Single Sign-On: Myth or Reality

Thomas R. Peltier, CISSP

Driving eBusiness Performance ***SM***

Abstract

- As enterprise computing becomes more and more complex, with business systems installed across multiple platforms, from mainframe to client-server to PC, the need for a secure way to provide users with a single authentication point becomes more and more important. There are a number of methods and products on the market today which provide some form of single sign-on, and each has advantages and risks.
- This session will examine what you will need to do to prepare for single sign-on. We will also identify a set of functional requirements for a single sign-on methodology, so that attendees will be better able to compare the products available.

Objectives

- At the conclusion of this workshop, attendees will:
  - understand the current push for single sign-on
  - be able to identify what their organization must do to prepare for SSO
  - have an understanding of what industry experts look for in SSO products
  - understand the basic principles of cryptography

Objectives

- At the conclusion of this workshop, attendees will:
  - be able to identify the current SSO players
  - be able to identify current SSO products and where to obtain additional information
  - understand current problems with SSO implementation

Format

- This workshop has been developed for you.
- Please feel free to:
  - ask questions
  - offer advise
  - provide observations
  - participate

Agenda

- Introduction
- Overview
- Requirements
- Single Sign-on Basics
- Single Sign-on Views

Agenda

- Elements of Single Sign-on
- Cryptography
- Standards Based Solutions
- Problems and Solutions
- References

Introduction

- Single sign-on (SSO) has generally been used as an umbrella term for the consolidation of platform-based administration, authentication and authorization functions.
- Can the vendor industry support a true *single* sign-on process?
- Due to the number of varied platforms and applications, it is unlikely and in some cases, impossible.

Introduction

- This fact - that SSO is a misnomer - has contributed (according to Gartner) to the failure of the sector to achieve rapid growth, despite widespread recognition of the "too many IDs and passwords" problem.

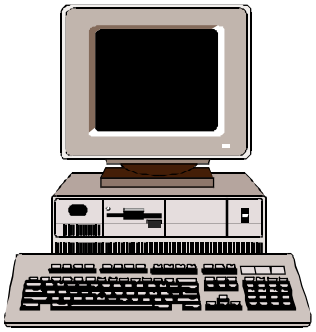
Introduction

- Historically each system vendor provided an authentication mechanism based upon its own system requirements which was adequate when users only needed to authenticate to one system.
- Today in a heterogeneous computing environment vendors face a dilemma. . . how to provide single logon to their user community.

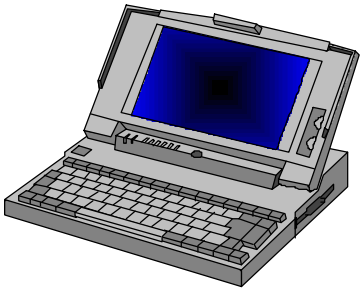
The Changing Environment

Fortress
Computer Room

Desktop
Computing



Remote Access
Computing



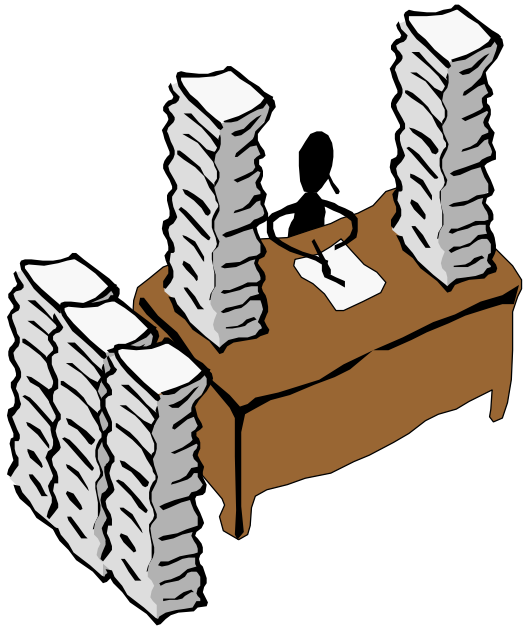
Unresponsiveness leads to:

Overview

- Users and administrators are greatly affected by the problem.
- Users who need to remember more than one id/password pair often use known, insecure practices like:
  - writing down passwords
  - using one password for all accesses
  - using a simple password

Overview

- Administrators face the nightmare of maintaining consistency and security for their varied user community across multiple platforms and policies.



Overview

- The dilemma with Single Sign-on (SSO) is that simple statements hide complex situations.
- What is implied but not stated by SSO is that providing a single logon involves a relationship to several security feature/mechanisms aside from authentication:
  - access control
  - security policy(trust)
  - encryption
  - key distribution

Overview

- Enterprise systems by definition are diverse. They consist of different operating systems, networks and utilities.
- Enterprise environments with local authentication consist of some combination of:
  - local authentication,
  - remote access authorization,
  - network authentication, and
  - application authentication.

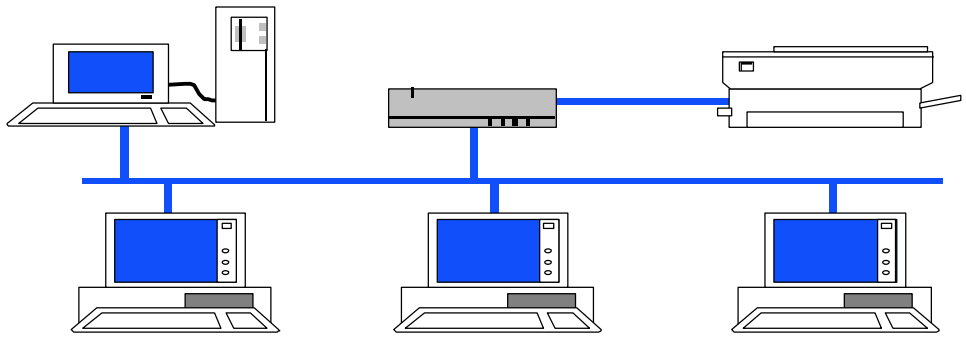
ISO Open Systems Interconnection (OSI) Model

TCP/IP Network Components

7 Application	Application Protocols
6 Presentation	
5 Session	
4 Transport	Transmission Control Protocol (TCP) User Datagram Protocol (UDP)
3 Network	Internet Protocol (IP)
2 Data Link	Network Interface Protocol (Ethernet, Token Ring, Arcnet, etc.)
1 Physical	

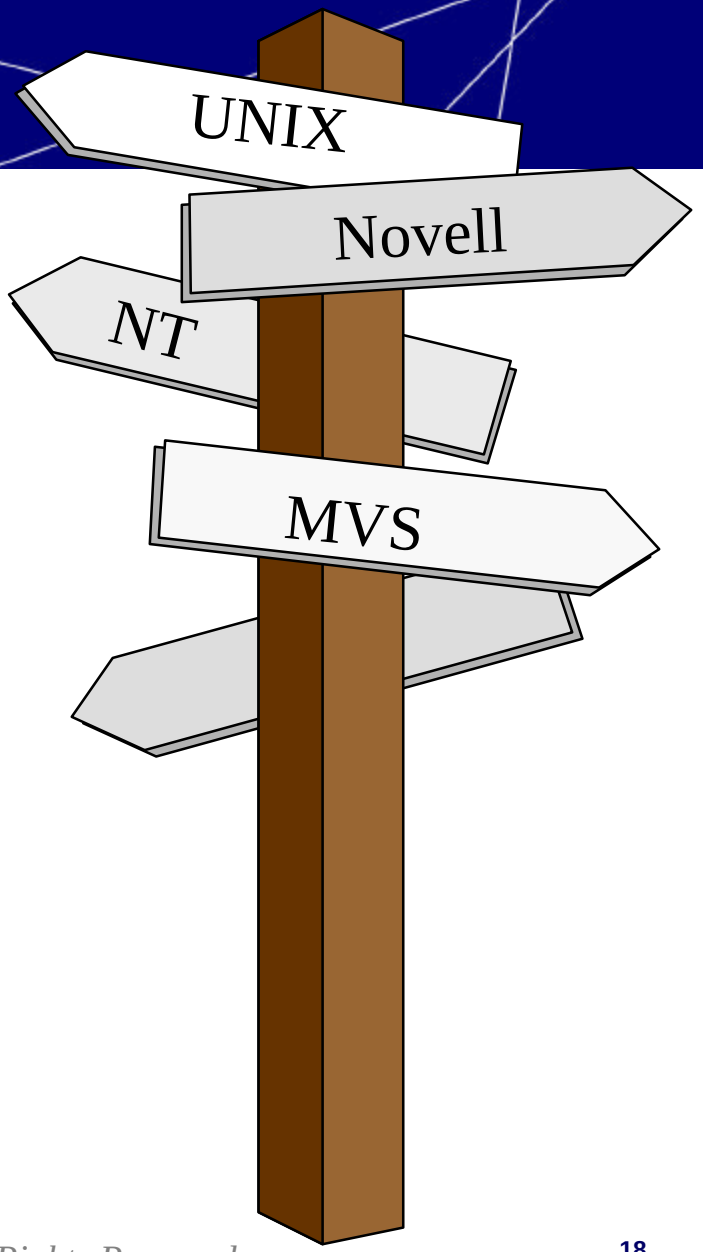
Overview

- In an environment where local authentication and network authentication are provided by different systems with different implementations and administrative policies, it is very difficult to establish confidence and consistency in the authentication of users.



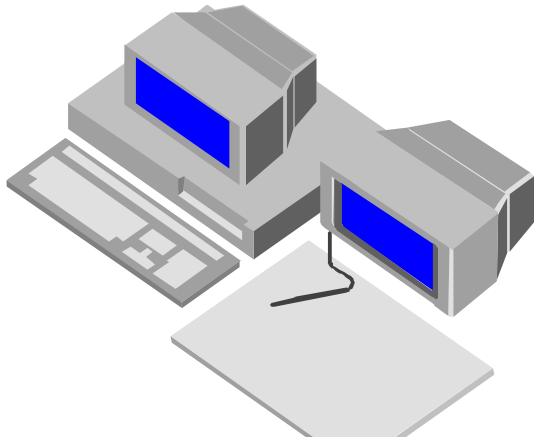
Overview

- Most vendors provide a local authentication mechanism which is specific to operating systems.
- Yet even within an operating system like UNIX, there is variability in the implementation of authentication.



Requirements

- Fundamentally, enterprises need to manage their computer resources from unauthorized access.
- Enterprise resources consist of independent sets of (possibly individually) managed computer resources.



Requirements

- One of the resources of an enterprise is its user community.
- Defining how a user is identified in the environment of multiple systems requires an abstraction on the notion of identity.
- To be successful, the SSO must have a common understanding of the user identity across all platforms.

Requirements

- Requirement #1 - Identity
  - A common definition of what constitutes a user identity. The identity must be part of a naming convention which is complete, unambiguous and secure. It must be consistent between the authentication and authorization models.
- While each enterprise manages policy at a high level, there is often a requirement for each system to influence the management of its resources on a “host” level.

Requirements

- Requirement #2 - Authentication
  - A need to allow host systems to be able to “constrain” the set of users allowed access to the host.
- Requirement #3 - Host Authorization
  - A need to allow host systems to be able to specify granularity based on device requirements.
- There are inherent contradictions in this set of needs. By definition each computer system understands “users” relative to its own mechanisms. Each system trusts its own mechanisms and distrusts anything outside its perimeter.

Requirements

- Requirement #4 - Authentication
  - Need to identify a mechanism by which authentication mechanism can negotiate an authentication sequence on behalf of the user.
- Requirement #5 - Authorization
  - Need to define a common understanding of trust associated with an authentication sequence.
- Once authentication has been established, SSO then needs to define how local and remote resources should be accessed by users, both native and remote, based on this abstract notion of identity.

Requirements

- Requirement #6
  - Need to define the relationship between authentication and authorization.
    - Authentication - an ability to identify who an individual or system actually is
    - Authorization - a process to allow authenticated programs, users or systems to access information processing resources available through systems and applications.

Requirements

- Solving the single sign-on problem then involves:
  - Requirement # 1 - common definition of what constitutes a user identity.
  - Requirement # 2 - Need to allow host systems to be able to “constrain” the set of users allowed access to the host.
  - Requirement # 3 - Need to allow host systems to specify granularity based of device.

Requirements

- Solving the single sign-on problem then involves:
  - Requirement # 4 - Need to identify a mechanism by which authentication mechanism can negotiate an authentication sequence on behalf of a user.
  - Requirement # 5 - Need to define a common understanding of trust associated with an authentication sequence.
  - Requirement # 6 - Need to define the relationship between authentication and authorization.

Requirements

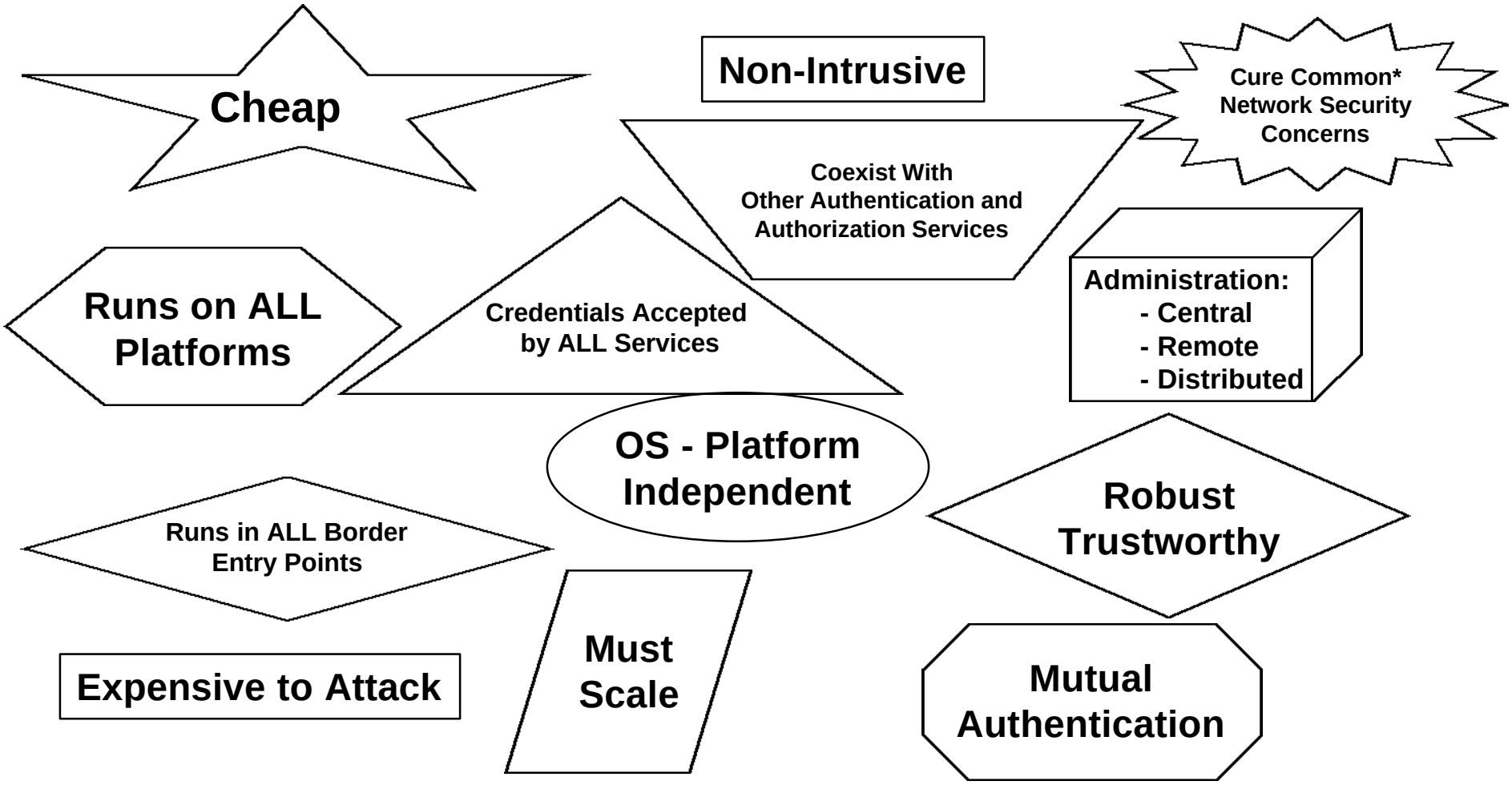
- Three of these requirements involve the definition of a security policy for a security domain.
  - Requirement # 1 - common definition of what constitutes a user identity.
  - Requirement # 5 - need to define a common understanding of trust associated with an authentication sequence.
  - Requirement # 6 - need to define the relationship between authentication and authorization.

Single Sign-on Basics

- Why is single sign-on needed?
  - Lack of secure channels
  - Initial identification and authorization
  - Synchronization of identification and authorization across the myriad of disparate, heterogeneous systems
- Why isn't a complete solution available?
  - Security is not a priority
  - Economics

Netigy

Single Sign-On Basics



Single Sign-on Basics

- What should a single sign-on product include?
  - Identification, authorization, and authentication
  - Client / server and distributed systems
  - Mainframe applications
  - Host security
  - Workstation security
  - Network security
  - The entire infrastructure

Single Sign-on Current Players

- The SSO market is very active:
- From 1997 to current, some long-heralded products became available:
  - Memco* and IBM
- Others matured significantly:
  - Platinum*, Unisys and CKS

Single Sign-on Current Players

- The SSO market is very active:
- Niche products were developed:
  - CyberSafe's TrustBroker, OpenVision/Veritas Axxion Authenticate, OpenHorizon Connection
- Deployments continue and are increasing, and users remain interested.
- However, there is movement in the sector toward mergers and acquisitions.

Single Sign-on Current Players

- **Vendor and Product Names**
  - Axent Technologies (www.axent.com) - Enterprise Resource Manager
  - Bull (www.bull.com) - AccessMaster
  - Century Analysis Inc. (www.cainc.com) - CAI-Net
  - Computer Associates International (www.cai.com) - Unicenter SSO
  - CKS (www.cksweb.com) -MyNet
  - CyberSafe (www.cybersafe.com) - TrustBroker Security Suite and Defensor

Single Sign-on Current Players

- **Vendor and Product Names**
  - Computer Associates Inc. (www.cai.com) - Platinum family
  - Hewlett-Packard (www.hp.com) - Praesidium SSO
  - IBM (www.ibm.com) - Global Sign-On
  - iT_SEC - iT_SecureSignOn
  - Proginet (www.proginet.com) - SecurPass
  - RSA Security (www.rsasecurity.com) - Boks SSO/SecurSight Manager
  - Softools (www.softools.fr) - SoftSSO
  - Unisys (www.unisys.com) - Single Point Security

Single Sign-on Current Players

- Century Analysis Inc. (www.cainc.com) - CAI-Net
  - CAI-Net III offers end users a workplace that allows them to, through a single master password per end user, gain seamless access to multiple applications simultaneously, independent of the workstation being used or the applications being accessed.
- Computer Associates International (www.cai.com) - Unicenter SSO
  - The Unicenter TNG Single Sign-On Option provides an easy point-and-click Windows-based interface enabling end users to access multiple, enterprise-wide, network applications with a secure single sign-on
- CKS (www.cksweb.com) -MyNet

Single Sign-on Current Players

- CyberSafe (www.cybersafe.com) - TrustBroker Security Suite and Defensor
  - The TrustBroker Suite features multi-platform, single sign-on authentication, including both Public Key and Kerberos encryption. It secures your organization's intranet and extranet against inside and outside threats, even when using unsecured networks (such as the Internet). It is scalable, interoperable on virtually any business platform, and flexible through its support of multiple authentication mechanisms (passwords, certificates, token cards, smart cards, etc.).
  - The Defensor Family of products was added to the **Trust**Broker Security Suite in December 1998. Defensor allows secure end-to-end communications between clients, servers, gateways and mainframes, regardless of the application, network technology or geographic location of the communicating parties. Authenticated users get secure, on-demand, above-the-network communications with their authorized applications based on "Who Can Do What" rules.

Single Sign-on Current Players

- Hewlett-Packard (www.hp.com) -
  - Praesidium SSOHP Praesidium/Single Sign On (SSO) has been specially developed to address the problems of multiple sign-ons which have arisen over the last few years from the development and ever-increasing use of client/server architecture in enterprise-scale businesses. This trend has resulted in an equal increase in the number of issues facing three different groups of people within the enterprises: the users, administration, and security; the majority of these issues arise from the number of passwords required to access even the most basic information.
- IBM (www.ibm.com) - Global Sign-On
  - IBM Global Sign-On is a secure, easy-to-use product that grants users access to the computing resources they are authorized to use—with just one logon. Designed for large enterprises consisting of multiple systems and applications within heterogeneous, distributed computing environments, Global Sign-On eliminates the need for end users to manage multiple logon IDs and passwords.

Single Sign-on Current Players

- Axent Technologies (www.axent.com) - Enterprise Resource Manager
  - Axent - ERM - Provides enterprise-wide user and resource administration, one-time authentication and single sign-on across distributed computing platforms.
- Bull (www.bull.com) - AccessMaster
  - ISM is a suite of tools for systems management that is broken up under 6 main functionality headings. AccessMaster is the security management component and one of ISM's highlights. There are two main components - a single sign-on product and standard authentication features built around a central data base of user profiles. The single sign-on capability allows a user to access multiple systems through the use of a single identifier and password combination. This is then used to access the user profile, and to show only the applications that he or she is authorized to see. This desktop lockdown is the fundamental basis for many security solutions where sensitive applications are restricted, so that only those that need them have access.

Single Sign-on Current Players

Proginet (www.proginet.com) -

SecurPass helps corporate security administrators, help desk staff and end users manage the complexities of multi-platform environments. SecurPass "harmonizes" native Microsoft Windows NT security with standard IBM mainframe, Novell, and UNIX security systems, providing password synchronization between different environments. SecurPass is the only solution of its kind which does not require code at every desktop.

Security Dynamics (www.securitydynamics.com) - Boks SSO/SecurSight Manager

SecurSight products are a family of plug-in security solutions for the enterprise. They include SecurID authentication, and the SecurSight Desktop, Manager, Agents and Agent Toolkit. They integrate the vendor's ACE/Server security software with public key cryptography and digital certificate security technology from RSA Data Security.

Single Sign-on Current Players

Softools (www.softools.fr) - SoftSSO

Unisys (www.unisys.com) - Single Point Security

Unisys offers a comprehensive approach to managing identity across large, heterogeneous environments. Single Point Security product line integrates hardware and software for global single sign-on (SSO), biometrics identification, user management, and protected communication across public networks with a full set of information security consulting services.

Netigy

Single Sign-on Current

Mainframes

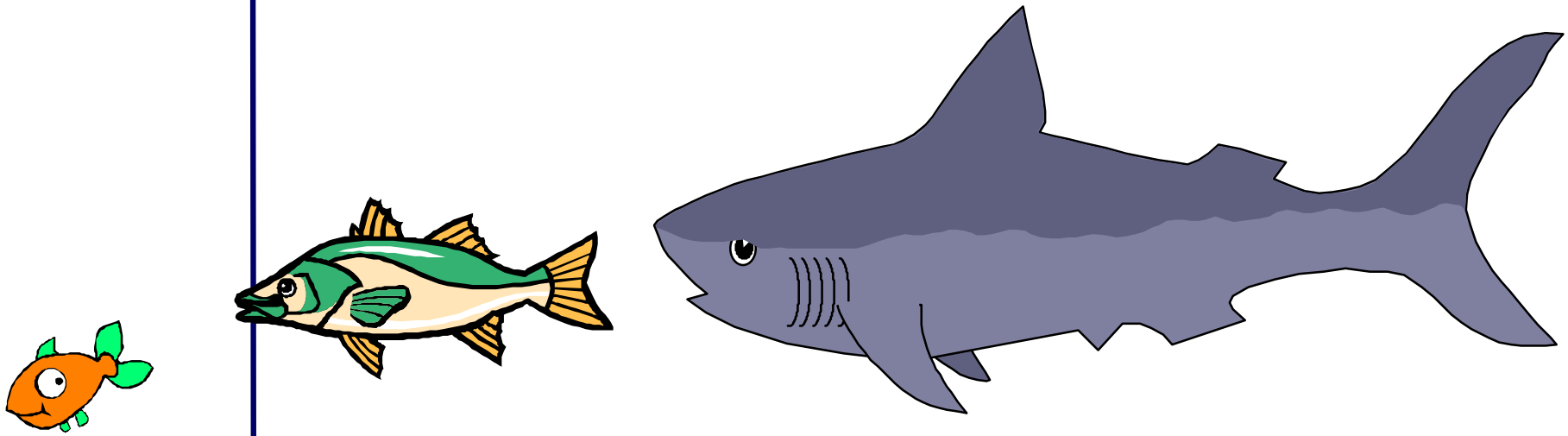
Product	HP	IBM	Unisys	DEC	Other
Axent - ERM	X	X			
Bull - AccessMaster		X			X
CA - Unicenter SSO	X	X			X
CKS - MyNet	X	X	X	X	X
CyberSafe - TrustBroker	X				

Single Sign-On Current Players

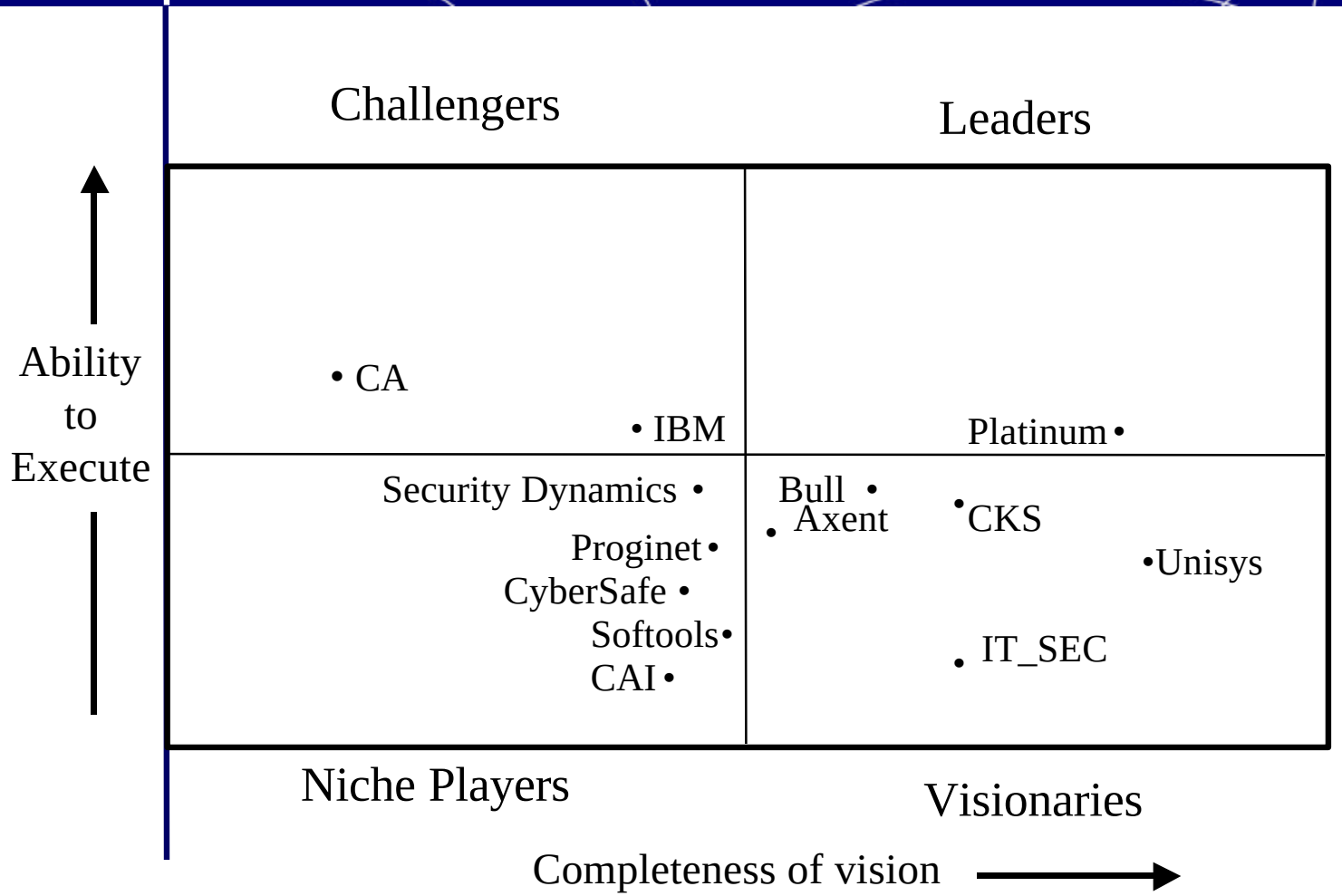
Product	Networks						
	UNIX	Windows	Netware	NT	SUN	OS/2	*
Axent - ERM	X	X	X		X		X
Bull - AccessMaster	X	X	X	X		X	
CA - Unicenter SSO		X		X			
CKS - MyNet	X	X	X	X		X	X
CyberSafe - TrustBroker	X	X		X		X	

* = Other networks (Axent - Iris, Solaris, CKS - DOS, TrustBroker - DOS, Macintosh)

Single Sign-on Current Players



Single Sign-on Current Players



Source: Gartner Group

Single Sign-on Current Players

- What makes up *Vision:*
  - Does the vendor have a strategic plan?
  - Is it in line with industry trends?
  - Does it match third-party beliefs in what is appropriate for the industry?
  - Is the vision comprehensive enough to establish a broad install base?

Single Sign-on Basics

- Users can use resources anywhere in the network no matter where they are.
- User profile knows what applications are authorized and where they can be found.
- With a single UID/password, a user can login to the enterprise network and access all network services and applications that they need to perform their jobs.
- Eliminate the need for users to have multiple usernames and passwords.

Single Sign-on Current Players

- In looking to a vendor, you might want to consider:
  - Their financial strength
  - Their ability to continue to improve the product
  - Marketing and sales capabilities
  - Integration abilities
  - Strategic alliances

Single Sign-on Considerations

- SSO and ACL rules often must be developed and administered separately.
  - Security administrators often must know syntax rules for multiple platforms.
  - Audit reports often must be defined and administered outside of products.
  - Complete solutions require an integration of several products.
  - Many products have limited proven maturity.
  - Trained staff are not always readily available.

Single Sign-on Considerations

- Using only one SSO server can introduce a single point of network failure.
- Few, if any, software solutions accommodate all major operating-system environments; a mix of solutions must be tailored to the enterprise's information-technology architecture and strategic direction.
- Substantial interface development and maintenance may be necessary, especially in the absence of industry based standards.

Single Sign-on Considerations

- The SSO server and other host security must be hardened since weaknesses can now be exploited across the enterprise.
- Most SSO-software packages include additional access-control features for which you are charged even if they are redundant of your existing controls.
- Establishing single-user IDs across an enterprise is no trivial management or administrative task.

Other Considerations

- Central user administration from a central point
- Accommodates local (distributed) administration
- Passwords, privileges, access controls
- Access control and role management
- User logging and auditing

Other Considerations

- No plain text passwords on the network
- No local, workstation password storage
- Compliant with standards
- Existing mechanisms preserved
- Accommodate sophisticated authentication
- Interoperability with other SSO environments

Cryptography

Required for single sign-on

Cryptography

Definition: the art of secret writing

- Writing that only the authorized can read
- The art and science of keeping messages secure
- How can you trust it?
  - Secrecy depends ONLY on the key(s)
  - Secrecy does NOT depend on a proprietary algorithm
  - Algorithm well known, widely scrutinized
  - Attacks discussed widely
  - Weaknesses acknowledged

Cryptography

Common questions

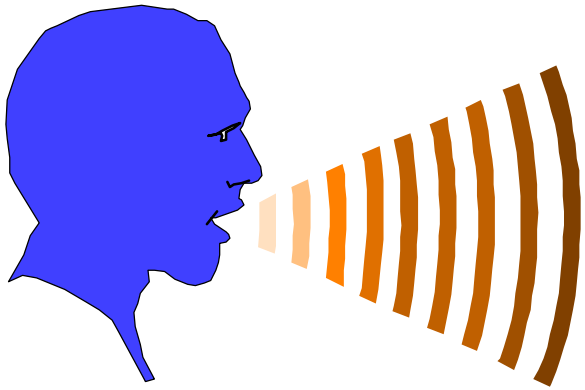
- Keys are seldom memorized
  - Where / how is your key stored?
  - How is it protected?
- All cryptography requires key distribution
  - How do you trust this mediation?
- Key distribution is not trivial
  - How are keys distributed?
- Cryptography is intrusive
  - How is it used without disrupting the infrastructure?

Cryptography

Trusted authority vouches for identity

All cryptographic schemes are mediated

- Secret key
  - Authentication Server
- Public key
  - Certification Authority



Cryptography

Certificates

- Binds user to ID
- Contains a description of the user (name, address)
- Guaranteed by issuing authority
- Issuing authority also needs one

Common root or cross certification

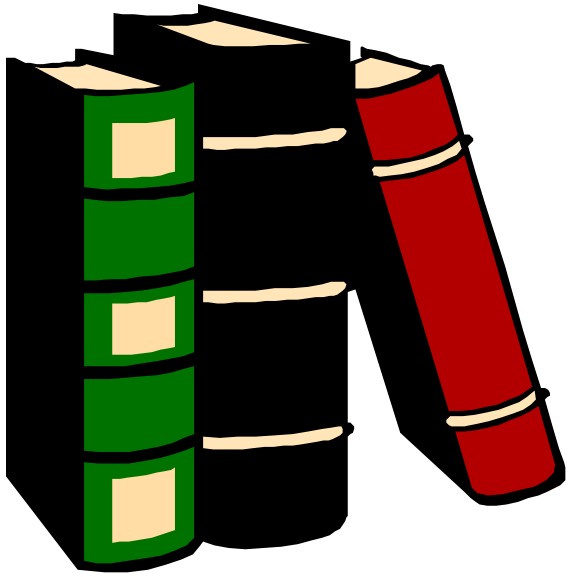
- Inter-organizational
- Intra-organizational

Classifying Solutions

- Product-based comparisons
  - Product surveys
  - Requirements-based comparisons
- Technology-based comparisons
  - Security service model comparisons
  - Methods comparison

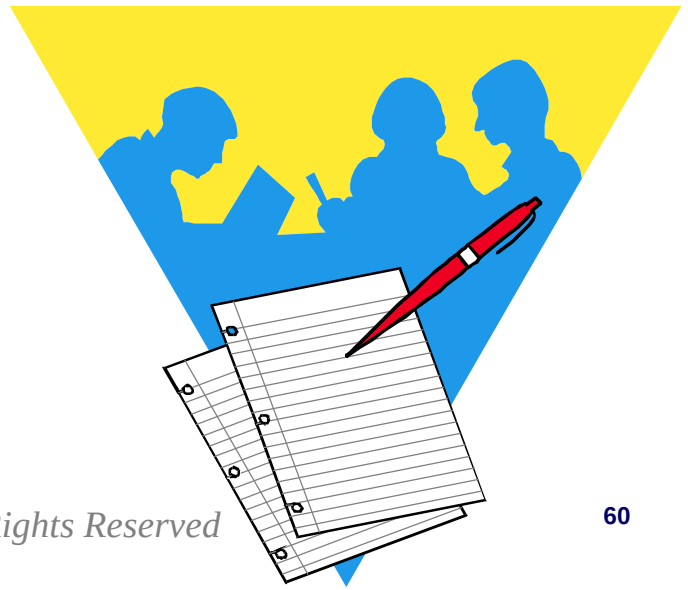
Success With Single Sign-on

- Establish requirements
  - Budget
  - Technical
  - Infrastructure
  - Personnel
  - Support
  - Administrative
  - Vendor



Success With Single Sign-on

- **Phased project plan**
  - Requirements and education
  - Establish a laboratory
  - Pilot(s)
  - One widespread application
  - Move into production



Problems and Solutions

- Lack of understanding - technological issues
  - Strengths, weaknesses
- Lack of understanding - organizational issues
  - Management, politics
- Unfounded vendor claims
  - Verify everything

Problems and Solutions

- Works in the lab - doesn't work in production
  - Ensure that the laboratory environment reflects your environment
  - Test every aspect of the pilot
    - Security
    - Performance
    - Administration, operations, and management

SSO Outlook

- The ability to reduce the number of log-ins for users in both deployed/package environments and future home-grown applications will continue to be improved.
- Scalability of user base in the thousands is currently under way.
- Customers should continue to see merges, acquisitions, and consolidations.

SSO Outlook

- The number of vendors in the field currently exceeds that required by demand.
- Consolidated authentication within NT 5.0 resources, or across all resources supporting public-key cryptography, is looming (although neither of these will be PA within the next year).

SSO Outlook

- The trends are positive, but a *single* log-on for all users in large mixed-platform environments will remain elusive.
- The product in maturing, and the ability to meet the customer's needs is nearly at hand.

Summary

- Single Sign-on (SSO) is **NOT** a security issue.
  - It is a customer convenience issue;
    - and
    - A cost savings issue.

Summary

- SSO will not be implemented until you are ready.
- To be ready, the infrastructure must meet minimum standards (most SSO will require fairly current operating systems).
- Standards must be established for identification of users (a common userid).
- You must establish what your organization's needs are and develop a set of specific requirements before you begin to examine SSO products.

Summary

- There is a “shaking out” of the vendors. Do your research to see who will remain viable.
- It may be necessary to look to third parties for analysis, organizations such as:
  - CSI Buyers Guide
  - Gartner
  - Meta
  - GIGA
  - DataPro
  - Periodicals

References

- A. Goscinski, “Distributed Operating Systems - The Logical Design”, Addison-Wesley, 1991, ISBN 0-201-41704-9.
- Raman Khanna (editor), “Distributed Computing - Implementation and Management Strategies”, Prentice Hall, 1994, ISBN 0-13-220138-0.
- SESAME - Belinda Fairthorne, OPENframework Security, Prentice Hall, NY, NY, 1993
- DCE
  - Guide to OSF/1 - A Technical Synopsis, O’Reilly & Associates, Sebastapol, CA, 1991
  - Harold Lockhart, OSF DCE - Guide to Developing Distributed Applications , McGraw Hill, New York, NY, 1994
  - Ward Rosenberry, David Kenney, & Gerry Fisher, Understanding DCE, O’Reilly & Associates, Sebastapol, CA, 1992.

References (continued)

- Charlie Kaufman, Radia Pearlman, and Mike Speciner, Network Security - Private Communication in a Public World, Prentice Hall, NY, NY, 1995
- William Stallings, Network and Internetwork Security - Principle and Practices, Prentice Hall, NY, NY, 1995
- Clifford Stoll, Silicon Snake Oil, Second Thoughts on the Information Highway, Doubleday, New York, NY, 1995
- Harry DeMaio, Every Manager's Guide to Keeping Vital Computer Data Safe and Sound, AMACOM New York, NY
- Deborah Russell & G.T. Gangemi, Computer Security Basics, O'Reilly & Associates, Sebastapol, CA, 1991.

References Continued

- Bruce Schneirer, “Applied Cryptography — Protocols, Algorithms, and Source Code in C - Second Edition”, John Wiley & Sons, Inc., 1996, ISBN 0-471-11709-9
- Edward Amoroso, Fundamentals of Computer Security Technology, Prentice Hall, NY, NY, 1994
- PKCS - RSA Data Security, 100 Marine Parkway, Redwood City CA 94065-9917, (415) 595-8782
- Needham, R.M. and Schroeder, M., “Using Encryption for Authentication in Large Networks of Computers,” Communications of the ACM Volume 21(12) pp. 993-999 (Dec. 1978).
- Denning, D.E., and Sacco, G.M., “Timestamps in Key Distribution Protocols,” Communications of the ACM Volume 24(8) pp. 533-536 (August 1981).

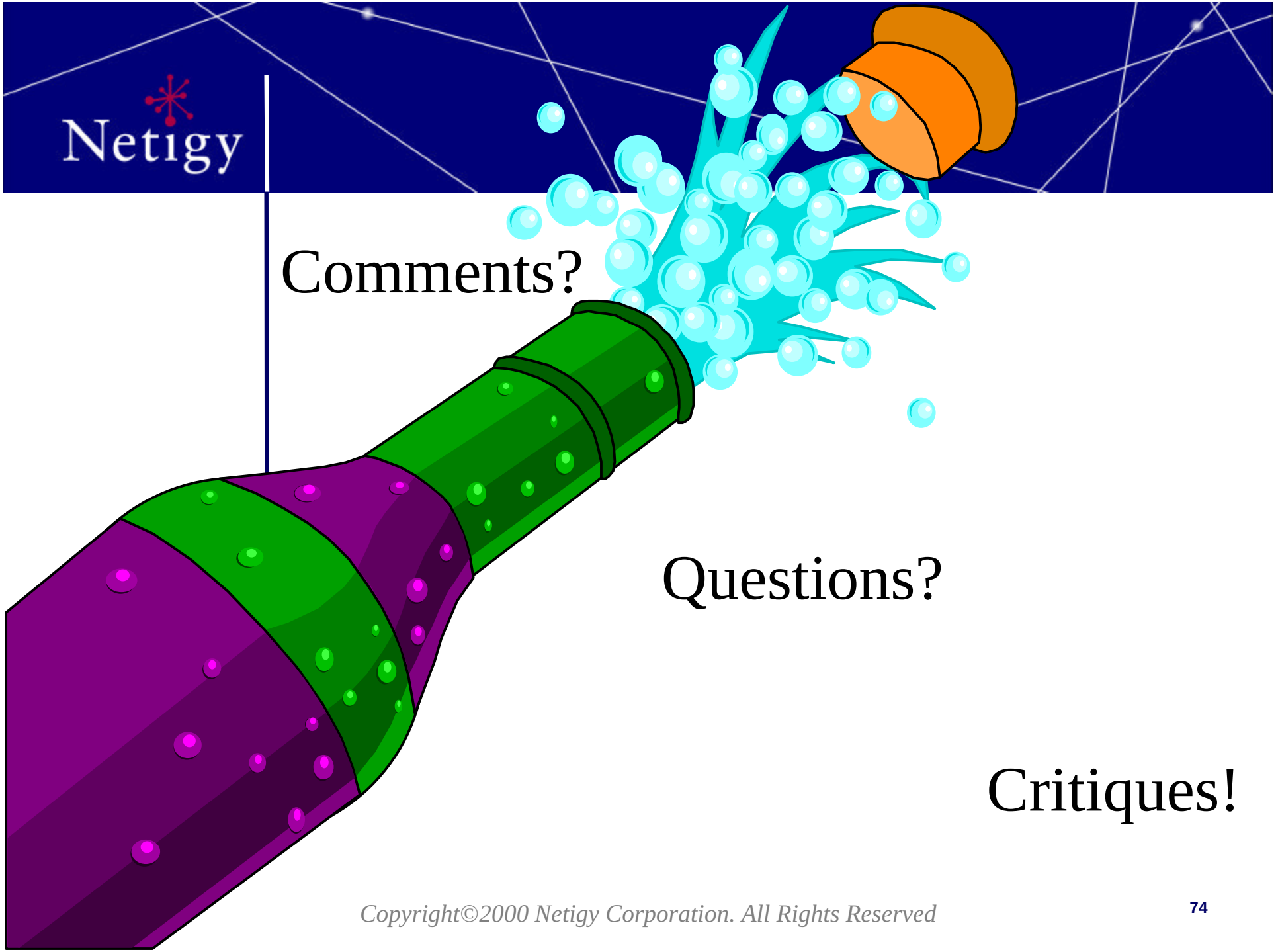
References (continued)

- OSF DCE Security Analysis Report, Bellcore Technology Licensing, 8 Corporate Place, Room 3A184, Piscataway, NJ 08854, (908) 699-5800
- Open User Recommended Solutions (OURS), 1 World Trade Center 78th Floor, New York, NY 10048-0202

References (continued)

- Joe Kovara - CyberSafe
- Glen Zorn - Microsoft Corporation
- Todd Sun - Formerly of Mergent International
- Robert Clyde - Axent Technologies, Inc.
- Larry Kilgallen - LJK Software
- Daniel Woolley - ICL
- Fred Trickey - **Netigy**
- Wes McClean - Consumer's Gas
- Others

Netigy



Comments?

Questions?

Critiques!

Single Sign-On: Myth or Reality

Thomas R. Peltier, CISSP

Driving eBusiness Performance ***SM***