

Automatic Speaker Verification (ASV) System Can Slash Helpdesk Costs

Table of Contents

<i>Executive Summary</i>	1
<i>Business Challenge</i>	1
<i>SentryCom Enterprise Voice Authentication Platform*</i>	2
<i>Technologies</i>	2
<i>Summary</i>	4
<i>Definitions and Acronyms</i>	4
<i>For More Information</i>	4
<i>References</i>	4

Executive Summary

In most enterprises, computer users must call the helpdesk every time they need to reset their domain access passwords—something users do so often, it can end up costing a company with 10,000 computer users more than \$1.5 million per year in helpdesk services.

Automatic speaker verification (ASV) technology from Israeli company SentryCom Ltd.—based on open, standards-based, modular platforms from Intel—allows users to change their own domain passwords without compromising security, enabling enterprises to dedicate their expensive helpdesk resources to more important tasks. The system can also be used to record time/attendance for the extended enterprise (for example, for mobile or remote employees working away from the office) and for secure corporate portal access from any PC using any wireless or wireline telephone.

Business Challenge

When an enterprise employee calls the helpdesk for a simple domain access password reset, a helpdesk employee normally has the caller answer a predetermined security question such as “What is your mother’s maiden name?” to verify the employee’s identity. This process is inconvenient and time-consuming. It is also basically insecure, since it relies on human accuracy.

Most importantly, having employees call the helpdesk for simple password resets is extraordinarily expensive. META Group estimates that an average computer user calls the company helpdesk 21 times a year. [Meta] On average, 30% of helpdesk calls are for password resets, with an average cost of \$25 per reset. [ComputerWorld] For a company with 10,000 users, that adds up to \$1,575,000 per year just for password resets.



SentryCom Ltd. is a General Member of the Intel® Communications Alliance: a community of communications and embedded developers and solution providers.

Replacing this awkward and expensive process with a self-service system is the obvious solution. It would also save the enterprise even more helpdesk time and money if the system could automatically:

- **Log time/attendance for roaming employees** using a phone within the extended enterprise.
- **Enable employees to gain secure Web access** from any PC using a phone within the extended enterprise.
- **Allow employees to use a single sign-on** to access multiple domains using a phone.

But it is challenging to find a system that can let employees perform all these functions quickly and easily and without compromising the enterprise's security or changing its infrastructure.

SentryCom Enterprise Voice Authentication Platform

The solution to these challenges is automatic speaker verification (ASV) technology, which verifies the caller's identity using biometric matching of voiceprints. Biometrics is the automated use of physiological or behavioral characteristics to determine or verify identity. Biometric voice recognition technology uses the distinctive aspects of the voice to verify the identity of individuals. This voice recognition technology differs from speech recognition, a technology that translates what a user is saying (a process unrelated to authentication). ASV technology verifies the identity of the individual who is speaking.

The ASV speaker verification process is fast, convenient, and secure. It does not force the employee to use expensive helpdesk resources for activities such as simple password changes. Also, it does not require the enterprise to change its infrastructure or the employees to change their habits.

SentryCom, based in Haifa, Israel, used ASV technology to develop its Enterprise Voice Authentication Platform* (EVAP*), which uses a simple challenge-response user interface to prevent recorded playback of the person's voice by asking the caller to say quasi-random pairs of letters or digits—for example, "twenty-six, forty-one" or "ninety-three, sixty-four." This helps to eliminate fraudulent access.

Technologies

The voice authentication engine is a key building block of EVAP, which integrates with Web and contact center applications to provide for secure and cost-efficient remote access. It is designed to increase and enhance security while improving end users' privacy and confidence.

In developing EVAP, SentryCom used a patented authentication technology to address the known difficulties of voice authentication, including:

- False rejection rate (FRR)
- False acceptance rate (FAR)
- Noise tolerance
- Voice variability over time
- Immunity to impostor "playback" attacks and mimics
- Speakers with colds or other voice-altering conditions
- Long enrollment sessions

A decision-making algorithm elps to solve the traditional weaknesses of voice authentication systems, reducing error rates (both FAR and FRR) without compromising the system's robustness. The authentication engine uses a text-dependent and language-independent interface as well as real-time, random, digit-pairs prompting to detect a "live" user and to prevent voice playback attack.

Data extracted from the user's voiceprint—which can be captured from PC microphones, telephones, and cellular phones—is passed on to the authentication engine.

As the user speaks, the shape of his or her vocal tract changes. The different shapes that the speaker's vocal tract assumes contribute to voiceprint personalization. When the speaker is prompted to talk, the voice authentication technology extracts the speaker's voiceprint and matches it with claimed Identity. If there is a good fit, then the speaker is accepted into the system and can proceed to use the application to which he or she has requested access.

The system is not affected by nasalization that occurs when the speaker has a cold, or by speakers with speech impediments, as long as the user is able to speak consistently between registration and authentication. It can also identify mimics, who largely

requires a flexible, cost-effective IVR platform. SentryCom choose to develop its IVR platform around the Intel® Dialogic® D/41JCT-LS Combined Media Board.

A four-port system provides sufficient concurrency for most enterprise needs. The four-port, analog D/41JCT-LS Combined Media Board is an ideal choice for developing global, enterprise applications such as IVR, unified messaging, and contact center applications. It supports voice, fax, and software-based speech recognition processing in a single PCI slot, providing four analog telephone interface circuits for direct connection to analog loop start lines. With a variety of international approvals, the D/41JCT-LS board cost effectively expands an application's ability to serve several global market segments. The SentryCom IVR solution is implemented in both English and Hebrew.

The authentication software runs on servers using Intel® processors and the Windows* operating system.

The middleware for the solution is Intel NetMerge® CT Application Development Environment, which helps speed development of IVR applications. This set of program building blocks is specifically designed to deliver the innovative features of Intel® telecommunications technologies in forms that are easier to use and quicker to learn than conventional hardware interfaces. It eliminates the need to learn telephony hardware, application programming interfaces, and protocols. This software reduces the need to write directly to a telephony device's API in C or C++.

Summary

The EVAP solution from SentryCom Ltd., based on open, standards-based, modular platforms from Intel, allows users to change their own domain passwords without compromising security, enabling enterprises to dedicate their expensive helpdesk resources to more important tasks. The system can also be used to record time/attendance for the extended enterprise (for example, for mobile or remote employees working away from the office) and for secure corporate portal access from any PC using any wireless or wireline telephone.

EVAP has been successfully tested for Web access with AnalystOnline, an Israeli financial portal, and with the Israeli Standards Institute—National Biometrics Knowledge Center. It is also in use with a multi-national company based in the UK,

which has successfully tested it for enterprise password reset. The Israeli Ministry of Trade and Commerce—Chief Scientist Office approved the use of the system for time/attendance reporting. It is currently being evaluated by financial institutions in Israel, the U.S., and Denmark.

Definitions and Acronyms

API	Application programming interface
ASV	Automatic speaker verification
CT	Computer telephony
EVAP	Enterprise Voice Authentication Platform
FAR	False acceptance rate
FRR	False rejection rate
IVR	Interactive voice response
PCI	Peripheral Component Interface
SSO	Single sign-on

For More Information

SentryCom Ltd. — <http://www.sentry-com.co.il>

Intel Dialogic D/41JCT-LS Combined Media Board Data Sheet — <http://www.intel.com/network/csp/products/6925web.htm>

Intel NetMerge CT Application Development Environment Data Sheets — <http://www.intel.com/network/csp/products/7445web.htm>

References

[Meta] “The Value of Identity Management: How Securing Identity Management Provides Value to the Enterprise,” Meta Group, 2002.

[ComputerWorld] “Want to Save Some Money? Automate Password Resets,” *ComputerWorld*, July 9, 2001.

FOR MORE INFORMATION

**Please contact your local Intel representative or
visit our websites at: www.intel.com/telecom/go**

This document and related materials and information are provided "as is" with no warranties, express or implied, including but not limited to any implied warranty of merchantability, fitness for a particular purpose, non-infringement of intellectual property rights, or any warranty otherwise arising out of any proposal, specification, or sample. Intel assumes no responsibility for any errors contained in this document and has no liabilities or obligations for any damages arising from or in connection with the use of this document.

This whitepaper is for informational purposes only, and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

Intel, Intel NetMerge, Pentium, Intel Centrino, the Intel logo are trademarks or registered trademarks of Intel Corporation and its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2004 Intel Corporation. All rights reserved.

00-9175-001 09/04