

# Creating Self Defending Applications to Repel Attackers

Michael Coates

@\_mwc

michael.coates@owasp.org

# Background

- OWASP - Global Board Chair
- Mozilla - Director of Security Assurance
  - ▶ Creator OWASP AppSensor Project
  - ▶ OWASP Top 10 - 2010 Contributing Author
  - ▶ <http://michael-coates.blogspot.com>
  - ▶ @\_mwc

# Reality

## Applications:

- Contain our most critical data & functionality
- Use custom code & have unique vulnerabilities
- Are constantly attacked
- Provide no visibility into ongoing malicious activity at app level

# Result

- Attackers constantly probe and attack applications without deterrence
- Organizations are unaware of when/how applications are compromised and abused

# Agenda

- Creating a Self Defending Application:
  - ▶ In the Code
  - ▶ In the Lifecycle & Organization
- Live Implementation

# Attack Aware Resources

- [buildsecurityin.us-cert.gov/swa/attackaware.html](http://buildsecurityin.us-cert.gov/swa/attackaware.html)
- [owasp.org/index.php/Category:OWASP\\_AppSensor\\_Project](http://owasp.org/index.php/Category:OWASP_AppSensor_Project)
- Cross Talk Sept, 2011  
[crosstalkonline.org/storage/issue-archives/2011/201109/201109-Watson.pdf](http://crosstalkonline.org/storage/issue-archives/2011/201109/201109-Watson.pdf)

PROTECTING AGAINST PREDATORY PRACTICES

## Creating Attack-Aware Software Applications with Real-Time Defenses

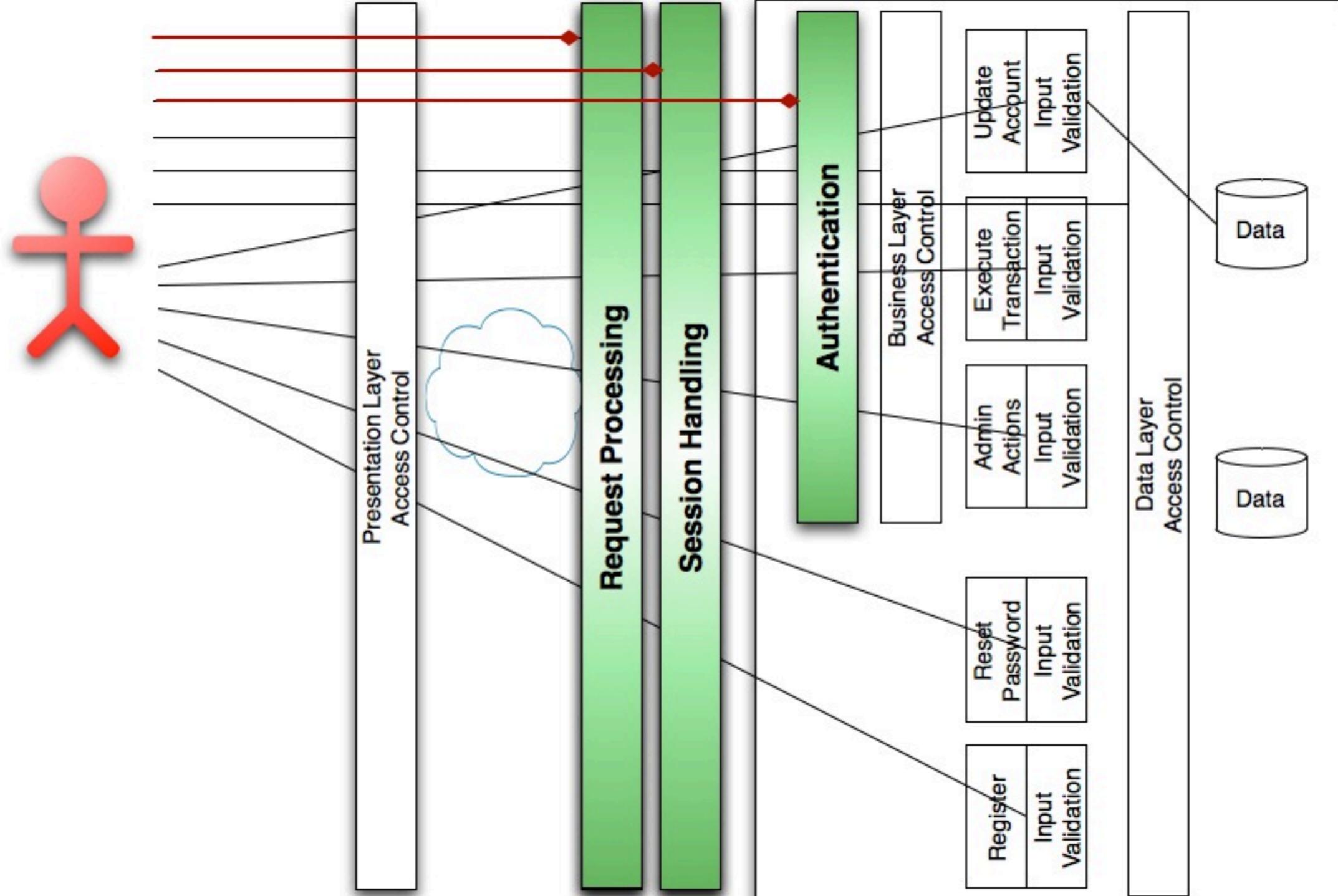
Colin Watson, OWASP  
Michael Coates, OWASP  
John Melton, OWASP  
Dennis Groves, OWASP

The screenshot shows the Software Assurance website. The header includes the title "Software Assurance" and the subtitle "Community Resources and Information Clearinghouse". Below the header is a navigation menu with links for HOME, ABOUT, RESOURCES, ADVISORIES, EVENTS, WEBINARS, PODCASTS, PROCESS VIEW, and GETTING STARTED. The main content area is divided into two columns. The left column contains a sidebar with links to SwA Communities, SwA Forums & Working Groups, Workforce Education & Training, Processes & Practices, Technology & Tools, Acquisition & Outsourcing, Measurement & Business Case, Malware & Cyber Observables, Resilient Software, SwA Market Place, SwA Landscape, SwA Ecosystem, Security Automation & Measurement, and Build Security In. The right column features the "Resilient Software" section, which discusses the goals of Software Assurance and the importance of resilience and survivability. It also mentions "The Rugged Software Manifesto" and "Creating Software that is Attack-Aware and Self-Defending (1)".

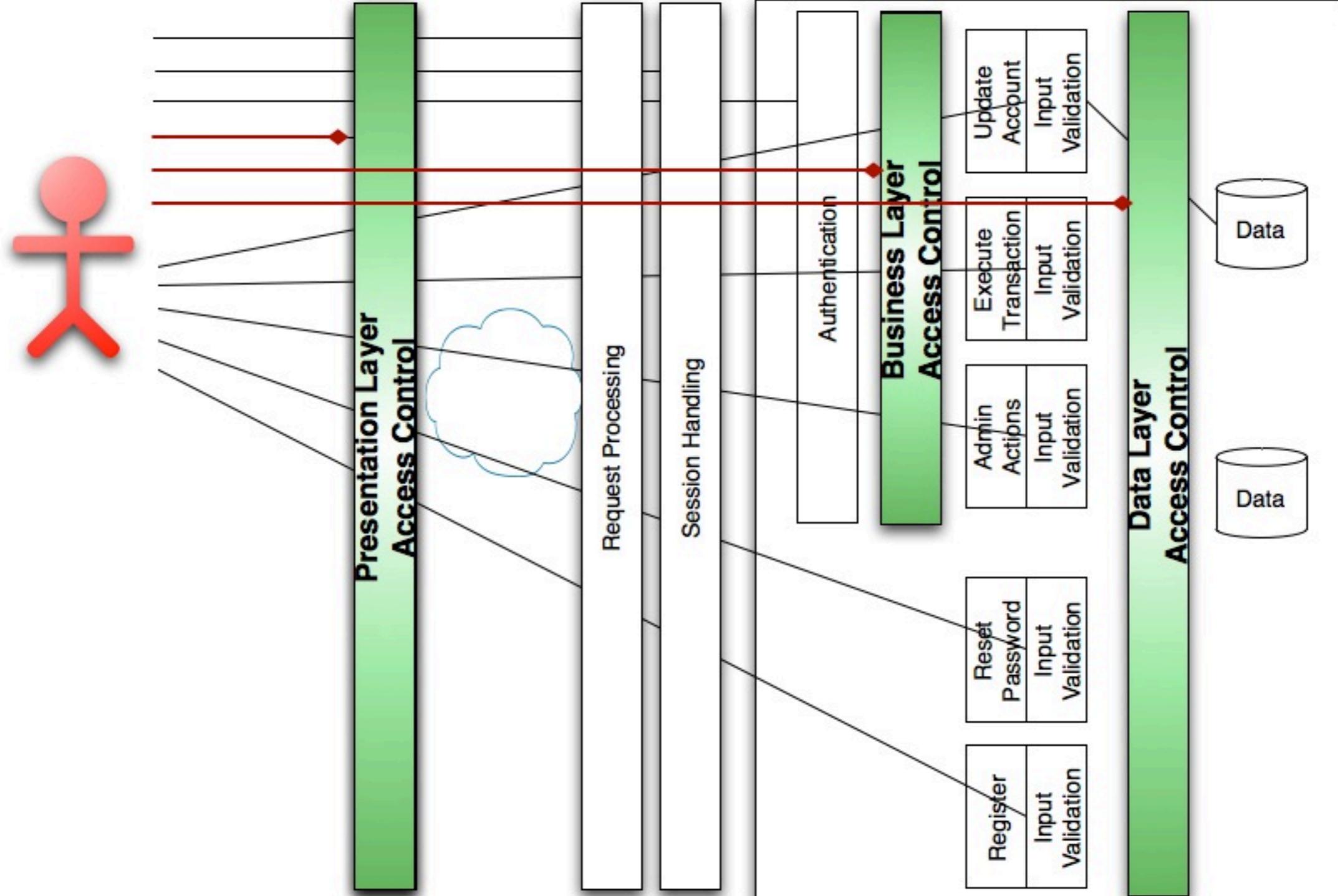
# Self Defending Applications

In The Code

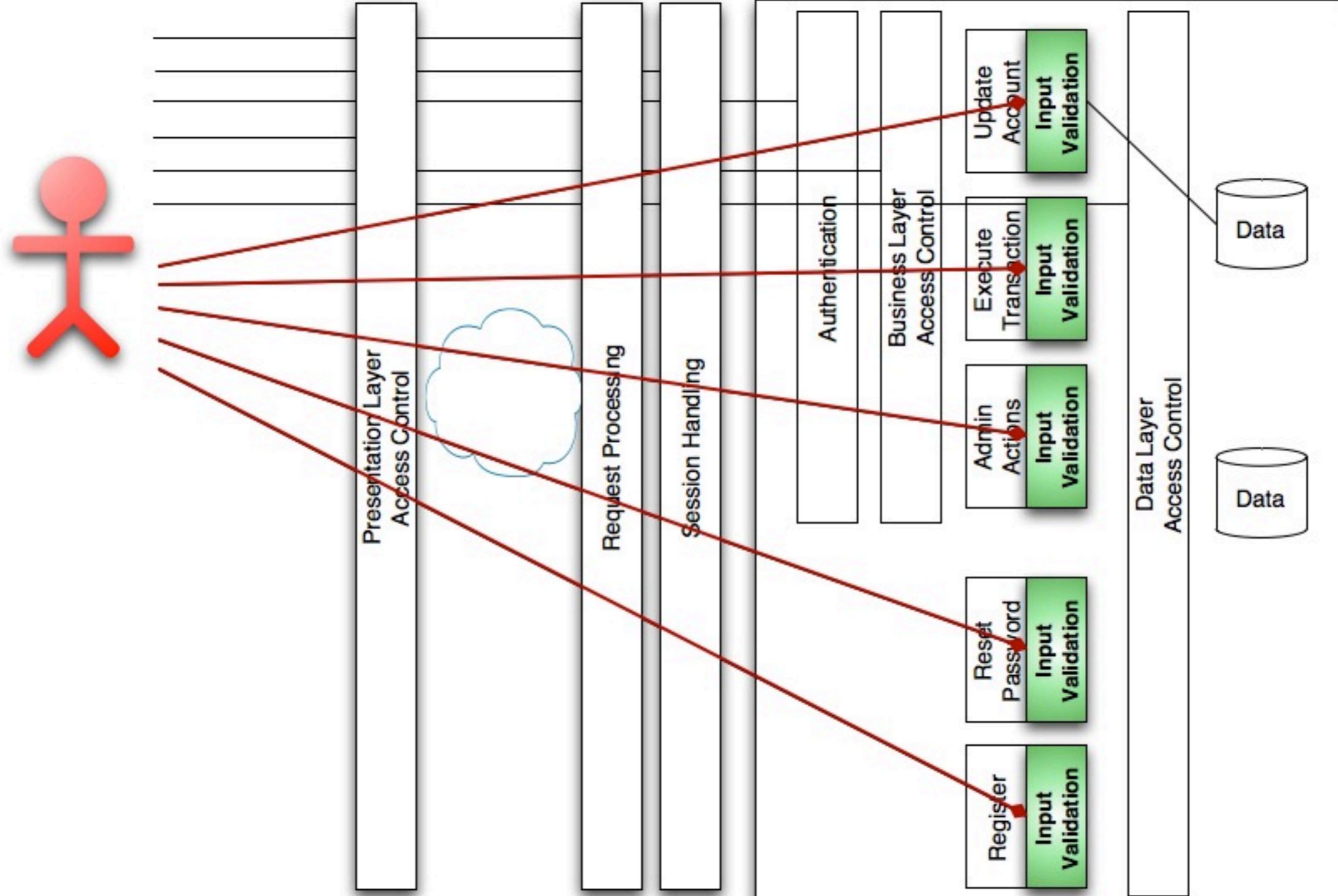
# Attack Points: Requests, Auth, Session



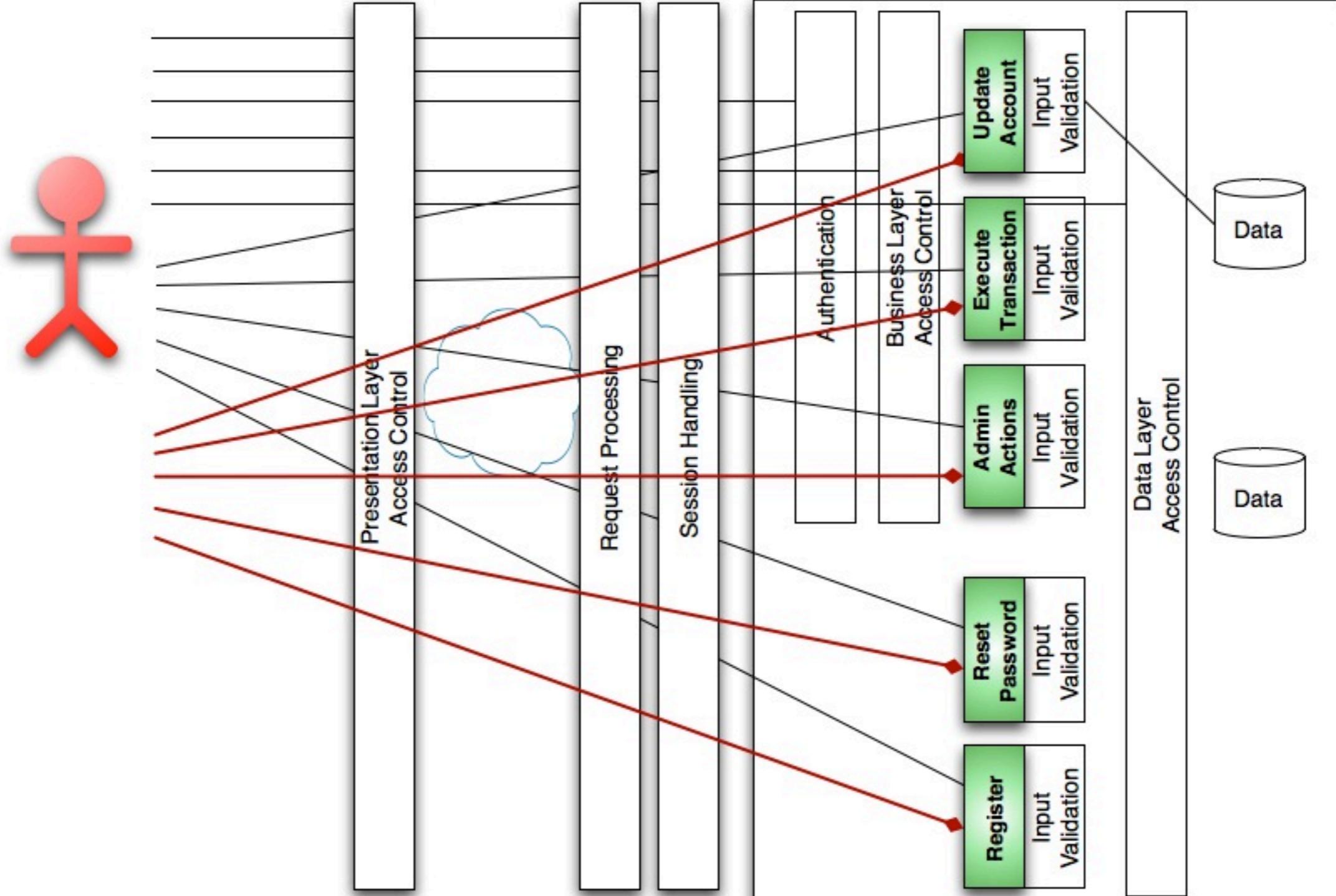
# Attack Points: Access Control



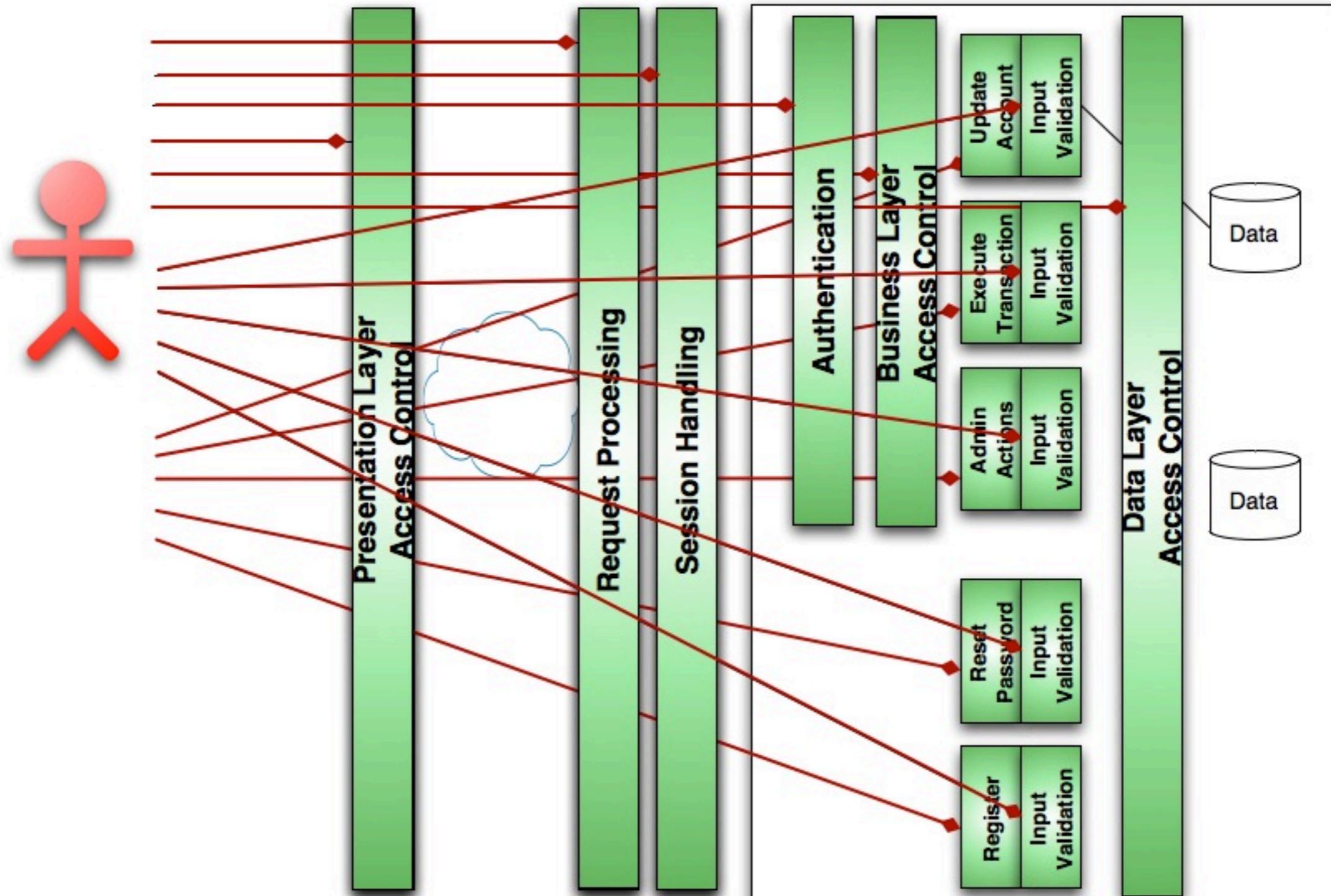
# Attack Points: Input Validation



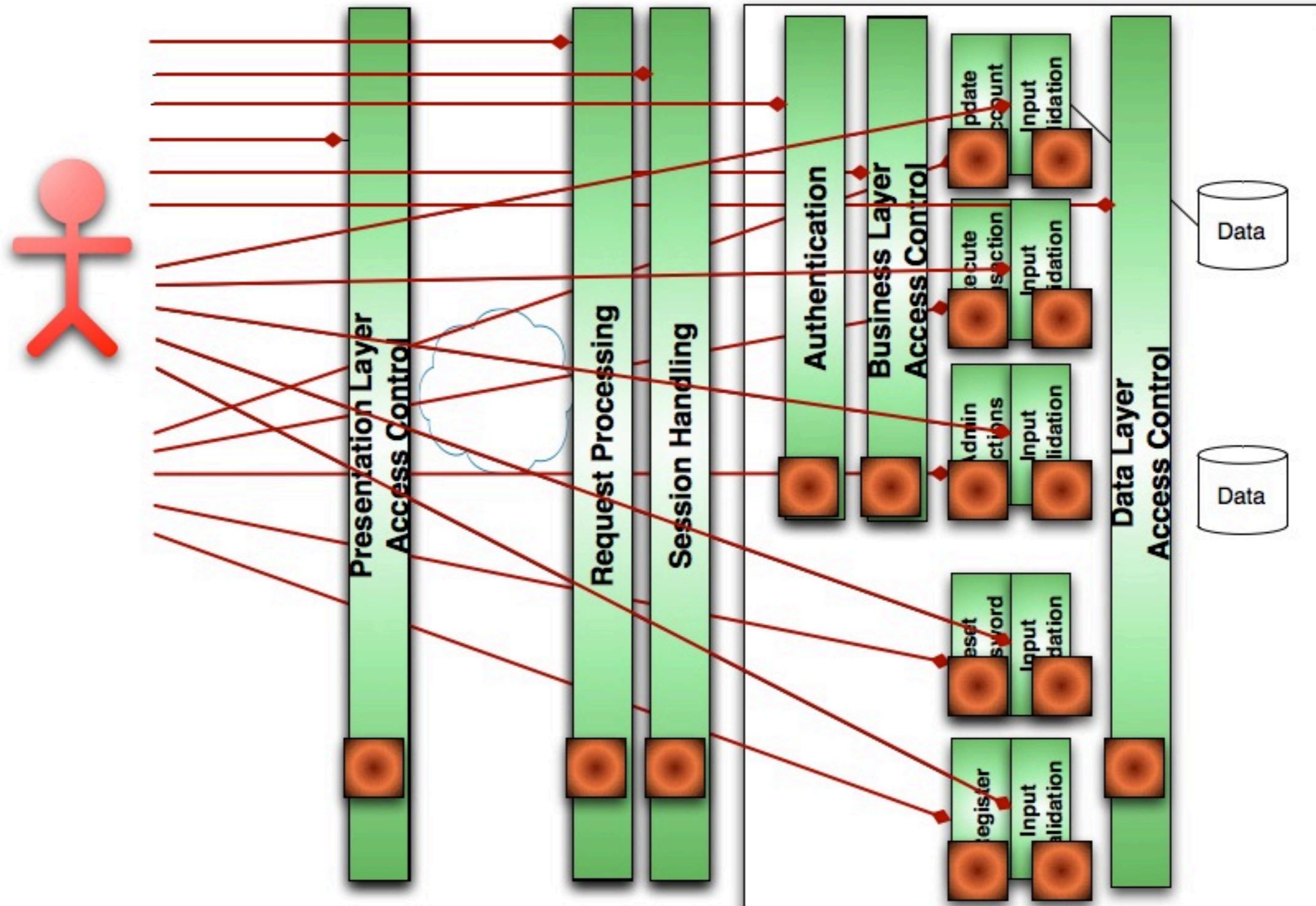
# Attack Points: Business Logic



# Attack Exposure



# Defend with: Detection Points



# Detecting Attacks

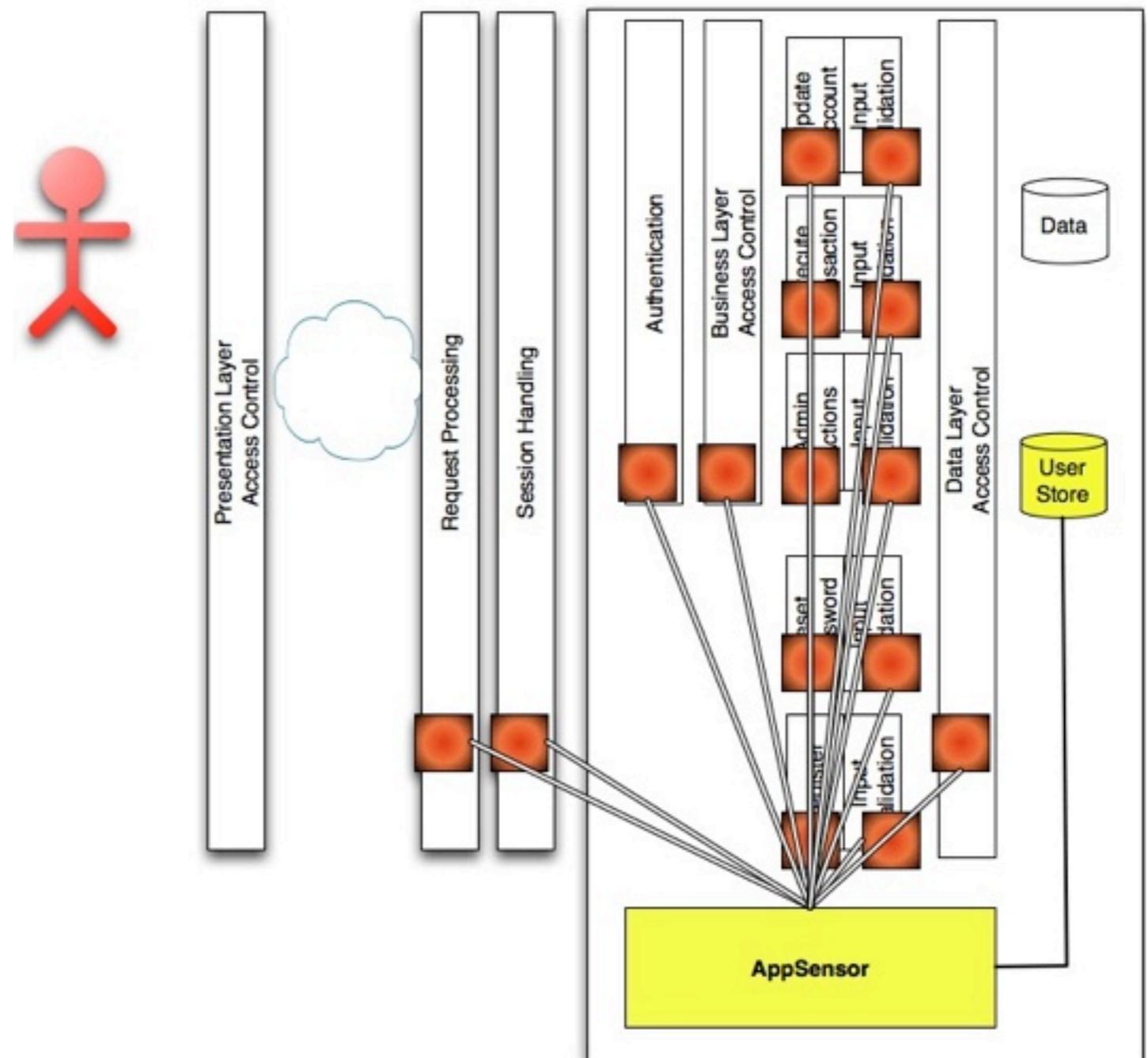
[http://www.owasp.org/index.php/AppSensor\\_DetectionPoints](http://www.owasp.org/index.php/AppSensor_DetectionPoints)

- 50+ attack detection points and growing
- Signature & Behavioral
- Many have nearly zero false positive rate
  - ▶ Can't be encountered accidentally by user
  - ▶ POST vs Get
  - ▶ ` OR `1'='1'

Detection Point Type	Code	Name
Signature	RE	Request Exceptions
	AE	Authentication Exceptions
	SE	Session Exceptions
	ACE	Access Control Exceptions
	IE	Input Exceptions
	EE	Encoding Exceptions
	CIE	Command Injection Exceptions
	FIO	File IO Exceptions
	HT	Honey Trap
Behavioral	UTE	User Trend Exceptions
	STE	System Trend Exceptions
	RP	Reputation

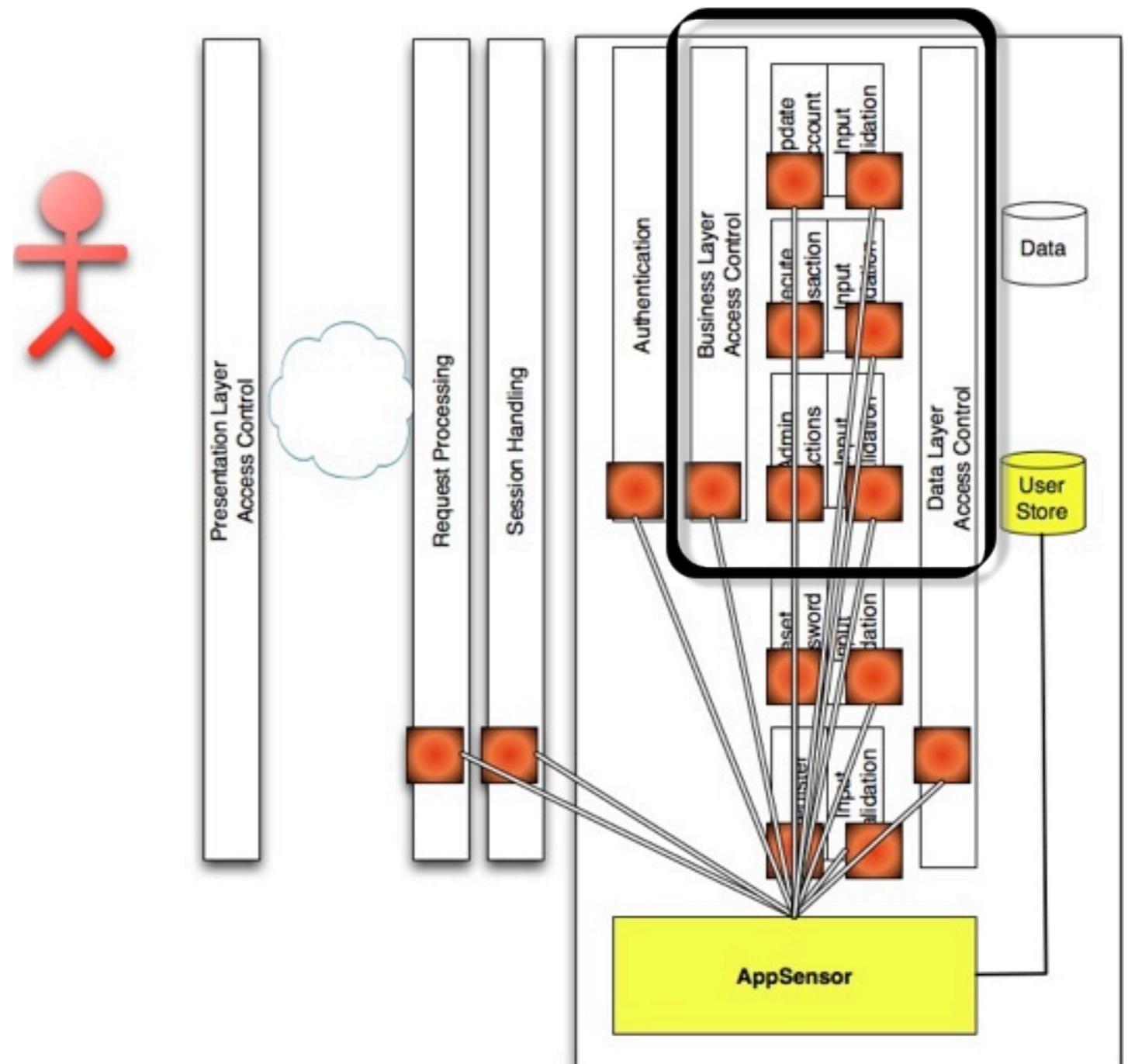
# Centralize Attack Detection Knowledge

- Detection Points Report to Central Location
- AppSensor Integrates w/User Store
- Enables Response Actions against User Object



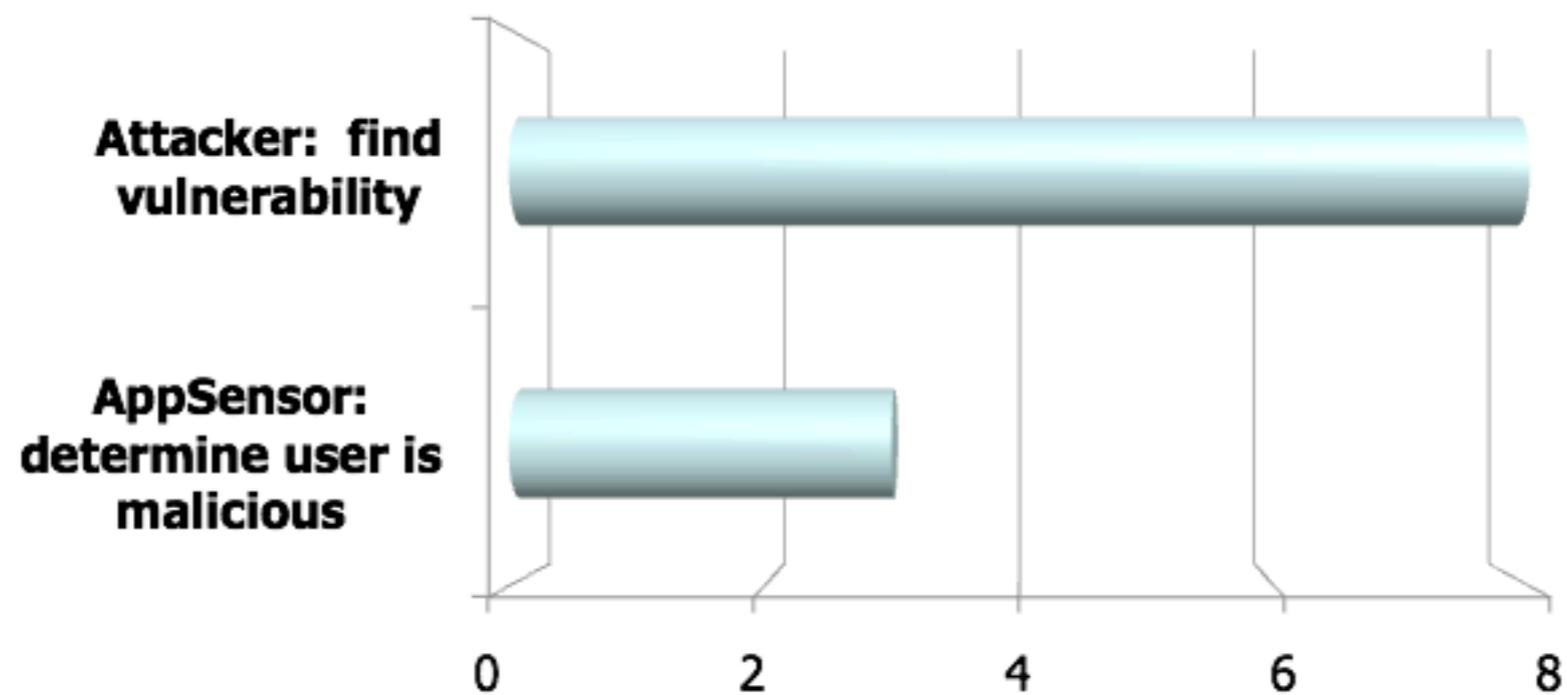
# Detect & Eliminate Threat

- Strong control of authenticated portion
  - ▶ Lockout user
  - ▶ Disable account
- Effective attack reporting for unauthenticated portion



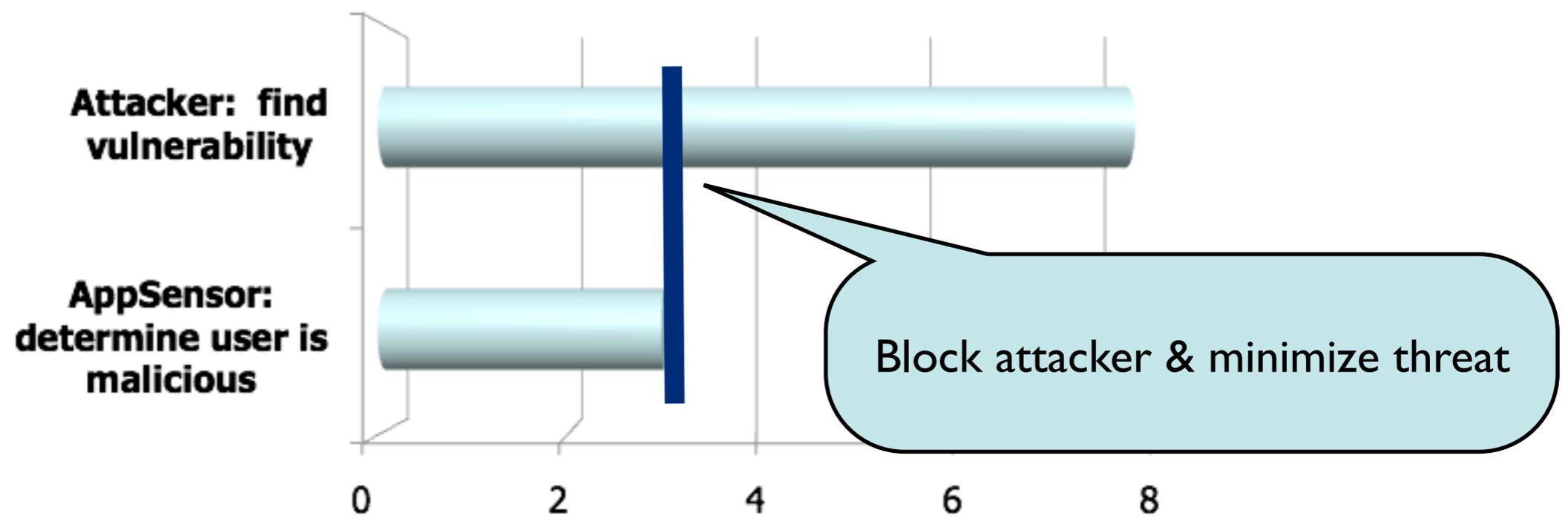
# App Defense Eliminates Threats

**Requests Needed for Attacker vs. AppSensor**



# App Defense Eliminates Threats

Requests Needed for Attacker vs. AppSensor



# Alternatives?

- Self Defending - in the app, full user object interaction, full app knowledge
- Web Application Firewall - generic attack detection
- Log Analysis - slow, reactive, ineffective

# Self Defending Applications

In The Lifecycle & Organization

# Threat Modeling

- ▶ Identify critical business functionality
- ▶ Capture abuse cases
- ▶ Define detection methods

# Example

## ■ Grant Permission Page **site.com/UpdatePermission**

### ▶ Inputs:

- targetUser - Integer
- grantPerm - Integer (1,2,3) (Read, Write Delete)

### ▶ Access Control Requirement:

- Page Access: Power User
- Functionality Access: Power User
- Target User: Non-admin

# Abuse Cases

- Non-integer submitted for targetUser
- Invalid number submitted for grantPerm
- Force browsing to page from unauthorized account (HTTP GET)
- Force submission to page from unauthorized account (HTTP Post)
- Target user is admin account
- Unexpected rate of use (100 perm changes in 10 seconds?)

# Risk Analysis

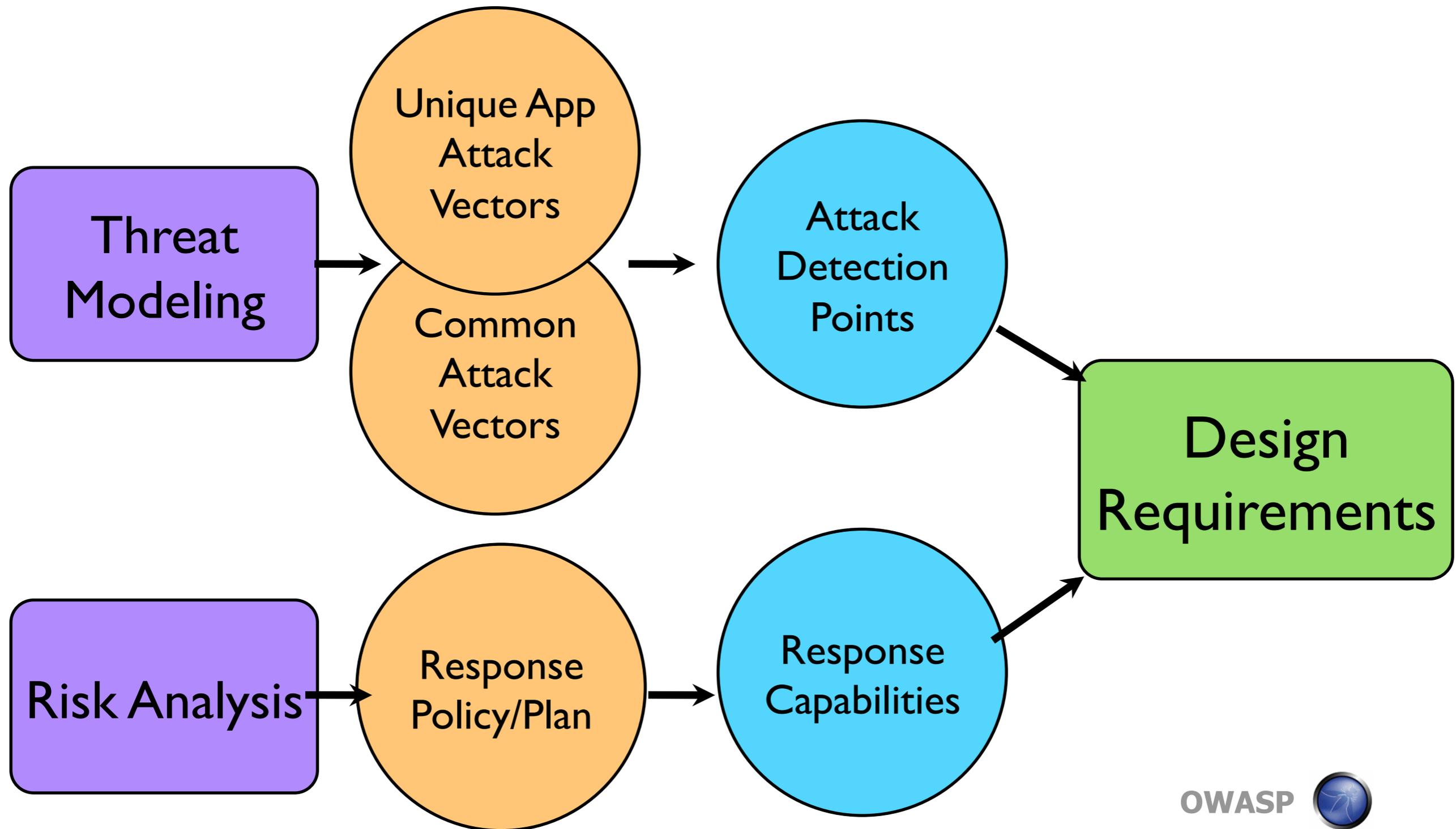
- Tolerance for Fraud & Abuse
- Define Acceptable Response
  - ▶ Alert Admins
  - ▶ Logout / Lock Accounts
  - ▶ Limit Functionality

# Response Options

**Table 1: AppSensor Responses**

CATEGORY		RESPONSE (ADDED SINCE v1.1)	
TYPE	DESCRIPTION	ID	DESCRIPTION
Silent	User unaware of application's response	ASR-A	Logging Change
		ASR-B	Administrator Notification
		ASR-C	Other Notification
Passive	Changes to user experience but nothing denied	ASR-D	User Status Change
		ASR-E	User Notification
		ASR-F	Timing Change
Active	Application functionality reduced for user(s)	ASR-G	Process Terminated
		ASR-H	Function Amended
		ASR-I	Function Disabled
		ASR-J	Account Logout
		ASR-K	Account Lockout
Intrusive	User's environment altered	ASR-L	Application Disabled
		ASR-M	Collect Data from User

# Timing & Flow



# Organization Support

Who	Action
Architects, Developers, Biz Owners, Security SMEs	Threat Modeling, Determine Detection Points
Biz Owners, Architects, Security SMEs	Determine Response Actions
Architects, Security SMEs	Design Response Architecture
Operations Team, Security SMEs	System Communication for Detection Logging & Response
Developers, Security SMEs	Implement Detection Point & Response Code
Monitoring Team, Security SMEs	Define monitoring thresholds, alerting/ action requirements



# Self Defending Applications

Live Implementations

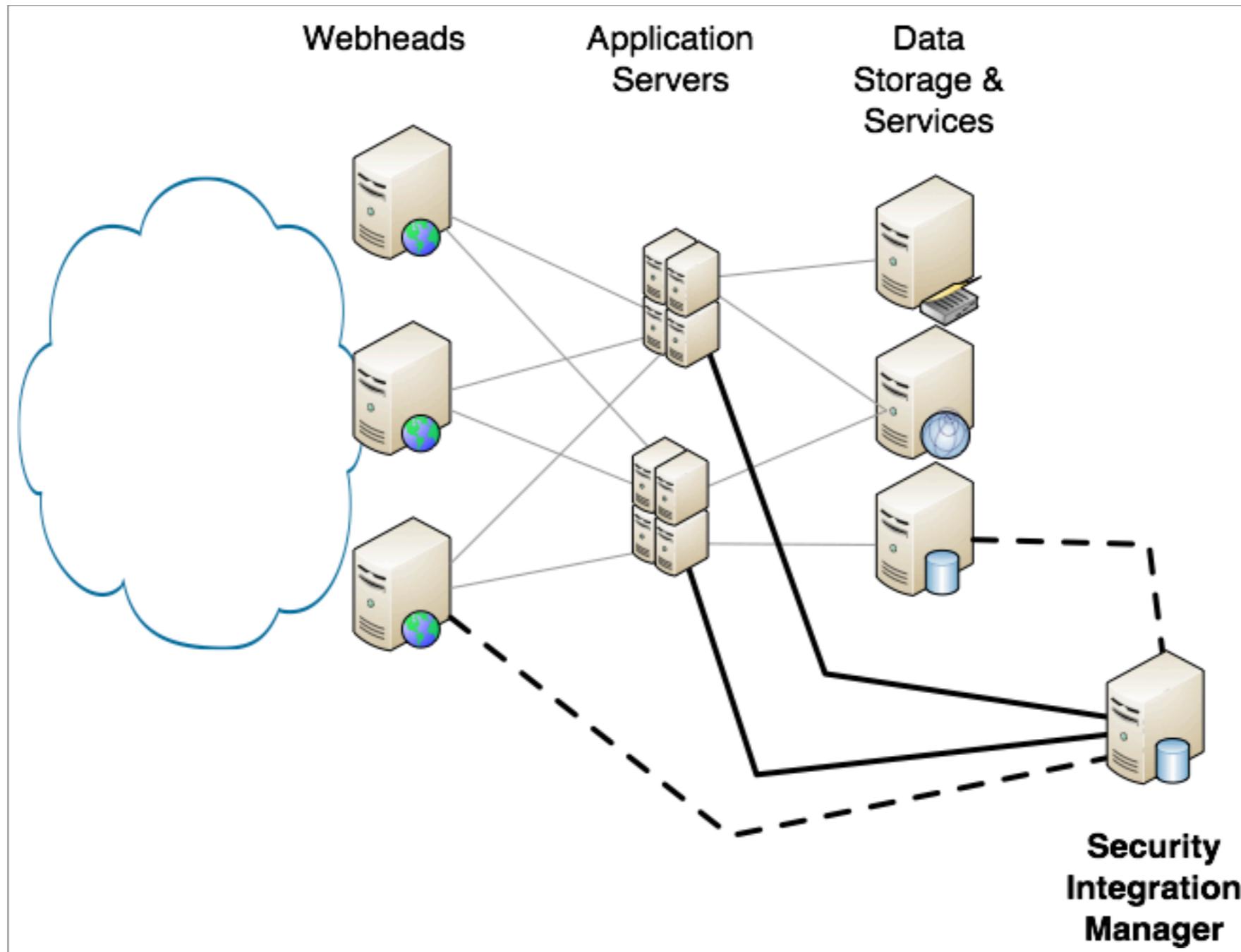


# Common Event Format (CEF)

- Emerging standard on logging format
- Easily parsed by security integration manager (sim)
- Enables AppSensor Logging

```
CEF:0|Mozilla|MozFooApp|1.0
|ACE0|Access Control Violation|8|rt=01
31 2010 18:30:01 suser=janedoe suid=55
act=Action Denied src=1.2.3.4
dst=2.3.4.5 requestMethod=POST
request=http://foo.mozilla.org/foo/
abc.php?a\b
cs1Label=requestClientApplication
cs1=Mozilla/5.0 (Macintosh; U; Intel Mac
OS X 10.6; en-US; rv:1.9.2.2) Gecko/
20100316 Firefox/3.6.2
msg=Additional Data here
```

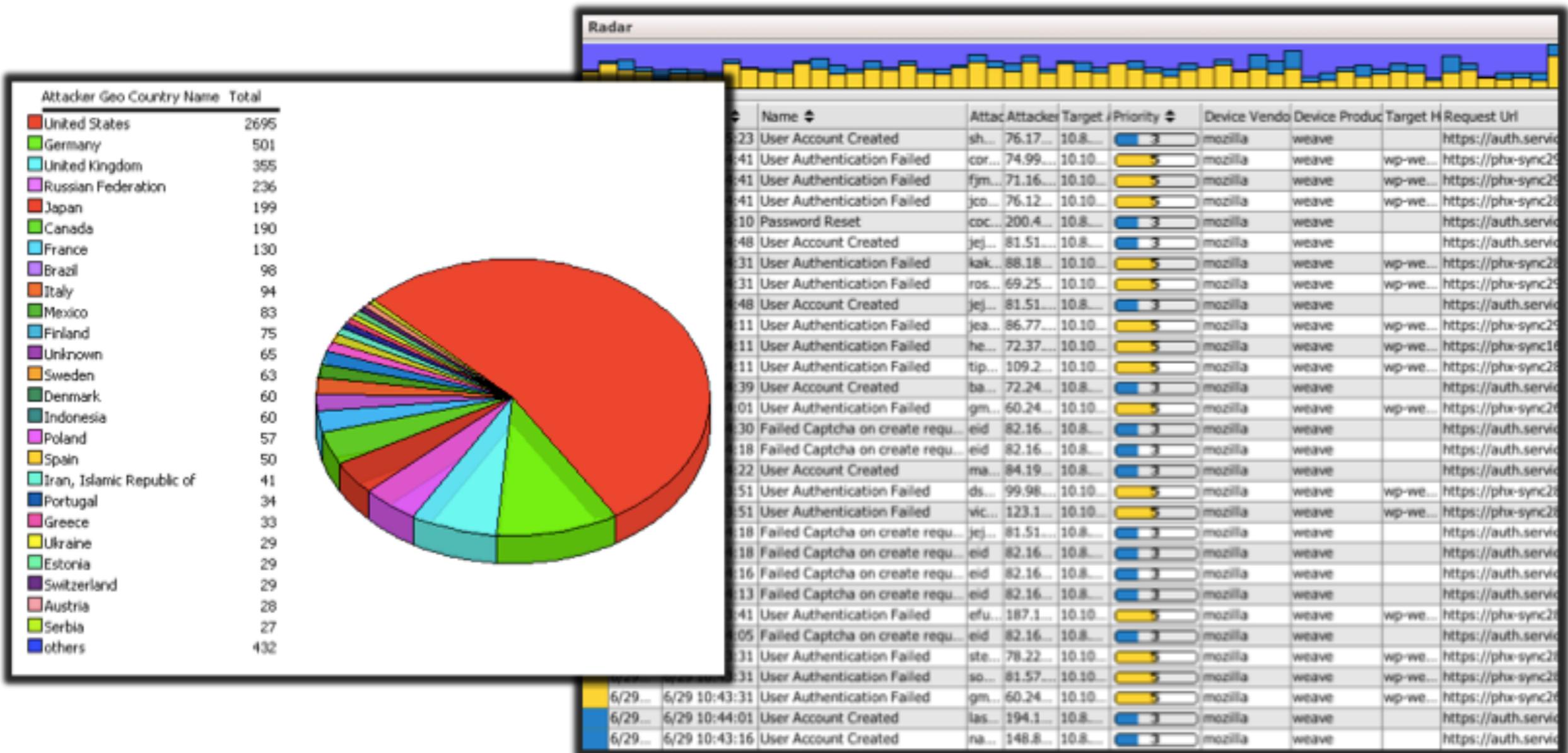
# SIM Deployment



# Full Stack Knowledge

- Application Layer - Custom attack / abuse notification
- Network Layer - IDS activity, firewall failures
- OS Layer - OS commands (AuditD), System event logs

# Data Analysis



Failed Captcha on Create  
User Account Created

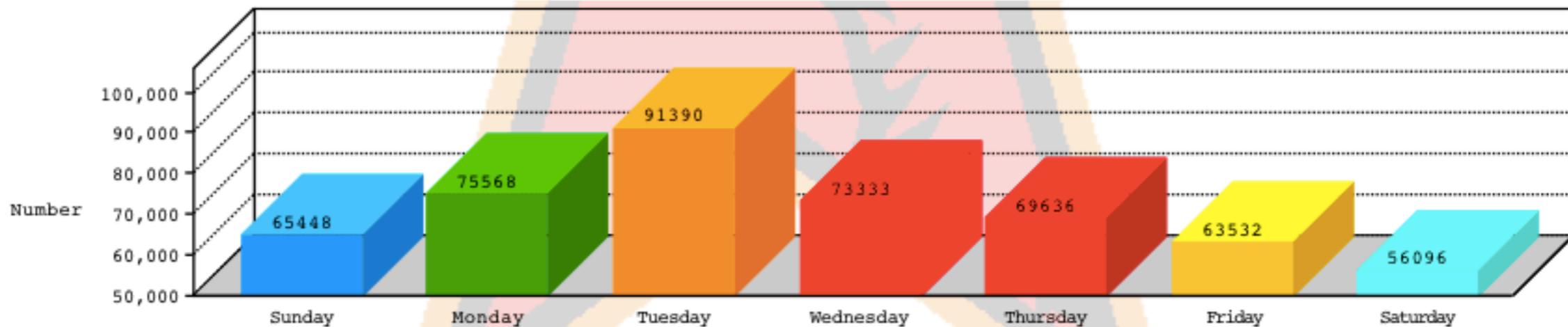
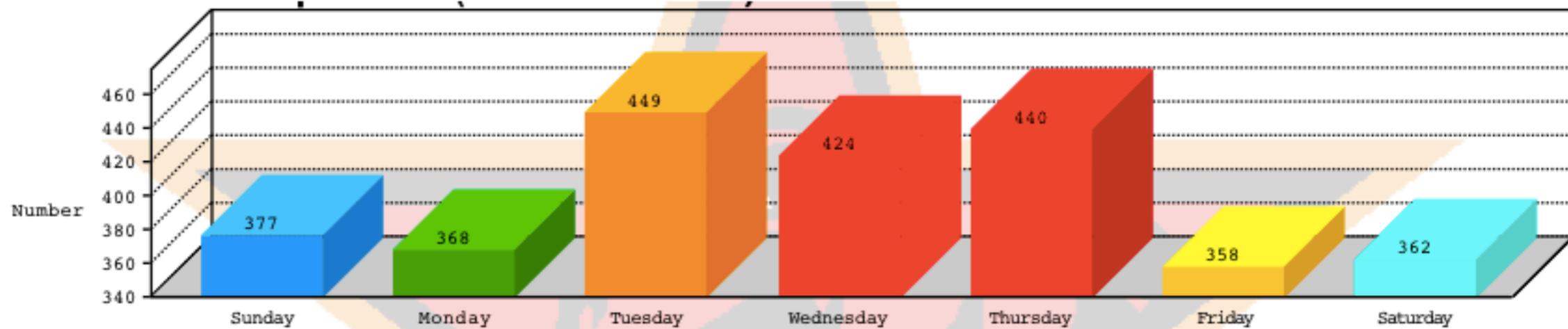
User Authentication  
Failed

# Trend Analysis

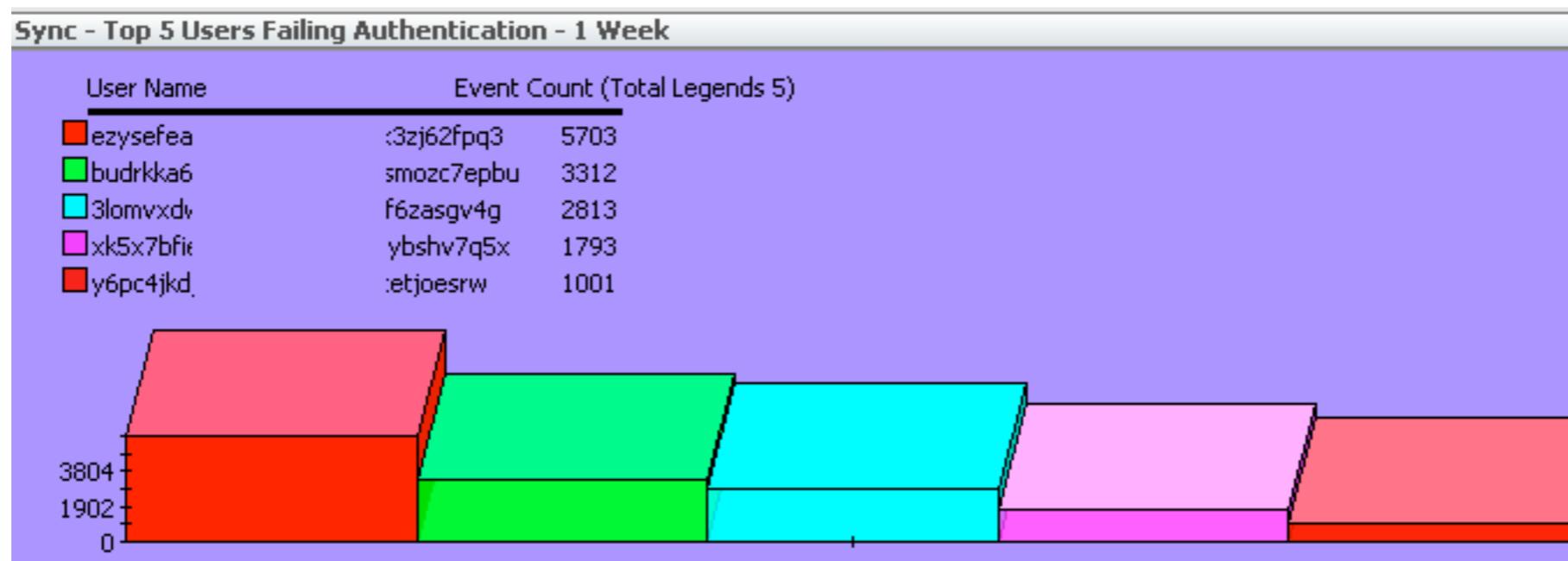
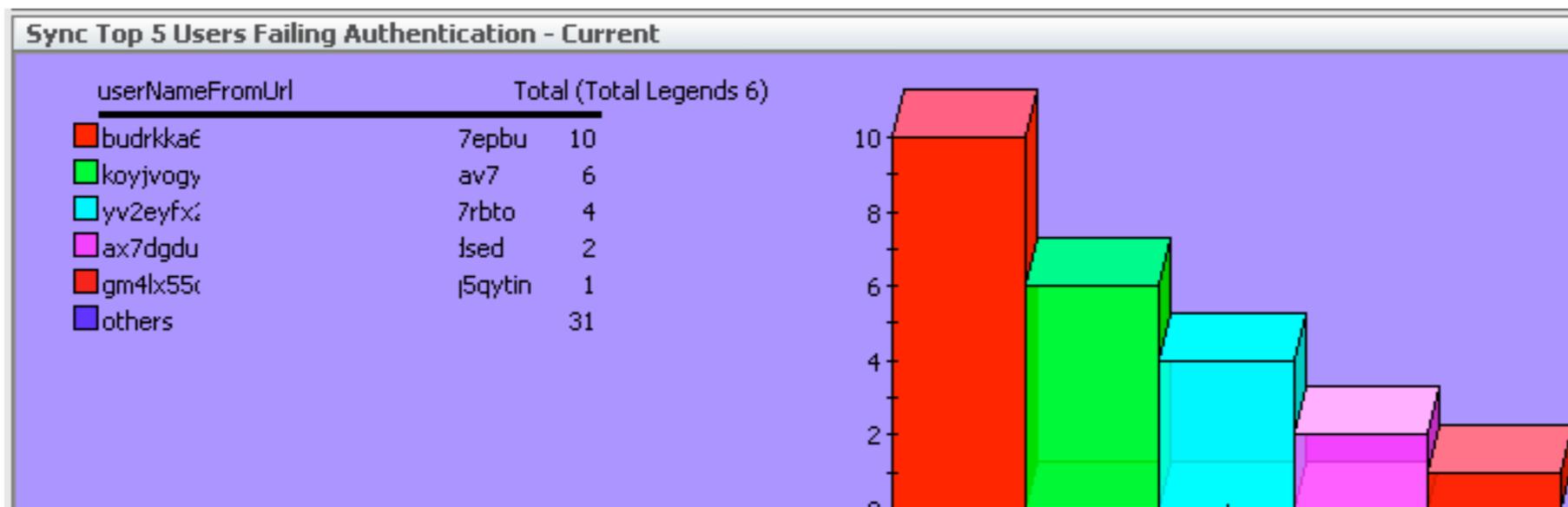


## Sync - Weekly Report

7 Day Window 08-29 to 09-04



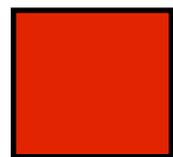
# Top Users Failing Auth within Application



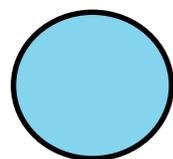
# App Use Mapping



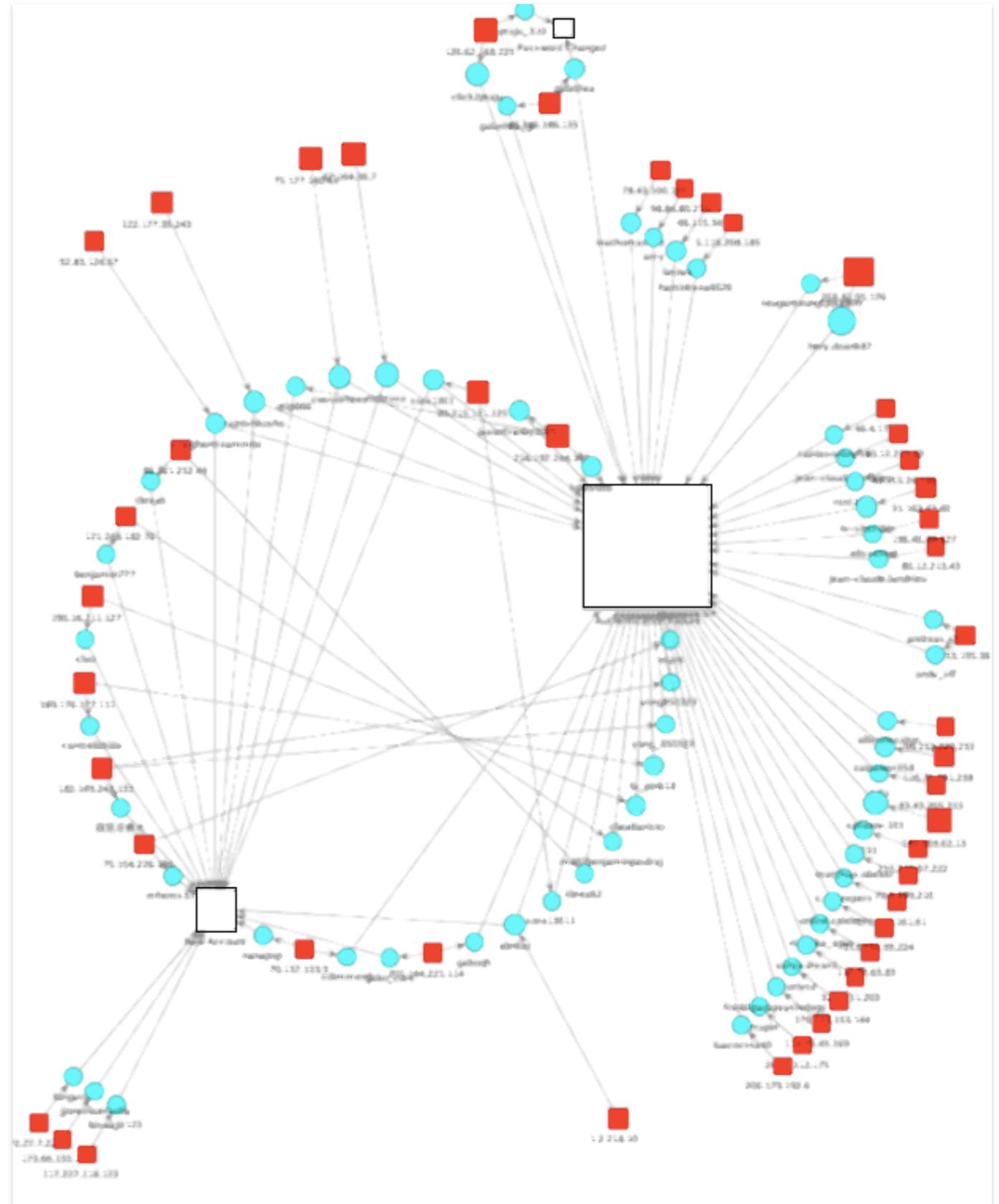
Operation



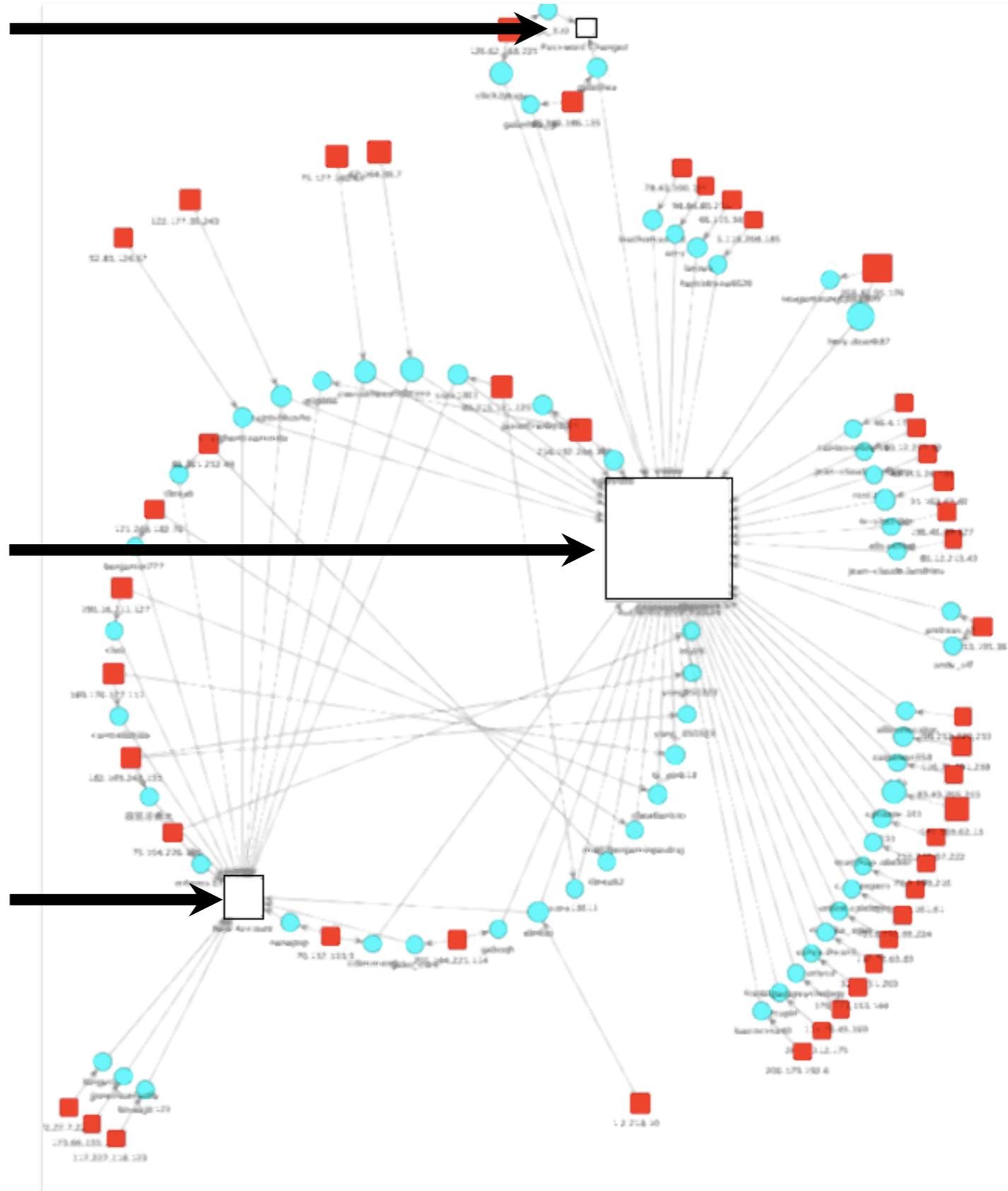
IP Address



Account



# Change Password

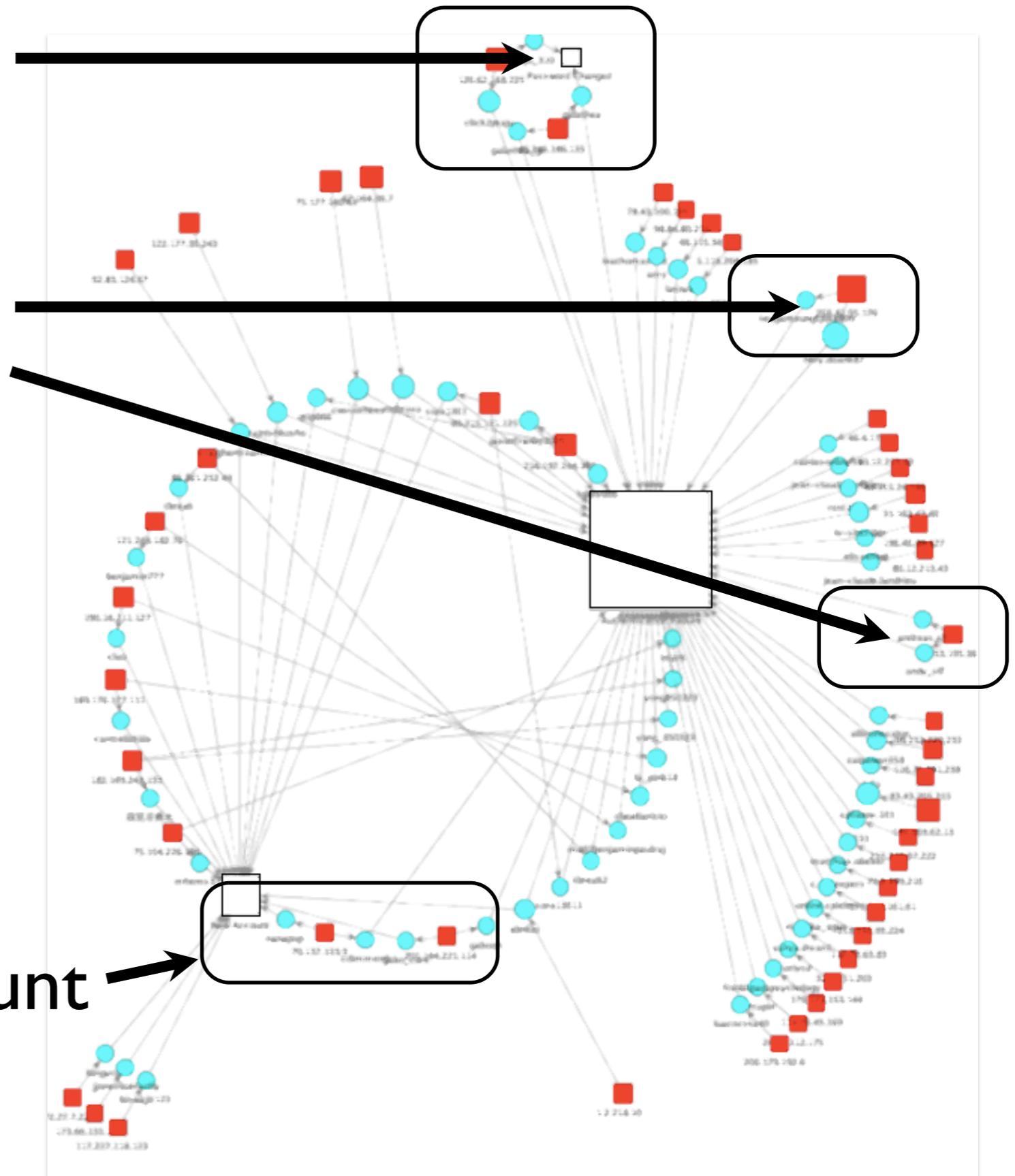


# Auth Failed

# New Account

acct 1 - pw change  
acct 2 - auth failed

1 IP Address,  
Multiple Users



Auth Fail, New Account

# Benefits

- Detecting Malicious Application Patterns
- Metrics for Application Level Use & Attacks
  - ▶ 900k CEF events per day
- Identify Application Bugs / Failures

# Summary

## Self Defending Applications:

- Detect Malicious Activity in Critical Apps
- Enable Immediate Response
- Prevent/Limit Compromise
- Require Organization Support

# Questions?

[http://www.owasp.org/index.php/Category:OWASP\\_AppSensor\\_Project](http://www.owasp.org/index.php/Category:OWASP_AppSensor_Project)

[owasp-appsensor-project@lists.owasp.org](mailto:owasp-appsensor-project@lists.owasp.org)

[michael.coates@owasp.org](mailto:michael.coates@owasp.org)

[mcoates@mozilla.com](mailto:mcoates@mozilla.com)

[michael-coates.blogspot.com](http://michael-coates.blogspot.com)

@\_mwc