Cross Platform Security using IBM's Websphere; take the Security Challenge!

Paul de Graaff
IBM Field Technical Sales Specialist

graaff@us.ibm.com

Acknowledgement

- Daniel TumSuden - IBM/Tivoli Systems
Agenda

- Introduction
- Authentication
- Websphere Authentication
- Websphere Single Signon
- Websphere Authorizations
- Websphere Application Security

Introduction
What is Security?

- measures taken to guard against espionage or sabotage, crime attack or escape
- freedom from danger
- freedom from fear or anxiety

Note: Merriam-Webster's Collegiate Dictionary

- protection from unwanted attacks!

Note: W. Kou Networking Security and Standards

Should we care about Security?

- Computer World Article 01/03/2001

CIOs not worried about Security !!!!!!!!
Elements of Websphere Security

Websphere Resources

Websphere Security

JAVA Security

CORBA Security

EJB Security

Java Security Classes

JVM

Platform Security

Operating System Security

Websphere Security Architecture

Web client

HTTP

Web Server

Security Plug-in

Security Application

Administrative Server

Application Server

Security Collaborator

access control

WebServer Resources

HTML

CGIs

Images

Websphere Resources

EJBs

JSPs

Servlets

stand-alone or java client or applet
Authentication

Architecture Choices for Web Security

- Where to authenticate: On a multipurpose web server, or a hardened gateway?

- Where to place web servers: in a DMZ, or in a trusted zone?

- How many entry points to your secured network - many or few?

- How many software distribution points - many or few?

- Entry-point security only, or End-to-End security?
Where to Authenticate: on a multipurpose web server, or on a hardened gateway? (scenario 1)

### Architecture Choice 1:

**Customers**

**Partners**

**Hackers**

(If authenticating users on a multipurpose web server)

Note: These Web servers have access to sensitive data

Some security designs run authentication checks only once a user reaches your web servers. Hackers and others without credentials will reach...

...a non-hardened box having access to sensitive data, leaving little or no margin for error with any security weakness.

Firewall Layer(s) let thru http traffic

Hackers are not challenged until they reach web servers. The web servers are not hardened, and they have access to sensitive data.

Enterprise Data

Where to Authenticate: on a multipurpose web server, or on a hardened gateway? (scenario 2)

### Architecture Choice 1:

**Customers**

**Partners**

**Hackers**

(If authenticating on a hardened gateway)

Note: These Web servers have access to sensitive data

Security checks stop hackers here at the hardened gateway

Users without credentials are stopped here at the hardened gateway

Best security practices recommend defense in depth: Stopping unauthenticated users in the DMZ (above) ......

......and securing machines with access to sensitive data in a more trusted layer (here).
Where to place web servers: in a DMZ, or in a trusted layer? (scenario 1)

**Architecture Choice 1:**

- **Hackers**
- **Internet Zone**
- **DMZ**
- **Trusted Zone**

*Firewall Layer(1) lets thru http traffic*

*Note: These Web servers have access to sensitive data*

*Some security tools can only authenticate at your web servers. To keep unauthenticated users out of the trusted zone, you must move your web servers into the DMZ ……*

*This does not offer protection as strong as placing your web servers in the trusted zone.*

Where to place web servers: in a DMZ, or in a trusted layer? (scenario 2)

**Architecture Choice 2:**

- **Hackers**
- **Internet Zone**
- **DMZ**
- **Trusted Zone**

*Firewall Layer(1) lets thru http traffic*

*Security checks stop hackers here in the DMZ*

*Users without proper credentials are stopped here in the DMZ*

*Best security practices recommend defense in depth: Stopping unauthenticated users on a hardened machine in the DMZ (above) ……*
Architecture Choice 3:

How many entry points to your secured network:
many or few? (scenario with "many")

(if using many entry points)

Architecture Choice 3:

How many entry points to your secured network:
many or few? (scenario with "few")

(if using few entry points)

......While other security designs let you open only a few entry points into your secured network, regardless of the number of web servers you are protecting.
How many entry points to your secured network: many or few? (potential exposure with “many”)

(if using many entry points - an example)

“oops...we forgot about one of our many entry points, and forgot to apply a needed fix there. That’s how they initially broke in.”

If using a high number of entry points, it is more likely that one will be mis-configured or forgotten......

......and with some designs, a break-in at the weakest point means that all your resources are now compromised.
Some security designs require platform-specific security code to be distributed & QA’d for each unique combination of OS, OS release, web server, and web server release...........
Do you want Entry-point security only, or End-to-End security?

If using only entry-point security, systems and flows in blue are secured……

…..and systems and flows in red are not secured (not by your web security tool).

End-to-end security means securing not just the “front door”, but also securing……

…..internal flows & data stores under a single framework, avoiding “islands of security”.

Architecture Choice 5:
Websphere Authentication

Authentication Options

Web Server or Web Security Tool

- LDAP
- OS registry
- password file
- database
- PKI
Authentication Options

- Where do you want the authentication to occur:
  - HTTP Server choices
    - IBM HTTP Server
    - Apache
    - Other
  - Websphere Application Server
  - Proxy or other?

HTTP Server Authentication

- IBM HTTP Server powered by Apache
  - None
  - Basic (encoded userid/pw)
    - User defined authentication File(s)
    - Group authentication File(s)
  - LDAP
  - Form based - redirect to a login URL
HTTP Server Administration (apache)

HTTP Server Authentication

- IBM HTTP Server for OS/390 (IHS)
  - None (public access)
  - Basic
    - UNIX password file
    - External Security Manager (RACF, ACF2 etc.)
    - LDAP
  - SSL Client Authentication - digital certificates
Websphere Authentication Options

Authentication Options set here

check to enable Security!
Websphere Authentication Options

**General**
- Application Defaults
- Authentication Mechanisms
- User Registry

**Challenge Type**
- Basic (User ID and Password)
- Certificate
- Custom
  - Login URL
  - Password URL

**Use SSL to connect client and Web server**
* - indicates a required field

**Authentication Mechanism**
- Specify how to authenticate clients when they try to access applications.

**Local Operating System**
- Lightweight Third Party Authentication (LTPA)
  - Time Duration (0-365)
  - Generate.xml
  - Generate from file
  - Generate to file

**Enable Single Sign-On**
- Domain
- Use LTPA connections only
Websphere Authentication Options

Note: the application should run under a privileged identity. In the case of AIX or Solaris, it is typically the "root" user. In the case of Windows NT, the system administrator needs to assign the user ID associated with the WebSphere AdminServer service the "Act as operating system" privilege.

Websphere Single Signon
Multiple Webservers - Authentication

Multiple Webservers - Single Signon
Cookie based Solution
Multiple Webservers - Single Signon
Proxy based solutions

Security Challenge

SecureWay Policy Director: Web Component

- Central Authentication service that maintains state
- Fine-Grained access control to Web resources
- Replicated servers with failover management for fault tolerance and high availability

- Provides Web Single Sign-On
- Offloads SSL & security logic from web servers
- Establishes secure path to browser
- Secures connections to protected web servers
- Caches policy for high performance
Sample Architecture and Request Flow

Tivoli SecureWay Policy Director Scope

Permissions framework for e-business
- Define and enforce permissions (authentication + access control) policy
- Privacy Mgr - Enforce Corporate Privacy Policy
- J2EE - Transparent J2EE Security
- MQSeries - Store-and-forward transactions
- CORBA - Iona ORBIX, Inprise Visibroker
- Custom Apps - Via use of the Open Group aznAPI
- TCP/IP Apps - Telnet, POP3
- Web/URL - HTML, Dynamic HTML, CGI, Servlets, WAP
- New Wireless support via WAP WML/MIME protocol

Coming soon
Websphere Single Signon - LTPA

- Allows delegation - passing of users identity around the distributed network

More Problems? Crossing boundaries!

OS/390 does not understand what a Windows/NT User is??

So how do I securely access my db2 data?

New Kerberos support in WAS 4 and DB2 V7
Websphere Authorizations

Who is authorized to access what page or execute what EJB or JSP etc?
IBM HTTP Server - Protection

- Protect & Protection directives in Websphere (all platforms):

  Protection internal_only   {
    Authtype Basic
    PasswdFile /pw.file
    Mask All@150.2.*.*
  }

  Protect /intonlydata/* internal_only
  Pass /* /html/*

IBM HTTP Server powered by apache

- Directives in HTTPD.CONF or HTAccess file

  AuthUserFile /otherdir/.htpasswd
  AuthGroupFile /dev/null
  AuthName SomeRealm
  AuthType Basic
  <Limit GET>
  require user john
  </Limit>
Websphere Application Server
Who is going to run this bean!

Multiple Webservers - Authorization
Cookie based Solution
Multiple Webservers - Authorization
Proxy based solutions

Websphere Application Security
What about your application - what security is needed within the application?

Is she allowed to buy stocks for this account, at this time of day, from a given network location etc. etc. ????

"Entitlements" Engine

What API can I code to?
"Entitlements" Engine ..... 

Like to use JAVA (JAAS) ? You can with PD ! 

Use pdpermission class for example ! or use opengroup aznAPI !

NY Times Website Hacked on 98/09/13