UNITE 2010

Secure Communications from Workstation to Server

UNITE Conference
Baltimore, MD
Grand Ballroom 10
25 May 2010 @ 2:45pm

Session MCP4029

Guy Bonney
Mike Recant

MGS INC
Computer Business Solutions

MGS, Inc.

- Software Engineering, Product Development & Professional Services firm founded in 1986
- We solve business problems with:
  - Products: SightLine™, CheckOut, MGSWEB Web Services, Deliver, C.A.T.T. , SecureCATT, and others
  - Professional Services
    - IT Management Planning
    - Capacity Planning and Management
    - Consulting and Technical Services including Performance Management and Hardware-Software-Network Integration
    - Application Development Services including Java/J2EE development and platform rehosting
    - Training Services
  - Software Engineering Services on ClearPath MCP, Windows, and UNIX platforms.

MGS INC

Computer Business Solutions

Secure Communication

- Requirements
  - Legal Environment
  - Best-practices
- Technology
  - MCP Server Environment
  - Secure Connection
  - Secure Authentication

MGS INC
Computer Business Solutions

Privacy Issues

- Now universal issue due to public awareness (7 o'clock news) and legal 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

States also regulate privacy

- Almost all states have privacy laws
- California (lots of regulations)
- Maryland (strong notification)
- Massachusetts (strongest act at this point)

MGS INC
Computer Business Solutions

California Office of Privacy Protection

- http://www.privacy.ca.gov/privacy_laws.htm

- Security of Personal Information - Civil Code section 1798.81.5. This law requires specified businesses to use safeguards to ensure the security of Californians' personal information (defined as name plus SSN, driver's license/state ID, financial account number) and to contractually require third parties to do the same. It does not apply to businesses that are subject to certain other information security laws. Penalties for breach of $3,000 per violation plus direct damages and attorney's fees/costs.
- Social Security Number Confidentiality - Civil Code sections 1798.85-1798.86, 1785.11.1, and 1785.11.6. This law restricts businesses and state and local agencies from publicly posting or displaying Social Security numbers. It also bans embedding SSNs on a card or document using a bar code, chip, magnetic strip or other technology, in place of removing the number as required by law.

- 1798.85. (a) Except as provided in this section, a person or entity may not do any of the following: (1) Publicly post or publicly display in any manner an individual' s social security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise make available to the general public. (2) Print an individual's social security number on any card required for the individual to access products or services provided by the person or entity. **(3) Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.**

MGS INC
Computer Business Solutions

Maryland Privacy Act

- In January 2008, the Maryland Personal Information Protection Act (PIPA) went into effect. The law requires any business that keeps electronic records containing the personal identifying information of Maryland residents to notify those residents if their information is compromised. A security breach can occur when a company's website is hacked, a computer is stolen, or data tapes are lost in the mail. Notifying consumers of the breach will allow them to protect themselves from fraud and identity theft that may result from someone obtaining their personal information.

- http://www.oag.state.md.us/idtheft/breacheNotices.htm shows a list of security breach notices posted by the Maryland Attorney General

MGS INC
Computer Business Solutions

Maryland Information Security Breach Notices

Case Number	Date Received	Business Name	No. of MD residents	Total breach size	Information breached	How breach occurred
182323	10/20/2009 0:00	Easybakeware.com	217		name, credit card info	website hacked
182395	12/11/2009 0:00	InterContinental Hotels Group	428		name, payment card number, expiration date, verification code	malicious software on website
172597	7/8/2009 12:00:00 AM	Experian	20		name, DOB, SSN	Hacking
181665	8/6/2009 12:00:00 AM	Network Solutions, LLC	13030		Name, Payment Card info	Hacking
172560	5/4/2009	LexisNexis	896		Name, DOB, SSN	Obtained through fraudulent accounts
168294	04/08/09	Peninsula Orthopaedic Associates	81274		name, address, SSN, DOB, insurance plan #, Insurance ID #	backup tapes stolen en route to storage facility
164547	12/16/08	Fiserv, Inc.		160000	unknown	online bill payment traffic redirected to hacker website in Ukraine
159174	10/03/08	The Image Group of Toledo, Inc	258		name, credit and debit card information	e-commerce website hacked with SQL injection virus
147639	02/05/08	Davidson Companies		230000		hacking: spyware used to gain access to company database
146156	01/22/08	Science Applications International Corporation (SAIC)	3		credit card # and security code, name, billing and shipping address, phone and fax number	hacking, malicious software uploaded to e-commerce website

MGS INC
Computer Business Solutions

Massachusetts Privacy Act

- Mass 201 CMR 17.00
  - Requires that Sensitive Personal Information (SPI) for a “person” (includes companies) resident in MASS must be protected.
  - SPI includes:
    - SSN
    - Driver’s license or Government ID #
    - Financial Account numbers
  - Requires a Compliance Program
  - Requires annual Compliance Audits

MGS INC
Computer Business Solutions

Massachusetts - continued

- Mass 201 CMR 17:00 – for ALL systems with sensitive personal information:
  - Requires secure authentication
  - Requires transmission encryption
  - Requires encryption of data stored on laptops and portable devices
  - Requires firewall protection and OS security patches for systems connected to the internet
  - Requires malware and antivirus software on internet connections

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, adhering to standards for PINS, adhering to DSS, and use of certified applications.

MGS INC
Computer Business Solutions

PCI – DSS Requirements

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
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for employees and contractors

MGS INC
Computer Business Solutions

We Are Responsible

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

Privacy Best Practices

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

MGS INC
Computer Business Solutions

Secure Communication

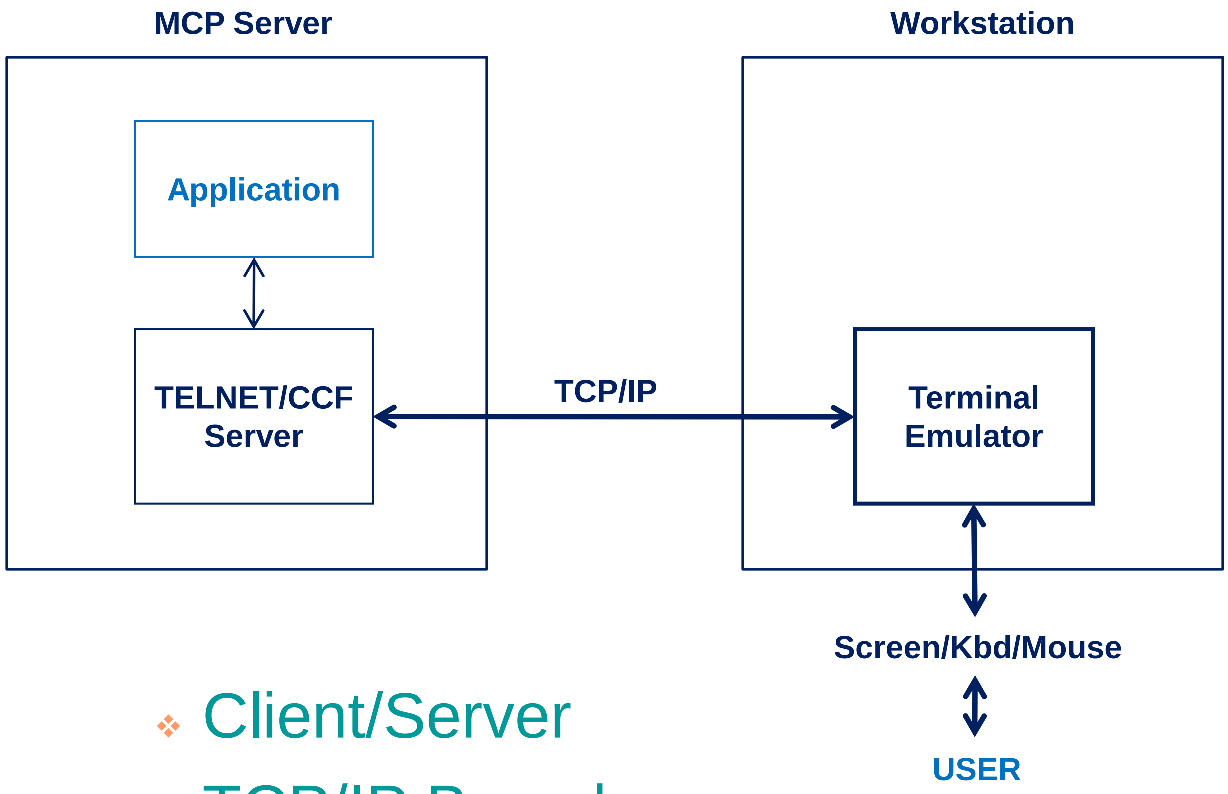
- Moving sensitive data from host to workstation and back is simple – or is it?
- We must discuss connections, encryption, and authentication to understand the entire picture.

MGS INC
Computer Business Solutions

Secure 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

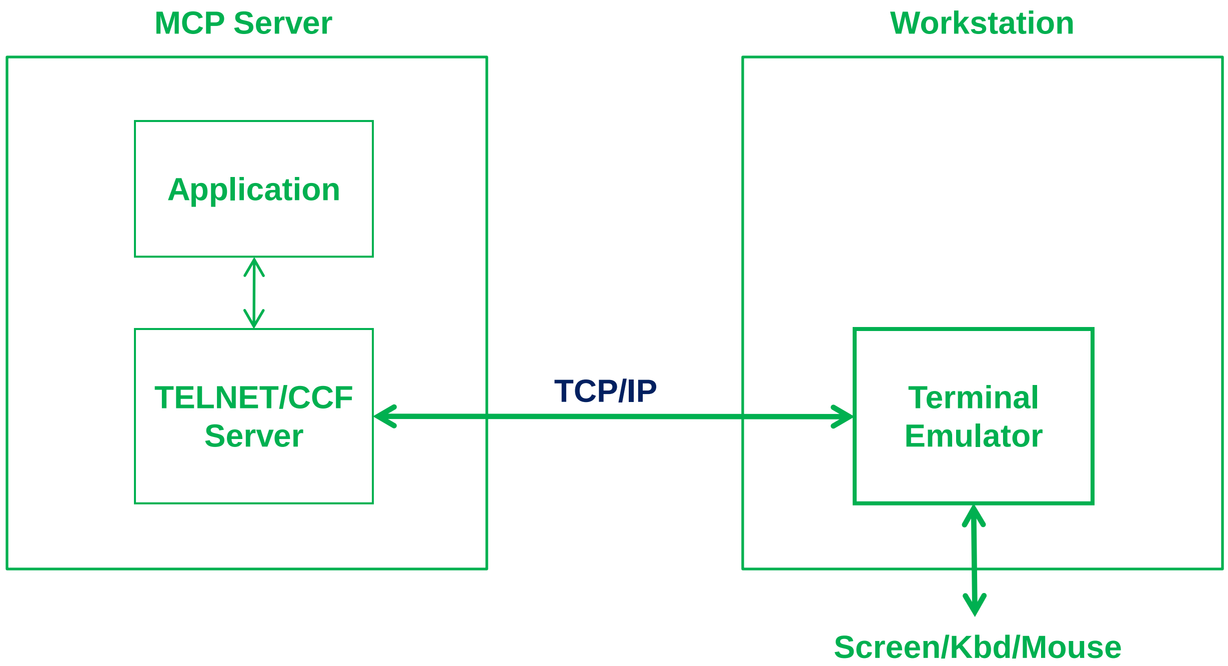
Basic MCP Connection



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

MGS INC
Computer Business Solutions

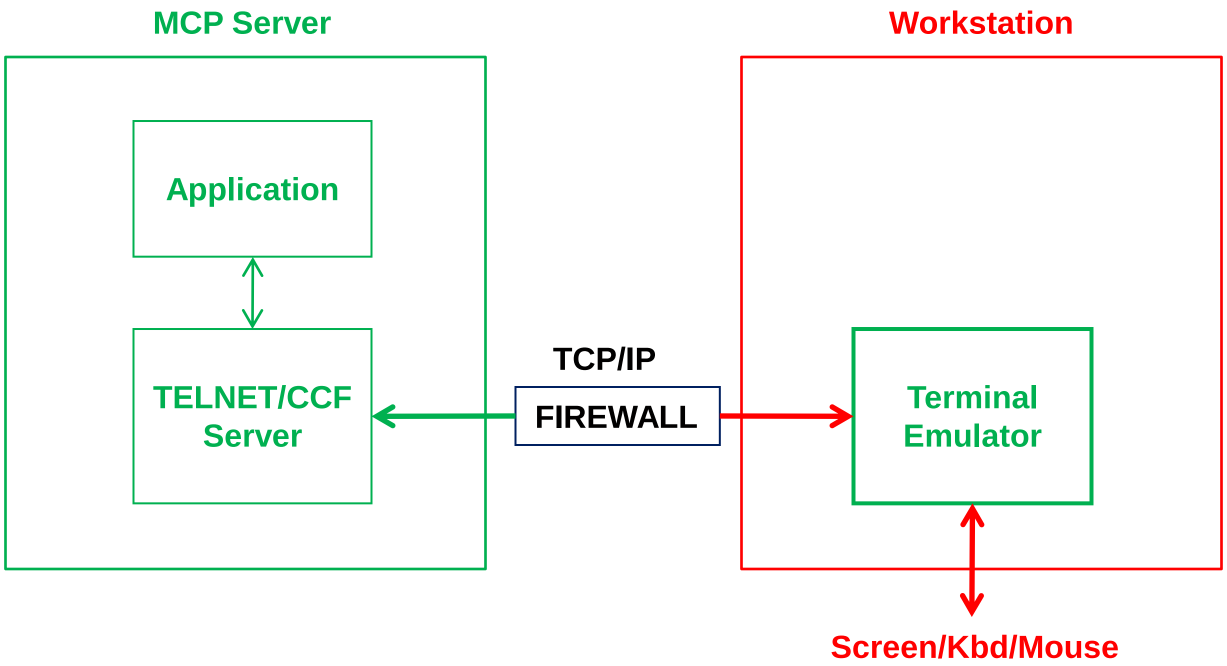
Trusted Basic Connection



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

MGS INC
Computer Business Solutions

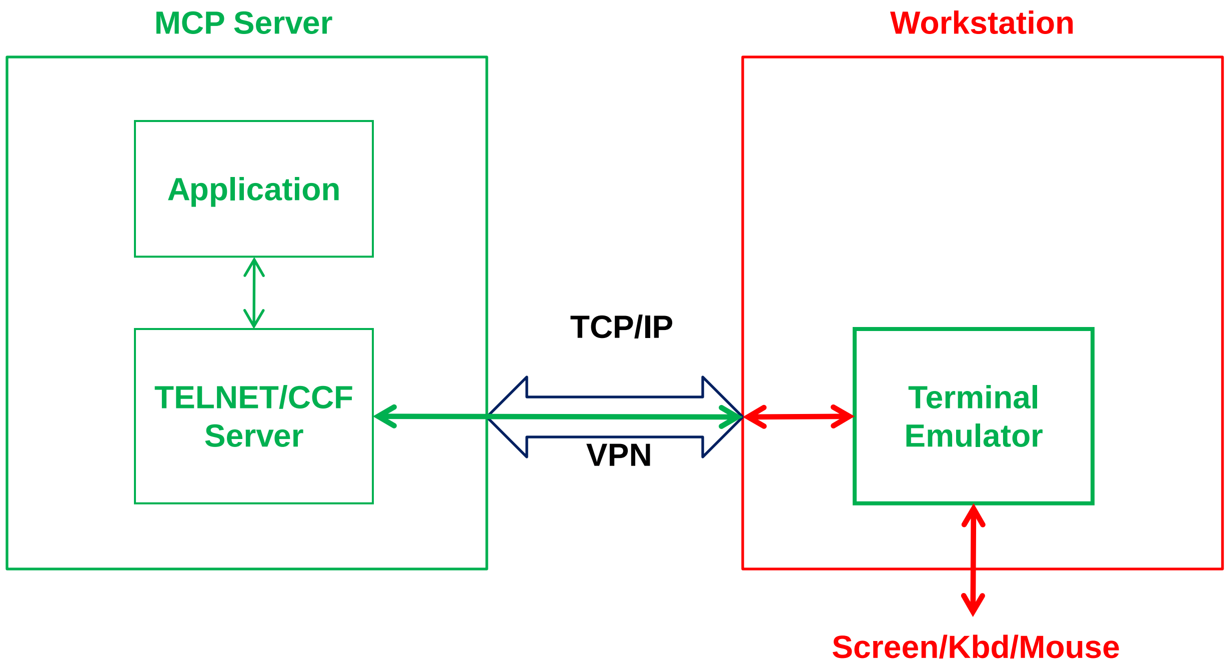
Untrusted Basic Connection



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

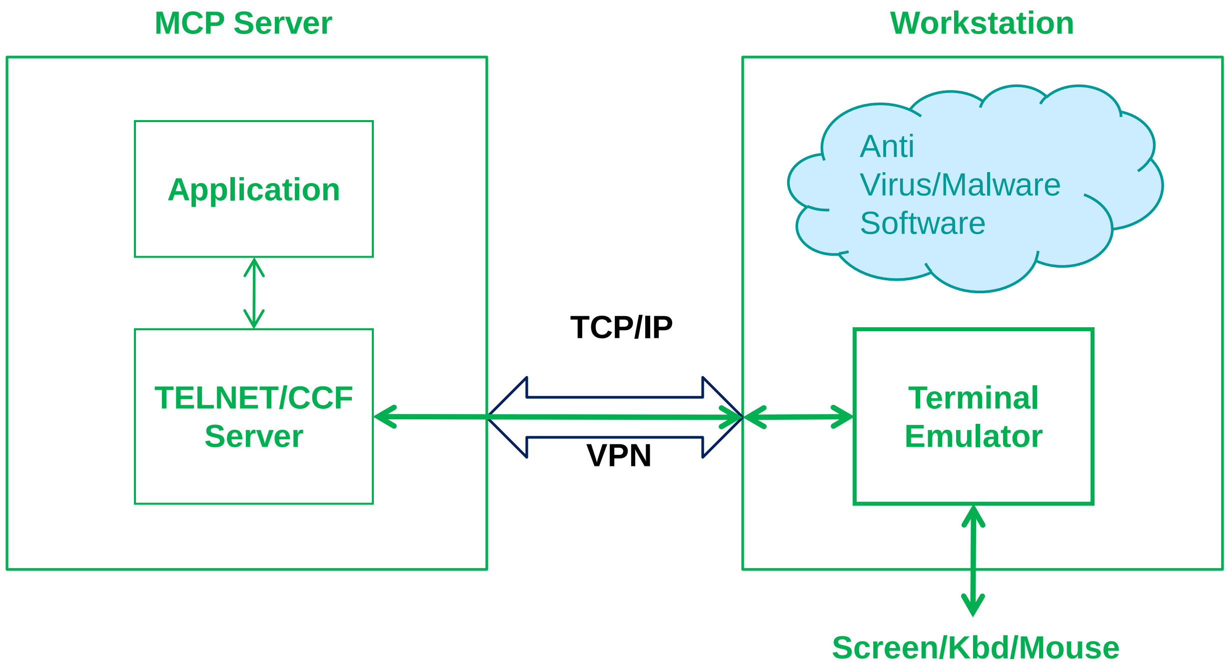
MGS INC
Computer Business Solutions

Virtual Private Network Connection



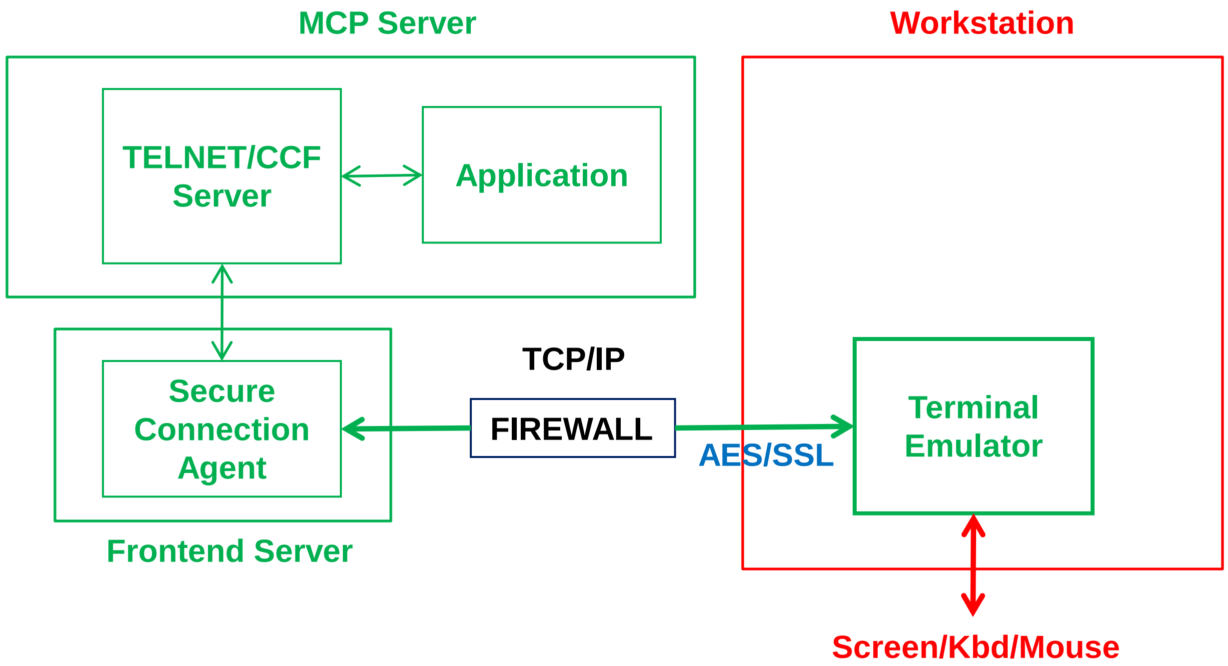
- Server is secure
- Server LAN is secure
- VPN to server is secure (IPSEC)
- Client is not secure

Virtual Private Network Connection



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

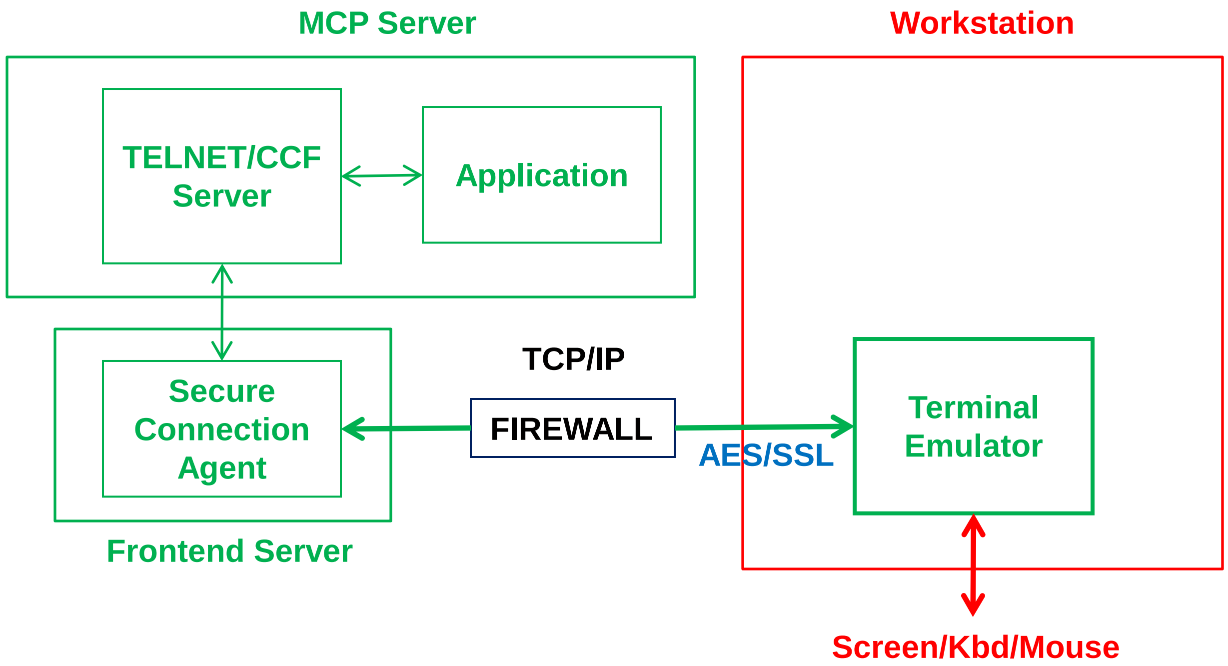
3-Tier Secure Connection



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

MGS INC
Computer Business Solutions

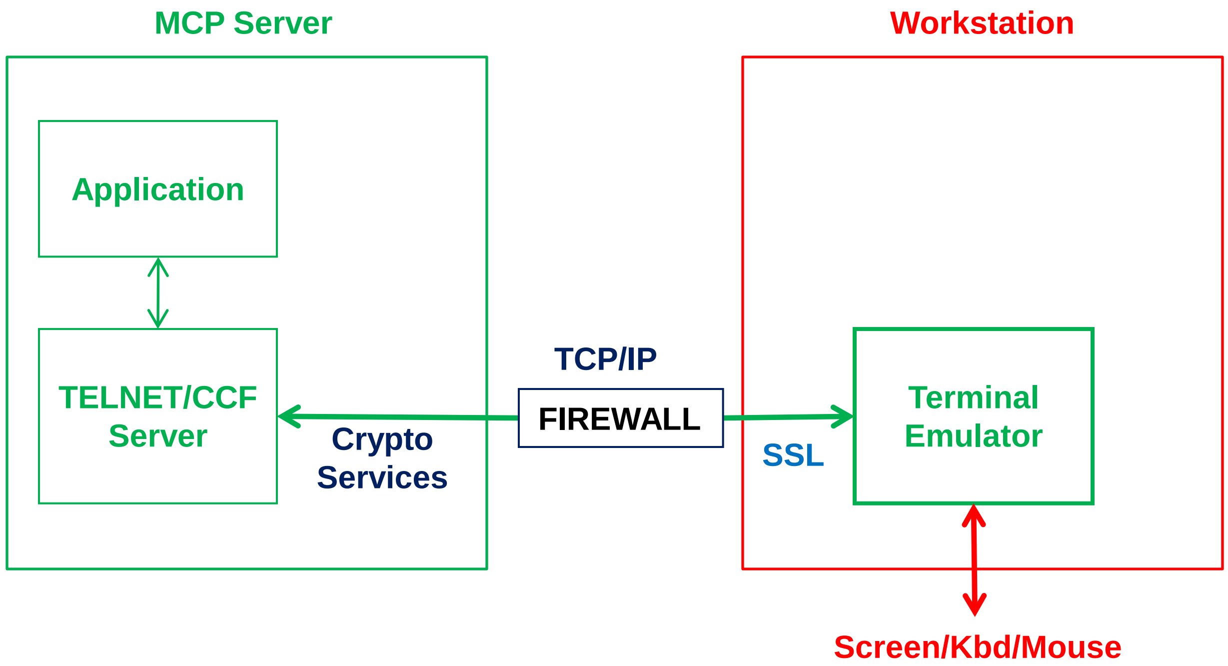
3-Tier Secure Connection



- Examples:
  - MGS SecureCATT
  - Unisys Secure Web Enabler (MCP 11 and 12)

MGS INC
Computer Business Solutions

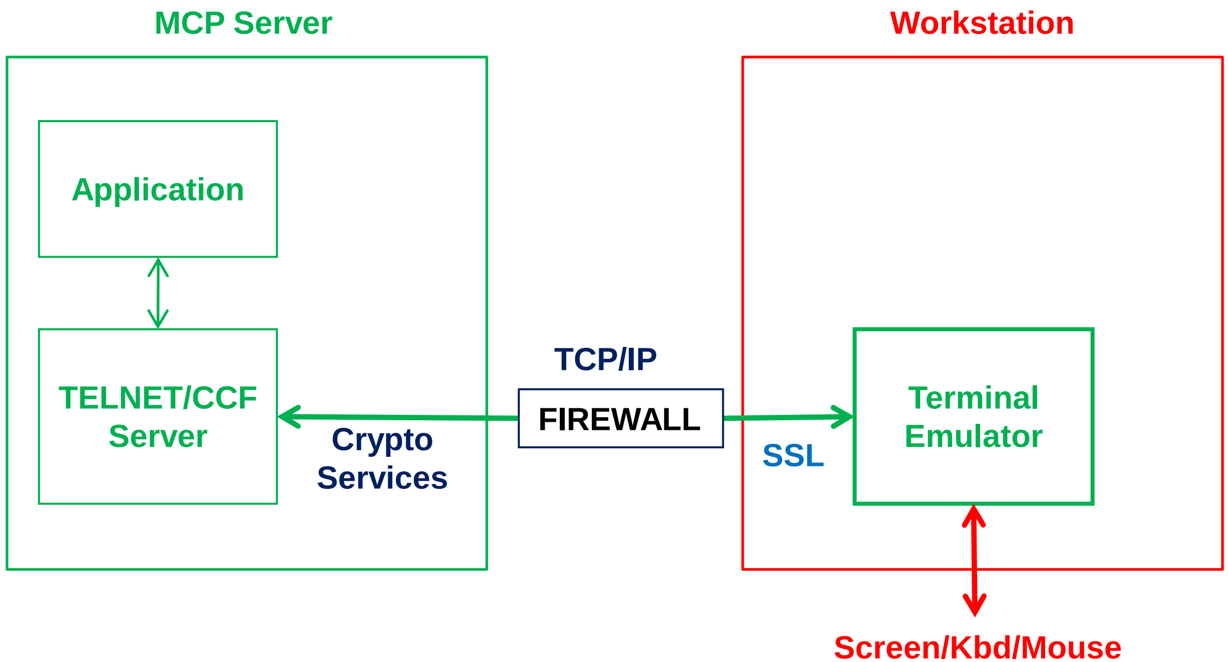
2-Tier Secure Connection



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

Computer Business Solutions

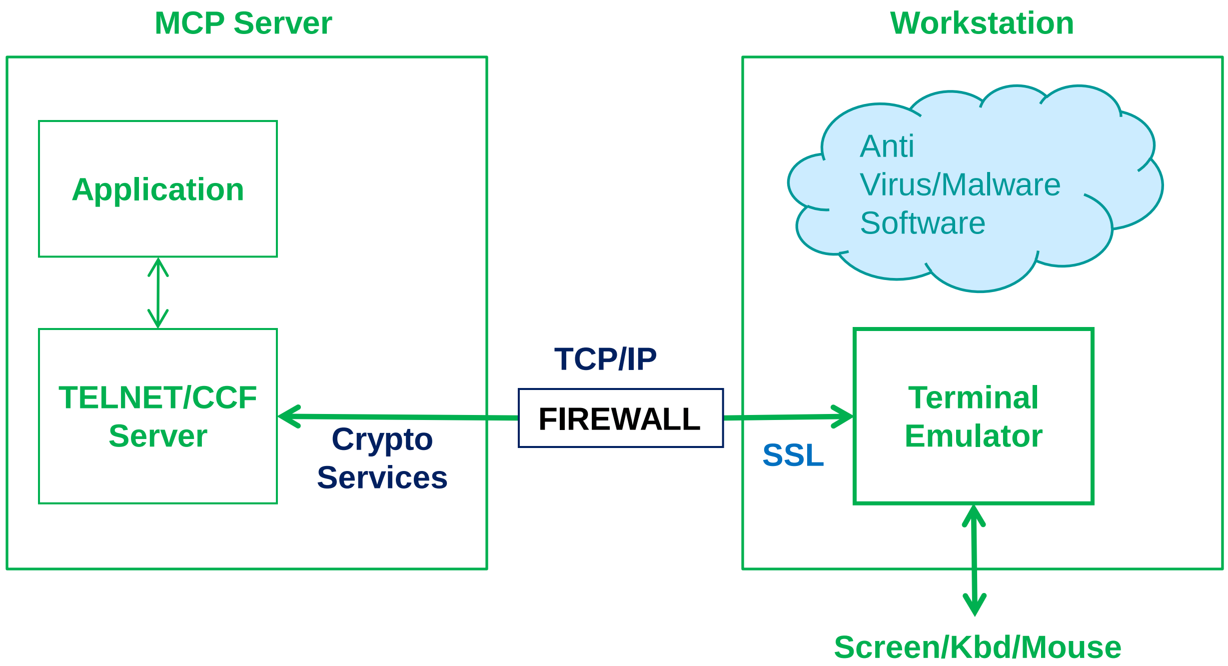
2-Tier Secure Connection



- Requires MCP 13
- Examples:
  - MGS C.A.T.T.
  - Unisys Secure Web Enabler
  - Attachmate Infoconnect v8.1 SP1

MGS INC
Computer Business Solutions

2-Tier Secure Connection



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

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

MGS INC
Computer Business Solutions

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 (MCP 13)

MGS INC
Computer Business Solutions

Authentication

- Secured Connection
  - Identification still an issue
  - Usercode/password insufficient
  - Traditional SSL (Server-side) only positively IDs server
  - Options:
    - Validate remote IP Address
    - Client-side SSL
    - “Physical” passwords

MGS INC
Computer Business Solutions

Authentication

- Validate Remote IP Address
  - MCP system can validate IP Address
  - Works best with 2-Tier Secure Connection
  - 3-Tier Secure Connection requires front-end support to propagate Remote IP Address
  - Downsides:
    - Spoofing (unlikely)
    - Network Address Translation

MGS INC
Computer Business Solutions

Questions?

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

This presentation will be available Thursday for download today at:

www.mgsinc.com/download.html

MGS INC
Computer Business Solutions

URLs of Interest

- http://search.usa.gov/search?locale=en&m=false&query=Privacy+Laws
- http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
- http://www.business.gov/business-law/privacy/
- https://www.pcisecuritystandards.org/index.shtml

MGS INC

Computer Business Solutions

Contact Information

- Guy Bonney
  - President, MGS, Inc.
  - Guy.Bonney@mgsinc.com
  - 804-379-0230 x11
  - www.mgsinc.com

- Mike Recant
  - VP Software Development
  - Mike.Recant@mgsinc.com
  - 804-379-0230 x12

MGS INC
Computer Business Solutions