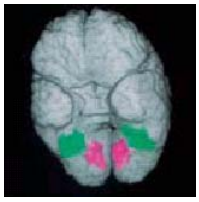
- Users start by getting to know a group of (typically 3 to 7) faces – their *passfaces* – which are assigned by the system at random from a large library of anonymous faces. This simple and intuitive initial *familiarization* process takes around 3 to 5 minutes for 5 passfaces.

- To authenticate a user, the system displays a 3 by 3 grid of faces containing one passface and 8 *decoy* faces positioned randomly within the grid.

- The user responds by indicating the position of their passface in the grid. This challenge/ response is repeated with each of the user's remaining passfaces – each time presented in a grid with 8 more decoy faces.
- The user is authenticated once all their passfaces have been recognized successfully.

THE PASSFACE™ SYSTEM - WHY IT WORKS

The Passface™ system is based on the human brain's remarkable ability to recognize individual faces*. This underlying principle is supported by extensive academic research and cognitive psychology experiments. Real User's own long-term trial with Passfaces™ at our Web site has operated successfully for over 15,000 users – some of these returning after two years of non-use and being able to immediately recognize their passfaces.



* Part of the brain (shown here in green) has evolved specifically for the purpose of face recognition and this instinctive ability is completely universal: only one in eight million (sighted) people – suffering from a condition known as prosopagnosia – experience any difficulty in recognizing familiar faces.

For further information on this subject and on the development of the Passface™ system, see our White Paper: "**The Science Behind Passfaces**"

PASSFACE™ SYSTEM BENEFITS

Real User's Passface™ personal authentication solution combines a comprehensive set of features and benefits that in other systems are typically mutually exclusive:

- **Security** – Passfaces provide a consistent, high-level of security for all users. Passfaces are randomly assigned to users by the system – so cannot be guessed by an attacker; and user compliance with security policies is assured, since passfaces cannot be written down, disclosed verbally or used for unauthorized applications.
- **Reliability** – Passfaces are "unforgettable" and can't be lost or left at home; and there is no additional hardware to break down or complex software to maintain.
- **Usability** – The Passface™ system is completely intuitive to use and works for everyone – independent of language, culture, age or education.
- **Scalability** – Passface™ solutions require no additional hardware and can be deployed very rapidly across any size network.
- **Flexibility** – Passface™ systems provide administrators with full flexibility to implement and manage their security policies.
- **Affordability –** Real User's Passface™ personal authentication products are very attractively priced and total cost of ownership is typically an order of magnitude below any alternative solution.

Forget P*55w*RDs!?

USE PASSFACES™

Try Passfaces™ for yourself at
www.realuser.com/demo

PASSFACE™ PRODUCTS

Real User's comprehensive range of products enable rapid deployment of Passfaces™ in enterprise networks – either as an "unforgettable" replacement for passwords and PINs or as an order-of-magnitude lower cost alternative to smart-cards and tokens for second-factor authentication:

- **Passfaces™ for Windows – Enterprise** – An out-of-the-box strong authentication solution for all Microsoft® Windows network environments and applications, including local and remote desktop logon, network resource access, IIS basic authentication, RAS, terminal services and Web services.
- **Passfaces™ for Windows Web Services** – An out-of-the-box strong authentication solution for Microsoft® Internet Information Server (IIS) based intranets, extranets, SSL-VPNs and enterprise Web Services (e.g. Outlook Web Access).
- **Passface™ Web Toolkit –** A set of software tools to enable OEMs, systems integrators and service providers to integrate Passface™ strong authentication into any enterprise intranet, extranet, Web service or identity management system.
- **Passface™ Win32 Toolkit** – A set of software tools to enable OEMs and systems integrators to integrate Passface™ strong authentication into Windows client-based applications.

THE REAL USER SOLUTION FOR THE WEB

Real User is working with its partners to provide an essential component of infrastructure for the World Wide Web. **The Real User Anonymous Authentication Service** will enable all Web users everywhere to simply, reliably and securely authenticate themselves anonymously – that is without [the Real User Service] ever requiring or storing any of the users' personal information. The Real User Service will provide an added level of security and privacy protection to all third-party services and applications on the Web that require authentication of their users, including:

- ***E-commerce*** – for "card-holder present" transactions;
- ***Identity management*** – providing enhanced privacy and security to services such as Microsoft® Passport and Liberty Alliance;
- ***Access control*** – to member and subscription services;
- ***E-Government*** – to provide a practical means of securing access on government to citizen applications.

For more information on Real User's unique Passface™ cognometric authentication solutions and to try the system as a user visit our Web site at **www.realuser.com**.

Real User Corporation

Headquarters
175, Admiral Cochrane Drive
Annapolis, MD 21401 USA
Tel: +1 410 224 4848

Email: **info@realuser.com**