

Threat Protection in a Service Oriented World


Andre Yee

CEO, NFR Security



(nfr)(security)

Web Services is Mainstream and Growing...



IDC estimates web services market growing to \$21.6B by 2009



87 of top 100 CIOs polled say that they are currently leveraging web services

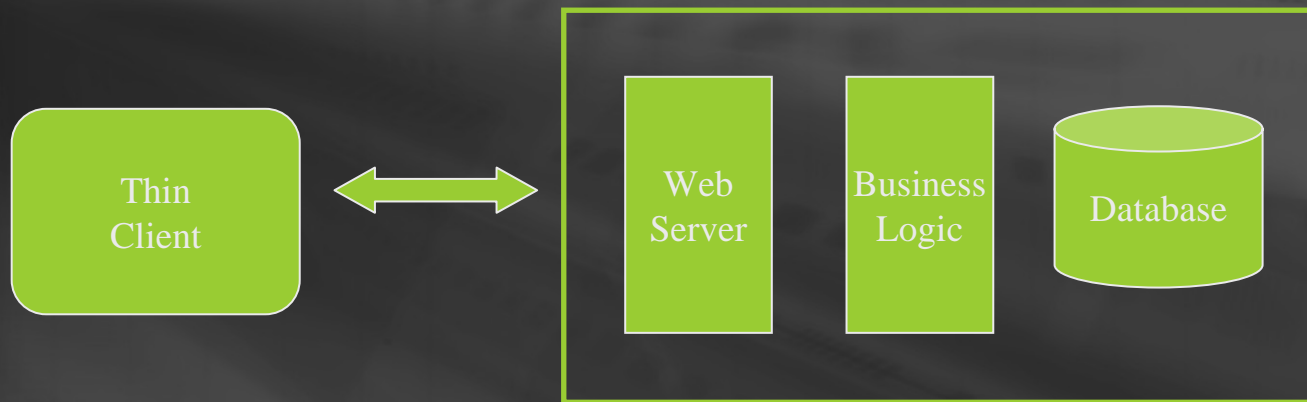
Goldman Sachs Survey, 2005

42% respondents endorsed SOA as the standard template for application development...same number cited security as chief concern...

Intelligent Enterprise Survey, 2006

“Simple” Web Application

- Monolithic
- Proprietary Message Format, HTML
- HTTP
- Web Server
- Simple Scripted Business Rules

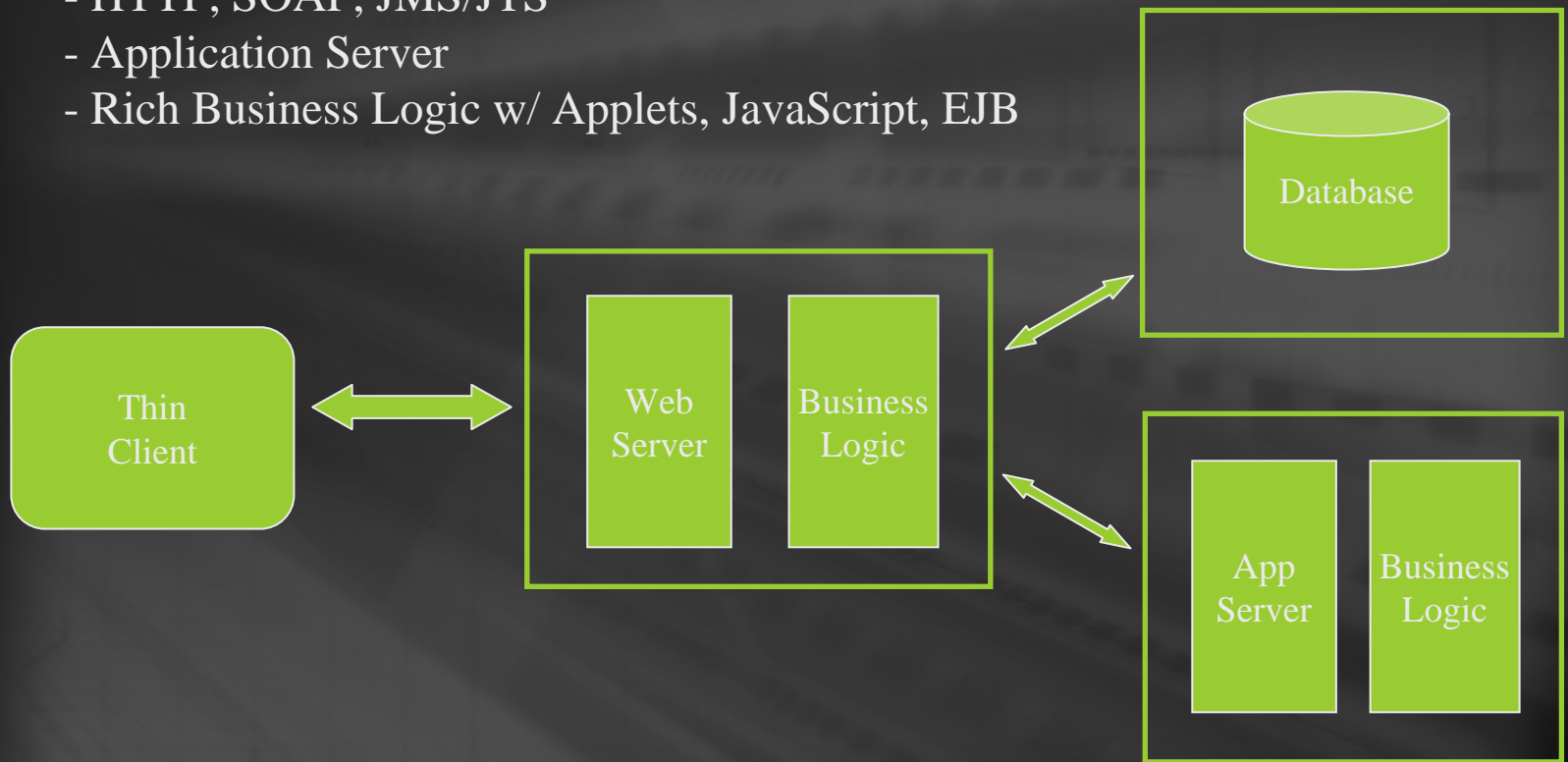


Security Challenges

- Effectively Monitoring Port 80
- Initial Attacks Targeting Web Servers
 - Denial-of-Service
 - Buffer Overflow
 - Unsecured Privileges/Directory Traversals
- Evolving to Web Application Attacks
 - SQL Injection via Web Interface
 - Parameter Manipulation
 - Cookie Tampering
 - Malicious scripting/Cross Site Scripting

"Federated" Web Application

- Federated, Intra-Enterprise, Scalable
- XML 1.0, Proprietary Message Format
- HTTP, SOAP, JMS/JTS
- Application Server
- Rich Business Logic w/ Applets, JavaScript, EJB



(nfr)(security)

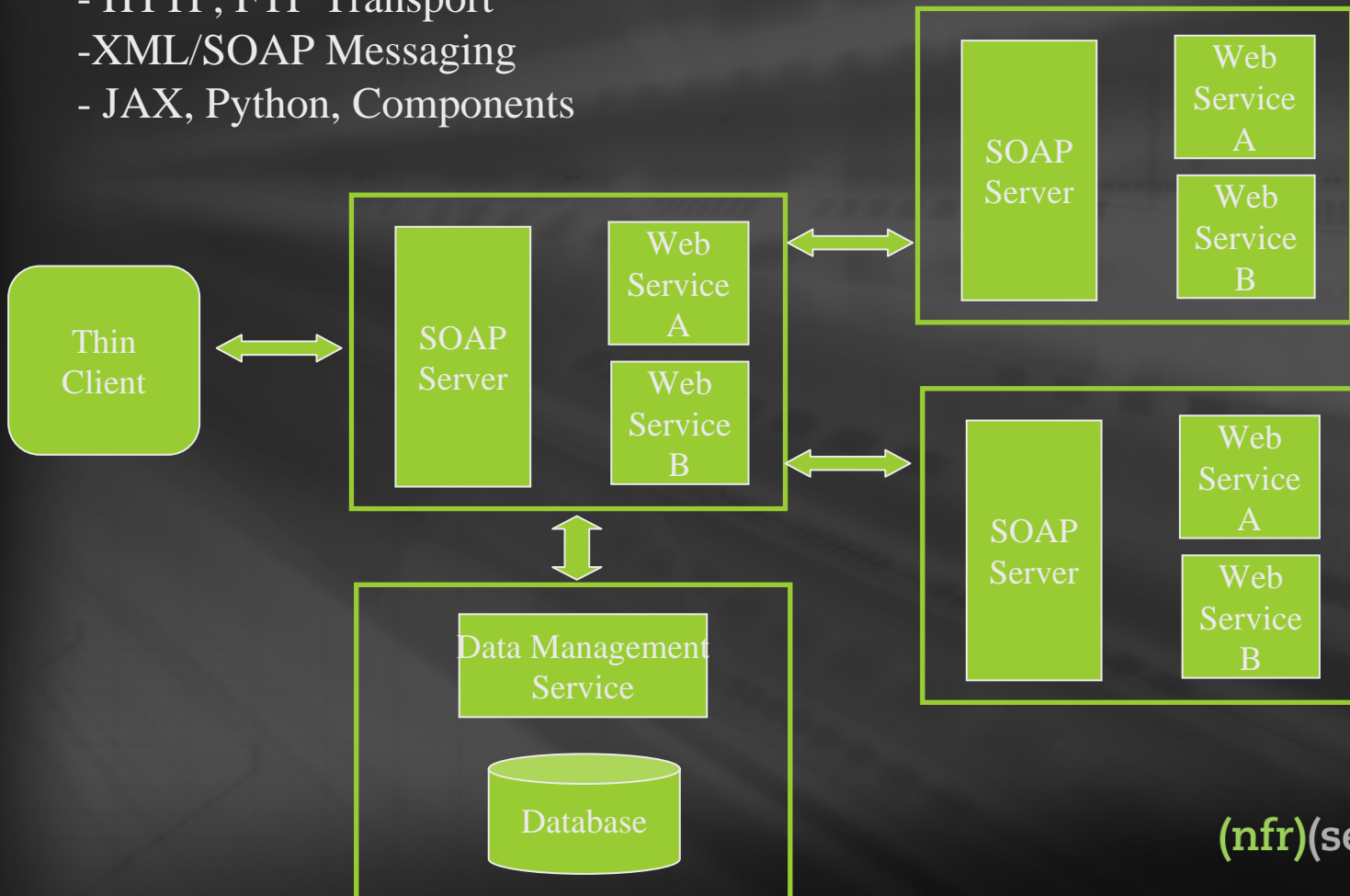
Security Challenges



- Single Sign-On
 - Delegating credentials to other services or resources
 - Example: web server to application server to database server
- XML Content Attacks
 - Recursive/Nested Payloads
 - Jumbo Payloads
 - Coercive Parsing
- Application Server Vulnerabilities
 - Example: Weblogic vulnerability/T-Mobile hack
- Reverse Engineering Components
 - Example: compromise client-side sign-on applet

Service Oriented Architecture

- Distributed, Inter-Enterprise
- Loosely coupled
- HTTP, FTP Transport
- XML/SOAP Messaging
- JAX, Python, Components



SOA Security Challenges - The Big Picture

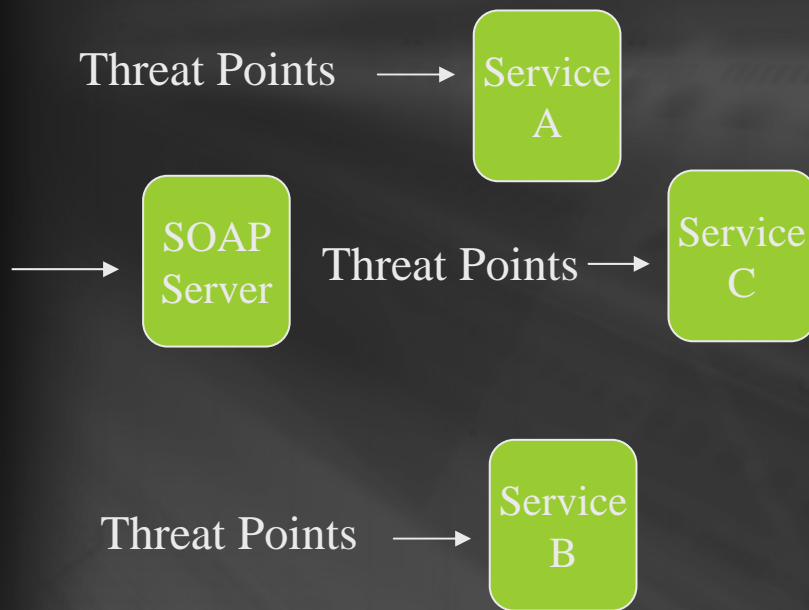
- Architecture Patterns
- Transactional/Messaging
- XML Based Threats



ocus)(know
sted)(focus
able)(truste
ful)(scalable
powerful)(s
ed)(powerf
nced)(pow
advanced)
nsive)(ac
(respon

Security Challenges - Architecture Patterns

SOA Results in Multiplication of Interface Points
=> Multiplication of Potential Threat Points



- Secure core web services against attack
- Contain attack and limit proliferation

Security Challenges – Architecture Patterns

SOA Results in Multiplication of Interface Points
=> Multiplication of Potential Threat Points

Threat Points →



Threat Points →

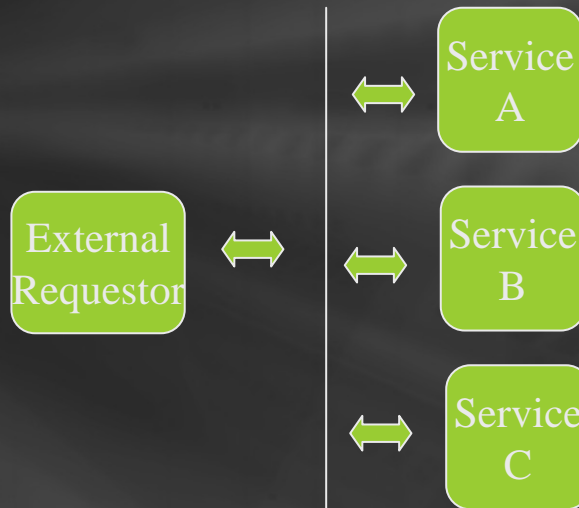


Countermeasure:

- Create internal protection zones for similarly typed services and/or critical services
- Protect each zone with inline intrusion prevention...tuned for endpoint services...

Security Challenges – Architecture Patterns

SOA Increase Complexities for Protecting Internal Services While Servicing External Requestors

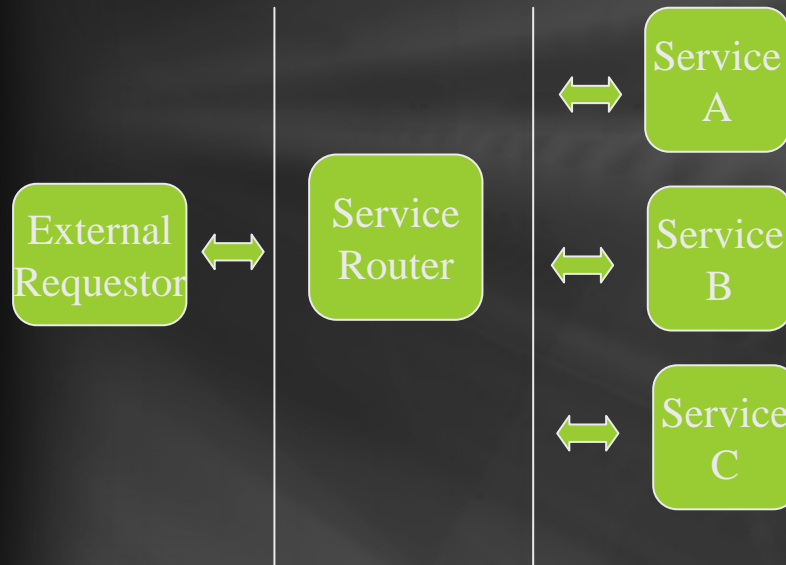


- Service external client requests leveraging multiple internal services
- Protect internal resources against external attackers
- Contain and limit attack

Externally facing services

Security Challenges - Architecture Patterns

SOA Increase Complexities for Protecting Internal Services While Servicing External Requestors

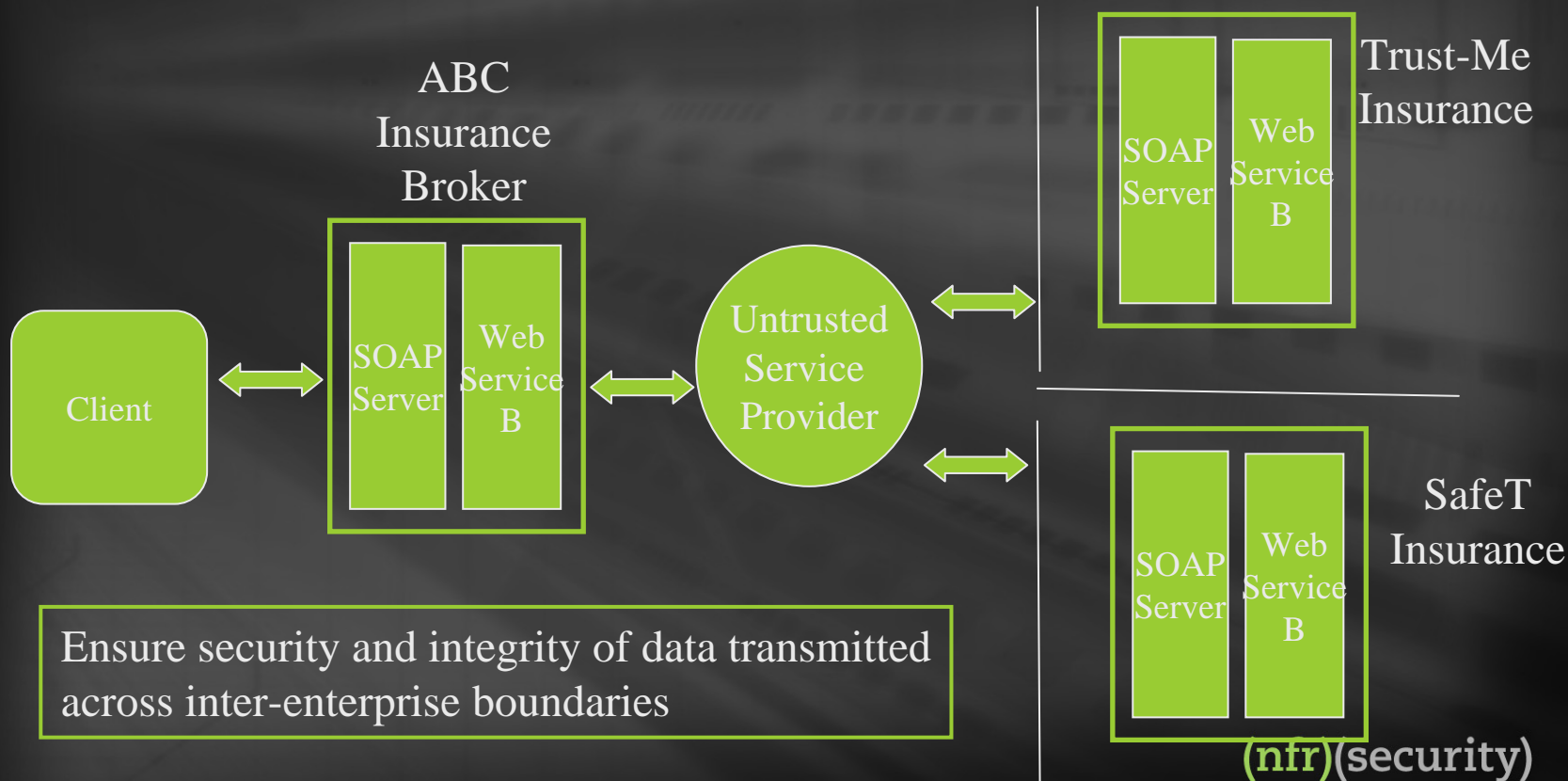


Countermeasure:

- Deploy service router on the perimeter
- Reinforce multi-layer security with IPS, XML firewalling

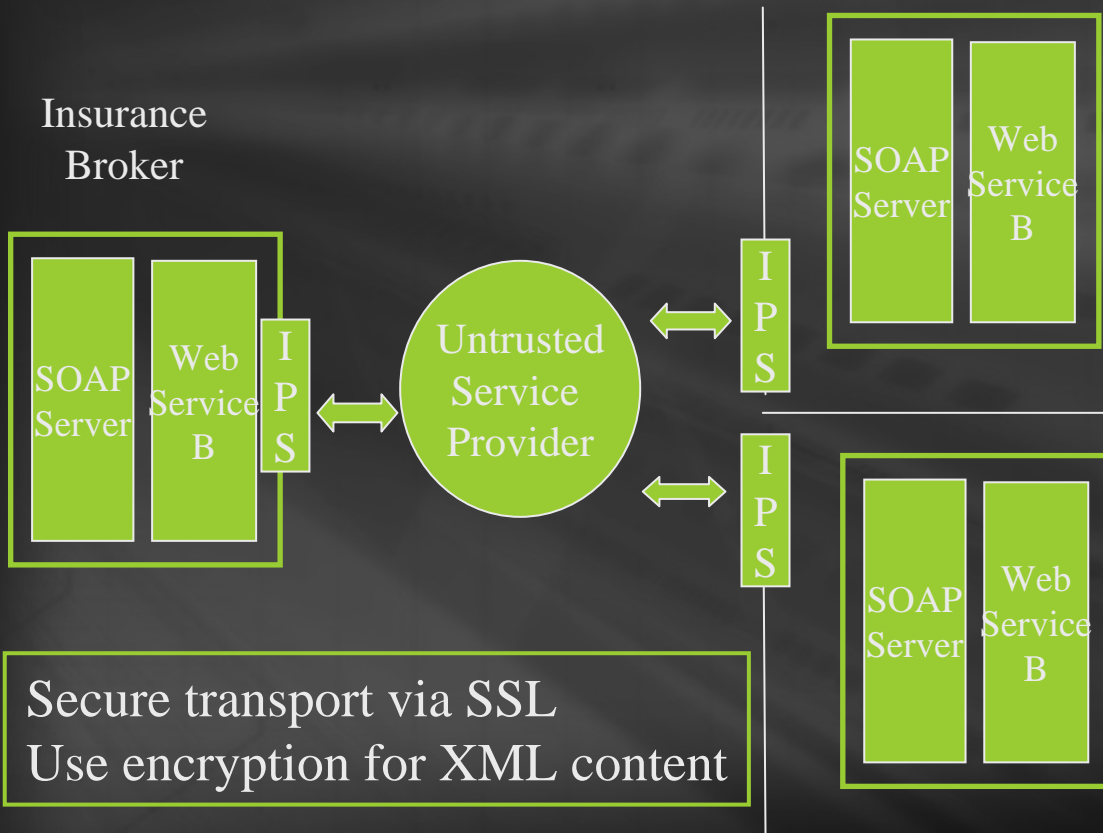
Security Challenges - Transactional Issues

SOA Inter-Enterprise Transactions May Traverse Untrusted Segments and Use Proprietary Protocols for Business Transactions



Security Challenges - Transactional Issues

SOA Inter-Enterprise Transactions May Traverse Untrusted Segments and Use Proprietary Protocols for Business Transactions

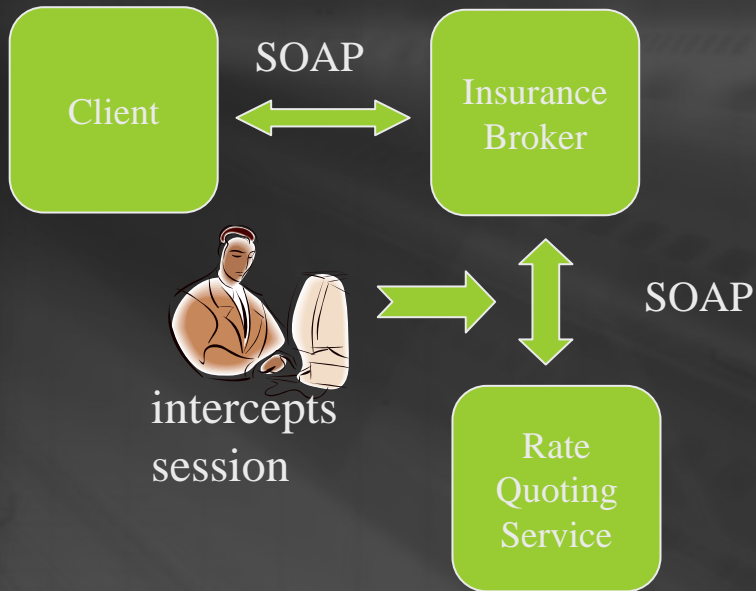


Secure transport via SSL
Use encryption for XML content

- Countermeasure:
- Deploy intrusion prevention at all trust points
 - Validate proprietary data exchange protocol
 - XML inspection

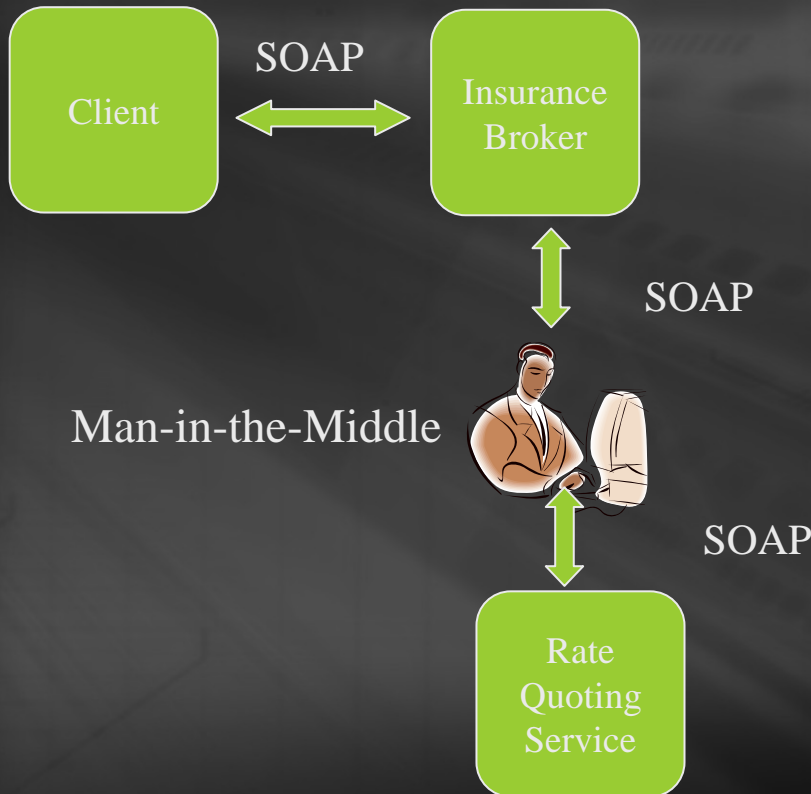
Security Challenges - Transactional Issues

Multi-hop Routing Susceptible to Man-in-the Middle Attacks and Tampering



Security Challenges - Transactional Issues

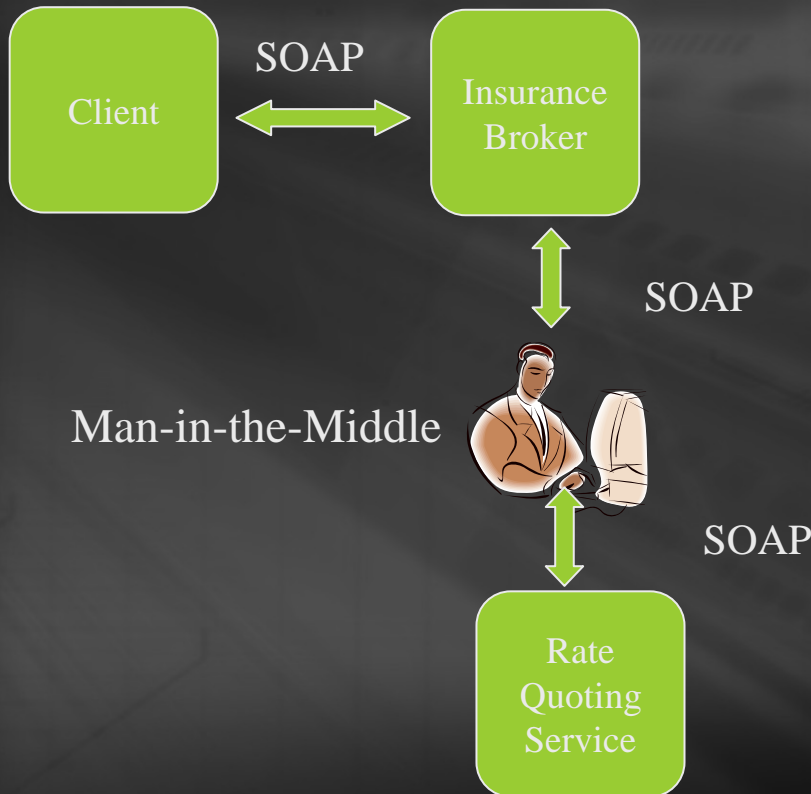
Multi-hop Routing Susceptible to Man-in-the Middle Attacks and Tampering



- XML tampering
- Changing of security credentials
- Regulatory compliance issues abound

Security Challenges - Transactional Issues

Multi-hop Routing Susceptible to Man-in-the Middle Attacks and Tampering



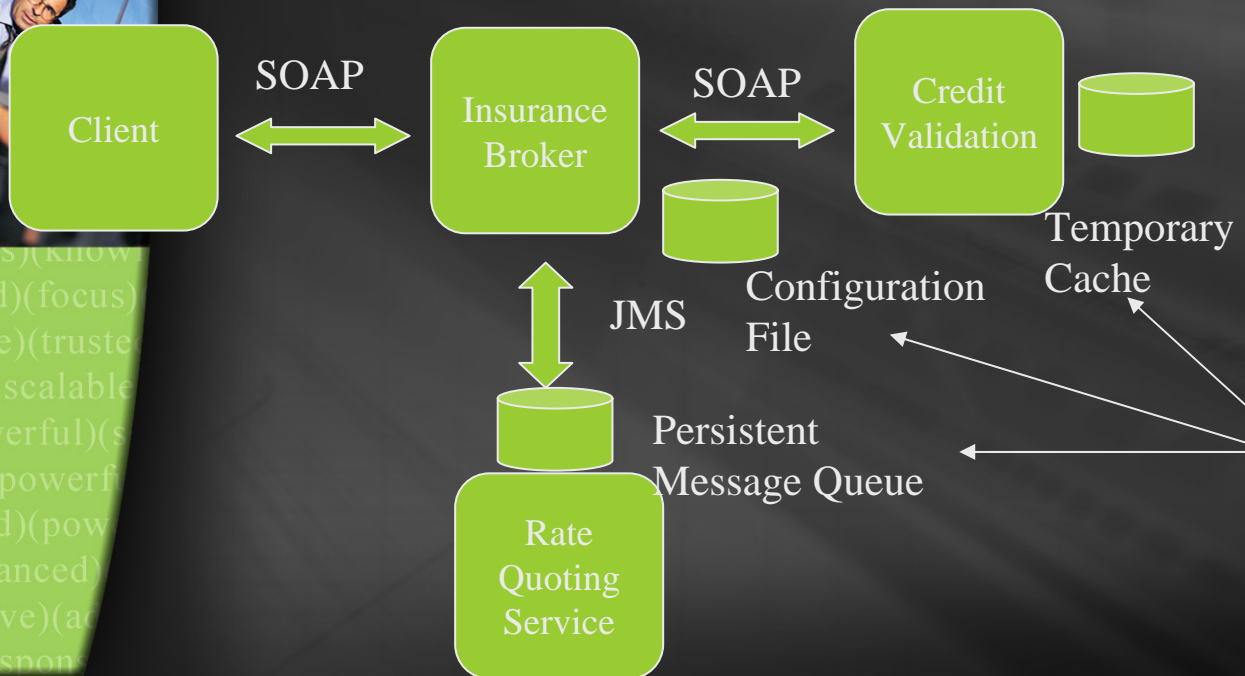
Countermeasure:
Use SSL to secure transport layer throughout multi-hop transaction
Encrypt XML messages
Use Digital Signatures

Security Challenges - Transactional Issues

Protection of Data at Rest in Intermediary Points Often Overlooked



ocus)(know
sted)(focus)
able)(truste
ful)(scalable
powerful)(s
ed)(powerf
nced)(pow
advanced)
nsive)(ac
(respon

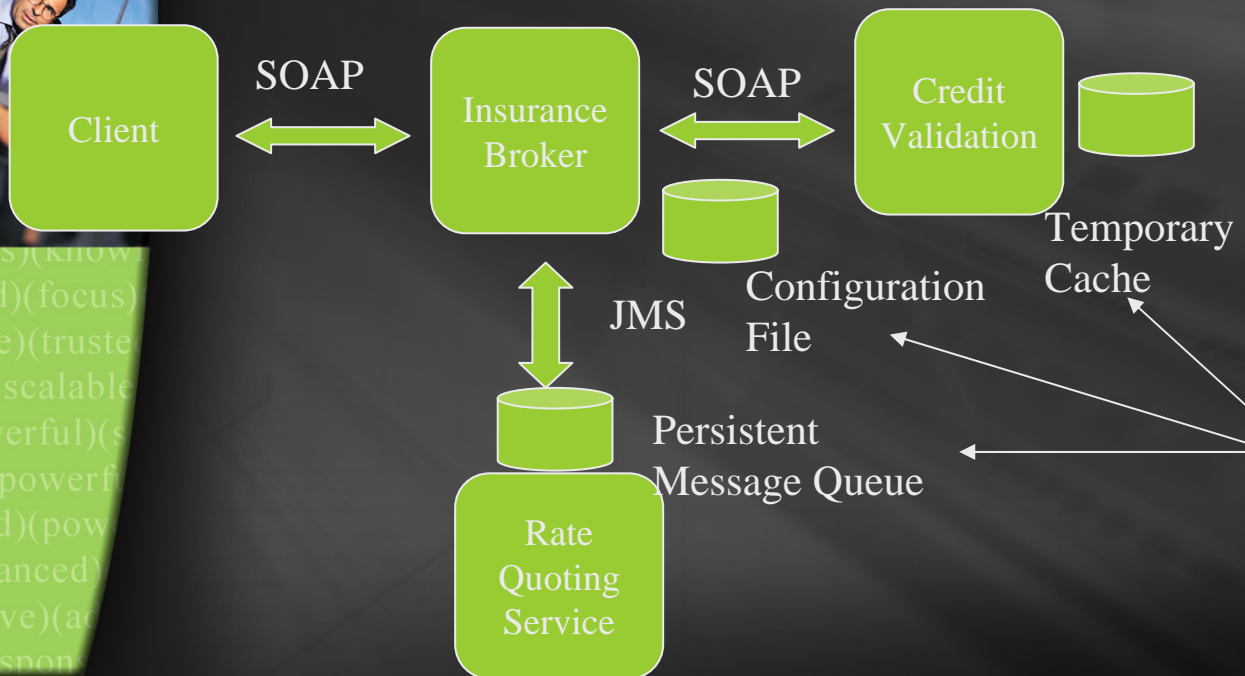


- Secure transient data
- May contain privacy data/enterprise sensitive info
- Examples: message queues, temporary cache or files.

Unsecured Data

Security Challenges - Transactional Issues

Protection of Data at Rest in Intermediary Points Often Overlooked



Countermeasures:

- Encrypt, when possible.
- Audit & lockdown intermediary data repositories
- Deploy appropriate security tools

Unsecured Data

Security Challenges – More Content Based Threats



- XQuery/SQL Injection
 - Inject XQuery as part of SOAP
- XML Morphing
 - Malicious modification of XML
- SOAP Routing Detour
 - Incorrect routing parameters
- Replay Attacks
 - Replaying valid message back to service
- WSDL Enumeration
 - Unauthorized execution of service methods
- Schema Poisoning
 - Modifying schema to cause inconsistencies with XML document

Tips on Securing Web Services



- Create Internal Trust Zones to Protect Critical Services
- Deny by Default
- Design Deployment Architecture with Attack Containment in Mind
- Secure Transport and Message Layers
- Use Industry Standard Authentication

Tips on Securing Web Services

- Validate and Version Control XML Schemas
- Inspect and Validate Incoming/Outgoing XML
- Regular Security Audits of the Business Process, Not Just the Organization
- Protect Temporary/Intermediary Data Stores
- Audit Trail of Entire Transaction Flow

Tips on Securing Web Services



- Secure Data On the Way Out
- Use Digital Signatures for Financial Reporting Compliance
- Design Web Services Security Under an Overall Security Architecture
- Defense In Depth, Patch Currency and Other Good Security Practices

Questions?



Contact me: ayee@nfr.com

Visit my blog: www.ebizq.net/blogs/security_insider

ocus)(know
sted)(focus)
able)(truste
ful)(scalable
powerful)(s
ed)(powerf
nced)(pow
advanced)
nsive)(ac
(respon