Application Defense:
An emerging Security Concept

Basit Hussain, Ph.D.
CTO Cerebit, Inc.
www.cerebit.com

Order of presentation

• Problem space and need
• Conventional wisdom
• Limitations and issues
• Application security solution
The need for application security

- 75% of attacks are initiated by insiders. (Source: CSI/ FBI 2002)
- A single security infraction costs $6.5M for theft of proprietary information and $4.4M for financial fraud. (Source: CSI/ FBI 2002)
- The aggregate loss reported by 223 organizations was $456 million. (Source: CSI/ FBI 2002)
- Threats to mission critical applications are not stopped by firewalls

"Enterprises will spend large amounts of money and time on building firewalls to cope with threats that can make the front page of a newspaper, but they will allow their users to gain deep access into company networks and applications with simple user IDs and passwords." (Source: Gartner, Oct 2002)
The need (a case study)

- **Fact:** In the case of U.S. vs. Osowski, November 2001, two employees participated in a scheme to defraud Cisco Systems to obtain unauthorized Cisco stock. As part of the scheme, they exceeded their authorized access to computer systems at Cisco on three occasions in order to access a computer system used to manage stock option disbursals. The total value of the Cisco stock pilfered on these occasions was approximately $7,868,637.

- What went wrong? **Inadequate authentication and authorization mechanisms led to monetary loss.**

- How could it be prevented? **Access control, audit activity and incident response would have pinpointed suspicious behavior well in time to avoid the loss.**

---

Information Security Pyramid

- Policy
- Application Security
- Operating System Security
- Infrastructure Security

*Copyright Cerebit, Inc. © 2003*
Typical physical network setup

- Remote User
- Partner's Users
- Internal Users
- Public Network (VPN, Dedicated Link, Frame relay, T1 etc.)
- Partner's Network
- Remote Branch
- Internal Resources
- Internal Users

Logical Corporate Network

- Employee Network
- Critical Servers
- Web Server
- Public Servers
- Public Network
- DNS Server
- SMTP Server
- Users
Typical Firewalls Setup

Critical Servers

Employee Network

Users

SMTP Server

DNS Server

Web Server

Public Servers

Public Network

Typical NIDS Setup

Critical Servers

Employee Network

Users

NIDS

DNS Server

Web Server

Public Servers

Public Network
Using NIDS and HIDS

Critical Resources: Authorization
Critical Resources: Details

Application 1:
- Securities Trading Service
- App. 1’s ACL
- App. 1’s Log

Application 2:
- Stock Quote Feed
- App. 2’s ACL
- App. 2’s Log

Application N:
- Market Reports
- App. N’s ACL
- App. N’s Log

Corporate Authentication System

NIDS

Issues

- Logs are distributed and difficult to analyze
  - different conventions and formats
- Access Control is distributed.
  - Have to add/delete users on each system
  - Error prone
- Firewalls do not protect against attacks from within or from partners
- Application level threats can traverse firewalls
- IDS is not very effective and may not signal in time
- SSL does not enforce “strong” authentication for users
  - Does not provide non-repudiation on transactions.
**Issues**

- Users roles are not well defined
- Access control cannot be fine tuned to emulate the business processes
- Applications do not usually provide good access control
- Applications may rely on crude access control built into the operating system

**IDS and Firewalls**

- Gartner:
  - IDS do not add an additional security layer as promised.
  - IDS are costly (why?) and an ineffective investment.
  - Recommends that enterprises focus on integrated network-level and application-level firewall.
  - What is that product? How complex is it? – Another Hype?
IDS Systems, and Firewalls

- Problems associated with IDSs are:
  - False positives and negatives
  - An increased burden on the IS organization by requiring full-time monitoring (24 hours a day, seven days a week, 365 days a year)
  - A taxing incident-response process
  - An inability to monitor traffic at transmission rates greater than 600 megabits per second
  - An organization should build an infrastructure that allows easy scalability as traffic increases and as more security rules are applied.
  - Too many events to be monitored manually by Managers.

Firewalls

- Network Security Managers are torn apart:
  - Need to block intruders
  - Need to allow traffic
    - Remote Branches not on network (cheaper)
    - Connections with partners --- Web-services
  - Firewalls block access, web services allow access.
  - What is done by one is undone by the other.
  - Too much security management needed.
How to Translate Business Rules to Security Policies?

- Firewalls and IDS are infrastructure (lower level) products.
- It is HARD to translate business rules to Firewall policies and IDS rules.
- The rules have to be distributed over the entire organization over multiple devices.
- Little central control.
- Problem is “Inherent” in the way things are handled not in a particular product.

An Analogy

- Software Development:
  - What is the most critical phase to catch defects?
    - Implementation?
    - Design?
    - Specifications?
  - Ans: Specifications... A defect at Specification phase is MOST expensive to fix.
- What is the best level place to provide security?
Analogy

- What is the most critical level to detect intrusions?
  - Hardware level
  - Software level
  - Network level
  - Infrastructure level
  - Application level
  - Business Level

Common Criteria

<table>
<thead>
<tr>
<th>Functional Point</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Mediation</td>
<td></td>
</tr>
<tr>
<td>User Management</td>
<td></td>
</tr>
<tr>
<td>Resource Management</td>
<td></td>
</tr>
<tr>
<td>Entitlement Management</td>
<td></td>
</tr>
<tr>
<td>Storage of Security Data</td>
<td></td>
</tr>
<tr>
<td>Systems Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td>Application Integration and</td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td></td>
</tr>
<tr>
<td>Proxy Access</td>
<td></td>
</tr>
</tbody>
</table>
### Common Criteria

<table>
<thead>
<tr>
<th>Functional Point</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit</td>
<td></td>
</tr>
<tr>
<td>Data Disposal</td>
<td></td>
</tr>
<tr>
<td>System Integrity</td>
<td></td>
</tr>
<tr>
<td>Security Administration</td>
<td></td>
</tr>
<tr>
<td>Guidance</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Functional Point</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td></td>
</tr>
<tr>
<td>Non-Repudiation</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>Authorization</td>
<td></td>
</tr>
<tr>
<td>Confidentiality</td>
<td></td>
</tr>
<tr>
<td>Data Integrity</td>
<td></td>
</tr>
</tbody>
</table>
Risks Associated with Online Registrations

Is my identity safe?

Is it really Mr. User?

Let's get to know Mr. User. Or let's register as Mr. User

Public Network

Corporate Authentication System

Firewall

Mr. User

Mr. Cracker

Risks with Online Transactions

Is it really Mr. User using his password?

Public Network

Corporate Authentication System

Firewall

Mr. User

Impersonator

Payday!

Interceptor

Payday!

Copyright Cerebit Inc. © 2003
Issues and Solutions

- Solution requirements
  - Ease of use
  - Simplified administration
  - Validity of user thru strong authentication
  - Non-repudiation of critical actions
  - Seamless integration into technology and business processes
  - Comprehensive audit trails
  - Incident response of anomalous activity

Enterprise Security Policy

- Understand Business Processes
- Identify the critical enterprise resources
- Conduct security audits
- Identify the leakage points
- Identify user types
- Define access needs of each role
Unified Application Defense

- Application 1: Securities Trading Service
- Application 2: Stock Quote Feed
- Application N: Market Reports

Optional Certification Authority (CA)

Central Logging

NIDS

Simplified Security Management

- Application 1: Securities Trading Service
- Application 2: Stock Quote Feed
- Application N: Market Reports

Access Control Point

Central ACLs

Audit

Security Manager

Copyright Cerebit, Inc. © 2003
Features of Application Security

- **Authentication.** Verify if users are who they claim to be.

- **Authorization.** Users can only access what the security policy allows.

- **Role-based access control.** Grant access based on the user’s role in the organization.

- **Data privacy.** Data integrity. **Data reliability.**

- **Data validation.** Process only if data is within pre-defined limits.

Features of Application Security

- **Non-repudiation on Transactions.** Important user actions carry proof of execution to prevent denial.

- **Session security.** User sessions are uniquely identifiable and not subject to masquerading.

- **Audit logs.** All actions are logged for audit use.

- **Single sign-on.** Usage of multiple systems or services does not require additional credentials.

- **Session time-out.** Session inactivity leads to session termination

- **Incident response.** Anomalous activity leads to immediate alarms to curtail damage.
Advantages of Application Defense

- All features of application security PLUS …
  - Consolidated logs
    - Run IDS rules at one place
  - Single point of policy control
  - Granular access control
  - Secure legacy systems
  - Interfaces with HTTP, SOAP, EJB, CORBA, RMI
  - Supports most authentication systems
  - Modular and expandable
  - Signed transactions
    - Non-repudiation per transaction

Benefits of Application Defense

- Reduced management
- Improved security
  - Secure what was not possible before
- Reduce risk and errors
- Comprehensive monitoring
- Incident response
- Forensic analysis
Contact information

Cerebit, Inc

12000 28th Street North, Second Floor

St. Petersburg, Florida 33716 USA

• basit@cerebit.com