



0121197 2676 0676026

Application Intrusion Detection

Drew Miller

Black Hat Consulting



0121197 2676 0676026

Application Intrusion Detection

- Introduction
- Mitigating Exposures
- Monitoring Exposures
- Response Times
- Proactive Risk Analysis
- Summary



0121197 2676 0676026

Introduction

- What is Application Intrusion Detection?
- Why would I use Application Intrusion Detection?
- What about IDS (Intrusion Detection Systems)?
- Exposures



0121197 2676 0676026

What is Application Intrusion Detection?

- You design the application
- You know the operating constraints
- Your code performs checks to maintain stability and functionality
- Why not add code that allows your application to “do something” when it is being attacked?



0121197 2676 0676026

What is Application Intrusion Detection? (cont.)

- Design explicitly
- Failure cases are attacks
 - Functional vs. Security
- Detect deviations
- Notify Personnel



0121197 2676 0676026

Explicit Design

- User requests must be defined
- State machine determines when requests can be made and by whom
- Server defines data sizes



0121197 2676 0676026

Failure Cases

```
if( request.Length > 32 )
{
    // then do work
}
else
{
    // buffer overflow attack in progress
}
```



0121197 2676 0676026

Failure Cases (cont.)

```
if( request == "Login" )
{
    // check state machine
    if( user logged in == true )
    {
        // out of state request, race condition or logical
        // attack in progress
    }
}
```




0121197 2676 0676026

Failure Cases (cont.)

- Testing vs. Real World Deployment
 - Bugs or Hacks
- Functional failures in an application during runtime in deployment are security flaws, not just functional flaws, and they should be treated as such!



0121197 2676 0676026

Notification

- Monitoring system is notified when attack possibilities are detected
- Notify People
 - Number of attempts
 - Type of attempt



0121197 2676 0676026

Introduction (cont.)

- What is Application Intrusion Detection?
- Why would I use Application Intrusion Detection?
- What about IDS (Intrusion Detection Systems)?
- Exposures



0121197 2676 0676026

Why would I use Application Intrusion Detection?

- Detection
- Prevention
- Protection



0121197 2676 0676026

Detection

- Will users forget passwords?
 - Yes.
- Will the authentication system notify such failures and security events?
 - Yes.
- Can the system be tuned to allow a certain deviation in authentication failures so that a single user doesn't set off emergency alarms, but a brute force attack would?
 - Yes.



0121197 2676 0676026

Prevention

- The security event logs show that there is a massive amount of brute forcing of possible table indices for my web application. What does that mean?
- Verify that your authorization model doesn't allow access to records that the user should not access. Gives you time to add more defenses such as hashing (index+magic value) table indices to negate index brute forcing completely.



0121197 2676 0676026

Protection

- Where are you protected?
- Where are you not protected?
- Real time auditing information that is generated from your application helps determine how well you are protected and gives you functional and even legally binding data about what is going on.



0121197 2676 0676026

Introduction (cont.)

- What is Application Intrusion Detection?
- Why would I use Application Intrusion Detection?
- What about IDS (Intrusion Detection Systems)?
- Exposures



0121197 2676 0676026

What about IDS (Intrusion Detection Systems)?

- Application layer packet filtering?
- Application layer state management?
- IDS must see data to analyze... what if my data is encrypted (which it should be)
- Application level intrusion detection cannot be duplicated successfully by a network IDS.



0121197 2676 0676026

Introduction (cont.)

- What is Application Intrusion Detection?
- Why would I use Application Intrusion Detection?
- What about IDS (Intrusion Detection Systems)?
- Exposures



0121197 2676 0676026

Exposures

- An exposure is a general term that refers to the knowledge a hacker has. It allows him or her to gain more information or use your system in ways that are not intended given the user.
 - Buffer Overflows
 - Injections
 - Information Leakage
 - Replay Attacks
 - Session Hijacking



0121197 2676 0676026

Application Intrusion Detection

- Introduction
- Mitigating Exposures
- Monitoring Exposures
- Response Times
- Proactive Risk Analysis
- Summary



0121197 2676 0676026

Mitigating Exposures

- These are exposures that we know we are stopping and we should know that we stop them.
- Data Restrictions
 - Buffer Overflows
 - Injections
 - Brute Forcing
- State
 - Race Conditions
 - Privilege Escalation
 - Authorization



0121197 2676 0676026



Data Restrictions

- Buffer Overflow Detection Demonstration
- A simple bounds checking routine will detect that a string is too large. If your client program was written to only allow the correct size, then someone is hacking your application.



0121197 2676 0676026

Data Restrictions (cont.)

- Brute Forcing Detection Demonstration
- Never deny access for more than a few seconds, or else brute force attacks can be used to cause denial of service to your clients.



0121197 2676 0676026

State

- Out-of-State User Request Demonstration
- Authorization models can be implemented with state machines to control who may access specific resources.



0121197 2676 0676026

State (cont.)

- Authorization Failure Demonstration
- When users fail authorization checks, it makes you wonder if the application should even allow the user to make the request...



0121197 2676 0676026

Application Intrusion Detection

- Introduction
- Mitigating Exposures
- Monitoring Exposures
- Response Times
- Proactive Risk Analysis
- Summary



0121197 2676 0676026

Monitoring Exposures

- These are exposures that we know we can not stop which makes it more important to know when they occur
- Local Protection (Modification Detection)
 - Log Files
 - Secrets
 - User Databases



0121197 2676 0676026

Log Files

- Created during deployment
- Recreated immediately after backup
- Log files should always exist
- Applications should always append data and never overwrite data



0121197 2676 0676026

Log Files (cont.)

- Log Files Demonstration
- Can't be modified without detection. Allow for non-repudiation in legal cases. Can help forensics when and if a system is exploited by a hacker.



0121197 2676 0676026

Secrets

- If a secret can't be found, fail to close instead of fail to open.
- This is purposefully causing yourself denial of service. Is that better than allowing hackers to have a free for all with your network application?



0121197 2676 0676026

User Databases

- Vulnerability
 - A missing user database means free access?
- Solution
 - Backup as often as performance allows when you are sure the system is clean. Deploy old backup to restore missing files deleted by hacker. Don't allow access to the application without authentication and authorization in place, even in such extreme situations as a worm or virus infecting your deployment system.



0121197 2676 0676026

User Databases (cont.)

- User Database Demonstration
- System Administrator vs. Application System Administrator
- Backups and Deployment



0121197 2676 0676026

Application Intrusion Detection

- Introduction
- Mitigating Exposures
- Monitoring Exposures
- Response Times
- Proactive Risk Analysis
- Summary



0121197 2676 0676026

Response Times

- Time to Hack vs. Time to Detect
- People
 - Pager Notification
 - Email Notification
 - On Duty Security Personnel
- Authorities
 - FBI, etc.
- Third-Party Vendors
 - Credit Card Companies



0121197 2676 0676026

Application Intrusion Detection

- Introduction
- Mitigating Exposures
- Monitoring Exposures
- Response Times
- Proactive Risk Analysis
- Summary



0121197 2676 0676026

Proactive Risk Analysis

- The Business Decision
 - We will take the risk to deploy with a known vulnerability.
 - Is detection as cheap as mitigation?
- Historical Data
 - Limited budgets, resources and/or performance limit security infrastructure. Use historical data to monitor or mitigate your most vulnerable areas.



0121197 2676 0676026

Application Intrusion Detection

- Introduction
- Mitigating Exposures
- Monitoring Exposures
- Response Times
- Proactive Risk Analysis
- Summary



0121197 2676 0676026

Summary

- Plan for exposure mitigation and monitoring
- Build common data, error handling, and auditing routines.
- Determine which exposures that are accessed by hackers should notify real people immediately.
- Build a response process to secure forensic data and restore the application to a known secure and working state after hackers attempt to break in.