Presented by IBM developerWorks

`ibm.com/developerworks/`

IBM

Achieving Enterprise Application Security

IBM developerWorks

2007 Jolt Hall of Fame Winner

Live!

Briefings

Presented by IBM developerWorks
ibm.com/developerworks/

Achieving Enterprise Application Security

IBM developerWorks
2007 Jolt Hall of Fame Winner
Live!
Briefings

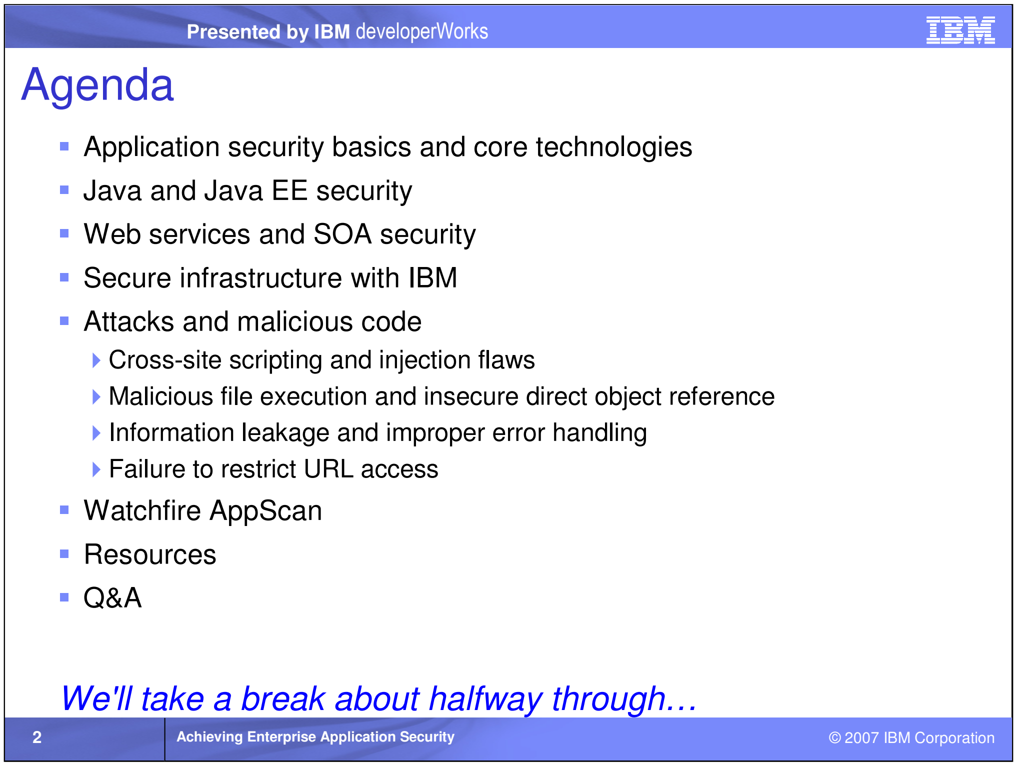
© 2007 IBM Corporation

Hello! And welcome to the IBM briefing on Achieving Enterprise Application Security. We'll be talking today about security technologies and techniques, and about the software products from IBM that can help you ensure that the applications you develop are secure..

You can get a copy of this presentation as a PDF file at the Web site where you registered to attend the briefing.

At the end of the briefing, we'll tell you about some resources that you can use to learn more about the products and technologies covered here today. A lot of those resources are located on the Web, so we'll be giving you the URLs for those resources. Don't worry about writing down those URLs as we show them to you and discuss them. The only URL you need is the address of the briefing page. On that page, you can download the presentation and you will then have all of those URLs. The URL for the briefing page is: http://www.ibm.com/developerworks/offers/techbriefings/details/security.html

That URL is also shown on the agenda sheet given you when you arrived today.



Presented by IBM developerWorks

Agenda

- Application security basics and core technologies
- Java and Java EE security
- Web services and SOA security
- Secure infrastructure with IBM
- Attacks and malicious code
  - Cross-site scripting and injection flaws
  - Malicious file execution and insecure direct object reference
  - Information leakage and improper error handling
  - Failure to restrict URL access
- Watchfire AppScan
- Resources
- Q&A

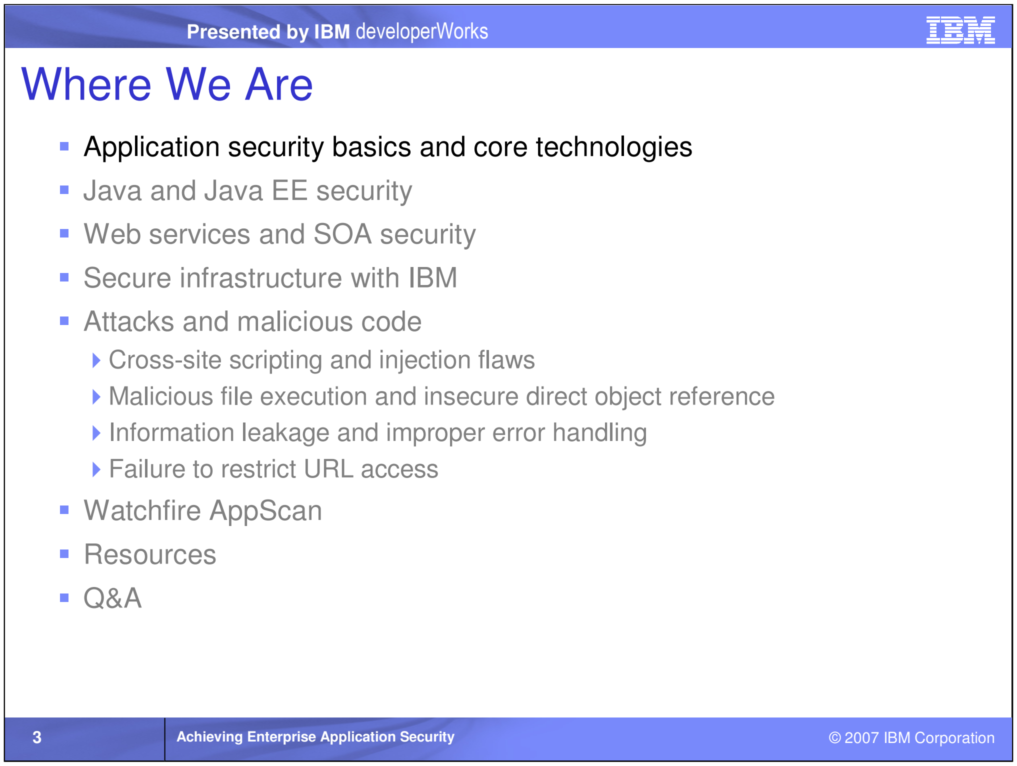
We'll take a break about halfway through…

2 Achieving Enterprise Application Security © 2007 IBM Corporation

We will be covering application security from end-to-end. We’ll start by examining the goals of application security, followed by a review of the basic security concepts. Next we’ll see how those basics are applied as we build our security stack, adding layers of defense. We’ll use Java and Java EE as our programming languages and environment to illustrate certain technologies and techniques.

We’ll proceed through the following topics:
- Application security and core technologies
- Java and Java EE security
- Web services and SOA security
- Secure infrastructure from IBM
- Attacks and malicious code with a close look at common application vulnerabilities
- Watchfire AppScan
- Resources and wrap up

The security tools and product from IBM we’ll discuss include:
- Rational Requisite Pro
- Rational Application Developer/Rational Software Architect
- Tivoli Access Manager
- Tivoli Identity Manager
- Tivoli Federated Identity Manager



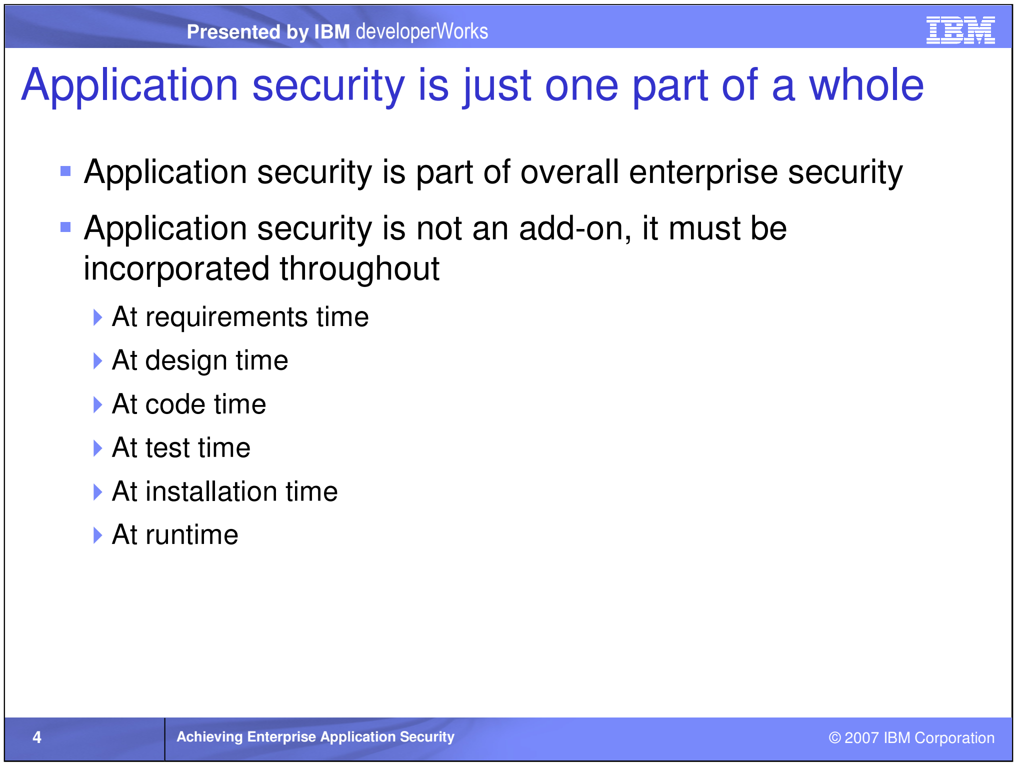
Presented by IBM developerWorks

Where We Are

- Application security basics and core technologies
- Java and Java EE security
- Web services and SOA security
- Secure infrastructure with IBM
- Attacks and malicious code
  - Cross-site scripting and injection flaws
  - Malicious file execution and insecure direct object reference
  - Information leakage and improper error handling
  - Failure to restrict URL access
- Watchfire AppScan
- Resources
- Q&A

3 Achieving Enterprise Application Security © 2007 IBM Corporation

Let’s get started.



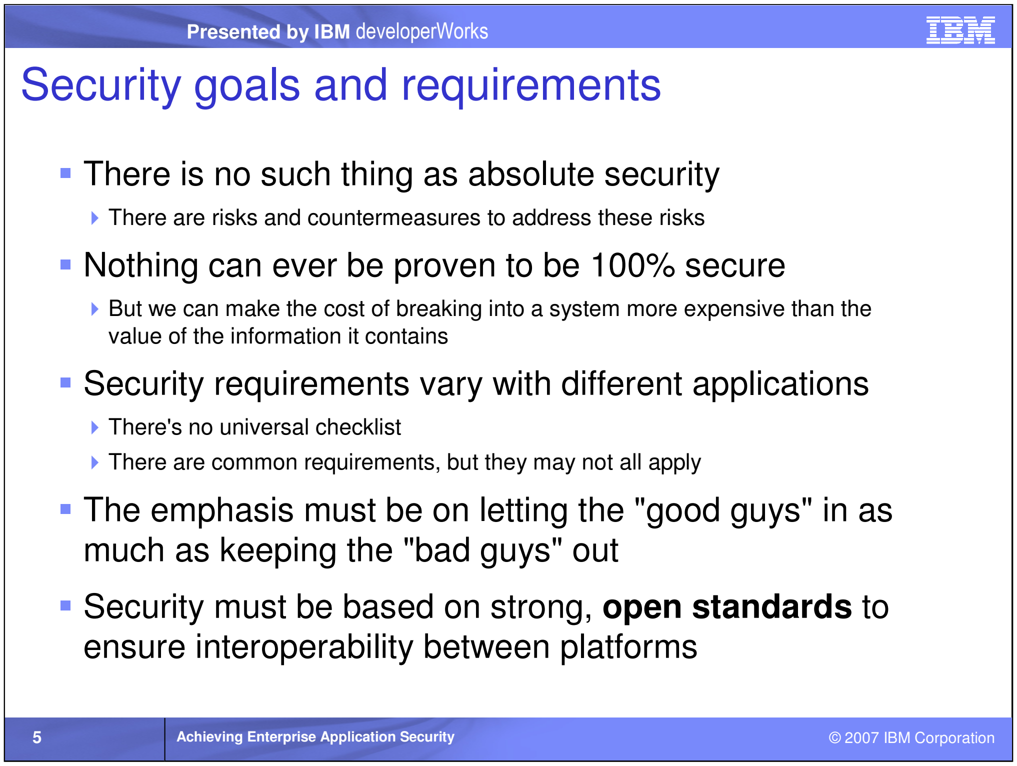
Presented by IBM developerWorks

Application security is just one part of a whole

- Application security is part of overall enterprise security
- Application security is not an add-on, it must be incorporated throughout
  - At requirements time
  - At design time
  - At code time
  - At test time
  - At installation time
  - At runtime

4 Achieving Enterprise Application Security © 2007 IBM Corporation

You can’t think of application security as something you add to software just before you deliver it. The security of the application must be a consideration all through the delivery lifecycle. And it must be integrated with the overall enteprise security strategy and plan.



Presented by IBM developerWorks

Security goals and requirements

- There is no such thing as absolute security
  - There are risks and countermeasures to address these risks
- Nothing can ever be proven to be 100% secure
  - But we can make the cost of breaking into a system more expensive than the value of the information it contains
- Security requirements vary with different applications
  - There's no universal checklist
  - There are common requirements, but they may not all apply
- The emphasis must be on letting the "good guys" in as much as keeping the "bad guys" out
- Security must be based on strong, **open standards** to ensure interoperability between platforms

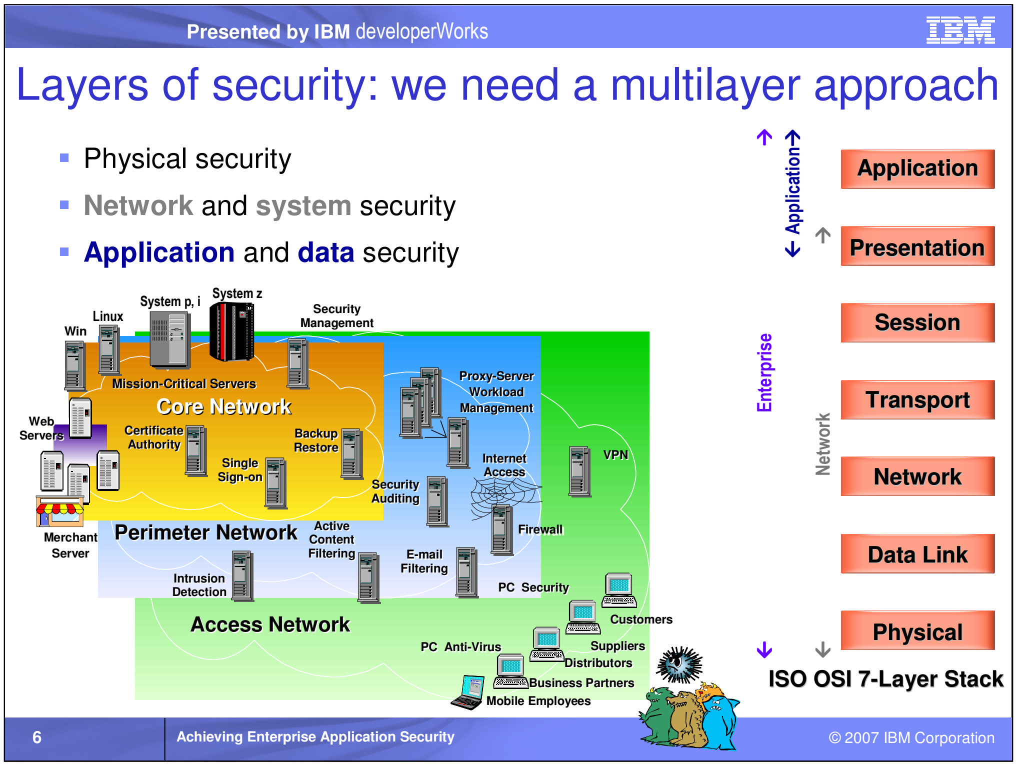
5 Achieving Enterprise Application Security © 2007 IBM Corporation

You have to bear in mind that there is no such thing as absolute security, that nothing can be 100% secure. It’s all a matter of trade-offs – how much the security costs in relation to the value of the information to be secured.

And there is no universal checklist that you can apply to every application. While there may be common requirements across many applications, each will have its own unique requirements.

Security measures cannot put major constraints on the usability of an application. You have to put us much emphasis on letting authorized users into your systems as you do on keeping unauthorized users out.

To ensure interoperability, the use of security standards is imperative.



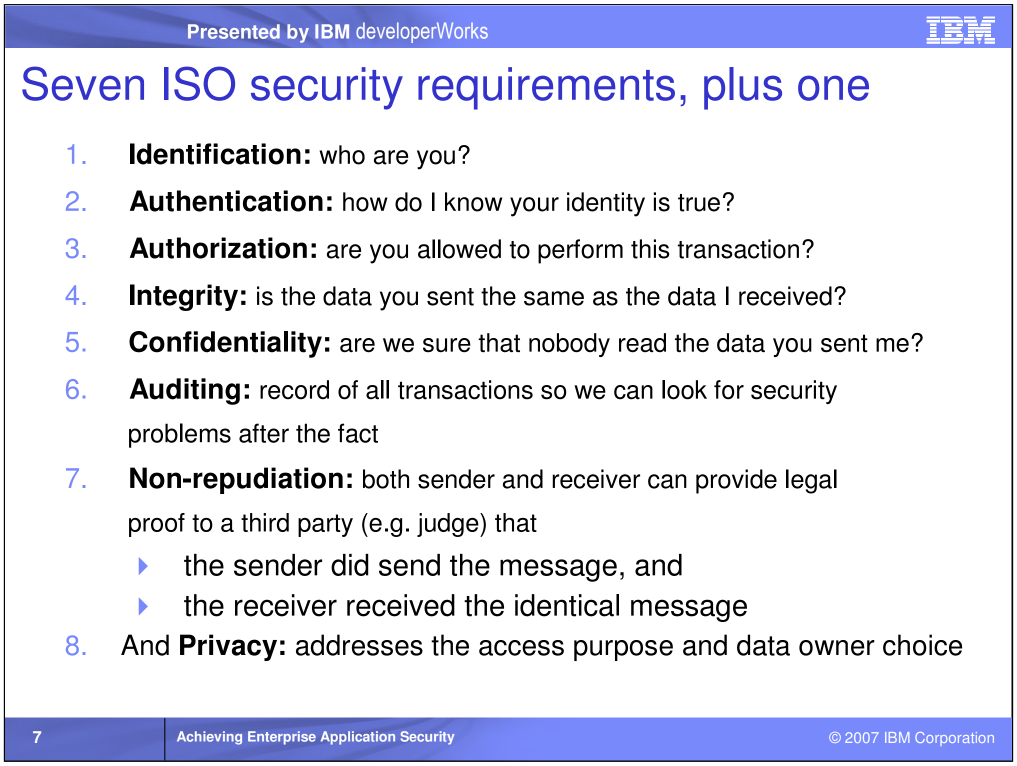
Presented by IBM developerWorks

Layers of security: we need a multilayer approach

- Physical security
- Network and system security
- Application and data security

6 Achieving Enterprise Application Security © 2007 IBM Corporation

In order to let the good guys in while keeping the bad guys out, security is required at many levels. We need to secure hardware, operating systems, application software, peripheral devices, and communications equipment. Successfully subverting any of these can compromise the system and the information stored on the system. Each point requiring security maps to a level in the OSI stack. The ISO OSI model is the International Standard Organization's Open System Interconnect (ISO/OSI) model. It defines seven network layers starting from the hardware and wiring and going all the way up to the applications running on the network. Each layer needs security. Today our focus will be on the application, but none of these other layers can be ignored in an enterprise.



Presented by IBM developerWorks

Seven ISO security requirements, plus one

1. **Identification:** who are you?
2. **Authentication:** how do I know your identity is true?
3. **Authorization:** are you allowed to perform this transaction?
4. **Integrity:** is the data you sent the same as the data I received?
5. **Confidentiality:** are we sure that nobody read the data you sent me?
6. **Auditing:** record of all transactions so we can look for security problems after the fact
7. **Non-repudiation:** both sender and receiver can provide legal proof to a third party (e.g. judge) that
   - the sender did send the message, and
   - the receiver received the identical message
8. And **Privacy:** addresses the access purpose and data owner choice

1. You usually identify yourself with your username.

2. Authentication can be with something you know such as a password, something you have such as a badge or dongle or smartcard, or something you are such as biometry, including fingerprint, retinal scan, etc.

3. Once you are authenticated, the next decision is whether you have permission to do what you are trying to do.

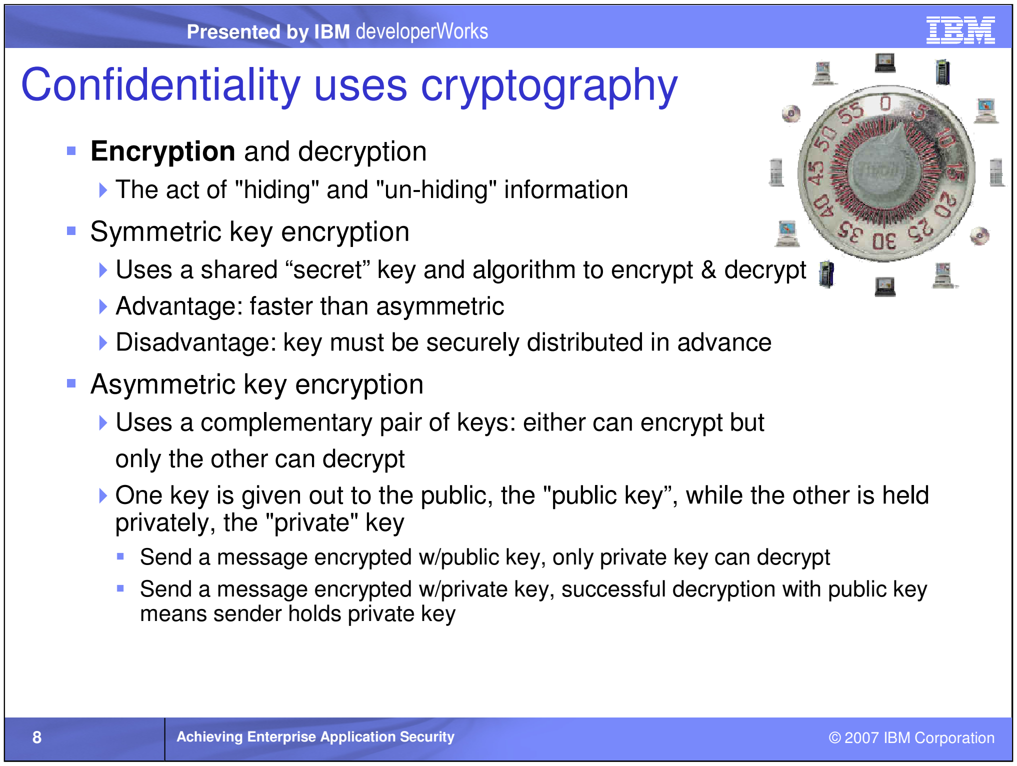
4. Integrity is all about making sure data doesn’t change in transit. We use hashing and digital signatures to help with this.

5. We use encryption to prevent unauthorized access to data.

6. Auditing is important, especially time-stamping of activity and transactions.

7. Auditing and digital signatures are used for non-repudiation,

8. Privacy is a little different. It’s a form of access control, but considers the purpose of access against the choices of the data subject (data owner),



Presented by IBM developerWorks

Confidentiality uses cryptography

- **Encryption** and decryption
  - The act of "hiding" and "un-hiding" information
- Symmetric key encryption
  - Uses a shared “secret” key and algorithm to encrypt & decrypt
  - Advantage: faster than asymmetric
  - Disadvantage: key must be securely distributed in advance
- Asymmetric key encryption
  - Uses a complementary pair of keys: either can encrypt but only the other can decrypt
  - One key is given out to the public, the "public key”, while the other is held privately, the "private" key
    - Send a message encrypted w/public key, only private key can decrypt
    - Send a message encrypted w/private key, successful decryption with public key means sender holds private key

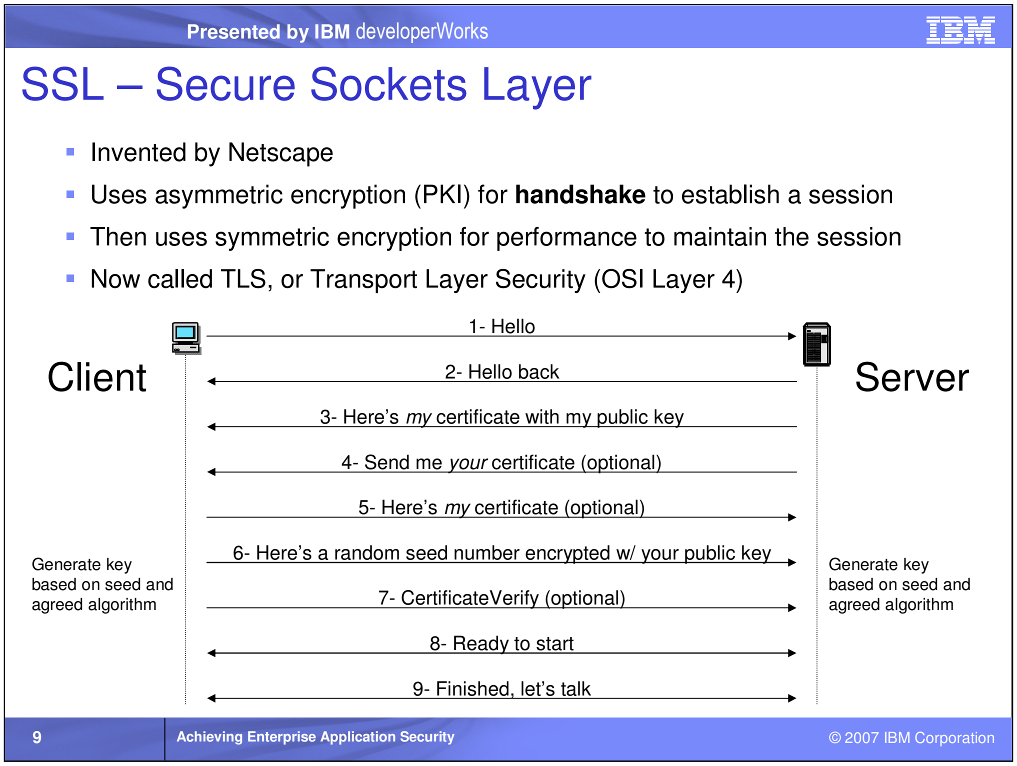
8 Achieving Enterprise Application Security © 2007 IBM Corporation

To ensure confidentiality, we use cryptography.

You can encrypt/decrypt using a "transformation" algorithm, such as reversing each bit in a message, or you can use a key (a number) with the algorithm to encrypt/decrypt, such as adding one to each byte in a message. Usually we use both, and there are several algorithms available. The key needs to be kept secret between the two parties wishing to securely communicate.

Symmetric encryption is also known as Secret Key encryption because a key is shared between two parties and the key must be kept secret. Its advantage is that it is fast. Its drawback is the “key distribution problem”: the key must remain secret, and it must be distributed securely to anyone we want to talk with; and, if we want secure conversations with n partners, we have to manage and distribute n keys, one for each. Offsetting this problem is the fact that symmetric encryption is very fast.

Asymmetric key encryption uses a pair of keys that work together to encrypt/decrpyt. One of these keys is provided publicly, and is thus called the “public key”. The other key is the “private key”, and is held by the owner. The holder of a public key can encrypt a message with that key, and is ensured that the only key that can decrypt it is the holder of the private key of the public/private key pair. Likewise, if a message is received and it can be decrypted by the public key, then you can be assured that the message was encrypted by the holder of the private key.



Presented by IBM developerWorks

SSL – Secure Sockets Layer

- Invented by Netscape
- Uses asymmetric encryption (PKI) for **handshake** to establish a session
- Then uses symmetric encryption for performance to maintain the session
- Now called TLS, or Transport Layer Security (OSI Layer 4)

Client

Server

1- Hello

2- Hello back

3- Here's *my* certificate with my public key

4- Send me *your* certificate (optional)

5- Here's *my* certificate (optional)

6- Here's a random seed number encrypted w/ your public key

7- CertificateVerify (optional)

8- Ready to start

9- Finished, let's talk

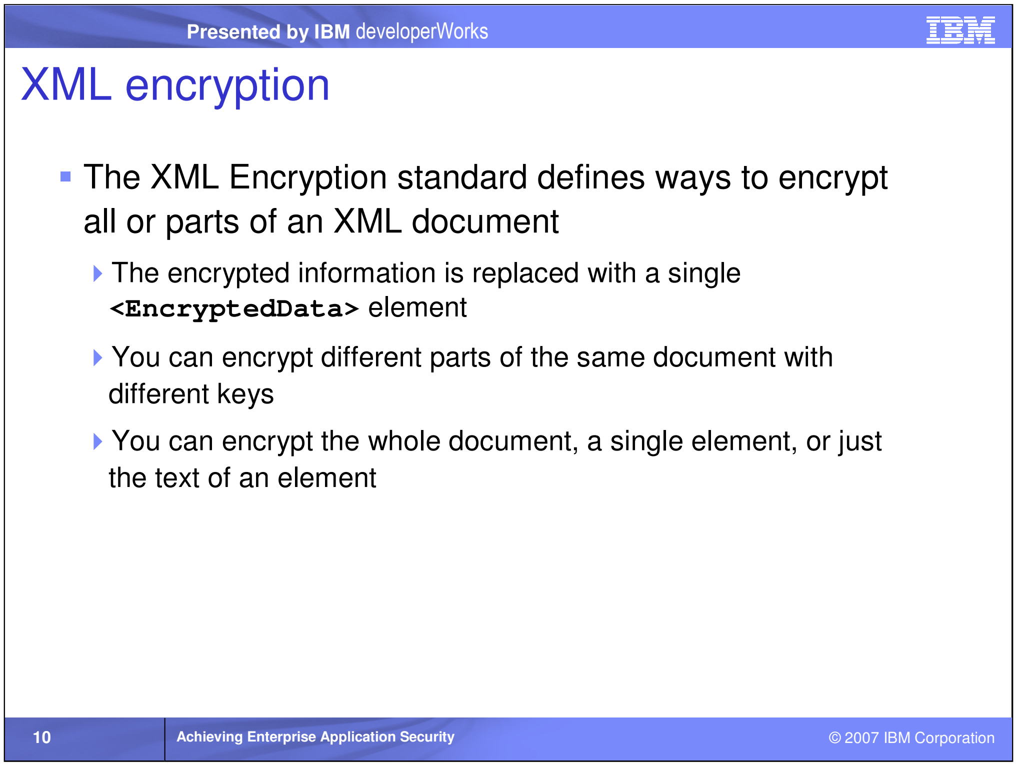
Generate key based on seed and agreed algorithm

Generate key based on seed and agreed algorithm

9 Achieving Enterprise Application Security © 2007 IBM Corporation

Secure Sockets Layer (SSL) allows encrypted messages to be sent over a network. SSL uses both asymmetric and symmetric encryption: public key infrastructure (PKI) is used to establish the secure session. Once established, symmetric encryption is used for the actual message traffic.

SSL V2 requires a server certificate only. Thus the client definitely knows the server. Usually the client user has to log into the server site so that authentication is in both directions. SSL V3 also requires a client certificate so that authentication is mutual, at the Transport layer (OSI Layer 4). The optional messages in the handshake are sent if client authentication is in use. The CertificateVerify message is used so the client can authenticate; without this message – just sending the client certificate earlier doesn't prove client identity.



Presented by **IBM** developerWorks

XML encryption

- The XML Encryption standard defines ways to encrypt all or parts of an XML document
  - The encrypted information is replaced with a single **`<EncryptedData>`** element
  - You can encrypt different parts of the same document with different keys
  - You can encrypt the whole document, a single element, or just the text of an element

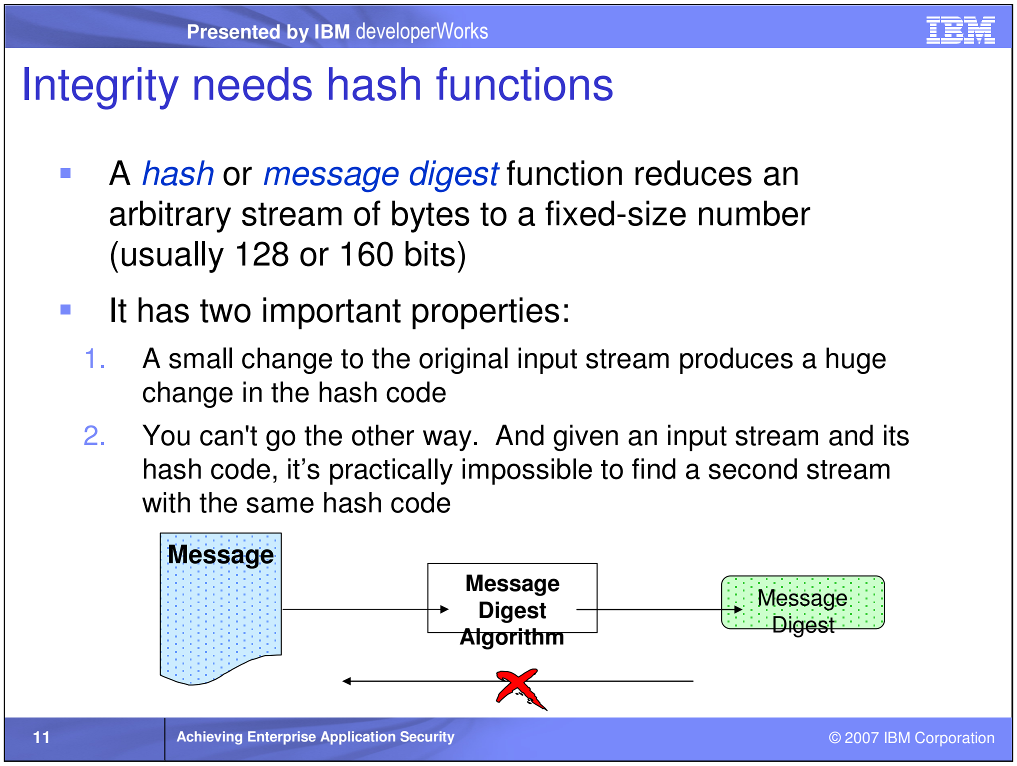
10 **Achieving Enterprise Application Security** © 2007 IBM Corporation

SSL encrypts all of the traffic between two endpoints. It may be that you only wish to encrypt some of the data that is being sent. If you send that data as an XML document, then XML Encryption can be used to encrypt all or part of that document.

The portion of the document that you wish to encrypt is replaced with an <EncryptedData> element, containing the encrypted data. Other XML Encryption elements contain information about how the data was encrypted, the key used, and other information.

Different keys can be used to encrypt different parts of the same document. This lets you send a document to multiple parties, and each party can only decrypt the portion that applies to them.

You can encrypt any portion of an XML document with XML encryption, from the whole document down to the text of a single element.



Presented by IBM developerWorks

Integrity needs hash functions

- A *hash* or *message digest* function reduces an arbitrary stream of bytes to a fixed-size number (usually 128 or 160 bits)
- It has two important properties:

1. A small change to the original input stream produces a huge change in the hash code
2. You can't go the other way. And given an input stream and its hash code, it’s practically impossible to find a second stream with the same hash code

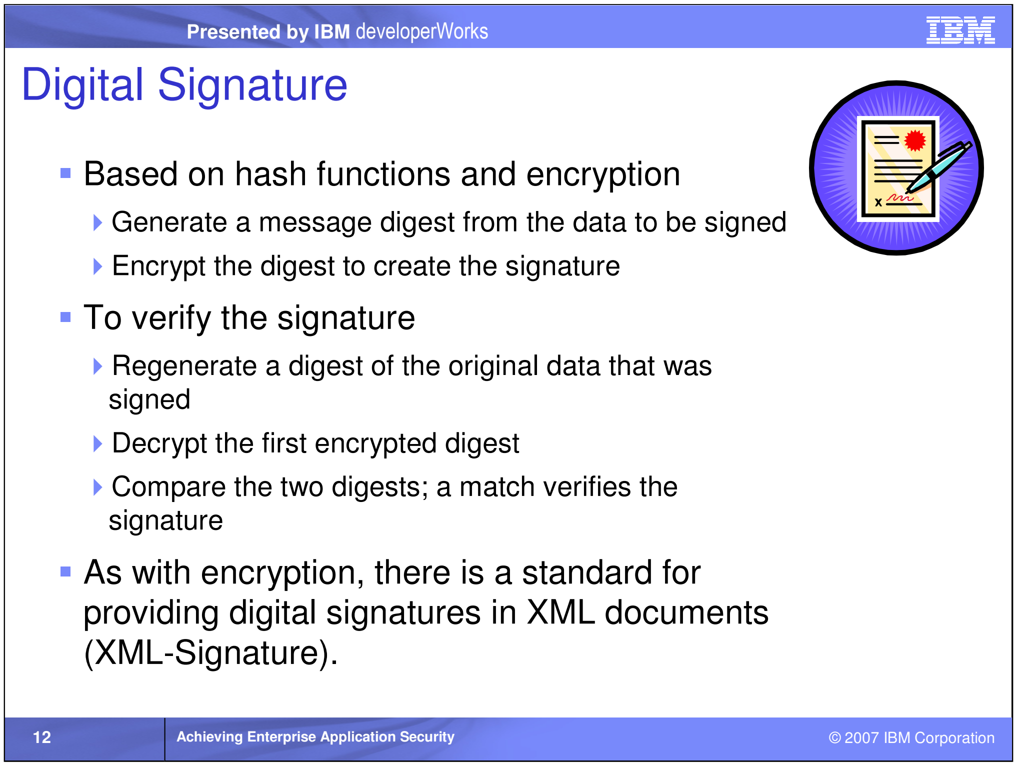
A hash or message digest function calculates a fixed-size number from an arbitrary stream of bytes.

There are two key features of hash algorithms that make them essential:

Any change to the input changes the output, so even a single bit difference to a 1MB document as input, will cause the digest to be different.

You cannot regenerate same input given output. You can't take a digest and figure out what the original input message or document was.

When a message is received with its hash, the receiver calculates the hash of the received message, and if it matches the hash sent by the sender, then the receiver knows that the message was not changed in the course of being sent.



Presented by IBM developerWorks

Digital Signature

- Based on hash functions and encryption
  - Generate a message digest from the data to be signed
  - Encrypt the digest to create the signature
- To verify the signature
  - Regenerate a digest of the original data that was signed
  - Decrypt the first encrypted digest
  - Compare the two digests; a match verifies the signature
- As with encryption, there is a standard for providing digital signatures in XML documents (XML-Signature).

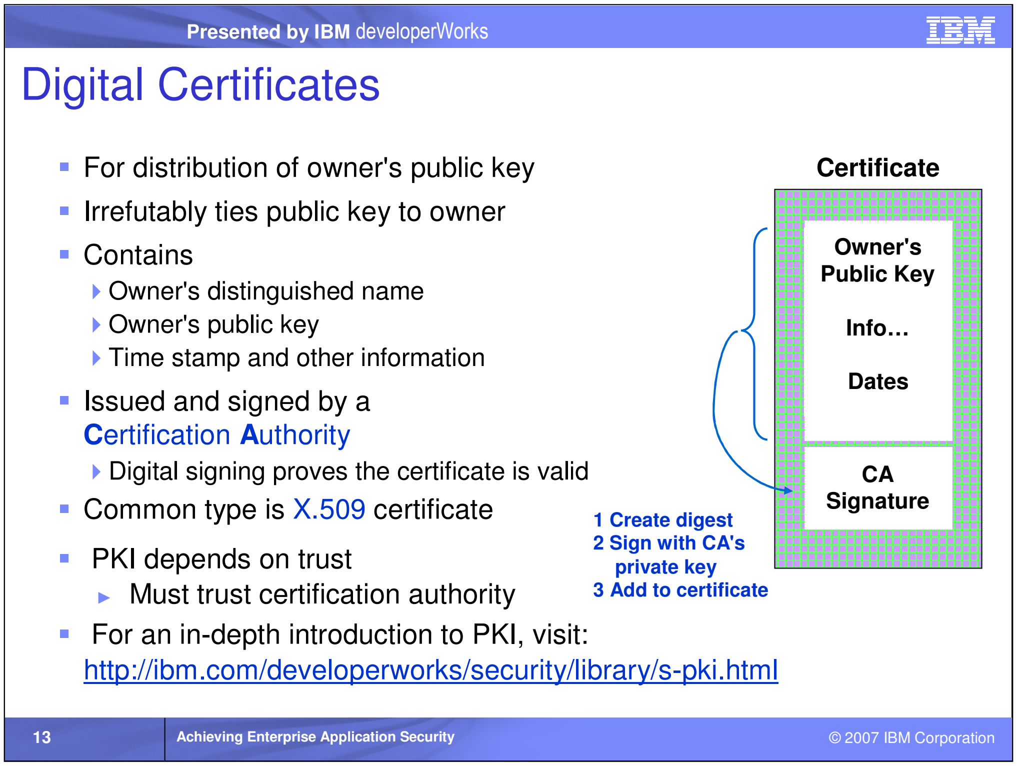
12 Achieving Enterprise Application Security © 2007 IBM Corporation

Digitial signatures combine encryption and hash functions to provide both integrity and a level of non-repudiation.

To create a digital signature, a hash or message digest is generated from the data to be signed, then the digest is encrypted with the sender's private key.

To verify the signature, the receiver regenerates a digest from the data, then decrypts the encrypted digest and compares the two digests. If they match, the signature is verified – the data did not change during transmission and we are ensured that the data came from the holder of the private key.

The XML Digital Signature standard specifies how to provide a digital signature of an XML document.



Presented by IBM developerWorks

Digital Certificates

- For distribution of owner's public key
- Irrefutably ties public key to owner
- Contains
  - Owner's distinguished name
  - Owner's public key
  - Time stamp and other information
- Issued and signed by a Certification Authority
  - Digital signing proves the certificate is valid
- Common type is X.509 certificate
- PKI depends on trust
  - Must trust certification authority
- For an in-depth introduction to PKI, visit: http://ibm.com/developerworks/security/library/s-pki.html

Certificate

Owner's Public Key

Info…

Dates

CA Signature

1 Create digest
2 Sign with CA's private key
3 Add to certificate

13 Achieving Enterprise Application Security © 2007 IBM Corporation

We distribute a public key using a digital certificate, which irrefutably ties a public key to its owner. Certificates are created as follows:

1. Owner generates a public/private pair of keys

2. Owner submits his distinguished name and the public key to a CA in a Certificate Request, while locking the private key up in a keyfile

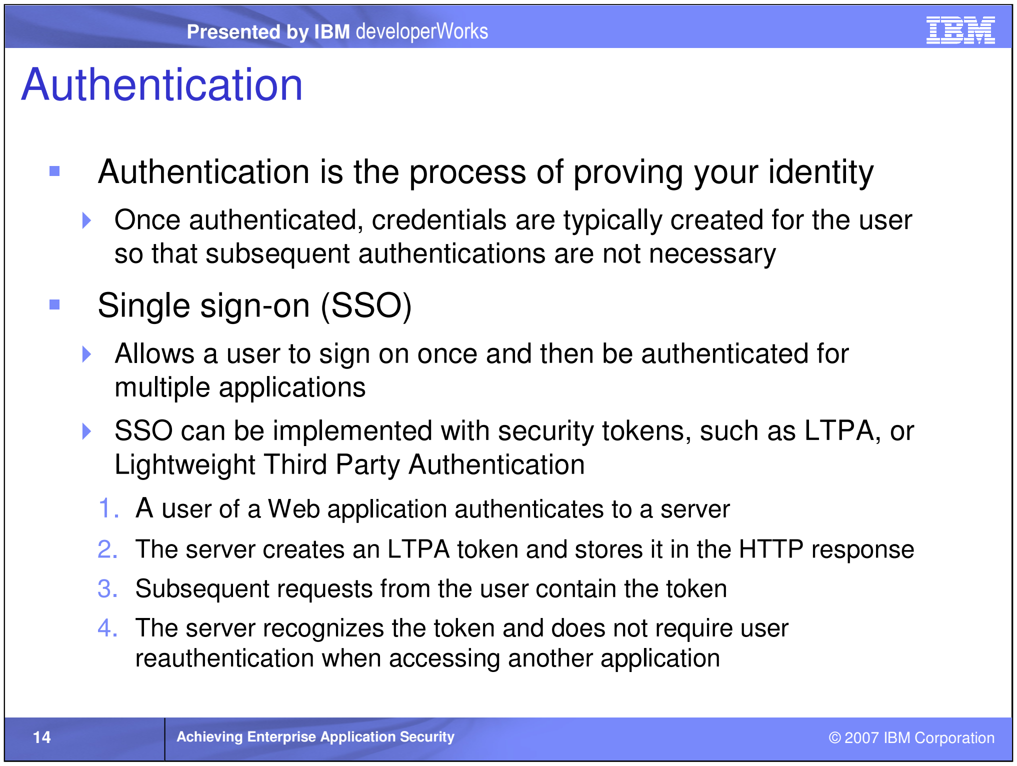
3. The CA verifies the owner and signs the certificate with the CA's private key (standard signature procedure)

4. Owner receives the signed certificate containing his public key and DN back from the CA.

The certificate can now be distributed to everyone -- this is how the public key inside is tied to the owner's identity and is made available to the public.

X.509 is a standard for public key infrastructure (PKI).

PKI depends on trusting the certificate issuers authority.



Presented by IBM developerWorks

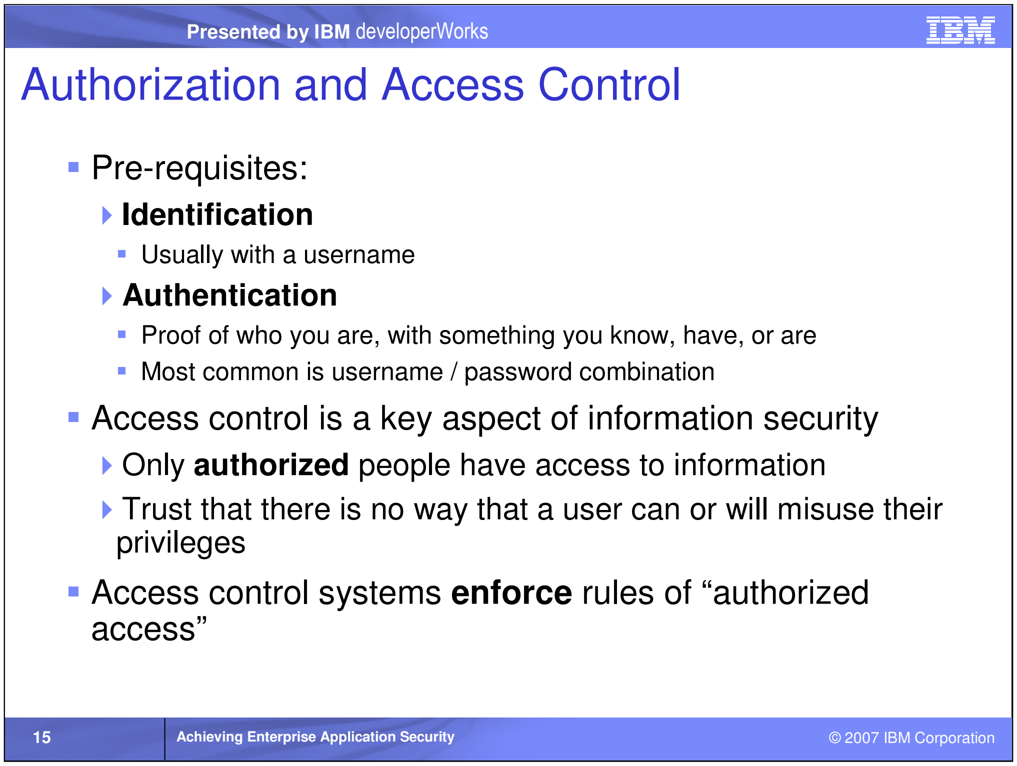
Authentication

- Authentication is the process of proving your identity
  - Once authenticated, credentials are typically created for the user so that subsequent authentications are not necessary
- Single sign-on (SSO)
  - Allows a user to sign on once and then be authenticated for multiple applications
  - SSO can be implemented with security tokens, such as LTPA, or Lightweight Third Party Authentication
    1. A user of a Web application authenticates to a server
    2. The server creates an LTPA token and stores it in the HTTP response
    3. Subsequent requests from the user contain the token
    4. The server recognizes the token and does not require user reauthentication when accessing another application

14 Achieving Enterprise Application Security © 2007 IBM Corporation

Authentication is the process of proving your identity, whether with a username/password, a certificate, or some other method. Once authenticated, some type of credentials are typically created for subsequent access to the same application.

Single sign-on (SSO) allows a user to sign on once and then be authenticated for multiple applications. The user authenticates to the server, and then a token is issued that can authenticate users to multiple applications.



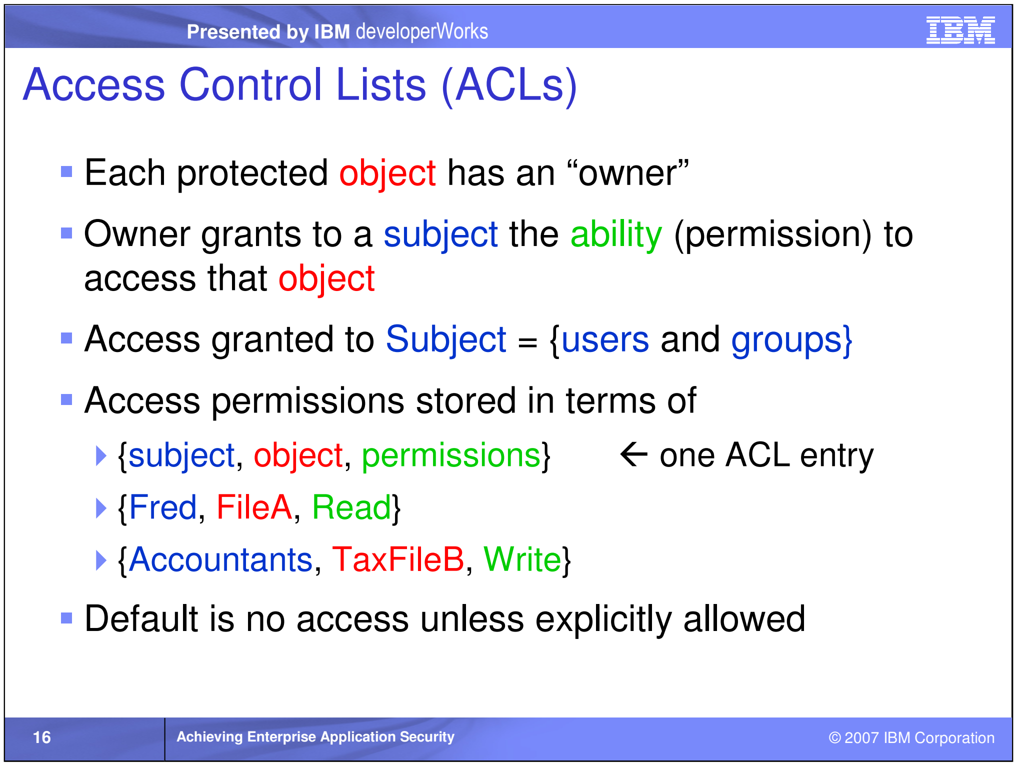
Presented by IBM developerWorks

Authorization and Access Control

- Pre-requisites:
  - **Identification**
    - Usually with a username
  - **Authentication**
    - Proof of who you are, with something you know, have, or are
    - Most common is username / password combination
- Access control is a key aspect of information security
  - Only **authorized** people have access to information
  - Trust that there is no way that a user can or will misuse their privileges
- Access control systems **enforce** rules of “authorized access”

15 Achieving Enterprise Application Security © 2007 IBM Corporation

Once a user has been identified and authenticated, we can begin to consider what that user is authorized to do and/or access in an application. Authorization rules and policies delineate which users are authorized to access certain functions or information. Access control systems enforce these rules.



Presented by IBM developerWorks

Access Control Lists (ACLs)

- Each protected object has an "owner"
- Owner grants to a subject the ability (permission) to access that object
- Access granted to Subject = {users and groups}
- Access permissions stored in terms of
  - {subject, object, permissions} ← one ACL entry
  - {Fred, FileA, Read}
  - {Accountants, TaxFileB, Write}
- Default is no access unless explicitly allowed

16 Achieving Enterprise Application Security © 2007 IBM Corporation

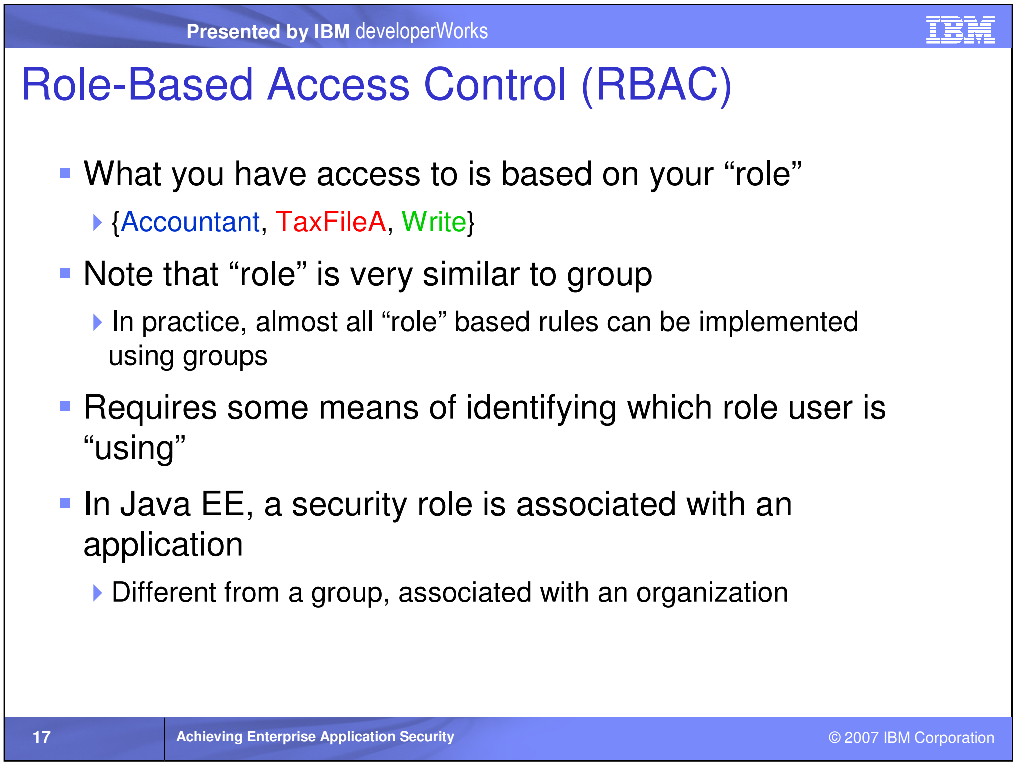
Access control lists are one way to enforce authorization rules.

Each object (file or other resource) that requires only authorized access has an owner. The owner grants permission to access an object. Permission also indicates the type of access that can occur.

Permission is granted to subjects, which can be individual users or user groups.

An entry in an ACL lists the subject, the object, and the permission, as shown in these examples.

The default is to allow no access unless explicitly granted.



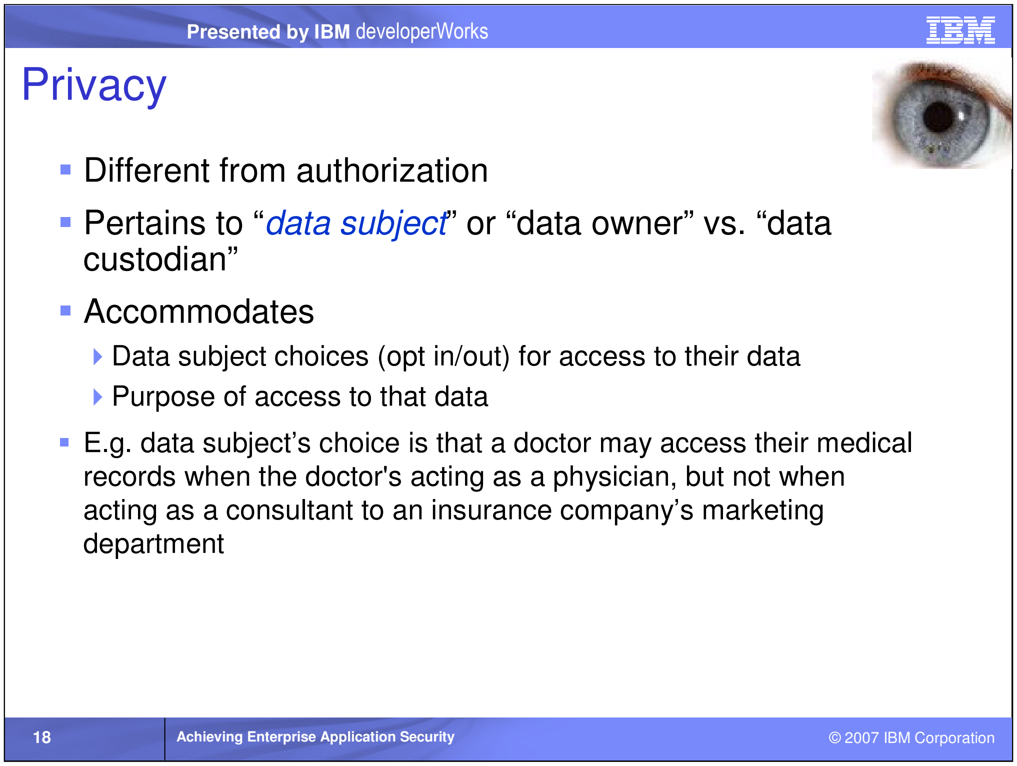
Presented by IBM developerWorks

Role-Based Access Control (RBAC)

- What you have access to is based on your "role"
  - {Accountant, TaxFileA, Write}
- Note that "role" is very similar to group
  - In practice, almost all "role" based rules can be implemented using groups
- Requires some means of identifying which role user is "using"
- In Java EE, a security role is associated with an application
  - Different from a group, associated with an organization

17 Achieving Enterprise Application Security © 2007 IBM Corporation

Role-based access control, such as that used by Java EE, provides a level of indirection that allows access control specifications to be independent of the location where the application is installed. The role, instead of a user or group, is specified in the ACL. The independence is due to the further mapping of users and groups to roles.



Presented by IBM developerWorks

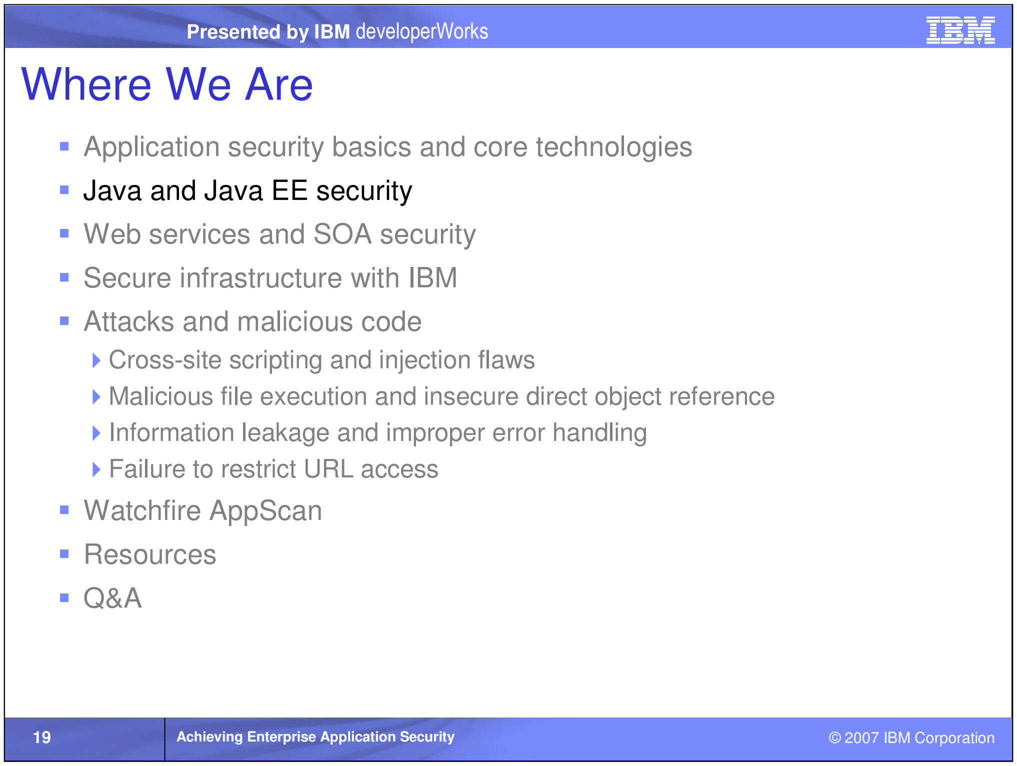
Privacy

- Different from authorization
- Pertains to “*data subject*” or “data owner” vs. “data custodian”
- Accommodates
  - Data subject choices (opt in/out) for access to their data
  - Purpose of access to that data
- E.g. data subject’s choice is that a doctor may access their medical records when the doctor's acting as a physician, but not when acting as a consultant to an insurance company’s marketing department

18 Achieving Enterprise Application Security © 2007 IBM Corporation

Privacy considerations are different from authorization. Privacy pertains to the data subject or data owner, i.e. who the information is about, as opposed to the data custodian who has physical possession of the data.

Privacy regulations often provide that data subjects be given choices about when, by whom, and for what purpose their data can be used. It is the data custodian’s job to ensure that the data subjects choices are enforced.



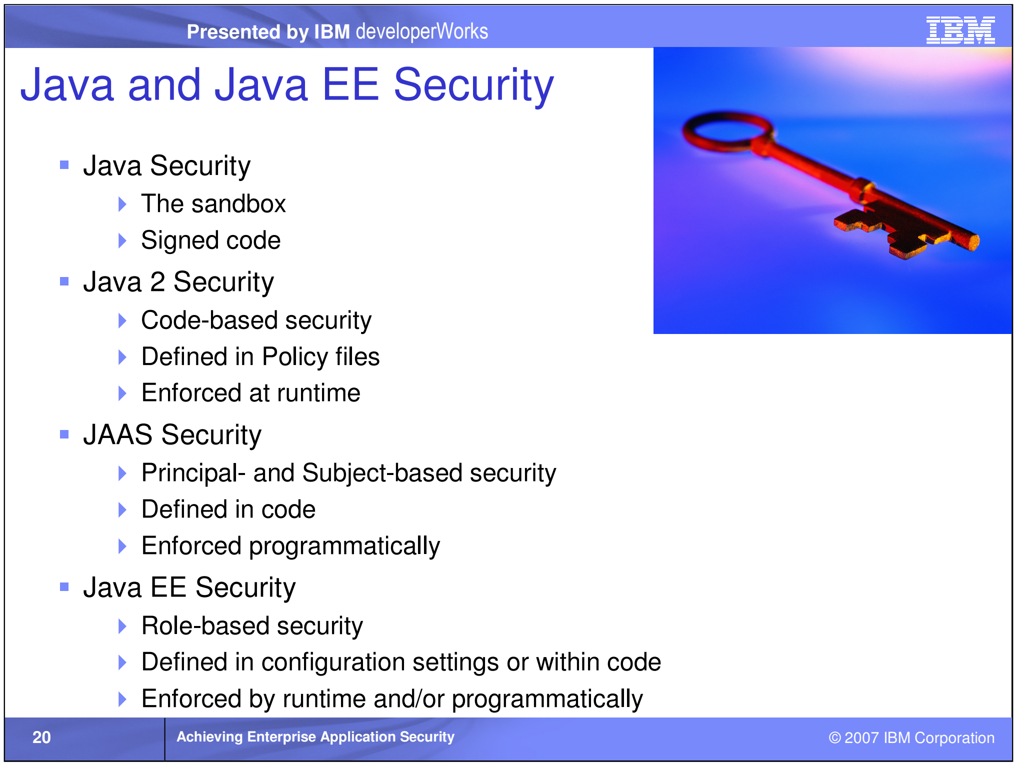
Presented by IBM developerWorks

Where We Are

- Application security basics and core technologies
- Java and Java EE security
- Web services and SOA security
- Secure infrastructure with IBM
- Attacks and malicious code
  - Cross-site scripting and injection flaws
  - Malicious file execution and insecure direct object reference
  - Information leakage and improper error handling
  - Failure to restrict URL access
- Watchfire AppScan
- Resources
- Q&A

19 Achieving Enterprise Application Security © 2007 IBM Corporation

Now we’ll look at Java and Java EE security.



Presented by IBM developerWorks

Java and Java EE Security

- Java Security
  - The sandbox
  - Signed code
- Java 2 Security
  - Code-based security
  - Defined in Policy files
  - Enforced at runtime
- JAAS Security
  - Principal- and Subject-based security
  - Defined in code
  - Enforced programmatically
- Java EE Security
  - Role-based security
  - Defined in configuration settings or within code
  - Enforced by runtime and/or programmatically

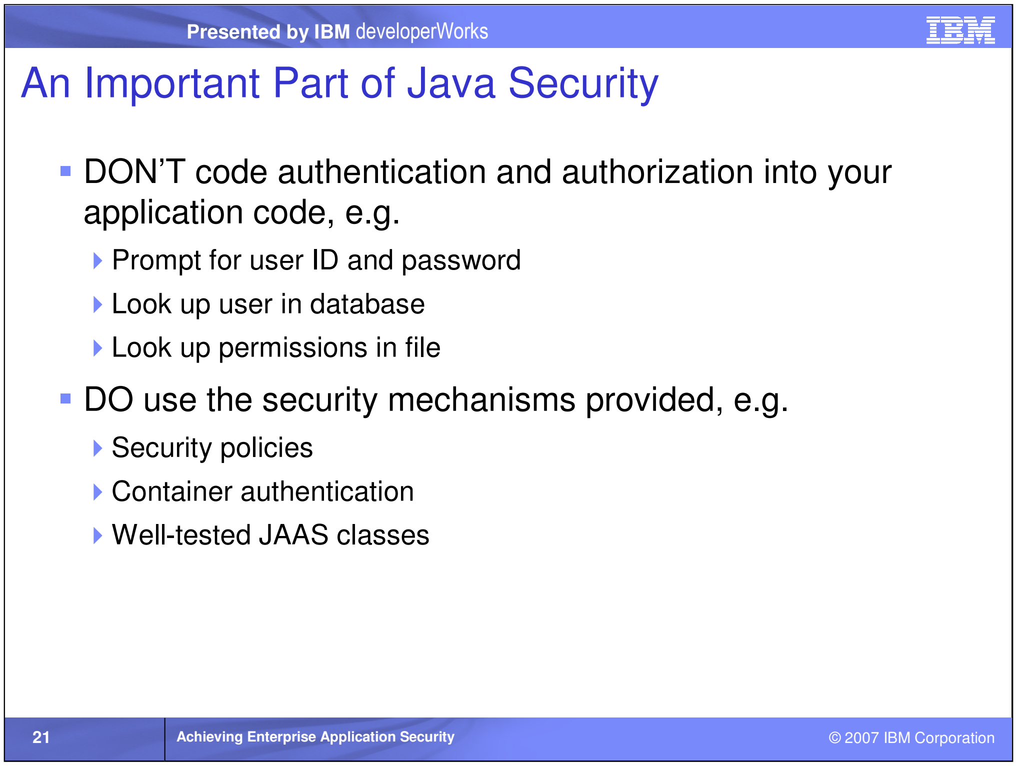
20 Achieving Enterprise Application Security © 2007 IBM Corporation

The original Java sandbox model prevented any code not on the CLASSPATH from accessing resources outside of the sandbox. This code, loaded by the ClassLoader, was untrusted. JDK 1.1 changed the sandbox model to allow signed code to access resources outside of the sandbox. This allowed signed code downloaded from Web sites to execute with trust as long as the signature could be validated.

With Java 2 security access control can be specified at the class level for particular resources and for particular types of access rather than all or nothing. Standalone applications can now be subject to security checking. The security policy is easy to configure and is stored external to the code, usually indicated by a URL. Thus the policy file can be local or remote.

JAAS is the Java Authentication and Authorization Service, and allows applications to authenticate and authorize independent of the underlying technology, e.g. user id/password, smartcard, biometrics, etc. JAAS allows access to resources (Subjects) to be controlled depending on who (Principals) is trying to access. JAAS is defined in application code and is enforced programmatically.

Jave EE security builds on Java 2 security and JAAS to provide role-based security for enterprise applications. Security “roles” are defined for an application, and users and groups are assigned to these roles at deployment time. Access to resources is assigned by role, and can be defined in deployment descriptors or can be coded using the JAAS APIs. Authentication is typically handled by the Java EE container.



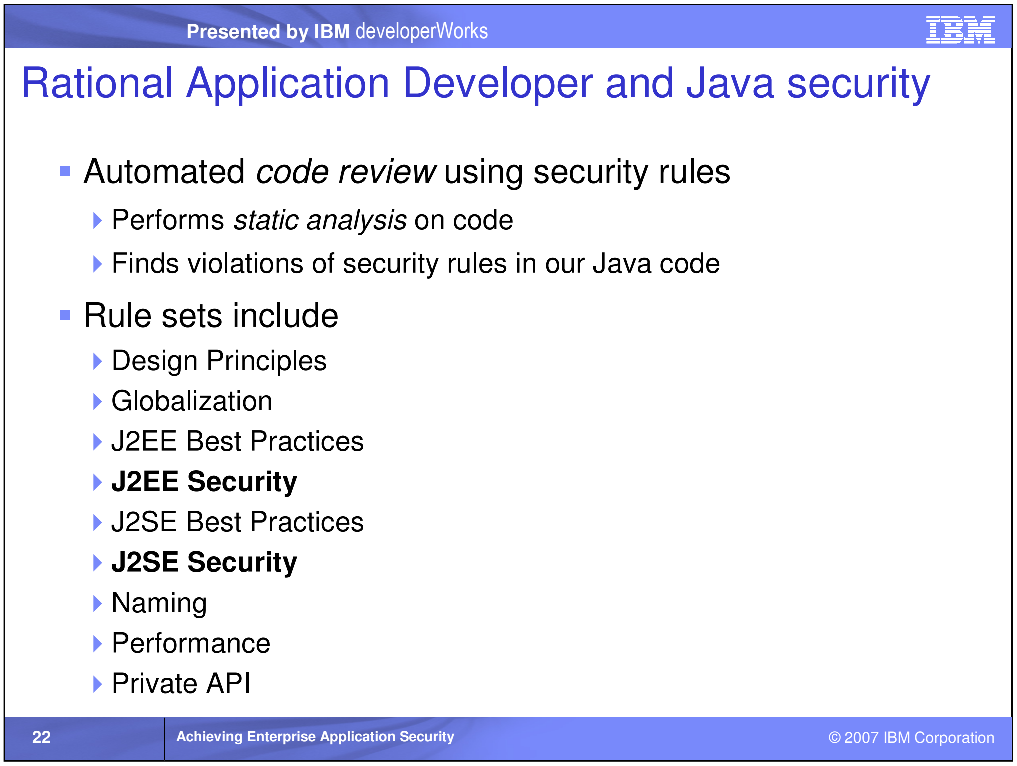
Presented by IBM developerWorks

An Important Part of Java Security

- DON'T code authentication and authorization into your application code, e.g.
  - Prompt for user ID and password
  - Look up user in database
  - Look up permissions in file
- DO use the security mechanisms provided, e.g.
  - Security policies
  - Container authentication
  - Well-tested JAAS classes

21 Achieving Enterprise Application Security © 2007 IBM Corporation

Don't put authentication and authorization code directly into your application code, as the example outlines. Use the Java Security mechanisms provided – they are much less likely to contain holes or vulnerabilities.



Presented by **IBM** developerWorks

Rational Application Developer and Java security

- Automated *code review* using security rules
  - Performs *static analysis* on code
  - Finds violations of security rules in our Java code
- Rule sets include
  - Design Principles
  - Globalization
  - J2EE Best Practices
  - **J2EE Security**
  - J2SE Best Practices
  - **J2SE Security**
  - Naming
  - Performance
  - Private API

22 Achieving Enterprise Application Security © 2007 IBM Corporation

Rational Application Developer/Software Architect provides a code review tool, which is a rule-based static analysis tool for automatic validation of Java code for correctness and compliance with coding standards and best practices.

Code review covers all of the types of potential problems shown here.

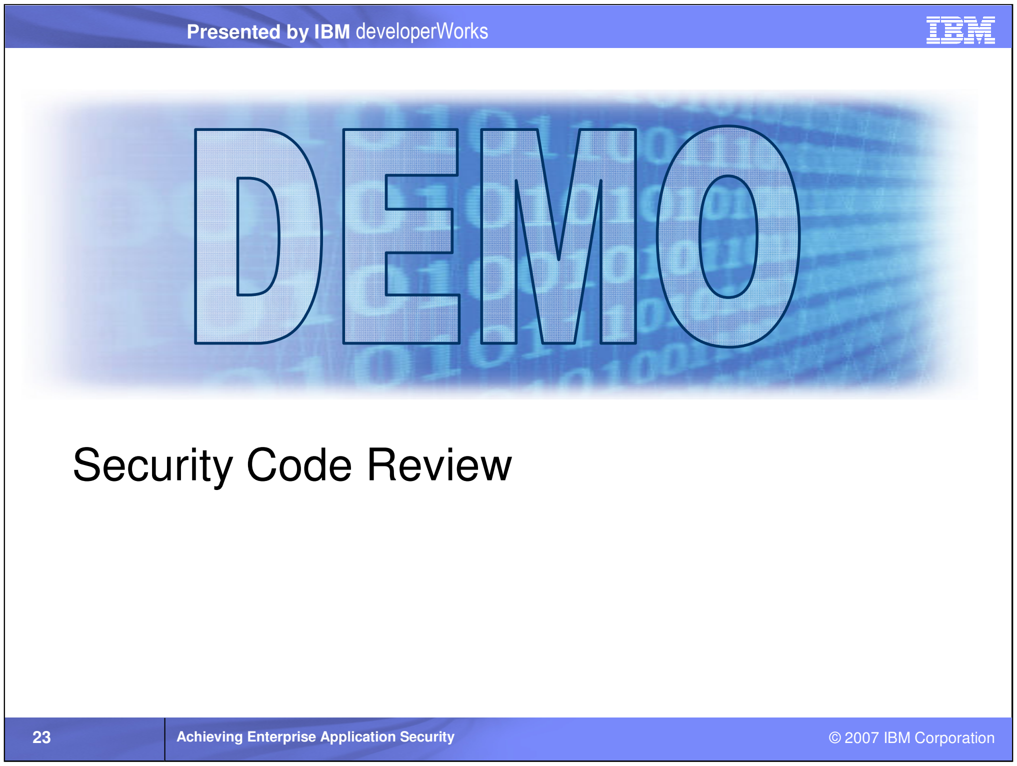
Each rule in the code review provides an explanation of the rule, examples of violations of the rule along with solutions to correct the example violation, and, possibly, a quick fix that can be applied automatically by Application Developer.

Each rule can be enabled or disabled individually or by category.

Users can also create their own rules from templates that are provided.

A Complete Code Review has over 200 rules, and a Quick Code Review has 34 of the most commonly breached rules.

The J2EE Security and J2SE Security rule categories cover potential problems for security code.



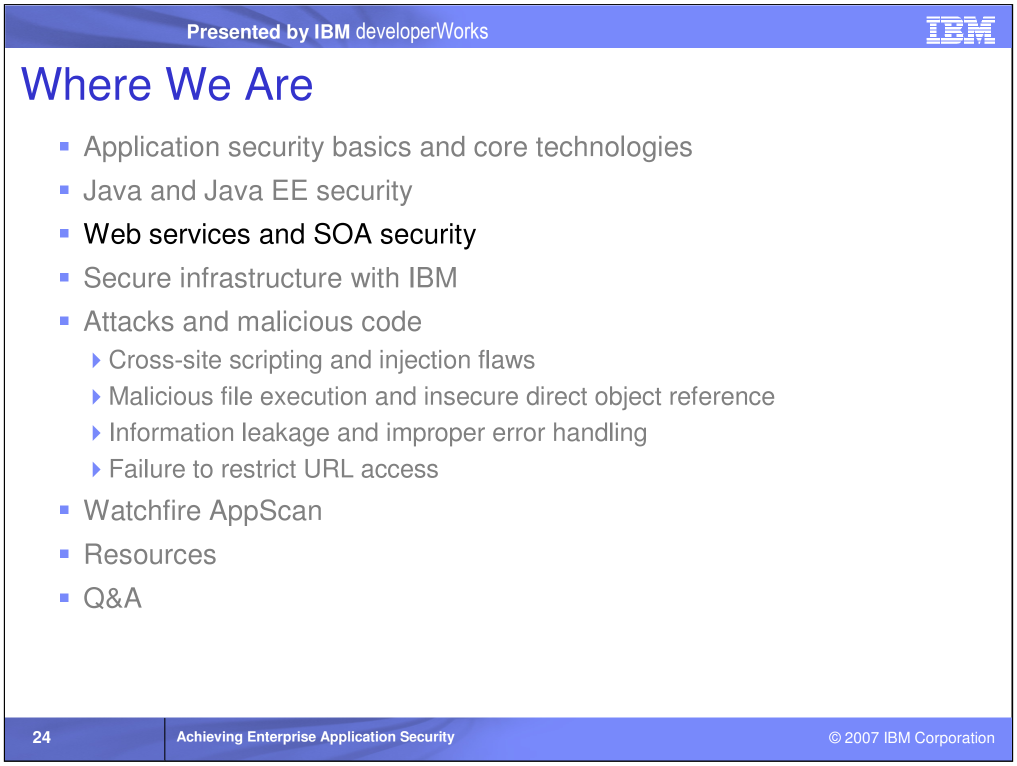
Presented by IBM developerWorks

DEMO

Security Code Review

23 Achieving Enterprise Application Security © 2007 IBM Corporation

Let’s take a look at a short demo of the code review capabilites of Rational Application Developer/Software Architect, particularly focusing on security code.



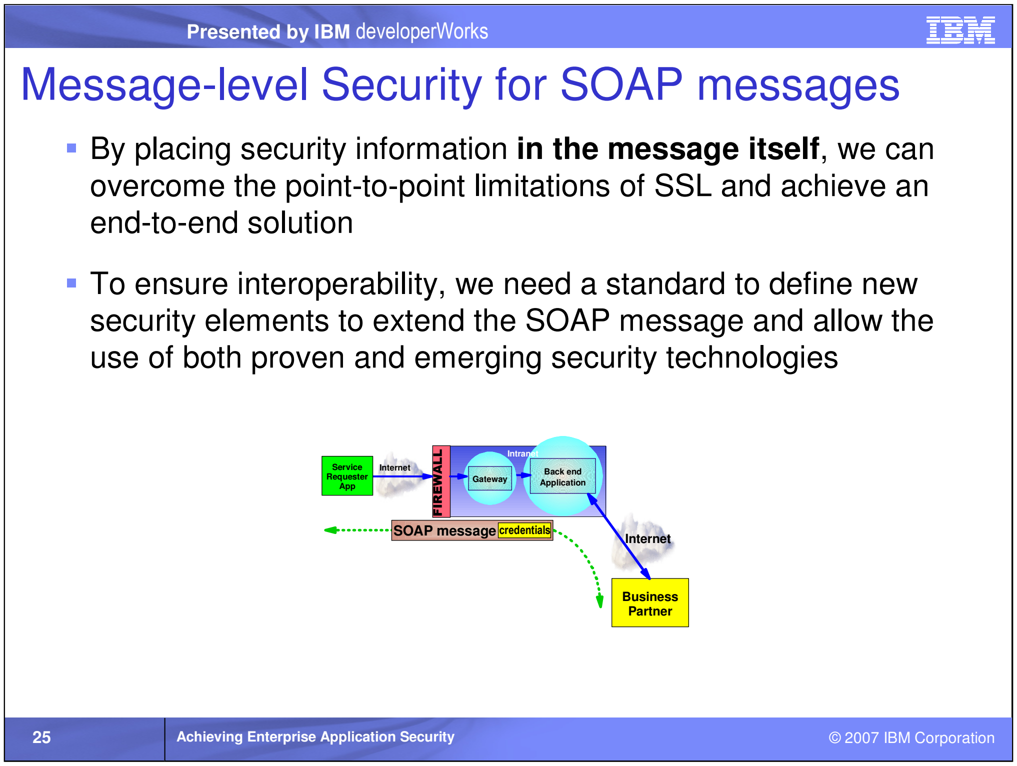
Presented by IBM developerWorks

Where We Are

- Application security basics and core technologies
- Java and Java EE security
- Web services and SOA security
- Secure infrastructure with IBM
- Attacks and malicious code
  - Cross-site scripting and injection flaws
  - Malicious file execution and insecure direct object reference
  - Information leakage and improper error handling
  - Failure to restrict URL access
- Watchfire AppScan
- Resources
- Q&A

24 Achieving Enterprise Application Security © 2007 IBM Corporation

Web services and SOA security is next.



Presented by IBM developerWorks

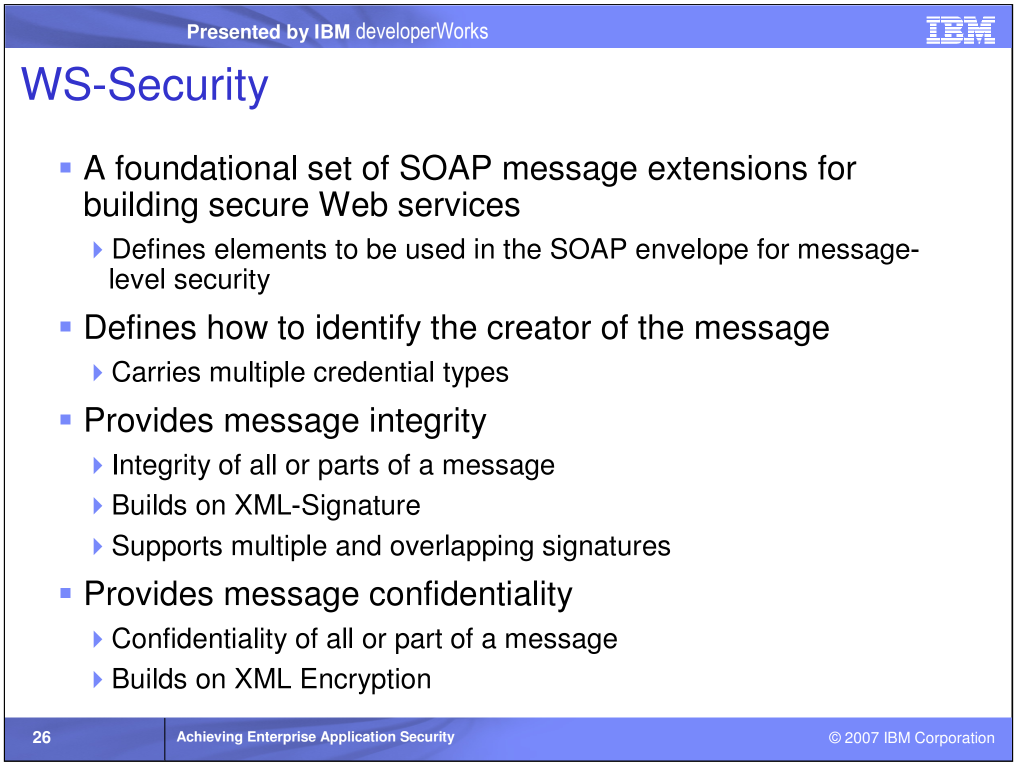
Message-level Security for SOAP messages

- By placing security information **in the message itself**, we can overcome the point-to-point limitations of SSL and achieve an end-to-end solution
- To ensure interoperability, we need a standard to define new security elements to extend the SOAP message and allow the use of both proven and emerging security technologies

25 Achieving Enterprise Application Security © 2007 IBM Corporation

We can use SSL to provide confidentiality and some integrity to messages we send over the Internet. The problem with SSL, though, is that it is point-to-point. If we want to send a message that may take several hops to reach its destination, each pair of hops will need to establish their own SSL session. Thus any security information about the original sender will be lost before reaching that destination using SSL.

The best solution is to put the security information in the message itself. For that to work, we need standards to ensure interoperability.



Presented by IBM developerWorks

WS-Security

- A foundational set of SOAP message extensions for building secure Web services
  - Defines elements to be used in the SOAP envelope for message-level security
- Defines how to identify the creator of the message
  - Carries multiple credential types
- Provides message integrity
  - Integrity of all or parts of a message
  - Builds on XML-Signature
  - Supports multiple and overlapping signatures
- Provides message confidentiality
  - Confidentiality of all or part of a message
  - Builds on XML Encryption

26 Achieving Enterprise Application Security © 2007 IBM Corporation

WS-Security defines a set of enhancements to the SOAP specification of messaging to enable protection of the message through authentication, confidentiality, and assurance of integrity. It builds on XML-Signature and XML Encryption, incorporating use of those standards to ensure message integrity and message confidentiality.

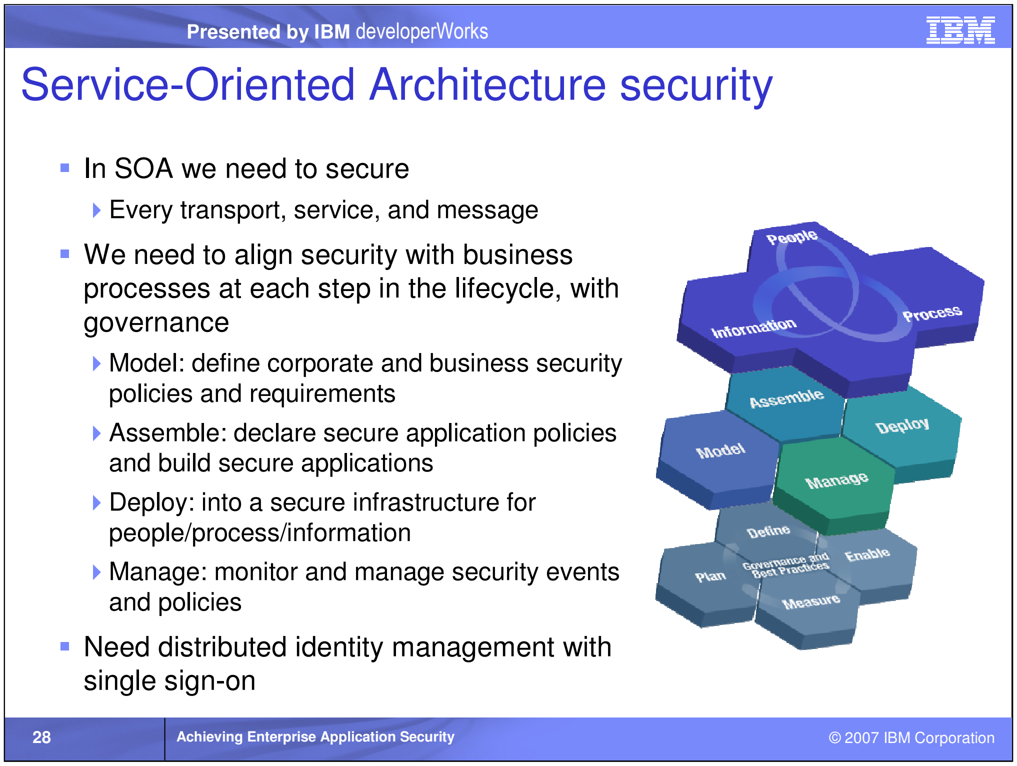
Presented by IBM developerWorks

DEMO

Add a Digital Signature to a Web Service

27 Achieving Enterprise Application Security © 2007 IBM Corporation

Developers depend on tools to help them incorporate security into the Web services they consume and produce. This demo shows how Rational Application Developer/Software Architect assists in the development of Web services, focusing on the facility with which a digital signature can be added to a service.



Presented by IBM developerWorks

IBM

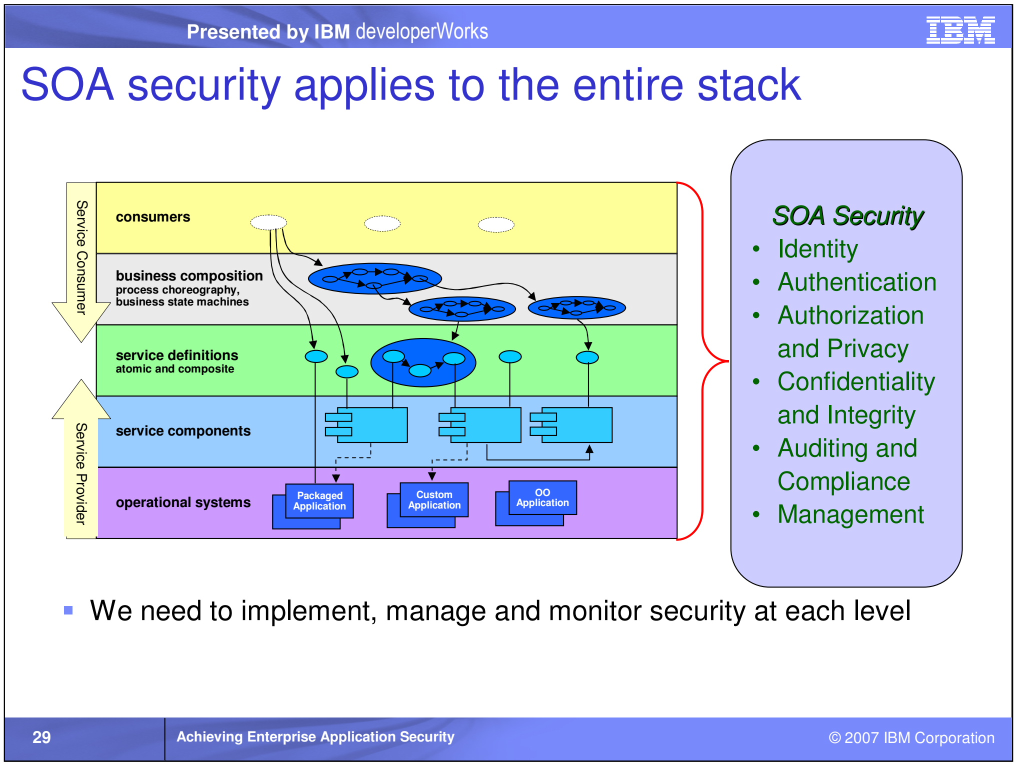
Service-Oriented Architecture security

- In SOA we need to secure
  - Every transport, service, and message
- We need to align security with business processes at each step in the lifecycle, with governance
  - Model: define corporate and business security policies and requirements
  - Assemble: declare secure application policies and build secure applications
  - Deploy: into a secure infrastructure for people/process/information
  - Manage: monitor and manage security events and policies
- Need distributed identity management with single sign-on

28 Achieving Enterprise Application Security © 2007 IBM Corporation

In a service-oriented architecture, every transport, service, and message must be secure. The business process must incorporate security at all phases of the lifecycle, following an appropriate governance model.

It is also essential to have distributed identity management with single sign-on capabilities.



Presented by IBM developerWorks

SOA security applies to the entire stack

Service Consumer

Service Provider

consumers

business composition
process choreography,
business state machines

service definitions
atomic and composite

service components

operational systems

Packaged Application

Custom Application

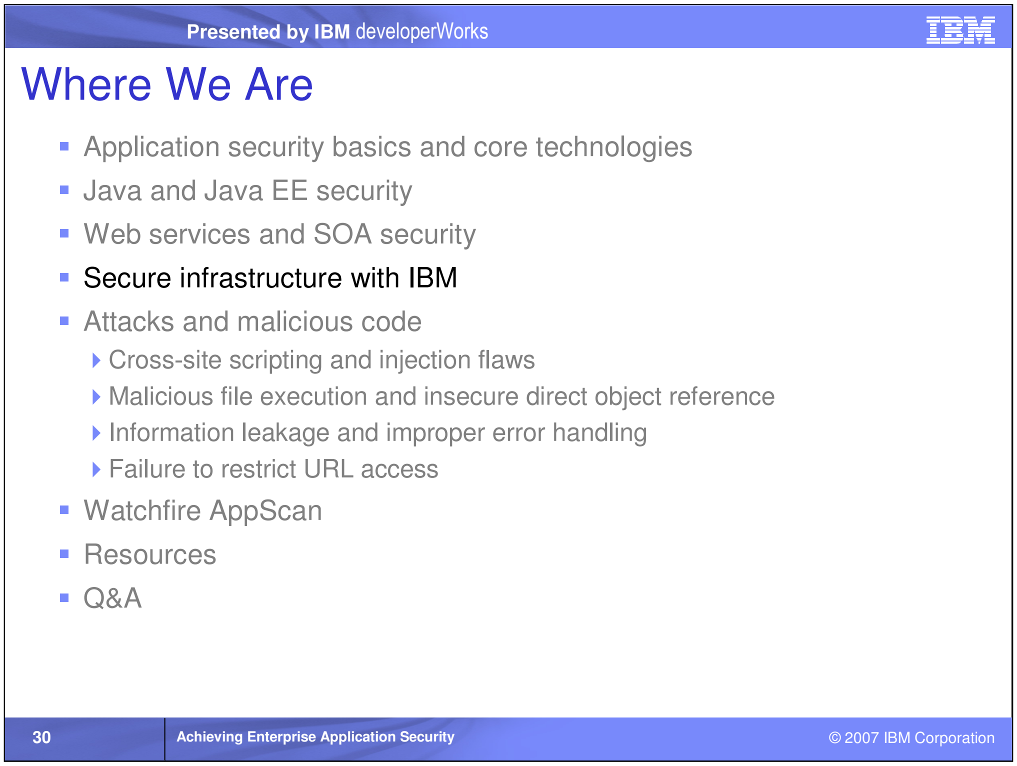
OO Application

SOA Security
- Identity
- Authentication
- Authorization and Privacy
- Confidentiality and Integrity
- Auditing and Compliance
- Management

- We need to implement, manage and monitor security at each level

29 Achieving Enterprise Application Security © 2007 IBM Corporation

With each service used in our architecture we need full security. We need to propagate identities throughout the architecture, where an individual may have different identities but only log in once. We also need all messages fully secure with all the Web service security we've already discussed, plus management of that across domains.



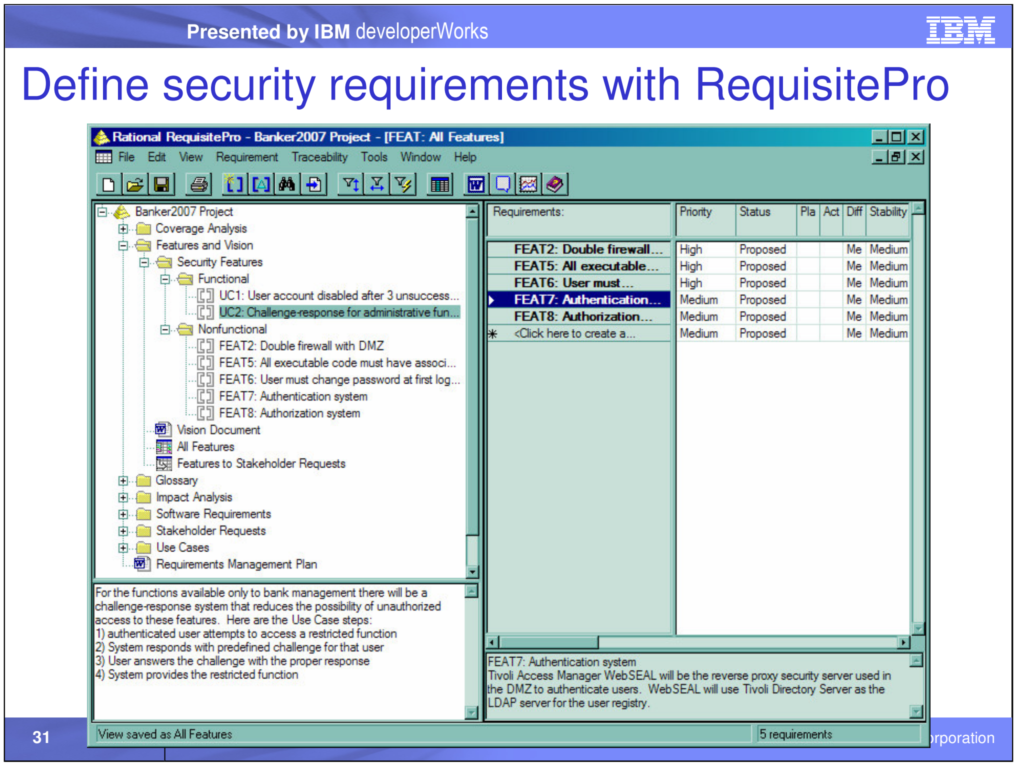
Presented by IBM developerWorks

Where We Are

- Application security basics and core technologies
- Java and Java EE security
- Web services and SOA security
- Secure infrastructure with IBM
- Attacks and malicious code
  - Cross-site scripting and injection flaws
  - Malicious file execution and insecure direct object reference
  - Information leakage and improper error handling
  - Failure to restrict URL access
- Watchfire AppScan
- Resources
- Q&A

30 **Achieving Enterprise Application Security** © 2007 IBM Corporation

Here we’ll look at some security products from IBM.


Presented by IBM developerWorks
IBM
Rational RequisitePro - Banker2007 Project - [FEAT: All Features]
File
Edit
View
Requirement
Traceability
Tools
Window
Help

Define security requirements with RequisitePro

- Banker2007 Project
  - Coverage Analysis
  - Features and Vision
    - Security Features
      - Functional
        - UC1: User account disabled after 3 unsuccess...
        - UC2: Challenge-response for administrative fun...
      - Nonfunctional
        - FEAT2: Double firewall with DMZ
        - FEAT5: All executable code must have associ...
        - FEAT6: User must change password at first log...
        - FEAT7: Authentication system
        - FEAT8: Authorization system
    - Vision Document
    - All Features
    - Features to Stakeholder Requests
  - Glossary
  - Impact Analysis
  - Software Requirements
  - Stakeholder Requests
  - Use Cases
  - Requirements Management Plan

For the functions available only to bank management there will be a challenge-response system that reduces the possibility of unauthorized access to these features. Here are the Use Case steps:
1) authenticated user attempts to access a restricted function
2) System responds with predefined challenge for that user
3) User answers the challenge with the proper response
4) System provides the restricted function

Requirements:	Priority	Status	Pla	Act	Diff	Stability
FEAT2: Double firewall...	High	Proposed			Me	Medium
FEAT5: All executable...	High	Proposed			Me	Medium
FEAT6: User must...	High	Proposed			Me	Medium
FEAT7: Authentication...	Medium	Proposed			Me	Medium
FEAT8: Authorization...	Medium	Proposed			Me	Medium
<Click here to create a...	Medium	Proposed			Me	Medium

FEAT7: Authentication system
Tivoli Access Manager WebSEAL will be the reverse proxy security server used in the DMZ to authenticate users. WebSEAL will use Tivoli Directory Server as the LDAP server for the user registry.

View saved as All Features

5 requirements

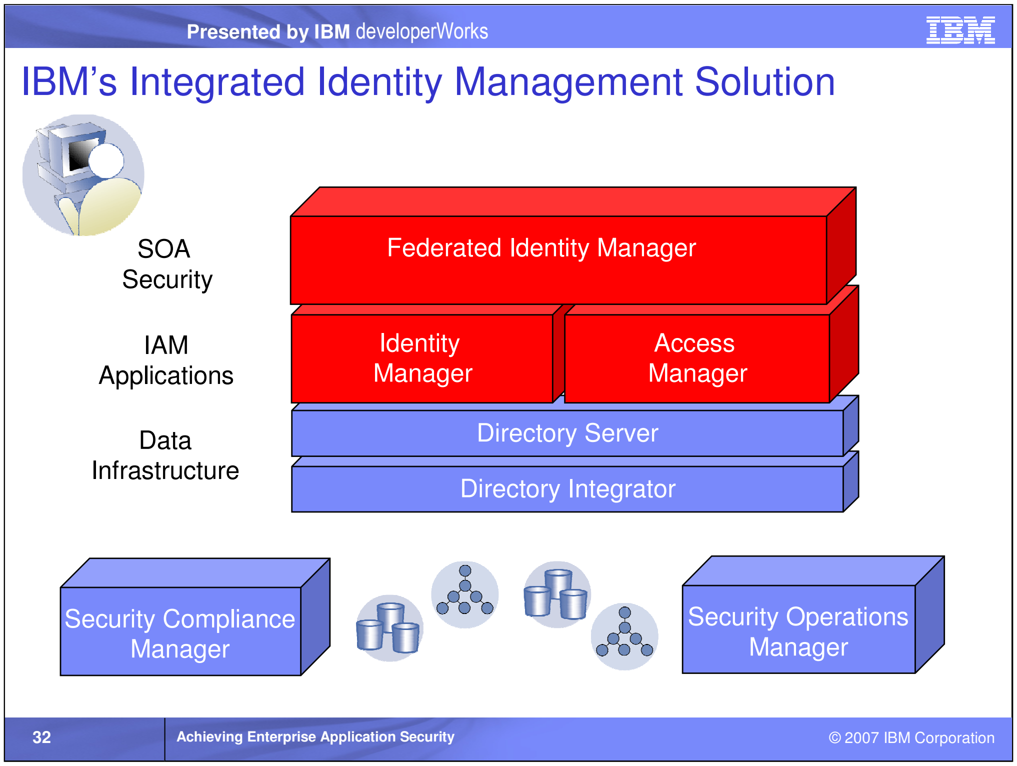
31

rporation

Before we get to the infrastructure products, I want to discuss how a couple of other products can be used as part of development in ensuring a secure application.

Rational RequisitePro is the tool of choice for definining project requirements. It is important that the security requirements of an application be captured as soon as possible in the development process.

Rational ClearQuest is a tool that provides end-to-end application development lifecycle management, with full traceability and integration with all the other Rational Software Delivery Platform products, including RequistePro. ClearQuest also supports test management with security. In order to make a change to a test plan, test suite, or other project artifact, ClearQuest can be configured to require a digital signature from the user to ensure compliance with government, corporate or industry regulations for IT governance.



Presented by IBM developerWorks

IBM's Integrated Identity Management Solution

SOA Security

IAM Applications

Data Infrastructure

Federated Identity Manager

Identity Manager

Access Manager

Directory Server

Directory Integrator

Security Compliance Manager

Security Operations Manager

32 Achieving Enterprise Application Security © 2007 IBM Corporation

These security products are under the Tivoli brand:

Identity Manager delivers provisioning, de-provisioning, and self-service. Tivoli Identity Manager is often abbreviated TIM.

Access Manager delivers controlled access to applications. Tivoli Access Manager is often abbreviated TAM.

Directory Server provides the most powerful and scalable LDAP-based directory in the industry. Tivoli Directory Server is often abbreviated TDS.

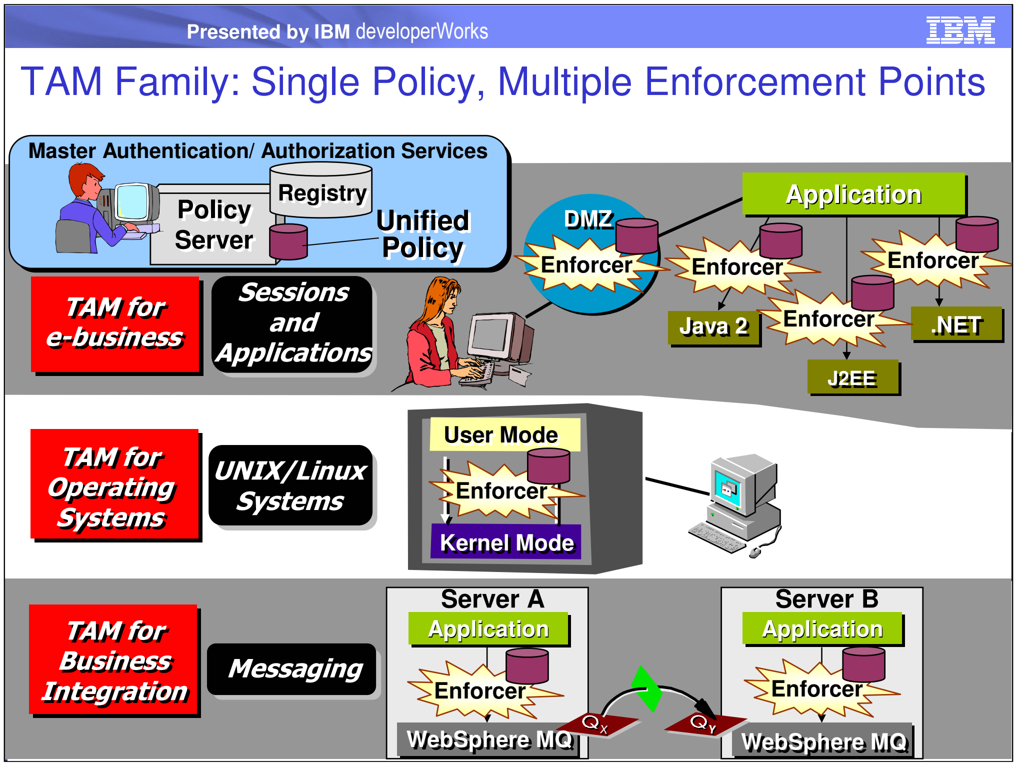
Directory Integrator addresses the underlying issue that the average large firm stores user information in 181 places (Forrester, 2000). Since this identity management software relies on having a clean, valid list of current users, how do we gather this pragmatically? Well, Directory Integrator allows us to synchronize all of these user information sources together to accomplish this goal. Tivoli Directory Integrator is often abbreviated TDI.

Security Compliance Manager is a security policy compliance product that checks systems and applications for vulnerabilities and identifies violations against security policies.

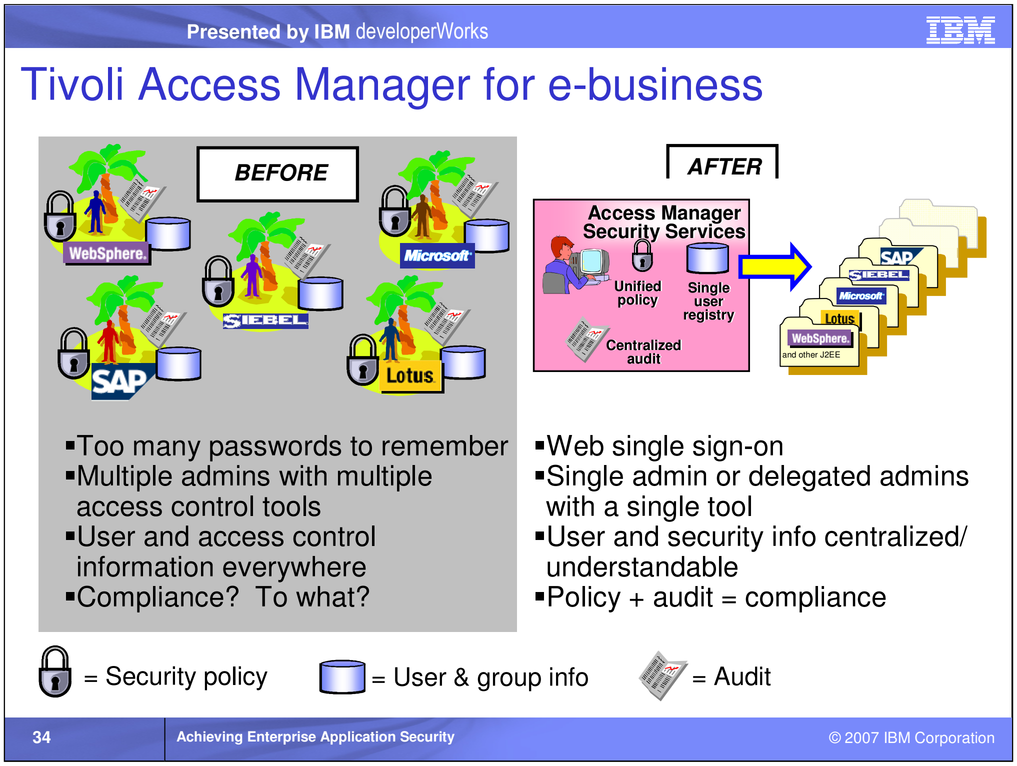
Security Operations Manager is a Security Information & Event Management (SIEM) solution to improve the effectiveness, efficiency, and visibility of security operations, succeeding Tivoli Risk Manager as security monitoring solution.

Finally, most firms are looking at delivering their next-generation applications through Web services, and security is the #1 issue there. Most folks call the technology for addressing this "federated identity management," and IBM Tivoli is one of the leaders, with Tivoli Federated Identity Manager, or TFIM.

We will take a closer look in the following slides at the products in red.



Tivoli Access Manager is an Integrated Security Platform for e-business that delivers single sign-on to Web-based applications and much more. It lets the right people in, to access the right applications and data by providing integrated, policy-based security management of users, access control, portals, Web applications, messaging applications, custom applications and more. It extends to address the security of the WebSphere MQ family (with Access Manager for Business Integration working with the base Access Manager's services), z/OS or OS390 and UNIX/Linux environments (with Access Manager for Operating Systems working with the base Access Manager's services) and ensures availability in multi-enterprise deployments. Key services that Access Manager provides are single sign-on to Web-based applications and (the heart of Access Manager) policy-based access to applications and data. In addition, the platform addresses distributed, delegatable management of users and access rights. The access rights or permissions address Web applications, including portals, and custom applications.



Presented by IBM developerWorks

Tivoli Access Manager for e-business

- Too many passwords to remember
- Multiple admins with multiple access control tools
- User and access control information everywhere
- Compliance? To what?

- Web single sign-on
- Single admin or delegated admins with a single tool
- User and security info centralized/ understandable
- Policy + audit = compliance

🔒 = Security policy ▭ = User & group info ✎ = Audit

34 Achieving Enterprise Application Security © 2007 IBM Corporation

Access Manager brings a directory-based, integrated approach to user management and security services for e-business.

The left-hand side of the picture depicts the “islands of security” approach ... wherein customers implement security within applications or more typically using unique security mechanisms provided by a particular application environment. There is nothing nefarious about this; it’s a natural thing to occur that companies implement security and develop specialized skills for each of the application areas they are investing in. But other than perhaps some significant expertise on the part of the security teams that have to stay on top of each application environment, what does the company gain from this? This kind of evolution is actually problematic, in that these security solutions can never be effectively cobbled together, and the result is that the company that is set up this way has no real idea what their e-business or Web security policy is.

The “after” picture is one involving partners, customers, employees, suppliers, and any other e-business participant attempting to access some resources in the secure intranet. By placing a security layer (HTTP reverse proxy called WebSEAL) in the demilitarized zone, we can accomplish secure, policy-based, and highly available transactions to take place.

The integration that Access Manager affords enables

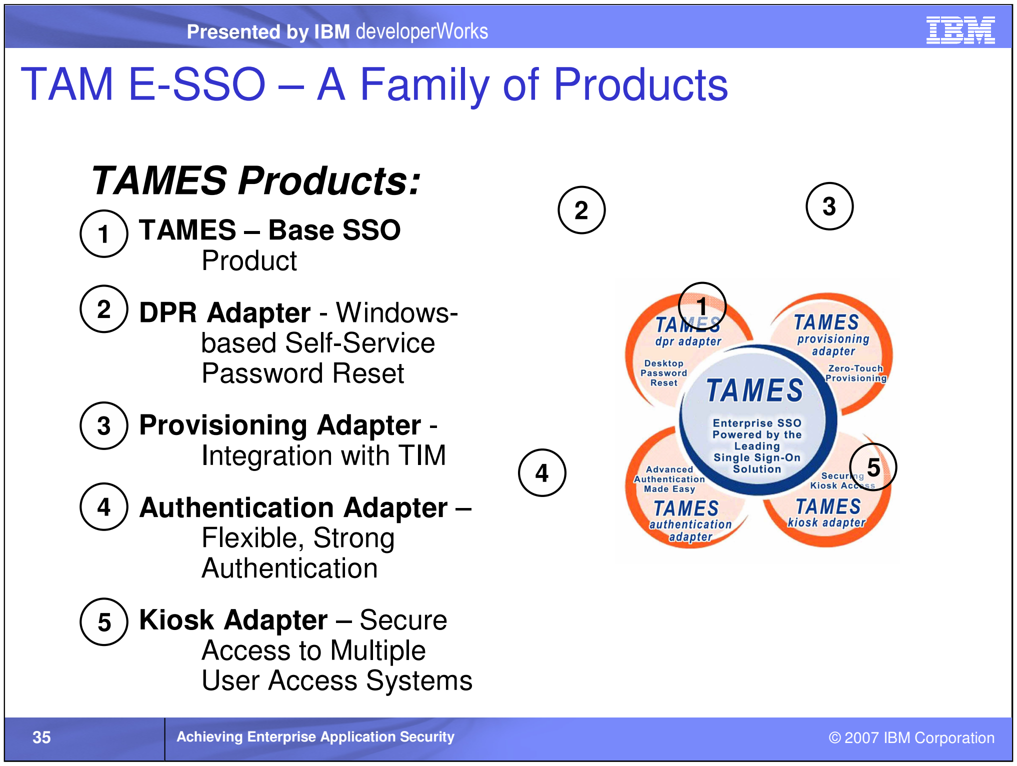
Sharing of user and group information in a common directory

Single sign-on to the target applications

Efficient exchange of personalization data to maximize the users’ satisfaction with the transaction

Defense in depth – the capability of layering access points, in order to prevent unauthenticated or unauthorized users from entering the secure intranet

Plug-and-play security for application providers such as Siebel, SAP, Plumtree, BroadVision and others



Presented by IBM developerWorks

TAM E-SSO – A Family of Products

TAMES Products:

1. **TAMES – Base SSO** Product
2. **DPR Adapter** - Windows-based Self-Service Password Reset
3. **Provisioning Adapter** - Integration with TIM
4. **Authentication Adapter** – Flexible, Strong Authentication
5. **Kiosk Adapter** – Secure Access to Multiple User Access Systems

2
3
1
TAMES
dpr adapter
Desktop Password Reset
TAMES
provisioning adapter
Zero-Touch Provisioning
TAMES
Enterprise SSO Powered by the Leading Single Sign-On Solution
4
5
Advanced Authentication Made Easy
TAMES
authentication adapter
Securing Kiosk Access
TAMES
kiosk adapter

35 Achieving Enterprise Application Security © 2007 IBM Corporation

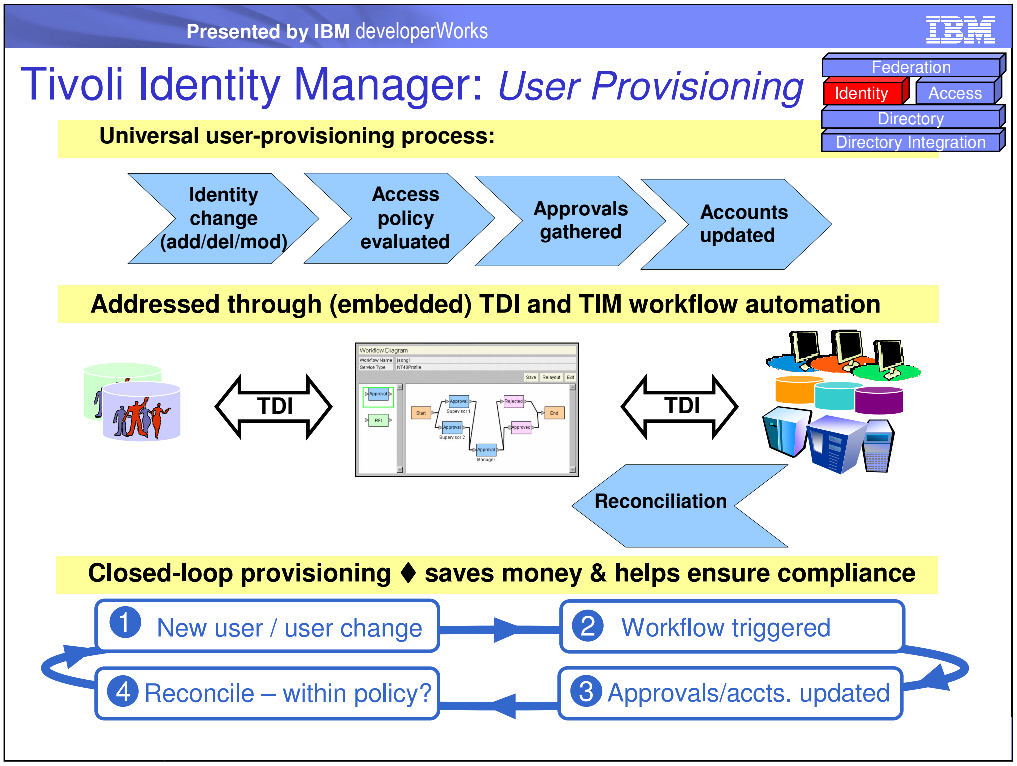
TAM for E-SSO (TAMES) is the enterprise single sign-on solution. TAMES's patented architecture eliminates the burden of integration so customers can start reaping the benefits of single sign-on in days - not months.

TAMES Desktop Password Reset (DPR) enables end user to reset their Windows password, without calling the help desk, directly from the locked workstation.

TAMES Authentication Adapter allows organizations to use any combination of tokens, smart cards, biometrics and passwords to control access to their applications.

TAMES Provisioning Adapter enables TIM system administrators to directly distribute user credentials — usernames and passwords — to the TAMES Enterprise Single Sign-On solution.

TAMES Kiosk Adapter provides automated termination of inactive sessions and application shutdown for Kiosk or shared workstation users.



Presented by IBM developerWorks

Tivoli Identity Manager: *User Provisioning*

Universal user-provisioning process:

Identity change (add/del/mod) → **Access policy evaluated** → **Approvals gathered** → **Accounts updated**

Addressed through (embedded) TDI and TIM workflow automation

Closed-loop provisioning ♦ saves money & helps ensure compliance

1 New user / user change

2 Workflow triggered

3 Approvals/accts. updated

4 Reconcile – within policy?

IBM Tivoli Identity Manager is one of the products in the IBM integrated identity management solution. Tivoli Identity Manager can automate the management and user provisioning of user identities across the e-business infrastructure. It can help reduce administration costs with delegated administration, centralized user account creation (including self-service interfaces), automated approvals processing that integrates with existing business processes and resource provisioning.

Let’s look at an example of automating the steps performed for managing a user.

An identity change is requested, such as create a new user account, modify a user account, or delete a user account. This identity change request could be automatically triggered by an event within your organization. For example, adding a new employee to the Human Resources (HR) Systems could automatically trigger the need to create a user account, based on that employee’s role within the organization.

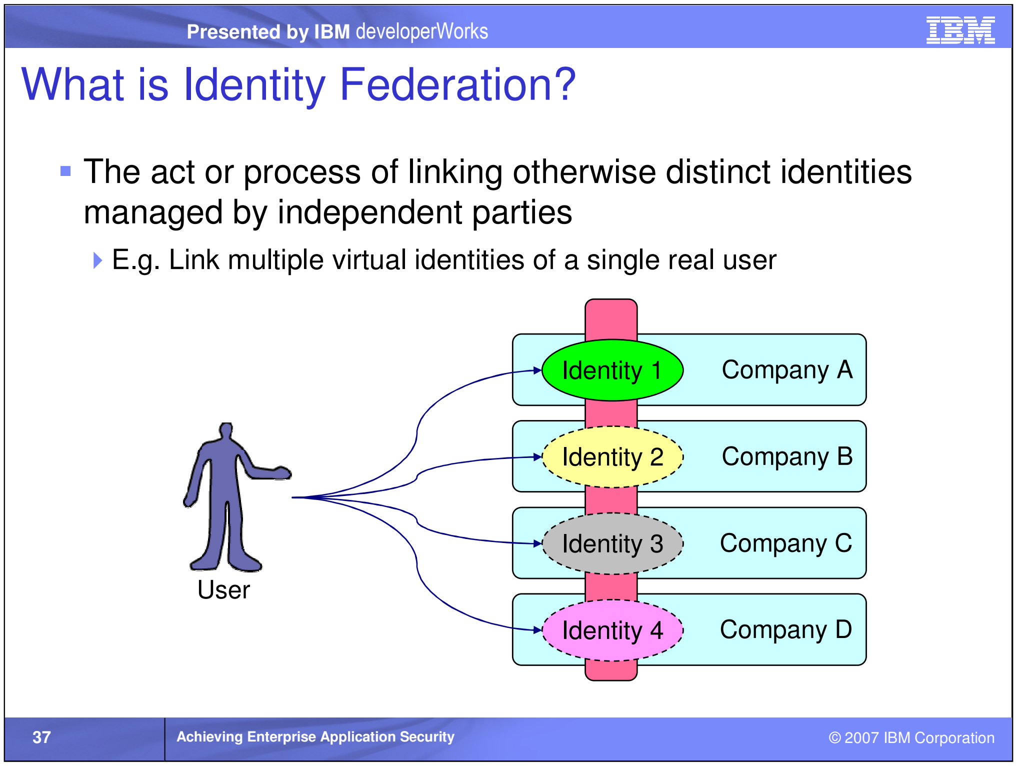
Tivoli Identity Manager then evaluates the access policy, using a powerful and flexible automated workflow engine that is GUI based.

An automated process is used to gather the required approvals. Automation can simplify and accelerate this process.

User accounts are then automatically created, updated, or removed on the corresponding operating systems, databases and applications. Tivoli Identity Manager has the industry’s most comprehensive list of supported agents that are used to provision and de-provision user accounts, as well as a toolkit to further extend the solution to additional endpoints.

Using bi-directional support, resources are also monitored for any changes made by local administrators, to ensure that those changes are in compliance with your organization’s security policies. If a local administrator change is not in compliance, it can be overridden.

Any time an identity change is made to a user, whether it’s add, modify, or delete, it is managed by Tivoli Identity Manager to help ensure consistent compliance with your organization’s security policy, and to leverage all of the automation and self-service capabilities for improved productivity. Tivoli Identity Manager helps automate the business processes of creating and provisioning users, managing users and also de-provisioning users.



Presented by IBM developerWorks

What is Identity Federation?

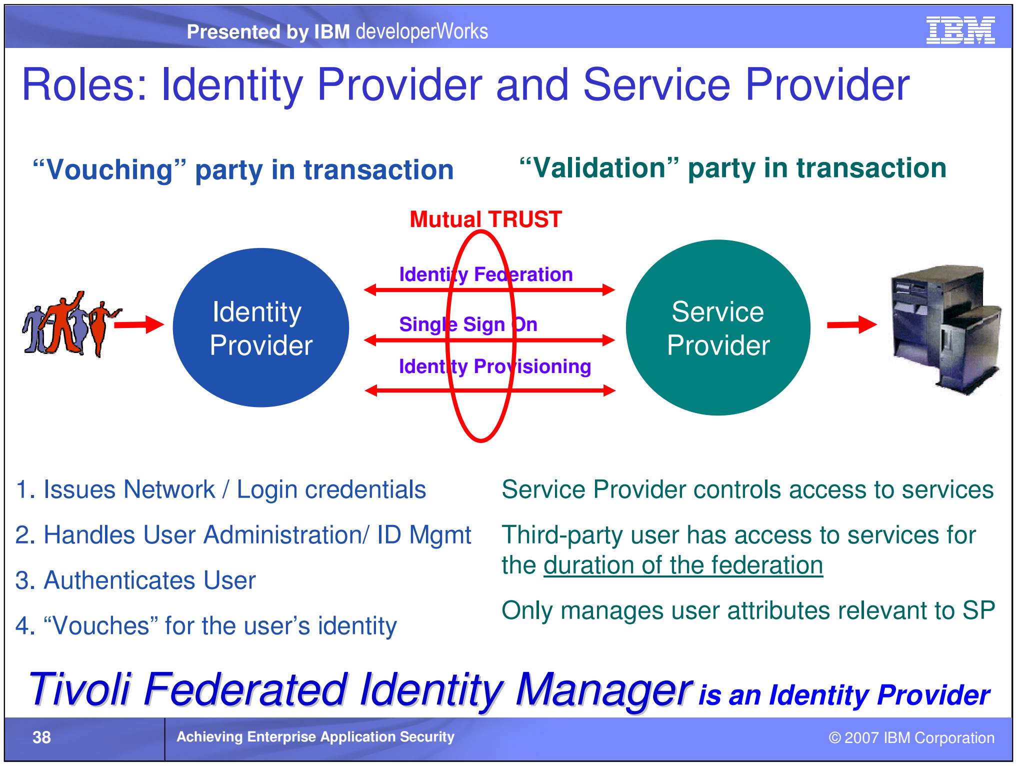
- The act or process of linking otherwise distinct identities managed by independent parties
  - E.g. Link multiple virtual identities of a single real user

37 Achieving Enterprise Application Security © 2007 IBM Corporation

Federated Identity Management can provide secure business-to-business integration to link identity providers and service providers, while improving the user experience. In this example, the user logs in to their financial institution, which is a trusted identity provider. The financial institution is performing the identity management functions to manage and provision the user on its systems.

When the user wants to access additional Web services that are being provided by other partner providers to the financial institution, the user experiences a seamless access to those Web services. Since the financial institution has already authenticated the user, the user is able to access the desired Web services from the other partner providers without logging in a second or third time. The Web service providers use the identity information that they are provided from the financial institution, which is the trusted identity provider in this example.

The user benefits by being able to seamlessly access all of the needed services from their financial institution, as well as from other trusted Web services providers. At the same time the Web services providers benefit by being able to provide their services to users without having to incur all of the expenses associated with managing the user's identity.



Presented by IBM developerWorks

Roles: Identity Provider and Service Provider

“Vouching” party in transaction

“Validation” party in transaction

Mutual TRUST

1. Issues Network / Login credentials
2. Handles User Administration/ ID Mgmt
3. Authenticates User
4. “Vouches” for the user’s identity

Service Provider controls access to services

Third-party user has access to services for the duration of the federation

Only manages user attributes relevant to SP

Tivoli Federated Identity Manager ***is an Identity Provider***

38 Achieving Enterprise Application Security © 2007 IBM Corporation

Within a federation, organizations play one or both of two roles: identity provider and/or service provider. The purpose of federated identity management is to link identity providers with service providers.

Identity Provider:

The identity provider (IdP) is the authoritative site responsible for authenticating an end user and asserting an identity for that user in a trusted fashion to trusted partners. The identity provider is responsible for account creation, provisioning, password management, and general account management, and also acts as a collection point or client to trusted identity providers.

Service Provider:

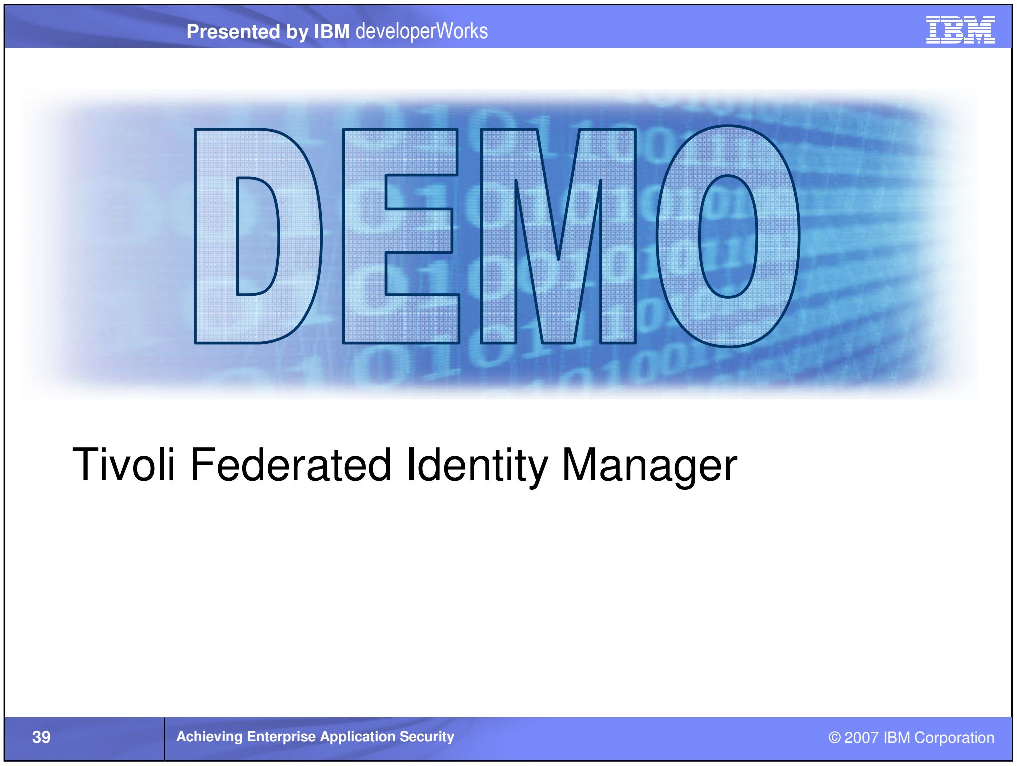
Those partners who offer services but do not act as identity providers are known as service providers. The service provider (SP) relies on the IdP to assert information about a user, leaving the SP to manage only those user attributes that are relevant to the SP.

In a federation

1. The user authenticates once, to trusted a identity provider

2. The user identity is managed by trusted the identity provider

3. Other Web services providers use identity information from the trusted identity provider



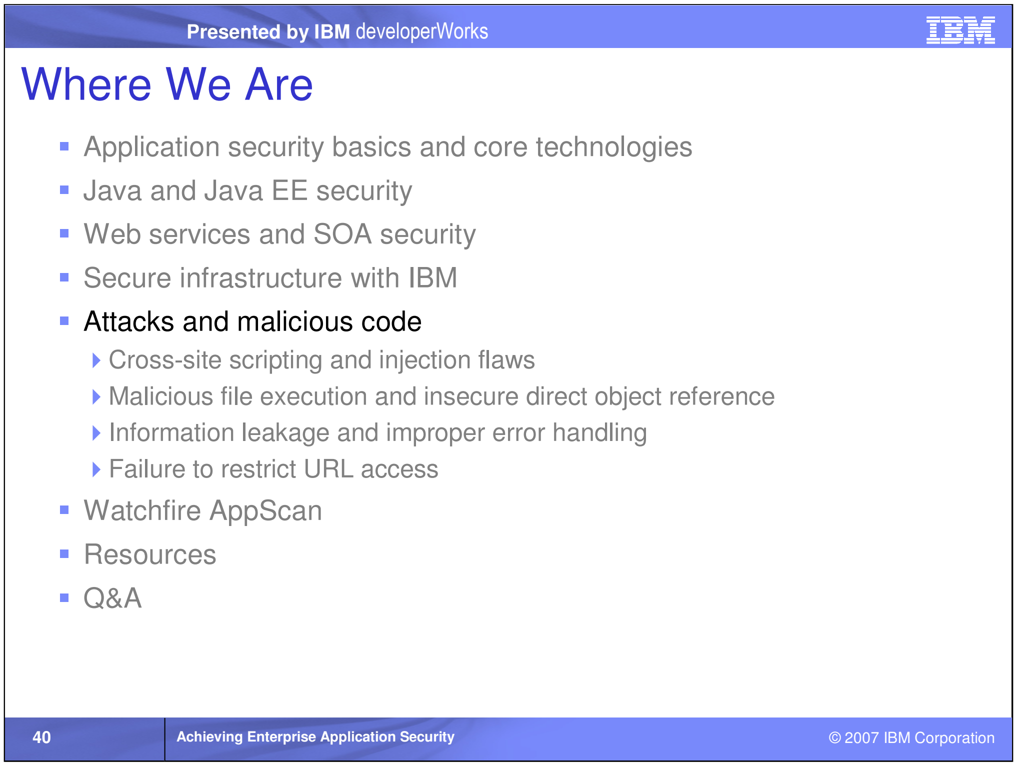
Presented by IBM developerWorks

DEMO

Tivoli Federated Identity Manager

39 Achieving Enterprise Application Security © 2007 IBM Corporation

We'll look at a short video showing how Tivoli Federated identity Manager enables single sign-on across federated domains.



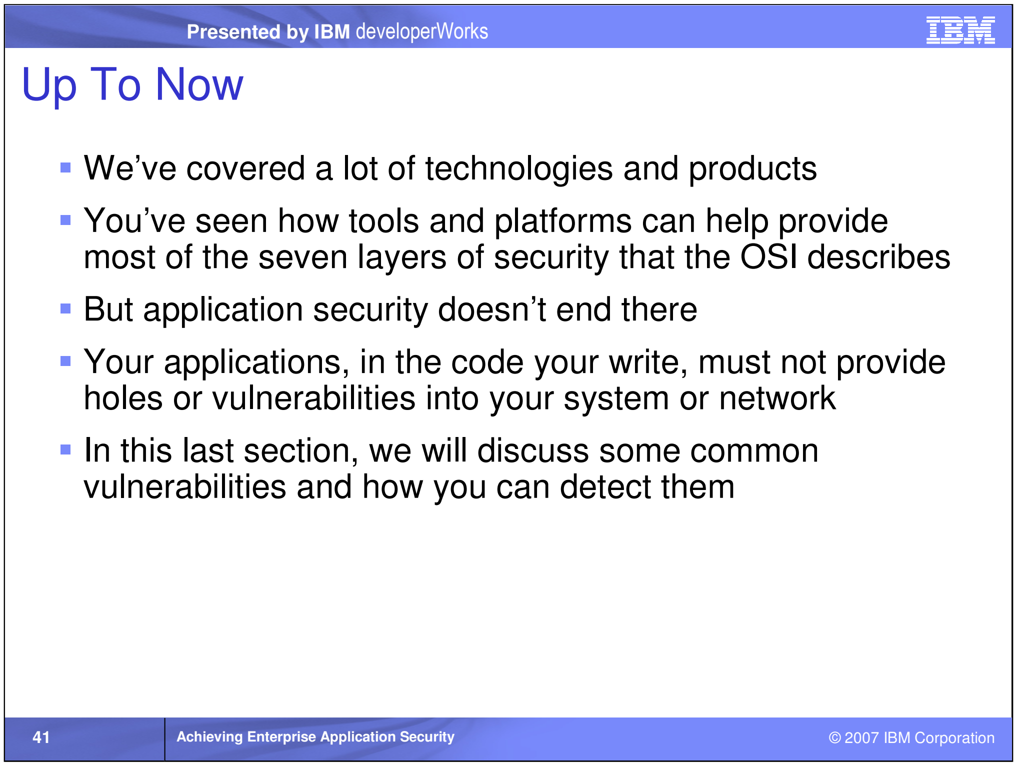
Presented by IBM developerWorks

Where We Are

- Application security basics and core technologies
- Java and Java EE security
- Web services and SOA security
- Secure infrastructure with IBM
- Attacks and malicious code
  - Cross-site scripting and injection flaws
  - Malicious file execution and insecure direct object reference
  - Information leakage and improper error handling
  - Failure to restrict URL access
- Watchfire AppScan
- Resources
- Q&A

40 Achieving Enterprise Application Security © 2007 IBM Corporation

Let’s move on and discuss attacks and malicious code.



Presented by IBM developerWorks

Up To Now

- We’ve covered a lot of technologies and products
- You’ve seen how tools and platforms can help provide most of the seven layers of security that the OSI describes
- But application security doesn’t end there
- Your applications, in the code your write, must not provide holes or vulnerabilities into your system or network
- In this last section, we will discuss some common vulnerabilities and how you can detect them

41 Achieving Enterprise Application Security © 2007 IBM Corporation

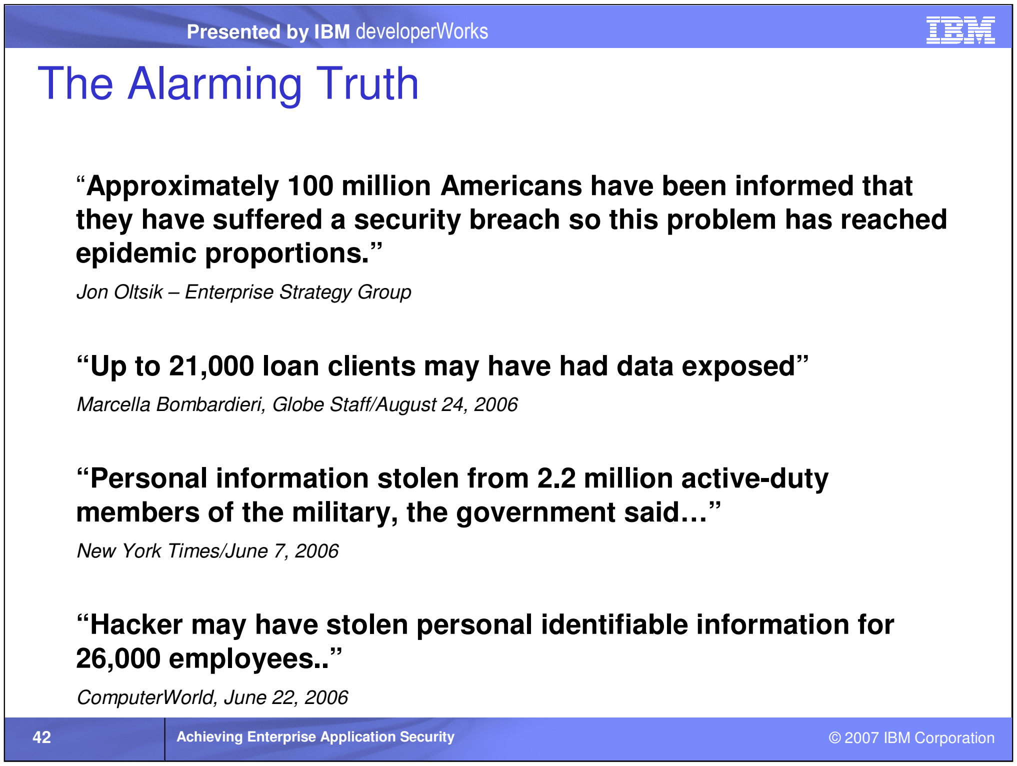
We’ve covered a lot of technologies and products.

You’ve seen how tools and platforms can help provide most of the seven layers of security that the OSI describes.

But application security doesn’t end there.

Your applications, in the code your write, must not provide holes or vulnerabilities into your system or network.

In this last section, we will discuss some common vulnerabilities and how you can detect them.



The Alarming Truth

“Approximately 100 million Americans have been informed that they have suffered a security breach so this problem has reached epidemic proportions.”

Jon Oltsik – Enterprise Strategy Group

“Up to 21,000 loan clients may have had data exposed”

Marcella Bombardieri, Globe Staff/August 24, 2006

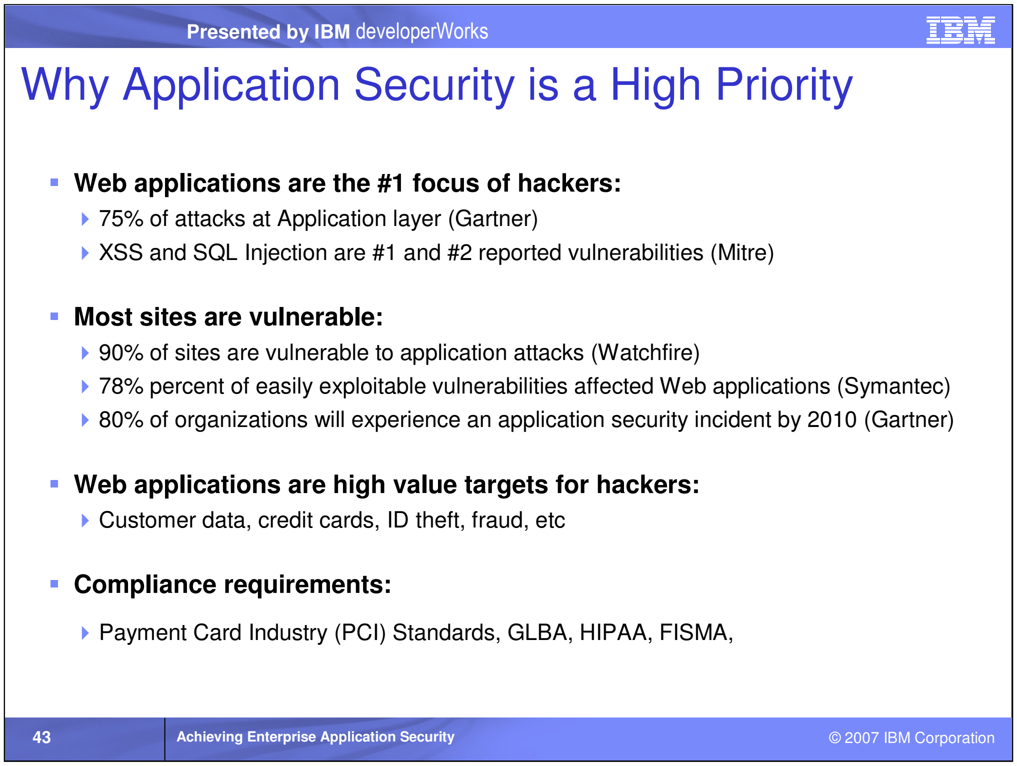
“Personal information stolen from 2.2 million active-duty members of the military, the government said…”

New York Times/June 7, 2006

“Hacker may have stolen personal identifiable information for 26,000 employees..”

ComputerWorld, June 22, 2006

There is a real problem out there.



Presented by IBM developerWorks

Why Application Security is a High Priority

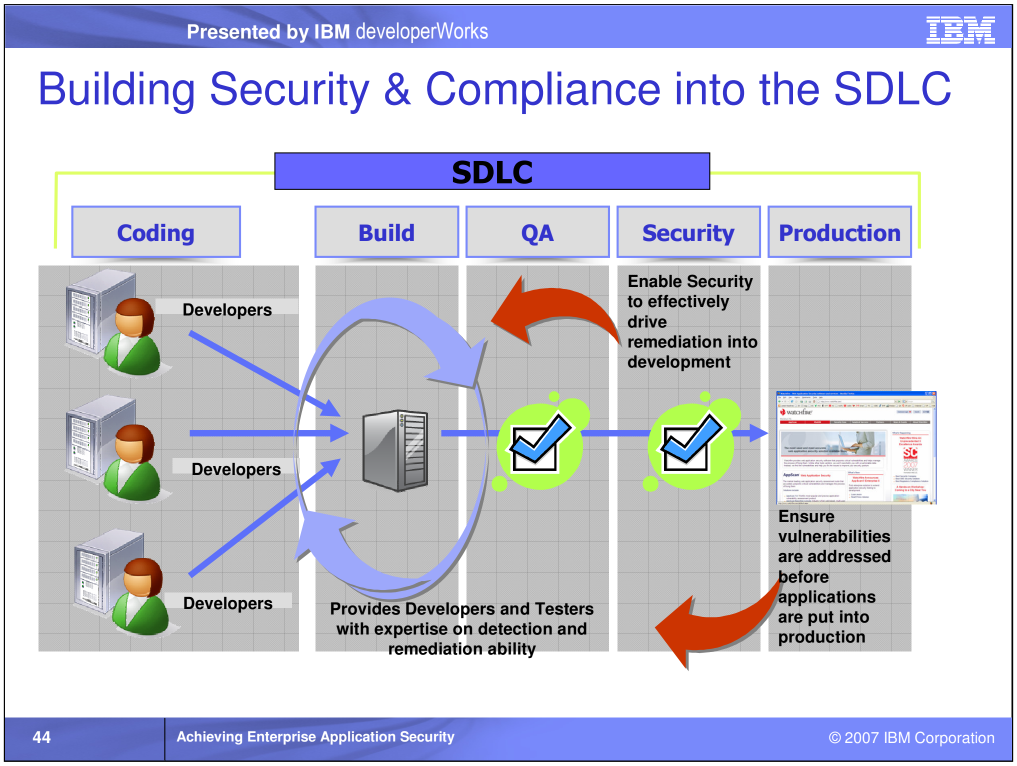
- **Web applications are the #1 focus of hackers:**
  - 75% of attacks at Application layer (Gartner)
  - XSS and SQL Injection are #1 and #2 reported vulnerabilities (Mitre)
- **Most sites are vulnerable:**
  - 90% of sites are vulnerable to application attacks (Watchfire)
  - 78% percent of easily exploitable vulnerabilities affected Web applications (Symantec)
  - 80% of organizations will experience an application security incident by 2010 (Gartner)
- **Web applications are high value targets for hackers:**
  - Customer data, credit cards, ID theft, fraud, etc
- **Compliance requirements:**
  - Payment Card Industry (PCI) Standards, GLBA, HIPAA, FISMA,

43 Achieving Enterprise Application Security © 2007 IBM Corporation

Here we see some statistics and figures that point at Web applications as being the most vulnerable and the most likely points of attack..

Hackers see Web applications as high value targets, containing the information they most want to get their hands on.

Additionally, the security (or not) of Web applications can have direct impact on compliance with standards and regulations like the Payment Card Industry (PCI) Standards, the Gramm-Leach-Bliley Act (GLBA) which regulates financial services, the Health Insurance Portability and Accountability Act (HIPAA) which regulates the health insurance and healthcare industry, and the Federal Information Security Management Act (FISMA) which regulates government agencies and government contractors.



Presented by IBM developerWorks

Building Security & Compliance into the SDLC

SDLC

Coding

Build

QA

Security

Production

Developers

Developers

Developers

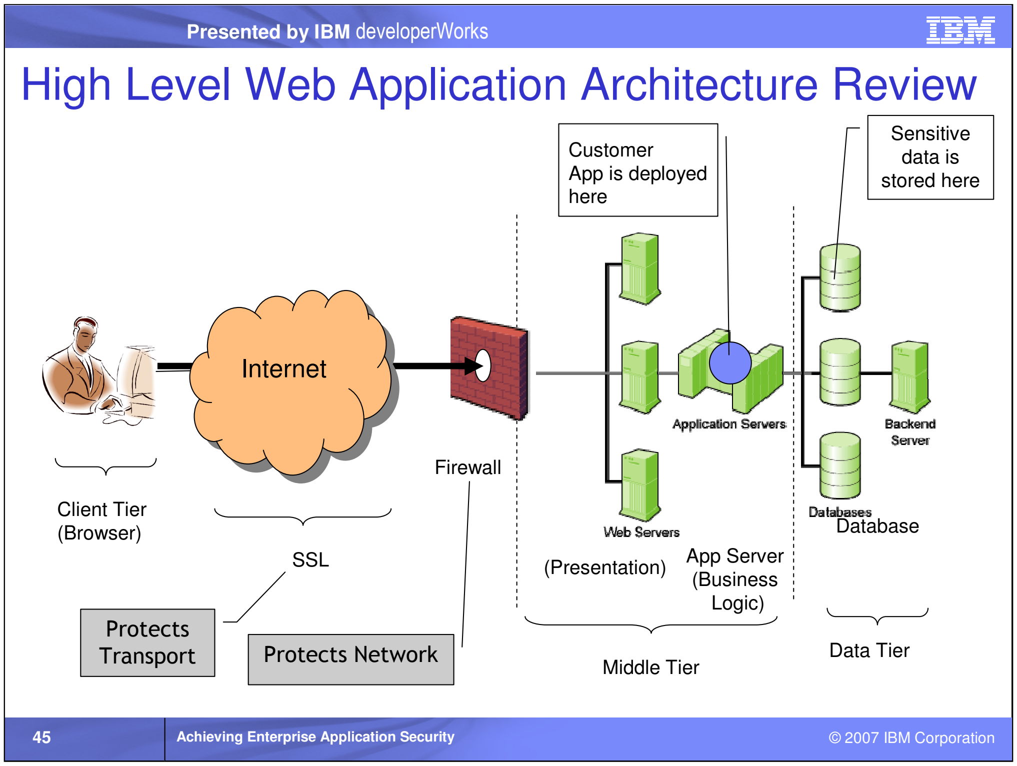
Provides Developers and Testers with expertise on detection and remediation ability

Enable Security to effectively drive remediation into development

Ensure vulnerabilities are addressed before applications are put into production

44 Achieving Enterprise Application Security © 2007 IBM Corporation

Security and compliance should be an important consideration during the Software Development Lifecycle. Watchfire solutions of AppScan and WebXM provide tools to ensure web security vulnerabilities are identified and addressed early in the lifecycle and also ensure that web sites are in compliance.

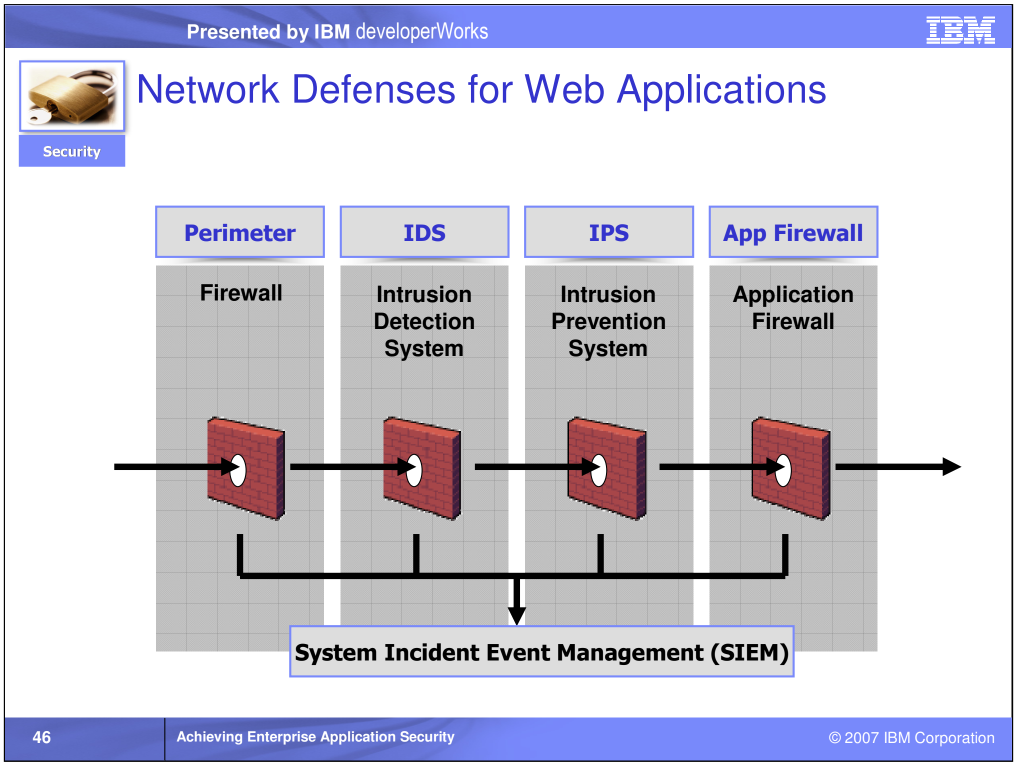


Presented by IBM developerWorks

High Level Web Application Architecture Review

45 Achieving Enterprise Application Security © 2007 IBM Corporation

In a typical Web application security landscape, the user on the left-hand side interacts with the server environment, on the right. The data that is exchanged back and forth between the user and server environment might be encrypted using SSL, or it may not be, but it moves across the firewalls, intrusion detection systems, intrusion prevention systems, routers, switches to the web server on the other side. Note that it is the web application that facilitates the exchange of data between the server environment and the user. It is interesting to stop and note that while the data received from the client is not to be trusted, the web application itself is implicitly trusted by the backend environment and is permitted to communicate with everything from the database to an LDAP authentication system or to the core network. Let’s take a little closer look at the network protections that might be associated with this exchange of data.



Presented by IBM developerWorks

Security

Network Defenses for Web Applications

Perimeter	IDS	IPS	App Firewall
Firewall	Intrusion Detection System	Intrusion Prevention System	Application Firewall

System Incident Event Management (SIEM)

46 Achieving Enterprise Application Security © 2007 IBM Corporation

The first barrier that an HTTP request encounters while crossing the network is a firewall. Firewalls are set up to allow outsiders access to specific resources, and to prevent them from accessing other resources. For example, an outside individual wouldn't be allowed to directly connect to a database, but they can make a request to a web server. This means the firewall would be configured to deny traffic on a standard database port 1443, but allow traffic through ports 80 and 443 - web application ports. This system is clearly no protection at all against malicious attacks.

The next protection an HTTP request encounters is an intrusion detection system. The IDS has been set up to look for signatures in the traffic that might indicate an attack. For example, they may look for a SQL statement embedded within a request, or they might look for a script tag for indicates a potential XSS attack. The challenge with these systems is that if the request is encoded in some alternative format (say UTF-7) or perhaps the traffic is encrypted using SSL, the intrusion detection system is often not able to interpret or understand the requests. The IDS offers little to no protection against the web application attack.

The next protection that an HTTP request might encounter is an intrusion prevention system or IPS. These systems are designed to explicitly block requests that are deemed to be malicious. It is very similar to the IDS, except that it takes an active role rather than a passive one. Again, if the traffic is encoded or encrypted, the systems may not be able to block malicious requests. The IPS offers little protection against the web application attack.

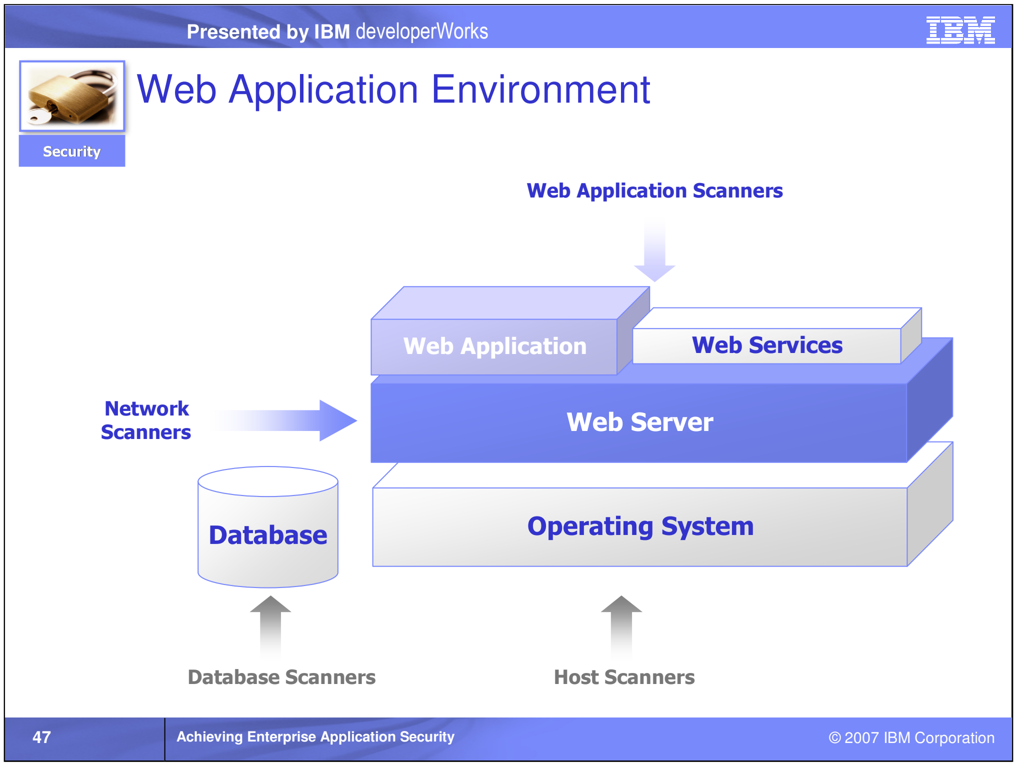
The lines are blurring actually, between the IDS and IPS systems.

The last system that the HTTP request might encounter before the web server is probably an application firewall. These are the smartest of all the network protections and can be configured explicitly to only allow through certain traffic that it knows to be good. The problem with these systems is that it's very expensive to maintain the correct configurations or valid algorithms to recognize good traffic. If the web application firewall has been designed to fail securely (a web application security principle), that is, if you're not sure what to do, they block the user, the web application firewall may block legitimate traffic. For this reason, most application firewalls are usually designed to break one of the founding principles of security (fail securely) by allowing through traffic that they don't understand.

There is one other issue with web application firewalls. They do not understand the application. As an example, they might be configured to allow a numerical value for a certain cookie value, but they do not know that my user is only allowed a value of 6014, but not 6015. A core principle in web application defense is that THE WEB APPLICATION MUST DEFEND ITSELF. Are web application firewalls valuable? Absolutely!

Another implicit challenge faced by the network protections is that they throttle and slow the data traffic. Some organizations are averse to decrypting and re-encrypting, or implementing systems that have noticeable degradation of the user experience.

All of these systems feed into the security incident and event management system. You may consider these devices as operational controls or real-time defense against the real-time attack. They are not used to find vulnerabilities but rather to protect the application in real time.



Presented by IBM developerWorks

Security

Web Application Environment

47 Achieving Enterprise Application Security © 2007 IBM Corporation

If the web application must defend itself, let's take a very high level look at web application vulnerability assessment (VA). This will consider the products that will be used to discover vulnerabilities within or related to the Web application. We will discuss these in the typical order of usage – not priority.

The first product to be considered is the host-based VA product. These look for issues on the boxes. The reason why these are used first and are the largest expenditure in this world as the box requires an operating system and the operating system needs to be locked down. Host-based products ensure that shares, configuration and patches are properly implemented. There can be no web application without an operating system and web server. Protections for vulnerabilities and problems found by these products include configuration changes and patches.

The second products we will consider are network scanners. As mentioned before, these products are not provided local credentials for the systems. Instead, they are used to scan the network, discovering devices (web servers in this case) and testing them for known vulnerabilities. For example, if you're running Apache 1.3.27, it is known to have current known vulnerabilities with negative content length buffer overflows. They also have some additional capabilities which we will discuss on the next slide. Network VA tools are usually used first as this is the most commonly used tool by the malicious individual. Thankfully, administrators also have access to this software and have considerable knowledge and experience at implementing protections at the network layer. Protections most often mean patching.

A third product that may or may not be used, is a specific type of host-based VA: database assessment. These products require credentials on the target database and similar to host-based assessment, offer suggestions for all problems through configuration and patching. There are really only two players here: AppSec Inc and NGS Software. These have not yet received wide market adoption and are often a piece of the pure host-based assessment.

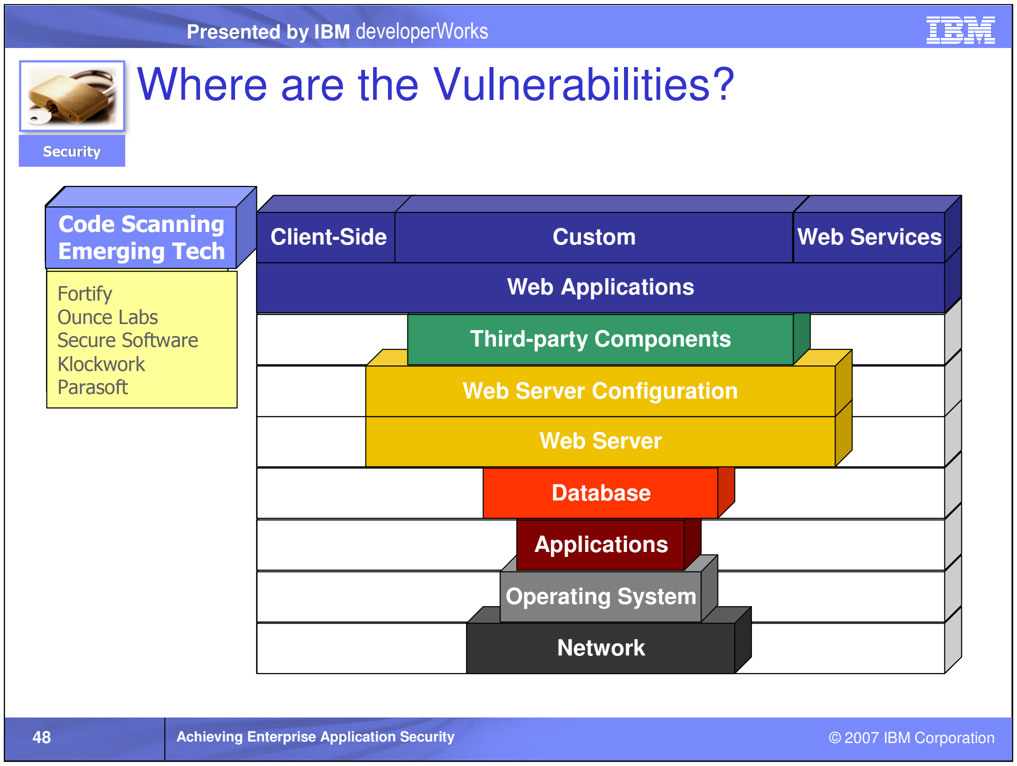
Up to this point, none of these vulnerability assessment products do anything to discover application specific vulnerabilities in the web application itself.

The next products that are usually used are black-box (outside-in) web application scanning products. This is clearly where Watchfire has the most significant focus.

The last products that might be used are white-box (inside-out) source code scanning products. These do not take a typical vulnerability reporting perspective and instead report on best practices for coding. Failure to adhere to the best practices may lead to application compromise. Issues reported by source code analysis are theoretical until verified by a security professional.

Unless an organization has implemented either black-box or white-box (complimentary views) of web application security, they are exposed to significant risk. The only way to test a web application is to understand all the inputs to the application and to comprehensively test these for security issues.

Let’s consider web application VA in the context of the larger picture and where the vulnerabilities are found.



Presented by IBM developerWorks

Where are the Vulnerabilities?

Security

Code Scanning Emerging Tech

Fortify
Ounce Labs
Secure Software
Klockwork
Parasoft

Client-Side	Custom	Web Services
Web Applications		
Third-party Components		
Web Server Configuration		
Web Server		
Database		
Applications		
Operating System		
Network		

48 Achieving Enterprise Application Security © 2007 IBM Corporation

This security stack clearly depicts the framework of the network through to web application. What areas do each of the VA tools address?

Let’s look at the network VA tools first. These do not have any permission on the operating system itself and includes products like Nessus, ISS Security Scanner, QualysGuard, and eEye Retina. These discover and search for vulnerabilities on the network (routers, switches, and firewalls) as well as web servers and known web applications.

Host-based assessment products look at applications. (Remember that the operating system is really just a foundational application.)

Database assessment products are specialized host-based products requiring credentials, that consider specific issues found in databases – another form of application.

Black-box application scanners consider everything at the top of this stack: from the web server to web server configuration, third party components and the web application itself. This might include client-side components such as JavaScript used in AJAX and Web 2.0, web services and service oriented architectures as well as the web application itself.

White-box application scanners are limited to the latter component. They can look at the source code of the web application itself, and only where the code is available.

So why is it that some network scanners claim that they can find and report on SQL injection, XSS and buffer overflows? This is because there is some overlap in capabilities. Some of these issues (XSS and buffer overflows) exist in the web server itself, while all three (SQL Injection, XSS and buffer overflows) can be found in third party components. Network scanners DO NOT explore the web application or find any issues that are introduced in the application itself.

Some overlap exists because both black-box application scanners and network scanners are able to find issues in the web server, web server configuration and third party components.

So is a web application scanning technology really necessary? Where do the vulnerabilities exist? It is interesting to realize that 10 years ago most of the vulnerabilities lived in the network or operating system. This is no longer the case. IT administrators to become very smart about security and products have gotten very mature in the lower levels of the stack, right up to, and including, third party components used by web applications. The people who understand security are those that control the network, operating systems and applications. These issues are solved through configuration and patching.

The challenge arises because they IT administrator does not understand the application – a requirement for securing the application. The web developer, who understands the application, does not understand security or have sufficient tools or knowledge to eliminate this issue. Further, while there a finite number of IPs in a network, or a finite number of ports on a device to be analyzed, a web application has a potentially infinite number of entry points, from forms, to query strings to cookies to header fields. This leaves the application with a significant number of vulnerabilities.

Crackers are not unaware of this. Gartner reports that 75% of attacks now occur at the network layer and Watchfire has found that 90% of applications are vulnerable.

One last thought. There is implicit trust in this stack. If the malicious individual is able to find an issue in the web application, keep in mind that the web application is typically trusted by the database, the applications, the operating system and the network. The entire system may be compromised.

Presented by IBM developerWorks

IBM

Security

The Myth: “Our Site Is Safe”

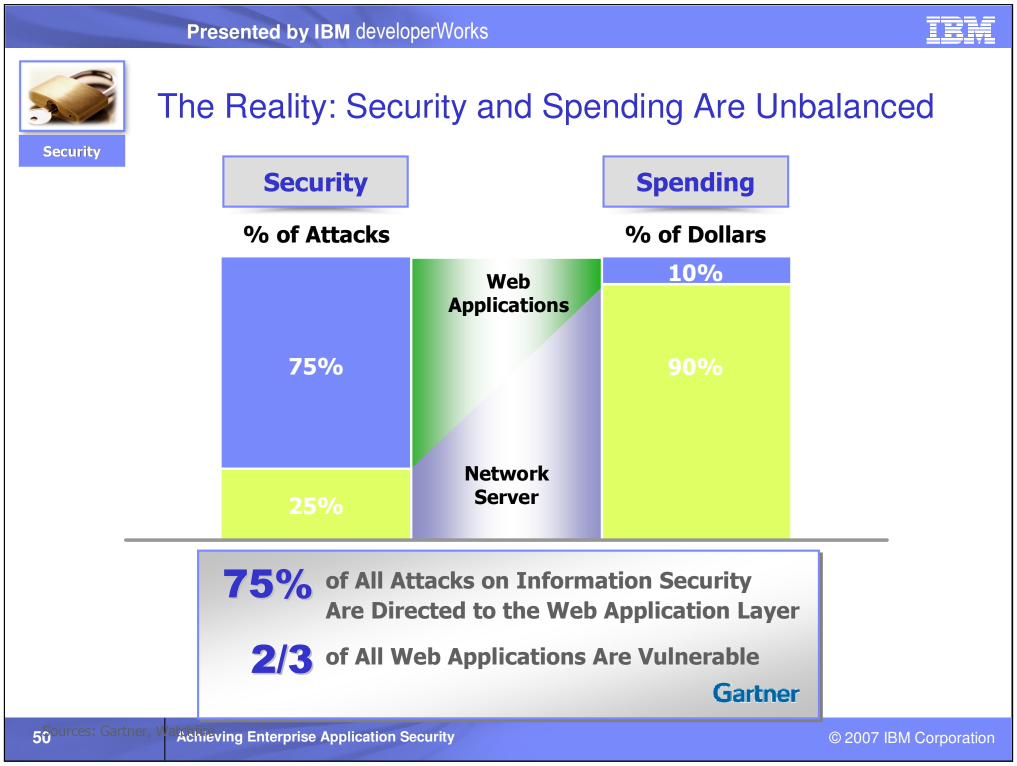
We Have Firewalls in Place

We Audit It Once a Quarter with Pen Testers

We Use Network Vulnerability Scanners

49 Achieving Enterprise Application Security © 2007 IBM Corporation

Every organization we visit, we hear the same things – we have firewalls, we audit once a quarter with penetration testers, we use network vulnerability scanners -- but when we show them the following slide, they have a different perspective.



Presented by IBM developerWorks

Security

The Reality: Security and Spending Are Unbalanced

75% of All Attacks on Information Security Are Directed to the Web Application Layer

2/3 of All Web Applications Are Vulnerable

Gartner

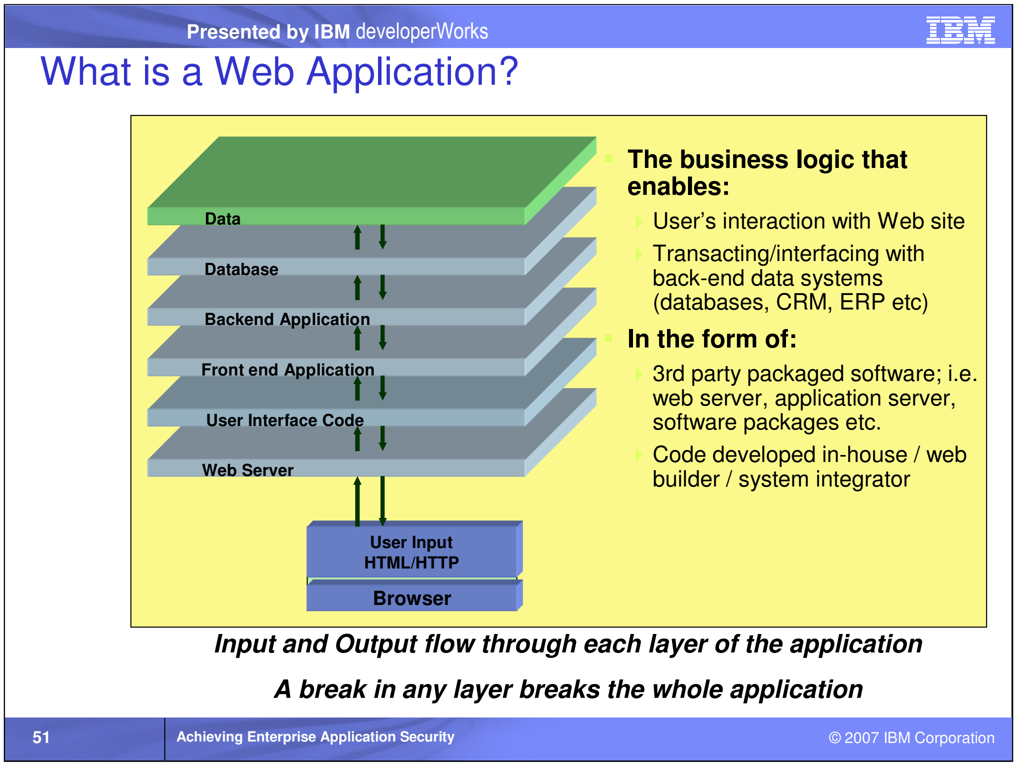
Sources: Gartner, Watchfire

50 Achieving Enterprise Application Security © 2007 IBM Corporation

We all know that enterprise web site security is critical; what's surprising is that the security risk and the associated level of spending to mitigate this risk are unbalanced.

75% of attacks occur through web applications, yet only 10% of the security spending dollars are in this area.

We've certainly seen our customer base become much more informed about the level of risk that web applications present, and adjust their spending accordingly



Presented by IBM developerWorks

What is a Web Application?

- **The business logic that enables:**
  - User's interaction with Web site
  - Transacting/interfacing with back-end data systems (databases, CRM, ERP etc)
- **In the form of:**
  - 3rd party packaged software; i.e. web server, application server, software packages etc.
  - Code developed in-house / web builder / system integrator

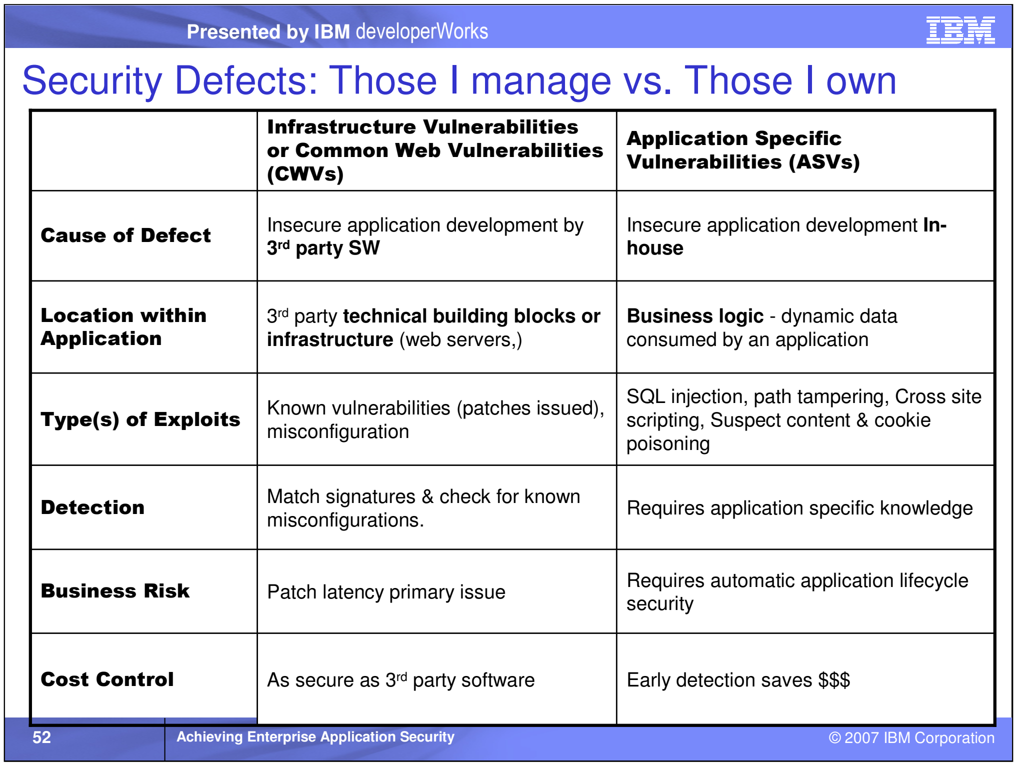
Input and Output flow through each layer of the application

A break in any layer breaks the whole application

51 Achieving Enterprise Application Security © 2007 IBM Corporation

If we look at the complexity of the web application, it is multi-layered and includes all the business logic that enables user's interaction with the web site and the transacting with the back-end data systems sitting behind the site. These applications come in the form of 3rd party packaged software and code developed in-house.

Even in a secure environment, so much has to go right for these layers to behave appropriately that it is amazing these sites work half the time!



Presented by **IBM** developerWorks

Security Defects: Those I manage vs. Those I own

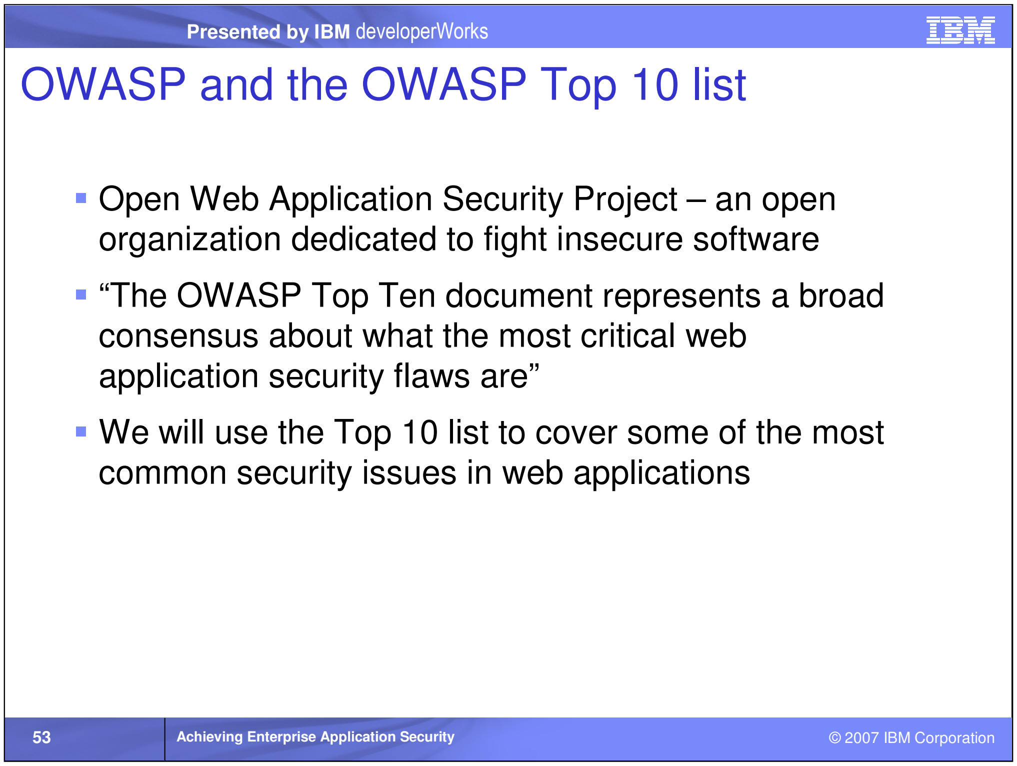
	Infrastructure Vulnerabilities or Common Web Vulnerabilities (CWVs)	**Application Specific Vulnerabilities (ASVs)**
Cause of Defect	Insecure application development by **3rd party SW**	Insecure application development **In-house**
Location within Application	3rd party **technical building blocks or infrastructure** (web servers,)	**Business logic** - dynamic data consumed by an application
Type(s) of Exploits	Known vulnerabilities (patches issued), misconfiguration	SQL injection, path tampering, Cross site scripting, Suspect content & cookie poisoning
Detection	Match signatures & check for known misconfigurations.	Requires application specific knowledge
Business Risk	Patch latency primary issue	Requires automatic application lifecycle security
Cost Control	As secure as 3rd party software	Early detection saves $$$

52 Achieving Enterprise Application Security © 2007 IBM Corporation

This chart details more of the differences between CWVs and ASVs and ultimately points out how an organization can most effectively reduce security defect costs.

Basically, an organization has very little control over the costs to find and fix CWVs and a lot of control over the costs to find and fix ASVs. CWVs are a result of 3rd party defects and as such can only be found once the application is in production. Because they are relatively easy to identify, and have patches issued for them that are publicly available their cost to the organization is relatively low in terms of finding and fixing. On the other hand, ASVs are defects introduced during the application development lifecycle, are very difficult to identify manually, and require the entire app lifecycle process for creating a fix, therefore, the ability to control the cost is relatively high.

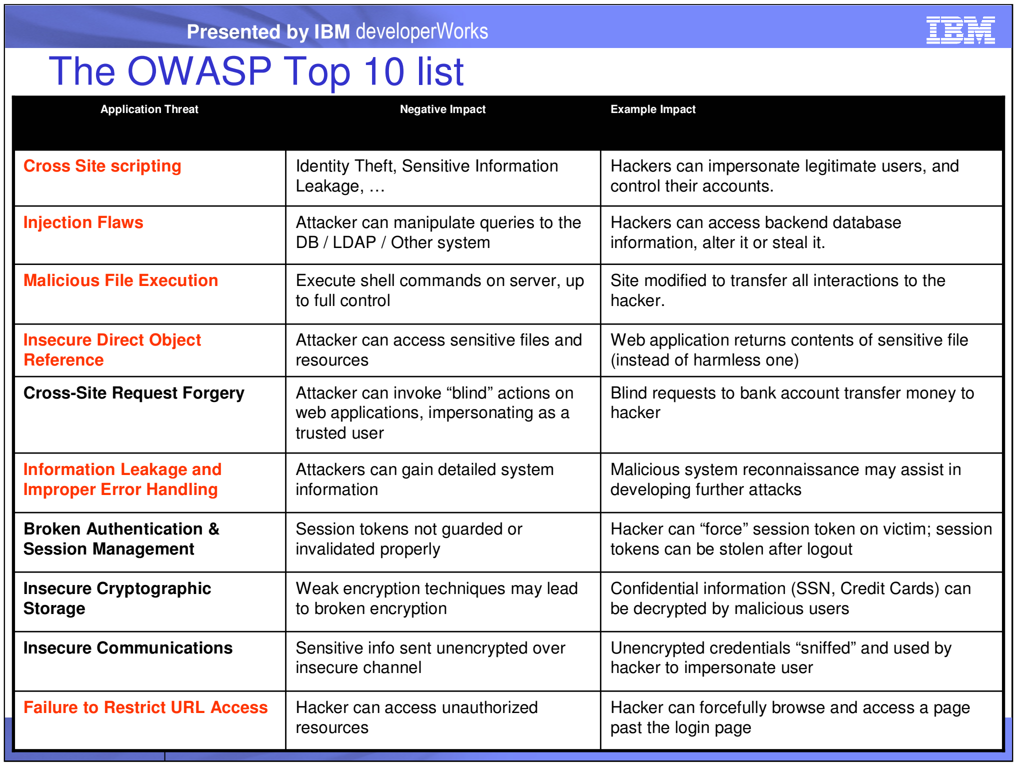
The cost to fix a vulnerability once it reaches deployments is 100 times greater than if it were caught and fixed in design. Because an ASV can be caught throughout the application lifecycle the organization has the ability to control this cost.



OWASP and the OWASP Top 10 list

- Open Web Application Security Project – an open organization dedicated to fight insecure software
- “The OWASP Top Ten document represents a broad consensus about what the most critical web application security flaws are”
- We will use the Top 10 list to cover some of the most common security issues in web applications

The Open Web Application Security Project (OWASP) is an open organization dedicated to fighting insecure software. The organization publishes a Top 10 list of the most critical web application security flaws.

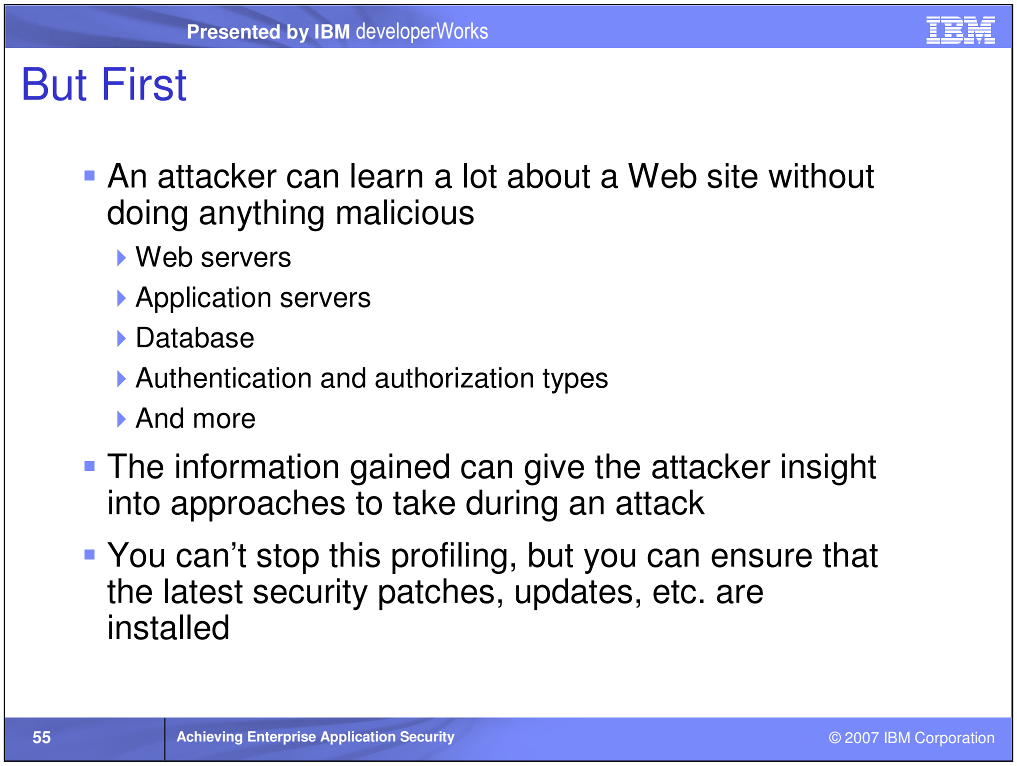


Presented by IBM developerWorks

The OWASP Top 10 list

Application Threat	Negative Impact	Example Impact
Cross Site scripting	Identity Theft, Sensitive Information Leakage, …	Hackers can impersonate legitimate users, and control their accounts.
Injection Flaws	Attacker can manipulate queries to the DB / LDAP / Other system	Hackers can access backend database information, alter it or steal it.
Malicious File Execution	Execute shell commands on server, up to full control	Site modified to transfer all interactions to the hacker.
Insecure Direct Object Reference	Attacker can access sensitive files and resources	Web application returns contents of sensitive file (instead of harmless one)
Cross-Site Request Forgery	Attacker can invoke “blind” actions on web applications, impersonating as a trusted user	Blind requests to bank account transfer money to hacker
Information Leakage and Improper Error Handling	Attackers can gain detailed system information	Malicious system reconnaissance may assist in developing further attacks
Broken Authentication & Session Management	Session tokens not guarded or invalidated properly	Hacker can “force” session token on victim; session tokens can be stolen after logout
Insecure Cryptographic Storage	Weak encryption techniques may lead to broken encryption	Confidential information (SSN, Credit Cards) can be decrypted by malicious users
Insecure Communications	Sensitive info sent unencrypted over insecure channel	Unencrypted credentials “sniffed” and used by hacker to impersonate user
Failure to Restrict URL Access	Hacker can access unauthorized resources	Hacker can forcefully browse and access a page past the login page

We will discuss the threats in red.



Presented by IBM developerWorks

But First

- An attacker can learn a lot about a Web site without doing anything malicious
  - Web servers
  - Application servers
  - Database
  - Authentication and authorization types
  - And more
- The information gained can give the attacker insight into approaches to take during an attack
- You can't stop this profiling, but you can ensure that the latest security patches, updates, etc. are installed

55 Achieving Enterprise Application Security © 2007 IBM Corporation

An attacker can learn a lot about a Web site without doing anything malicious, such as the Web servers used, the application servers used, the database used, authentication and authorization types, and much more.

The information gained can give the attacker insight into approaches to take during an attack.

You can't stop this profiling, but you can ensure that the latest security patches, updates, etc. are installed.

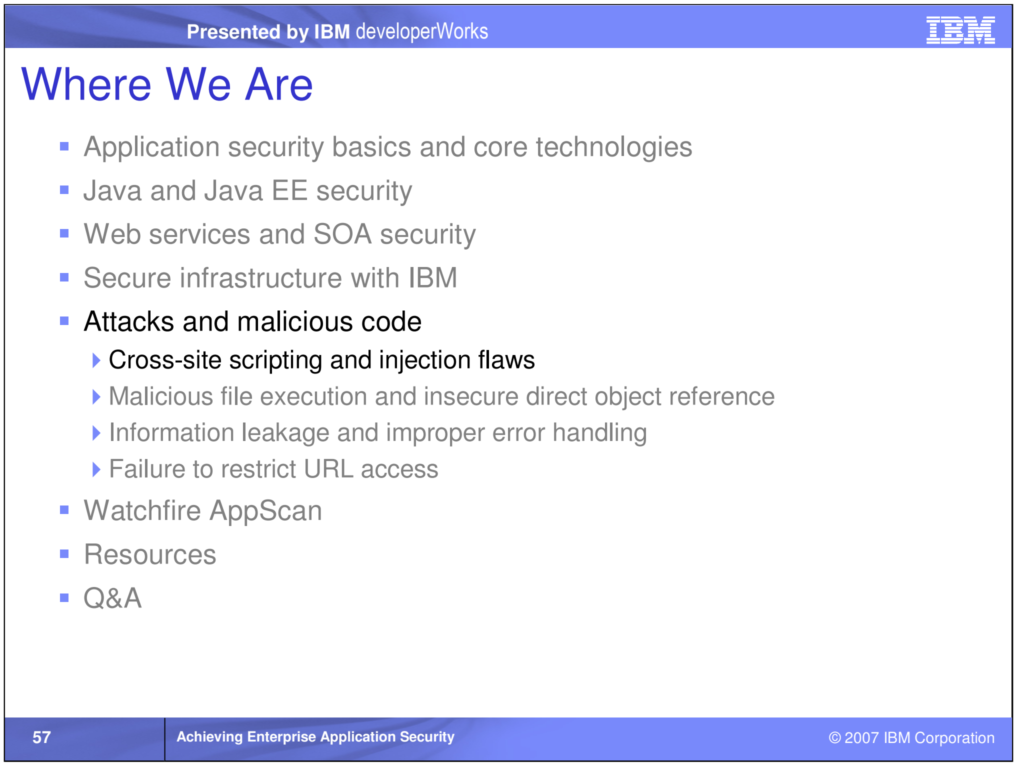
Presented by IBM developerWorks

DEMO

Profile Web Application

56 Achieving Enterprise Application Security © 2007 IBM Corporation

This demo shows some of the information that an attacker can get from profiling a Web application.



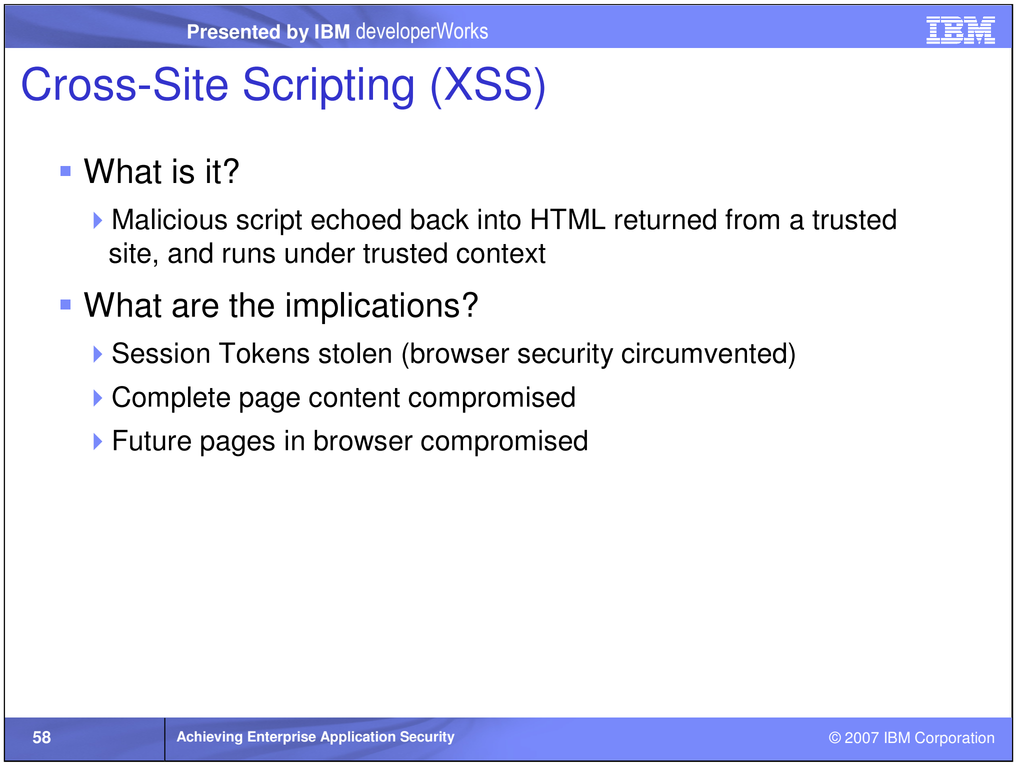
Presented by IBM developerWorks

Where We Are

- Application security basics and core technologies
- Java and Java EE security
- Web services and SOA security
- Secure infrastructure with IBM
- Attacks and malicious code
  - Cross-site scripting and injection flaws
  - Malicious file execution and insecure direct object reference
  - Information leakage and improper error handling
  - Failure to restrict URL access
- Watchfire AppScan
- Resources
- Q&A

57 Achieving Enterprise Application Security © 2007 IBM Corporation

Cross-site scripting and injection flaws are major vulnerabilities in Web applications.



Presented by IBM developerWorks

Cross-Site Scripting (XSS)

- What is it?
  - Malicious script echoed back into HTML returned from a trusted site, and runs under trusted context
- What are the implications?
  - Session Tokens stolen (browser security circumvented)
  - Complete page content compromised
  - Future pages in browser compromised

58 Achieving Enterprise Application Security © 2007 IBM Corporation

A Cross Site Scripting attack, attempts to echo back a malicious script in the HTML returned from a trusted site. Since the script is echoed back from a trusted site, it runs in the context of that site.

The implications of XSS are:

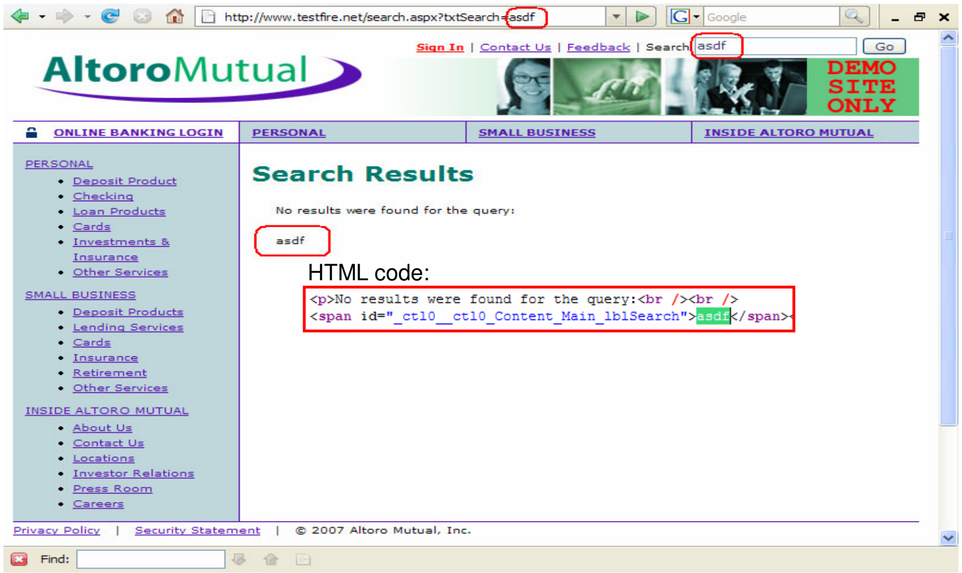
Stealing HTTP session tokens

Page content may be compromised (this may include “local” site defacement, or hijacking of the browser’s session using scripting)

Future pages may be contaminated as well (by hijacking the session)

Presented by IBM developerWorks

XSS Example …



Search Results

No results were found for the query:

asdf

HTML code:

```
<p>No results were found for the query:<br /><br />
<span id="_ctl0__ctl0_Content_Main_lblSearch">asdf</span><
```

Let’s take a look at the following banking web site – this site contains a search function, that allows users to search the site for specific text. If we type the string “asdf”, the response to the search will contain that string, inside the results page, in what we call “free HTML context”.

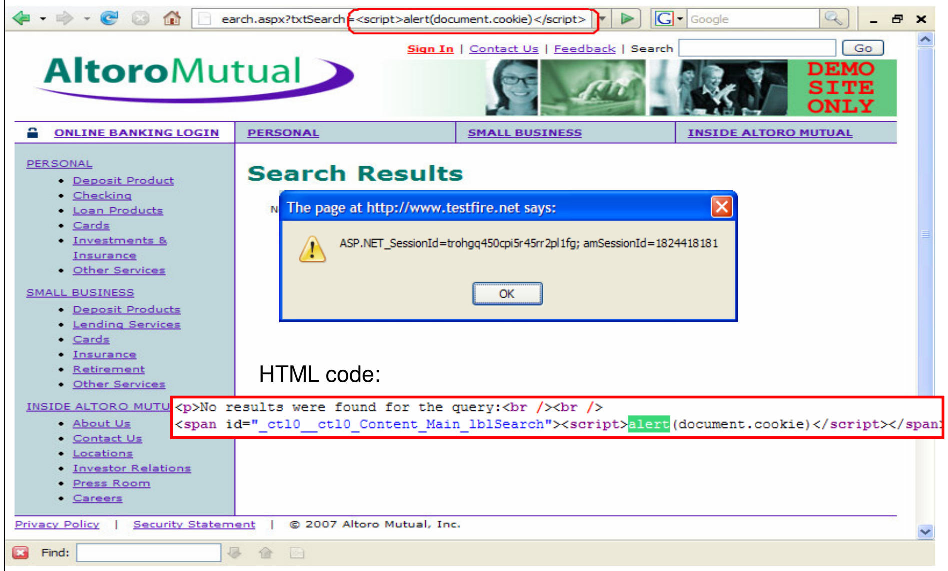
What will happen if instead of typing “asdf”, we will type some JavaScript code?

Let’s try to type the following JavaScript code:

<script>alert(document.cookie)</script>

Presented by IBM developerWorks

XSS Example



```
earch.aspx?txtSearch=<script>alert(document.cookie)</script>
```

The page at http://www.testfire.net says:

ASP.NET_SessionId=trohgq450cpi5r45rr2pl1fg; amSessionId=1824418181

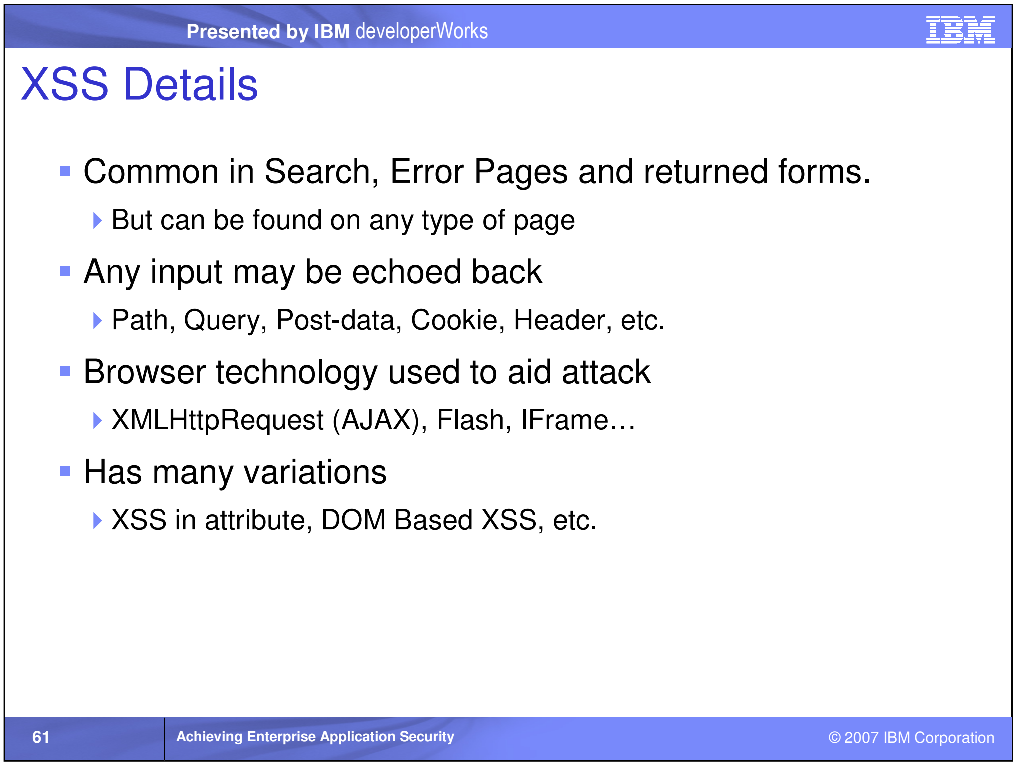
HTML code:

```
<p>No results were found for the query:<br /><br />
<span id="_ctl0__ctl0_Content_Main_lblSearch"><script>alert(document.cookie)</script></span
```

60 Achieving Enterprise Application Security © 2007 IBM Corporation

As you can see – the piece of JavaScript code that we wrote, was echoed back by the site’s search function – since it was returned from the banking application, it had access to the Document Object Model (DOM), and could access the current session cookie.

In this situation, I myself planted this JavaScript code in the web page, but in a XSS attack, it is the attacker who creates a link that contains the malicious JavaScript, and then sends this link to the victim. When the victim clicks on the link, the malicious JavaScript will be echoed back from the trusted site.



Presented by IBM developerWorks

XSS Details

- Common in Search, Error Pages and returned forms.
  - But can be found on any type of page
- Any input may be echoed back
  - Path, Query, Post-data, Cookie, Header, etc.
- Browser technology used to aid attack
  - XMLHttpRequest (AJAX), Flash, IFrame…
- Has many variations
  - XSS in attribute, DOM Based XSS, etc.

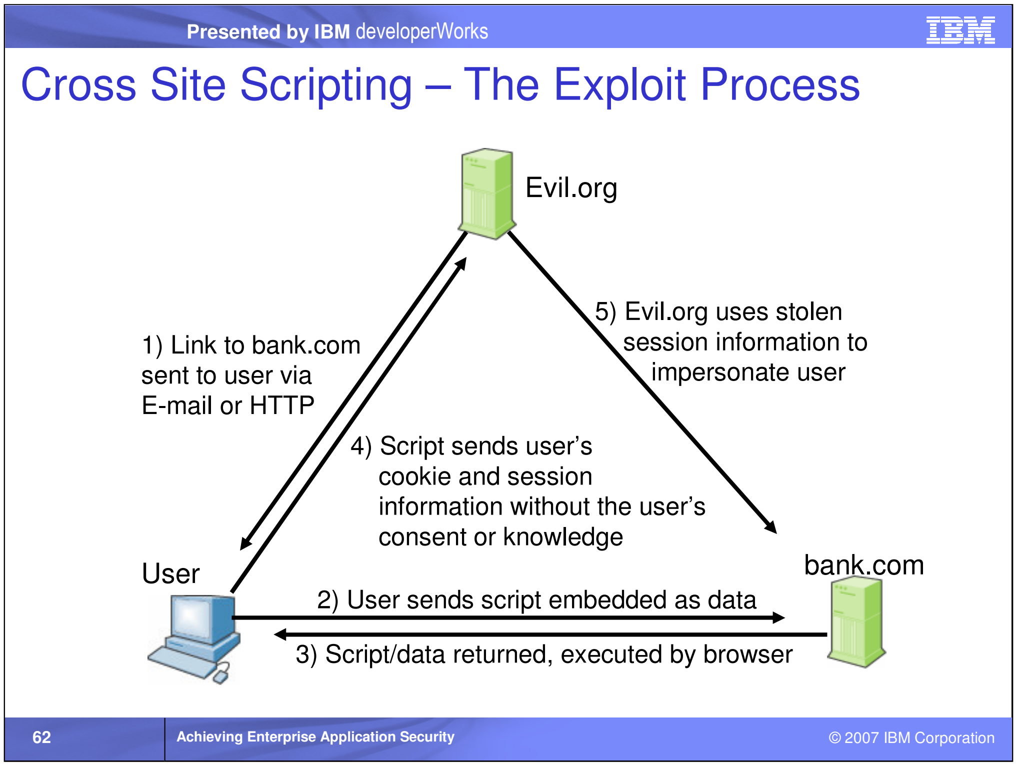
61 Achieving Enterprise Application Security © 2007 IBM Corporation

XSS usually occurs in pages that echo back user input, for example – search pages, error pages and forms that are returned in subsequent pages.

Echoed input can come from any part of the HTTP message that is used by the application, for example: parts of the path, query, cookie or other headers.

Some browser technologies can help with mounting the XSS attack, for example XMLHttpRequest (used in AJAX), flash objects or IFrames.

There are several different flavors and variations of XSS, for example – XSS in HTML attributes, DOM Based XSS, etc.



Presented by IBM developerWorks

Cross Site Scripting – The Exploit Process

Evil.org

1) Link to bank.com sent to user via E-mail or HTTP

2) User sends script embedded as data

3) Script/data returned, executed by browser

4) Script sends user's cookie and session information without the user's consent or knowledge

5) Evil.org uses stolen session information to impersonate user

User

bank.com

62 Achieving Enterprise Application Security © 2007 IBM Corporation

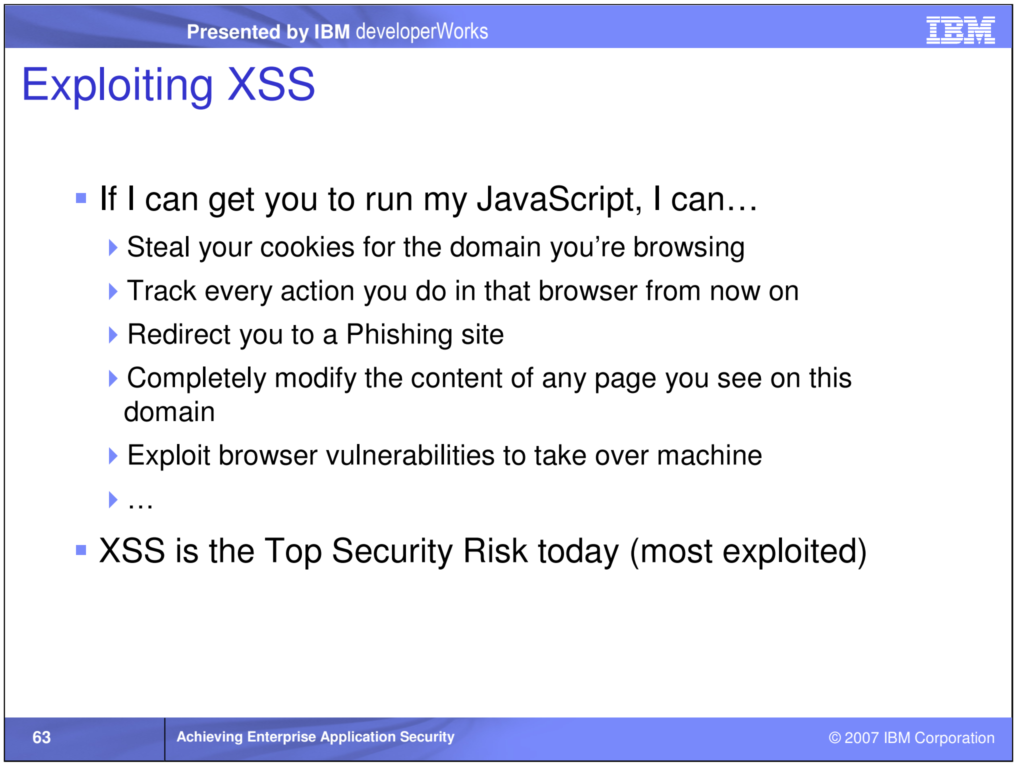
Let's take a look at the chain of events during a XSS attack.

The attack creates and sends the victim a link to bank.com (a trusted site). The link contains a search string (or any other string that is echoed back), which contains a malicious JavaScript code.

The victim, clicks on this link, since he/she trusts the bank.com web site.

The bank.com web application, echoes back the malicious JavaScript code inside the response page. This JavaScript is executed in the security context of bank.com, since it is echoed by from that site. This means that it has access to DOM elements belonging to this domain/session.

The malicious script sends the current cookie and session information, without the victim's consent, to the evil.org web site, where the hacker is waiting for it.



Presented by IBM developerWorks

Exploiting XSS

- If I can get you to run my JavaScript, I can…
  - Steal your cookies for the domain you're browsing
  - Track every action you do in that browser from now on
  - Redirect you to a Phishing site
  - Completely modify the content of any page you see on this domain
  - Exploit browser vulnerabilities to take over machine
  - …
- XSS is the Top Security Risk today (most exploited)

63 Achieving Enterprise Application Security © 2007 IBM Corporation

If a hacker can get you to run a JavaScript, he/she can:

- Steal your cookies for the domain you're browsing

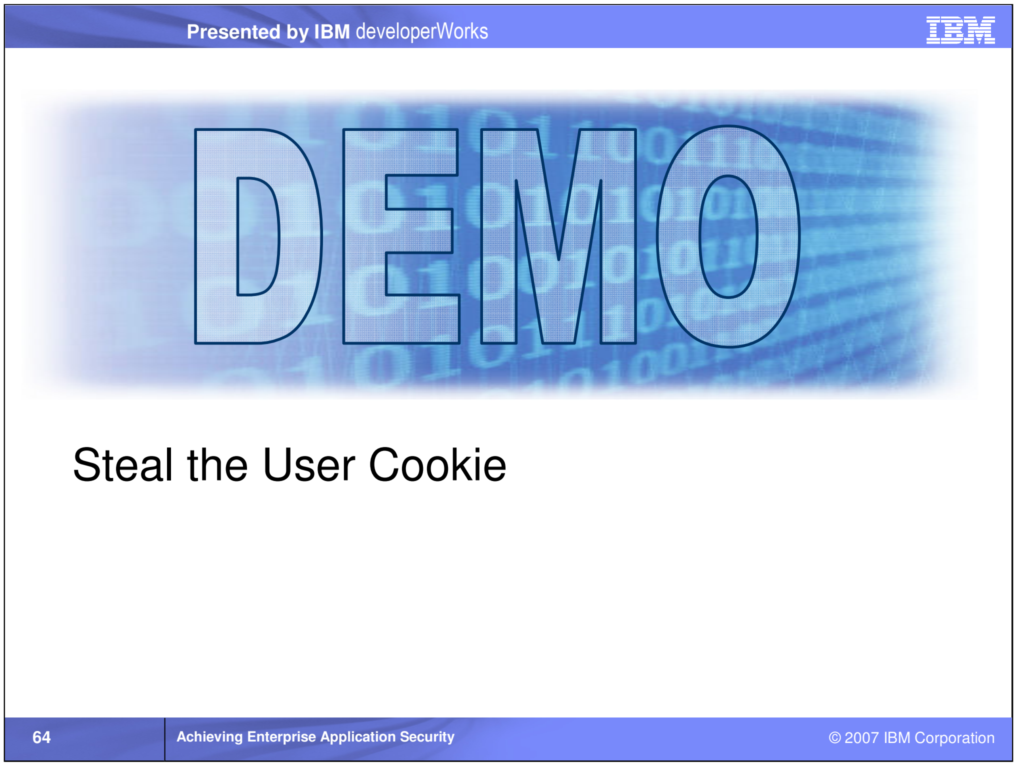
- Completely modify the content of any page you see on this domain

- Track every action you do in that browser from now on

- Redirect you to a Phishing site

- Exploit browser vulnerabilities to take over machine

XSS is currently one of the "hottest" security risks



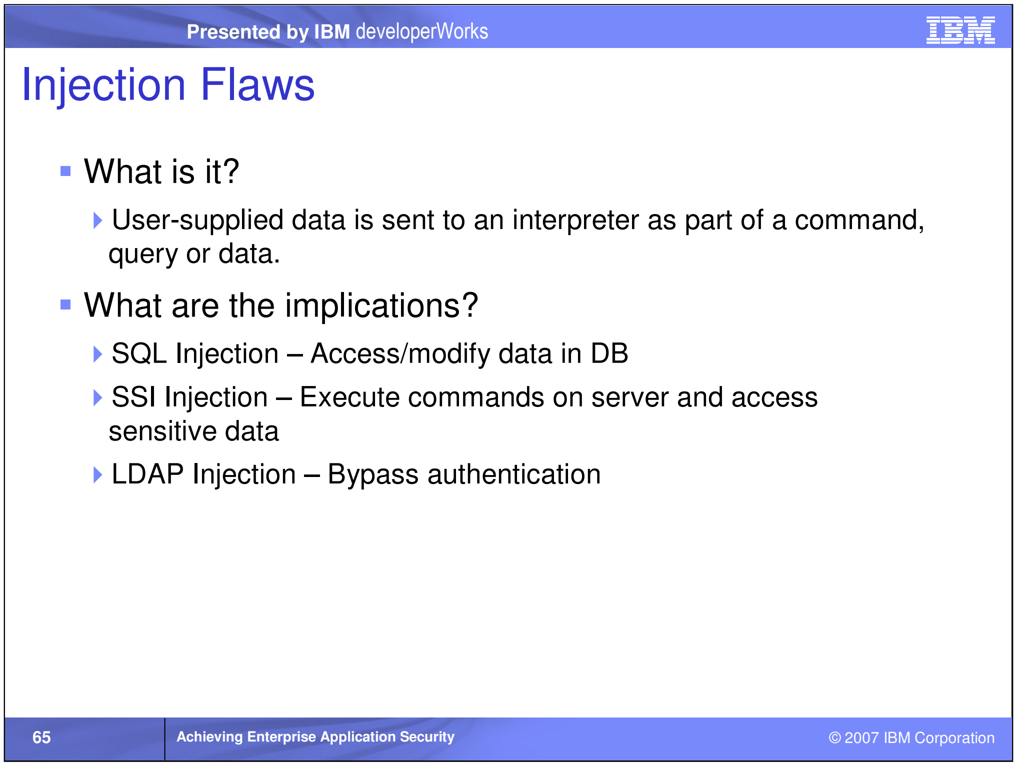
Presented by IBM developerWorks

DEMO

Steal the User Cookie

64 Achieving Enterprise Application Security © 2007 IBM Corporation

This demo shows a vulnerability that could be exploited through cross-site scripting.



Presented by IBM developerWorks

Injection Flaws

- What is it?
  - User-supplied data is sent to an interpreter as part of a command, query or data.
- What are the implications?
  - SQL Injection – Access/modify data in DB
  - SSI Injection – Execute commands on server and access sensitive data
  - LDAP Injection – Bypass authentication

65 Achieving Enterprise Application Security © 2007 IBM Corporation

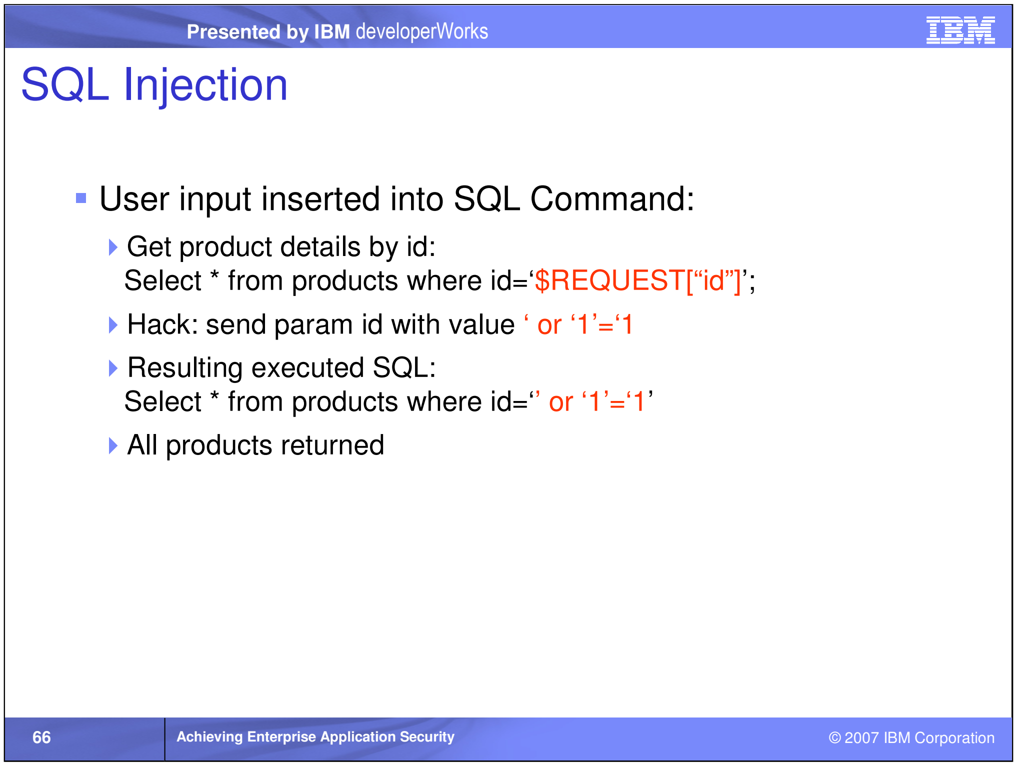
Injection flaws occur when user supplied data, is sent to an interpreter as a part of a command, query or data. The main issue here is that user input is not sanitized, and is embedded in pre-existing commands.

Injection flaws can occur in:

SQL queries (known as SQL Injection)

Server Side Includes (execute commands on the web server)

LDAP queries – used to bypass authentication



Presented by IBM developerWorks

SQL Injection

- User input inserted into SQL Command:
  - Get product details by id:
    Select * from products where id=‘$REQUEST[“id”]’;
  - Hack: send param id with value ‘ or ‘1’=‘1
  - Resulting executed SQL:
    Select * from products where id=‘’ or ‘1’=‘1’
  - All products returned

66 Achieving Enterprise Application Security © 2007 IBM Corporation

SQL Injection occurs when user input is embedded as-is inside a pre-built SQL query. For example:

Let’s assume that our web application receives a product ID as input, and presents that product’s page. The SQL query looks like this:

“Select * from products where id=‘” + $REQUEST[‘id’];

You should note, that the query is basically a text string, and user input is concatenated to it. In this example, the user string is surrounded by apostrophes. Let’s take a look at what will happen if we submit the product ID value of ‘ or ‘’=‘

The query will be:

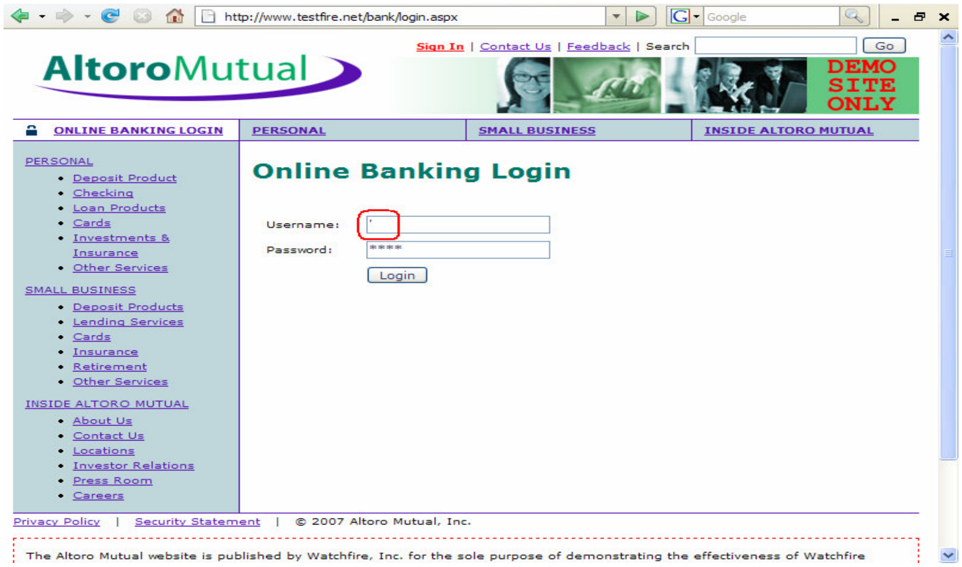
SELECT * from products where id=‘’ or ‘’=‘’;

You should pay attention to the fact that the WHERE criteria here is basically a Boolean TRUE.

Since the results of this query matches every entry in the database, all the products will be returned.

Presented by IBM developerWorks

SQL Injection Example …



Online Banking Login

Username: '

Password: ****

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire

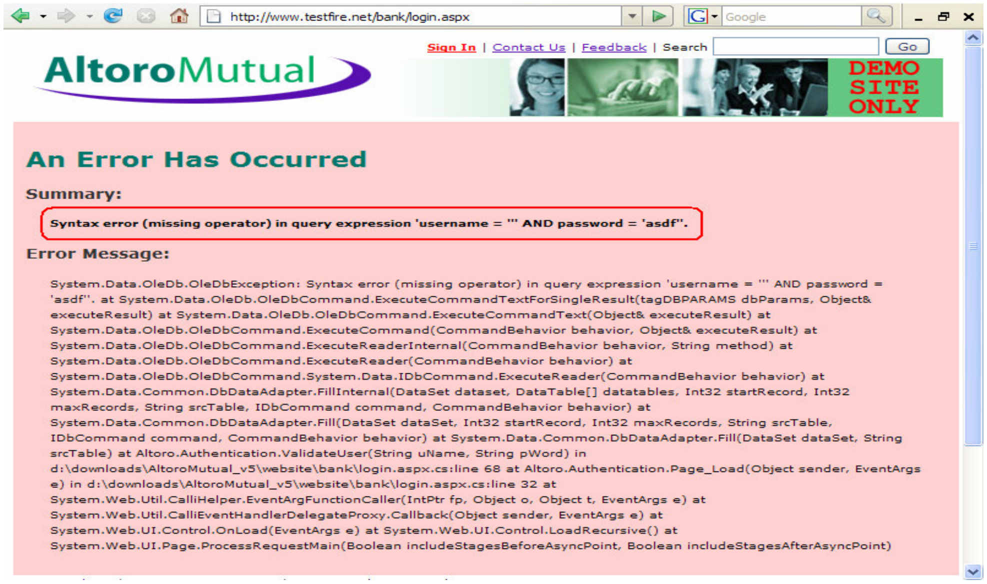
67 | Achieving Enterprise Application Security | © 2007 IBM Corporation

Let’s take a look at how SQL Injection can assist a hacker to bypass the login mechanism of a banking application:

First, in order to sense that SQL Injection is possible, the hacker will injection the character apostrophe (‘), as the user name

Presented by IBM developerWorks

SQL Injection Example



http://www.testfire.net/bank/login.aspx
Google
Sign In | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY

An Error Has Occurred

Summary:

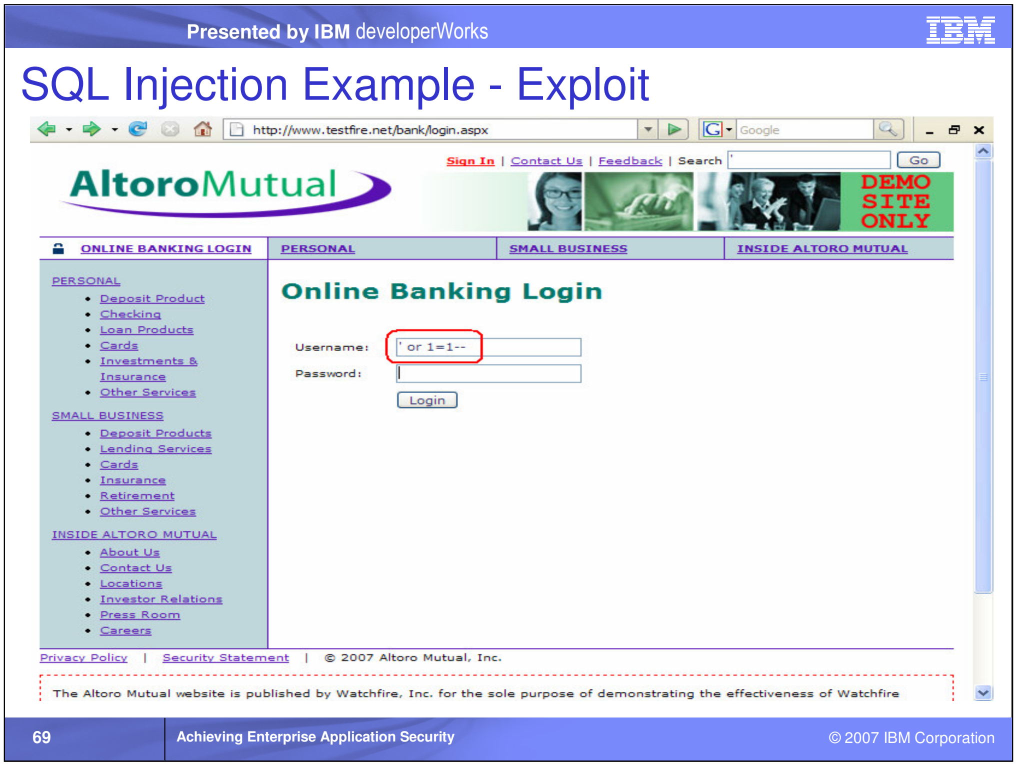
```
Syntax error (missing operator) in query expression 'username = ''' AND password = 'asdf''.
```

Error Message:

```
System.Data.OleDb.OleDbException: Syntax error (missing operator) in query expression 'username = ''' AND password =
'asdf''. at System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSingleResult(tagDBPARAMS dbParams, Object&
executeResult) at System.Data.OleDb.OleDbCommand.ExecuteCommandText(Object& executeResult) at
System.Data.OleDb.OleDbCommand.ExecuteCommand(CommandBehavior behavior, Object& executeResult) at
System.Data.OleDb.OleDbCommand.ExecuteReaderInternal(CommandBehavior behavior, String method) at
System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior) at
System.Data.OleDb.OleDbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior) at
System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32
maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) at
System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable,
IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String
srcTable) at Altoro.Authentication.ValidateUser(String uName, String pWord) in
d:\downloads\AltoroMutual_v5\website\bank\login.aspx.cs:line 68 at Altoro.Authentication.Page_Load(Object sender, EventArgs
e) in d:\downloads\AltoroMutual_v5\website\bank\login.aspx.cs:line 32 at
System.Web.Util.CalliHelper.EventArgFunctionCaller(IntPtr fp, Object o, Object t, EventArgs e) at
System.Web.Util.CalliEventHandlerDelegateProxy.Callback(Object sender, EventArgs e) at
System.Web.UI.Control.OnLoad(EventArgs e) at System.Web.UI.Control.LoadRecursive() at
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint)
```

68 Achieving Enterprise Application Security © 2007 IBM Corporation

This yields a very informative SQL error message, which helps the attacker to devise the next phase of the injection



Presented by IBM developerWorks

SQL Injection Example - Exploit

Online Banking Login

Username: ' or 1=1--

Password:

69 Achieving Enterprise Application Security © 2007 IBM Corporation

Now, the hacker attempts to send the username: ‘ or 1=1—

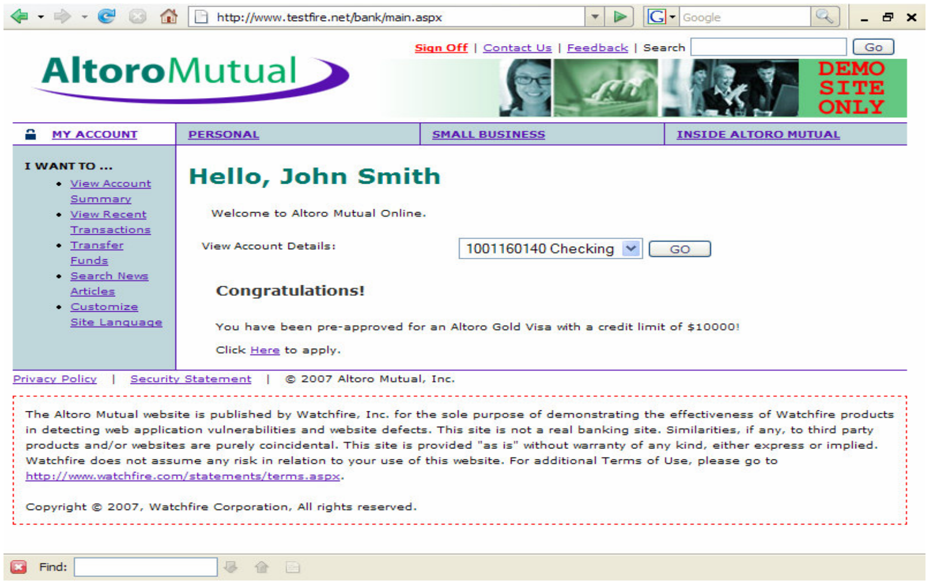
Note: the apostrophe is used to close the string context in which our input is embedded in.

1=1 is a Boolean TRUE

-- is used in MS SQL to comment out everything after the – sign, so we don’t have to worry about the rest of the SQL query

Presented by IBM developerWorks

SQL Injection Example - Outcome



I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

Hello, John Smith

Welcome to Altoro Mutual Online.

View Account Details: 1001160140 Checking GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

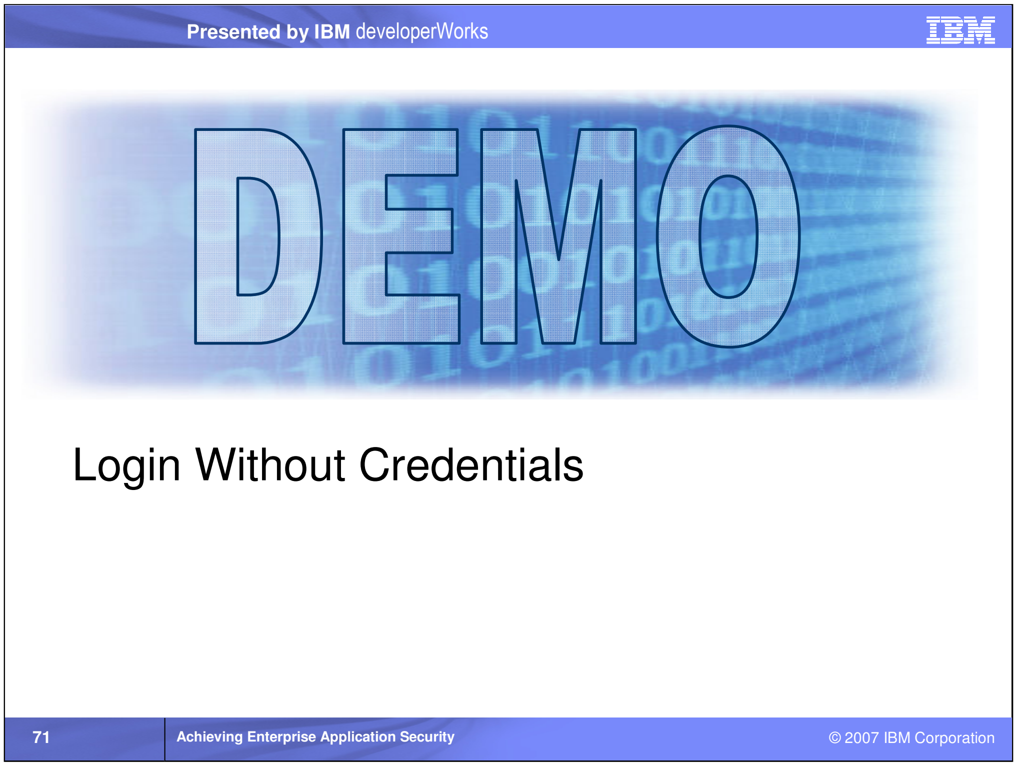
Privacy Policy | Security Statement | © 2007 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to http://www.watchfire.com/statements/terms.aspx.

Copyright © 2007, Watchfire Corporation, All rights reserved.

70 Achieving Enterprise Application Security © 2007 IBM Corporation

After sending this SQL injection payload, we will be logged into the application, as the first user in the user's table - without having to supply actual credentials.

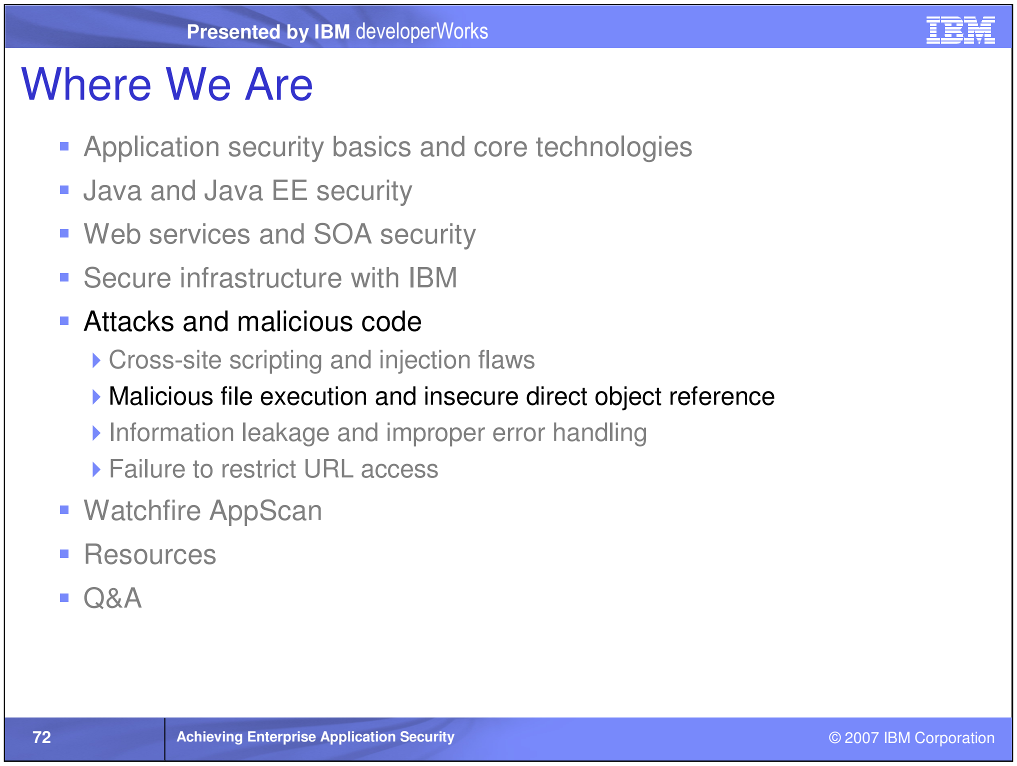


Presented by IBM developerWorks

Login Without Credentials

71 Achieving Enterprise Application Security © 2007 IBM Corporation

This demo shows how SQL injection can be used to login to a site without a proper username and password..



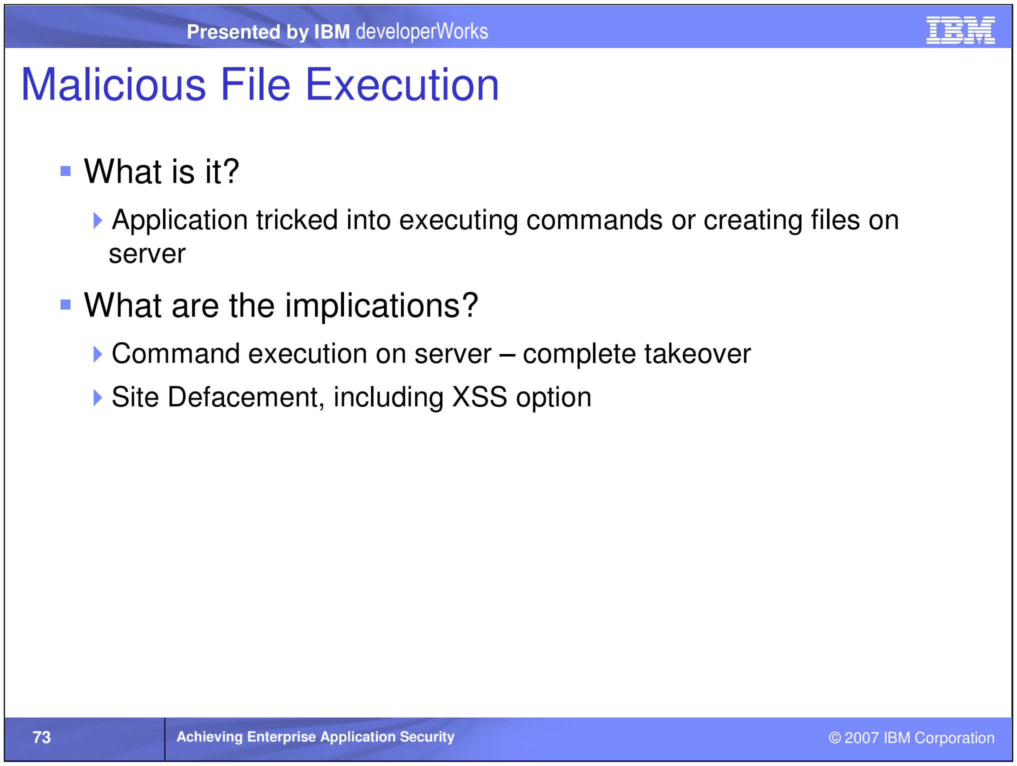
Presented by IBM developerWorks

Where We Are

- Application security basics and core technologies
- Java and Java EE security
- Web services and SOA security
- Secure infrastructure with IBM
- Attacks and malicious code
  - Cross-site scripting and injection flaws
  - Malicious file execution and insecure direct object reference
  - Information leakage and improper error handling
  - Failure to restrict URL access
- Watchfire AppScan
- Resources
- Q&A

72 Achieving Enterprise Application Security © 2007 IBM Corporation

Next we’ll discuss malicious file execution and insecure direct object reference.



Presented by IBM developerWorks

Malicious File Execution

- What is it?
  - Application tricked into executing commands or creating files on server
- What are the implications?
  - Command execution on server – complete takeover
  - Site Defacement, including XSS option

73 Achieving Enterprise Application Security © 2007 IBM Corporation

In Malicious File Execution, the hacker attempts to trick the application into executing commands or creating files on the server.

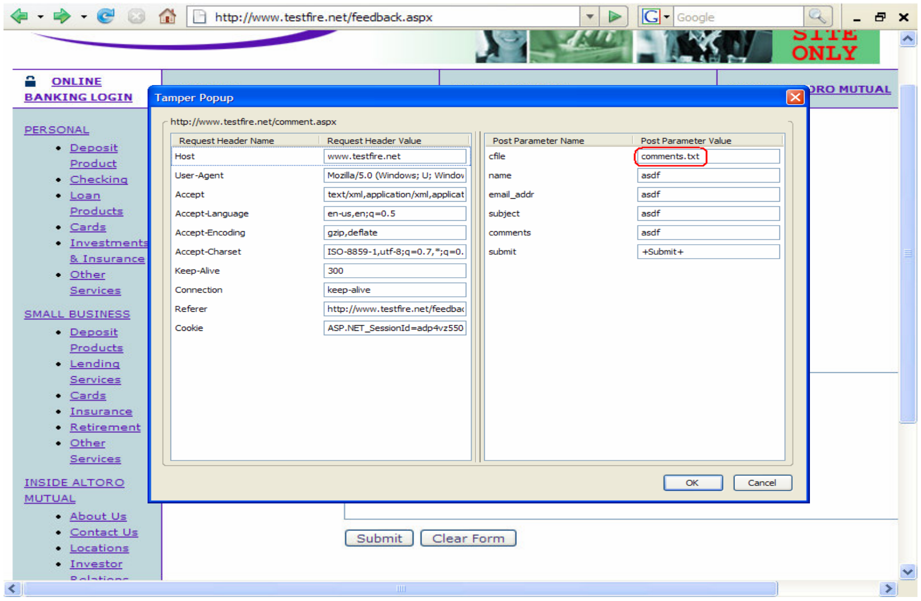
The implications of this attack are:

- The hacker can execute remote commands on the server, which means a complete takeover

- The hacker may deface the web site.

Presented by IBM developerWorks

Malicious File Execution Example …



http://www.testfire.net/comment.aspx

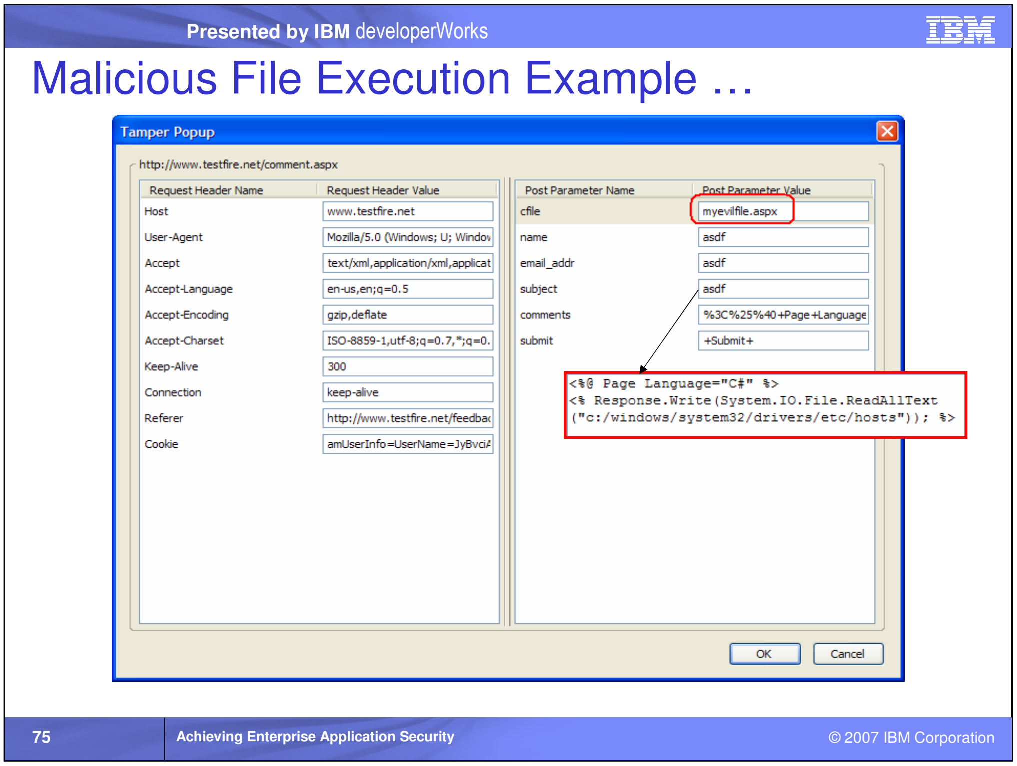
Request Header Name	Request Header Value
Host	www.testfire.net
User-Agent	Mozilla/5.0 (Windows; U; Windov
Accept	text/xml,application/xml,applicat
Accept-Language	en-us,en;q=0.5
Accept-Encoding	gzip,deflate
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.
Keep-Alive	300
Connection	keep-alive
Referer	http://www.testfire.net/feedbac
Cookie	ASP.NET_SessionId=adp4vz550

Post Parameter Name	Post Parameter Value
cfile	comments.txt
name	asdf
email_addr	asdf
subject	asdf
comments	asdf
submit	+Submit+

74 Achieving Enterprise Application Security © 2007 IBM Corporation

Let’s take a look at our banking application again –

The application contains a feedback form, which allows users to send the application owner all sorts of feedback. This feedback is submitted and appended to a file on the operating system. Since the application was designed poorly, the location of the feedback is taken from a “hidden” form parameter called “cfile”. All a hacker has to do in order to “create” a new file on the operating system, is manipulate the value of the “cfile” parameter to a different filename, and submit contents to that file (submitted as feedback).



Malicious File Execution Example …

http://www.testfire.net/comment.aspx

Request Header Name	Request Header Value
Host	www.testfire.net
User-Agent	Mozilla/5.0 (Windows; U; Windov
Accept	text/xml,application/xml,applicat
Accept-Language	en-us,en;q=0.5
Accept-Encoding	gzip,deflate
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.
Keep-Alive	300
Connection	keep-alive
Referer	http://www.testfire.net/feedbac
Cookie	amUserInfo=UserName=JyBvciA

Post Parameter Name	Post Parameter Value
cfile	myevilfile.aspx
name	asdf
email_addr	asdf
subject	asdf
comments	%3C%25%40+Page+Language
submit	+Submit+

```
<%@ Page Language="C#" %>
<% Response.Write(System.IO.File.ReadAllText
("c:/windows/system32/drivers/etc/hosts")); %>
```

75 Achieving Enterprise Application Security © 2007 IBM Corporation

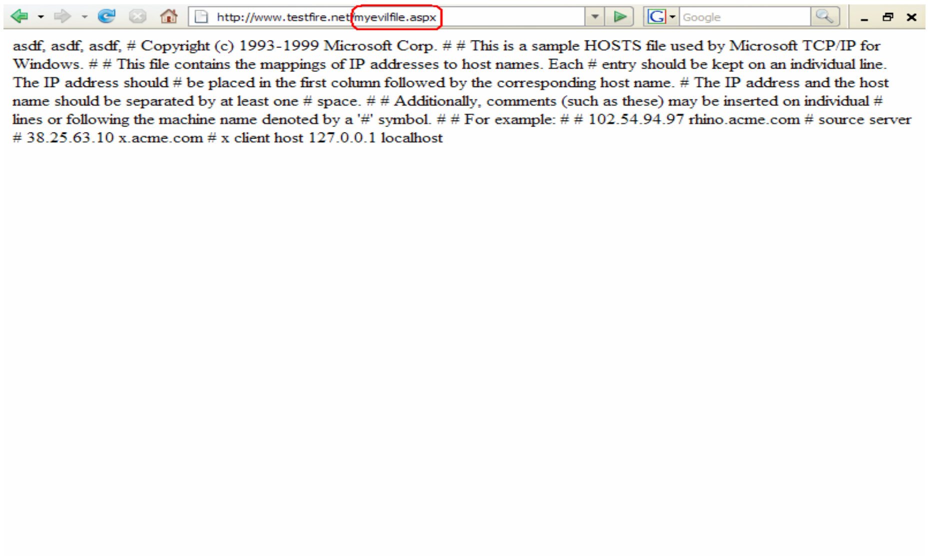
Let’s perform the attack –

We change the value of the cfile parameter to myevilfile.aspx (we are creating an ASPX file, which is a server-side Microsoft ASP.NET script)

Instead of a feedback, we’ll fill this file with some C# code, that will reveal the contents of the system’s hosts file

Presented by IBM developerWorks

Malicious File Execution Example

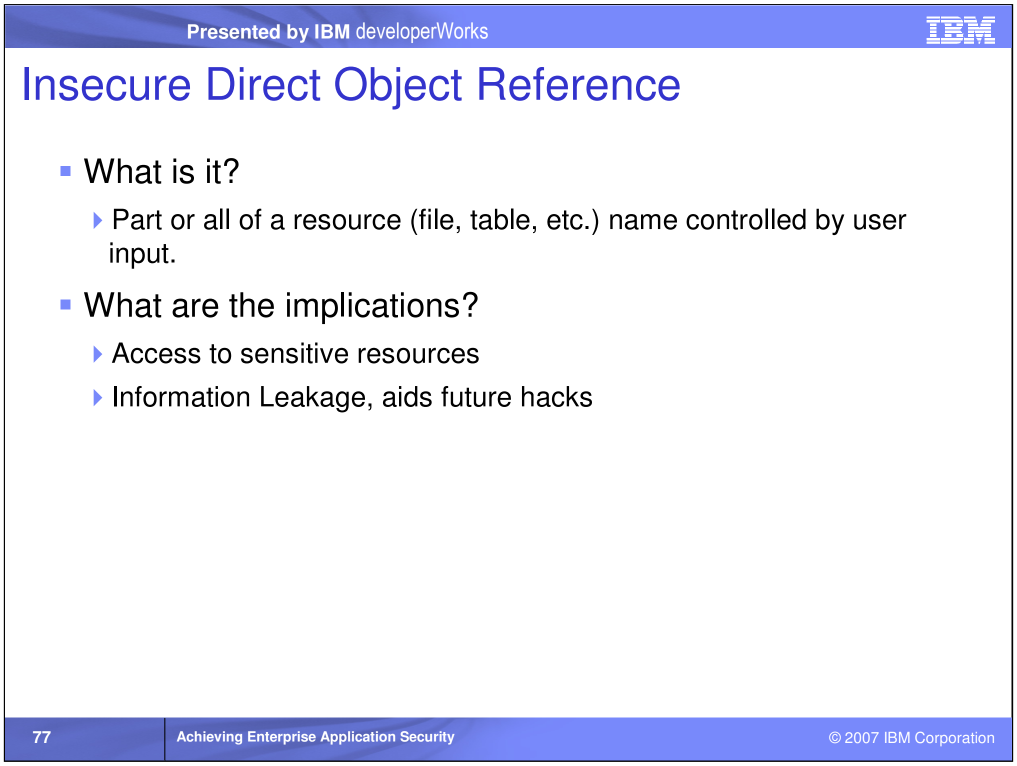


asdf, asdf, asdf, # Copyright (c) 1993-1999 Microsoft Corp. # # This is a sample HOSTS file used by Microsoft TCP/IP for Windows. # # This file contains the mappings of IP addresses to host names. Each # entry should be kept on an individual line. The IP address should # be placed in the first column followed by the corresponding host name. # The IP address and the host name should be separated by at least one # space. # # Additionally, comments (such as these) may be inserted on individual # lines or following the machine name denoted by a '#' symbol. # # For example: # # 102.54.94.97 rhino.acme.com # source server # 38.25.63.10 x.acme.com # x client host 127.0.0.1 localhost

76 Achieving Enterprise Application Security © 2007 IBM Corporation

When requesting the server-side script we just created, the application will execute it for us, revealing the contents of the hosts file.

Game Over!



Presented by IBM developerWorks

Insecure Direct Object Reference

- What is it?
  - Part or all of a resource (file, table, etc.) name controlled by user input.
- What are the implications?
  - Access to sensitive resources
  - Information Leakage, aids future hacks

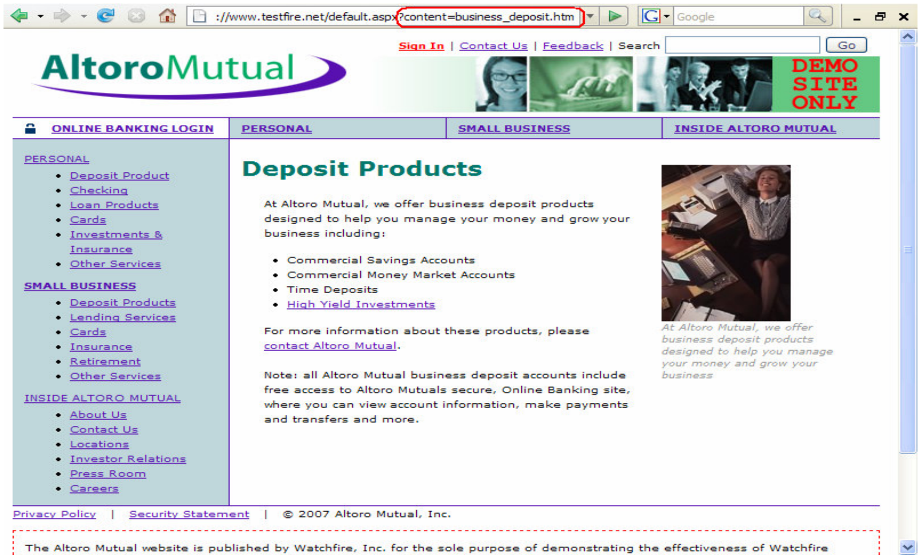
77 Achieving Enterprise Application Security © 2007 IBM Corporation

In several scenarios, it may be possible for an attacker to manipulate the web application to disclose a resource such as a sensitive file. This can occur by either guessing a common file name and location and attempting to request it, or by manipulating a parameter value that is used to access a file, as will be seen in the next example.

The implications of Insecure Direct Object Reference is usually information leakage or access to sensitive resources.

Presented by IBM developerWorks

Insecure Direct Object Reference – Example …



://www.testfire.net/default.aspx?content=business_deposit.htm

Deposit Products

At Altoro Mutual, we offer business deposit products designed to help you manage your money and grow your business including:

- Commercial Savings Accounts
- Commercial Money Market Accounts
- Time Deposits
- High Yield Investments

For more information about these products, please contact Altoro Mutual.

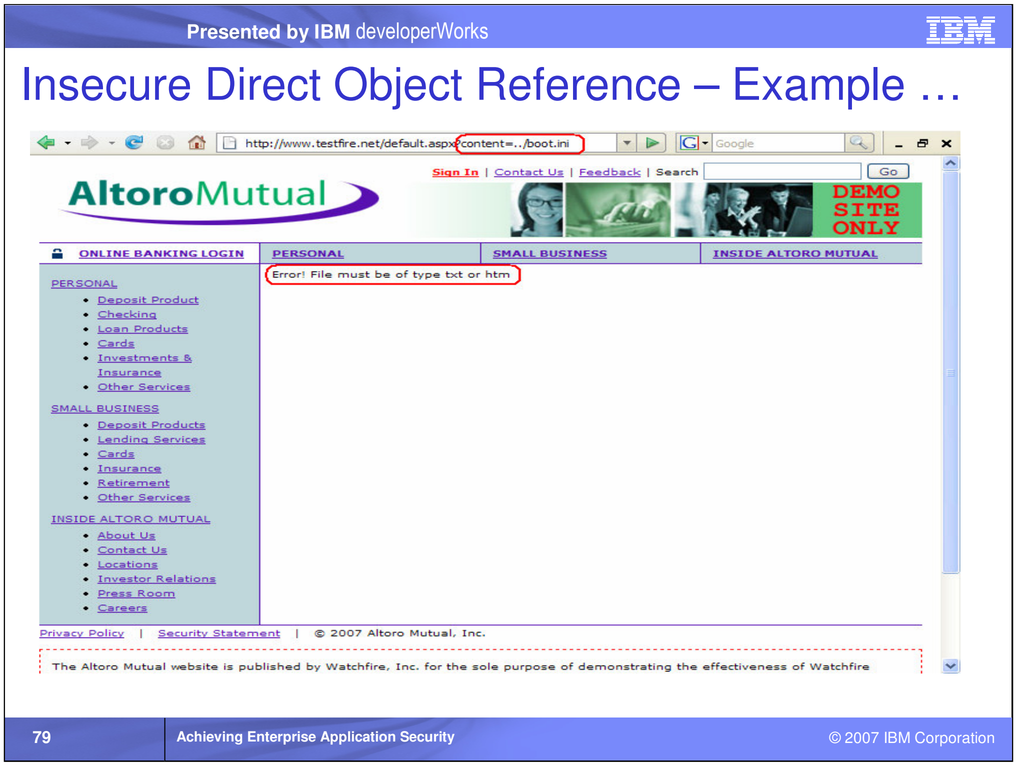
Note: all Altoro Mutual business deposit accounts include free access to Altoro Mutuals secure, Online Banking site, where you can view account information, make payments and transfers and more.

At Altoro Mutual, we offer business deposit products designed to help you manage your money and grow your business

Privacy Policy | Security Statement | © 2007 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire

In this example, we see that a web application that uses a parameter called “content”, which points to the contents of the page to be displayed. An attacker might attempt to manipulate the parameter value, from “business_deposit.htm”, which is the valid page, to some other file – for example, the Boot.ini which is a system file.



Presented by IBM developerWorks

Insecure Direct Object Reference – Example …

http://www.testfire.net/default.aspx?content=../boot.ini

Error! File must be of type txt or htm

© 2007 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire

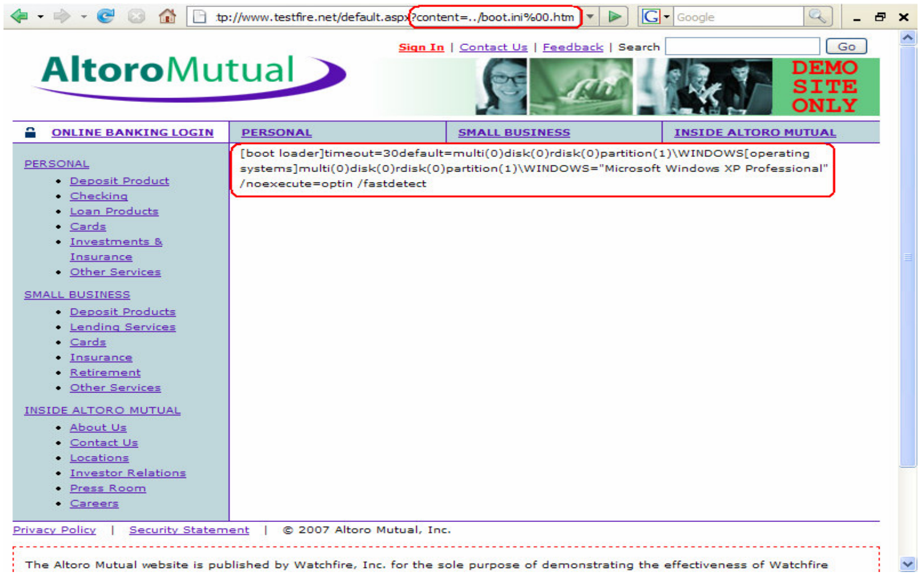
79 Achieving Enterprise Application Security © 2007 IBM Corporation

The attempt failed, and the system disclosed that it only allows parameter value (file names) that end with either txt or htm as their file extension.

Let’s try a little trick called “Poison Null Byte”, we’ll write the file we actually want to open which is Boot.ini, but append a NULL character and the extension the application is looking for (in this example .htm)

Presented by IBM developerWorks

Insecure Direct Object Reference – Example



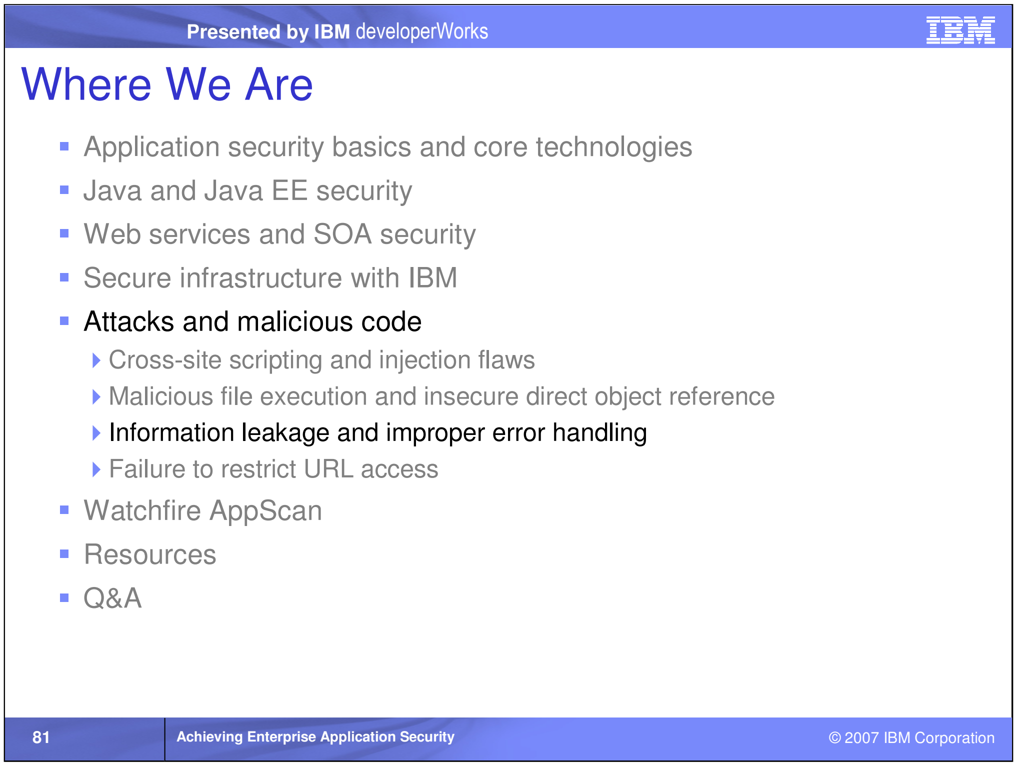
tp://www.testfire.net/default.aspx?content=../boot.ini%00.htm

```
[boot loader]timeout=30default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS[operating
systems]multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional"
/noexecute=optin /fastdetect
```

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire

Bingo! – we managed to circumvent the file extension validation, and open a sensitive system file.

Using this technique, we can manipulate the application to hand us the contents of other, more sensitive files, such as databases, customer files, etc.



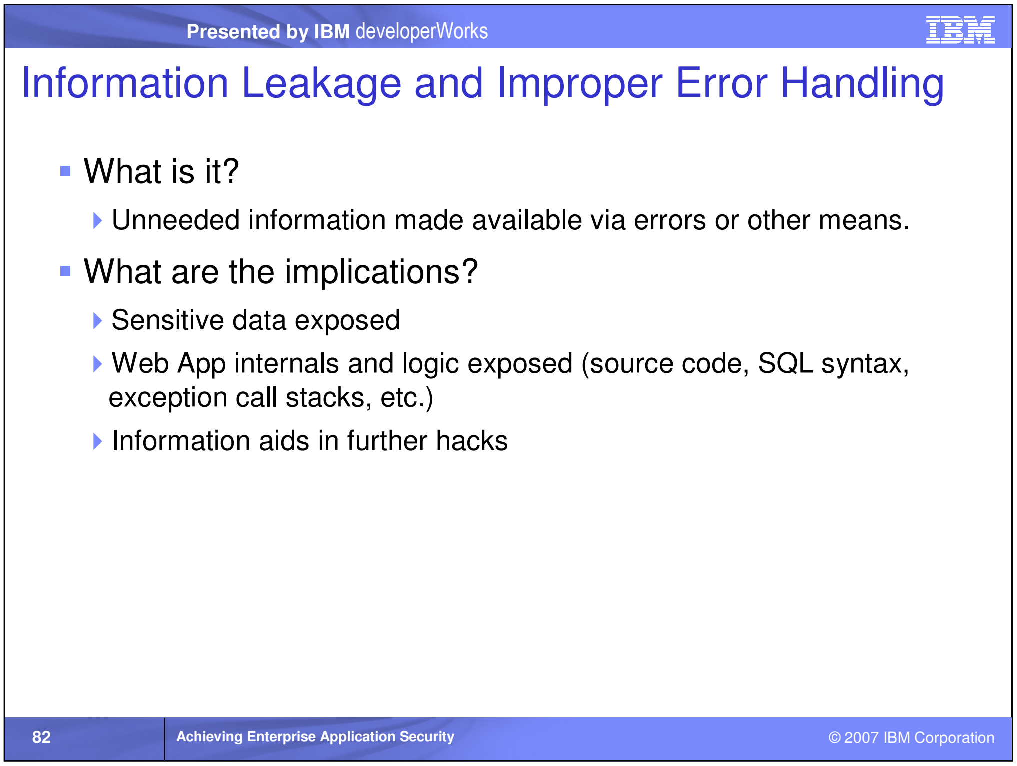
Presented by IBM developerWorks

Where We Are

- Application security basics and core technologies
- Java and Java EE security
- Web services and SOA security
- Secure infrastructure with IBM
- Attacks and malicious code
  - Cross-site scripting and injection flaws
  - Malicious file execution and insecure direct object reference
  - Information leakage and improper error handling
  - Failure to restrict URL access
- Watchfire AppScan
- Resources
- Q&A

81 Achieving Enterprise Application Security © 2007 IBM Corporation

Now let’s turn to information leakage and improper error handling, and see how those vulnerabilities can be exploited by an attacker.



Presented by IBM developerWorks

Information Leakage and Improper Error Handling

- What is it?
  - Unneeded information made available via errors or other means.
- What are the implications?
  - Sensitive data exposed
  - Web App internals and logic exposed (source code, SQL syntax, exception call stacks, etc.)
  - Information aids in further hacks

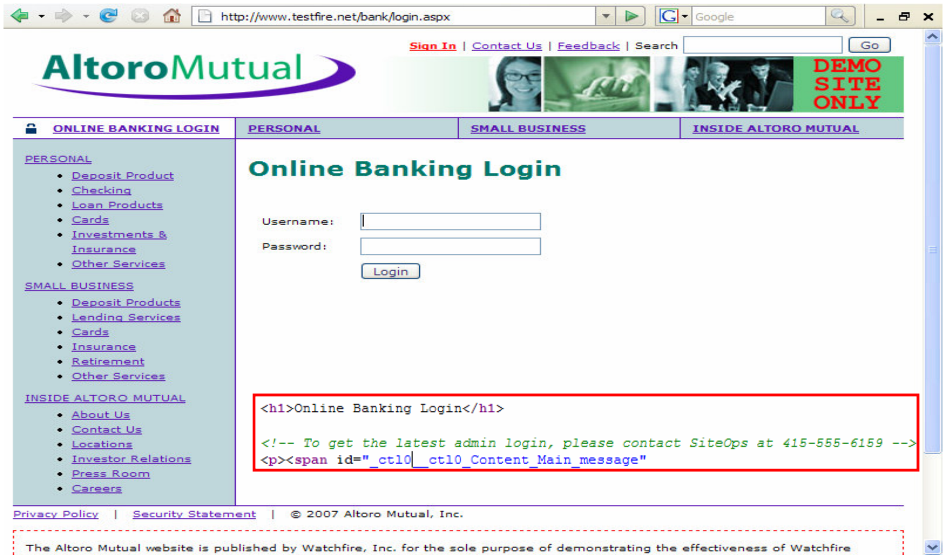
82 Achieving Enterprise Application Security © 2007 IBM Corporation

Let's move on to the next item on the OWASP Top 10 list - Information Leakage and Improper Error Handling.

Information leakage vulnerabilities usually do not allow a hacker to perform malicious actions, but rather enable the attacker to gather sensitive information, either about the application or about its users. This usually happens when application debugging information is not sanitized from response pages, when all sorts of errors (such as SQL error messages as shown before) occur, but it can also happen from more naive mistakes, such as leaving personal information or debugging remnants inside HTML comments.

The implication of Information leakage can range between sensitive data being exposed, to web application internal logic being visible to the hacker.

Information Leakage Example



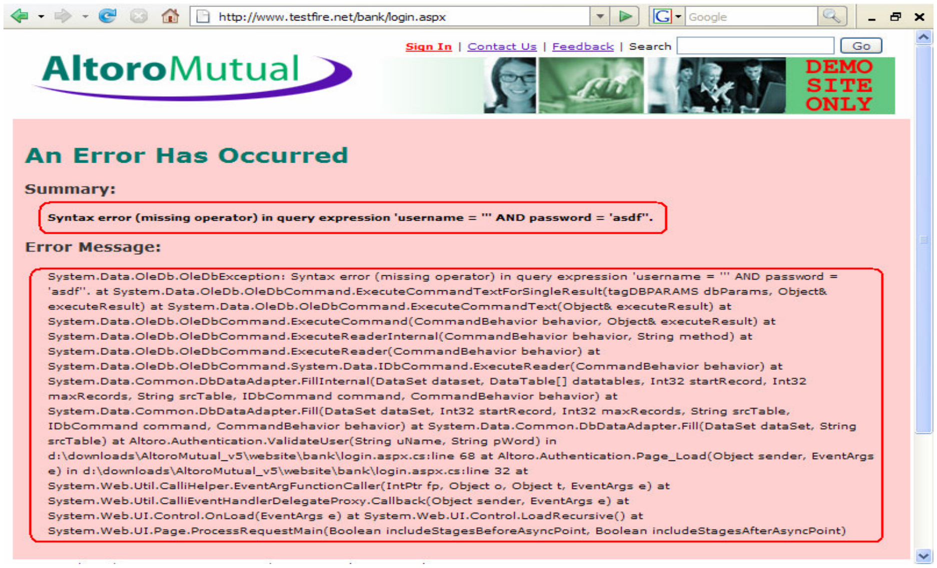
```
<h1>Online Banking Login</h1>

<!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
<p><span id="_ctl0__ctl0_Content_Main_message"
```

Let’s take a look at two information leakage examples:

The first example is a simple one – the administrator left his/her phone number inside HTML comments, assuming that users do not read them. This information can be harvested and later on used for social engineering purposes

The second example is the same as our previous SQL Injection scenario – if we submit a value (in this case apostrophe), that the application does not know how to handle, it might spit back debugging information.

Improper Error Handling Example


http://www.testfire.net/bank/login.aspx
Google
Sign In | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY

An Error Has Occurred

Summary:

Syntax error (missing operator) in query expression 'username = ''' AND password = 'asdf''.

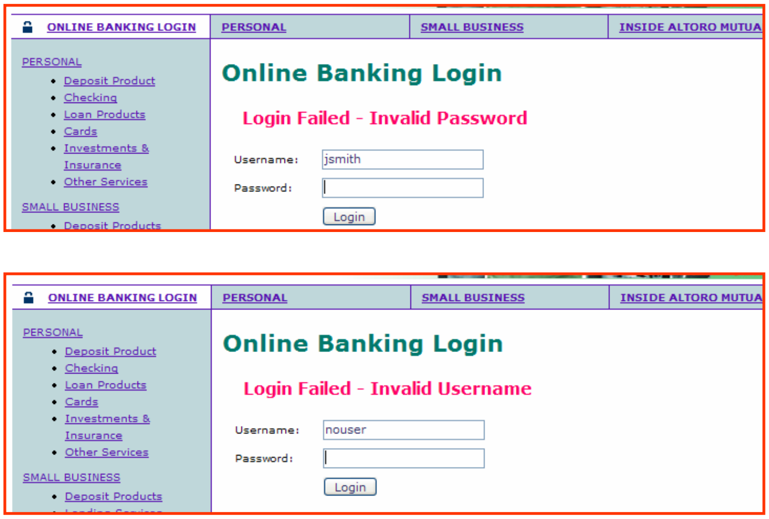
Error Message:

```
System.Data.OleDb.OleDbException: Syntax error (missing operator) in query expression 'username = ''' AND password =
'asdf''. at System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSingleResult(tagDBPARAMS dbParams, Object&
executeResult) at System.Data.OleDb.OleDbCommand.ExecuteCommandText(Object& executeResult) at
System.Data.OleDb.OleDbCommand.ExecuteCommand(CommandBehavior behavior, Object& executeResult) at
System.Data.OleDb.OleDbCommand.ExecuteReaderInternal(CommandBehavior behavior, String method) at
System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior) at
System.Data.OleDb.OleDbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior) at
System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32
maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) at
System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable,
IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String
srcTable) at Altoro.Authentication.ValidateUser(String uName, String pWord) in
d:\downloads\AltoroMutual_v5\website\bank\login.aspx.cs:line 68 at Altoro.Authentication.Page_Load(Object sender, EventArgs
e) in d:\downloads\AltoroMutual_v5\website\bank\login.aspx.cs:line 32 at
System.Web.Util.CalliHelper.EventArgFunctionCaller(IntPtr fp, Object o, Object t, EventArgs e) at
System.Web.Util.CalliEventHandlerDelegateProxy.Callback(Object sender, EventArgs e) at
System.Web.UI.Control.OnLoad(EventArgs e) at System.Web.UI.Control.LoadRecursive() at
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint)
```

What you see here, is the response to the form submission, which included an apostrophe character as the user name.

This error page reveals information about the type of SQL database that is used, and about the structure of the SQL query, allowing us to further devise a SQL Injection attack against the web application

Information Leakage – Different User/Pass Error



Online Banking Login

Login Failed - Invalid Password

Username: jsmith

Password:

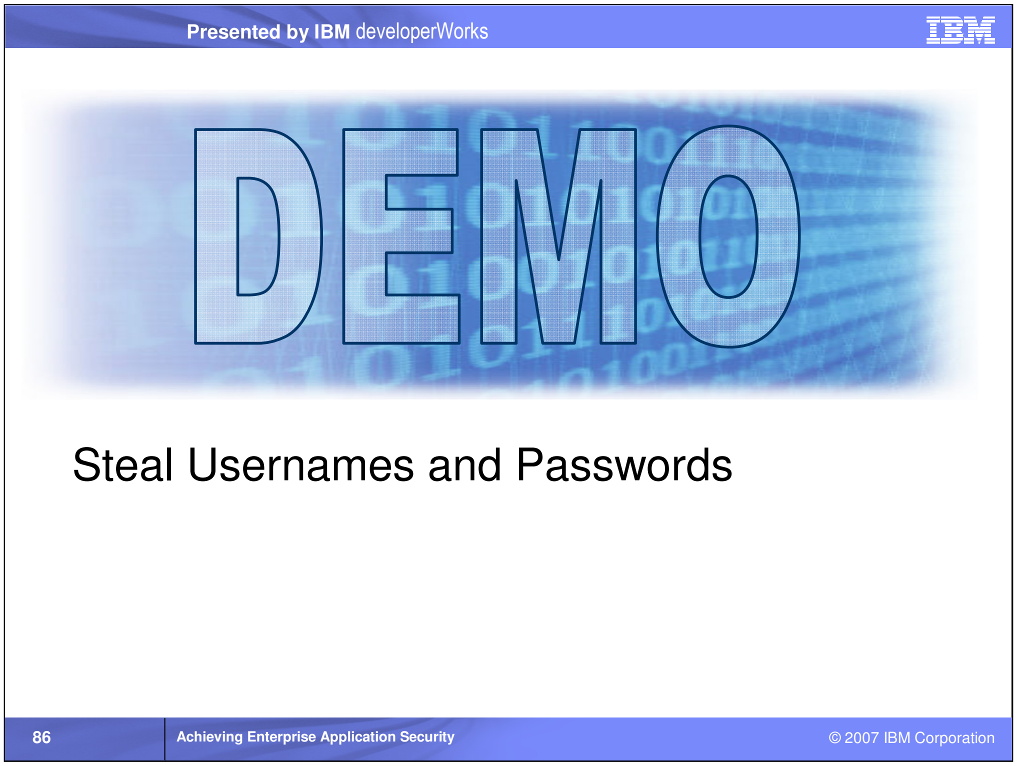
Online Banking Login

Login Failed - Invalid Username

Username: nouser

Password:

One last example of information leakage, which is also very common, is verbose login error messages. Some applications, will present the user with different error messages when the login process failed due to invalid username or invalid password (as seen in this slide). While this is not a severe issue, it narrows down the amount of time it will take the hacker to guess (or brute force) his/her way into the application.



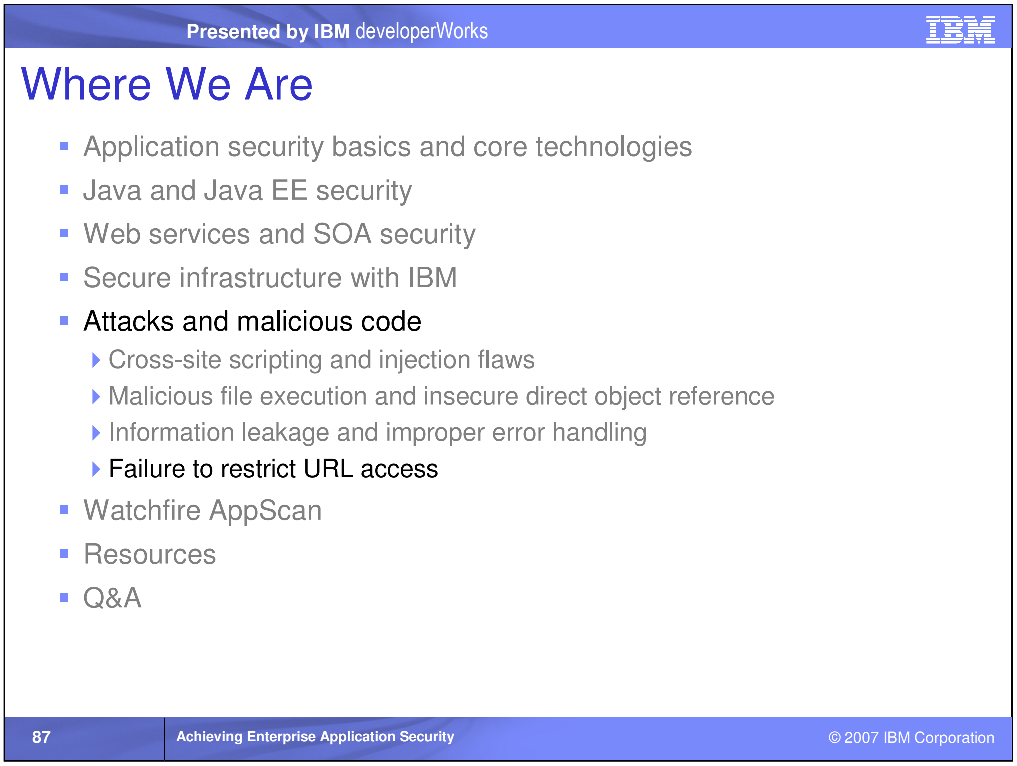
Presented by IBM developerWorks

DEMO

Steal Usernames and Passwords

86 Achieving Enterprise Application Security © 2007 IBM Corporation

This demo shows how to use information leakage to steal the usernames and passwords from a site.



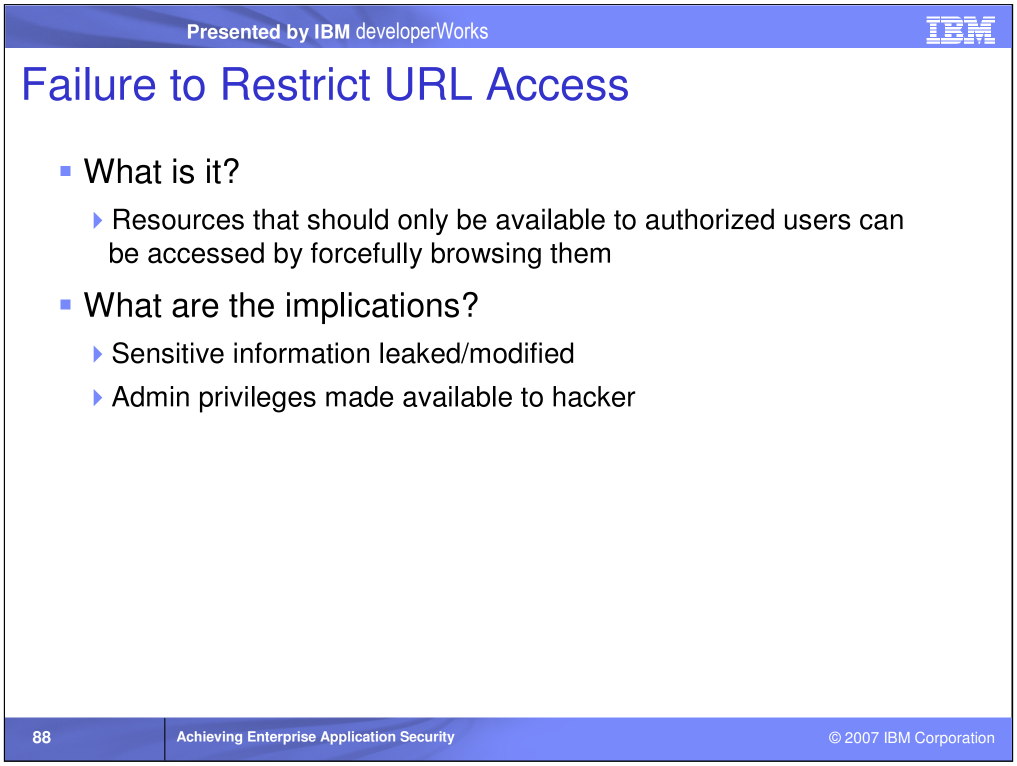
Presented by IBM developerWorks

Where We Are

- Application security basics and core technologies
- Java and Java EE security
- Web services and SOA security
- Secure infrastructure with IBM
- Attacks and malicious code
  - Cross-site scripting and injection flaws
  - Malicious file execution and insecure direct object reference
  - Information leakage and improper error handling
  - Failure to restrict URL access
- Watchfire AppScan
- Resources
- Q&A

87 Achieving Enterprise Application Security © 2007 IBM Corporation

The last vulnerability we will look at is failure to restrict URL access.



Presented by IBM developerWorks

Failure to Restrict URL Access

- What is it?
  - Resources that should only be available to authorized users can be accessed by forcefully browsing them
- What are the implications?
  - Sensitive information leaked/modified
  - Admin privileges made available to hacker

88 Achieving Enterprise Application Security © 2007 IBM Corporation

One of the most common security issues in web applications is the lack of proper access restrictions. Many people forget that not having a link to a resource, doesn’t mean that hackers can’t guess it. You should always limit user’s access, by putting URL access restrictions. Portions of the site that belong to administrators, should never be accessed by regular users.

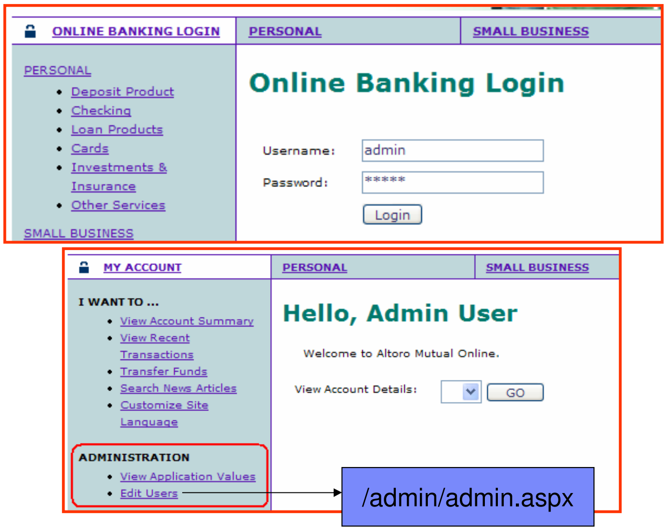
Failing to create proper access restrictions on web application resources might lead to:

-Information leakage

-Privilege escalation

Presented by IBM developerWorks

Failure to Restrict URL Access - Admin User Login



ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

Online Banking Login

Username: admin

Password: *****

Login

MY ACCOUNT | PERSONAL | SMALL BUSINESS

I WANT TO ...
- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION
- View Application Values
- Edit Users

Hello, Admin User

Welcome to Altoro Mutual Online.

View Account Details: GO

/admin/admin.aspx

We'll now take a look at a simple Privilege Escalation example -

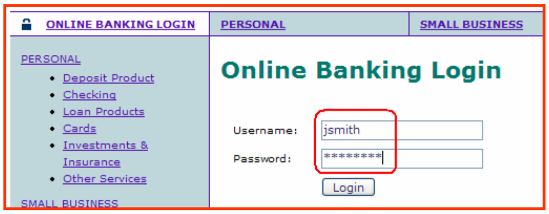
This example, shows how unrestricted access to the administration page, may lead to complete compromise of the web application.

When we log into the application as the administrator, we are presented with a link to the user account editing page. Naturally, this link doesn't appear in regular users' screens, nor should it be accessible for them.

Since the application doesn't restrict access to this page, a hacker can attempt to guess that link, and take over the web application, as will be seen in the following slide.

Presented by IBM developerWorks

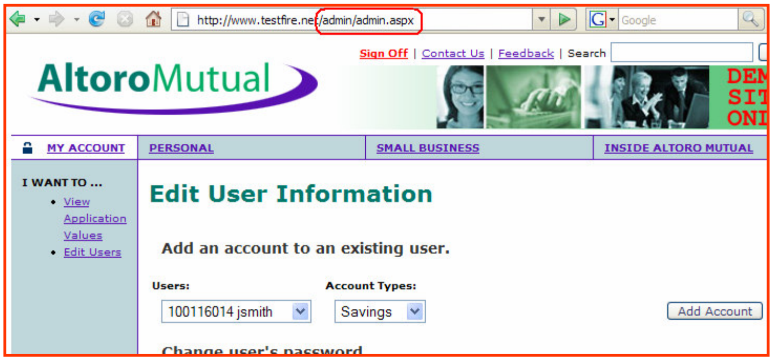
Forceful Browse to Admin Page



Online Banking Login

Username: jsmith

Password: ********



Edit User Information

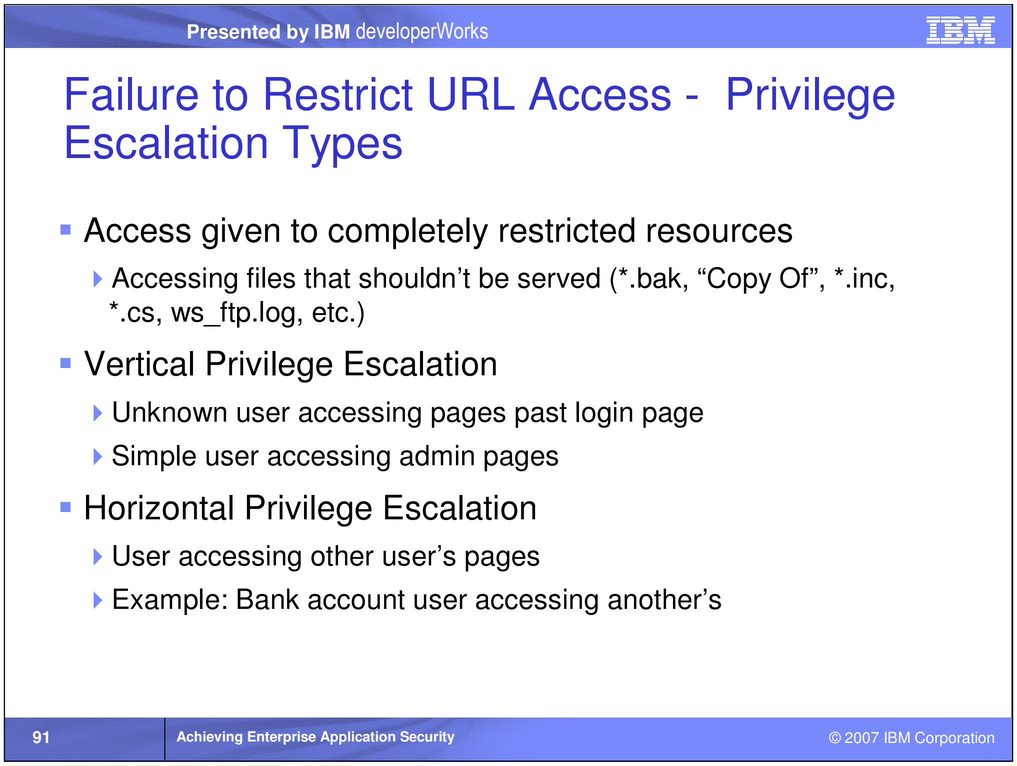
Add an account to an existing user.

Users: 100116014 jsmith

Account Types: Savings

Change user's password

In this slide you see how the user authenticates as a regular user, but since the application did not have proper URL access permissions, the user guessed the link to the administration page, and was able to perform actions on behalf of the administrator, without having to log in as a high privileged user.



Presented by IBM developerWorks

Failure to Restrict URL Access - Privilege Escalation Types

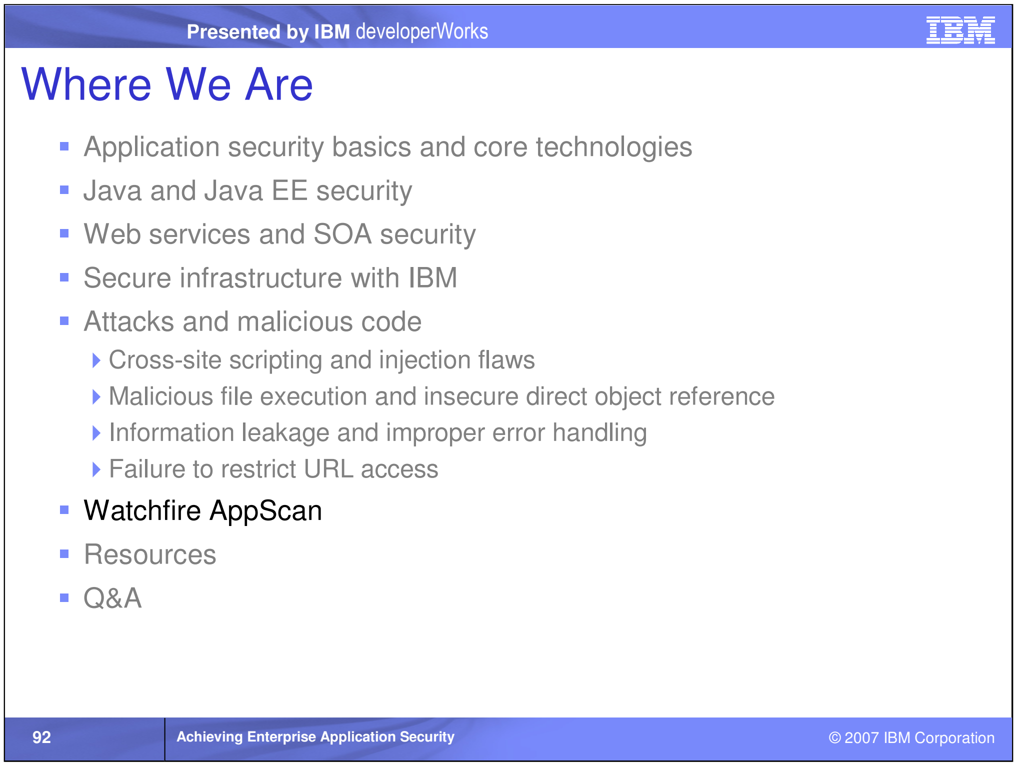
- Access given to completely restricted resources
  - Accessing files that shouldn’t be served (*.bak, “Copy Of”, *.inc, *.cs, ws_ftp.log, etc.)
- Vertical Privilege Escalation
  - Unknown user accessing pages past login page
  - Simple user accessing admin pages
- Horizontal Privilege Escalation
  - User accessing other user’s pages
  - Example: Bank account user accessing another’s

91 Achieving Enterprise Application Security © 2007 IBM Corporation

You should always block users from requesting and retrieving restricted resources (for example, backup files, log files, source code files, etc.)

Regular users shouldn’t be allowed to access pages that belong to higher privileged users (this is referred to as vertical PE)

Regular users shouldn’t have access to other regular users’ pages (this is referred to horizontal PE)



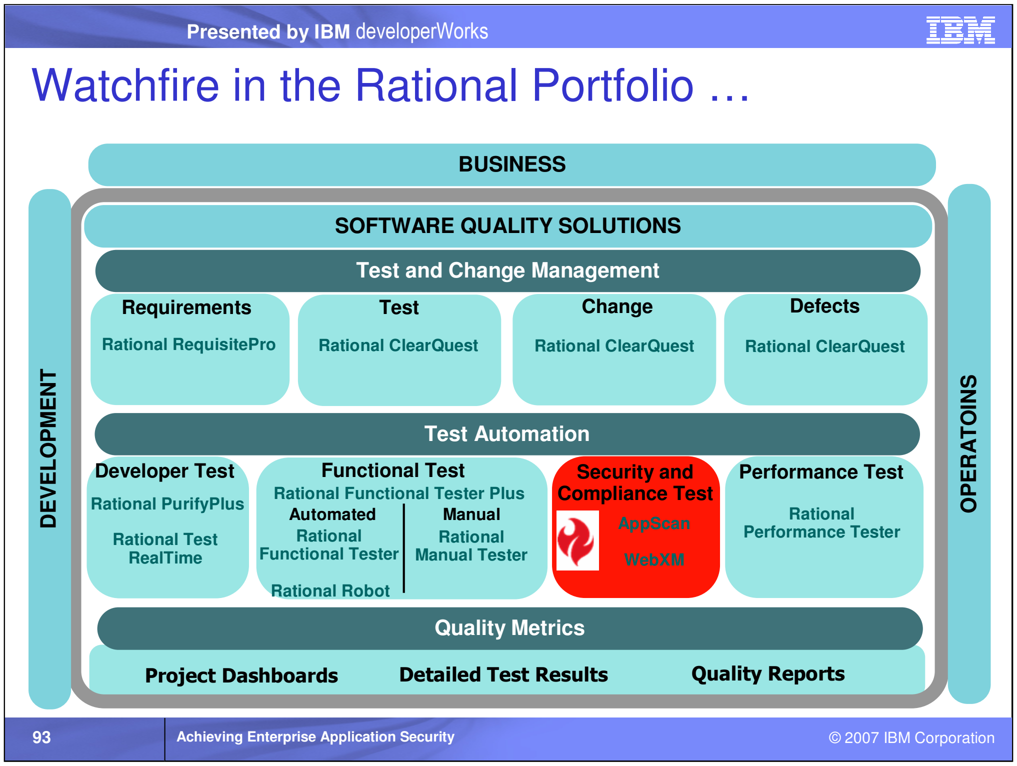
Presented by IBM developerWorks

Where We Are

- Application security basics and core technologies
- Java and Java EE security
- Web services and SOA security
- Secure infrastructure with IBM
- Attacks and malicious code
  - Cross-site scripting and injection flaws
  - Malicious file execution and insecure direct object reference
  - Information leakage and improper error handling
  - Failure to restrict URL access
- Watchfire AppScan
- Resources
- Q&A

92 Achieving Enterprise Application Security © 2007 IBM Corporation

Watchfire AppScan can help you find vulnerabilities in your Web applications.



Presented by IBM developerWorks

Watchfire in the Rational Portfolio …

BUSINESS

DEVELOPMENT

OPERATOINS

SOFTWARE QUALITY SOLUTIONS

Test and Change Management

Requirements
Rational RequisitePro

Test
Rational ClearQuest

Change
Rational ClearQuest

Defects
Rational ClearQuest

Test Automation

Developer Test
Rational PurifyPlus
Rational Test RealTime

Functional Test
Rational Functional Tester Plus
Automated
Rational Functional Tester
Rational Robot
Manual
Rational Manual Tester

Security and Compliance Test
AppScan
WebXM

Performance Test
Rational Performance Tester

Quality Metrics

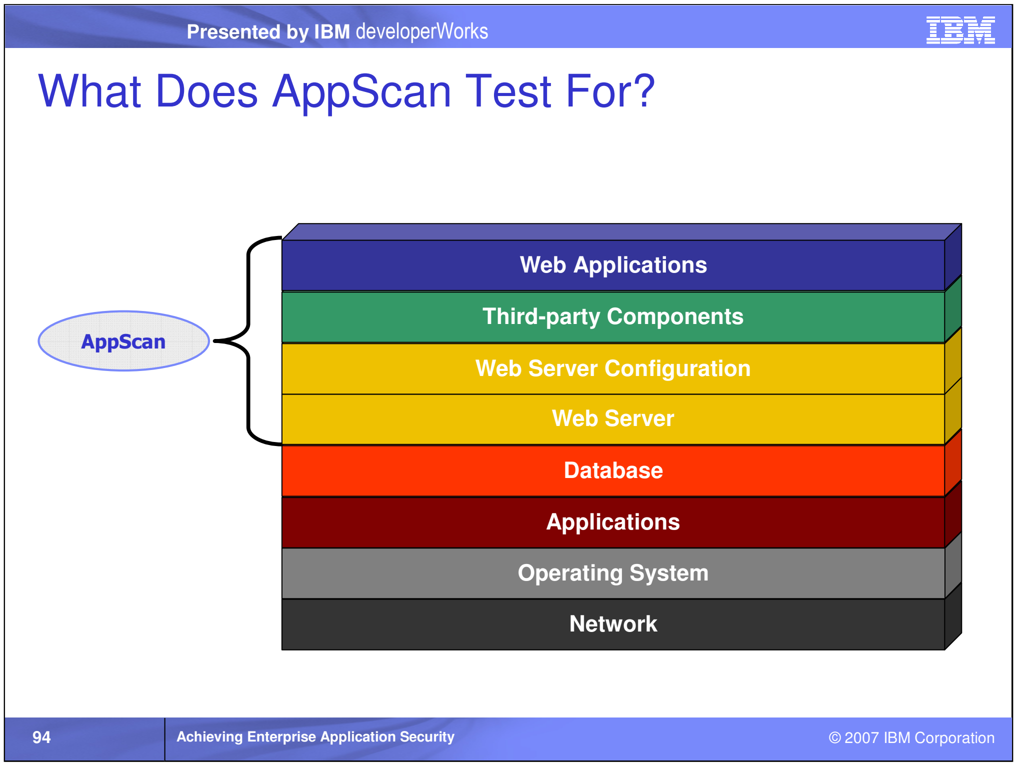
Project Dashboards

Detailed Test Results

Quality Reports

93 Achieving Enterprise Application Security © 2007 IBM Corporation

Rational has an integrated solution that allows for Testing(both manual and automated) and Change management. Watchfire's tools AppScan and WebXM expand our exisitng solution to allow for security and compliance testing. WebXM allows organizations to ensure the complicance of their web sites and AppScan the quality and security of the websites.



Presented by IBM developerWorks

What Does AppScan Test For?

AppScan

Web Applications

Third-party Components

Web Server Configuration

Web Server

Database

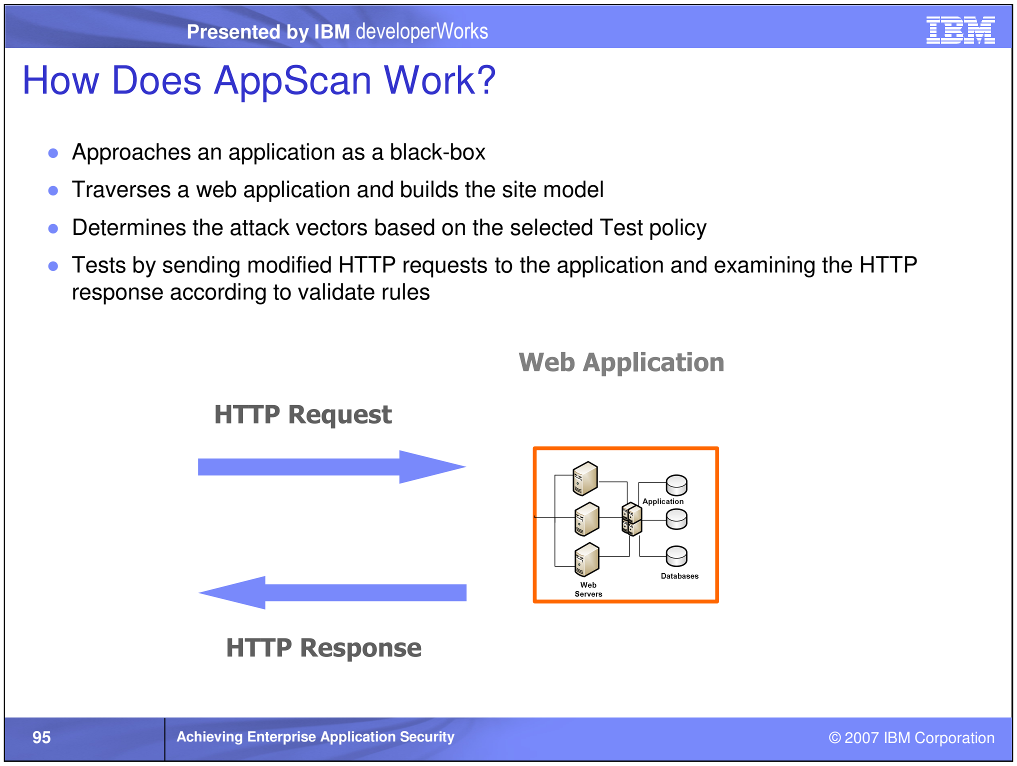
Applications

Operating System

Network

94 Achieving Enterprise Application Security © 2007 IBM Corporation

In the stack shown, AppScan focuses on the Web server, its configuration, third-party components in the Web server environment, and Web applications that operate in the Web server.



Presented by IBM developerWorks

How Does AppScan Work?

- Approaches an application as a black-box
- Traverses a web application and builds the site model
- Determines the attack vectors based on the selected Test policy
- Tests by sending modified HTTP requests to the application and examining the HTTP response according to validate rules

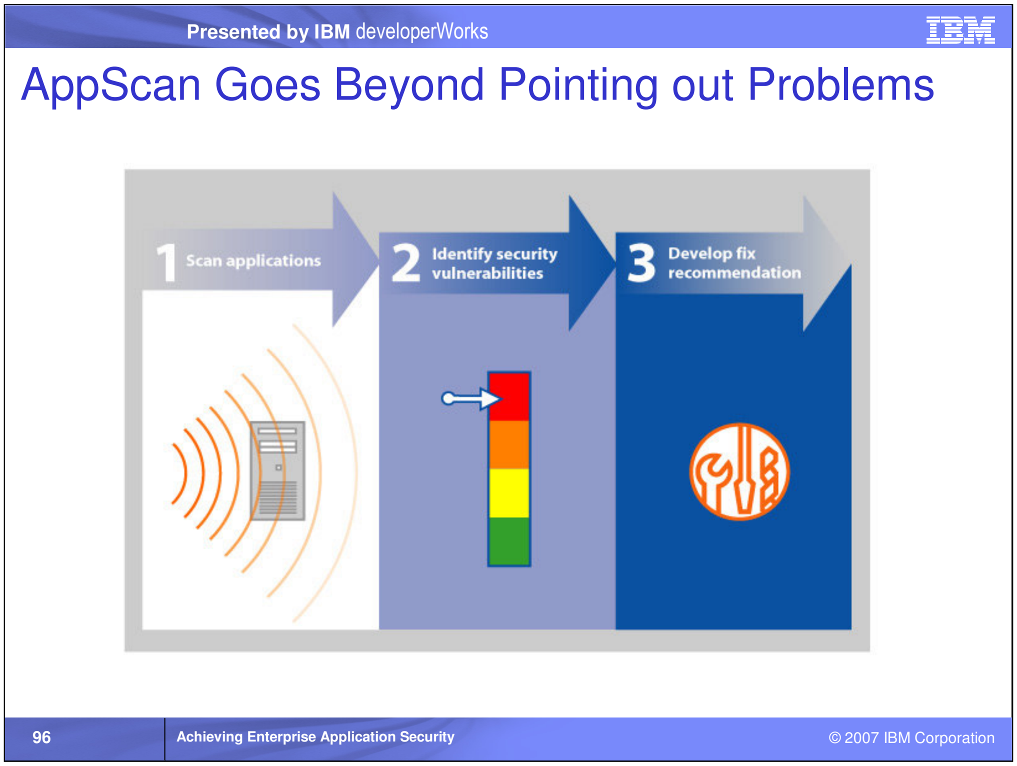
Web Application

HTTP Request

HTTP Response

95 Achieving Enterprise Application Security © 2007 IBM Corporation

AppScan scans for vulnerabilities by traversing an application similarly to the way a user browses a website. It starts from the home page or some other entry point, as defined by the user, and follows all the links. Each page is analyzed, and based on the characteristics of the page, AppScan sends a number of tests. The tests are sent in the form of HTTP requests. AppScan determines the presence of vulnerabilities based on the responses from the web server. The application is treated as a black box and AppScan communicates with it just like a browser does.



Presented by IBM developerWorks

AppScan Goes Beyond Pointing out Problems

1 Scan applications

2 Identify security vulnerabilities

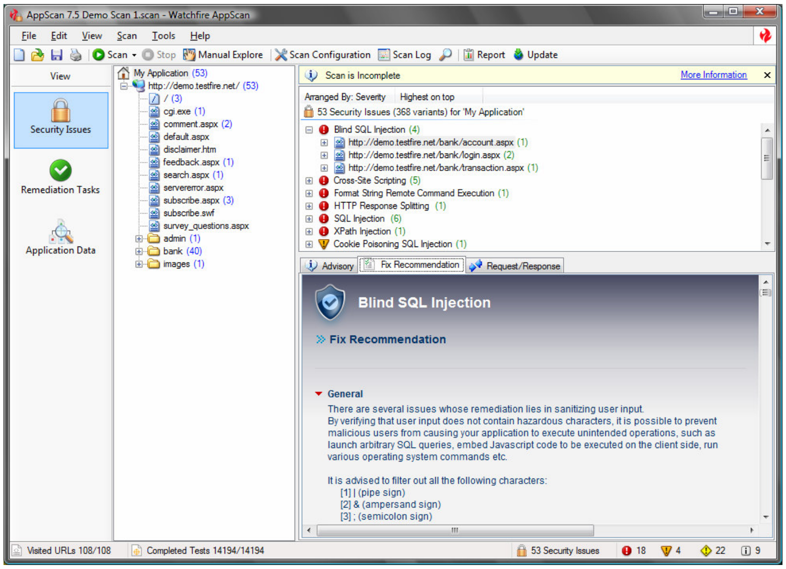
3 Develop fix recommendation

96 Achieving Enterprise Application Security © 2007 IBM Corporation

AppScan does not just merely find the problems in your Web application, but also provides recommendations on how to fix each problem found.

Presented by IBM developerWorks

Actionable Fix Recommendations



Scan is Incomplete

53 Security Issues (368 variants) for 'My Application'

- Blind SQL Injection (4)
  - http://demo.testfire.net/bank/account.aspx (1)
  - http://demo.testfire.net/bank/login.aspx (2)
  - http://demo.testfire.net/bank/transaction.aspx (1)
- Cross-Site Scripting (5)
- Format String Remote Command Execution (1)
- HTTP Response Splitting (1)
- SQL Injection (6)
- XPath Injection (1)
- Cookie Poisoning SQL Injection (1)

Blind SQL Injection

Fix Recommendation

General

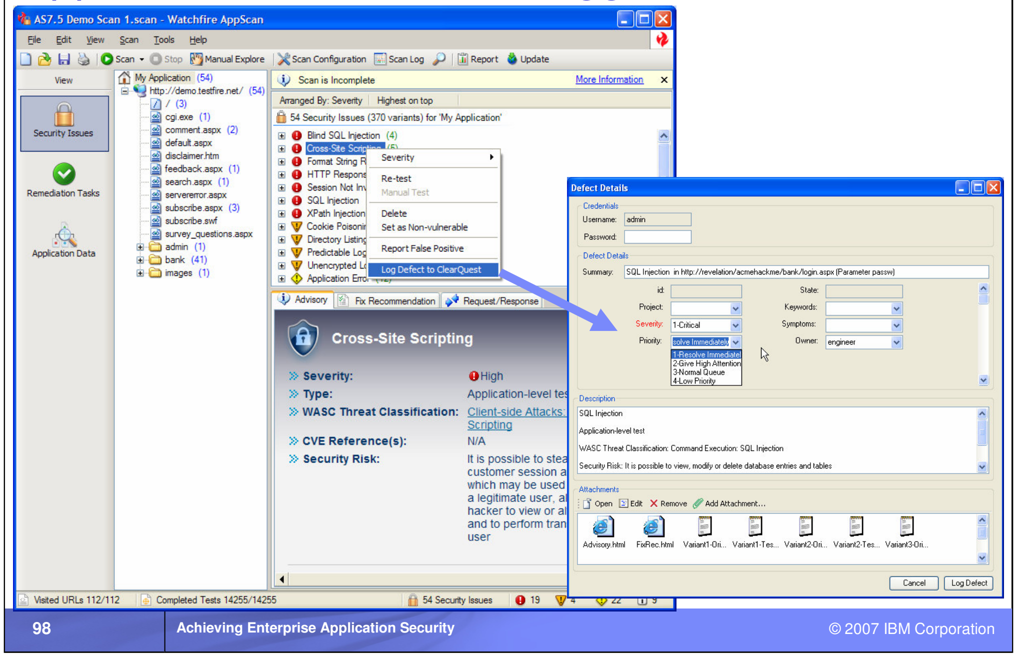
There are several issues whose remediation lies in sanitizing user input.
By verifying that user input does not contain hazardous characters, it is possible to prevent malicious users from causing your application to execute unintended operations, such as launch arbitrary SQL queries, embed Javascript code to be executed on the client side, run various operating system commands etc.

It is advised to filter out all the following characters:
[1] | (pipe sign)
[2] & (ampersand sign)
[3] ; (semicolon sign)

Actionable fix recommendations provide detailed information on the problem and steps you can take to fix it.

Presented by IBM developerWorks

AppScan with QA Defect Logger for ClearQuest



My Application (54)
http://demo.testfire.net/ (54)
/ (3)
cgi.exe (1)
comment.aspx (2)
default.aspx
disclaimer.htm
feedback.aspx (1)
search.aspx (1)
servererror.aspx
subscribe.aspx (3)
subscribe.swf
survey_questions.aspx
admin (1)
bank (41)
images (1)

Scan is Incomplete More Information

Arranged By: Severity | Highest on top

54 Security Issues (370 variants) for 'My Application'

- Blind SQL Injection (4)
- Cross-Site Scripting (5)
- Format String R
- HTTP Respons
- Session Not Inv
- SQL Injection
- XPath Injection
- Cookie Poisonir
- Directory Listing
- Predictable Log
- Unencrypted L
- Application Erro

Cross-Site Scripting

Severity: High
Type: Application-level tes
WASC Threat Classification: Client-side Attacks: Scripting
CVE Reference(s): N/A
Security Risk: It is possible to stea customer session a which may be used a legitimate user, al hacker to view or al and to perform tran user

Visited URLs 112/112 | Completed Tests 14255/14255 | 54 Security Issues | 19 | 4 | 22 | 9

Credentials
Username: admin
Password:

Defect Details
Summary: SQL Injection in http://revelation/acmehackme/bank/login.aspx (Parameter passw)
id:
State:
Project:
Keywords:
Severity: 1-Critical
Symptoms:
Priority: solve Immediately
Owner: engineer

1-Resolve Immediatel
2-Give High Attention
3-Normal Queue
4-Low Priority

Description
SQL Injection

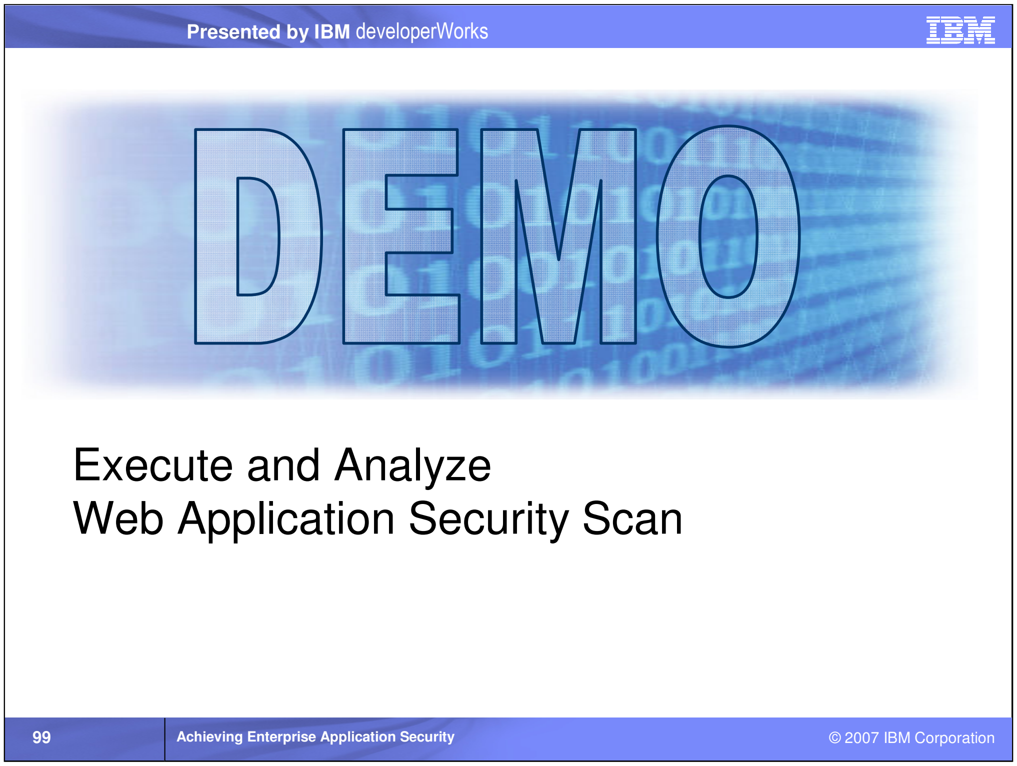
Application-level test

WASC Threat Classification: Command Execution: SQL Injection

Security Risk: It is possible to view, modify or delete database entries and tables

Attachments
Advisory.html | FixRec.html | Variant1-Ori... | Variant1-Tes... | Variant2-Ori... | Variant2-Tes... | Variant3-Ori...

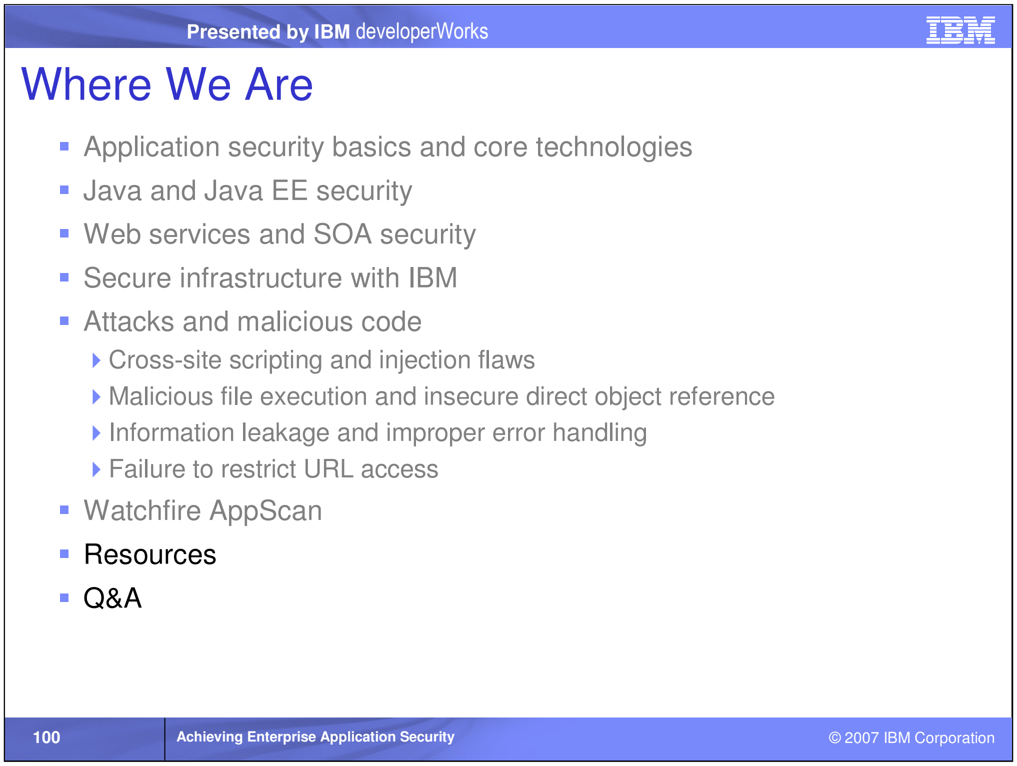
AppScan integrates with Rational ClearQuest, so that security issues can be logged as defects into ClearQuest for assignment and tracking.



DEMO

Execute and Analyze
Web Application Security Scan

This demo shows AppScan in action.



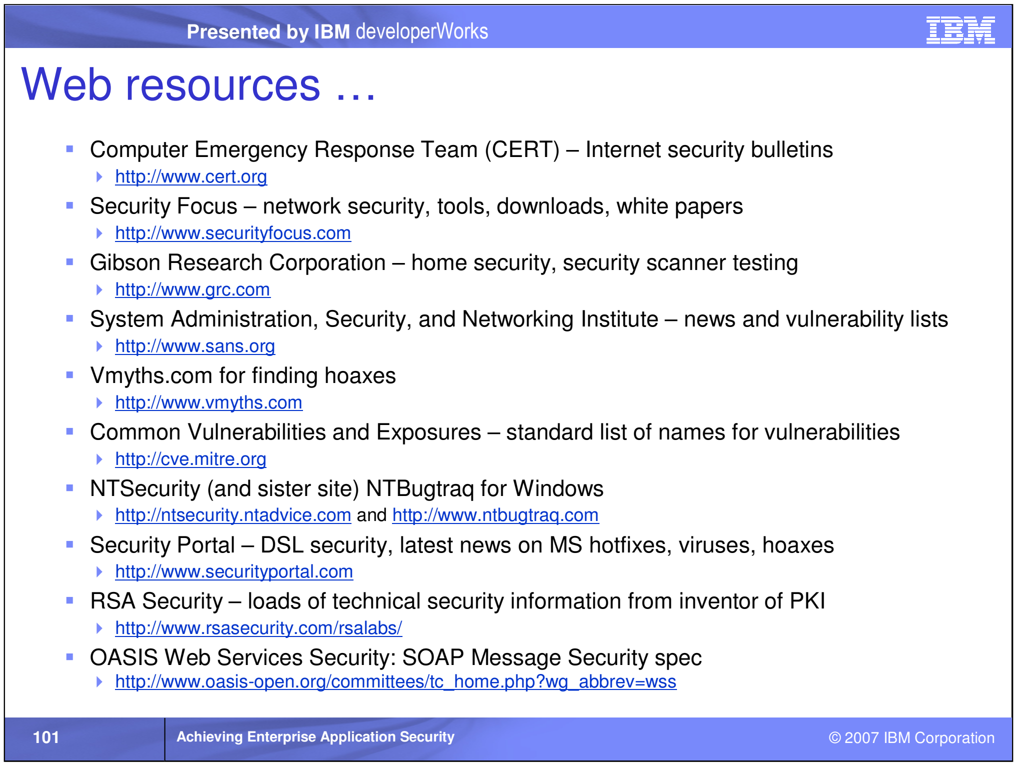
Presented by IBM developerWorks

Where We Are

- Application security basics and core technologies
- Java and Java EE security
- Web services and SOA security
- Secure infrastructure with IBM
- Attacks and malicious code
  - Cross-site scripting and injection flaws
  - Malicious file execution and insecure direct object reference
  - Information leakage and improper error handling
  - Failure to restrict URL access
- Watchfire AppScan
- Resources
- Q&A

100 Achieving Enterprise Application Security © 2007 IBM Corporation

Here we’ll give you some resources you can use to learn more about what was covered today and about other IBM products and technologies.

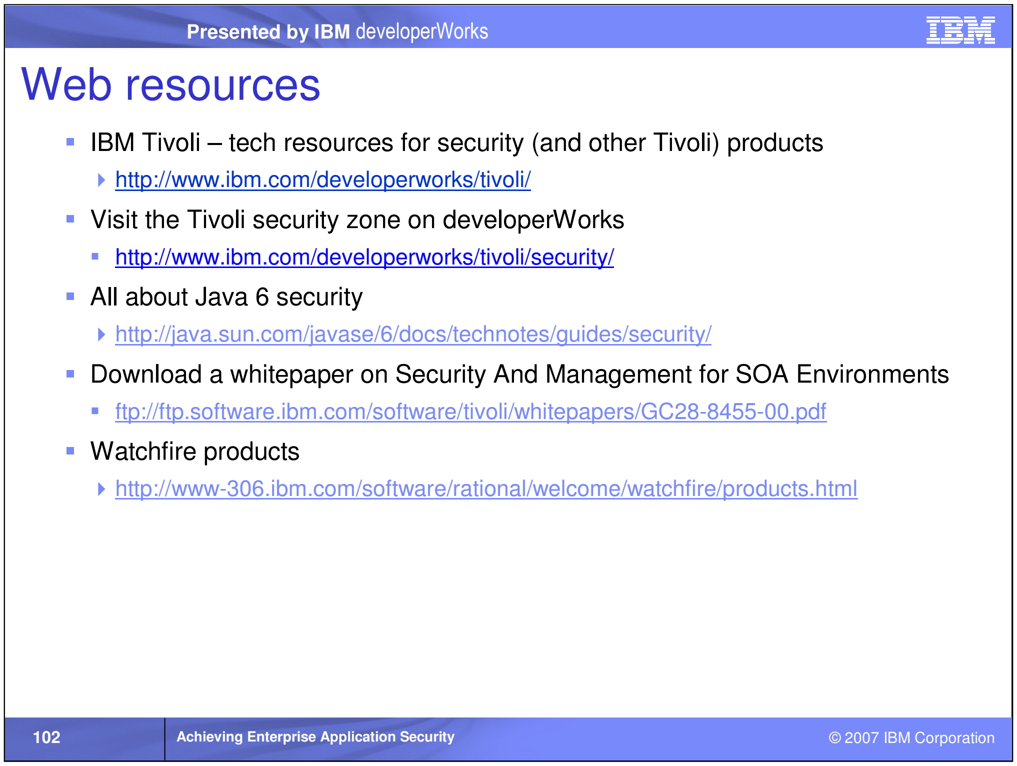


Presented by IBM developerWorks

Web resources …

- Computer Emergency Response Team (CERT) – Internet security bulletins
  - http://www.cert.org
- Security Focus – network security, tools, downloads, white papers
  - http://www.securityfocus.com
- Gibson Research Corporation – home security, security scanner testing
  - http://www.grc.com
- System Administration, Security, and Networking Institute – news and vulnerability lists
  - http://www.sans.org
- Vmyths.com for finding hoaxes
  - http://www.vmyths.com
- Common Vulnerabilities and Exposures – standard list of names for vulnerabilities
  - http://cve.mitre.org
- NTSecurity (and sister site) NTBugtraq for Windows
  - http://ntsecurity.ntadvice.com and http://www.ntbugtraq.com
- Security Portal – DSL security, latest news on MS hotfixes, viruses, hoaxes
  - http://www.securityportal.com
- RSA Security – loads of technical security information from inventor of PKI
  - http://www.rsasecurity.com/rsalabs/
- OASIS Web Services Security: SOAP Message Security spec
  - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

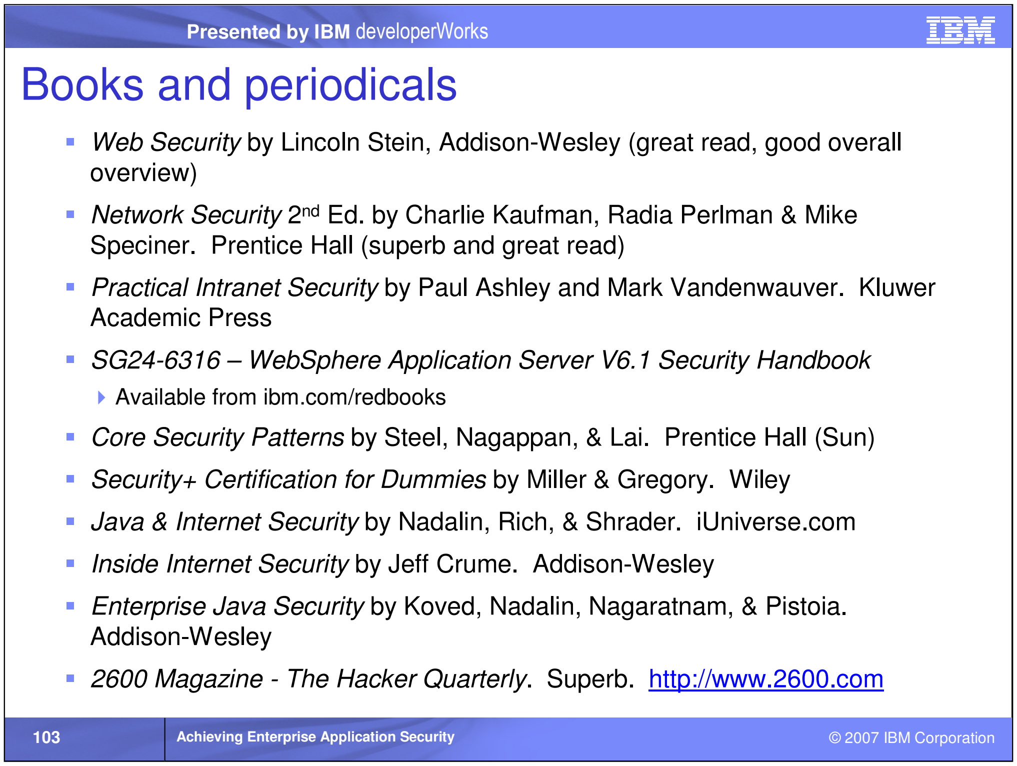
101 Achieving Enterprise Application Security © 2007 IBM Corporation



Presented by IBM developerWorks

Web resources

- IBM Tivoli – tech resources for security (and other Tivoli) products
  - http://www.ibm.com/developerworks/tivoli/
- Visit the Tivoli security zone on developerWorks
  - http://www.ibm.com/developerworks/tivoli/security/
- All about Java 6 security
  - http://java.sun.com/javase/6/docs/technotes/guides/security/
- Download a whitepaper on Security And Management for SOA Environments
  - ftp://ftp.software.ibm.com/software/tivoli/whitepapers/GC28-8455-00.pdf
- Watchfire products
  - http://www-306.ibm.com/software/rational/welcome/watchfire/products.html



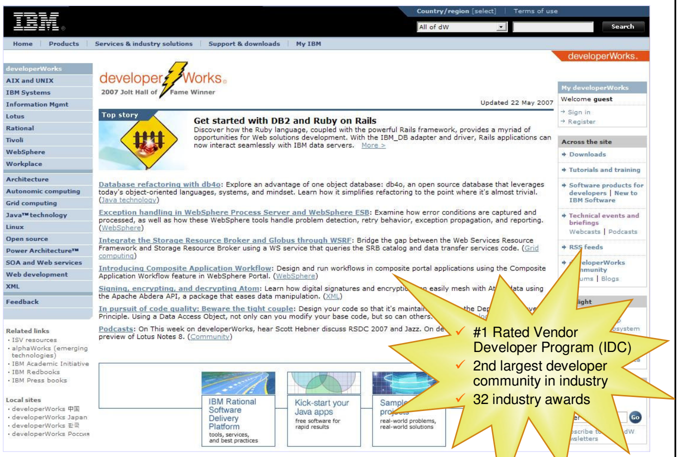
Presented by IBM developerWorks

Books and periodicals

- *Web Security* by Lincoln Stein, Addison-Wesley (great read, good overall overview)
- *Network Security* 2nd Ed. by Charlie Kaufman, Radia Perlman & Mike Speciner. Prentice Hall (superb and great read)
- *Practical Intranet Security* by Paul Ashley and Mark Vandenwauver. Kluwer Academic Press
- *SG24-6316 – WebSphere Application Server V6.1 Security Handbook*
  - Available from ibm.com/redbooks
- *Core Security Patterns* by Steel, Nagappan, & Lai. Prentice Hall (Sun)
- *Security+ Certification for Dummies* by Miller & Gregory. Wiley
- *Java & Internet Security* by Nadalin, Rich, & Shrader. iUniverse.com
- *Inside Internet Security* by Jeff Crume. Addison-Wesley
- *Enterprise Java Security* by Koved, Nadalin, Nagaratnam, & Pistoia. Addison-Wesley
- *2600 Magazine - The Hacker Quarterly*. Superb. http://www.2600.com

Get additional resources from IBM developerWorks

- **Technical resources**
  - How-to information
  - Sample code
  - Roadmaps
  - Trial downloads
  - Tutorials
  - Technical articles
  - Webcasts
  - Demos
  - Academic portals
  - Sample projects
- **Web communities**
  - Technology zones
  - Brand zones
  - alphaWorks
  - Discussion forums
  - Blogs
  - Wikis
  - RSS Feeds
  - Podcasts
  - Localized sites in key non-US markets



Country/region [select] | Terms of use

All of dW ▾ Search

Home | Products | Services & industry solutions | Support & downloads | My IBM

developerWorks.

developerWorks 2007 Jolt Hall of Fame Winner

developerWorks
AIX and UNIX
IBM Systems
Information Mgmt
Lotus
Rational
Tivoli
WebSphere
Workplace
Architecture
Autonomic computing
Grid computing
Java™ technology
Linux
Open source
Power Architecture™
SOA and Web services
Web development
XML
Feedback

Related links
- ISV resources
- alphaWorks (emerging technologies)
- IBM Academic Initiative
- IBM Redbooks
- IBM Press books

Local sites
- developerWorks 中国
- developerWorks Japan
- developerWorks 한국
- developerWorks Россия

Updated 22 May 2007

Top story

Get started with DB2 and Ruby on Rails
Discover how the Ruby language, coupled with the powerful Rails framework, provides a myriad of opportunities for Web solutions development. With the IBM_DB adapter and driver, Rails applications can now interact seamlessly with IBM data servers. More >

Database refactoring with db4o: Explore an advantage of one object database: db4o, an open source database that leverages today's object-oriented languages, systems, and mindset. Learn how it simplifies refactoring to the point where it's almost trivial. (Java technology)

Exception handling in WebSphere Process Server and WebSphere ESB: Examine how error conditions are captured and processed, as well as how these WebSphere tools handle problem detection, retry behavior, exception propagation, and reporting. (WebSphere)

Integrate the Storage Resource Broker and Globus through WSRF: Bridge the gap between the Web Services Resource Framework and Storage Resource Broker using a WS service that queries the SRB catalog and data transfer services code. (Grid computing)

Introducing Composite Application Workflow: Design and run workflows in composite portal applications using the Composite Application Workflow feature in WebSphere Portal. (WebSphere)

Signing, encrypting, and decrypting Atom: Learn how digital signatures and encryptio easily mesh with At data using the Apache Abdera API, a package that eases data manipulation. (XML)

In pursuit of code quality: Beware the tight couple: Design your code so that it's maintain the Dep Principle. Using a Data Access Object, not only can you modify your base code, but so can others.

Podcasts: On This week on developerWorks, hear Scott Hebner discuss RSDC 2007 and Jazz. On de preview of Lotus Notes 8. (Community)

IBM Rational Software Delivery Platform
tools, services, and best practices

Kick-start your Java apps
free software for rapid results

Sample projects
real-world problems, real-world solutions

My developerWorks
Welcome **guest**
→ Sign in
→ Register

Across the site
- Downloads
- Tutorials and training
- Software products for developers | New to IBM Software
- Technical events and briefings
  Webcasts | Podcasts
- RSS feeds
- developerWorks community
  Forums | Blogs

Go

- ✓ #1 Rated Vendor Developer Program (IDC)
- ✓ 2nd largest developer community in industry
- ✓ 32 industry awards

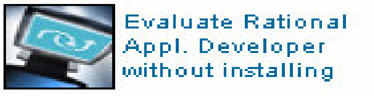
- **Support in the community**
  - developerWorks Live! Briefings
  - User Group support
  - Academic & University events

Download and evaluate the IBM Software Discussed Today

It's easier than ever to get your hands on IBM trial software!

You'll now find trials of a wide selection of IBM's software development and testing tools, as well as middleware, in one convenient location. Visit developerWorks to download and evaluate:

- Rational Application Developer
- Callisto Simultaneous Release project
- Tivoli Identity and Access Management



You will also find a collection of supporting materials for each download, including complimentary tech support, discussion forums, installation guides, demos & tutorials, ROI/business justification materials, and information on how to buy.

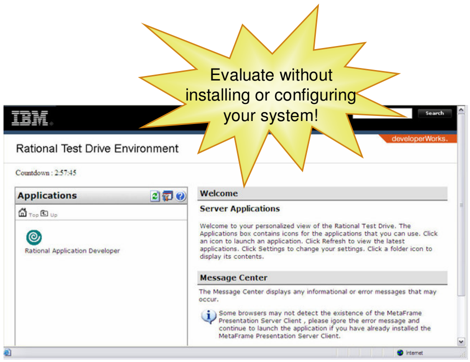
ibm.com/developerworks/downloads/

You may also order a Software Evaluation Kit DVD (Windows or Linux versions available) from which to download the latest IBM trial software:

ibm.com/developerWorks/offers/sek

New! Test-drive IBM Rational software online

- In addition to the trial downloads, you may now explore the capabilities of some Rational products online.
  - Register to receive an entrance ID & password and explore the product for up to three hours per session
  - Use your own data and files during your online trials to try out real-world scenarios
  - Products available:



Evaluate without installing or configuring your system!

Rational Test Drive Environment

Countdown : 2:57:45

Applications

Rational Application Developer

Welcome

Server Applications

Welcome to your personalized view of the Rational Test Drive. The Applications box contains icons for the applications that you can use. Click an icon to launch an application. Click Refresh to view the latest applications. Click Settings to change your settings. Click a folder icon to display its contents.

Message Center

The Message Center displays any informational or error messages that may occur.

Some browsers may not detect the existence of the MetaFrame Presentation Server Client , please igore the error message and continue to launch the application if you have already installed the MetaFrame Presentation Server Client.

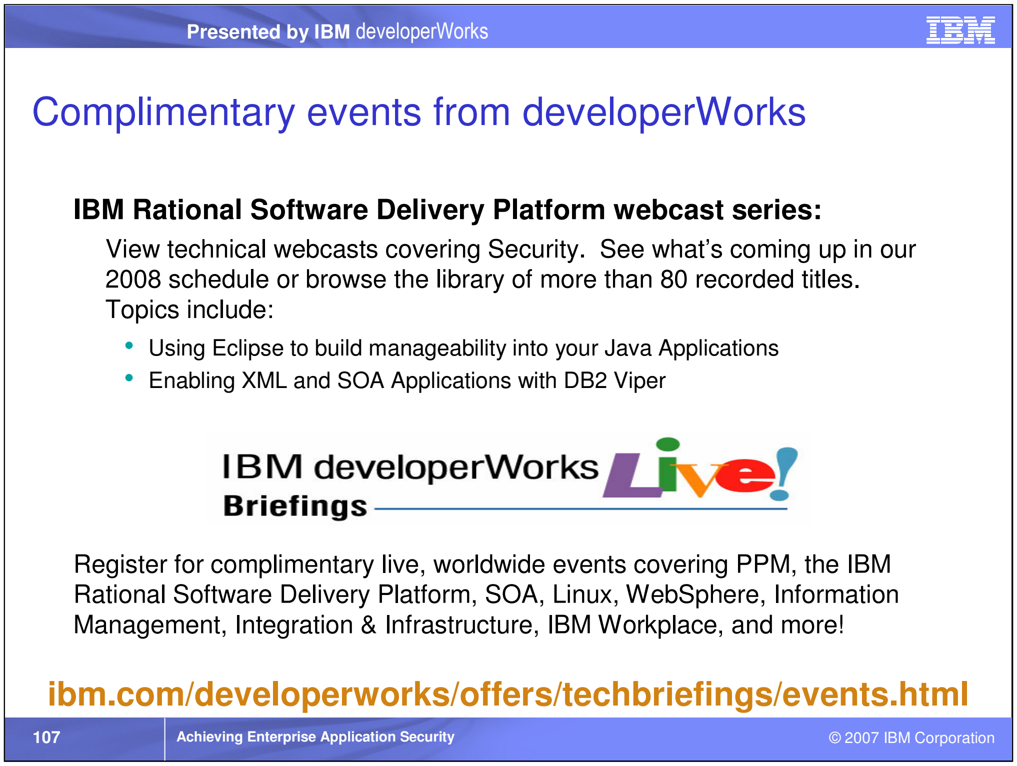
Evaluate Rational Appl. Developer without installing

New! Evaluate Rational ClearCase without installing

New! Try Rational ClearQuest as a download or online

New! IBM Rational Build Forge

ibm.com/developerWorks/onlinetrials



Presented by IBM developerWorks

Complimentary events from developerWorks

IBM Rational Software Delivery Platform webcast series:

View technical webcasts covering Security. See what's coming up in our 2008 schedule or browse the library of more than 80 recorded titles. Topics include:

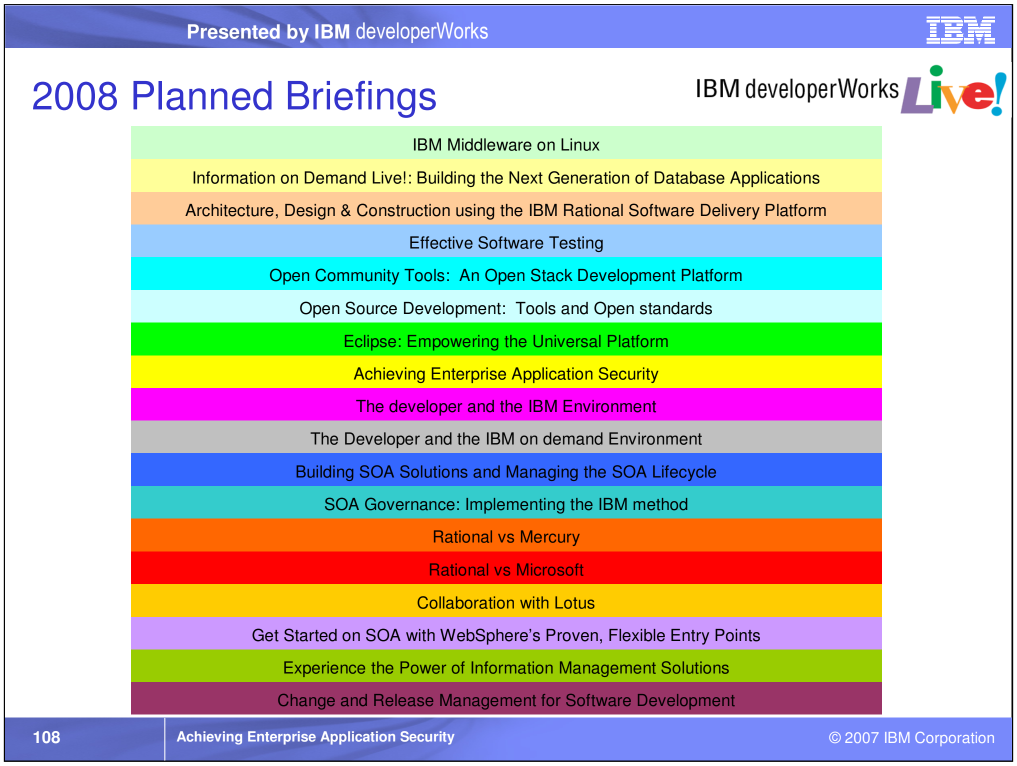
- Using Eclipse to build manageability into your Java Applications
- Enabling XML and SOA Applications with DB2 Viper

IBM developerWorks Live!
Briefings

Register for complimentary live, worldwide events covering PPM, the IBM Rational Software Delivery Platform, SOA, Linux, WebSphere, Information Management, Integration & Infrastructure, IBM Workplace, and more!

ibm.com/developerworks/offers/techbriefings/events.html

107 Achieving Enterprise Application Security © 2007 IBM Corporation

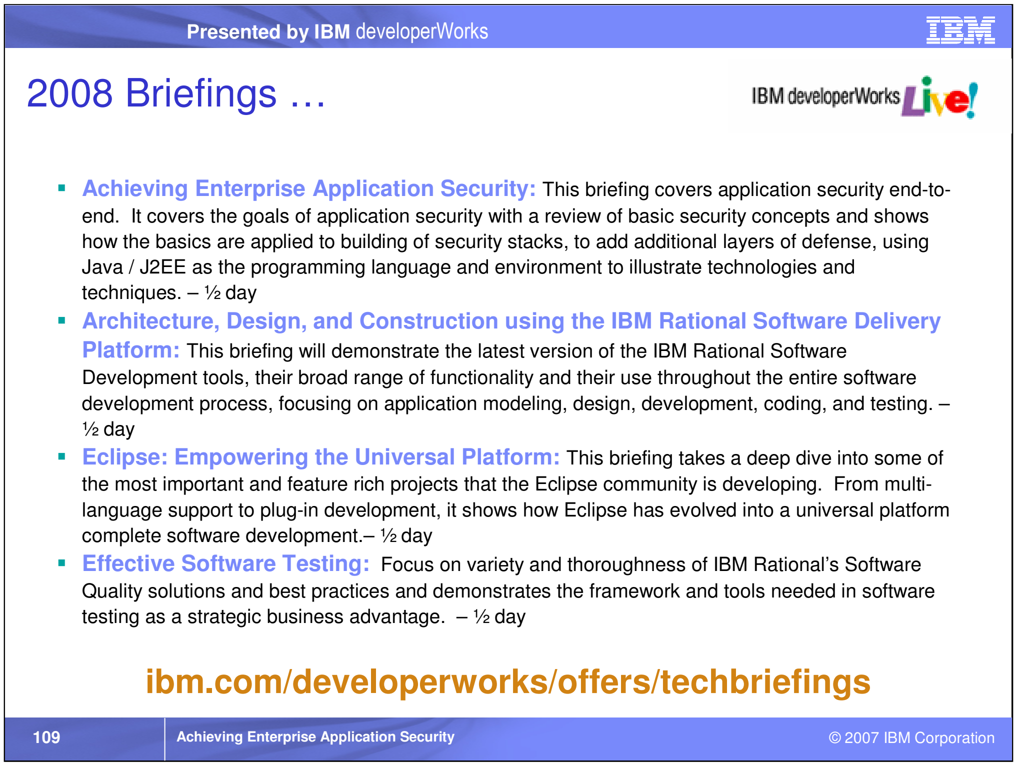


Presented by IBM developerWorks

2008 Planned Briefings

IBM developerWorks Live!

- IBM Middleware on Linux
- Information on Demand Live!: Building the Next Generation of Database Applications
- Architecture, Design & Construction using the IBM Rational Software Delivery Platform
- Effective Software Testing
- Open Community Tools: An Open Stack Development Platform
- Open Source Development: Tools and Open standards
- Eclipse: Empowering the Universal Platform
- Achieving Enterprise Application Security
- The developer and the IBM Environment
- The Developer and the IBM on demand Environment
- Building SOA Solutions and Managing the SOA Lifecycle
- SOA Governance: Implementing the IBM method
- Rational vs Mercury
- Rational vs Microsoft
- Collaboration with Lotus
- Get Started on SOA with WebSphere's Proven, Flexible Entry Points
- Experience the Power of Information Management Solutions
- Change and Release Management for Software Development



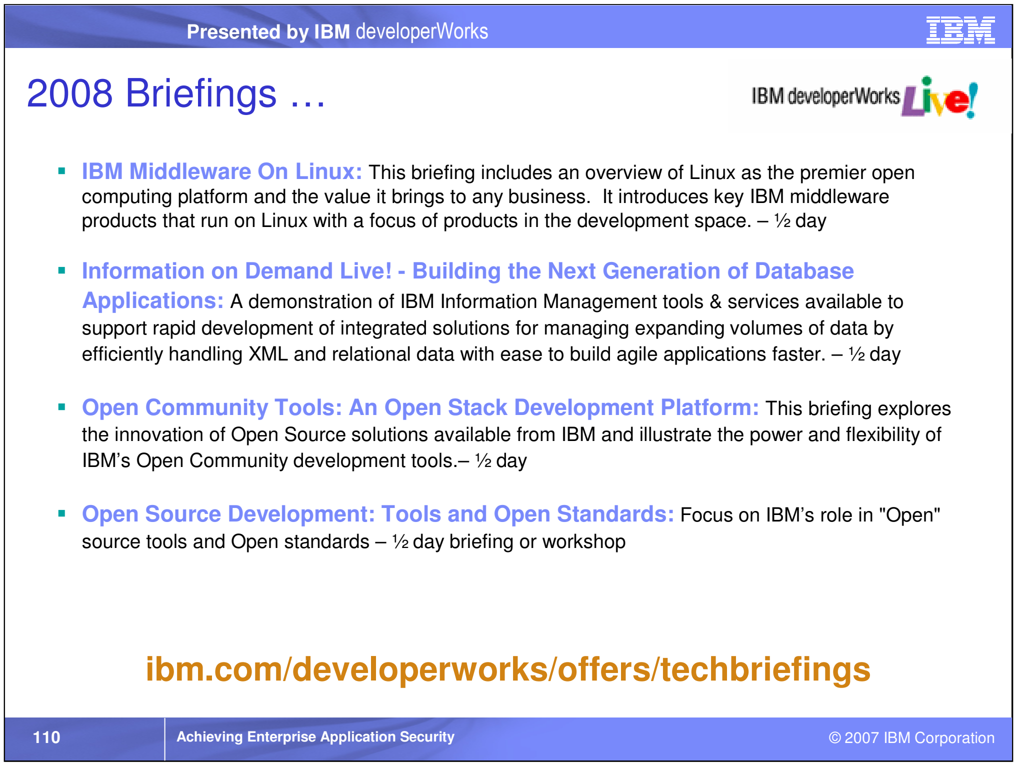
Presented by IBM developerWorks

2008 Briefings …

- **Achieving Enterprise Application Security:** This briefing covers application security end-to-end. It covers the goals of application security with a review of basic security concepts and shows how the basics are applied to building of security stacks, to add additional layers of defense, using Java / J2EE as the programming language and environment to illustrate technologies and techniques. – ½ day
- **Architecture, Design, and Construction using the IBM Rational Software Delivery Platform:** This briefing will demonstrate the latest version of the IBM Rational Software Development tools, their broad range of functionality and their use throughout the entire software development process, focusing on application modeling, design, development, coding, and testing. – ½ day
- **Eclipse: Empowering the Universal Platform:** This briefing takes a deep dive into some of the most important and feature rich projects that the Eclipse community is developing. From multi-language support to plug-in development, it shows how Eclipse has evolved into a universal platform complete software development.– ½ day
- **Effective Software Testing:** Focus on variety and thoroughness of IBM Rational's Software Quality solutions and best practices and demonstrates the framework and tools needed in software testing as a strategic business advantage. – ½ day

ibm.com/developerworks/offers/techbriefings

109 Achieving Enterprise Application Security © 2007 IBM Corporation



Presented by IBM developerWorks

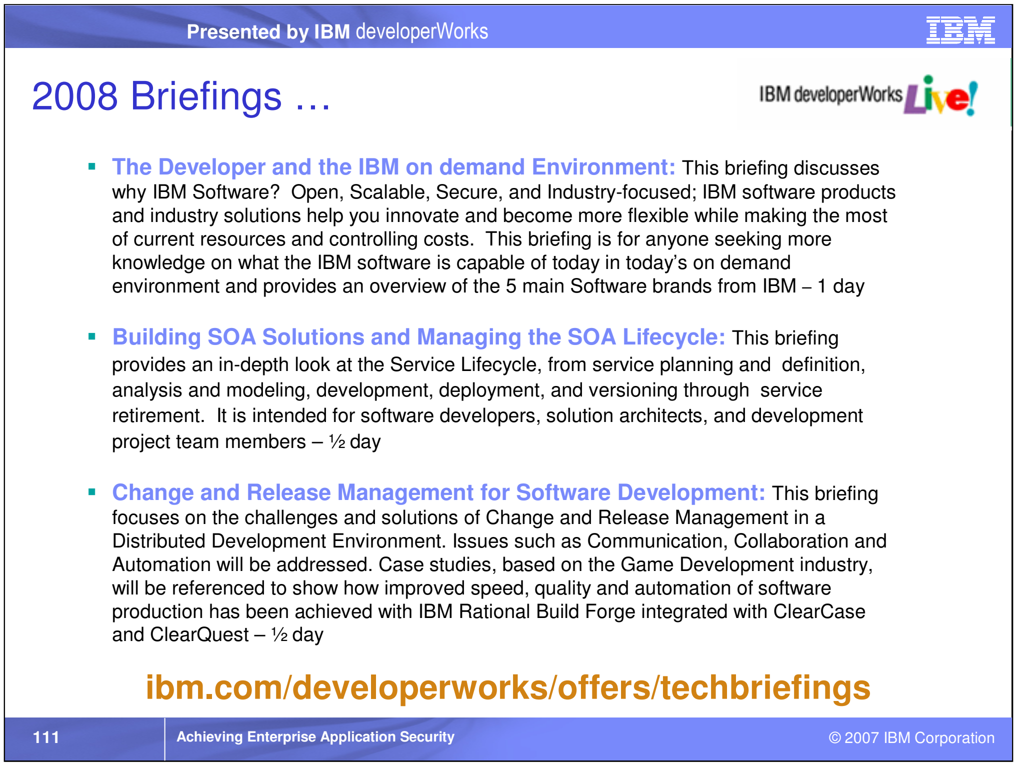
2008 Briefings …

IBM developerWorks Live!

- **IBM Middleware On Linux:** This briefing includes an overview of Linux as the premier open computing platform and the value it brings to any business. It introduces key IBM middleware products that run on Linux with a focus of products in the development space. – ½ day
- **Information on Demand Live! - Building the Next Generation of Database Applications:** A demonstration of IBM Information Management tools & services available to support rapid development of integrated solutions for managing expanding volumes of data by efficiently handling XML and relational data with ease to build agile applications faster. – ½ day
- **Open Community Tools: An Open Stack Development Platform:** This briefing explores the innovation of Open Source solutions available from IBM and illustrate the power and flexibility of IBM's Open Community development tools.– ½ day
- **Open Source Development: Tools and Open Standards:** Focus on IBM's role in "Open" source tools and Open standards – ½ day briefing or workshop

ibm.com/developerworks/offers/techbriefings

110 Achieving Enterprise Application Security © 2007 IBM Corporation



Presented by IBM developerWorks

2008 Briefings …

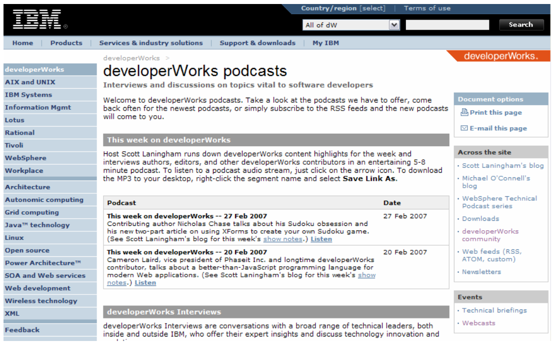
IBM developerWorks Live!

- **The Developer and the IBM on demand Environment:** This briefing discusses why IBM Software? Open, Scalable, Secure, and Industry-focused; IBM software products and industry solutions help you innovate and become more flexible while making the most of current resources and controlling costs. This briefing is for anyone seeking more knowledge on what the IBM software is capable of today in today's on demand environment and provides an overview of the 5 main Software brands from IBM – 1 day
- **Building SOA Solutions and Managing the SOA Lifecycle:** This briefing provides an in-depth look at the Service Lifecycle, from service planning and definition, analysis and modeling, development, deployment, and versioning through service retirement. It is intended for software developers, solution architects, and development project team members – ½ day
- **Change and Release Management for Software Development:** This briefing focuses on the challenges and solutions of Change and Release Management in a Distributed Development Environment. Issues such as Communication, Collaboration and Automation will be addressed. Case studies, based on the Game Development industry, will be referenced to show how improved speed, quality and automation of software production has been achieved with IBM Rational Build Forge integrated with ClearCase and ClearQuest – ½ day

ibm.com/developerworks/offers/techbriefings

111 Achieving Enterprise Application Security © 2007 IBM Corporation

developerWorks podcasts



Country/region [select] | Terms of use

All of dW | Search

Home | Products | Services & industry solutions | Support & downloads | My IBM

developerWorks >

developerWorks.

developerWorks
AIX and UNIX
IBM Systems
Information Mgmt
Lotus
Rational
Tivoli
WebSphere
Workplace
Architecture
Autonomic computing
Grid computing
Java™ technology
Linux
Open source
Power Architecture™
SOA and Web services
Web development
Wireless technology
XML
Feedback

developerWorks podcasts

Interviews and discussions on topics vital to software developers

Welcome to developerWorks podcasts. Take a look at the podcasts we have to offer, come back often for the newest podcasts, or simply subscribe to the RSS feeds and the new podcasts will come to you.

This week on developerWorks

Host Scott Laningham runs down developerWorks content highlights for the week and interviews authors, editors, and other developerWorks contributors in an entertaining 5-8 minute podcast. To listen to a podcast audio stream, just click on the arrow icon. To download the MP3 to your desktop, right-click the segment name and select **Save Link As**.

Podcast	Date
This week on developerWorks -- 27 Feb 2007 Contributing author Nicholas Chase talks about his Sudoku obsession and his new two-part article on using XForms to create your own Sudoku game. (See Scott Laningham's blog for this week's show notes.) Listen	27 Feb 2007
This week on developerWorks -- 20 Feb 2007 Cameron Laird, vice president of Phaseit Inc. and longtime developerWorks contributor, talks about a better-than-JavaScript programming language for modern Web applications. (See Scott Laningham's blog for this week's show notes.) Listen	20 Feb 2007

developerWorks Interviews

developerWorks Interviews are conversations with a broad range of technical leaders, both inside and outside IBM, who offer their expert insights and discuss technology innovation and

Document options
- Print this page
- E-mail this page

Across the site
- Scott Laningham's blog
- Michael O'Connell's blog
- WebSphere Technical Podcast series
- Downloads
- developerWorks community
- Web feeds (RSS, ATOM, custom)
- Newsletters

Events
- Technical briefings
- Webcasts

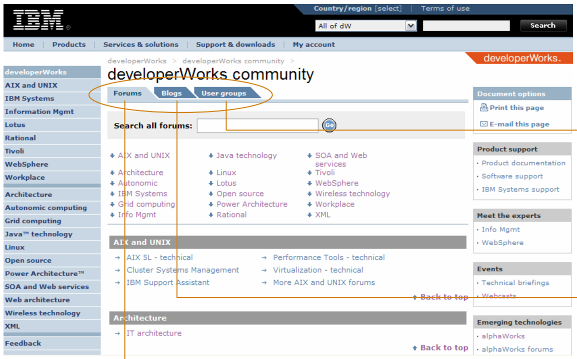
- Tune in to hear the latest MP3 recordings on a variety of technical subjects by industry experts and luminaries.
- "This week on developerWorks" podcast features developerWorks content highlights for the week and interviews authors, editors, and other developerWorks contributors in an entertaining 5-8 minute podcast.
- Other podcasts include IBM Fellow Grady Booch as he discusses innovation and evolution in IT, being an IBM Fellow, and keeping an eye on the horizon.

- Subscribe to the RSS feeds and the new developerWorks podcasts will come to you!

RSS Add custom dW RSS feeds - now improved with HTML

ibm.com/developerworks/podcast

developerWorks community resources



Country/region [select] | Terms of use

All of dW | Search

Home | Products | Services & solutions | Support & downloads | My account

developerWorks.

developerWorks > developerWorks community >

developerWorks community

Forums | Blogs | User groups

developerWorks
- AIX and UNIX
- IBM Systems
- Information Mgmt
- Lotus
- Rational
- Tivoli
- WebSphere
- Workplace
- Architecture
- Autonomic computing
- Grid computing
- Java™ technology
- Linux
- Open source
- Power Architecture™
- SOA and Web services
- Web architecture
- Wireless technology
- XML
- Feedback

Search all forums: Go

- AIX and UNIX
- Architecture
- Autonomic
- IBM Systems
- Grid computing
- Info Mgmt
- Java technology
- Linux
- Lotus
- Open source
- Power Architecture
- Rational
- SOA and Web services
- Tivoli
- WebSphere
- Wireless technology
- Workplace
- XML

AIX and UNIX
- → AIX 5L - technical
- → Cluster Systems Management
- → IBM Support Assistant
- → Performance Tools - technical
- → Virtualization - technical
- → More AIX and UNIX forums

Back to top

Architecture
- → IT architecture

Back to top

Document options
- Print this page
- E-mail this page

Product support
- Product documentation
- Software support
- IBM Systems support

Meet the experts
- Info Mgmt
- WebSphere

Events
- Technical briefings
- Webcasts

Emerging technologies
- alphaWorks
- alphaWorks forums

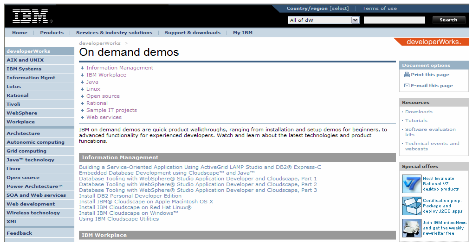
▪**User Groups:**
Join independent, user-run member-ship organizations to collaborate and learned from shared knowledge and experiences

▪**Blogs:**
Read the latest blogs from IBM & other industry experts

▪**Technical forums:**
Chat with your peers and other technical experts about IBM products and technologies

ibm.com/developerWorks/forums

Fast track your skills with On demand demos



developerWorks >

On demand demos

- Information Management
- IBM Workplace
- Java
- Linux
- Open source
- Rational
- Sample IT projects
- Web services

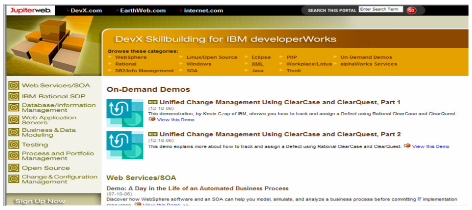
IBM on demand demos are quick product walkthroughs, ranging from installation and setup demos for beginners, to advanced functionality for experienced developers. Watch and learn about the latest technologies and product funcations.

Information Management

Building a Service-Oriented Application Using ActiveGrid LAMP Studio and DB2® Express-C
Embedded Database Development using Cloudscape™ and Java™
Database Tooling with WebSphere® Studio Application Developer and Cloudscape, Part 1
Database Tooling with WebSphere® Studio Application Developer and Cloudscape, Part 2
Database Tooling with WebSphere® Studio Application Developer and Cloudscape, Part 3
Install DB2 Personal Developer Edition
Install IBM® Cloudscape on Apple Macintosh OS X
Install IBM Cloudscape on Red Hat Linux®
Install IBM Cloudscape on Windows™
Using IBM Cloudscape Utilities

IBM Workplace

ibm.com/developerWorks/offers/lp/demos



On-Demand Demos

NEW **Unified Change Management Using ClearCase and ClearQuest, Part 1**
(12-18-06)
This demonstration, by Kevin Czap of IBM, shows you how to track and assign a Defect using Rational ClearCase and ClearQuest.
View this Demo

NEW **Unified Change Management Using ClearCase and ClearQuest, Part 2**
(12-18-06)
This demo explains more about how to track and assign a Defect using Rational ClearCase and ClearQuest. View this Demo

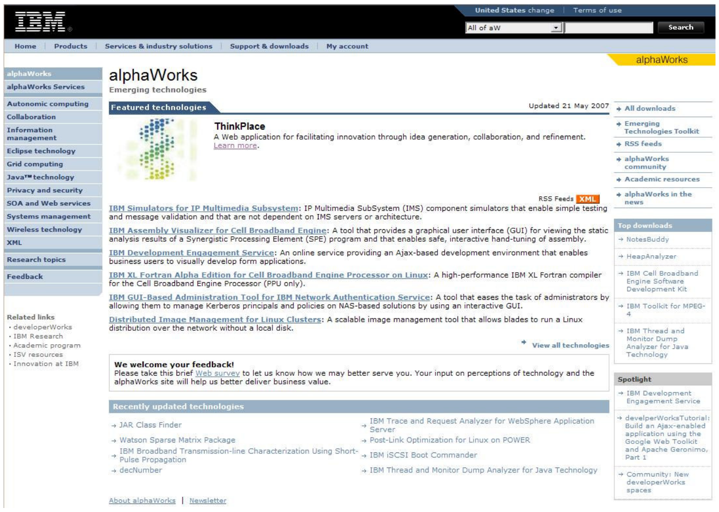
Web Services/SOA

Demo: A Day in the Life of an Automated Business Process
(07-10-06)
Discover how WebSphere software and an SOA can help you model, simulate, and analyze a business process before committing IT implementation resources. View this Demo >>

devx.com/OnDemandDemos

- Visit **developerWorks** or our partner portal on **DevX** for easy access to:
  - On demand demos featuring the latest IBM products and technology
  - Real world development scenarios
  - Technology-focused “how to” training demos
    - Short video clips
    - Beginner to advanced skill levels
  - Additional product and technical resources to accompany each demo

alphaWorks emerging technologies



United States change | Terms of use

All of aW | Search

Home | Products | Services & industry solutions | Support & downloads | My account

alphaWorks

- alphaWorks
- alphaWorks Services
- Autonomic computing
- Collaboration
- Information management
- Eclipse technology
- Grid computing
- Java™ technology
- Privacy and security
- SOA and Web services
- Systems management
- Wireless technology
- XML
- Research topics
- Feedback

Related links

- developerWorks
- IBM Research
- Academic program
- ISV resources
- Innovation at IBM

alphaWorks

Emerging technologies

Featured technologies

Updated 21 May 2007

ThinkPlace

A Web application for facilitating innovation through idea generation, collaboration, and refinement. Learn more.

RSS Feeds XML

IBM Simulators for IP Multimedia Subsystem: IP Multimedia SubSystem (IMS) component simulators that enable simple testing and message validation and that are not dependent on IMS servers or architecture.

IBM Assembly Visualizer for Cell Broadband Engine: A tool that provides a graphical user interface (GUI) for viewing the static analysis results of a Synergistic Processing Element (SPE) program and that enables safe, interactive hand-tuning of assembly.

IBM Development Engagement Service: An online service providing an Ajax-based development environment that enables business users to visually develop form applications.

IBM XL Fortran Alpha Edition for Cell Broadband Engine Processor on Linux: A high-performance IBM XL Fortran compiler for the Cell Broadband Engine Processor (PPU only).

IBM GUI-Based Administration Tool for IBM Network Authentication Service: A tool that eases the task of administrators by allowing them to manage Kerberos principals and policies on NAS-based solutions by using an interactive GUI.

Distributed Image Management for Linux Clusters: A scalable image management tool that allows blades to run a Linux distribution over the network without a local disk.

→ View all technologies

We welcome your feedback!
Please take this brief Web survey to let us know how we may better serve you. Your input on perceptions of technology and the alphaWorks site will help us better deliver business value.

Recently updated technologies

- JAR Class Finder
- Watson Sparse Matrix Package
- IBM Broadband Transmission-line Characterization Using Short-Pulse Propagation
- decNumber
- IBM Trace and Request Analyzer for WebSphere Application Server
- Post-Link Optimization for Linux on POWER
- IBM iSCSI Boot Commander
- IBM Thread and Monitor Dump Analyzer for Java Technology

About alphaWorks | Newsletter

- All downloads
- Emerging Technologies Toolkit
- RSS feeds
- alphaWorks community
- Academic resources
- alphaWorks in the news

Top downloads

- NotesBuddy
- HeapAnalyzer
- IBM Cell Broadband Engine Software Development Kit
- IBM Toolkit for MPEG-4
- IBM Thread and Monitor Dump Analyzer for Java Technology

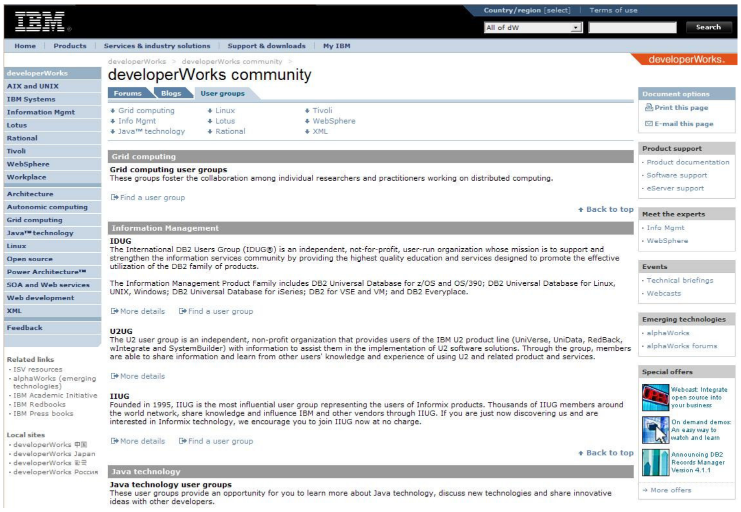
Spotlight

- IBM Development Engagement Service
- develperWorksTutorial: Build an Ajax-enabled application using the Google Web Toolkit and Apache Geronimo, Part 1
- Community: New developerWorks spaces

alphaWorks.ibm.com

Presented by IBM developerWorks

User Group Communities



Home | Products | Services & industry solutions | Support & downloads | My IBM

Country/region [select] | Terms of use

All of dW | Search

developerWorks.

developerWorks > developerWorks community >

developerWorks community

Forums | Blogs | User groups

- Grid computing
- Info Mgmt
- Java™ technology
- Linux
- Lotus
- Rational
- Tivoli
- WebSphere
- XML

Grid computing

Grid computing user groups
These groups foster the collaboration among individual researchers and practitioners working on distributed computing.

Find a user group

Back to top

Information Management

IDUG
The International DB2 Users Group (IDUG®) is an independent, not-for-profit, user-run organization whose mission is to support and strengthen the information services community by providing the highest quality education and services designed to promote the effective utilization of the DB2 family of products.

The Information Management Product Family includes DB2 Universal Database for z/OS and OS/390; DB2 Universal Database for Linux, UNIX, Windows; DB2 Universal Database for iSeries; DB2 for VSE and VM; and DB2 Everyplace.

More details | Find a user group

U2UG
The U2 user group is an independent, non-profit organization that provides users of the IBM U2 product line (UniVerse, UniData, RedBack, wIntegrate and SystemBuilder) with information to assist them in the implementation of U2 software solutions. Through the group, members are able to share information and learn from other users' knowledge and experience of using U2 and related product and services.

More details

IIUG
Founded in 1995, IIUG is the most influential user group representing the users of Informix products. Thousands of IIUG members around the world network, share knowledge and influence IBM and other vendors through IIUG. If you are just now discovering us and are interested in Informix technology, we encourage you to join IIUG now at no charge.

More details | Find a user group

Back to top

Java technology

Java technology user groups
These user groups provide an opportunity for you to learn more about Java technology, discuss new technologies and share innovative ideas with other developers.

developerWorks
- AIX and UNIX
- IBM Systems
- Information Mgmt
- Lotus
- Rational
- Tivoli
- WebSphere
- Workplace
- Architecture
- Autonomic computing
- Grid computing
- Java™ technology
- Linux
- Open source
- Power Architecture™
- SOA and Web services
- Web development
- XML
- Feedback

Related links
- ISV resources
- alphaWorks (emerging technologies)
- IBM Academic Initiative
- IBM Redbooks
- IBM Press books

Local sites
- developerWorks 中国
- developerWorks Japan
- developerWorks 한국
- developerWorks Россия

Document options
- Print this page
- E-mail this page

Product support
- Product documentation
- Software support
- eServer support

Meet the experts
- Info Mgmt
- WebSphere

Events
- Technical briefings
- Webcasts

Emerging technologies
- alphaWorks
- alphaWorks forums

Special offers
- Webcast: Integrate open source into your business
- On demand demos: An easy way to watch and learn
- Announcing DB2 Records Manager Version 4.1.1

→ More offers

ibm.com/developerworks/usergroups

IBM Software User Group Community

Tivoli

- All Tivoli software user communities: http://www-306.ibm.com/software/tivoli/tivoli_user_groups/community.html
- Global Software User Group community: www.tivoli-ug.org

WebSphere

- Global WebSphere User Group community: www.websphere.org

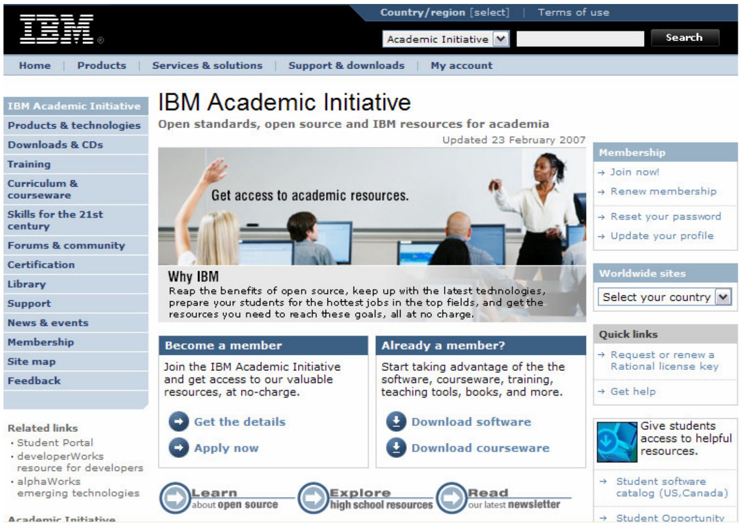
Information Management

- Enterprise Content Management/UserNet: http://www.filenet.com/usergroup
- U2 User Groups: http://www.u2ug.org

Rational

- Global Rational User Group community: www.rational-ug.org

IBM Academic Initiative



Country/region [select] | Terms of use
Academic Initiative
Search
Home | Products | Services & solutions | Support & downloads | My account

IBM Academic Initiative
Products & technologies
Downloads & CDs
Training
Curriculum & courseware
Skills for the 21st century
Forums & community
Certification
Library
Support
News & events
Membership
Site map
Feedback

Related links
- Student Portal
- developerWorks resource for developers
- alphaWorks emerging technologies

Academic Initiative

IBM Academic Initiative

Open standards, open source and IBM resources for academia

Updated 23 February 2007

Why IBM

Reap the benefits of open source, keep up with the latest technologies, prepare your students for the hottest jobs in the top fields, and get the resources you need to reach these goals, all at no charge.

Become a member

Join the IBM Academic Initiative and get access to our valuable resources, at no-charge.

- Get the details
- Apply now

Already a member?

Start taking advantage of the the software, courseware, training, teaching tools, books, and more.

- Download software
- Download courseware

Learn about open source
Explore high school resources
Read our latest newsletter

Membership

- → Join now!
- → Renew membership
- → Reset your password
- → Update your profile

Worldwide sites

Select your country

Quick links

- → Request or renew a Rational license key
- → Get help

Give students access to helpful resources.

- → Student software catalog (US,Canada)
- → Student Opportunity

ibm.com/university/scholars/academicinitiative

SAVE THE DATE!
WHERE TEAMS ARE R-HEROES
RU READY TO SAVE THE DAY?

Presented by IBM developerWorks

IBM Rational Software Development Conference

June 1-5, 2008
Walt Disney World Swan and Dolphin
Orlando, Florida

- Attend the 2008 Executive Summit
- Over 300 Sessions – 14 Tracks
- 3 & 5 Hour Technical Workshops
- Keynotes with Industry Leading Experts
- Exhibit Hall Showcasing Complimentary Product and Services
- Unlimited Networking Opportunities
- Access to the Executive Summit
- BOA Workgroup Sessions
- IBM Solution Center
- Interactive Birds-of-a-Feather Sessions
- Evening Receptions
- Over 3,000 Customers and Partners
- Access to IBM Engineers & IBM Research

Register with this discount code (HDDE) and receive $100 off your registration fee!

Visit **www.ibm.com/rational/rsdc** for more information

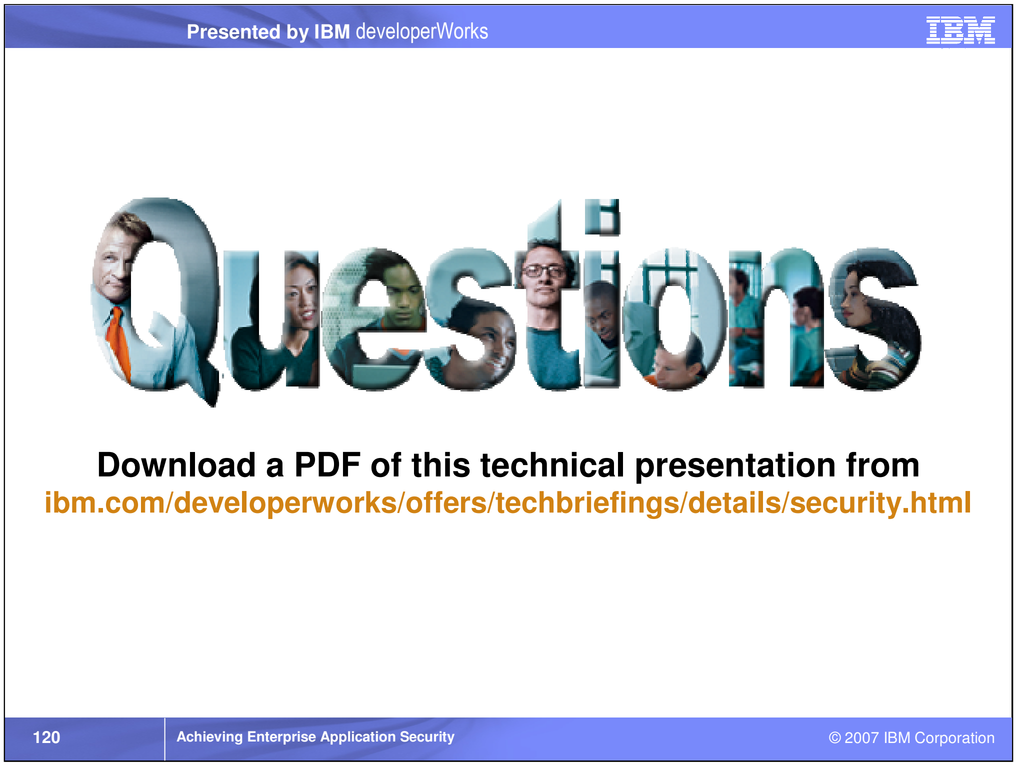
Brand Awareness

Creates a community online before RSDC

Attendees make their own videos and webcam videos about WHAT KEEPS THEM RATIONAL? I.e., what products, services, and/or results of these that keeps them sane on the job… in other words, what keeps them part of the Rational Family… keeps them coming to RSDC year after year.

Now… not all the video blogging will be done BEFORE the event.

We can have some hotly contested video blogging gong on AT the event as well.



Presented by **IBM** developerWorks

Questions

Download a PDF of this technical presentation from
ibm.com/developerworks/offers/techbriefings/details/security.html

120 Achieving Enterprise Application Security © 2007 IBM Corporation

Presented by IBM developerWorks

Thank You

121

Achieving Enterprise Application Security

© 2007 IBM Corporation