



## **A LOOMING IT CRISIS:**

# **INFORMATION DEGRADATION IN SERVICE-ORIENTED ARCHITECTURES**

A WHITE PAPER

Forum Systems, Inc.

BOSTON, MA  
95 Sawyer Road, suite 110  
Waltham, MA 02453

SALT LAKE CITY, UT  
45 West 10000 South, suite 415  
Sandy, UT 84070

TOLL FREE  
1-866-333-0210

[WWW.FORUMSYSTEMS.COM](http://WWW.FORUMSYSTEMS.COM)



## TABLE OF CONTENTS

YOU'RE INFORMATION AT THEIR FINGERTIPS...	3
WHAT IS 21ST CENTURY INFORMATION DEGRADATION?	4
SERVICE-ORIENTED ARCHITECTURE AND INFORMATION SHARING	5
HOW TO PREVENT INFORMATION DEGRADATION WITHIN SOAs	7
FORUM SYSTEMS: SERVICE-ORIENTED SECURITY SOLUTIONS	9
<i>FORUM'S SOA SECURITY BEST PRACTICES</i>	9
<i>FORUM SECURE SOA INFRASTRUCTURE</i>	11

Author: Walid Negm  
Vice President of Marketing  
Forum Systems Inc.

Release Date: 6/01/2005





## YOU'RE INFORMATION AT THEIR FINGERTIPS...

A growing number of major institutions are finding themselves on the front page of newspapers in stories of stolen corporate data and violations of consumer privacy. Companies such as HSBC, Bank of America, MasterCard, ChoicePoint and Lexus Nexus were just some of the recent victims of online security breaches. In the case of ChoicePoint, a data broker, confidential credit card information and other reports on more than 150,000 consumers were exposed to con men posing as legitimate customers.

In another incident, a hacker was able to access 40 million credit card numbers by infiltrating the network belonging to CardSystems Solutions, a company that specializes in the processing of payment data. MasterCard International investigations revealed that CardSystems had certain vulnerabilities that allowed unauthorized outsiders to access the card numbers, 13.9 million of which were connected to MasterCard.

While online security breaches vary, identity theft, information leakage and malicious software attacks are the most common and costly. The Federal Trade Commission (FTC) has estimated that, during 2003, almost ten million Americans discovered that they were the victims of identity theft, with a total cost to businesses and consumers approaching \$50 billion<sup>1</sup>. In 2005, the damages due to computer virus attacks were estimated at \$55 billion worldwide<sup>2</sup>.

And these numbers are on the rise. In a recent report, Gartner Group estimated 70 percent of the attack paths against Internet-connected systems that were closed by network firewalls will be reopened in 2005. This prediction has already been validated during the first quarter of this year in which US companies disclosed considerable business impacts:

- Stock price drops of 15% first day of trading following disclosure
- Liability exposure exceeding 78% of enterprise value (insured)
- Write-off 1% of Gross Margin<sup>3</sup>

It is unfair to classify these institutions as being simply negligent; instead we point to fundamental changes in business practices caused by Internet technologies and most recently through the adoption of Service-Oriented Architectures (SOAs). This white paper reviews the transformative effects that SOAs have on information and how to prevent data from natural losses or falling into the wrong hands.

---

<sup>1</sup> FDIC 2003 study, <http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html>;

<sup>2</sup> news.zdnet.com, 1/16/04

<sup>3</sup> Dow Jones Newswire, Companies Pay a Price For Security Breaches, 2005



## WHAT IS 21ST CENTURY INFORMATION DEGRADATION?

We should first differentiate between data and information. Data is the raw material while information is data assembled in meaningful ways. For example, customer records in a database may contain a customer's name, social security number and postal address each of which can be referred to as "data". A customer profile that aggregates this data into a specific context and presentable form is considered "information."

The traditional definition of information degradation refers to data that fades away on storage devices becoming completely or partially irrecoverable. However, today's information is extremely dynamic in nature: constantly shared, edited, updated and modified. The need to account for the integrity of data as it is being transported, shared and consumed has now become a business mandate.

**Information degradation** is defined as an organization losing data quality due to **corruption, irrelevance, or inconsistency** that can prohibit the organization from accurately performing vital business functions. Information degradation can be caused intentionally by criminals, natural disasters, hardware and software failures, human errors, or due to software design flaws.

QUALITY FACTOR	IMPACT ON INFORMATION	CAUSE OF DEGRADATION
<b>CORRUPTION</b>	Update, modification or deletion of data from its original and accurate form; loss of data fidelity or signal. Accidental or malicious	<ul style="list-style-type: none"><li>• Unauthorized data write, mangling, substitution; breach of trust</li><li>• Physical or virtual data lose</li><li>• Fraud &amp; deception e.g. using identity theft</li></ul>
<b>RELEVANCE</b>	Nullification or jeopardizing the usefulness of data. Accidental or malicious	<ul style="list-style-type: none"><li>• Unauthorized data viewing/reading; breach of trust</li><li>• Data theft: physical or digital</li><li>• Prevention of the timely delivery of data; Manipulating timing of execution i.e. check knitting</li><li>• Placing data into incorrect contexts</li><li>• Violation of digital rights</li></ul>
<b>CONSISTENCY</b>	Inability to ascertain the accuracy of data over time and across different regions. Accidental or malicious	<ul style="list-style-type: none"><li>• Transactional or database integrity failures</li><li>• Synchronization issues</li><li>• Service level or policy violations</li><li>• Version control failures</li></ul>



## SERVICE-ORIENTED ARCHITECTURE AND INFORMATION SHARING

Over the last 20 years, enterprises have moved from mainframes, to client-server computing and now to distributed n-tier architectures. This transition has impacted how data is created, stored and shared:

- **Decentralized databases:** A single purchase order may involve pulling data from multiple databases, on different servers across different geographic regions.
- **Increased data requirements:** Data collection technologies such as RFID are creating massive amounts of digital data that must be managed on a timely basis.
- **More places for data to go:** Routing of data across enterprise boundaries can leave more footprints across potentially un-trusted sites.

Service-Oriented Architecture builds upon distributed computing by adding a framework for the modularization of applications and processes using open standards. The Extensible Markup Language (XML) is clearly the most enabling technology of SOAs. Service-orientation has a significant impact on data and ultimately its accessibility as information:

- **SOA disaggregates data:** SOAs are designed to bring distributed data together. CapitalOne can receive an on-line loan application; which automatically triggers a request for a credit check from a company like Experian. There is no need for CapitalOne or Experian to keep customer information in their centralized databases. Both companies can directly query from vendors who keep updated information.
- **SOA standardizes data and metadata:** For SOA to succeed, software must be able to “talk” to one another and that language of common communication is XML. SOA requires open semantics and non-proprietary data formatting and XML provides this. It’s an XML world: Industry specific vocabularies (e.g. Accord, Swift etc.); security specifications (e.g. XML Encryption, Web Services Security) and data about data or “metadata” (e.g. WS-Policy, WS-Addressing).
- **SOA makes data highly accessible:** Published specifications of how to access Web services are a key premise of useful SOAs. Discovering, locating and then “binding” to a published Web service is part and parcel of the vision of the service-oriented enterprise. These “business API’s” make data available in real-time and on-demand like never before.



Distributed computing and SOAs raise a number of security questions that can be tied back to data quality factors:

- **CORRUPTION:** If a document is sent to one organization that shares it with another, then how can one guarantee the integrity of the original content?
- **RELEVANCE:** If one of the granular operations that make up a composite Web service is made unavailable by a denial of service attack, how can you assure transactional integrity?
- **CONSISTENCY:** If a request for a quote is available by a number of public Web services, how does the consumer guarantee the authenticity and credibility of the result?

On the flip side, SOAs can also enhance the quality of data using the following technology and methods:

- **Web Services** can actually disguise data mappings and how a transaction will ultimately be completed. In malevolent settings the lack of process and computing visibility yields a safer environment. So while the social security number may be known, access to the purchase order request is not available.
- **Web Services Security** specifications are a key enabler in ensuring trust, authentication, authorization, interoperability, confidentiality, integrity and non-repudiation
- **Web Service Description Language (WSDL) and XML Schema's** offers a consistent and well-known method of interacting with data that can avoid the errors associated with using proprietary interfaces and data formats
- **SOA Governance** advocates the reliance on enforceable policy specifications that are not present in traditional application development methodologies
- **SOA Registry** promotes shared business rules and metadata that encourages consistent data across applications



## HOW TO PREVENT INFORMATION DEGRADATION WITHIN SOAS

Even though emerging innovative technologies are often a major competitive advantage, organizations must still actively manage risks associated with them. It is dangerous to argue that since no exploit has taken place a threat does not exist. Enterprises that wait for a vulnerability to turn into a real threat may suffer irreversible setbacks to their competitive advantage in the marketplace

Preventing information degradation within SOAs should be proactively undertaken by adopting the following service-oriented security measures:

1. Data-level security mechanisms
2. Scrutiny towards internal security
3. Vulnerability management and risk assessment
4. Enterprise policy management

### 1. Data-Level Security Measures

Standardized data-level (granular and fine-grained) security on documents, messages and transactions is needed to address integrity, confidentiality, authenticity and authorization of information within SOAs.

XML is becoming the most prevalent data format moving across networks and processed by business applications and data centers. In light of this, specialized measures to inspect, examine, analyze and secure XML need to be put into place to safe guard integrity and prevent degradation.

Recommendations:

- Self-descriptiveness of security entitlements/attributes
- Context-dependant policy enforcements
- Specification of privacy preferences and policies
- Privacy preserving protocols
- Dynamic trust interactions
- Formalized evidence collection

### 2. Vulnerability Management and Risk Assessment

Once data-level security is fully established organizations should actively look at flaws or weaknesses in SOA design and implementation to pre-empt potential threats. This is even more critical in a loosely coupled and federated SOA environment where vulnerabilities can start a cascading chain of data loss.



Recommendations:

- Web services vulnerability testing
- Risk scoring
- Specialized risk analysis - threat discovery
- Vulnerability metabase and alert notification systems
- Threat detection / threat avoidance / threat tolerance
- Anomaly-based and self-learning

### **3. Internal Security Scrutiny**

This means moving beyond the front-door alarm system to installing countermeasures for “bad” behavior by the employee, contractor or malicious user across the SOA. A required key assumption is that the network perimeter is no longer the fail-safe checkpoint beyond which unrestricted trust should be granted. Enterprises should continuously collect and use evidence to ascertain the ongoing trustworthiness of users.

Recommendations:

- XML virus propagation protection
- Enterprise application integration security
- Application intrusion prevention
- Behavior, intent and pattern recognition
- Software development life cycle management

### **4. SOA Policy Management**

When constructing an SOA, the notion of policy should be a starting point in understanding how an organization functions both internally and externally. Whether IT focuses on security, transactions or liability, SOA policy management should be driven top down and reconciled bottom-up.

Recommendations:

- SOA policy governance
- Compliance management and enforcement
- Safe and secure cryptography
- Application-level audits



## FORUM SYSTEMS: SERVICE-ORIENTED SECURITY SOLUTIONS

Since all clients and service/resource providers participating in an SOA setting have to install some sort of XML component, hackers and malicious users are free to discover vulnerabilities resident in XML parsers, WSDL<sup>4</sup> end-points and SOAP<sup>5</sup> processors. More over, client/server and Web application security controls were not designed for a threat profile brought on by a constantly evolving set of XML-related specifications. The limitations in traditional security controls lies in their inability to inspect and act upon machine-to-machine interactions that use XML, SOAP and the WS-\* OASIS<sup>6</sup> standards.

Forum Systems is the leader in Web Services and SOA security with solutions that address both trust management as well as threat protection against a growing list of security concerns:

- Parameter Tampering: Manipulated XML values are used to conduct fraudulent transactions
  - Coercive Parsing: Corrupted XML/SOAP messages are used to disrupt and disable unprepared and vulnerable services
  - Recursive Payload: Deeply nested XML documents are constructed to exhaust computing resources
  - WSDL Scanning: Business API's are probed for sensitive data and vulnerabilities
  - External Entity Attacks: External references can be made to import compromised data
  - SOAP Routing Detours: Messages are re-directed to malevolent processing intermediaries
  - SOAP with malicious software: SOAP hides and obscures viruses, spyware and other unwanted programs
  - SQL Injections into SOAP: SQL code is modified and left undetected because it is embedded in XML
  - WS-Security Spoofing: SOAP security contexts are overridden to gain unauthorized data access
- SOA Security Best Practices

### SOA SECURITY BEST PRACTICES

Forum Systems strongly recommends that security be integral to SOAs. SOA security must explicitly address XML data security requirements beyond transport and user protections. SOA security must support confidentiality, authentication, integrity, authorization and non-repudiation of service-to-service interactions using self-descriptive entitlements and attributes. SOA security must also address XML-related vulnerabilities to avoid impending threats.

---

<sup>4</sup>W3C Web Services Description Language

<sup>5</sup>W3C Simple Object Access Protocol

<sup>6</sup>Organization for the Advancement of Structured Information Standards (OASIS)



The following list of SOA security best practices:

- **Web Services and XML Security Standards:** Adoption of Open specifications of the World Wide Web Consortium (W3C), Organization for the Advancement of Structured Information Standards (OASIS) for the enforcement of confidentiality and integrity of Web services
- **XML Threat Prevention:** Deep inspection, validation, monitoring and filtering of Web services and XML transactions. Actively defending and avoiding against pattern and signature-recognizable XML-vectored attacks, intrusions and malicious software
- **Security Policy Management:** Management and the governance of rules must be derived from business, organizational and enterprise requirements. Centralized Policy Decision Points (PDP) as well as distributed policy Enforcement Points (PEP) need to be deployed
- **Authentication:** Verifying proof of an asserted identity; authentication should be facilitated and resolved using transport (e.g. SSL X.509 Certificates) as well as message-based protocols (e.g. SAML/WS-Security Assertions)
- **Identity Mapping:** Transforming an identity that exists in one domain to an identity within another domain
- **Authorization:** Resolving a policy based on access control decision.
- **Credential Conversion:** Provides mapping of one type of credential to another such as an X.509 Certificate to a Kerberos/WS-Security token
- **Trust Delegation:** Bridging the differences between mechanisms associated with authentication, assertions and entitlements to enable a federated trust model
- **Audit:** Tracking, monitoring and reporting of security related events
- **Privacy:** Policy driven enforcement of personally identifiable information using both transport (e.g. SSL session encryption) as well message-based protocols (e.g. XML-Encryption)
- **Safe and Secure Cryptography:** Private keys and passwords once compromised void the trust model that depends on them. A secure SOA must offer robust and tamper resistant storage of private keys, passwords and algorithms.
- **Vulnerability Management and Risk Assessment.** Organizations should actively look at flaws and weaknesses in SOA design and implementation to pre-empt potential threats.





## FORUM SECURE SOA INFRASTRUCTURE

Security must be integral to an SOA because it changes the way information is created, shared and destroyed. SOA security needs to explicitly address XML data security requirements beyond transport and user protections. SOA security must support confidentiality, authentication, integrity, authorization and non-repudiation of service-to-service interactions using self-descriptive entitlements and attributes. XML-related vulnerabilities must also be addressed by SOA security in order to avoid impending threats.

Forum Systems SOA life-cycle security solutions enable trust management, threat protection and information assurance of XML, Web Services and Service-Oriented Architectures. The following sections describe Forum's market-leading capabilities that are deployed within the world's largest and most discerning telecommunications, financial services, e-retail, and US Federal Government organizations.

**For more information on Forum XWall Web Services Firewall and other SOA security products please visit [www.forumsys.com](http://www.forumsys.com)**

### **Adaptive Hardware and Software**

SOA security aspects must be considered at the edge of the network; within the datacenter as well as at end-points and application containers. Forum Systems offers organizations the flexibility to mix hardware and software where they are needed for the most effective security environment and at the lowest cost of ownership.

- Hardware: 1U Appliance, IBM eBlade, PCI cards, x32-bit, x64-bit
- Third-Party Platforms: Microsoft ISA Server 2004, Crossbeam, NetContinuum, Network Engines
- Software: Windows, Linux, IBM AIX, Sun Solaris, Sun Trusted Solaris

### **Hardened Security Assurance**

FIPS (Federal Information Processing Standard) is a US Government certification program that prescribes detailed security requirements for cryptographic-based systems when used within US Federal agencies. FIPS is also important to the Canadian government including many governments in Europe. In sensitive SOA settings, security policies need to be processed inside FIPS 1402- Level II certificated enclosures from the hardware chassis, cryptographic modules, motherboard & interfaces.

- FIPS 140-2 Level III Key Management
- Full Appliance Chassis FIPS 140-2 Level II Validation
- DoD/PKI Certification
- Common Criteria EAL 4+



### **Intelligent XML Malware Protections**

Analyst's project XML-based network traffic will grow from 15 percent in 2004 to almost 50 percent in 2008. This explosive growth has opened the door for virus writers to bypass firewalls and anti-virus scanners that cannot recognize XML's data format and security context. Forum Systems was the first to introduce XML malware protection for security countermeasures against XML-vectored viruses, worms and unwanted programs.

- Real-time XML virus and malware scanning
- Automatic anti-virus updates
- Large binary attachments support
- SOAP with binary attachment processing (DIME and MIME)