Concepts of Web Services Security

Session MCP/OS/MTP 4066
2:45–3:45pm, Halloween 2017

MGS INC
Computer Business Solutions

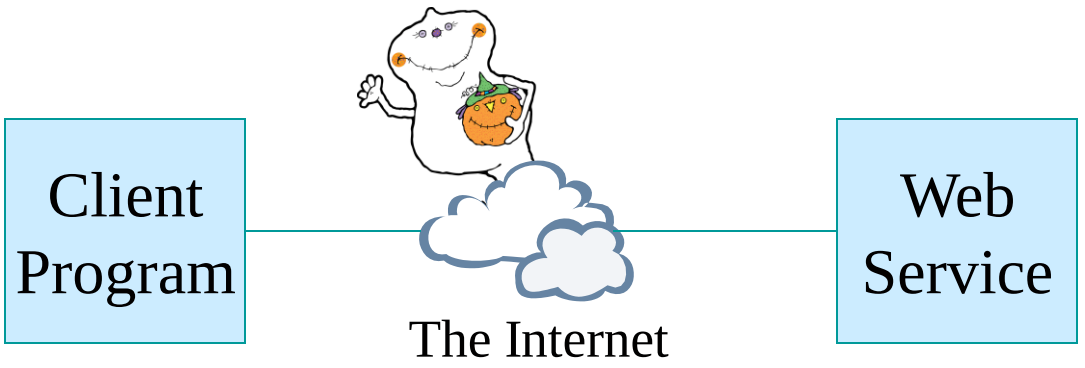
MGS, Inc.

- Software Engineering, Product & Services firm founded in 1986
- Products and services to solve business problems:
  - **Software Engineering Services**
  - **Professional Services**
    - **Management Support**
    - **Consulting and Technical Services**
    - **Application Development**
  - **Product Development**
    - **Performance/Capacity Management**
    - **Web Services**
    - **MCP Client Communications**

MGS INC
Computer Business Solutions

Web Services – Overview

- Goal
  - Make network program-to-program exchanges as easy as browsing the Web



MGS INC
Computer Business Solutions

Web Services – Overview

- The Web Services concept contains extremely powerful elements:
  - Simple, well-defined, standards-based interface
  - Technology independent implementation
  - Services have a description file
- “Loose Coupling” between provider and consumer
  - Anonymous client
  - Flexible data content
  - asynchronous

MGS INC
Computer Business Solutions

Web Services – Overview

- Abstracts out business functionality
  - Creates machine (technology) independent functionality
  - Indirect reference to a business service
- Leverage existing business functionality
  - Rewrites/Redesigns are expensive
  - Placing a Web Services envelope around existing functionality is relatively inexpensive
  - Preserves investment in known, reliable business solutions

MGS INC
Computer Business Solutions

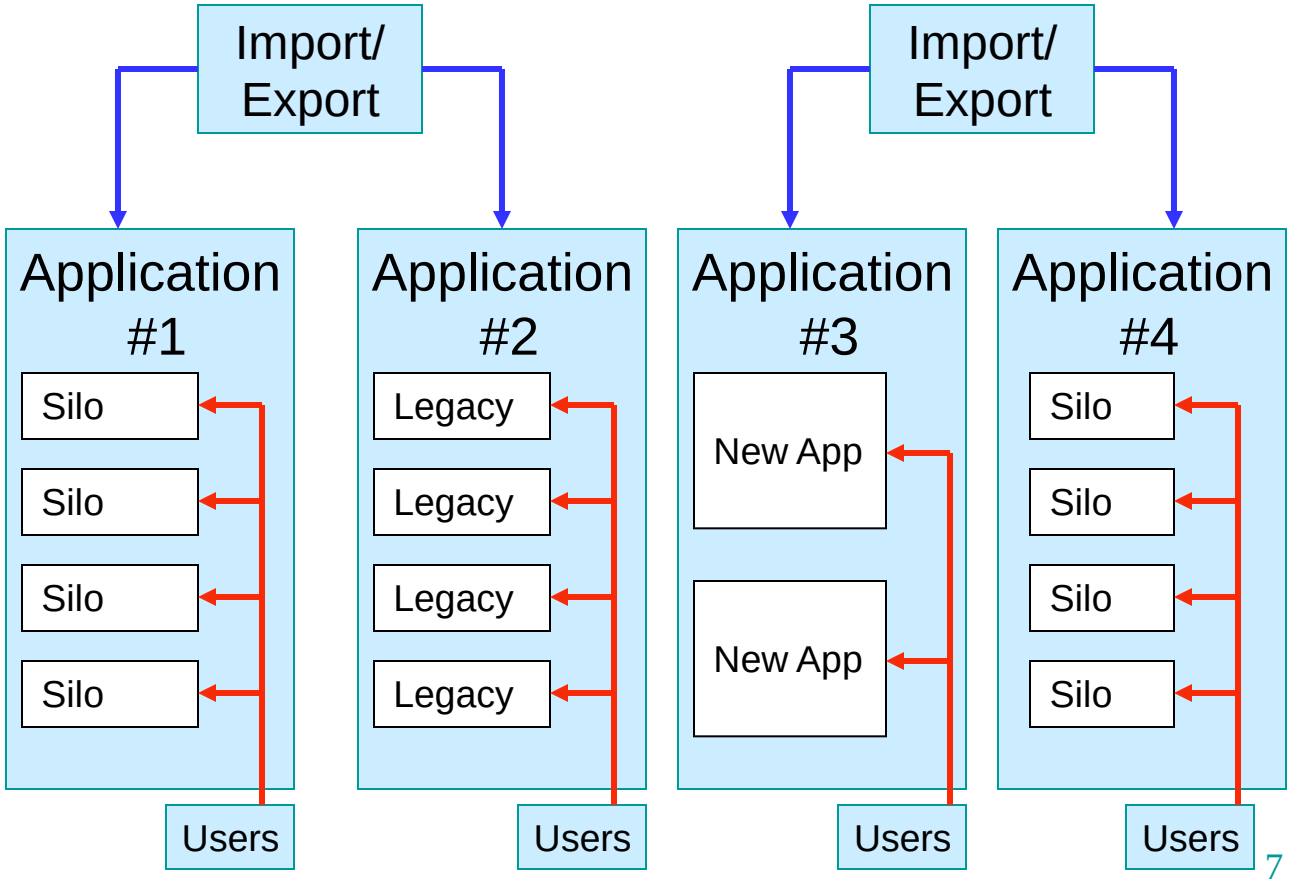
Web Services – Overview

- Services Oriented Architecture (SOA)
  - Componentize Enterprise business functions
  - Encapsulate existing business functions for easier access
  - IT Functionality now available as a set of objects that can be mixed and matched as needed
  - Application development done by architecting service consumers

MGS INC
Computer Business Solutions

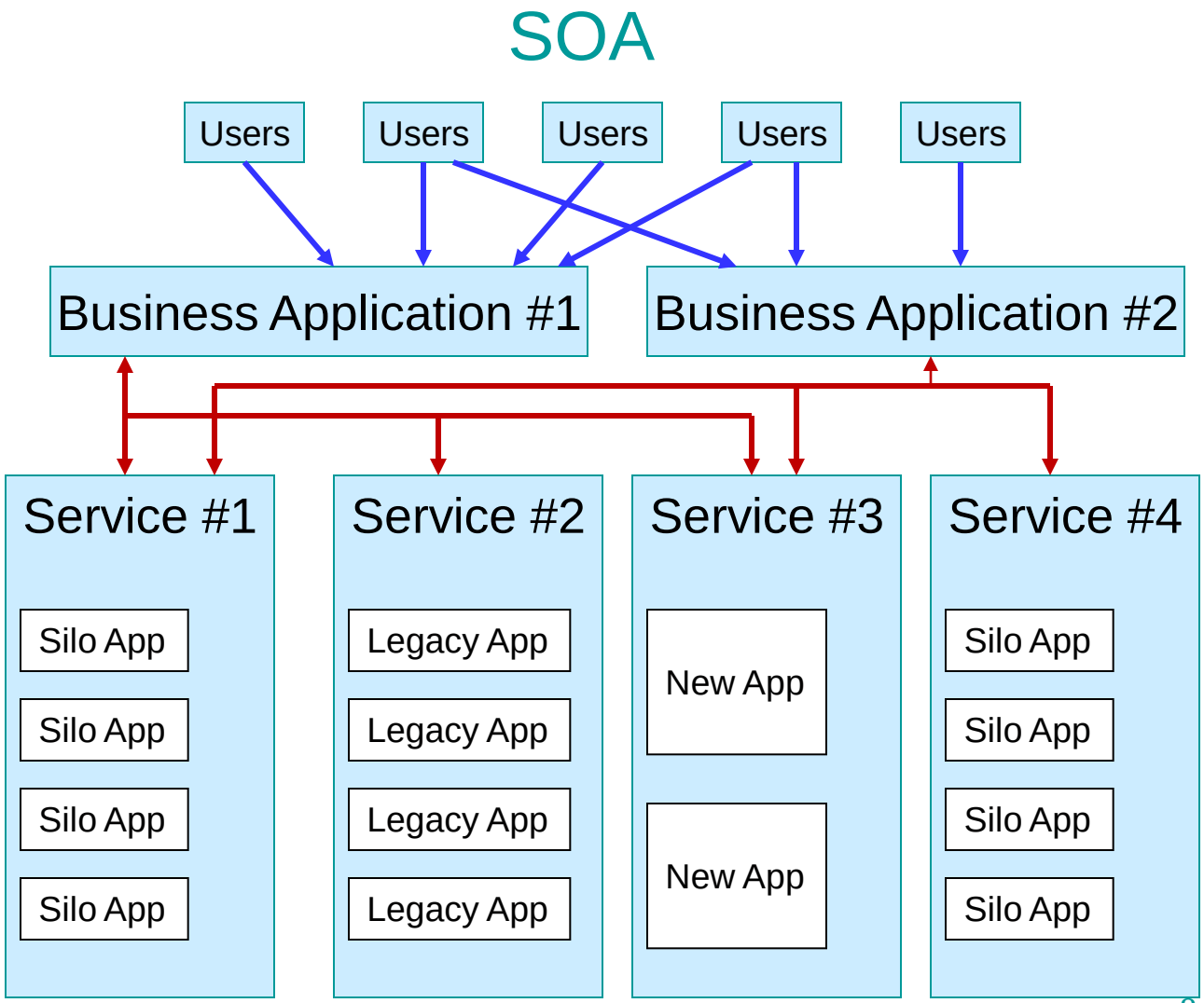
Web Services – Overview

Traditional Architecture



MGS INC
Computer Business Solutions

Web Services – Overview



MGS INC
Computer Business Solutions

Web Services – Overview

- Built on proven Internet communications standards
  - **TCP/IP – Transmission Control Protocol / Internet Protocol**
  - **TLS – Transport Layer Security (formerly SSL)**
  - **HTTP – HyperText Transfer Protocol**
  - **SOAP protocol**
  - **XML – eXtensible Markup Language**
- Includes service description
  - **WSDL – Web Services Description Language**

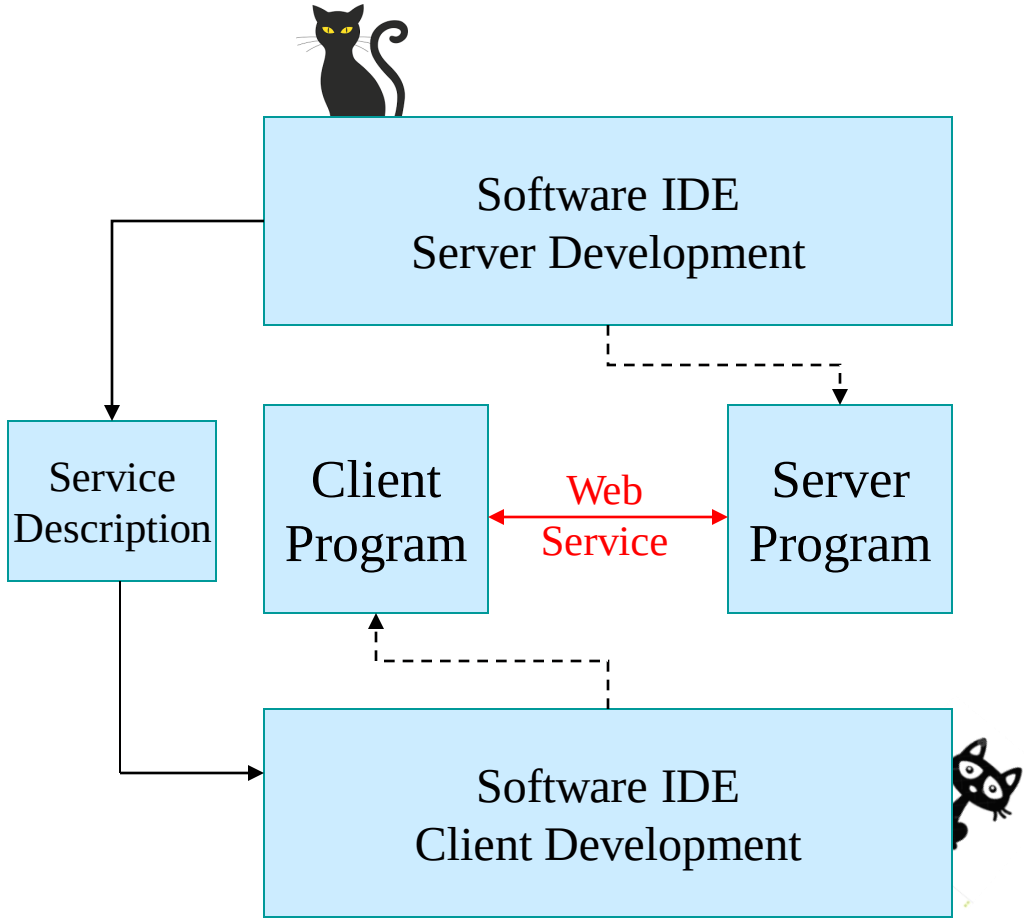
MGS INC
Computer Business Solutions

Web Services – Overview

- Supported by software IDEs
  - Automatic creation of Web Services objects
  - Web Services Server object support
    - WSDL generation
    - Server program
  - Web Services Client object support
  - Included as part of the application framework
    - Microsoft .NET
    - Oracle/Sun JAVA
    - Unisys Agile Business Suite
    - Unisys ePortal
    - MGS-Web

MGS INC
Computer Business Solutions

Web Services – Overview



MGS INC
Computer Business Solutions

Web Services- Technology

WSDL File Excerpt:

```
<message name="WSTEST_SCRN01">
  <part name="Trancode" type="xsd:string" />
  <part name="Input_data" type="xsd:string" />
</message>
<message name="WSTEST_SCRN01Response">
  <part name="Trancode" type="xsd:string" />
  <part name="Input_data" type="xsd:string" />
  <part name="statusLine" type="xsd:string" />
</message>

<service name="COMSWebServices">
  <documentation>Access COMS applications via Web Services
  </documentation>
    <port name="WSTEST" binding="wsdl:WSTESTHttpBinding">
    <soap:addresslocation=
            "http://laptop1mcp/COMSWebServices/" />
    </port>
</service>
```

MGS INC
Computer Business Solutions

Web Services – Technology

SOAP Request:

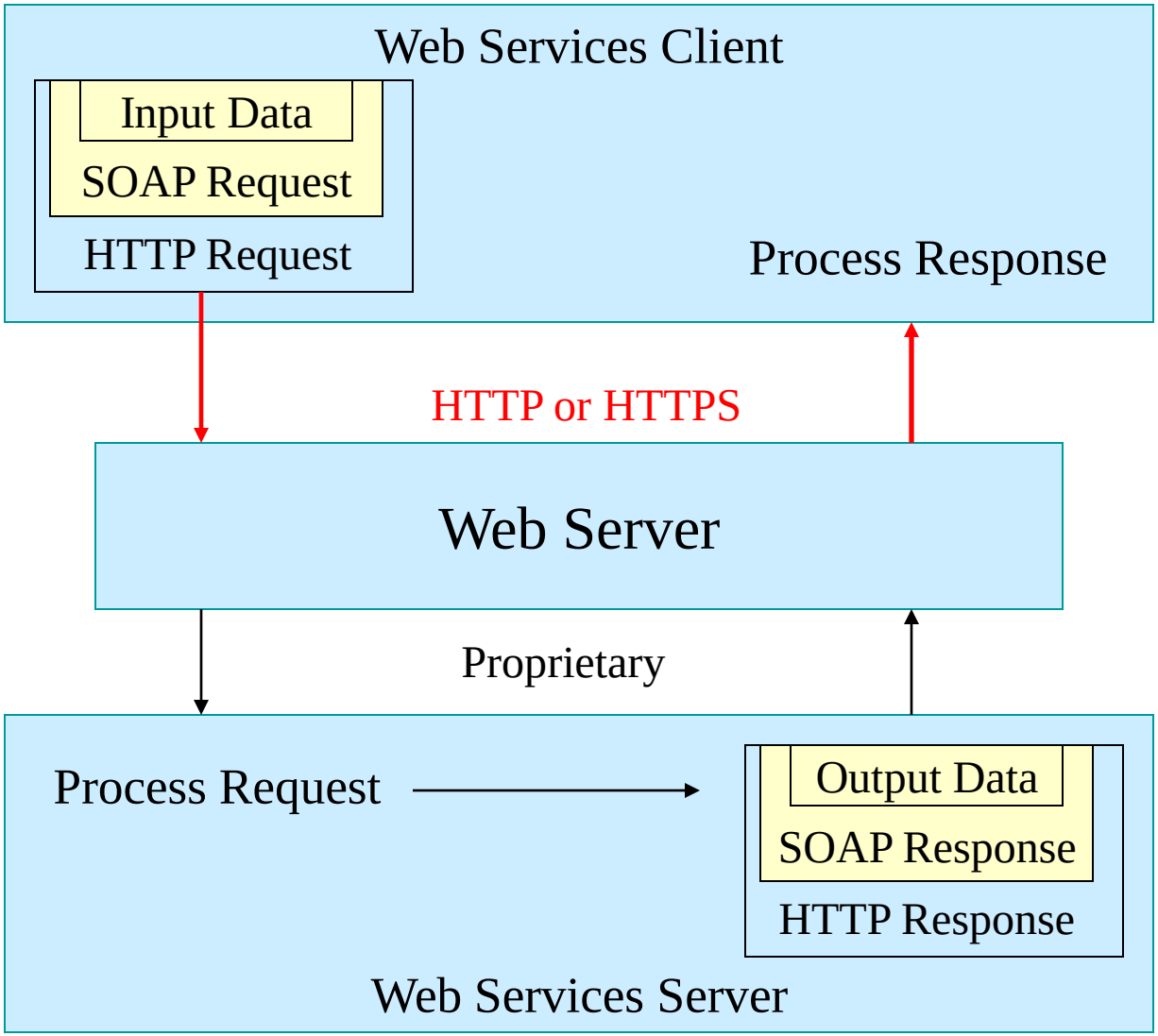
```
<soap:Envelope>
  <soap:Body>
    <tns:WSTEST_SCRN01>
      <Trancode>SCRN01</Trancode>
      <InputData>lower case letters</InputData>
    </tns:WSTEST_SCRN01>
  </soap:Body>
 </soap:Envelope>
```

SOAP Response:

```
<soap:Envelope>
  <soap:Body>
    <tns:WSTEST_SCRN01Response>
      <Trancode>SCRN01</Trancode>
      <InputData>LOWER CASE LETTERS</InputData>
      <statusLine />
    </tns:WSTEST_SCRN01Response>
  </soap:Body>
 </soap:Envelope>
```

MGS INC
Computer Business Solutions

Web Services – Technology



Indicates XML Encoding

MGS INC

Computer Business Solutions

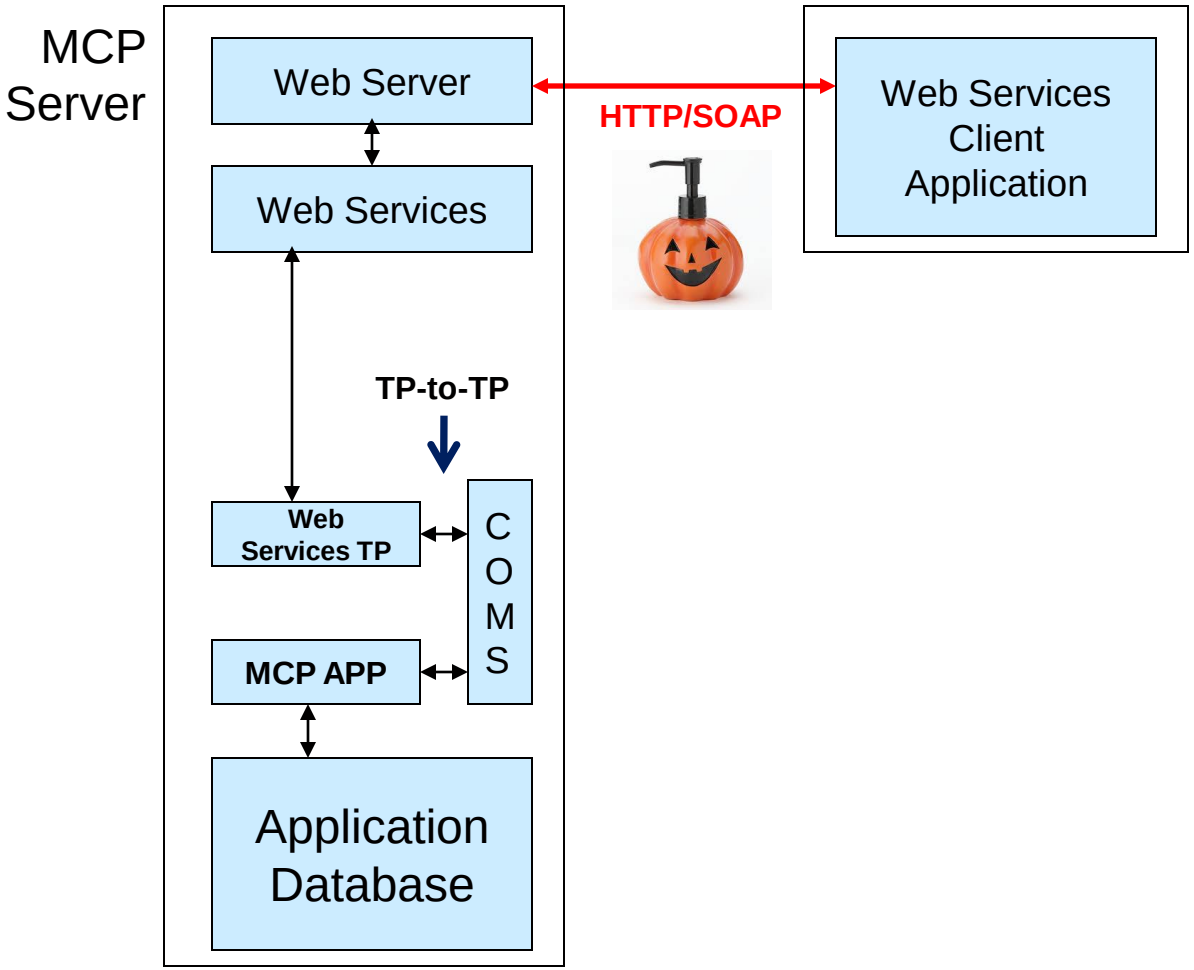
Web Services Server - MCP

- MCP Based Web Service
  - Web Service Server runs under MCP control
  - Routes incoming call to MCP App via COMS station or COMS TP-to-TP

MGS INC
Computer Business Solutions

Web Services Server - MCP

- MCP Based Web Service



MGS INC
Computer Business Solutions

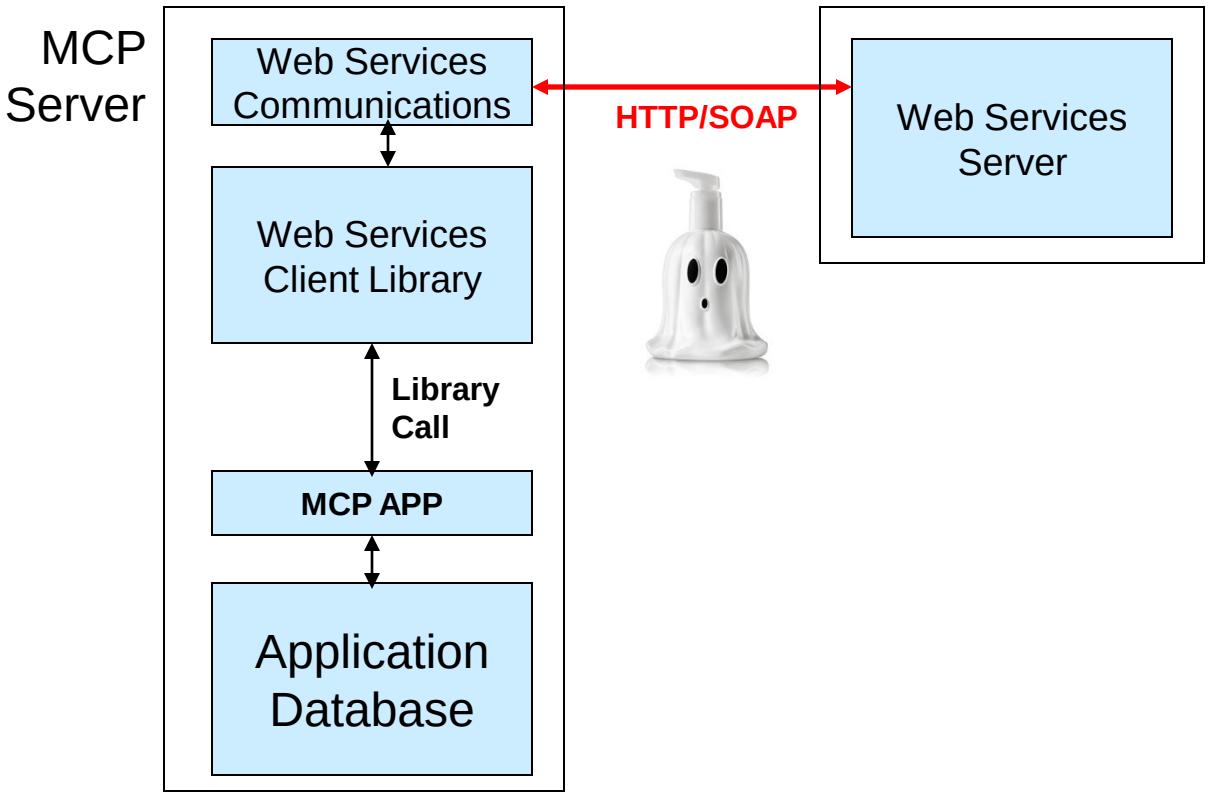
Web Services Client - MCP

- MCP Based WS Client
  - Allows MCP applications to make a Web Services call on another server
  - MCP Application does a simple library call to make the outbound WS Client call

MGS INC
Computer Business Solutions

Web Services Client - MCP

- MCP Based WS Client



MGS INC
Computer Business Solutions

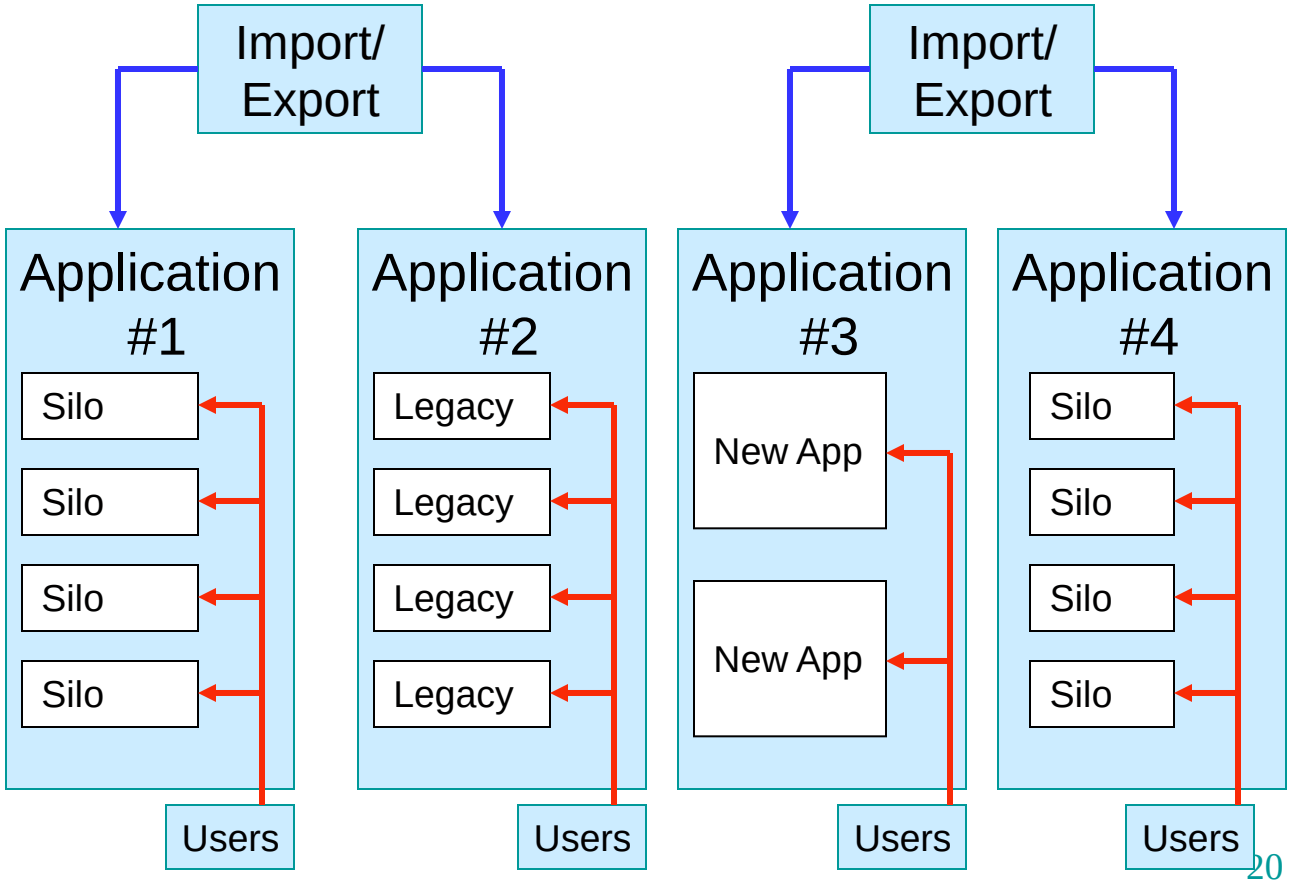
Web Services - Security

- Digital security has three parts:
  - Identification
    - Authentication
    - Digital signature
  - Encryption
  - Journaling
- Web Services moves security considerations to a different place
  - May not be at the user's interface point
  - Often a machine-to-machine
  - The "other" machine may not be trusted
- The SOA changes the security landscape

MGS INC
Computer Business Solutions

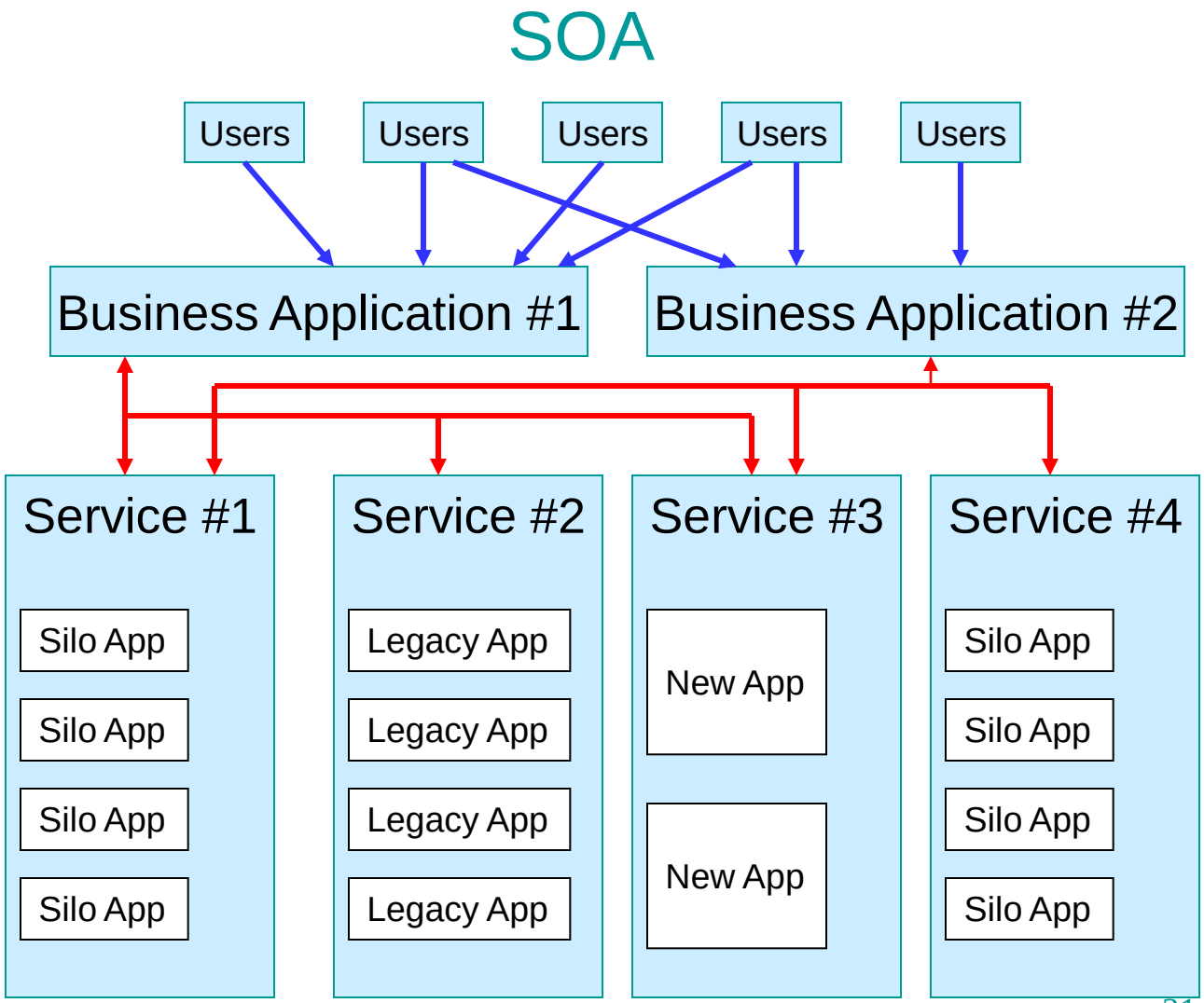
Web Services – Security

Traditional Architecture



MGS INC
Computer Business Solutions

Web Services – Security



MGS INC
Computer Business Solutions

Security - Connections

- Persistent Connections
  - MCP TCP/IP connect/disconnect slows throughput
  - On close, TCP/IP port must “time wait” for TTL*2 seconds on most systems
  - Most servers default to persistent HTTP connections
    - Connection:Keepalive
  - Client then controls persistence
  - Persistence provides a 4 to 50 times throughput increase

MGS INC
Computer Business Solutions

Security - Connections

- Non-Persistent Connection

Client Connect ---------->
<---------- Server Accept

SOAP Request ---------->
<---------- SOAP Response

Client Disconnect ---------->

Client Connect ---------->
<---------- Server Accept

SOAP Request ---------->
<---------- SOAP Response

Client Disconnect ---------->

MGS INC
Computer Business Solutions

Security - Connections

- Persistent Connection

```
Client Connect      ---------->
                    <----------  Server Accept

SOAP Request        ---------->
                    <----------  SOAP Response

SOAP Request        ---------->
                    <----------  SOAP Response

SOAP Request        ---------->
                    <----------  SOAP Response

Client Disconnect   ---------->
```

MGS INC
Computer Business Solutions

Security - Connections

- Pipelining
  - Requires a persistent connection
  - Multiple requests are sent without waiting for responses
  - Responses return in send-order
  - Most web servers (including ATLAS) support this
  - Use controlled by whether WS Client application is coded to take advantage of this

Security - Connections

- Piplining

```
Client Connect          ---------------->
                        <----------------  Server Accept

SOAP Request            ---------------->
SOAP Request            ---------------->
SOAP Request            ---------------->

                        <----------------  SOAP Response
                        <----------------  SOAP Response
                        <----------------  SOAP Response

Client Disconnect       ---------------->
```

MGS INC
Computer Business Solutions

Web Services - Security

- Controlling security at different levels and different ways
  - TLS/SSL (encryption)
  - HTTP Logon (authentication)
  - SOAP Headers (authentication)
  - Actual WS call to logon (authentication)
  - WS-Security (authentication, signature, encryption)

Security - Transport

- Transport Layer Security (TLS)
  - TLS similar but robust than SSL
  - TLS – Authenticates server
    - Get certificate from Server
    - Validate certificate from a trusted Certificate Authority
  - Two way TLS
    - Client Authenticates server
    - Server Authenticates client
  - Encryption, provided by the certificate keys, is transparent to application
  - Application must get/supply authentication info through an external interface

Security - Transport

- Transport Layer Security (TLS)
  - TLS 1.0, 1.1 and 1.2 based on relatively weak-to-moderate key encryption protocols and data can be seen if key is externally known
  - TLS 1.3 (under development) encryption is more robust and the key cannot be externally provided
  - TLS 1.3 Lack of external key provision is “sniffer” unfriendly

Security - HTTP

- HTTP Logon
  - Logon required for a specific virtual directory
  - Uses HTTP AUTHORIZATION header
  - BASIC uses a Base64 exchange so SSL/TLS is required for secure communications
  - DIGEST uses MD5 encrypted exchange
  - NTLM provides username/pw encryption and is non re-playable
  - No data encryption
  - Application must get/supply authentication info through an external interface

Security – SOAP Header

- SOAP Headers
  - One must pre-acquire authentication information before the Web Service call
  - The SOAP message can contain both a HEADER section as well as a body
  - Authentication information is provided as in SOAP HEADER fields
  - TLS is still needed to encrypt HEADERs
  - Application must supply authentication info using special code by setting the header fields

Security – SOAP Header

- SOAP Headers

```
<Envelope>
 <Header>
  <ABECHeader xmlns="service.abec.com">
  <MessageData>
       <MessageID>568425287</MessageID>
  </MessageData>
  <UserAuthorization>
       <UserName>MS0281331</UserName>
       <UserPassword>x@32!aX49#$&</UserPassword>
  </UserAuthorization>
  </ABECHeader>
 </Header>
 <Body>
   ..... SOAP body …..
 </Body>
</Envelope>
```

MGS INC
Computer Business Solutions

Security – Logon Transaction

- WS Call to Logon
  - One must pre-acquire authentication information (usercode/password)
  - An initial web services call is made for authentication
  - The response contains a token to be placed in the body of all subsequent web services calls
  - Application must be “token” aware
  - TLS is still needed to encrypt dialogs

MGS INC
Computer Business Solutions

Security – Logon Transaction

- WS Call to Logon

```
Client Connect          ---------->
                        <----------  Server Accept

Logon Request           ---------->
                        <----------  Logon Response (token)

SOAP Request (token)    ---------->
                        <----------  SOAP Response

SOAP Request (token)    ---------->
                        <----------  SOAP Response

SOAP Request (token)    ---------->
                        <----------  SOAP Response

Client Disconnect       ---------->
```

MGS INC
Computer Business Solutions

Security – WS-Security

- WS-Security (WSS)
  - Originally developed by IBM, Microsoft, VeriSign and Forum Systems
  - Attach signature and encryption headers to SOAP messages
  - Provides end-to-end integrity for each message
  - Protocol uses SAML, Kerberos and x.509 certificates
  - Requires application awareness

Security – Summary

- Solutions
  - Will be dependent on the technology used and the connection type
  - Use a front-end Web Services pass-thru processor to do encryption (TLS), authentication (back-end systems are trusted) and journaling
  - Note, the front-end processing may be on the same system as the Web Service
  - Use TLS to obfuscate user/password authentication and Web Service contents
  - Have username/password aware applications

Additional Questions?

Michael S. Recant
V.P. Software Development

MGS, Inc.
583A Southlake Boulevard
Richmond, VA 23236

Voice: (804)379-0230
Fax: (804)379-1299
Email: Mike.Recant@mgsinc.com
Web: www.mgsinc.com

MGS INC
Computer Business Solutions

UNITE 2017 Conference

Concepts of Web Services Security

This presentation is available on our WEB site
http://www.mgsinc.com/download.html

MGS INC
Computer Business Solutions