Bracing your infrastructure for XML Web Services

Eugene Kuznetsov
Chairman & CTO
DataPower
Agenda

- Won’t talk about applications, software, tools or platforms…
- Web services are also about networks
- New protocols create new pressures and demands on existing networks
- Network infrastructure for Web services:
  - Network equipment
  - Network services
- Challenges
  - Performance
  - Security
  - Expense
- A new approach
Technology and Specifications

- **Foundation**
  - XML
  - SOAP
  - XPath/XSLT
  - XSD

- **Security Building Blocks**
  - XML Digital Signature
  - XML Encryption

- **Upper-Layer Protocols/Standards**
  - WS-Security
  - SOAP Security
  - XKMS
  - SAML
  - XACML

- **Not in themselves solutions**
  - Rapidly mutating
Performance Challenge

- XML is a text-based self-tagging format
- Same messages up to 20 times larger than binary
- Example:
  - 0xA13FF51301 [5 bytes] →
  - <?xml version="1.0" ?> <invoice><no>1001</no>
    <product><sku>150591501</sku></product></invoice> [95 bytes]
- Variable length fields, variable encodings
- Complex processing model – XPath, XML Security, SOAP
- Result:
  - Some XML apps literally grind to a halt
  - Website pages taking 10 seconds to load
  - More and more hardware required
Current Approach to XML Performance

- Buy more general-purpose server hardware
  - $ to purchase, $$$ to operate
- Avoid XML/SOAP for high-speed systems
- Use non-standard “subset” of XML
  - defeats interoperability, costs more in the end
- Cut out application features
  - undercuts business objective for using XML
- Hand-tune the XML processing software in the app
  - takes a long time for even minor improvements
  - expensive programming resources
  - every minute spent on “XML stack” is a minute not invested in core application

Need to make XML Web Services FASTER
Why Web Services Security?

- New connectivity → new risks
- How is XML/WS different than current systems?
- The very value of XML Web Services comes from connecting sensitive systems
- Technology much more flexible and powerful than previously widely deployed
- SOAP designed to bypass existing network security infrastructure
- “Implementation of Microsoft SOAP, a protocol running over HTTP precisely so it could bypass firewalls, should be withdrawn. According to the Microsoft documentation: "Since SOAP relies on HTTP as the transport mechanism, and most firewalls allow HTTP to pass through, you'll have no problem invoking SOAP endpoints from either side of a firewall." – Bruce Schneier
- Why is SOAP designed to do this?

Need to make XML Web Services SAFER
“Internal” Systems

- A lot of XML and XML web services “inside the firewall” → no security needs?
- Erosion of enterprise perimeter
- Pilot mode web services
- Insider attack risk
- “Semi-trusted” environments
- Regulatory / policy requirements
- Internal → external (intentional or not)
- Unattractive architectural choices
  - Spend time upfront on security
  - Get pilot up and audit/secure code later
XML Security Challenges

- New technology, rapidly changing standards
  - Lack of strategic clarity, lots of marketing noise
  - Many immature products and architectures
  - Getting and staying on top technology changes, training staff
  - Very broad set of potential threats

- Organizational challenges
  - Who is responsible for XML/WS security?
  - Pressure to get new apps into production
  - Trading partners, business units

- Is there anything rational to be done?

- Architectural choices
  - Spend a lot of time upfront on security?
  - Get pilot app up and audit/secure code later?
  - Code all XML security into the app?
  - Write one’s own XML proxy software, install on server in DMZ?
  - Who would manage security operations in production?

- A security breach is very expensive

Need to make XML Web Services SAFER
New Approach to XML challenges
Offload to XML-Aware network devices
XML-aware Network Infrastructure

The
- Performance
- Security
- Manageability

that you expect from your IP network for your XML apps
XML-Aware Network Devices

- New type of content-aware networking equipment
  - capable of XML-processing, SOAP support
  - New name: “WS-aware”, or “XML-aware”, or “XML-router”..
- Network hardware capable of parsing and processing XML data streams
- SOAP load balancer
- XML firewall, XML security gateway
- XML accelerator/off-loader
- WS billing / payment processor
"I really only need to deal with the business part of the XML message payload, and all the other stuff should go into the infrastructure. I used to parse HTTP-Post messages but I don't do that today, the infrastructure does that for you."

TN Subramaniam
CTO, RouteOne
Benefits of the XML-aware Networking Approach

- **CIOs & CSOs**
  - Cut ownership costs
  - Shift to message-level security
  - Leverage current investments

- **Application Architects**
  - Separation of concerns
  - Reduced debugging cycles
  - Simplified deployments

- **Network Managers**
  - Instant XML-aware security, routing without programming
  - Improved reliability, scalability, manageability
  - Fewer servers and less complexity
“Performance has challenged XML implementers since we introduced XML in 1998. I knew new technologies would overcome the challenge and allow developers to take full advantage of XML and Schema based validation. [XML-aware network technologies] make it practical to truly take advantage of XML throughout the enterprise.”

Dave Hollander
Co-Inventor of XML
XML-Aware Networks

• **XML-aware network equipment**
  - XML accelerators
  - XML routers
  - XML firewalls
  - XML security gateways
  - Policy execution & enforcement points
  - A scaleable model for message-level security and policy

• **XML-aware network services**
  - Value-added networks for the 21st century
  - Powered by XML-aware network equipment and registries
  - Services themselves are invoked via messages

• **XML-aware network is SOA component**
XML Accelerators

- Offload XML Processing to dedicated Network Hardware
- Schema Validation
- XML Transformation, XSLT
- Compression
- Legacy↔XML Conversion
- XML Parsing Acceleration

Hardware-based XML acceleration applicable to broad variety of XML processing.
XML Routers

- Content-based routing based on dynamic XPath tables
- SOAP protocol routing and load balancing
- Message enrichment via headers
- Publish-Subscribe based on content in messages
- Message duplication & relay
- QoS and QoP based on message content
- Routing and delivery independent of producers or consumers

XML Routing distributes information in a content-aware pub-sub intelligence network for analysis.
XML Security Gateways, XML Firewalls

- **XML/SOAP Firewall**
  - Filter on any content, metadata or network variables
- **Data Validation**
  - Approve incoming/outgoing XML and SOAP at wirespeed
- **Field Level XML Security**
  - Encrypt and sign individual message fields, non-repudiation
- **XML Web Services Access Control**
  - Authenticate, Authorize, Audit, integrate w. existing systems
- **MultiStep & XML Routing**
- **Transport Layer Flexibility**
  - SSL acceleration, message queue connectivity, non-SOAP
- **Service Virtualization**
- **Configuration & Administration**
“XML firewalls free application developers from having to protect their apps against every possible type of attack. They also ease the task of managing cryptographic operations on XML...the XS40 has wire-speed XML processing capabilities almost 10 times faster than software-based XML processing solutions.”

Phillip J. Windley
InfoWorld Test Center
XML Security Deployment Ecosystem

- External PKI infrastructure: CA servers, services
- Application Infrastructure: web servers, application servers, integration servers
- Management Infrastructure: systems, network, security and logging
XML Security is XML Processing

- Security of the XML engine controls security of an XML firewall
- Performance is key to security
  - Each security function requires XML processing
  - Must implement all practices without any compromise
  - Need ability to scale as content and user base grows
XML-Aware Networking centralizes security

- Benefits of moving message-level security into the network
  - Secure multiple apps without multiple code changes
  - Boost performance while reducing cost and complexity
  - Perform security functions *before* they reach app servers

<table>
<thead>
<tr>
<th>Distributed</th>
<th>Centralized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update thousands of app servers individually</td>
<td>Secure all apps instantly</td>
</tr>
<tr>
<td>No new coding</td>
<td></td>
</tr>
</tbody>
</table>

- New firewall filter
- Secure auditing
- Key revocation
- New XML standard
- Access control update
- Change purchase order schema

HP World 2004 Solutions and Technology Conference & Expo

22
“Integrating MQ with a reliable, high-performance security gateway is a tremendous advantage for our customers needing to securely integrate with partners over the Internet.”

Rachel Helm
Director, WebSphere Product Management, IBM
XML-Aware Network Services

- New “in-the-network” services for WS
- Directories/registries of web services, UDDI, etc.
- Edge processing and acceleration
- Guaranteed delivery of XML docs & transactions
- Cryptographic tokens and PKI certificates
- Managed security service providers for WS
- Fully outsourced deployment infrastructure
- Web Services Networks (WSN’s)
XML hardware encourages interoperability

- Coupled to the other systems by Ethernet jack, not custom code
- Separation of concerns
- Network gear business model based on “out-of-the-box” interop
- Large software vendors focused on creating XML-enabled platforms
  - Functionality and development tools benefit
  - Interop is necessarily secondary, standards wars looming
- Network vendors architecturally unable to achieve “lock-in”
- Focused on a concrete set of challenges
  - XML security performance
  - Interoperability.
Conclusion

- **Bad**
  - Scalability: XML is bandwidth, CPU and memory intensive
  - Performance: some XML apps literally grind to a halt
  - Insecure: connecting systems never before connected
  - Insecure: clear text over HTTP with no inherent security
  - Standards are still in flux
  - Financial, technical and organizational challenge

- **Good**
  - Dramatically lowering cost & time for EAI / b2b
  - Flexible websites and one-source publishing
  - Code reuse, easy debugging
  - XML is foundation for web services
  - Broadest industry support since HTTP

- **Conclusions**
  - Separate security, acceleration, routing from the application logic
  - Centralize security in network
  - Can use XAN to make XML Web Services FASTER, SAFER and CHEAPER