E-COMMERCE and SECURITY - 1DL018

Spring 2008

An introductory course on e-commerce systems

alt. http://www.it.uu.se/edu/course/homepage/ehandel/vt08/

Kjell Orsborn
Uppsala Database Laboratory
Department of Information Technology, Uppsala University,
Uppsala, Sweden
Online security

ch 11

Kjell Orsborn

Department of Information Technology
Uppsala University, Uppsala, Sweden
The E-commerce Security Environment: The Scope of the Problem

- Overall size of cybercrime unclear; amount of losses significant but stable; individuals face new risks of fraud that may involve substantial uninsured losses
  - Symantec: Cybercrime on the rise from 2006
  - Internet Crime Complaint Center (IC3): Logged 1 000 000+ consumer complaints about alleged online fraud or cyber crime and referred 460,000+ complaints to law enforcement agencies
  - 2007 Computer Security Institute (CSI) survey: 46% detected security breach; 91% suffered financial loss as a result. The average annual loss reported in this year’s survey shot up to $350,424 from $168,000 the previous year.
  - Underground economy marketplace that offers sales of stolen information growing.
Cybercrime: types of attacks against computer systems

E-commerce,
Laudon,
4th & 3rd ed.

- Insider abuse: 59%
- Virus: 52%
- Nigerian letter fraud: 50%
- Laptop/mobile device theft: 26%
- Phishing: 25%
- IM misuse: 25%
- Denial of service: 25%
- Unauthorized access to information: 21%
- Bots: 17%
- Theft of data: 17%
- Abuse of wireless network: 13%
- Financial fraud: 12%
- Password sniffing: 10%
- Web site defacement: 10%

CSI, 2005
The E-commerce Security Environment

- Data
- Technology solutions
- Policies and procedures
- Laws and standards
The Different Dimensions of E-commerce Security
(E-commerce, Laudon, 3rd ed., 2007)

• Integrity
  – The ability to ensure that information being displayed on a web site or transmitted or received over the internet has not been altered in any way by an unauthorized party

• Nonrepudiation
  – The ability to ensure that e-commerce participants do not deny (i.e. repudiate) their online actions

• Authenticity
  – The ability to identify the identity of a person or entity with whom you are dealing in the internet

• Confidentiality
  – The ability to ensure that messages and data are available only to those who are authorized to view them

• Privacy
  – The ability to control the use of information about oneself

• Availability
  – The ability to ensure that an e-commerce site continues to function as intended
The Different Dimensions of E-commerce Security
(E-commerce, Laudon, 3rd ed., 2007)

<table>
<thead>
<tr>
<th>DIMENSIONS</th>
<th>CUSTOMER’S PERSPECTIVE</th>
<th>MERCHANT’S PERSPECTIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>Has information I transmit or receive been altered?</td>
<td>Has data on the site been altered without authorization? Is data being received from customers valid?</td>
</tr>
<tr>
<td>Nonrepudiation</td>
<td>Can a party to an action with me later deny taking the action?</td>
<td>Can a customer deny ordering products?</td>
</tr>
<tr>
<td>Authenticity</td>
<td>Who am I dealing with? How can I be assured that the person or entity is who they claim to be?</td>
<td>What is the real identity of the customer?</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Can someone other than the intended recipient read my messages?</td>
<td>Are messages or confidential data accessible to anyone other than those authorized to view them?</td>
</tr>
<tr>
<td>Privacy</td>
<td>Can I control the use of information about myself transmitted to an e-commerce merchant?</td>
<td>What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?</td>
</tr>
<tr>
<td>Availability</td>
<td>Can I get access to the site?</td>
<td>Is the site operational?</td>
</tr>
</tbody>
</table>
The tension between security and other values

- **Security vs. ease of use:**
  - the more security measures added, the more difficult a site is to use, and the slower it becomes

- **Security vs. desire of individuals to act anonymously**
Security Threats in the E-commerce Environment

• Three key points of vulnerability:
  – Client
  – Server
  – Communications channel
A Typical E-commerce Transaction

Vulnerable Points in an E-commerce Environment

**Security Risks**

**Internet communications**

**Servers**
- ISP
- Merchant
- Banks

**Clients**
- Business
- Home

- Tapping and sniffing
- Alteration of messages
- Theft and fraud

- DoS attack
- Hacking
- Malicious code attack
- Theft and fraud
- Line taps
- Vandalism

- Malicious code attack
- Line taps
- Physical loss of computer

**SOURCE:** Boncella, 2000.
Malicious Code

- **Viruses:**
  - Have ability to replicate and spread to other files; most also deliver a “payload” of some sort (destructive or benign); include macro viruses, file-infecting viruses, and script viruses

- **Worms:**
  - Designed to spread from computer to computer

- **Trojan horse:**
  - Appears to be benign, but then does something other than expected

- **Bots:**
  - Can be covertly installed on computer; responds to external commands sent by the attacker
Unwanted Programs

• Installed without the user’s informed consent
  – Browser parasites: Can monitor and change settings of a user’s browser
  – Adware: Calls for unwanted pop-up ads
  – Spyware: Can be used to obtain information, such as a user’s keystrokes, e-mail, IMs, etc.
Phishing and Identity Theft

• Any deceptive, online attempt by a third party to obtain confidential information for financial gain
  – Most popular type: e-mail scam letter
  – One of fastest growing forms of e-commerce crime
Hacking and Cybervandalism

- **Hacker**: Individual who intends to gain unauthorized access to computer systems
- **Cracker**: Hacker with criminal intent (two terms often used interchangeably)
- **Cybervandalism**: Intentionally disrupting, defacing or destroying a Web site
- **Types of hackers include:**
  - White hats
  - Black hats
  - Grey hats
Credit Card Fraud

• Fear that credit card information will be stolen deters online purchases
• Hackers target credit card files and other customer information files on merchant servers; use stolen data to establish credit under false identity
• One solution: New identity verification mechanisms
Spoofing (Pharming) and Spam (Junk) Web Sites

- **Spoofing (Pharming)**
  - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
  - Threatens integrity of site; authenticity

- **Spam (Junk) Web sites**
  - Use domain names similar to legitimate one, redirect traffic to spammer-redirection domains
DoS and DDoS Attacks

• Denial of service (DoS) attack
  – Hackers flood Web site with useless traffic to inundate and overwhelm network

• Distributed denial of service (DDoS) attack
  – Hackers use numerous computers to attack target network from numerous launch points
Other Security Threats

• Sniffing: Type of eavesdropping program that monitors information traveling over a network; enables hackers to steal proprietary information from anywhere on a network
• Insider jobs: Single largest financial threat
• Poorly designed server and client software: Increase in complexity of software programs has contributed to increase in vulnerabilities that hackers can exploit
Technology Solutions

- Protecting Internet communications (encryption)
- Securing channels of communication (SSL, S-HTTP, VPNs)
- Protecting networks (firewalls)
- Protecting servers and clients
Tools Available to Achieve Site Security

- Encryption
- Firewalls
- Security Tools
- Network Security Protocols
- Access Controls
- Virtual Private Networks
- Authentication
- Tunneling
- Proxy/Agent Systems
- Intrusion Detection

Security Management
Protecting Internet Communications: Encryption

- **Encryption:**
  - Process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and receiver
- **Purpose:**
  - Secure stored information and information transmission
- **Provides:**
  - Message integrity
  - Nonrepudiation
  - Authentication
  - Confidentiality
Symmetric Key Encryption

- Also known as secret key encryption
- Both the sender and receiver use the same digital key to encrypt and decrypt message
- Requires a different set of keys for each transaction
- Advanced Encryption Standard (AES):
  - Most widely used symmetric key encryption today; offers 128-, 192-, and 256-bit encryption keys; other standards use keys with up to 2,048 bits
Public Key Encryption

• Solves symmetric key encryption problem of having to exchange secret key
• Uses two mathematically related digital keys – public key (widely disseminated) and private key (kept secret by owner)
• Both keys used to encrypt and decrypt message
• Once key used to encrypt message, same key cannot be used to decrypt message
• For example, sender uses recipient’s public key to encrypt message; recipient uses his/her private key to decrypt it
Public Key Cryptography – A Simple Case

1. Original message

Buy Cisco @ $25

2. Recipient's public key

3. Message encrypted in cipher text

10101101110001

4. Internet

5. Recipient's private key

Buy Cisco @ $25

Sender

Recipient
Public Key Encryption using Digital Signatures and Hash Digests

• Application of hash function (mathematical algorithm) by sender prior to encryption produces hash digest that recipient can use to verify integrity of data

• Double encryption with sender’s private key (digital signature) helps ensure authenticity and nonrepudiation
Public Key Cryptography with Digital Signatures

1. Original message

2. Hash function

3. Recipient's public key

4. Sender's private key (digital signature)

5. Signed cipher text

6. Sender's public key

7. Recipient's private key

Cipher text (including hash digest)

Authenticated cipher text

Buy XYZ @ $52
Digital Envelopes

• Addresses weaknesses of public key encryption (computationally slow, decreases transmission speed, increases processing time) and symmetric key encryption (faster, but more secure)

• Uses symmetric key encryption to encrypt document but public key encryption to encrypt and send symmetric key
Public Key Cryptography: Creating a Digital Envelope
Digital Certificates and Public Key Infrastructure (PKI)

• Digital certificate includes:
  – Name of subject/company
  – Subject’s public key
  – Digital certificate serial number
  – Expiration date
  – Issuance date
  – Digital signature of certification authority (trusted third party institution) that issues certificate
  – Other identifying information

• Public Key Infrastructure (PKI): refers to the CAs and digital certificate procedures that are accepted by all parties
Digital Certificates and Certification Authorities
Limits to Encryption Solutions

• PKI applies mainly to protecting messages in transit
• PKI is not effective against insiders
• Protection of private keys by individuals may be haphazard
• No guarantee that verifying computer of merchant is secure
• CAs are unregulated, self-selecting organizations
Securing Channels of Communication

• **Secure Sockets Layer (SSL):**
  – Most common form of securing channels of communication; used to establish a secure negotiated session (client-server session in which URL of requested document, along with contents, is encrypted)

• **S-HTTP:**
  – Alternative method; provides a secure message-oriented communications protocol designed for use in conjunction with HTTP

• **Virtual Private Networks (VPNs):**
  – Allow remote users to securely access internal networks via the Internet, using Point-to-Point Tunneling Protocol (PPTP)
Secure Negotiated Sessions Using SSL

Session ID and methods of encryption negotiated.
Certificates exchanged. Identity of both parties established.
Client generates session key, and uses server public key to create digital envelope. Sends to server. Server decrypts using private key.
Encrypted transmission using client-generated session key begins.
Protecting Networks: Firewalls and Proxy Servers

• Firewall: Hardware or software filters communications packets; prevents some packets from entering the network based on a security policy

• Firewall methods include:
  – Packet filters
  – Application gateways

• Proxy servers: Software servers that handle all communications originating from or being sent to the Internet
Firewalls and Proxy Servers

Firewall

- Clients
- Firewall
- Web Server
- Remote Client
- Internet
- Remote Server

Proxy Server

- Clients
- Internal Network
- Proxy Server
- External Network
- Internet
- Remote Client
- Remote Server
Protecting Servers and Clients

• Operating system controls: Authentication and access control mechanisms
• Anti-virus software: Easiest and least expensive way to prevent threats to system integrity
Policies, Procedures & Law: Developing an E-commerce Security Plan

1. Perform a risk assessment
2. Develop a security policy
3. Develop an implementation plan
4. Create a security organization
5. Perform a security audit
Types of Payment Systems

• Cash
• Checking Transfer
• Credit Card
• Stored Value
• Accumulating Balance
Cash

- Legal tender
- Most common form of payment in terms of number of transactions
- Instantly convertible into other forms of value without intermediation
- Portable, requires no authentication
- “Free” (no transaction fee), anonymous, low cognitive demands
- Limitations: easily stolen, limited to smaller transaction, does not provide any float
Checking Transfer

- Funds transferred directly via signed draft/check from a consumer’s checking account to merchant/other individual
- Most common form of payment in terms of amount spent
- Can be used for small and large transactions
- Some float
- Not anonymous, requires third-party intervention (banks)
- Introduces security risks for merchants (forgeries, stopped payments), so authentication typically required
Credit Card

• Represents account that extends credit to consumers; allows consumers to make payments to multiple vendors at one time

• Credit card associations:
  – Nonprofit associations (Visa, MasterCard) that set standards for issuing banks

• Issuing banks: Issue cards and process transactions

• Processing centers (clearinghouses): Handle verification of accounts and balances
Stored Value

- Accounts created by depositing funds into an account and from which funds are paid out or withdrawn as needed
  - Examples: Debit cards, gift certificates, prepaid cards, smart cards
  - Peer-to-peer payment systems such as PayPal a variation
Accumulating Balance

- Accounts that accumulate expenditures and to which consumers make period payments
  - Examples: Utility, phone, American Express accounts
### Dimensions of Payment Systems

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Cash</th>
<th>Personal Check</th>
<th>Credit Card</th>
<th>Stored Value (Debit Card)</th>
<th>Accumulating Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instantly convertible without...</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Low transaction cost for small...</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Low transaction cost for large...</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Low fixed costs for merchant</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Refutable (able to be repudiated)</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no (usually)</td>
<td>yes</td>
</tr>
<tr>
<td>Financial risk for consumer</td>
<td>yes</td>
<td>no</td>
<td>up to $50</td>
<td>limited</td>
<td>no</td>
</tr>
<tr>
<td>Financial risk for merchant</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Anonymous for consumer</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Anonymous for merchant</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Immediately respondable</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Security against unauthorized use</td>
<td>no</td>
<td>some</td>
<td>some</td>
<td>some</td>
<td>some</td>
</tr>
<tr>
<td>Tamper-resistant</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Requires authentication</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Special hardware required</td>
<td>no</td>
<td>no</td>
<td>yes—by merchant</td>
<td>yes—by merchant</td>
<td>yes—by merchant</td>
</tr>
<tr>
<td>Buyer keeps float</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Account required</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Has immediate monetary value</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>
E-commerce Payment Systems

• Credit cards are dominant form of online payment, accounting for around 70% of online payments in 2007

• Other e-commerce payment systems:
  – Digital cash
  – Online stored value systems
  – Digital accumulating balance payment systems
  – Digital credit accounts
  – Digital checking
How an Online Credit Transaction Works

1. Consumer makes purchase
2. SSL provides secure connection through Internet to merchant server
3. Merchant software contacts clearinghouse
4. Clearinghouse verifies account and balance with issuing bank
5. Issuing bank credits merchant account
6. Monthly statement issued with debit for purchase

MERCHANT

CLEARINGHOUSE

MERCHANT BANK

CONSUMER’S CARD ISSUING BANK

Secure line
Limitations of Online Credit Card Payment Systems

- **Security**: neither merchant nor consumer can be fully authenticated
- **Cost**: for merchants, around 3.5% of purchase price plus transaction fee of 20 – 30 cents per transaction
- **Social equity**: many people do not have access to credit cards
Digital Wallets

• Seeks to emulate the functionality of traditional wallet
• Most important functions:
  – Authenticate consumer through use of digital certificates or other encryption methods
  – Store and transfer value
  – Secure payment process from consumer to merchant
• Early efforts to popularize have failed
• Newest effort: Google Checkout
Digital Cash

• One of the first forms of alternative payment systems
• Not really “cash”: rather, form of value storage and value exchange that has limited convertibility into other forms of value, and requires intermediaries to convert
• Most early examples have disappeared; concepts survive as part of P2P payment systems
Online Stored Value Systems

• Permit consumers to make instant, online payments to merchants and other individuals based on value stored in an online account
• Rely on value stored in a consumer’s bank, checking, or credit card account
• PayPal most successful system
• Smart cards another example
  – Contact and contactless
  – Mondex, Octopus
Digital Accumulating Balance Payment Systems

• Allows users to make micropayments and purchases on the Web, accumulating a debit balance for which they are billed at the end of the month

• Examples: Valista’s PaymentsPlus, Clickshare
Digital Checking Payment Systems

- Extends functionality of existing checking accounts for use as online shopping payment tool
- Example: PayByCheck
Wireless Payment Systems

- Use of mobile handsets as payment devices well-established in Europe, Japan, South Korea
- Not very well established yet in U.S, but with growth in Wi-Fi and 3G cellular phone systems, this is beginning to change
Electronic Billing Presentment and Payment (EBPP)

- Online payment systems for monthly bills
- EBPP expected to grow rapidly, to an estimated 40% of all households by 2007
- Main business models in EBPP market include:
  - Biller-direct
  - Consolidator
- Above are supported by EBPP infrastructure providers
Cryptography

• One of the strongest tools in the developer’s arsenal
• Many commercial products
• Still some restrictions on export
• Long history from Roman times
• Technologies based on encryption
• Some encryption-based technologies
  – Message digest functions
  – Digital signatures
  – Digital certificates
Symmetric key encryption

- The sender of secure data encrypts the data using an algorithm which depends on its operation on a key.
- The encrypted data is sent over some insecure medium such as the Internet.
- The key is conveyed to the recipient of the message using some secure method.
- The recipient receives the key and then uses it to decrypt the message that has been received.
- Symmetric algorithms
  - Large number
  - DES and Triple DES (3DES) are the most popular
  - Takes a lot of effort to crack
  - All algorithms are very efficient
Asymmetric cryptography

• Also known as public key cryptography
• Keys must be generated in pairs and it must be computationally infeasible to obtain one key from the other key alone.
• Information that is encrypted by one key can be decrypted only by the other key of the key pair, and information decrypted by one of the keys could only have been encrypted by the other key of the key pair.
• Two keys a public key and a private key
• The process of asymmetric encryption
  – A user publishes their public key, for example on their Web site.
  – Anyone who wants to send a message to the recipient uses the public key to carry out encryption.
  – The encrypted text is processed by the recipient who applies a decryption algorithm which employs the secret key.
• Some technologies:
  – Diffie Hellman Key exchange, RSA, ElGamal, The digital signature standard
Properties

• When they use sufficiently large keys both methods are secure.
• Public key encryption is easier to implement because there is no need to worry about transmitting keys over some secure medium.
• The processing power required for symmetric key encryption is much lower than for public key encryption. This means that for the bulk transmission of data symmetric key encryption is normally preferred.
Some products

- PGP
- PCT (dying)
- SHTTP (dying out)
- SET for credit card payments
- SSL the most popular
- DNSSEC
SSL

• Secure Sockets Layer
• Most popular cryptographic technology
• Supports both symmetric and asymmetric methods
• Wide variety of algorithms: DES, DSA, RSA, MD5
• Uses public key cryptography to start communication and establish protocol parameters
• Uses symmetric cryptography for bulk transfer
• Authorisation at both the client and server
Java SE Security Overview

- Underlying the Java SE Platform is a dynamic, extensible security architecture, standards-based and interoperable.
- Security features – cryptography, authentication and authorization, public key infrastructure, and more – are built in.
- The Java security model is based on a customizable "sandbox" in which Java software programs can run safely, without potential risk to systems or users.
## Java SE Security Overview

<table>
<thead>
<tr>
<th>High-level Features</th>
<th>Low-level Features</th>
<th>Benefits</th>
<th>References</th>
</tr>
</thead>
</table>
| Platform Security   | Built-in language security features enforced by the Java compiler and virtual machine: | Provides a safe and secure platform for developing and running applications. Compile-time data type checking and automatic memory management leads to more robust code and reduces memory corruption and vulnerabilities. Bytecode verification ensures code conforms to the JVM specification and prevents hostile code from corrupting the runtime environment. Class loaders ensure that untrusted code cannot interfere with the running of other Java programs. | • The Java Language Specification  
• The Java Virtual Machine Specification |
### Java SE Security Overview

<table>
<thead>
<tr>
<th>High-level Features</th>
<th>Low-level Features</th>
<th>Benefits</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cryptography</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Comprehensive API with support for a wide range of cryptographic services including digital signatures, message digests, ciphers (symmetric, asymmetric, stream &amp; block), message authentication codes, key generators and key factories</td>
<td>Provides an extensible, full featured API for building secure applications:</td>
<td>• Java Cryptography Architecture (JCA) (includes the Java Cryptographic Extension (JCE))</td>
</tr>
<tr>
<td></td>
<td>• Support for a wide range of standard algorithms including RSA, DSA, AES, Triple DES, SHA, PKCS#5, RC2, and RC4.</td>
<td>• Algorithm and implementation independent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PKCS#11 cryptographic token support</td>
<td>• Provider-based (pluggable) architecture</td>
<td></td>
</tr>
</tbody>
</table>
## Java SE Security Overview

<table>
<thead>
<tr>
<th>High-level Features</th>
<th>Low-level Features</th>
<th>Benefits</th>
<th>References</th>
</tr>
</thead>
</table>
| Authentication and Access Control | • Abstract authentication APIs that can incorporate a wide range of login mechanisms through a pluggable architecture.  
• A comprehensive policy and permissions API that allows the developer to create and administer applications requiring fine-grained access to security-sensitive resources. | Enables single sign-on of multiple authentication mechanisms and fine-grained access to resources based on the identity of the user or code signer. Recent support (in JDK 5) for timestamped signatures makes it easier to deploy signed code by avoiding the need to re-sign code when the signer's certificate expires. | • Java Security Architecture  
• Java Authentication and Authorization Service (JAAS)  
• Policy Implementation and Syntax  
• Signature Timestamp Support |
Java SE Security Overview …

<table>
<thead>
<tr>
<th>High-level Features</th>
<th>Low-level Features</th>
<th>Benefits</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Communications</td>
<td>APIs and implementations for the following standards-based secure communications protocols: Transport Layer Security (TLS), Secure Sockets Layer (SSL), Kerberos (accessible through GSS-API), and the Simple Authentication and Security Layer (SASL). Full support for HTTPS over SSL/TLS is also included.</td>
<td>Authentica...</td>
<td>• Java Secure Socket Extension (JSSE)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Java GSS-API (JGSS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Java SASL API</td>
</tr>
</tbody>
</table>
# Java SE Security Overview

<table>
<thead>
<tr>
<th>High-level Features</th>
<th>Low-level Features</th>
<th>Benefits</th>
<th>References</th>
</tr>
</thead>
</table>
| Public Key Infrastructure (PKI) | Tools for managing keys and certificates and comprehensive, abstract APIs with support for the following features and algorithms:  
- Certificates and Certificate Revocation Lists (CRLs): X.509  
- Certification Path Validators and Builders: PKIX (RFC 3280), Online Certificate Status Protocol (OCSP)  
- KeyStores: PKCS#11, PKCS#12  
- Certificate Stores (Repositories): LDAP, java.util.Collection | Eases the development and deployment of complex PKI applications. Recent support (in JDK 5) for OCSP provides a more scalable and timely method for applications to check certificate revocation status. | X.509 Certificate and Certificate Revocations Lists (CRLs)  
Java CertPath API  
On-Line Certificate Status Protocol (OCSP)  
Java PKCS#11 Reference Guide |