

Passlogy Co., Ltd. PatternPass 1000



Test Summary

Evaluation of Token-less PASSLOGIC One-time Password Authentication System

Premise: In today's networks, the challenge of implementing a secure one-time password authentication system that is flexible and easy-to-use, could be made more user-friendly and less complex. IT security administrators need to consider the trade-offs between simplicity, security, maintenance and cost of operation when evaluating various one-time password authentication mechanisms.

Passlogy Co., Ltd. commissioned The Tolly Group to evaluate the PASSLOGIC token-less one-time password (OTP) authentication system running on its PatternPass 1000 appliance. The PASSLOGIC technology implemented a patented 2-way, 2-factor, one-time password authentication mechanism that does not require a dedicated hardware token.

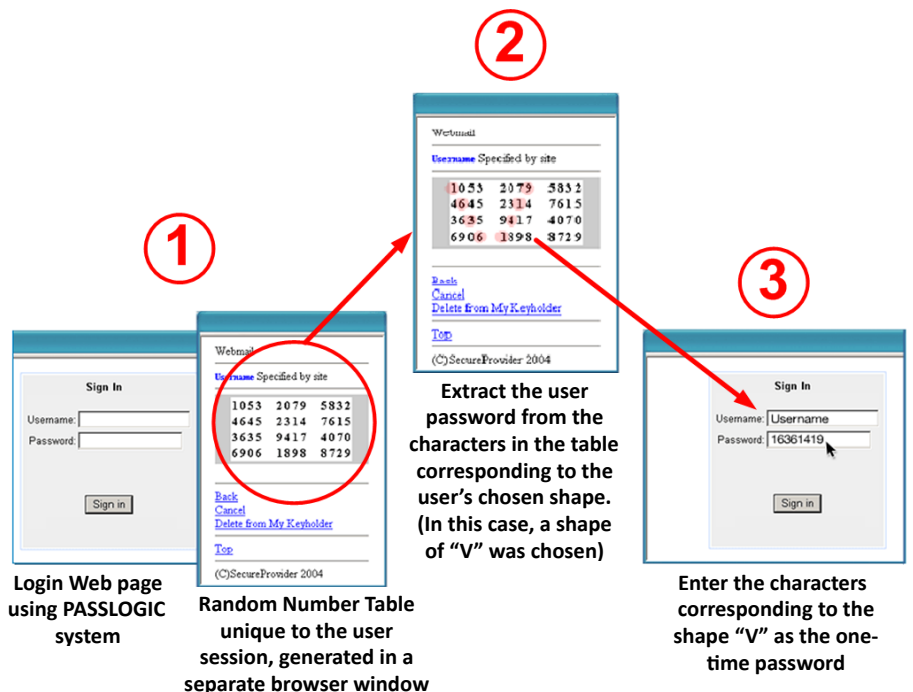
Tests focused on the ability of Passlogy's PatternPass 1000 appliance and PASSLOGIC system to resist security events such as brute-force attacks or random account locking attacks. Engineers also tested the compatibility of the PASSLOGIC system to work in an SSL VPN scenario, as well as using multiple portable devices like portable game devices, PDAs, mobile phones, etc. to generate the one-time password.

Tests were conducted in October 2008.

Test Highlights

- ▶ Resists brute-force and account lock attacks under normal operating conditions
- ▶ Compatible with remote access solutions like SSL VPNs
- ▶ Provides a convenient and flexible one-time password authentication using cell phones, portable gaming devices, PDAs, etc. equipped with a Web browser
- ▶ Reduces support costs and administrative burden of maintaining dedicated hardware tokens

PASSLOGIC One-time Password Generation Scheme



Source: The Tolly Group, October 2008

Figure 1

Executive Summary

Passlogy's PASSLOGIC token-less, one-time, password authentication system provides a flexible technology that can be implemented easily, and cost-effectively to provide one-time password generation on any mobile device equipped with a Web browser, to provide a powerful and easy-to-use authentication mechanism.

One-time password authentication systems greatly reduce the risk of unauthorized access to protected resources due to compromised passwords. However, higher security often comes with higher cost, and increases the system administrator's work. Passlogy's PatternPass 1000 appliance implementing PASSLOGIC seeks to address such issues.

Passlogy's PASSLOGIC token-less one-time password authentication mechanism provides users with a URL to access a Web page displaying a matrix consisting of randomly generated numbers or characters; out of which, the users extract a unique one-time password comprising of numbers or characters. The password is extracted by selecting the numbers from positions in the matrix that form a shape of the user's choosing. (See Figure 1.) The authentication procedure follows a challenge and response model as illustrated in Figure 2.

Tests showed that PASSLOGIC technology provided ways to guard successfully against password compromising attacks using brute-force techniques or random account locking attempts. Engineers note

that such attacks are highly unlikely to succeed unless the attacker possesses very intimate knowledge of the working of the PASSLOGIC technology, along with other conditions like a compromised user login and the associated user-specific URL required to access the random number table containing the user's one-time password.

Tests also showed that the PASSLOGIC system can be integrated into a remote access scenarios like using SSL VPNs to connect to a remote office over the Internet.

Engineers also verified that the PASSLOGIC system could be made to work with any devices equipped with a Web browser and connected to the Internet to download the random number table containing the one-time password for the user for that session. This is particularly useful when the user is mobile, by being able to use portable devices like PDAs, smartphones (like the Apple iPhone), portable

gaming devices (like the Sony PSP), etc. to access one-time password(s) for any compatible services using PASSLOGIC technology for authentication.

Tolly Group engineers also tested the performance of the PatternPass 1000 appliance while handling a high volume of transactions trying to fetch the random number tables containing the one-time password for the users. The PatternPass 1000 appliance was able to serve up to an average of 54 transactions per second over a 100-Mbps Fast Ethernet connection.

In conclusion, PASSLOGIC technology for token-less OTP authentication provides a secure, flexible and easy-to-use authentication system that can augment almost any existing authentication mechanism.

TEST RESULTS & METHODOLOGY

The Tolly Group engineers tested a Passlogy PatternPass 1000 appliance running a Passlogy Software Suite. The PatternPass 1000 appli-

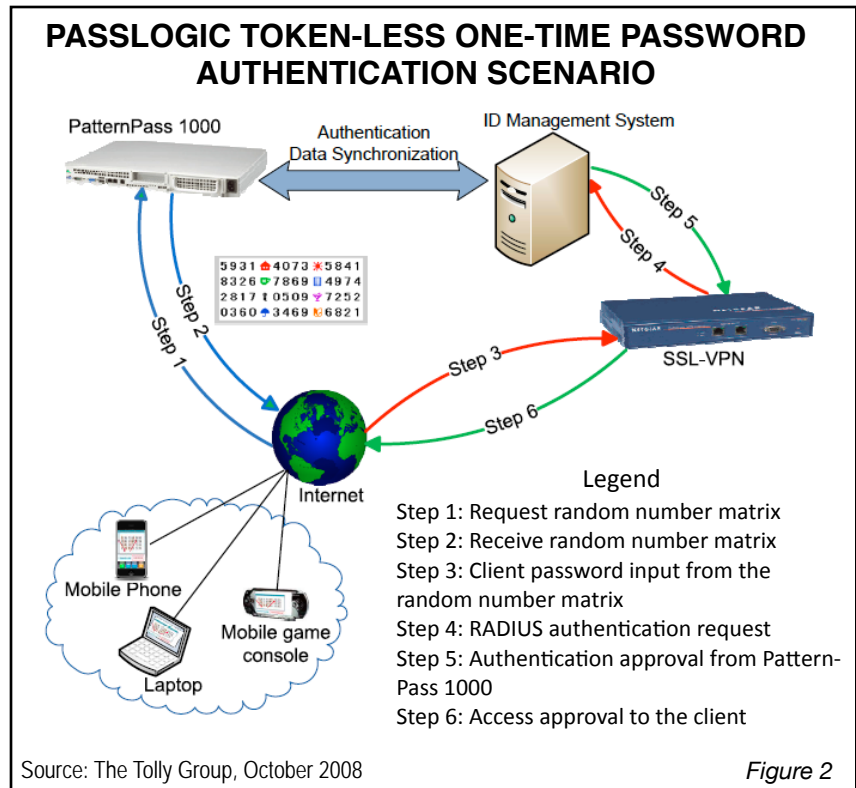


Figure 2

ance was configured with a 2.8-GHz Intel Xeon CPU (800-MHz FSB, 2MB Level 2 cache), 1 GB DDR2 RAM, two 36 GB HDD in RAID1, running Red Hat Enterprise Linux 3 ES - Kernel version 2.6.9-67.0.15.EL. The Passlogy Software Suite used Passlogy-Core-V2.1.1, Administrative software version 1.0.4.1, and Authentic Software Version Passlogic - FA (1.0.0.0) release date 07/06/2007.

BRUTE FORCE ATTACK TEST

Engineers tested the PatternPass 1000 appliance with PASSLOGIC software by launching brute-force attacks against it with three hacking tools: EAT Brutus, Hydra, and WFUZZ. Each tool tried a large number of numeric passwords in succession within a very short time. None of the tools were successful in cracking the password via brute force. Engineers loaded a file with multiple usernames and a file with multiple passwords; each file containing at least 10 MB of data. After each attack, the log from the program was checked to see

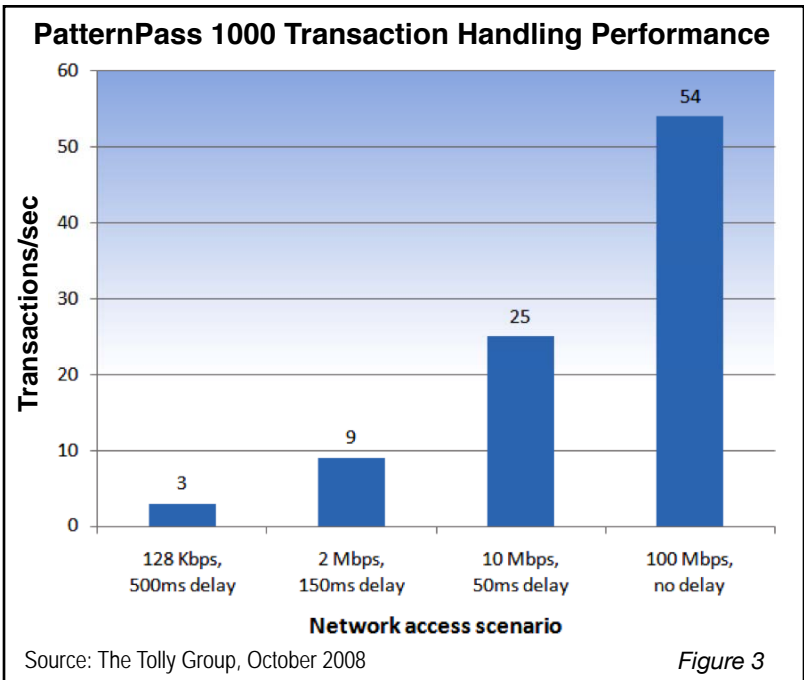
if any attack was successful - and no attacks were successful. Also, Wireshark traffic captures during the attack confirmed that all of the requests were rejected.

RANDOM ACCOUNT LOCK ATTACK TEST

Engineers tried to lock an account by typing the wrong password multiple times, to check if the account would get locked. Tolly engineers were unable to lock the user account without running a custom script that accessed the user-specific URL to generate the random number matrix, and then ran a subsequent attack script to enter multiple invalid passwords to lock the user account.

Unless the random number matrix was requested by the user, the one-time password would never be created, and hence the user account could not be locked by entering invalid passwords.

Engineers note that unless the attacker possessed detailed knowledge of the PASSLOGIC authentication technology, and gained possession of the user-specific URL required to generate the random number matrix



Passlogy Co., Ltd.



PatternPass 1000 with PASSLOGIC

Token-less, One-time Password Authentication System

Product Specifications

Vendor-supplied information not necessarily verified by The Tolly Group

Passlogy Co., Ltd. PASSLOGIC

Benefits:

- Strong authentication:** PASSLOGIC's patented 2-way 2-factor one-time password system uses the "Challenge-Response" method, which is the strongest authentication combination available within OTP systems, and prevents both account lock and brute force attacks, which are normally not preventable with hard tokens or regular passwords
- Cost-efficient, lean administration:** Only a Web browser is needed. No token management costs involved, and the administrator can set various factors given that tighten or loosen. Thus it is acclaimed by organizations with high-user volume, global enterprises with users dispersed world wide, air or land transportation firms with frequent travelers, or educational institutions with high turnovers.
- Proven track record:** PASSLOGIC is one of the leading authentication systems in Japan and has over 400,000 licensed users, including leading financial institutions

Features:

- Desirable usage:** Strengthened password with ID management systems such as Single Sign-On, and Remote access via Remote Desktop and SSL VPN, etc.
- Tried and true compatible devices/software:** HP IceWall SSO, Sun Java System Access Manager, Windows Server 2003, Citrix XenApp, Juniper SA, F5 FirePass, etc.
- Compatible protocol:** ID Management (Active Directory, LDAP, SQL) Authentication: (RADIUS, HTTP/XML, Reverse Proxy), Thin client (RDP, ICA)

Passlogy Co., Ltd.

US Contact:
 575 Lexington Ave #400
 New York, NY 10022
 Phone (212) 527-7540 Fax: (212) 504-8192
 Email: info@PatternPass.com
 URL: www.PatternPass.com

containing the user's one-time password for that session, it would be highly unlikely for the attacker to generate an attack that could lock the user account by entering invalid passwords.

PORTABLE DEVICE USAGE SCENARIOS

Engineers used a Web browser on an Apple iPhone smart phone and a Sony PlayStation Portable (PSP) to access the user-specific URL to generate the random number matrix to extract the user's one-time password. This proved that any device equipped with a Web browser connected to the Internet could be used to generate a new one-time password with the PASSLOGIC system.

TRANSACTION RATE PERFORMANCE TEST

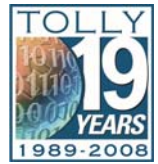
Engineers tested the capability of the PatternPass 1000 appliance and the PASSLOGIC software to serve a high volume of user requests to generate their unique random number matrices con-

taining their unique one-time password for that session.

Engineers launched a custom script that launched a set of 10,000 requests to generate the random number matrices. The script launched dynamically increasing number of threads simultaneously to generate the 10,000 total requests, and reported the number of successful transactions per second that generated a unique random number table.

Tests were done on various simulated network links using the Anue GEM Ethernet Advanced Network Emulator: 100 Mbps with no delay, 10 Mbps with 50ms delay, 2 Mbps with 150ms delay and 128 Kbps with 500ms delay. Each test was repeated three times and the results averaged to ensure repeatability of results. Results showed that the PatternPass 1000 appliance averaged up to 54 transactions per second (see Figure 3). Passlogy estimates the PatternPass 1000 appliance would serve up to 90,000 customers assuming each user accesses the system once per hour, and assuming a one-second response time.

The Tolly Group is a leading global provider of third-party validation services for vendors of IT products, components and services. The company is based in Boca Raton, FL and can be reached by phone at (561) 391-5610, or via the Internet at:



Web: <http://www.tolly.com>,
E-mail: sales@tolly.com

Test Equipment Summary		
Vendor	Product	Web URL:
Anue Systems, Inc.	GEM Ethernet Advanced Network Emulator	http://www.anuesystems.com

Terms of Usage

USE THIS DOCUMENT ONLY IF YOU AGREE TO THE TERMS LISTED HEREIN.

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase must be based on your own assessment of suitability.

This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental and consequential damages which may result from the use of information contained in this document.

The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers.

When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from The Tolly Group's Web site. All trademarks are the property of their respective owners.

208290-qjtupo1-cdb-20JAN09verg