UNITE 2022

Secure MCP Communications from Workstation to Cloud

Session 4037, Feb 3, 13:30-14:30

Michael Recant
VP Software Development
MGS, Inc.

MGS INC
Computer Business Solutions

MGS, Inc.

- Software Engineering, Product Development & Professional Services firm founded in 1986
- We solve business problems with:
  - Products:
    - SightLine™ Performance/Capacity
    - MGSWEB Web Services
    - Deliver
    - C.A.T.T. Terminal Emulator
    - File Manager for MCP
  - Professional Services
    - Performance/Capacity Management
    - Installation Services
    - MCP Training
  - Software Engineering Services
    - ClearPath MCP
    - Windows

MGS INC
Computer Business Solutions

Secure Communication

- Affected Technology
  - MCP Server Environment
  - Communication Connection
  - Secure Authentication
- Requirements
  - Legal
  - Best-practices
  - Secure corporate data
  - Ensure customer privacy

MGS INC
Computer Business Solutions

Secure Communication

- Individual Privacy Requirements
- Federal Regulations
  - Gramm-Leach-Bliley Act: The Safeguards Rule
  - Fair Credit Reporting Act (FCRA)
  - Federal Trade Commission
  - HIPAA – Health & Human Services

MGS INC
Computer Business Solutions

Secure Communication

- Example:
  Payment Card Industry (PCI)
  Security Standards Council
- PCI Data Security Standard (DSS) applies to all entities that store, process or transmit cardholder data.
- Compliance is a process which involves certified assessment

MGS INC
Computer Business Solutions

PCI – DSS Requirements

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

We Are Responsible

- Laws and regulations change how we must handle and secure data.
- Our organizations are just the starting point.
- Due diligence for 3rd party service providers is also mandatory.

MGS INC
Computer Business Solutions

Privacy Best Practices

- Create a privacy governance plan
- Inventory data movement
- Assess organizational breach risk
- Secure paper documents
- Encrypt stored data
- Encrypt data on portable devices
- Encrypt data transmission
- Audit compliance with the plan annually

MGS INC
Computer Business Solutions

Secure Client Communication

- Moving sensitive data from host to workstation and back is simple – or is it?
- Client are no longer guaranteed to be co-located with servers and can connect from anywhere
- We must discuss connections, encryption, and authentication to understand the entire picture.

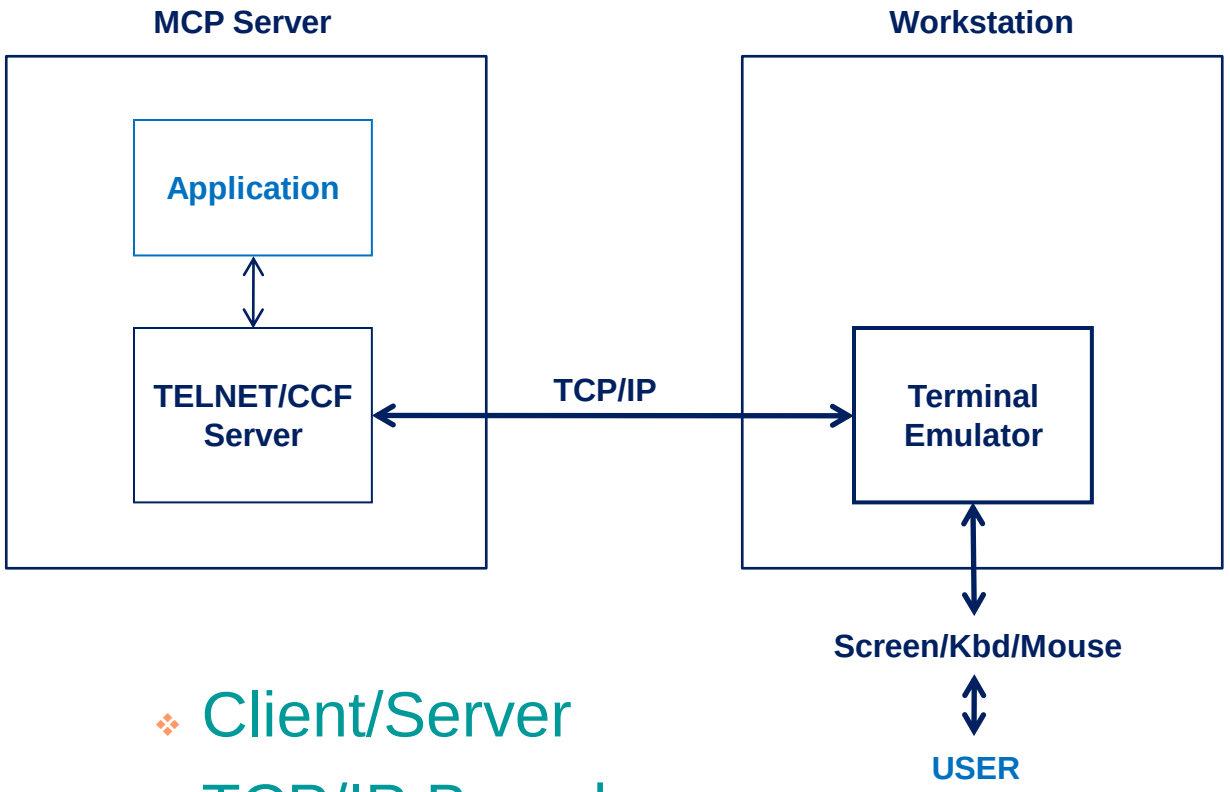
MGS INC
Computer Business Solutions

Secure Client Communication

- Securing MCP Connections
  - Basic MCP Connection
  - Trusted Basic Connection
  - Untrusted Basic Connection
  - Virtual Private Network
  - 3-Tier Secure Connection
  - 2-Tier Secure Connection
- Securing MCP Authentication
  - Unsecure Connection
  - Secure Connection

MGS INC
Computer Business Solutions

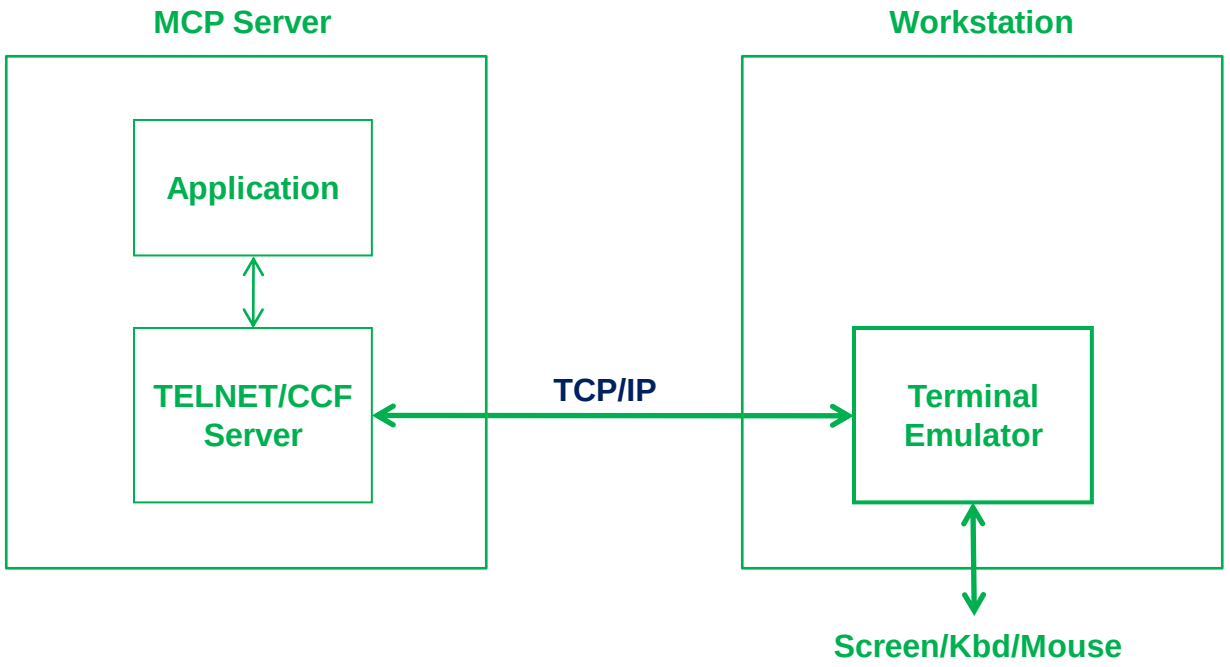
Basic MCP Connection



- Client/Server
- TCP/IP Based
- Terminal Protocol (Telnet/CCF)
- Goal: connect **USER** with **APPLICATION**

MGS INC
Computer Business Solutions

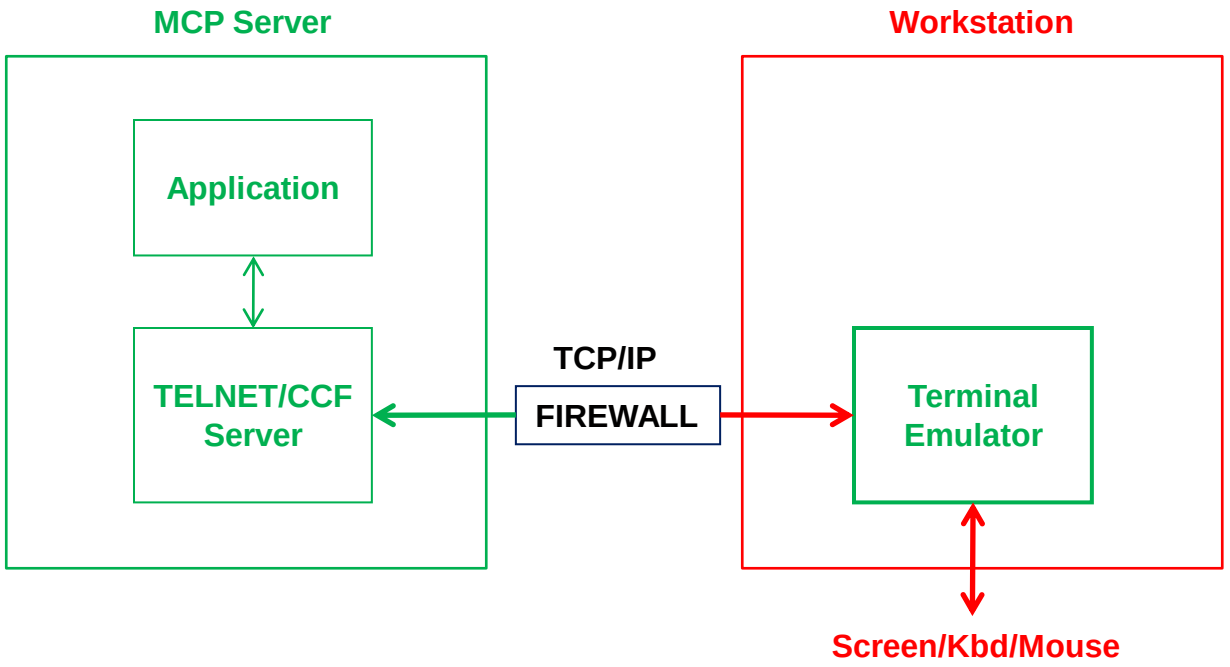
Trusted Basic Connection



- Server is secure
- LAN is secure
- Client is secure
- Secure connection not needed

MGS INC
Computer Business Solutions

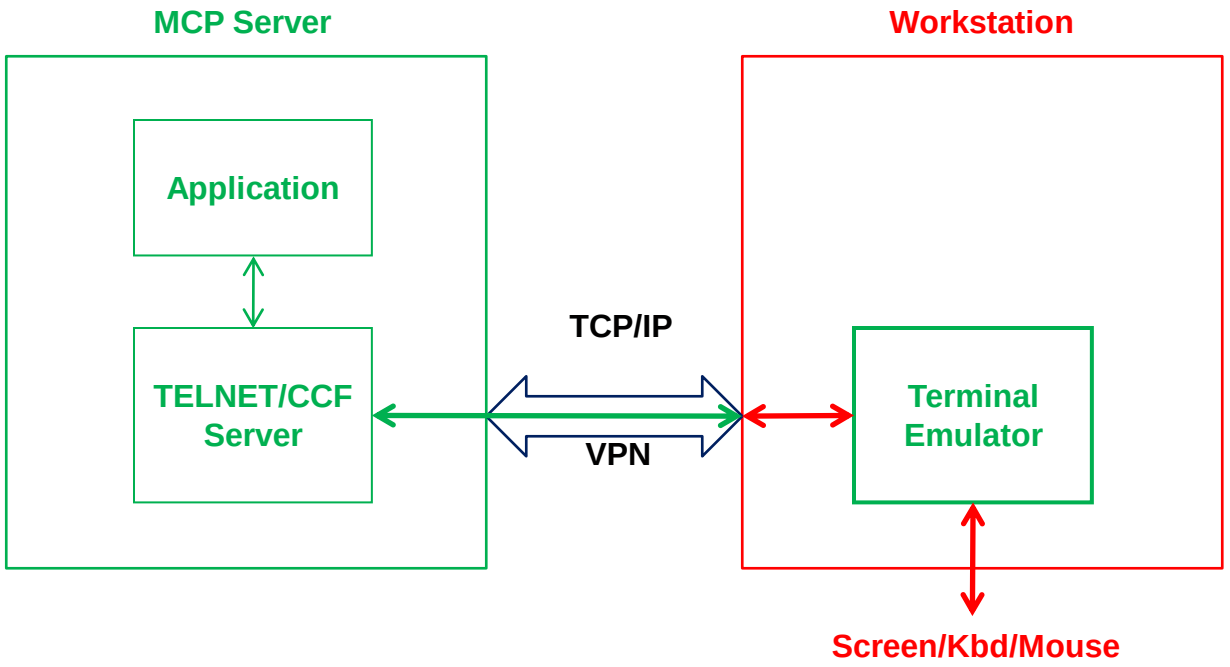
Untrusted Basic Connection



- Server is secure
- Server LAN is secure
- Client is not secure
- Client LAN is not secure

MGS INC
Computer Business Solutions

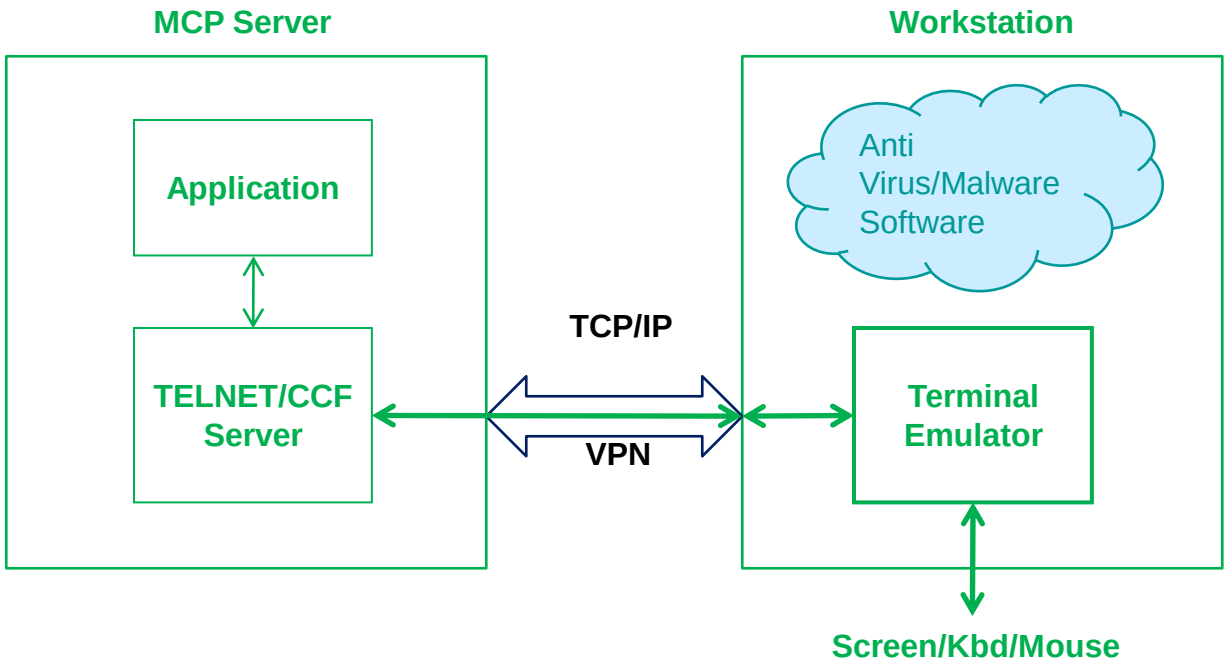
Virtual Private Network Connection



- Server is secure
- Server LAN is secure
- VPN to server is secure
- Client is not secure

MGS INC
Computer Business Solutions

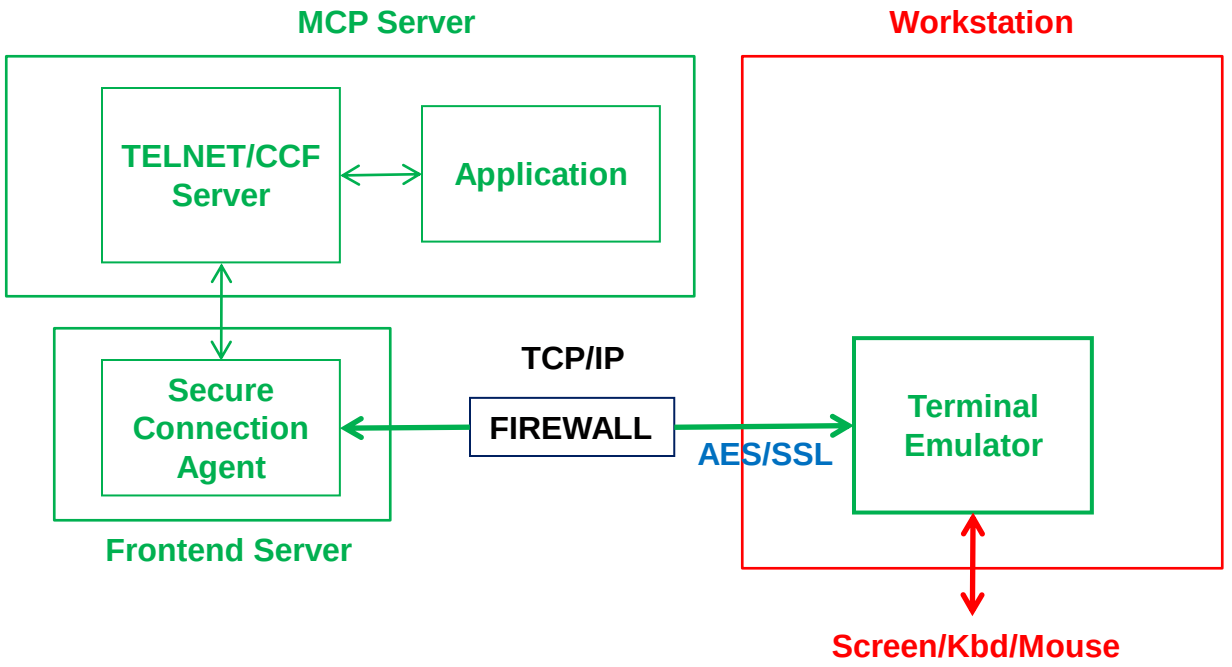
Virtual Private Network Connection



- Use Anti Virus software to secure the workstation
- Secure-workstation practices

MGS INC
Computer Business Solutions

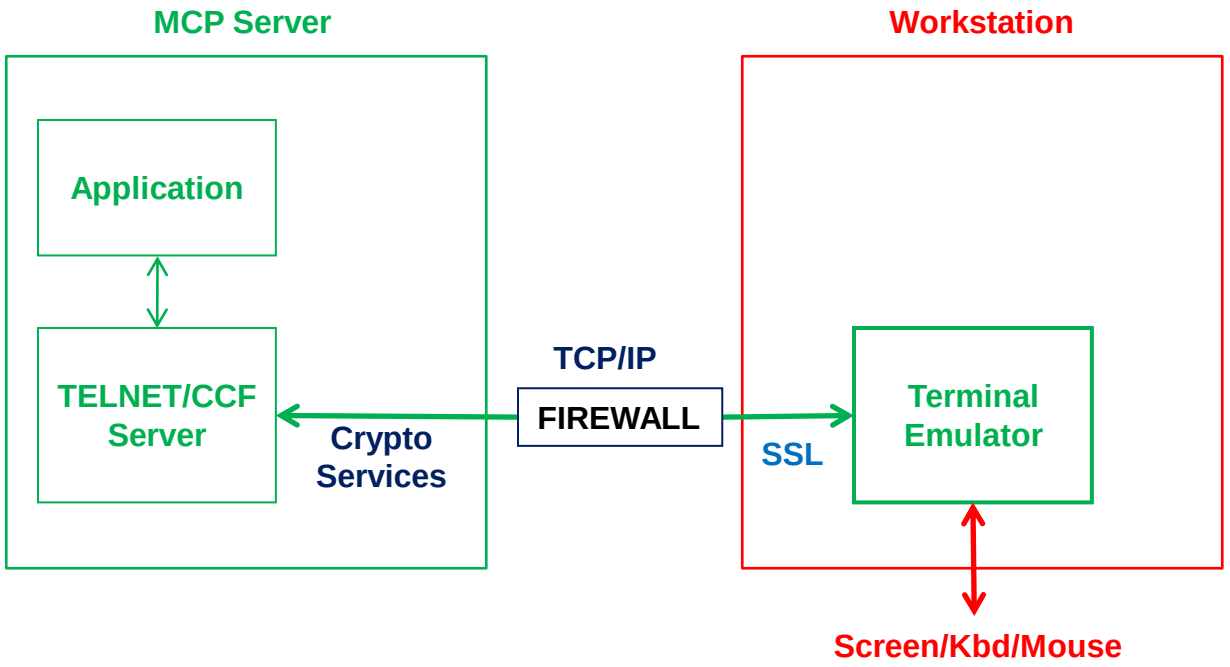
3-Tier Secure Connection



- Server and Server LAN secure
- Frontend Server secure
- Emulator connection is secure
- Client is not secure

MGS INC
Computer Business Solutions

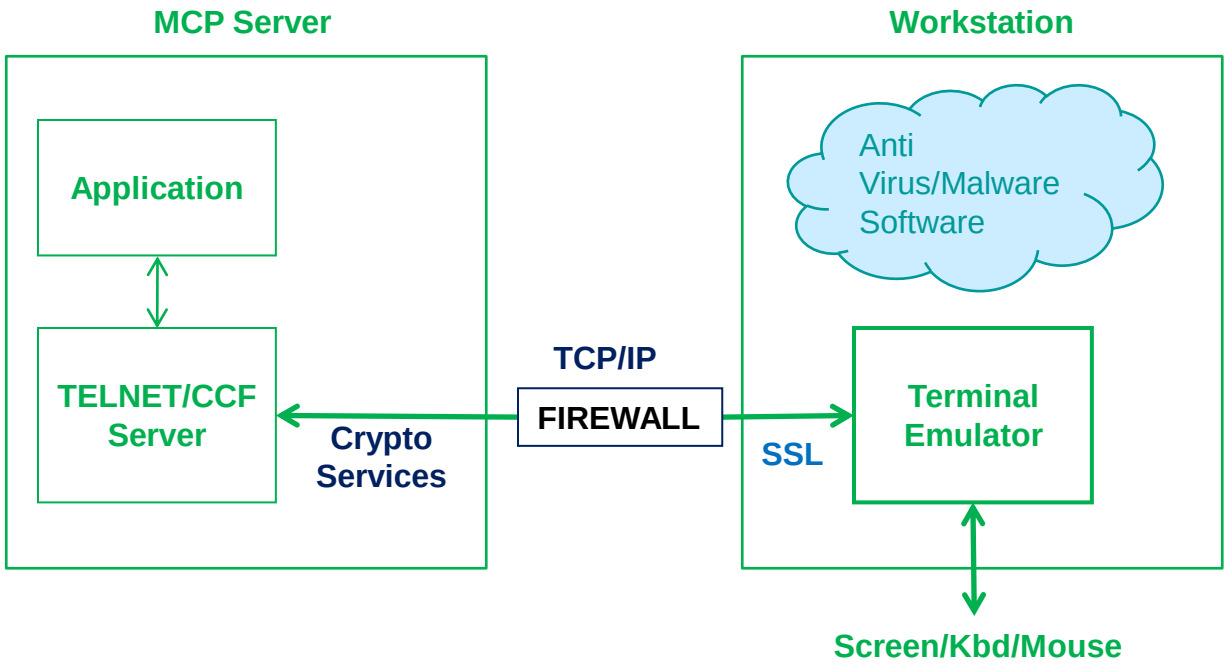
2-Tier Secure Connection



- Server is secure
- Emulator connection is secure
- MCP based SSL connection requires Crypto support

MGS INC
Computer Business Solutions

2-Tier Secure Connection



- Use Anti Virus software to secure the workstation
- Secure-workstation practices

MGS INC
Computer Business Solutions

Authentication

Do you know who is at the other end?

MGS INC
Computer Business Solutions

Authentication

- Unsecured Connection
  - Problem 1: Telnet and CCF use clear-text authentication
  - Problem 2: Is the end-user really authorized to use the usercode/password?
  - Kerberos option for Telnet only solves Problem 1

Authentication

- Secured Connection
  - Problem 1 goes away, clear-text authentication is no longer an issue as connection is secure
  - Kerberos required for Unisys Secure Telnet

MGS INC
Computer Business Solutions

Authentication

- Secured Connection
  - Identification still an issue
  - Usercode/password insufficient
  - Traditional SSL (Server-side) only positively IDs server
  - Options:
    - Client-side SSL
    - Physical device
    - 2 Factor Authentication

MGS INC
Computer Business Solutions

Secure Computer-to-Computer Communication

- Server-to-workstation is only part of the Secure Communications problem
- Today's processing require server-to-server dialogs

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

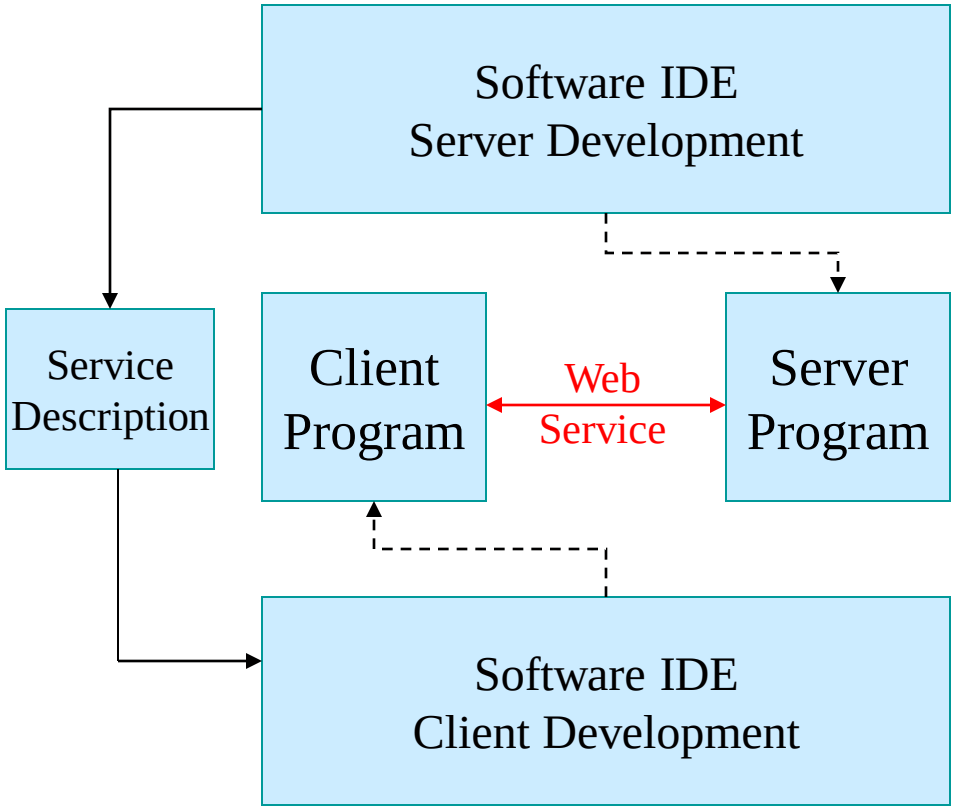
MGS INC
Computer Business Solutions

Web Services – Overview

- 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

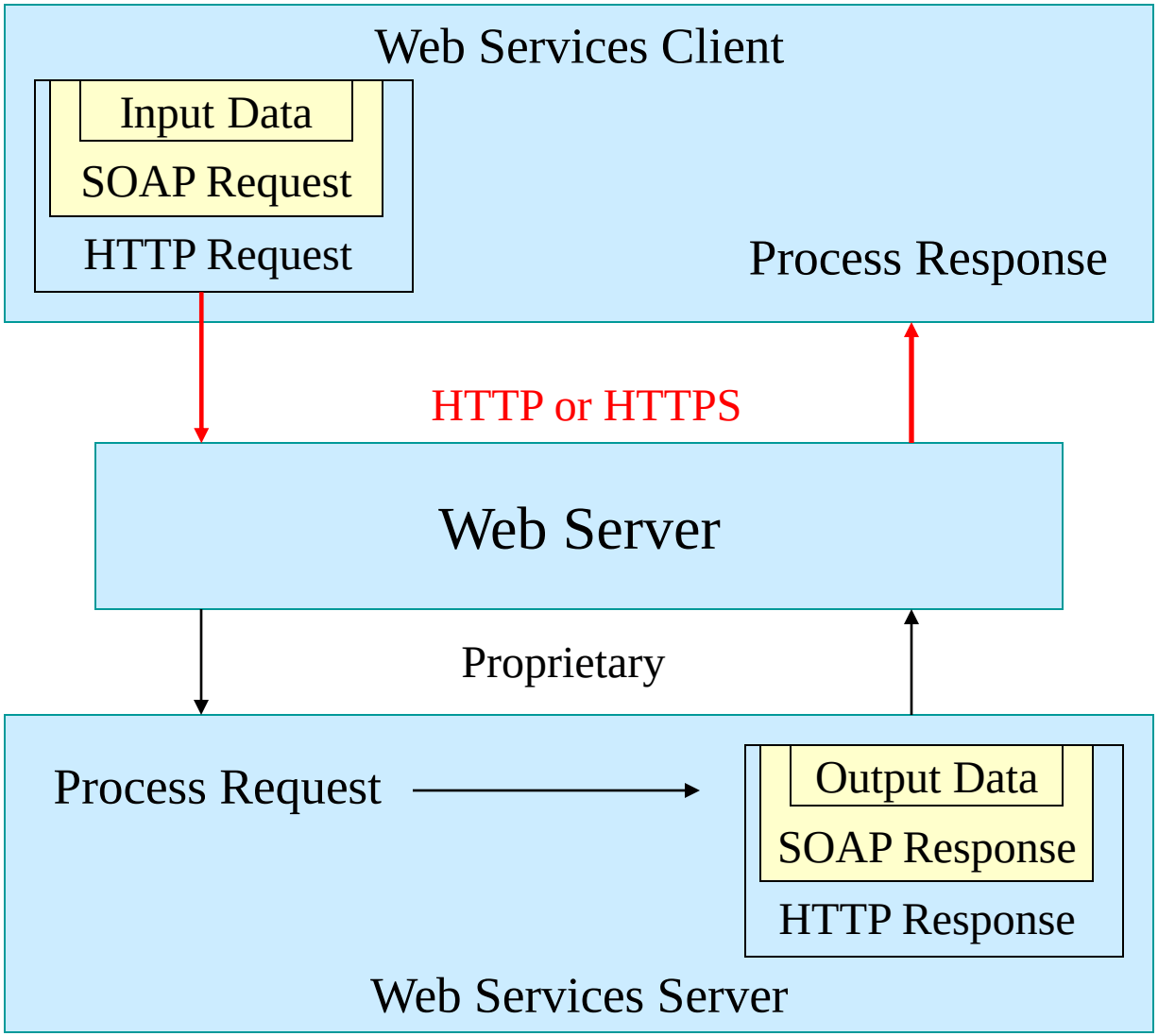
Web Services – Overview



MGS INC
Computer Business Solutions

Web Services – Technology

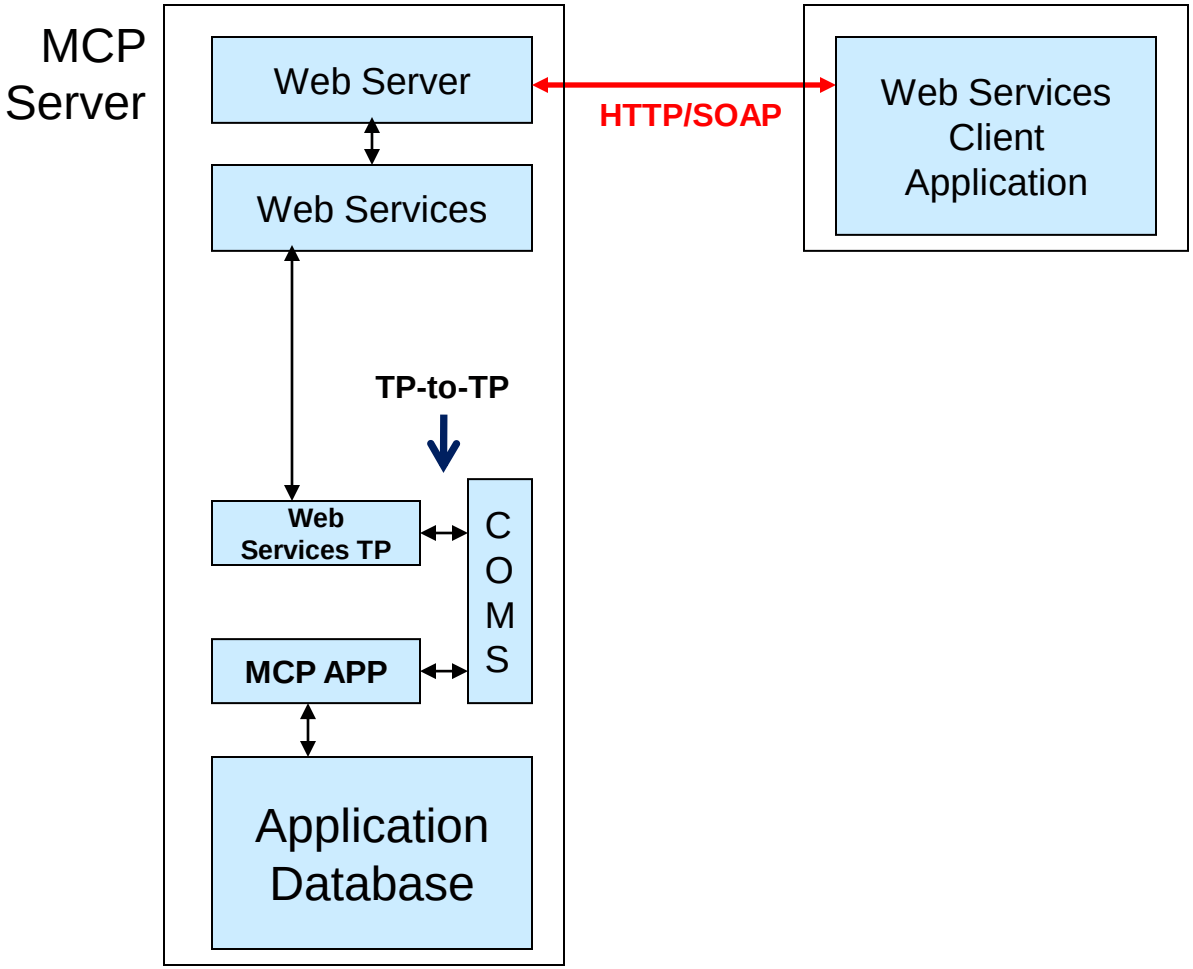
Indicates XML Encoding



MGS INC
Computer Business Solutions

Web Services Server - MCP

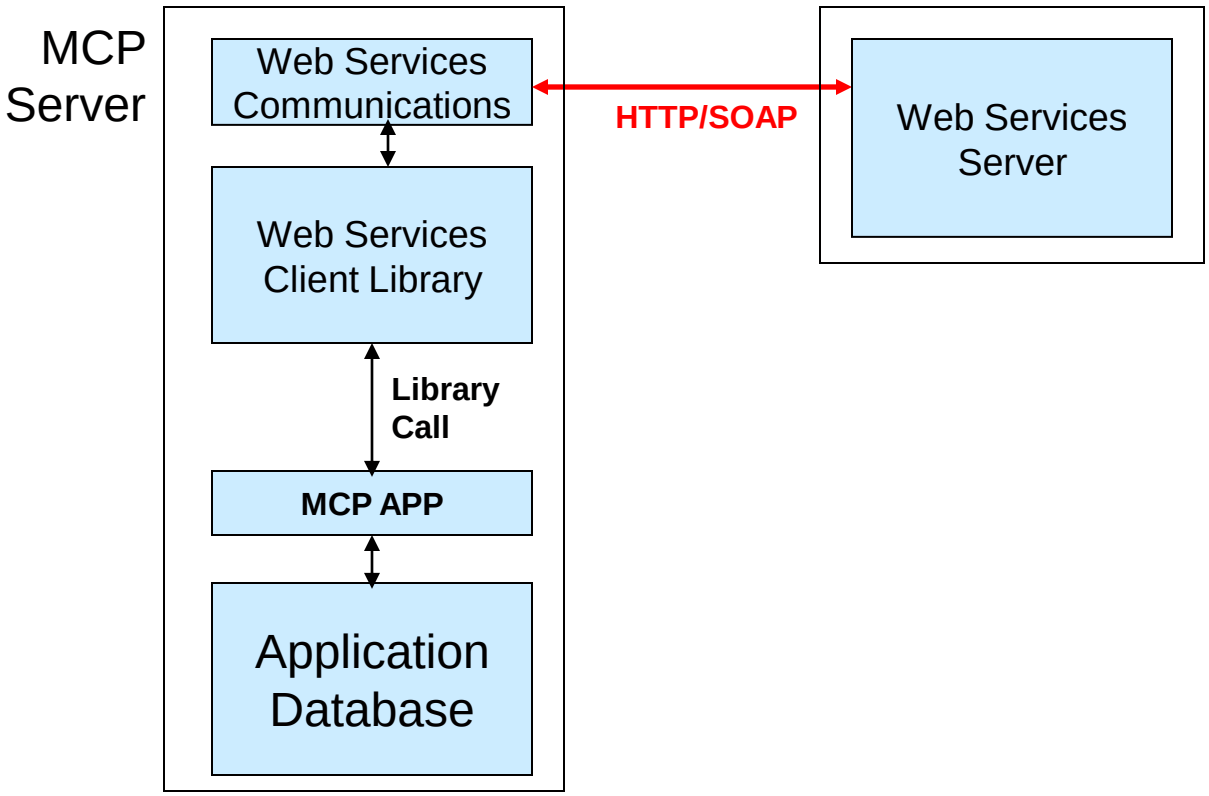
- MCP Based Web Service



MGS INC
Computer Business Solutions

Web Services Client - MCP

- MCP Based WS Client



MGS INC
Computer Business Solutions

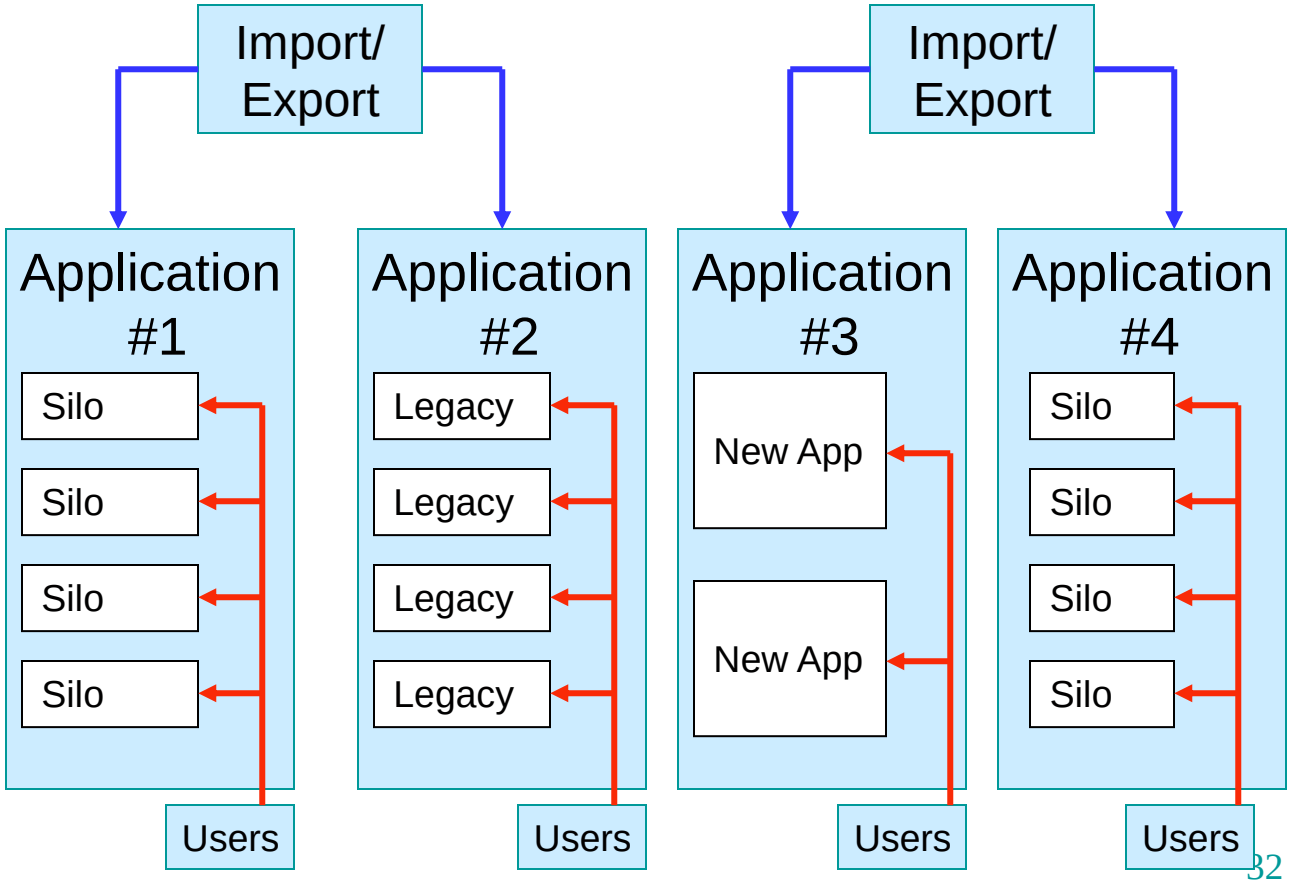
Web Services - Security

- 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

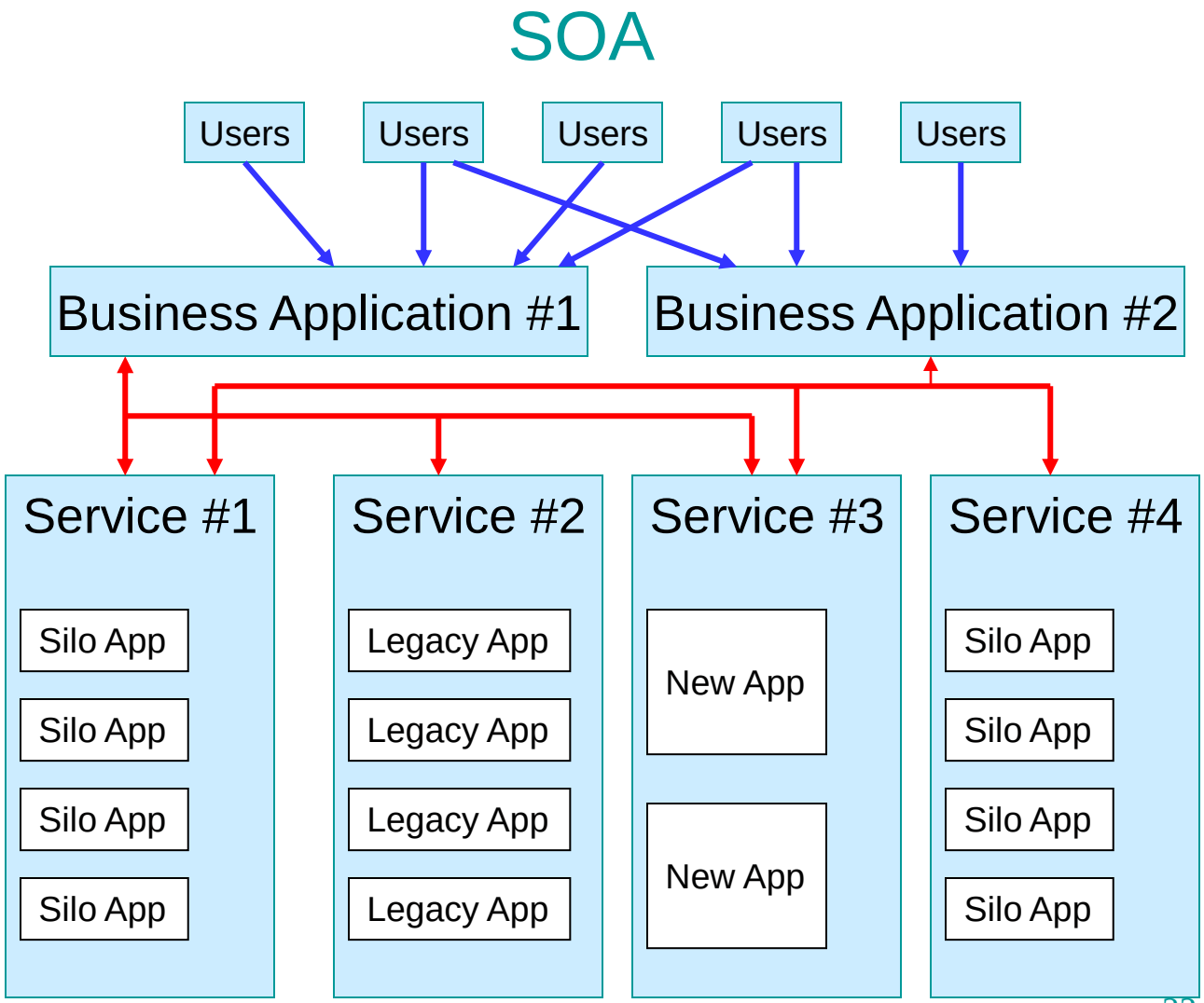
Web Services – Security

Traditional Architecture



MGS INC
Computer Business Solutions

Web Services – Security



MGS INC
Computer Business Solutions

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)

MGS INC
Computer Business Solutions

Security - Transport

- Transport Layer Security (TLS)
  - 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

MGS INC
Computer Business Solutions

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 encryption is more robust and the key cannot be externally provided as it is recreated for each session
  - 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

MGS INC
Computer Business Solutions

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

Questions?

- Thank you for your attention
- Are there any questions?

This presentation is available at:

www.mgsinc.com/download.html

MGS INC
Computer Business Solutions

Contact Information

- Michael Recant
  - VP Software Development
  - Mike.Recant@mgsinc.com
  - 11506 Allecingie Pkwy, Suite 2B
    Richmond, VA 23235
  - Phone: 804-379-0230
    Fax: 804-379-1299
  - www.mgsinc.com

MGS INC
Computer Business Solutions