

FORUM SYSTEMS INC.

WHITE PAPER

# **SSL: Not Enough for Today's Web Services**

---

© Forum Systems Inc.  
40 Williams Street • Suite G20  
Wellesly, MA 02481  
Phone 781-263-5400 • Fax 781-263-5401

45 West 10000 South • Suite 415  
Sandy, UT 84070  
Phone 801-313-4400 • Fax 801-313-4401



# Table of Contents

Executive Summary.....pg 2  
SSL: Not Enough.....pg 3  
Why Is XML Data Vulnerable.....pg 4  
The New Challenge of XML Security.....pg 5  
The Forum Systems Solution.....pg 6

## Executive Summary

As more and more businesses move their transactions and data across the Internet they are faced with a significant security gap - *How to guarantee the protection and security of business critical data over increasingly complex trading relationships and web services throughout the entire data lifecycle.*

Today, business to business integrations rely upon browser-based Secure Socket Layer (SSL) as the primary mechanism to secure business to business data exchanges. SSL provides excellent security between two entities by securing the communication channel at the packet data level. SSL does this by offering in-transit confidentiality (using encryption technology) between two SSL-enabled parties. Unfortunately, while this data sits on either end of the communication link, it is left completely unsecured. Today, corporations are exposing critical business data to theft and tampering as it lies vulnerable on web and application servers. The problem: SSL was never designed to secure Internet-based web services where transactions flow in a store-and-forward communication mode.

**This document addresses the need for a comprehensive security solution for today's Web Services.**

## SSL: Not Enough

### The Problem with SSL

SSL is great at what it was designed for- securing internet transactions during the session. It provides excellent security by encrypting everything while information travels along the internet superhighway from on-ramp to exit. But, how many car-jacking incidents happen while cars are moving along an expressway? None. They happen when stopped at a traffic light, in a club, or parked in an unsecured garage. It is quite the same with information. Few information-jackings happen while data is in transit. In fact the FBI estimates that over 70% of security breaches come from inside, when data is stored on networks, behind the firewall.

SSL is insufficient in the following, more specific ways:

- SSL is designed to work between point A and B. Often times in a business transaction, there are multiple points, C, D-Z.
- SSL is not data aware; it simply protects the entire document. This means that when a document reaches its destination, the entire document is automatically decrypted for all eyes to see.
- SSL begins and ends with a communication session- there is not persistent security, leaving information vulnerable where it is stored.
- SSL was never meant to handle the complex security needs of the Web Services environment.

## Why is XML Data Vulnerable?

Convinced that enterprises need more than the standard SSL? Good. Here is the reason that more precautions are needed when dealing with XML (eXtensible Markup Language). XML data is smart, content aware information. XML is the 'simplified' offspring of its complicated parent SGML (Standard Generalized Markup Language). It is human as well as computer readable. Without knowing XML one can decipher information easily. Take the XML document below for example, viewing it through the eyes of an intruder wanting to 'borrow' sensitive information.

```
<?xml version="1.0"?>
<!DOCTYPE customer_order SYSTEM "custord.dtd">
<customer_order>
  <items>
    <item>
      <name>Turnip Twaddler</name>
      <qty>3</qty>
      <price>9.95</price>
    </item>
    <item>
      <name>Snipe Curdler</name>
      <qty>1</qty>
      <price>19.95</price>
    </item>
  </items>
  <customer>
    <name>Doug Tidwell</name>
    <street>1234 Main Street</street>
    <city state="NC">Raleigh</city>
    <zip>11111</zip>
  </customer>
  <credit_payment>
    <card_issuer>American Express</card_issuer>
    <card_number>1234 567890 12345</card_number>
    <expiration_date month="10" year="2004"/>
  </credit_payment>
</customer_order>
```

The sensitive information such as the name, address, credit card number and expiration date are easy to pick out. The document even exclaims that 1234 567890 12345 is the card number. This is what is meant by content aware- the tags announce where information is. This is why XML data is vulnerable. But companies trust their trading partners, and their customers trust SSL. Do customers know that their credit card information is sent to multiple locations just to place an order for a compact disc? The Federal Trade Commission suggests:

*Keep your personal information private. Don't disclose your personal information - your address, telephone number, Social Security number, bank account number or e-mail address - unless you know who's collecting the information, why they're collecting it and how they'll use it.*

Without knowing the who, where, what and why's of e-shopping how can customers and vendors ensure the safety of consumer information? Without the knowledge of the customer or the e-store, information is made vulnerable.

## The New Challenge of XML Security

As more and more businesses move their transaction over the internet they are faced with a new challenge: how to guarantee that sensitive information will be protected as it moves between multiple trading partners, and when it is stored in databases and networks. Currently, while information sits on either end of a business transaction, it is left completely unsecured, exposing critical data to theft and tampering. If each employee that has access to information were trustworthy, and no one was tempted to steal information, the way e-business is done today would suffice.

Unfortunately this is not the case.

Some may choose to hire a personal security guard to protect their car while they are at work. Companies deploy firewalls to secure their information where it is stored. But, what happens when the security guard or someone that is trusted behind the firewall is the one 'borrowing' information? This is the real challenge facing e-business today. Remember, the FBI estimates that over 70% of theft happens from inside, behind the firewall- performed by someone that was trusted. So how do people make it so that their personal security guards cannot tell the difference between their Ferrari and the Geo parked next to it? The answer: data-level encryption. Make every car look exactly the same. There are no Ferrari tags, no Geo tags, just cars. No information more valued or more useful than the rest. Forum Systems provides you with the technology to make this happen- the ability to protect business critical information.

## The Forum Systems Solution

The Forum Sentry™ XML and Web Services Security Appliance meets the demands for security that is specifically designed for business data in a multiple-hop environment and Web Services by providing the four cornerstones of e-business security.

- **End-to-End Data Integrity:** Completeness and accuracy are the ultimate goals when sharing data in a complex computing environment. Forum Systems' Appliances can proactively detect when critical business transactions and data is touched or manipulated in-transit between multiple trading partners or while in storage. Forum Systems Appliances allow enterprises to apply authentication policies to targeted data elements within XML data and Web Services.
- **Data-Level Confidentiality:** Enterprise information must be kept safe from the global threat of interception. This goes for basic transactions as well as intellectual property being shared among business partners. Forum Systems Appliances provide "selective secrecy" when valuable data is being transmitted or stored in various places around the Internet.

- ❑ **XML Web Service Auditing.** Business intelligence starts with logging every business transaction entering and leaving the enterprise. Forum Systems Appliance transparently track the activities of Web Services as well as it's reliability and downtime. Forum Systems Appliances externally archive collected data to analyze security breaches, business operation performance and regulatory compliance.
- ❑ **XML Data Processing.** Web Services and XML data processing takes away valuable computer and network resources from Application and e-Business Servers. Forum Systems Appliances apply real-time XML operations such as Validation and Transformation at the edge of the network and forward the results on to the next destination.

In short, the Forum Sentry™ Security Appliance allows enterprises to selectively encrypt sensitive information in a document. Take the XML data example from before. In a typical transaction that document will be sent to the e-store, the bank, the credit card company, and any trading partners and clearinghouses. This significantly increases the risk of theft or tampering. Not everyone who will see the transaction needs to view the sensitive credit card information. The following example shows the same document after data level encryption:

```
<?xml version="1.0"?><customer_order>
  <items>
    <item>
      <name>Turnip Twaddler</name>
      <qty>3</qty>
      <price>9.95</price>
    </item>
    <item>
      <name>Snipe Curdler</name>
      <qty>1</qty>
      <price>19.95</price>
    </item>
  </items>
  <customer>
    <name>Doug Tidwell</name>
    <street>1234 Main Street</street>
    <city state="NC">Raleigh</city>
    <zip>11111</zip>
  </customer>
  <EncryptedElement
algorithm= "DES/CBC/PKCS5Padding"contentType="text/xml"
encoding="base64"v="S5Rirg//pNQ=">vJqNpDrQT1vmCVbyGJflwdIDBYoGXXGmutgz6TVGoPuKVG7IxNEN50iK
w8pmtxFixz5hOChOXgTtPqktQhEHO5+vLOLAFgIioDIRQGHHmHng3CLd+8tKVG7IxNEN50iKw8pmtxFixz5hOC
hOXgTtPqktQhEHO5+vLOLAFgIioDIRQGHHmHng3CLd+vrT8wxPBCRSMUpx4d2TGXW2tqSepam0ZxdmwUXw
NSAgaR8hmiromD+bh+tDomPv7eFZ4no5ft3JGwxPBCRSMUpx4d2TGXW2tqSepam0ZxdmwUXwNSAgaR8hmiromD
+bh+3t0t
rLJwVupF/5vaIJimUSuUkkgYg8x9AcS/kXJxHpmM=pecGzIMf+8A=</EncryptedElement></customer_order>
```

The information is now safe to share between all trading partners. Only the intended recipients will be able to decrypt the sensitive information. If there is attempted theft of Forum protected information, even if the hard drive is taken, the information will remain encrypted and protected. Without the key, it is impossible to decrypt.

Forum Systems Inc. develops and markets network security equipment that actively guards business-critical data as it moves between and within enterprises by protecting specific content within XML and non-XML Documents – securing information throughout the entire data lifecycle.

Using Forum Systems XML security infrastructure, Global 1000 companies, service providers, ISVs and systems integrators can build secure trading networks and web services for strategic applications such as: supplier procurement, financial exchanges and insurance processing.