Internet Security and Cluster Technologies for Reliable E-Commerce Services

Kai Hwang
Internet and Cluster Computing Laboratory
University of Southern California

Keynote Speech, SSGRR-2000
L’Aquila, Italy, July 31, 2000
Internet-based Society in the new millennium

- E-Business, E-Commerce
- Metacomputing Grid
- E-Education, E-Society
- E-Government, . . . . .

By year 2001, the global theater of E-commerce will reach US $13 trillion; 42% of which will be at B2B, 20% at B/C2G, and 38% at B2C levels.
Hot Issues in E-Commerce

- Enabling technologies, web-servers, ...
- Security, reliability, and data Recovery
- Databases and datamining techniques
- Fast communication protocols, etc.
- eCash, eCheque, eBank, eSociety, eGovernment, eEntertainment, eTravel, ...
- Groupware, Middleware, and Infowares
- ISPs, ASPs, and Decision support systems

. . . . . . . . .
Underlying Technologies for E-Commerce Services

Core Technologies
- Scalability
- Data Warehousing
- RAS
- UNIX/Linux
- Networking
- RDBMS
- Open Standards

Enabling Technologies
- OLAP
- HTML/XML
- Messaging
- Security
- COM/DCOM/DNA
- CORBA/IiOP
- Performance Measurement
- Knowledge Management

Decision-Support Technologies
- Personalization
- Relationship management

Billing/Payment Systems
- Advertising/Promotions
- Data Mining
- Supply Chain Management

Source: Kalakota and Robinson, e-Business: Roadmap for Success, Addison-Wesley, 1999
Threats on Internet

- Confidentiality - Eavesdropping
- Integrity - Modification of data or viruses
- Authenticity - “Spoofing”
- Availability - “SYN flooding” or DOS Attacks
Securing E-commerce with intrusion control and automatic recovery from malicious attacks

Highly secure and reliable enterprise applications with intrusion prevention and automatic recovery from malicious hackers or unexpected crashes or threats.

Fault tolerance

Increasing reliability

Frontend firewall security architecture

Web sites with no security protection

Single server SMP server Cluster of servers

Increasing scalability

No data protection
Collaborative security agents working collectively to counteract hackers and intruders
10 Most Critical Internet Security Threats
due to software vulnerability on Web servers

- BIND (Berkeley Internet Name Domain)
- CGI (Common Gateway Interface)
- RPC in rpc.ttdbserved (toolTalk), . .
- RDS security hole in Microsoft IIS
- sadmind and mounted on Unix machines
- Sendmail buffer overflow, pipe attacks,
- File sharing via NetBIOS and NT ports
- User Ids as root/Adm with no passwords
- IMAP and POP buffer overflow
- Default SNMP community string
E-Commerce Security Component Technologies

- Client software enhancement
- Server software enhancement
- Middleware for clustering
- Network transport protocols
- Security & Assurance Policies
Major Research Tasks in Securing E-Commerce Web Sites

- **Task 1**: Security testbed construction and reliability enhancement with multi-server clustering and checkpointing RAIDs
- **Task 2**: Development of multi-agent security software environment
- **Task 3**: New policies, standards and component technologies for security, assurance, and confidentiality in E-commerce
- **Task 4**: Integrating with B2B or B2G processes in global supply chain management
Architecture of A Highly Secure Web Site for E-Business Services

Intranet servers

Switch

Security controller

Firewall

Internet

E-commerce Server Cluster

September 7, 2000

K. Hwang at USC
Prototype has 16 Pentinum PCs housed in two 9-ft computer racks.

All PCs run with the Redhat Linux version 6.0 (Kernel version 2.2.5)

All 16 PC nodes are interconnected by a 100 Mbps Fast Ethernet

The cluster is ported with DQS, LSF, MPI, PVM, TreadMarks, Elias, and NAS benchmarks, etc.

Scaling to a future system with 100’s to 1000’s of future processors interconnected by Gigabit networks

Web site: http://andy.usc.edu/trojan/
Trojans cluster built at USC Internet and Cluster Computing Laboratory
## Attack Characteristics and Countermeasures in Federated E-commerce

<table>
<thead>
<tr>
<th>Attack characteristics</th>
<th>Attack Type</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address Spoofing</strong></td>
<td>From internal or external against host</td>
<td>Firewall and use stronger authentication methods&lt;br&gt;Firewalls are ineffective against internal attacks</td>
</tr>
<tr>
<td><strong>Software vulnerabilities</strong></td>
<td>From external against the host</td>
<td>Firewall to filter some of the traffic before it reaches the web server.&lt;br&gt;Firewalls are very effective in blocking external attacks&lt;br&gt;Agent can do a better job here</td>
</tr>
<tr>
<td><strong>Flooding the host</strong></td>
<td>From internal or external against the host</td>
<td>Creating Redundant resources&lt;br&gt;Creating redundant resources helps withstand this attack for a longer time and it is not a complete solution</td>
</tr>
<tr>
<td><strong>Personated endpoints</strong></td>
<td>From internal or external against host or other agents</td>
<td>Strong authentication and digital certificates that rely on private keys.&lt;br&gt;Very effective for both internal and external attacks</td>
</tr>
<tr>
<td><strong>User impersonation</strong></td>
<td>From internal or external against other agent</td>
<td>Use of Digital Certificates&lt;br&gt;Very effective for both internal and external attacks</td>
</tr>
<tr>
<td><strong>Viruses &amp; Trojan Horse programs</strong></td>
<td>From internal or external against the host</td>
<td>Virus Scanning and Content Filtering.&lt;br&gt;The information for virus scanning and content filtering needs to be continuously updated, else it will become ineffective</td>
</tr>
</tbody>
</table>
Architecture of the security controller built with a cluster of Linux servers

- Defined Security Policy
- Decision Making System
- Agent Controller
- Communication Agents

- Intrusion Database
  - Agent Security Infrastructure
  - Agent PKI
  - Agent Name Service

- Data-Mining Agents
Distributed RAID-x Architecture

Cluster Network

Node 0

P/M

CDD

B0
B12
B24
B25'
B26'
B27'
B4
B16
B28
B29'
B30'
B31'
B8
B20
B32
B33'
B34'
B35'

D0
D4
D8

Node 1

P/M

CDD

B1
B13
B25
B14'
B15'
B24'
B5
B17
B29
B18'
B19'
B28'
B9
B21
B33
B22'
B23'
B32'

D1
D5
D9

Node 2

P/M

CDD

B2
B14
B26
B3'
B12'
B13'
B6
B18
B30
B17'
B16'
B17'
B10
B22
B34
B11'
B20'
B21'

D2
D6
D10

Node 3

P/M

CDD

B3
B15
B27
B0'
B1'
B2'
B7
B19
B31
B4'
B5'
B6'
B11
B23
B35
B8'
B9'
B10'

D3
D7
D11

September 7, 2000 K. Hwang at USC
Benchmark Performance of Distributed RAID Architectures

(a) Large read (20MB per client)
(b) Small read (32KB per client)
(c) Large write (20MB per client)
(d) Small write (32KB per client)
Trojans Linux Cluster
with Middleware for Security and Checkpoint Recovery

- Programming Environments (Java, EDI, HTML, XML)
- Web Windows User Interface
- Other Subsystems (Database, OLTP, etc.)

Single System Image (SSI) Infrastructure

Security and Checkpointing middleware

- Linux Server
- Linux Server

Gigabit Network Interconnect
Intelligent Agent-based E-Commerce Infrastructure

- Need a robust testbed
  - WWW Servelet + SSL + Applet
  - Mobile agent platform:
    - IBM Aglet
    - JATLite (KQML)
    - ObjectSpace Voyager (CORBA, XML)

- EDI vs. XML data flow model
Adaptive Security Control
with intelligent agents to detect threats, to learn from intrusion patterns, and to safeguard E-business operations
Electronic Solutions

- Confidentiality
- Origin Authentication
- Content Integrity
- Non-repudiation of origin/receipt
- Availability

- Data Encryption
- Digital Signatures, Certificates, Digital Ids
- Hash Algorithms, Message Digests, Digital Signatures
- Digital Signatures, Audit Logs
- Redundant Systems, Automatic Failover
Public-Key Cryptography

- Secure E-mail and other communications
  - Secure Internet communications
  - S/MIME standard
  - Lotus Notes, Entrust, PGP

- Secure WWW transactions
  - Consumer-merchant purchases
  - On-line banking
  - SSL, S-HTTP, SET

- Business-to-business transactions
  - Electronic Data Interchange
  - Electronic Trading
Secure Communication with Public-Key Cryptography
Non-Repudiation of Origin

- This technique protects the receiver of a message from sender’s denial of having sent it.
- Protection is achieved by including a digital signature, obtained by encrypting message with a public and/or private keys.
Collaborative Security Projects
between USC and Industrial partners

- **Internet payment system**
  - Credit card payment with enhanced SSL protocol
  - Micro payment with wallet server

- **Internet security control**
  - New cryptographic algorithms
  - S-MIME protocol revision (PKCS)
  - Wireless security control

- **Securing mobile agents in personalized E-commerce using PDA, cellular phone, etc.**
Concluding Remarks:

- Intrusion-proof web servers and firewalls are in great demand in E-business services
- Distributed checkpointing to secure federated E-commerce operations
- Distributed RAID for Unix, Windows NT, and Linux web servers in cluster or grid environments
- Clustered security appeals to consolidated web services and global supply chain management