

# Internet & V5R1 Security

By  
Wayne O. Evans

---

---

---

---

---

---

---


---

## iSeries & AS/400 Security

**DISCLAIMER**  
The security recommendations and any programming source are offered "AS IS" for your consideration. Wayne O. Evans consulting makes no warranties or representations as to the quality of the examples. ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE SPECIFICALLY DISCLAIMED

**REPRODUCTION**  
permission is granted to make a limited number of copies of this material for non-commercial purposes, provided this page and the title page are included with all copies.

AS/400 and OS/400 are registered trademarks of the IBM corporation



**Wayne O Evans**  
5677 West Circle Z St  
Tucson, AZ 85713  
Tel (520)-578-7785  
Fax (520)-578-7786  
WOEvans@aol.com

---

---

---

---

---

---

---

---

## Agenda

- Internet security exposures
  - Active and passive attacks
- OS/400 V5R1 enhancements

---

---

---

---

---

---

---

---

## Internet Security Threats

- Large numbers of users on the internet
- Small percentage attempt harmful actions
  - Hackers are informal groups of individuals that share
    - Tips and tools on hacking
    - Lists of sites exploited

E  
X  
P  
O  
S  
U  
R  
E

---

---

---

---

---

---

---

---

## Internet Security Threats

- Graffiti
- Spoofing
- Sniffing
- Denial of service

E  
X  
P  
O  
S  
U  
R  
E

---

---

---

---

---

---

---

---

## Graffiti

Results of a Graffiti attack on the Spice Girls Home page



- Hackers modify the home page to add their own message
- Sights that have been compromised include FBI, NASA, COKE, YAHOO

E  
X  
P  
O  
S  
U  
R  
E

---

---

---

---

---

---


---

---

# Graffiti

**Yahoo  
page  
after  
attack**

P4NTZ/H4Gis - WORLD  
DOM1N4T10N '97



For the past month, anyone who has viewed Yahoo's page & used their search engine, now has a logic bomb/worm implanted deep within their computer.

The worm part of this 'virus,' (in layman's terms) spreads itself across internal networks that the infected machine is on.  
Binary programs are also infected.

On Christmas Day, 1998, the logic bomb part of this 'virus,' will become active, wreaking havoc upon the entire planet's networks.

E  
X  
P  
O  
S  
U  
R  
E

■ For a detailed list of sites that have hackers have modified see

[//www.antonline.com/archives/pages/](http://www.antonline.com/archives/pages/)

---

---

---

---

---

---

---

---

---

---

## Preventing Graffiti

- Government and commercial web sites have been vandalized in the past
- Use resource security to prevent write access by \*PUBLIC and QTMHTTP user profile
- Use server directives to explicitly control actions of users

---

---

---

---

---

---

---

---

---

---

## Thwarting Graffiti Artists and Crackers

- If you are not using HTTP
  - Prevent automatic HTTP server start

**CHGHTTPA AUTOSTART(\*NO)**

  - Prevent HTTP server start by disabling the QTMHTTP user profile
- If you are running HTTP
  - Do not allow directories to be viewed
  - Only run the \*ADMIN server instance to perform administrative functions
  - Use secure sockets when running \*ADMIN functions

---

---

---

---

---

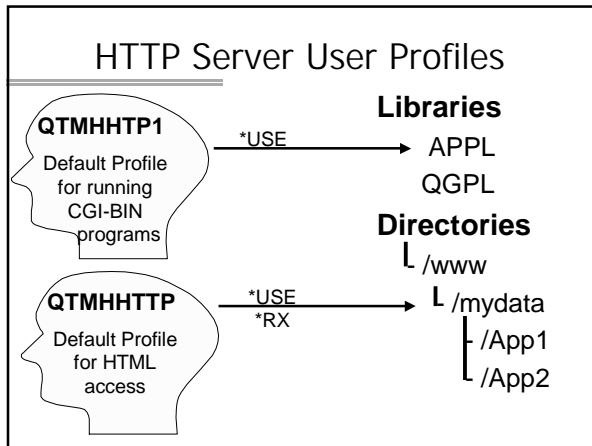
---

---

---

---

---




---

---

---

---

---

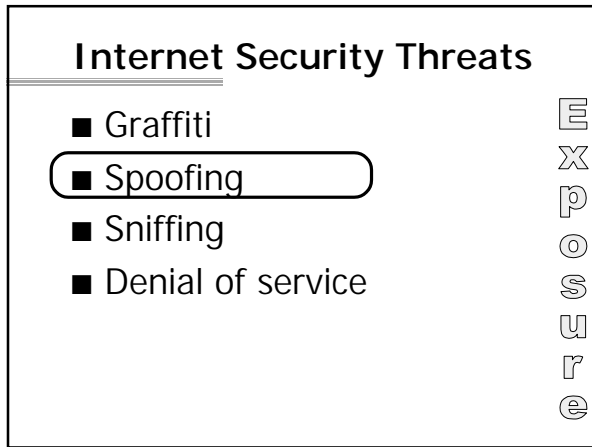
---

---

---

---

---




---

---

---

---

---

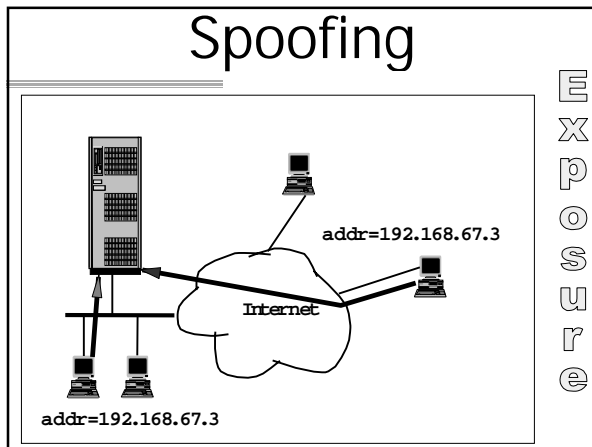
---

---

---

---

---




---

---

---

---

---

---

---

---

---

---

## Spoofting

- Attack where IP address is changed to appear to be a trusted location
- Security design should not be dependent upon IP address

E  
X  
P  
O  
S  
U  
R  
E

---

---

---

---

---

---

---

---

## Internet Security Threats

- Graffiti
- Spoofting
- Sniffing
- Denial of service

E  
X  
P  
O  
S  
U  
R  
E

---

---

---

---

---

---

---

---

## Sniffing

- The TCP/IP allows systems in network to view transactions
  - Viewing of passwords is possible
  - Viewing of credit card transactions
- Protect confidentiality with encryption of sensitive data

E  
X  
P  
O  
S  
U  
R  
E

---

---

---

---

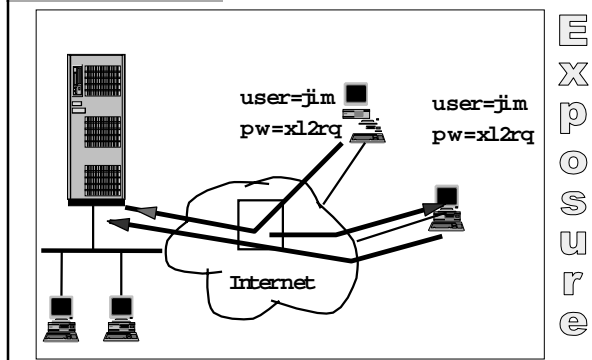
---

---

---

---

# Sniffing



---

---

---

---

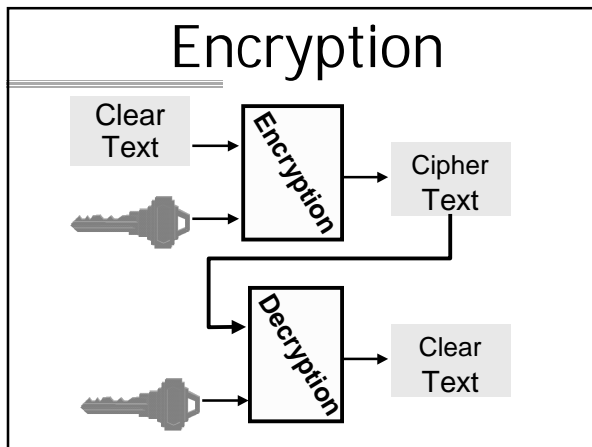
---

---

---

---

# Encryption



---

---

---

---

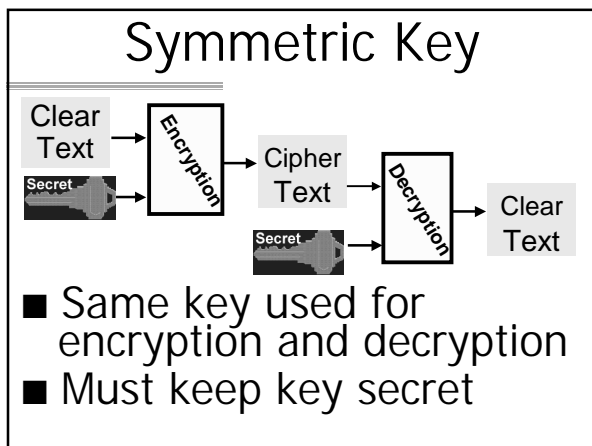
---

---

---

---

# Symmetric Key



---

---

---

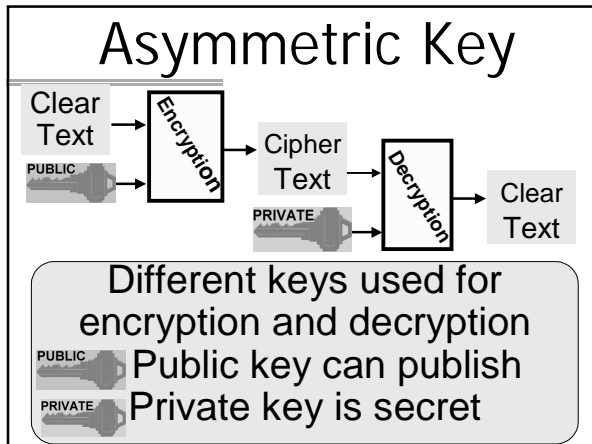
---

---

---

---

---




---

---

---

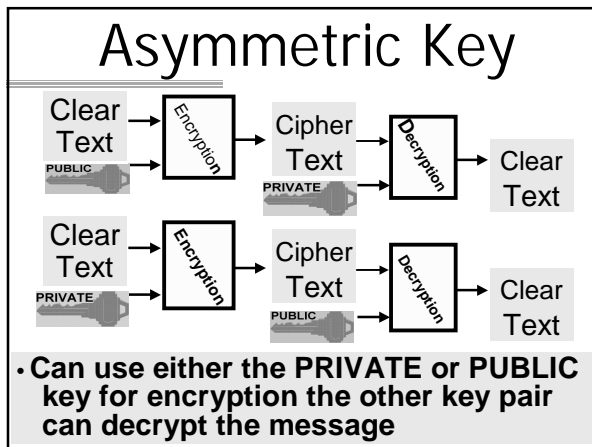
---

---

---

---

---




---

---

---

---

---

---

---

---

- ## Encryption
- **Symmetric (secret key)**
    - Same key to encrypt and decrypt data
    - Must keep key secret
    - Relatively fast
    - Example: DES (data encryption standard)
  - **Asymmetric (public key)**
    - Different keys to encrypt and decrypt
    - Public encryption key can be published
    - More computation overhead than symmetric key
    - Example: RSA and PGP

---

---

---

---

---

---

---

---

# Certificate



A digital certificate is like a passport



- Establishes the holders identity
- Issued by an certificate authority

---

---

---

---

---

---

---

---

## Certificate

A certificate associates a participant to public key

### Digital Certificate

- |   |  |
|---|--|
| Wayne O Evans   | ■ "Distinguished name"                         |
| Tucson, Arizona   | holders name and address                       |
| May 8, 2001   | ■ Creation date                                |
| May 8, 2003   | ■ Expiration date                              |
|  | ■ Public key of HOLDER                         |
|  | ■ Digital signature of certification authority |

---

---

---

---

---

---

---

---

## Uses of a Digital Certificate



- Authentication of holder
- Privacy of transaction
- Integrity of transaction
- Non-repudiation

---

---

---

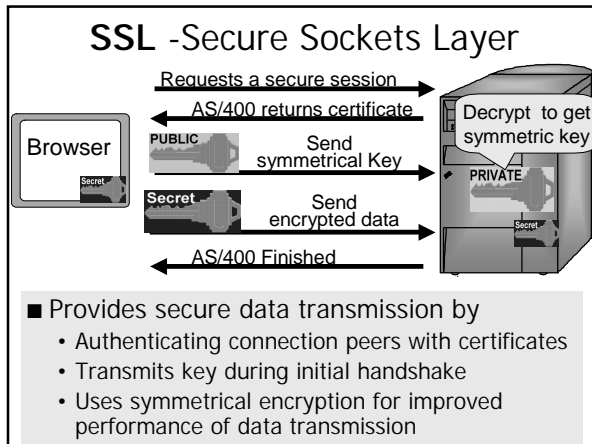
---

---

---

---

---




---

---

---

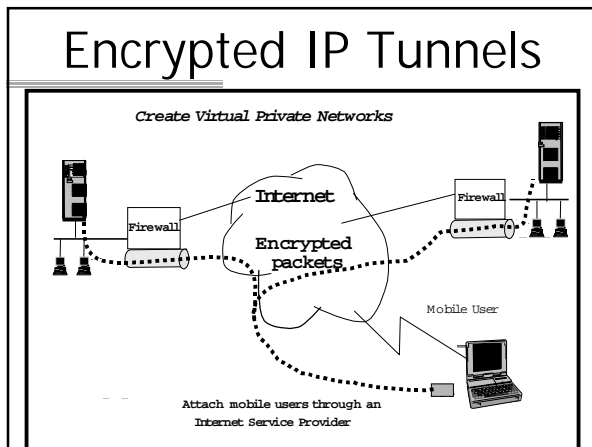
---

---

---

---

---




---

---

---

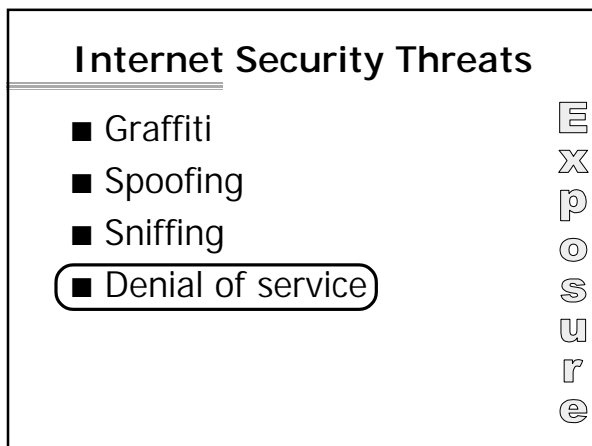
---

---

---

---

---




---

---

---

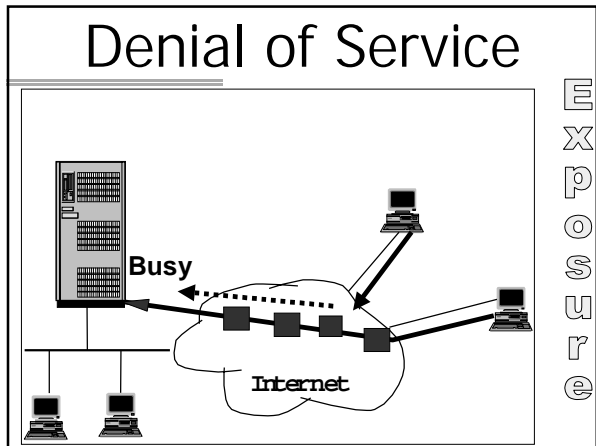
---

---

---

---

---




---

---

---

---

---

---

---

---

## Denial of Service

- Attack where system is flooded with requests so that users can not perform normal activity
- The denial of service attack does not mean your system security has been compromised but the system is kept busy and cannot perform normal work
- Use a separate processor for web access

E  
X  
P  
O  
S  
U  
R  
E

---

---

---

---

---

---

---

---

## Internet Connection Wizard

- IBM guidelines based on input of i400 users
- Based on User Centered Design (UCD) testing performed in the Rochester lab
- The wizard is organized around three common scenarios:
  1. Behind a firewall
  2. Outside a firewall
  3. Directly connecting through a dial-up connection

<http://www.iseries.ibm.com/tcpip/iwizard.htm>

---

---

---

---

---

---

---

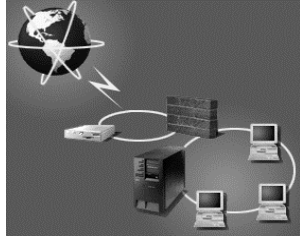
---

## Recommended Configurations

### Behind the Firewall

•Configure a connection to the network

- Configure routes to your firewall and intranet
- Protect with IP Packet Filtering
- Configure a public IP address for the i400 (Virtual IP)
- Configure i400 as a Web Server
- Configure your i400 as an HTTP proxy server



The most common Internet scenario for i400 users

---

---

---

---

---

---

---

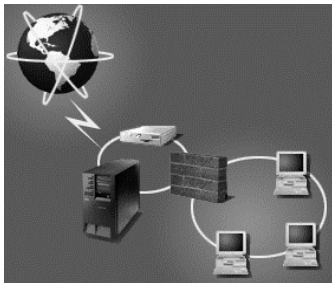
---

## Recommended Configurations

### On the DMZ (boundary network)

•Configure a connection to the network

- Configure routes to your firewall and intranet
- Protect using IP Packet filtering
- Configure i400 as a Web Server
- Configure as an HTTP proxy server



---

---

---

---

---

---

---

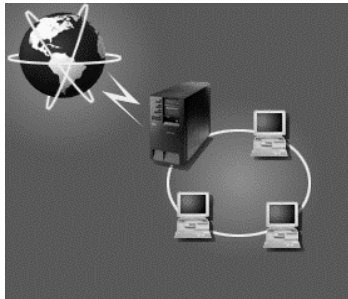
---

## Recommended Configurations

### Direct Connect

•Configure a dial-up (modem) connection to your ISP

- Configure i400 connection to intranet
- Configure i400 as an HTTP proxy server



---

---

---

---

---

---

---

---

### Recommended Configurations

**Internet only system** (Sacrificial Internet System)

- Configure i400 connection to internet
- Configure non TCP/IP connection to production i400
- Production i400 has no internet connection

Connection not TCP/IP

Avoids multiple platforms and easy to configure but more \$\$

---

---

---

---

---

---

---

---

### Security Enhancements

- Object Signature to Detect Tampering
- Password Length
- Program Observability
- Additional Encryption Standard
- IBM 4758 Cryptographic Coprocessor
- Kerberos Client

---

---

---

---

---

---

---

---

### Object Signing Enhancements V5R1

**New support allows signing of all AS/400 executables**

- Detect tampering of software
- Verify the origin of software

**Verification of Signed Executables**

- OS/400, LPPs and PTFs are signed
- New APIs allow for signing of user applications
- GUI interface in DCM provides signing interface
- Verification occurs during restore
- Verification via CHKOBJITG command

---

---

---

---

---

---

---

---

User profile password enhancement V5R1

---

**New system value QPWLVL**

- Controls the password level of the system
  - **0** - 10 byte length and netserver pwds are retained
  - **1** - 10 byte length and netserver pwds are eliminated
  - **2** - 128 character length, old and new pwds formats are retained
  - **3** - 128 character length, old pwd formats are removed

..

---

---

---

---

---

---

---

---

User profile password enhancement V5R1

---

**New system value QPWLVL**

- Controls the password level of the system

<b>QPWLVL</b>			
Len	Char Set	Old Passwords	
<b>0</b>	10 Name	netserver pwds are retained	
<b>1</b>	10 Name	netserver pwds are eliminated	
<b>2</b>	128 Expanded	formats are retained	
<b>3</b>	128 Expanded	formats are removed	

- Change is effective on then next IPL

---

---

---

---

---

---

---

---

User Profile Password Rules V5R1

---

**QPWLVL 2 and 3 Expanded Character Set**

- Password length, 1 - 128 characters
- User profile passwords are case sensitive
- Imbedded blanks are allowed, "This is my New Password"
- Trailing blanks are removed, password cannot be all blanks

Default is PWDLVL 0, V4R5 rules, 10 character limit with restricted character set

---

---

---

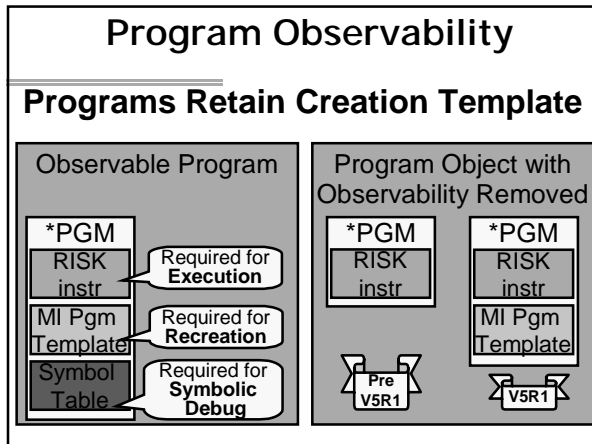
---

---

---

---

---




---

---

---

---

---

---

---

---

---

---

### Program Observability

#### Programs Retain Creation Template

- No user interface to access the program creation data after observability is removed
- Allows re-creation of the program object in order to help assure integrity
- Enables program recreation for new hardware or improved translator technology
- NOTE: Program size will be greater in V5R1 than a program with observability removed in a previous release

Change will not affect typical installation

---

---

---

---

---

---

---

---

---

---

### Advanced Encryption Standard

#### New data encryption standard being adopted to replace long time standard Data Encryption Standard (DES)

- Rijndael Algorithm
- For application use through the MI CIPHER instruction
- Faster than DES

DES will continue to be supported  
 Change is not important to typical installation

---

---

---

---

---

---

---

---

---

---

## Hardware Cryptography

V5R1

### SSL Usage of IBM 4758 Cryptographic Coprocessor



- SSL is enabled to use the 4758 for SSL Handshake processing
- To enable SSL usage of the 4758 card:
  - Configure 4758 card via V5R1 GUI
  - Change DCM configuration to indicate that card is to be used for an application's SSL processing
  - Any application enabled to use SSL can then take advantage of the 4758 card
- Two methods of using the card:
  - Create and store private key on the 4758 card takes advantage of 4758 card's key storage security
  - Create and store private key in software encrypted with master key of 4758 card allows load balancing of SSL Handshake processing across multiple 4758 cards

---

---

---

---

---

---

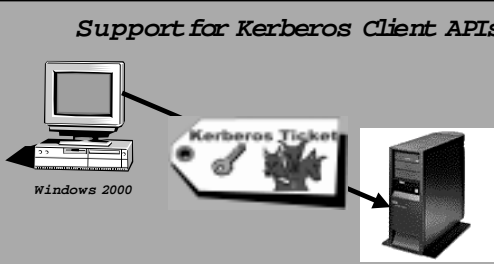
---

---

## Kerberos Client APIs

V5R1

*Support for Kerberos Client APIs*



An OS/400 Application can use the **Kerberos** client APIs to authenticate users

---

---

---

---


---

---


---

---

## What is Kerberos?



- Kerberos is a three party network authentication protocol designed by MIT
- Kerberos is designed to provide strong authentication for client/server applications by using secret-key cryptography.



The name Kerberos comes from Greek mythology; it is the three-headed dog that guarded the entrance to Hades.

---

---

---

---

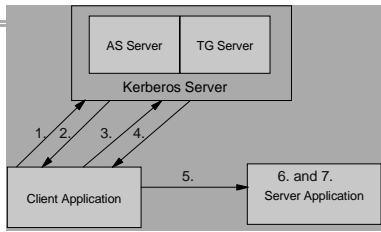
---

---

---

---

## How Does Kerberos Work?



1. Clients request ticket-granting-ticket (TGT) from a Kerberos Authentication Server (AS)
  2. Kerberos AS server returns TGT to client
- Note: 1. and 2. often occur at initial login  
-- not at application runtime

---

---

---

---

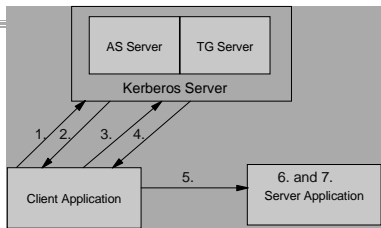
---

---

---

---

## How Does Kerberos Work?



3. Clients request service-ticket (ST) from Kerberos Ticket Granting server passing in the TGT received in previous step.
4. Kerberos TG server returns the ST to the client

---

---

---

---

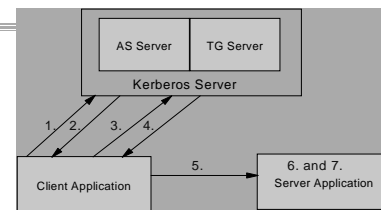
---

---

---

---

## How Does Kerberos Work?



5. Clients pass ST to application providing desired service (not part of Kerberos or GSS API protocols)
6. Server application verifies the ST is valid and determines who is requesting the service (who the user is)
7. Server enforces whatever security semantics it wishes

---

---

---

---

---

---

---

---

## Kerberos Client APIs

- **GSS API**
  - An API for secure exchange of information between applications
  - Generic Security Service (GSS) Application Programming Interface (API) defined in RFCs1509, 1964, and 2078
- **Kerberos**
  - Three party distributed authentication protocol
  - Kerberos Version 5 protocol (RFC 1510)
  - Many of the defacto standard Kerberos protocol APIs that are prevalent in the industry today
  - Shipped as V4R5 PTFs (SF63662), part of base in V5R1

---

---

---

---

---

---

---

---

## Comparison

### SSL advantages over Kerberos?

- SSL doesn't require an accessible trusted third party
- SSL can be used to establish a secure connection even when one end of the connection doesn't have a "secret" (a.k.a. "key" or "password").

SSL is ideal for secured Web communication where there is a large user base which is not known in advance

---

---

---

---

---

---

---

---

## Comparison

### What does Kerberos give me that SSL doesn't?

- **Key revocation**  
 Revocation of compromised certificate is not supported in SSL  
 Kerberos tickets become unusable as soon as any cached tickets expire, on the order of hours
- **Key security**  
 Verisign certificate has to live on hard disk  
 Kerberos does not require storage of any sort of certificate only a password which should not be written down

---

---

---


---

---

---

---

---



## Comparison

What does Kerberos give me that SSL doesn't?

- Open Standard
  - Kerberos doesn't infringe on any patents.
  - Kerberos standards documenting have been developed openly for free from the start
- Flexibility
  - Changing to a new authentication technology (new kind of SmartCard with its own algorithm) has no impact on clients only KDC

Kerberos was developed by MIT and is widely used in the academic community and is required to connect to some networks

---

---

---


---

---

---

---

---



## More Information

- Bill Bryant, "Designing an Authentication System: A Dialogue in Four Scenes"  
<<http://web.mit.edu/kerberos/www/dialogue.html>>  
>  
Explanation of Kerberos protocol, in plain English.
- Jeffrey I. Schiller, "Secure Distributed Computing", Scientific American, November 1994, pp 72-76.  
Overview that covers the Kerberos protocol and how Kerberos is used at MIT
- The MIT Kerberos web page  
<<http://web.mit.edu/kerberos/www/>>  
Has many links pointing to Kerberos resources

---

---

---


---

---

---

---

---



## Conclusion

---

---

---

---

---

---

---

---

## Internet Security Principles

- Simplicity of security design
  - Multiple layers of protection
- Testing of applications
- Education of users

---

---

---

---

---

---

---

---

## AS/400 Internet Summary

- AS/400 makes a good internet server
  - Security built in
  - Strong host level security
  - Security integrated into communication security

---

---

---

---

---

---

---

---

## QUESTIONS



- If you have additional questions or want more information please contact me

**Wayne O. Evans**

Phone (520) 578-7785  
Fax (520) 578-7786

WOEvans@AOL.com  
home page: WWW.WOEVANS.COM

---

---

---

---

---

---

---

---