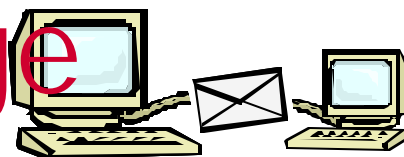




The Open Group EMA Forum

The Message



Volume 2 Issue 1

January 2002

Inside Look at Integrated Information Infrastructure (In3)-2002

Offering business value to CIOs who face constantly changing business needs and ever tightening budgets is the week-long winter quarterly conference of The Open Group in Anaheim, CA.

From 9 a.m., Monday, 21 January through noon, Friday, 25 January 2002, opportunities abound for learning from key visionaries in the open systems, standards, and certification world.

Speakers the first day will focus on the vision of the Integrated Information Enterprise and on understanding the need and facilitating the solution. Hear from the following leaders:

- Dawn Meyerriecks, CTO Defense Information Systems Agency
- John Tritak, Director, Critical Infrastructure Assurance Office
- Ronald J. Dorman, Princi-

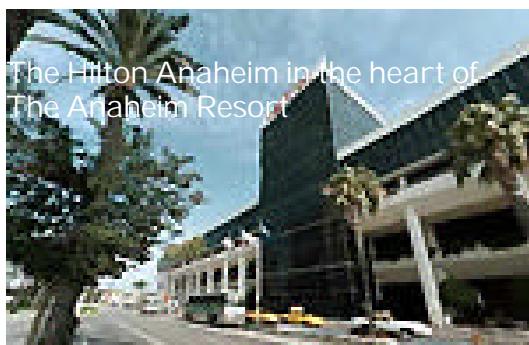
pal Director Interoperability, Defense Information Systems Agency,

- Jack Walicki, Chief Technical Officer, Middleware Division, Hewlett-Packard
- Peter J. Sevcik, President,

of Open Technologies and Standards, Novell, Inc.

Several forums of The Open Group will be engaged in discussions on identity management (see page 3 for full description) on Wednesday. And on Thursday, the day begins with John Zachman, Chief Executive Officer of the Zachman Institute for Framework Advancement will present a tutorial on the Framework for Enterprise Architecture. The end of Thursday provides the opportunity to learn about one requirement for information integration from Harald Tveit Alvestrand, Cisco Fellow, Cisco Systems.

Get involved at In3 



The Hilton Anaheim in the heart of The Anaheim Resort

NetForecast-Application Metrics

The morning of the second day is devoted to case studies and business scenarios, with afternoon sessions exploring The Open Group's activities that support Integrated Information Infrastructure. Morning speakers present government and commercial perspectives:

- Joanne Woytek, SEWP Program Manager, NASA
- Winston Bumpus, Director

Inside

Capitol Message Page 2
Identity Management Page 3
Embracing Instant Messaging Page 4
Industry Message Page 7
Meeting the Challenge Page 8
Upcoming Events Page 8

Message Board

Soon the EMA Forum will mark its one year anniversary in its current structure. The year has been replete with activity from retaining members to securing new ones to engaging in the third phase of the Secure Messaging Challenge (story on page 8).



We thank individuals and corporations for their support.

Message Metrics

CIO.com/metrics,
December 13, 2001

Security More than 70% of Americans are concerned about Internet security, and the same percent expressed at least "some" faith in the U.S. government to prevent cyber attacks. Another 74% are worried about what may happen to their person information over the Internet.

CIO.com/metrics,
December 19, 2001

CRM Gartner predicts that over the next five years all CRM software and new license revenue will show a compound annual growth rate of 5.6% worldwide. Yet 2001 revenues are predicted to drop 8% from 2000 levels.

CIO.com/metrics,
January 2, 2002

Mobile Phones Western Europe holds 25% of the worldwide mobile phone market.

Capitol Message

CIO Magazine,
November 15, 2001

The U.S. government's police powers have always been a point for debate and since the September 11 attacks the debate has been revived. Now most Americans seem to think that less "privacy is a small price to pay to sniff out terrorists."

How will new antiterrorism legislation affect businesses? Stewart Baker, a lawyer with Steptoe and Johnson (Washington, D.C.) and former general counsel to the National Security Agency, sees little direct effect on most companies. He says, "Unless you are the CIO of the Cali cartel you probably won't see the FBI knocking on the door to your data center too often."

Weighing in on the U.S. government's role is J. William Gurley, partner with Benchmark Capital, who believes that "The only people. . . who use encryption products are those who loathe or at the very least mistrust the government." While the government should not give up on computer surveillance, it should be realistic about the type of "magic" spy technologies available. (Fortune, October 15, 2001)

Business Week online,
December 6, 2001

Since his appointment as Special Advisor to the President for Cyberspace Security, Richard A. Clarke has moved toward build-

(see Capitol Message, page 6)



The Open Group EMA Forum

The Open Group's EMA Forum is a leading association for the e-business and messaging industries.

The Forum's diverse membership focuses on providing interoperable solutions for business leaders through informing and educating, fulfilling customer driven requirements, promoting and endorsing standards based solutions, and influencing public policy.

Steering Board

Chair

Dean Richardson

The Boeing Company
dean.richardson@boeing.com

Vice Chair

Dennis Cannon

Compaq Computer Corporation
dennis.cannon@compaq.com

James A. McDermott

ExxonMobil
james.a.mcdermott@exxonmobil.com

Glenn Parsons

Nortel Networks
gparsons@nortelnetworks.com

Michèle Rubenstein

solutions4networks
mrubenstein@s4nets.com

David Zimmer

American Eagle Group
dazimmer@ameagle.com

EMA Program Manager and
Editor-in-Chief. . Teresa L. Schauer

Managing Editor. . Renée Barnow

The Message

is published bi-monthly
by the

The Open Group
EMA Forum

Phone +1.703.549.2417

Fax +1.560.258.2622

Any unauthorized reproduction
constitutes a violation of federal law.

Submit comments or articles to
Renée Barnow

rbarnow@writelineunlimited.com

Fax +1.202.686.3550

Exploring Identity Management through Integrated Forums of The Open Group

Wednesday, 23 January, offers a wonderful opportunity to experience the essence of The Open Group at a session on identity management sponsored by the Directory Interoperability, EMA, and Security Forums.

With membership in multiple user communities (e.g., work and home), people's rights and privileges differ. Problems involved in managing these identities, rights, and privileges and respecting individuals' desires to limit the number of their community identities while still having those identities recognized and accepted by different IT programs is the focus of the full-day program.

Leading off the full-day program is Burton Group CEO Jamie Lewis whose keynote address, "The Emerging Infrastructure for Identity and Access Management" will set the stage for the open sessions that follow. During the open sessions, end-user companies and vendors will discuss some of the following identity management issues:

- Controlling access
- Keeping track of people who are always moving
- Delivering facilities to meet

people's personal needs and preferences

- Leveraging legacy and "incompatible" architecture

Morning sessions focus on the identity management problem and afternoon sessions explore possible solutions and ways for moving forward.

Winston Bumpus, Director of Open Technologies and Standards at Novell, Inc. and chair of the Directory Interoperability Forum will conduct the first of two morning sessions that includes speakers from the healthcare industry.

The second morning session features presentations from the supplier's perspective (Dean Sepstrup, Enterprise Messaging, Outlook Product Manager, The Boeing Company), from the perspective of the mobile environment (Ed Harrington, VP Business Development & Strategy, Nexor Pic and Chair of The Open Group Mobile and Directory Working Group), and from the role-based perspective (Vance Heron, NASA Jet Propulsion Laboratory).



Exploring possible solutions will be a member of the EMA Forum Secure Messaging Challenge (story on page 8), a member of the Liberty Alliance Project, and Jackson Shaw, Product Manager, Windows 2000 Server Marketing, Microsoft.

Wednesday's integrated forums' session will end by looking at ways the IT industry and its user community can move ahead. The last session of the day begins with a presentation and ends with a panel discussion.

In his description of the Identity Management Business Scenario, Chris Harding, The Open Group Directory Interoperability Forum Executive Director, will address the current state of the scenario's development and new issues that emerge from the day's earlier sessions.

The day dedicated to an integrated look at identity management will close with a discussion where a panel of users and vendors will offer their views on moving forward and respond to specific points the audience raises. Steven Jenkins will moderate the panel discussion.

Embracing Instant Messaging Today

by *Matthew C. Smith*, CEO, PresenceWorks, Inc.



Today's IT managers are under pressure to create a sensible and useful corporate instant messaging strategy. This pressure comes from executive offices and grass roots and is complicated by the fact that consumer IM networks, which have all the users, aren't built for corporate needs. Some IT managers are examining stand-alone IM networks, some are trying to block all IM traffic, and some are waiting on the sidelines. Where will you be?

PresenceWorks Inc., an integrator in Presence and IM solutions, believes that no action is the worst action, especially because there are clear ways IT managers can craft simple, effective solutions that capture the best features of consumer instant messaging (huge quantities of users, "presence" their online/offline presence) and still meet corporate requirements (IT oversight, logging, and security.) And best of all, no one has to switch instant messaging software.

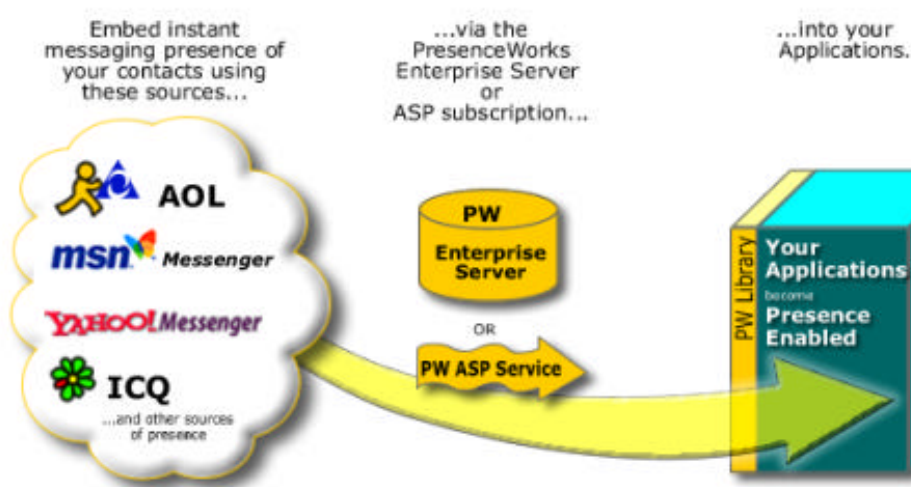
The Big Question

How can IT managers capture immediate business benefits from today's incompatible, insecure consumer IM systems, and still be in a great position to embrace future changes in IM standards?

The Short Answer

Don't install one particular IM system. Instead, turn your current applications into Buddy Lists that support all IM systems.

The Big Picture



Completing the Picture

1. Are companies currently using and benefiting from instant messaging?

Yes and no.

Internal and external people are clamoring for and using instant messaging, although it is entirely un-leveraged beyond its simplest use. In addition, there are security weaknesses, and in the case of financial companies, potential regulatory breaches.

2. Which Instant Messaging ("IM") software do people

want to use?

AIM, MSN, Yahoo, and ICQ.

Instant Messaging is an important issue today primarily due to the enormous installed base.

The underlying technology of live text is not especially hard to reproduce—the enrollment of large portions of business and consumers users is **very** hard to reproduce. New solutions for IM need to address this installed base.

3. Do companies promote using IM internally?

No.

In general, employees are discouraged from using IM, but do so anyway because it is an effective communications tool.

4. Should companies try to force their outside contacts to switch to different IM software?

No.

100 million people have selected an IM, and loaded it with their buddies. Good luck getting them to stop using it.

(see Embracing IM Today, page 5)

(Embracing IM Today, continued from page 4)

5. Is it possible for employees using ordinary business software to communicate with outside IM users?

Yes.

This is done by embedding instant messaging functionality directly into business software using PresenceWorks Presence Server and integration tools.

6. Can IM conversations be secure?

Yes.

With PresenceWorks, companies deliver one-way messages to people, which pop up on the recipients' IM. The one-way message contains a link inviting the recipient to finish the conversation elsewhere—such as in a secure Web chat room.

7. Does this mean companies need to run compatible IM software internally?

No.

Corporations don't need multiple installations of consumer IM software to contact outside IM users. In fact companies don't need any IM software installed internally. PresenceWorks software enables this by embedding IM functionality directly into business software.

8. Must companies pick one IM network for internal and external communication?

No.

By definition, picking one network leaves out people who aren't on that network. Furthermore, the consumer IM services do not offer security and logging features that many corporations want, so any choice would have built-in flaws. Therefore, although there

may be specific needs for an internal-only IM solution, companies must still find ways to IM with people outside their company, and they must still address security flaws.

9. Does this mean companies must run two or more different IM systems, one for internal and one for external?

No.

Because PresenceWorks embeds "I'm online" presence indicators next to the contact names in existing corporate software,



(such as Outlook, Siebel, or databases), employees can

then launch IM sessions directly from within that software.

10. Can companies have the best of four worlds? Internal IM system + security + outsiders using different IM's + nobody switches

Yes.

Here's how:

- (a) Embed presence (online/offline) information into existing corporate software.
- (b) Click a contact name in this existing software to launch an IM session.
- (c) Send messages to outside users' IM software from within existing software.
- (d) Include URL invitation in outgoing message inviting recipients to have conversation off the IM network.
- (e) Pull recipients, via the URL, into a secure Web-based chat room hosted by Company, meeting SEC and security

requirements.

(f) Chat in secure privacy, with any tools Company chooses to include in hosted chat room, including customer account information, SSL security, logging, and authentication.


Result: Company gets to take advantage of existing IM technology today to increase revenue and strengthen relationships with customers and colleagues.

11. Bonus question: How does this model support future changes in instant messaging and presence?

By embedding generic presence indicators into pre-existing applications, IT managers can change the source of that presence at any time without any visible change to the application.

Beyond the Buddy List

When people turn on their instant messengers, their presence information is made available to others, which people normally think of in terms of a "buddy list." Buddy lists are limited to a maximum of 150 names. Worse, buddy lists only display screen names—confusing little codenames that are entirely out of context, and that don't display any of the contact information already accumulated about a given person.

With PresenceWorks, businesses are no longer limited to buddy lists—the Presence information of unlimited business contacts can be displayed directly within the company's software, along with all the contact data already possessed 

(Capitol Message, continued from page 2)

ing a secure network for the government separate from the Internet and urged cell phone companies to make wireless frequencies available to government emergency personnel during crises.

Benefits of a dedicated government network include avoiding denial-of-service attacks as well as fewer viruses. Access to the network would require a biometric smart card.

An advocate of cybersecurity, Clarke says most companies are not paying enough for IT security. "They buy firewalls and an intrusion-detection system and think they're done. But that's just the beginning."

Federal Computer Week,
December 10, 2001

A study by the Association for Federal Information Resources Management (AFFIRM) reveals that improving electronic services, not security, is the number one challenge. In this year's survey of 80 chief information officers and senior technology officials at federal agencies, security fell to fifth from third place last year. Full survey results follow, with 2000's rank in parentheses.

1. Using IT to improve service to customers, stakeholders, and citizens. (8)
2. Making the business and cultural changes necessary for full e-government transformation. (NA)

3. Hiring and retaining skilled professionals. (1)
4. Obtaining adequate funding for IT programs and projects. (4)
5. Preventing unauthorized system intrusions. (3)
6. Formulating or implementing an agency IT architecture. (6)
7. Building effect relationships in support of IT initiatives with agency senior executives. (7)
8. Capturing, organizing, and making accessible agency knowledge and expertise (knowledge management). (8)
9. Simplifying business processes to maximize the benefits of technology. (10)
10. Unifying "islands of automation," or separate systems for separate units, within lines of business. (NA)

Business Week online,
December 13, 2001

According to sources on Capitol Hill, obtaining funding to secure the Internet from attack will be easy, with demands on researchers harder. Congress will spend to get a network that is not only "more secure, but one that can heal itself if it's damaged." Researchers warn that the task is a daunting one.

PCWORLD.com
January 4, 2002

Still more relating to the "key logger system" ([The Message](#),

Volume 1, Issue 2 (September 2001) and Volume 1, Issue 3 (November 2001) Capitol Message, is news that the U.S. government is permitted to use secretly installed keystroke logging tools to defeat encryption. U.S. District Court Judge Nicholas H. Politan rejected a defense motion to suppress computer evidence gained in the FBI case against an accused Mafia loan shark. In rejecting the defense arguments, Judge Politan indicated that the summary description of the keystroke logger made public in court met the defendant's need to know what facts or documents the prosecutors are likely to use at trial to make their case. Politan stated, "We must be ever vigilant against the evisceration of Constitutional rights at the hands of modern technology."

Memorable Messages

From CIO.com

"Don't look at the past and assume that's the future. Look at the enemy's strengths and your vulnerability. You've got to realize that the worst case does sometimes happen."

Richard Clarke
*Special Advisor to the President for
Cyberspace Security*

From GWSAE Fast Read

"You can never plan the future by the past."

Anonymous
"There is no security on this earth; there is only opportunity."
Douglas MacArthur

Industry Message

The Wall Street Journal,
December 6, 2001

email Security Combining the efficiency of the Internet with such attributes of postal mail and courier services as privacy, return receipts, and tracking is PostX, a company founded in 1996. Wrapping email in a protected format that appears like an envelope on the screen, the company's software makes it possible for only the person who enters the correct password to open the envelope. PostX helped the U.S. Postal Service develop its electronic postmark.

Business Week online,
December 11, 2001

Open Source Security Waltham, MA-based Guardent rolled out a hardware security appliance that relies solely on open source programs to monitor and guard corporate networks. The company says one of the 10 largest financial institutions in the U.S. is among the beta customers of the device, incorporates a handful of customized versions of well-known open source security software tools.

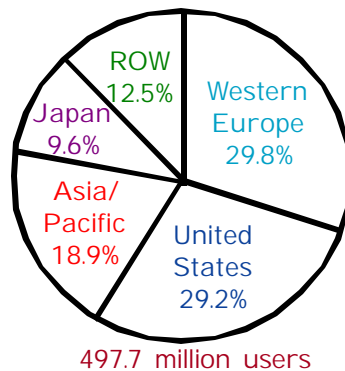
Open source security products will most likely struggle without seals of approval from the National Institute of Standards & Technology. Another problem, "As open source pushes into more complex pieces of software, such as firewalls and IDS, frequent code-patching can spawn its own difficulties."

The Wall Street Journal,
December 18, 2001

Workplace Security In for 2002 is workplace security. Managers with security know-how have risen in importance in their companies and consultants who formerly gave advice about the Internet are now selling security expertise.

CIO.com, eBusiness Trends,
January 3, 2002

Internet Use By the end of 2001, the number of people using the Internet in Western Europe had exceeded the num-



497.7 million users

Source: IDC's Internet Commerce
Market Model version 7.3, 2002

ROW=Rest of the World

ber of U.S. users. Between 2000 and 2005, the compound annual growth rate of Internet users worldwide is expected to be 19%. IDC predicts that by 2005, there will be 941.8 million Internet users worldwide, close to double the number of users in 2001 (497.7 million).

Outpacing Western Europe's population of Internet users between 2000 and 2005, will be Asia/Pacific users. By the end of 2005, this population is expected to post a 29% compound annual growth rate and to surpass the

U.S. as the second most populous region of Internet users.

The International Herald
Tribune, January 10, 2002

Internet Security A report from The Computer Science and Telecommunications Board, part of the National Research Council says that for U.S. computer networks, "Cybersecurity today is far worse than what known best practices can provide."

Message Corner

From Fast Company,
November 2001

"Ever since April 14, 2000, the question has been, When is this thing (the Internet business. . .) going to turn around? The answer is in the McKinsey [e-performance] survey. . . . If the S&L/real estate crisis is a suitable analogy, it'll take about five years. . . . Along the way, there's lots of money to be made."

Five Rules for Webyfying Finance

"Rule #1: The Internet changes everything—but it doesn't change everything overnight.

Rule #2: There is no such thing as first-mover advantage.

Rule #3: Some of the old rules still rule.

Rule #4: Your choice: dotcom, dotcorp, or both?

Rule #5: First we overestimated the Internet; don't underestimate it now."

*Interview with Janey Place,
Mellon Financial*

Meeting the EMA Forum Secure Messaging Challenge

Exhilaration best describes the EMA Challenge Team's activities in meeting the Secure Messaging Challenge. In a short and concentrated six months through determined and dedicated activity, the Challenge Team has moved from design and development to demonstration. At 6:30 p.m., Tuesday, 22 January, as part of The Open Group's Quarterly Conference in Anaheim, the Challenge Team, which The Boeing Company is supporting, will debut its efforts: The standards-based exchange of highly encrypted email.

Test cases considered included sending encrypted messages to multiple recipients in multiple domains and determining if the client application will detect that a recipient's public key is not authentic.

In the first, the test would be successful if the messaging client retrieved the correct public key for each recipient and properly encrypted the message for each recipient (internal or external). In the second, the test would be successful if the messaging client detected that the public key was not accompanied by the correct certificate.

Upcoming Events

- 21-25 January 2002* Quarterly Conference
Anaheim, CA
- 22 January 2002* EMA Forum Secure Messaging Challenge
Demonstration and Cocktail Reception
Anaheim, CA
- 23 January 2002* Identity Management, Joint Meeting of
EMA, Directory Interoperability, and
Security Forums
Anaheim, CA
- 8-12 April 2002* Quarterly Conference
Paris, France
- 22-26 July 2002* Quarterly Conference
Boston, MA

Current testing involves four functionally complete LDAP/messaging systems, with a fifth in progress. Root certificates have been mutually exchanged, as have several messages. By mid-January, formal testing is expected to end. All progress to date will be presented at the conference in Anaheim.


The presentation will cover the Secure Messaging Challenge's history and current status (Dean Sepstrup, The Boeing Company, Co-Chair EMA Challenge) and details on testing methodology (Paul Van Avery, FTT Consultants).

After the presentation, the audience will be turned loose on demonstration workstations. Attendees will be able to experience first-hand actual working systems without requiring manual operation to retrieve the recipient encryption key.

As the Challenge Team partners have been building the architecturally compliant systems, they have been documenting "lessons

learned," which will be made available in a toolkit, planned for release in late January after formal testing and results verification. The toolkit will include "lessons learned" during the planning, implementation, and testing for the Challenge.

The Secure Messaging Challenge was intended to implement and test some, not all, aspects of Public Key Infrastructure; the intent was to plan, implement, and test those components of a Public Key Infrastructure that are needed to support a secure messaging system. The Challenge Team is excited by its progress in meeting the challenge and looks forward to sharing its enthusiasm and results and in obtaining feedback on 22 January in Anaheim.

The demonstration is open to all Conference attendees 

For your interest—The Message body text is "A Caslon Regular" and headline text is "Broadband ICG."