Advanced Threat Modeling

A 50 Minute Session

cigital

Software Confidence. Achieved.

John Steven
Software Security Principal
Technical Director
Office of the CTO
Cigital Inc.

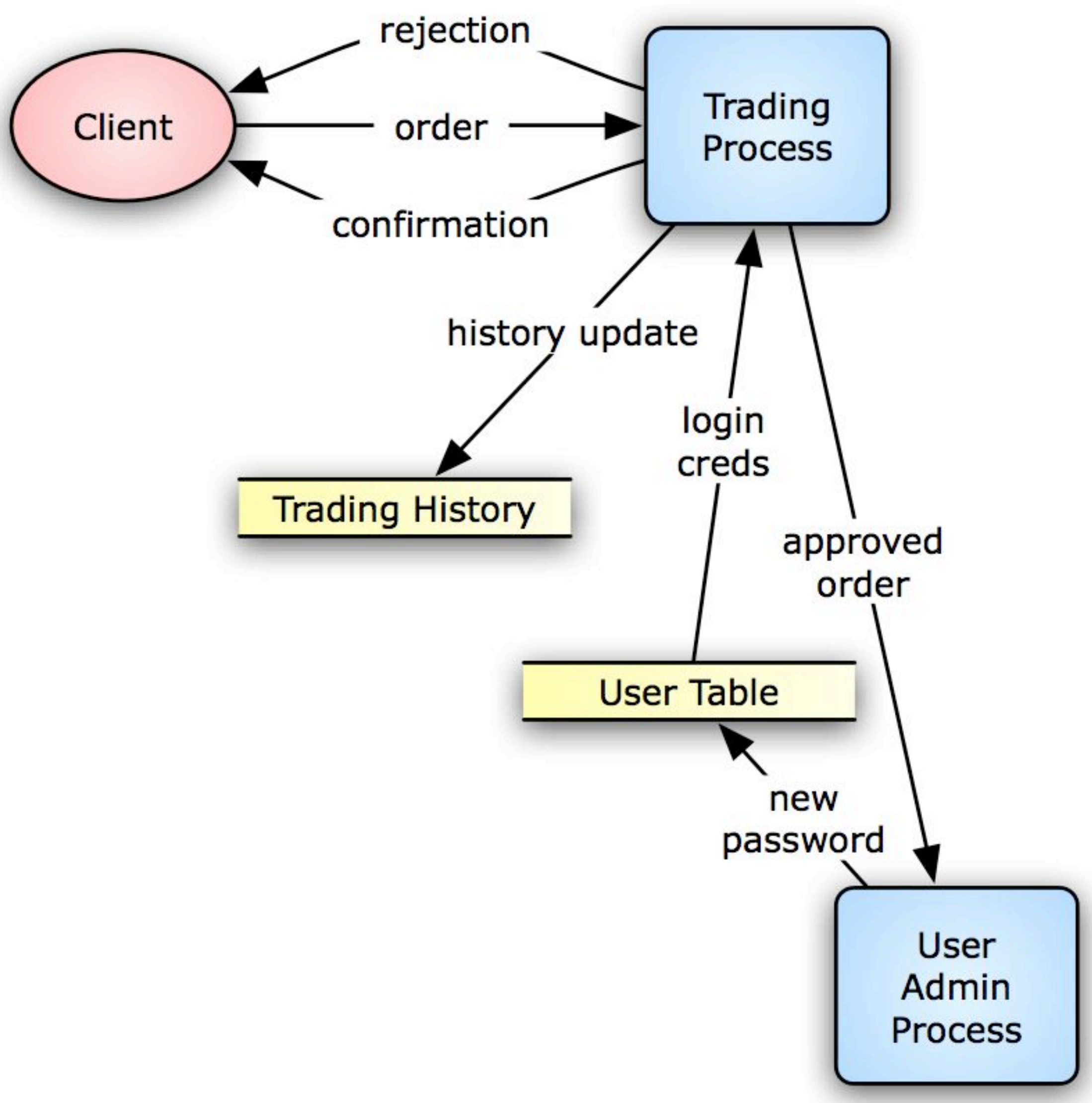
The many faces of threat modeling

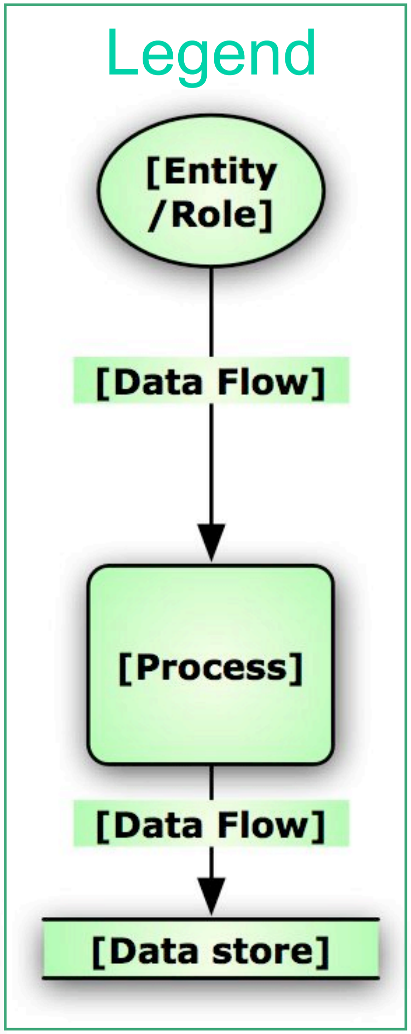
- What is a threat?
- Who builds a threat model?
- What are its critical elements?
- Who consumes it?
  - For what?

A Few Words on STRIDE

- A conceptual checklist
  - Backed by DFDs
- Given our previous slide, what’s good? What’s bad?

An Example DFD





cigital

Use Threat Modeling to Identify…

- Where potential threats exist relative to the architecture
- How threats escalate privilege
  - …become more formidable
- Specify vectors of attack
- Identifies components and assets worth protecting

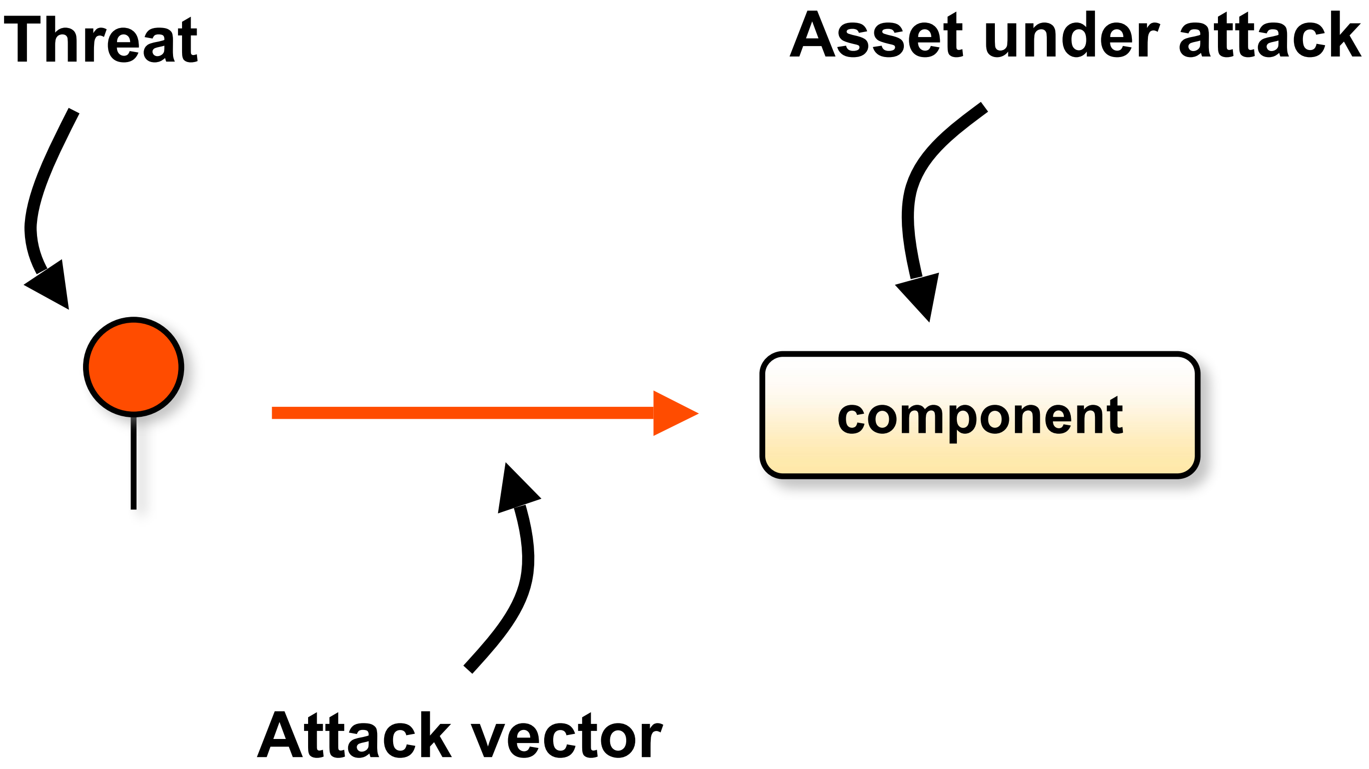
… Ties technical risk & business assets to application design;

…Ties attacks to role, privilege, and capability;

…Drives security analysis, testing.

cigital

The visual elements



Threat

Asset under attack

component

Attack vector

Sensitive Data Analysis

Sensitive data analysis and the human factor

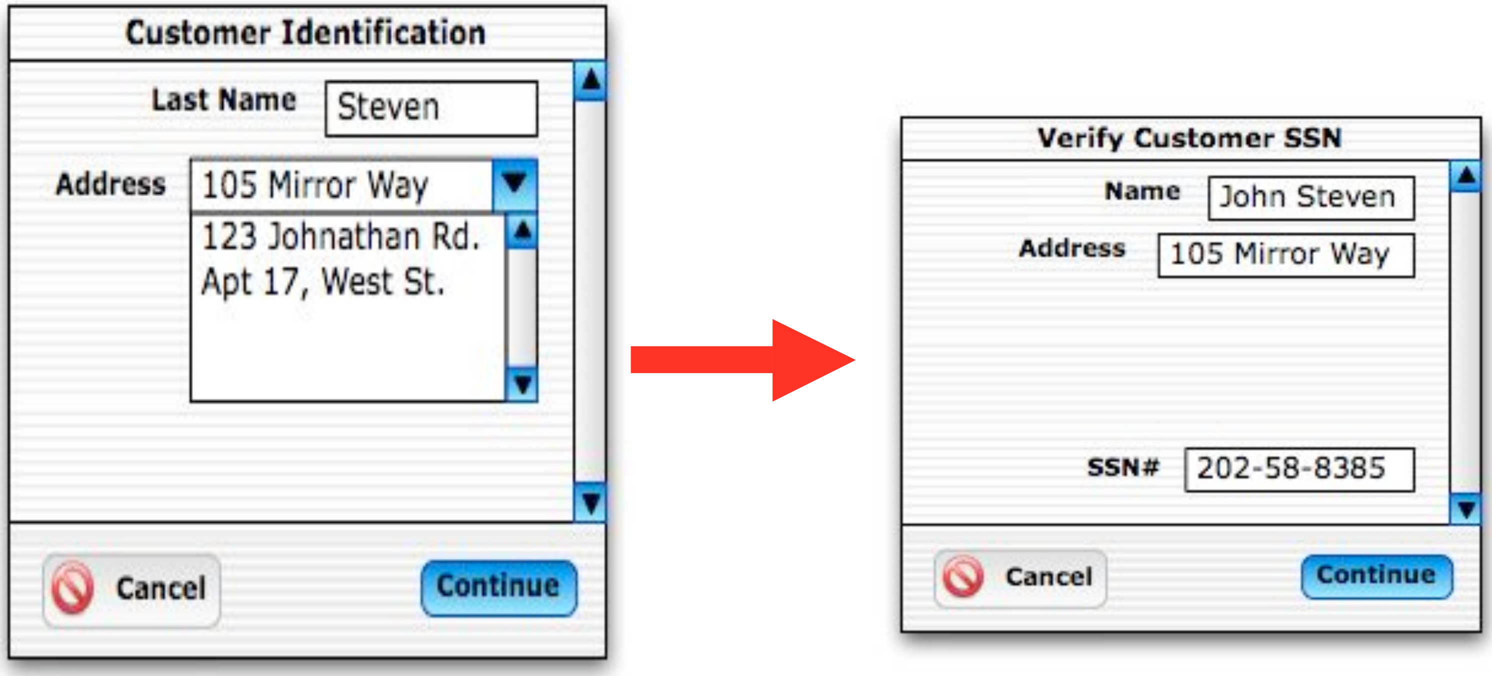
Example: Design for Sensitive Information

- *Steal credentials or secrets embedded in the client*
  - *Read client-cached values, even from different users*

- Example: Build a web-based customer service application:
  - Supports: account maintenance, password reset, etc.
  - Customer identified by Social Security Number (SSN)
  - Customer has a password for web application

cigital

Example Application Flow Begins



Customer Identification

Last Name: Steven

Address: 105 Mirror Way

123 Johnathan Rd.
Apt 17, West St.

Verify Customer SSN

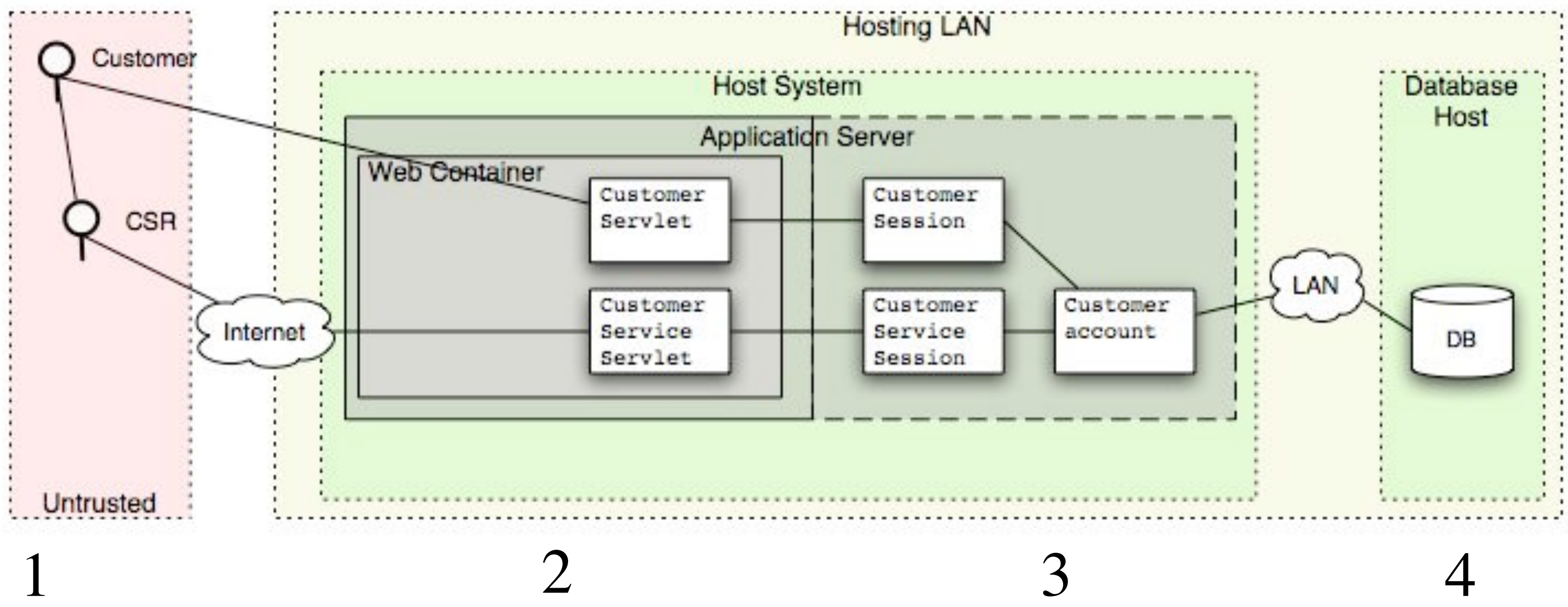
Name: John Steven

Address: 105 Mirror Way

SSN#: 202-58-8385

- “What’s your last name Sir?”
- “Verify your address.”
- “For security purposes, verify the last four digits of your social security number.”

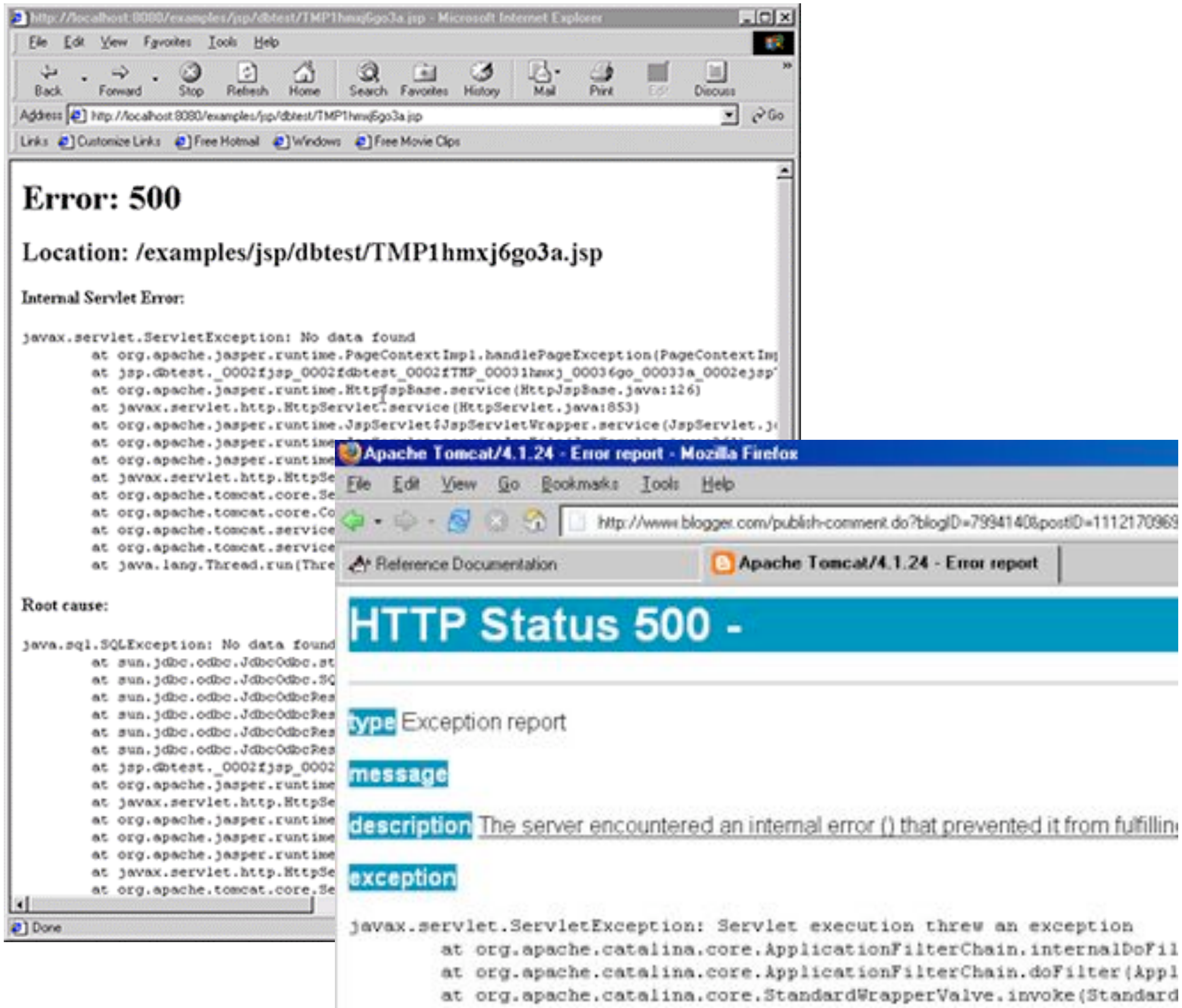
What does that imply about data in this system?



In what zones (by number) is what information present?
What design problems have we created for ourselves?

What are we going to do about it?

What kinds of users do these messages help?


http://localhost:8080/examples/jsp/dbtest/TMP1hmxj6go3a.jsp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://localhost:8080/examples/jsp/dbtest/TMP1hmxj6go3a.jsp
Go
Links Customize Links Free Hotmail Windows Free Movie Clips
Done

Error: 500

Location: /examples/jsp/dbtest/TMP1hmxj6go3a.jsp

Internal Servlet Error:

```
javax.servlet.ServletException: No data found
        at org.apache.jasper.runtime.PageContextImpl.handlePageException(PageContextIm
        at jsp.dbtest._0002fjsp_0002fdbtest_0002fTMP_00031hmxj_00036go_00033a_0002ejsp
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:126)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:853)
        at org.apache.jasper.runtime.JspServlet$JspServletWrapper.service(JspServlet.j
        at org.apache.jasper.runtime
        at org.apache.jasper.runtime
        at javax.servlet.http.HttpSe
        at org.apache.tomcat.core.Se
        at org.apache.tomcat.core.Co
        at org.apache.tomcat.service
        at org.apache.tomcat.service
        at java.lang.Thread.run(Thre
```

Root cause:

```
java.sql.SQLException: No data found
        at sun.jdbc.odbc.JdbcOdbc.st
        at sun.jdbc.odbc.JdbcOdbc.SQ
        at sun.jdbc.odbc.JdbcOdbcRes
        at sun.jdbc.odbc.JdbcOdbcRes
        at sun.jdbc.odbc.JdbcOdbcRes
        at sun.jdbc.odbc.JdbcOdbcRes
        at jsp.dbtest._0002fjsp_0002
        at org.apache.jasper.runtime
        at javax.servlet.http.HttpSe
        at org.apache.jasper.runtime
        at org.apache.jasper.runtime
        at org.apache.jasper.runtime
        at javax.servlet.http.HttpSe
        at org.apache.tomcat.core.Se
```

Apache Tomcat/4.1.24 - Error report - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.blogger.com/publish-comment.do?blogID=7994140&postID=111217096
Reference Documentation
Apache Tomcat/4.1.24 - Error report

HTTP Status 500 -

type Exception report

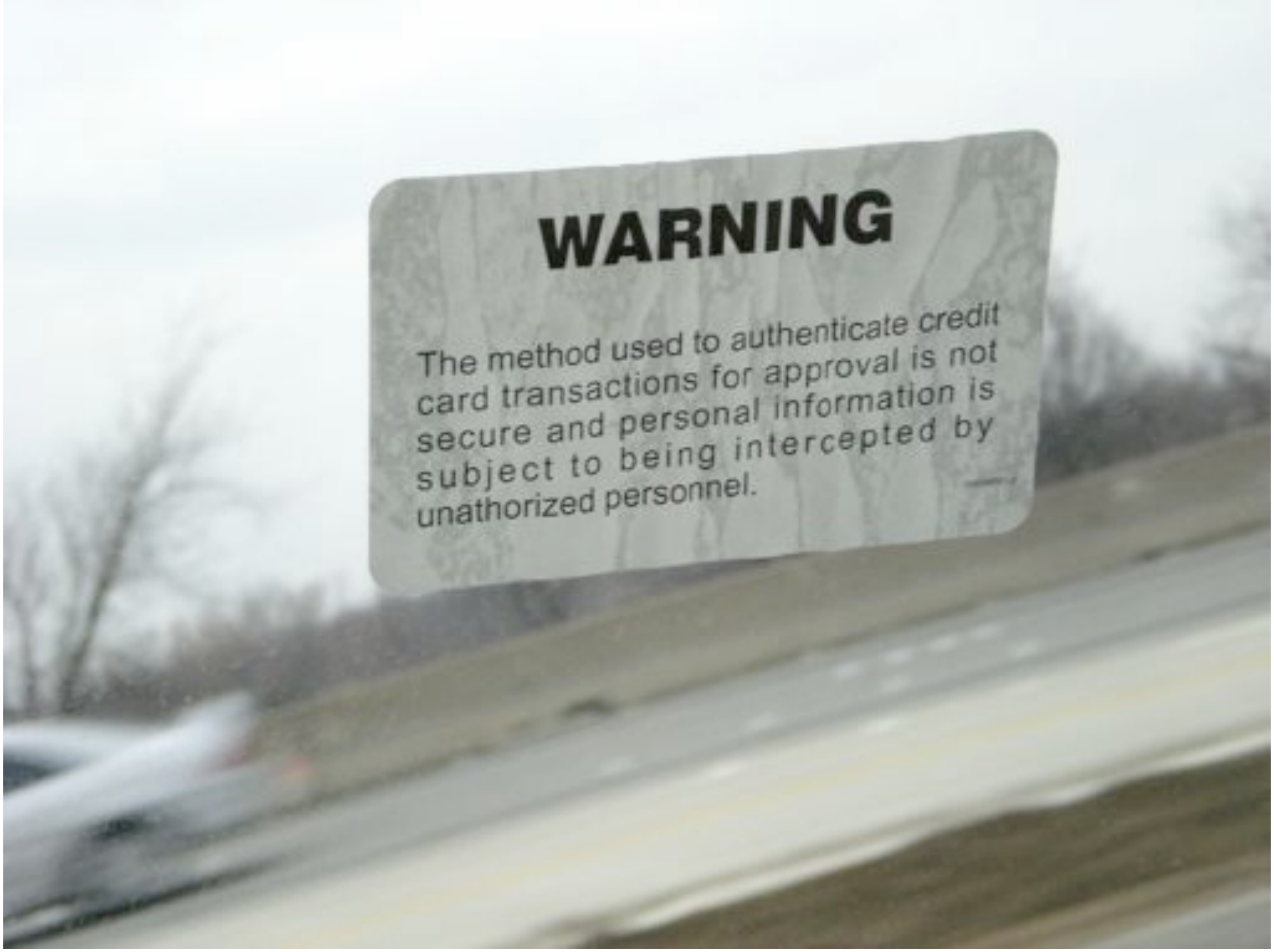
message

description The server encountered an internal error () that prevented it from fulfillin

exception

```
javax.servlet.ServletException: Servlet execution threw an exception
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFil
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(Appl
        at org.apache.catalina.core.StandardWrapperValve.invoke(Standard
```

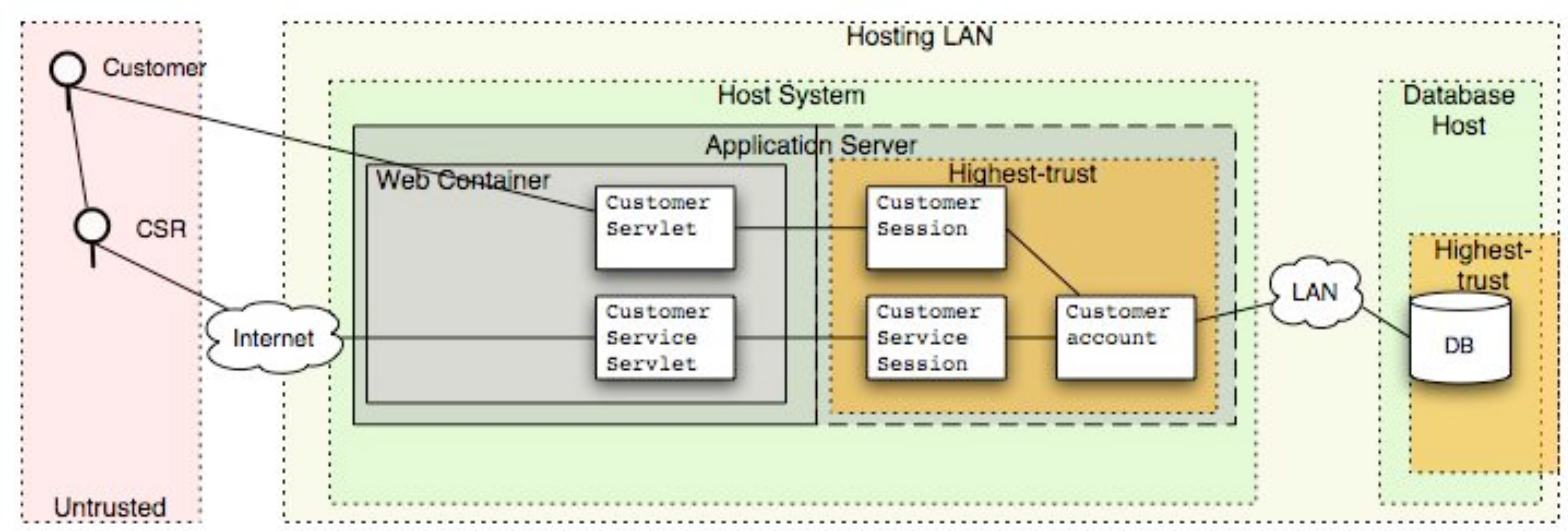
Users often make bad decisions



WARNING

The method used to authenticate credit card transactions for approval is not secure and personal information is subject to being intercepted by unathorized personnel.

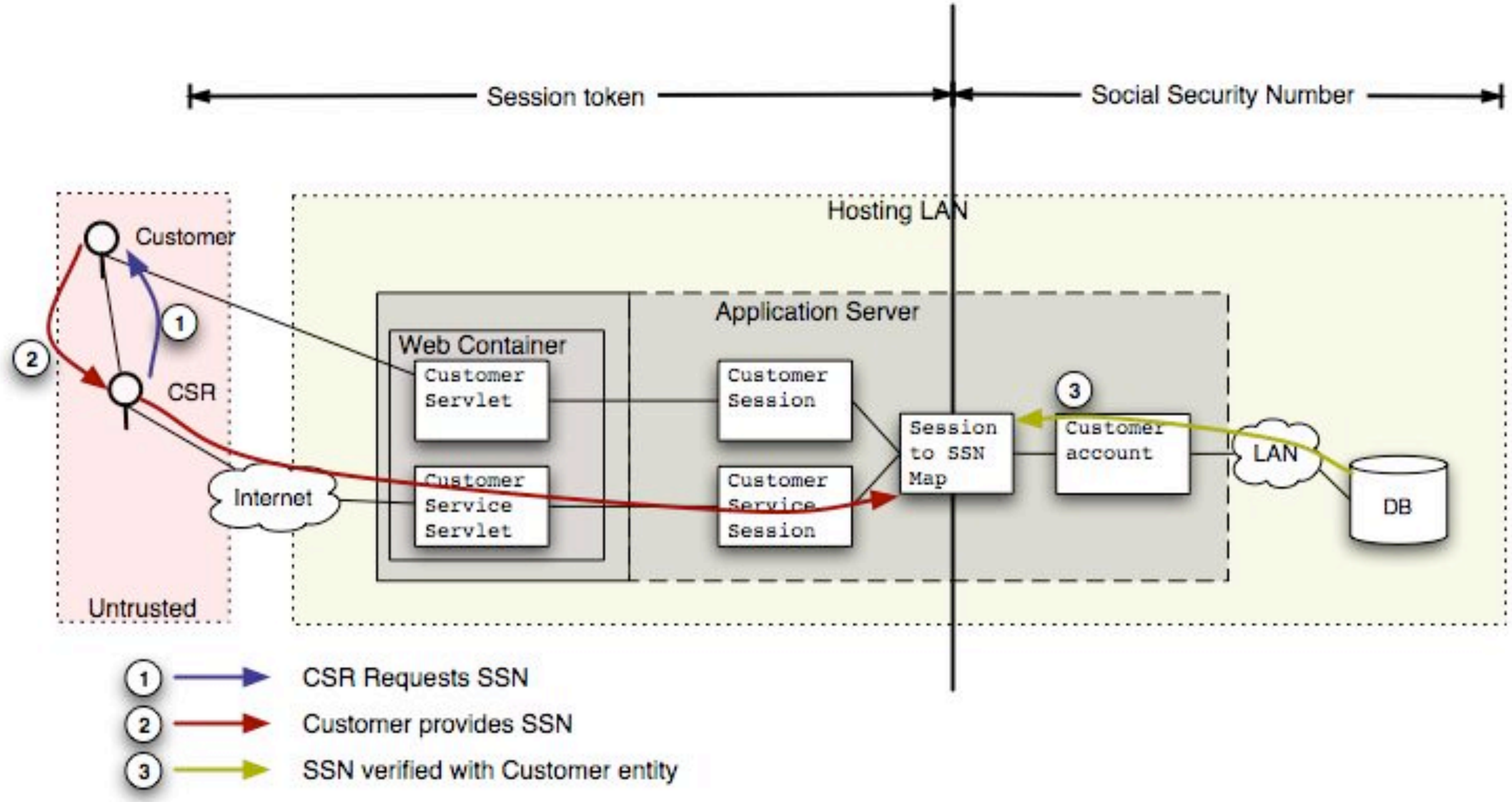
Build Trust Zones into the Application



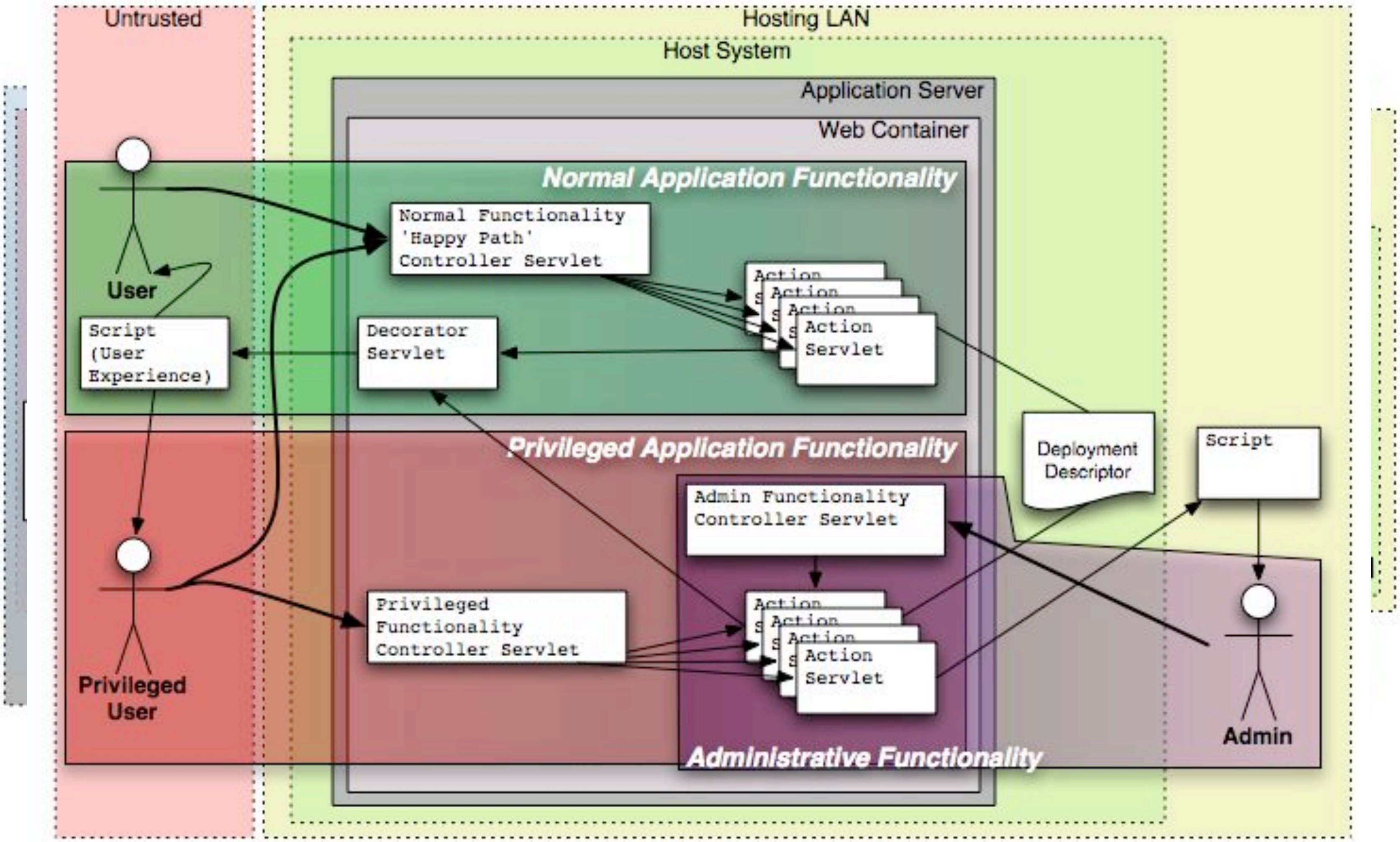
- Why should sensitive information leave the marked high-trust zone?

1. The customer knows their SSN, don’t present them with it
2. The CSR should ask for and enter the SSN, not be presented with it
3. Use programmatic means to verify SSN in the application server

What That Might Look Like



Using Structure to Separate Privilege


Untrusted
Hosting LAN
Host System
Application Server
Web Container
Normal Application Functionality
Normal Functionality 'Happy Path' Controller Servlet
Action Servlet
User
Script (User Experience)
Decorator Servlet
Privileged Application Functionality
Admin Functionality Controller Servlet
Deployment Descriptor
Script
Privileged User
Privileged Functionality Controller Servlet
Admin
Administrative Functionality

Threat Modeling: Methodology

Anchor in Software Architecture

Consider where attacks occur

Top-down

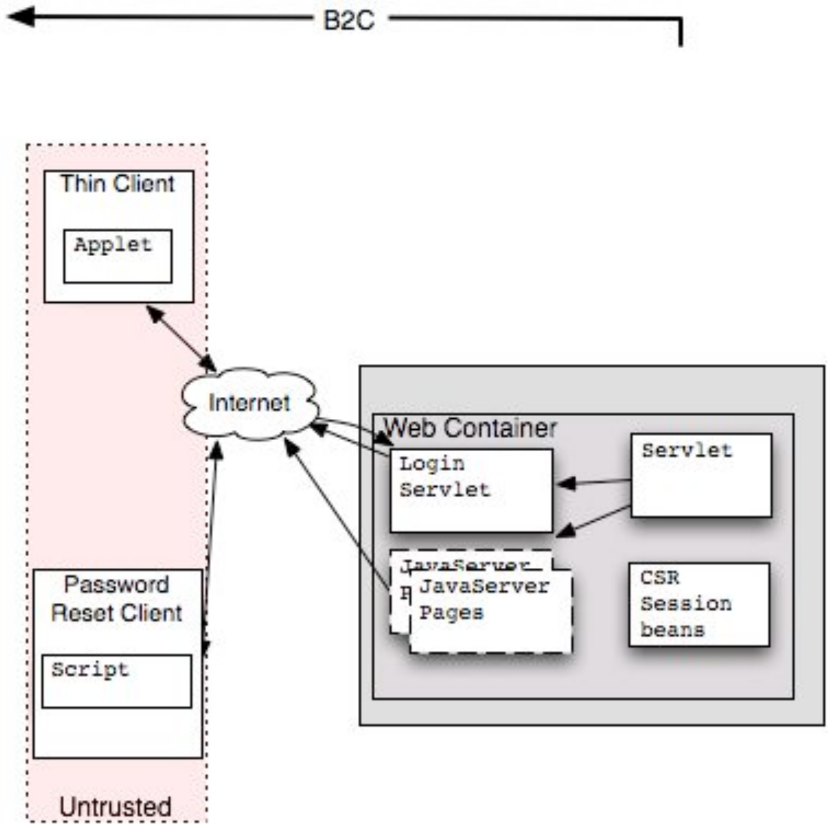
- Enumerate business objects
  - Sensitive data
  - Privileged functionality

Bottom-up

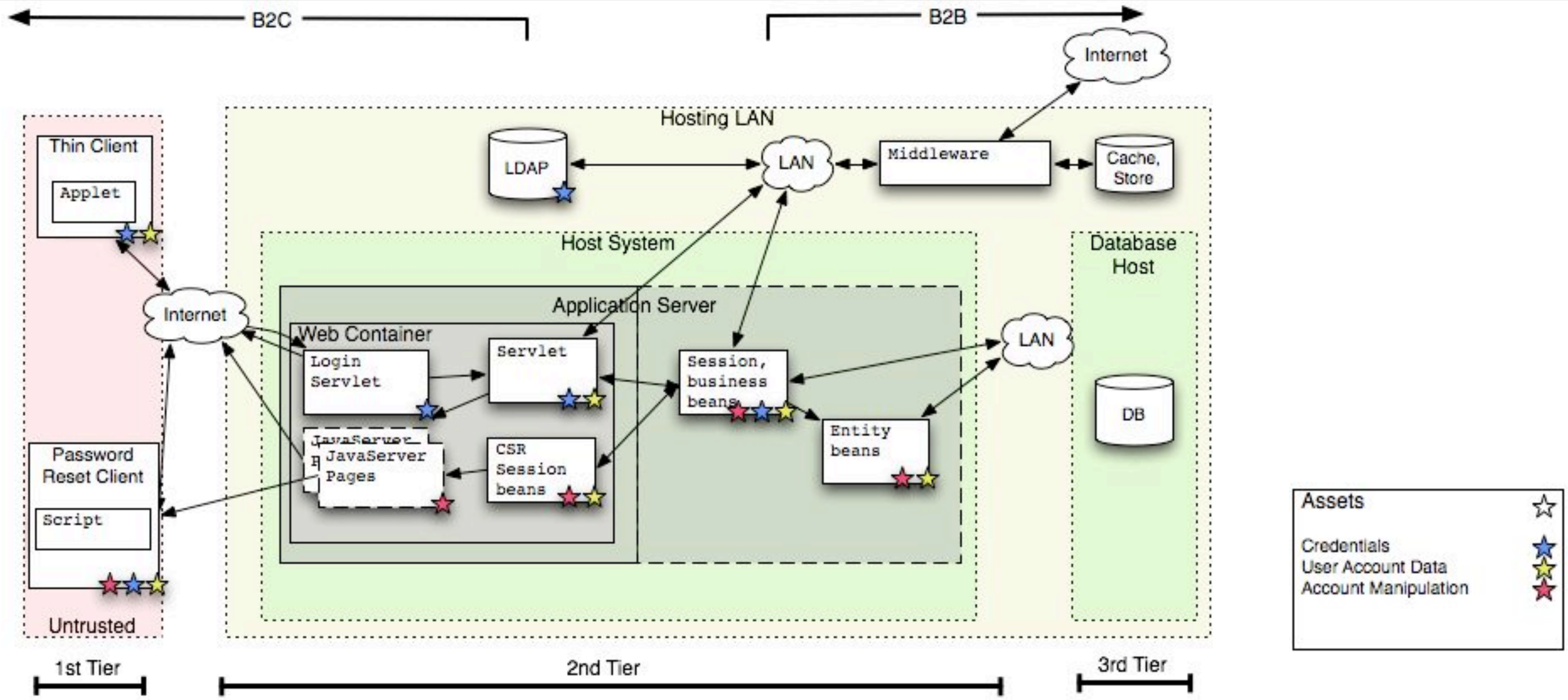
- Enumerate application entities
  - Sensitive data
  - Privileged functionality

Look for

- Middleware
- Open source
- Frameworks



Identify Critical Application Assets



Identify

- Sensitive data
- Privileged function

What would trust zones look like?

Look out for:

- Proxies, facades, etc.
- Services: ws-, beans, etc.
- UI vs. implementation
- Aggressive caching schemes

Anchor Threats in Use Cases

Consider attack surface

- Actors become Threats
- Use becomes misuse

Top-down

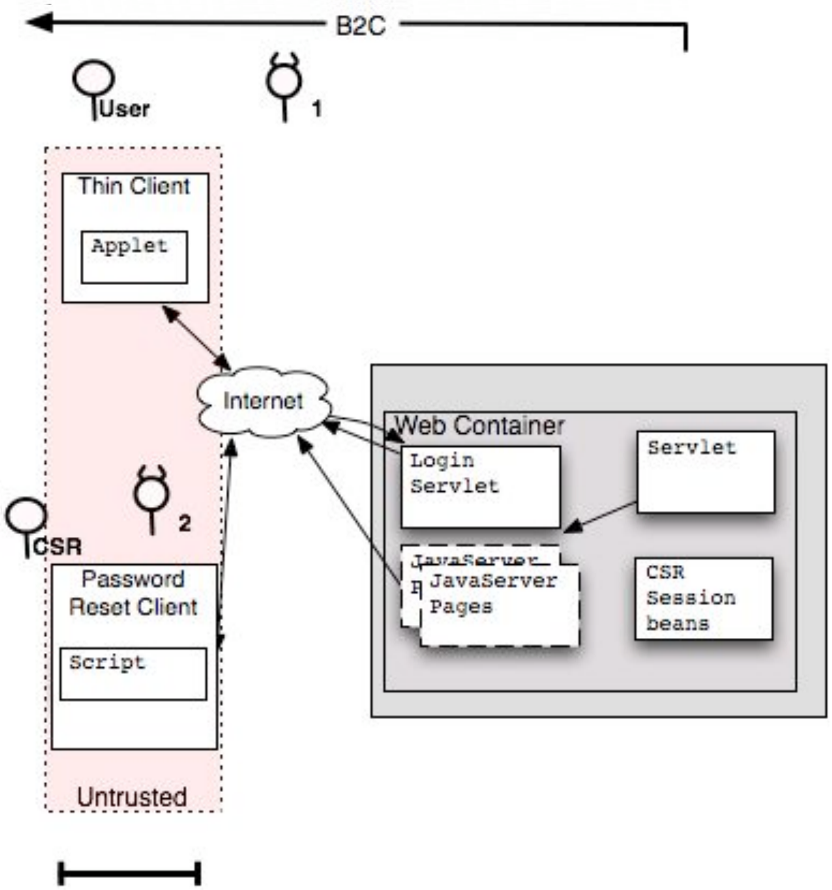
- Enumerate elements closest to Threat actors

Bottom-up

- Think like code analysis tool

Look for:

- Interfaces, services
- Systems, Proxies
- Middleware
- Inputs (of any kind)



Start with ‘high value’ Attack Vectors

Annotating with initial attacks

- Select a target objective
- Chose attacks that bridge gap

Top-down

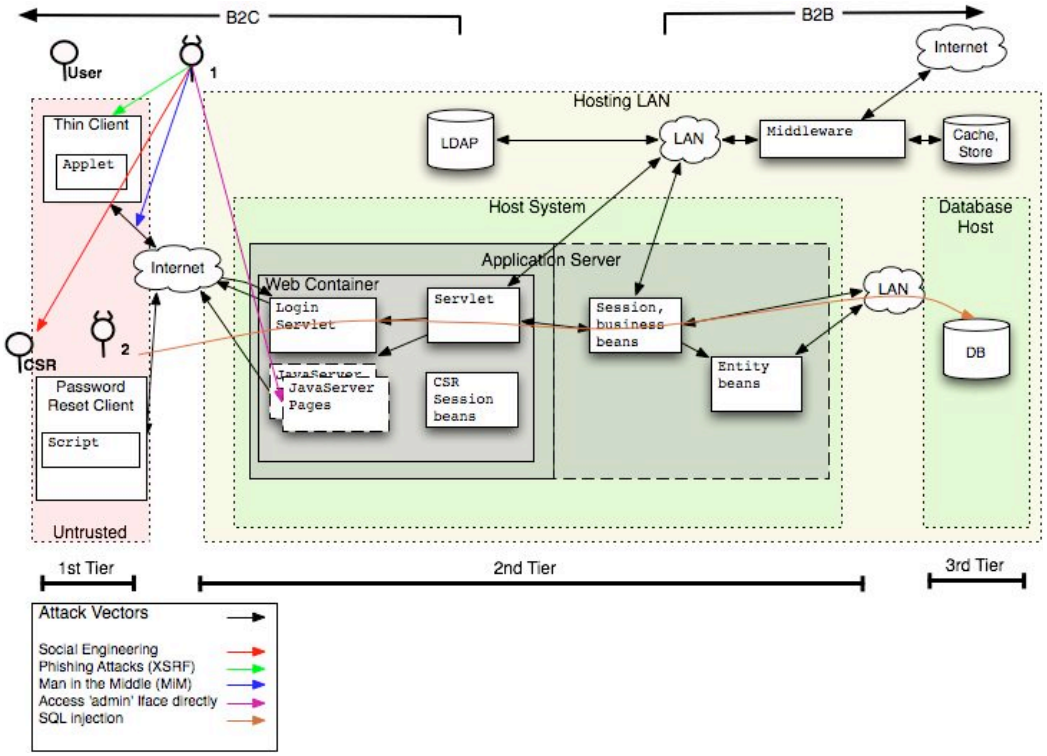
- Pilfer community resources

Bottom-up

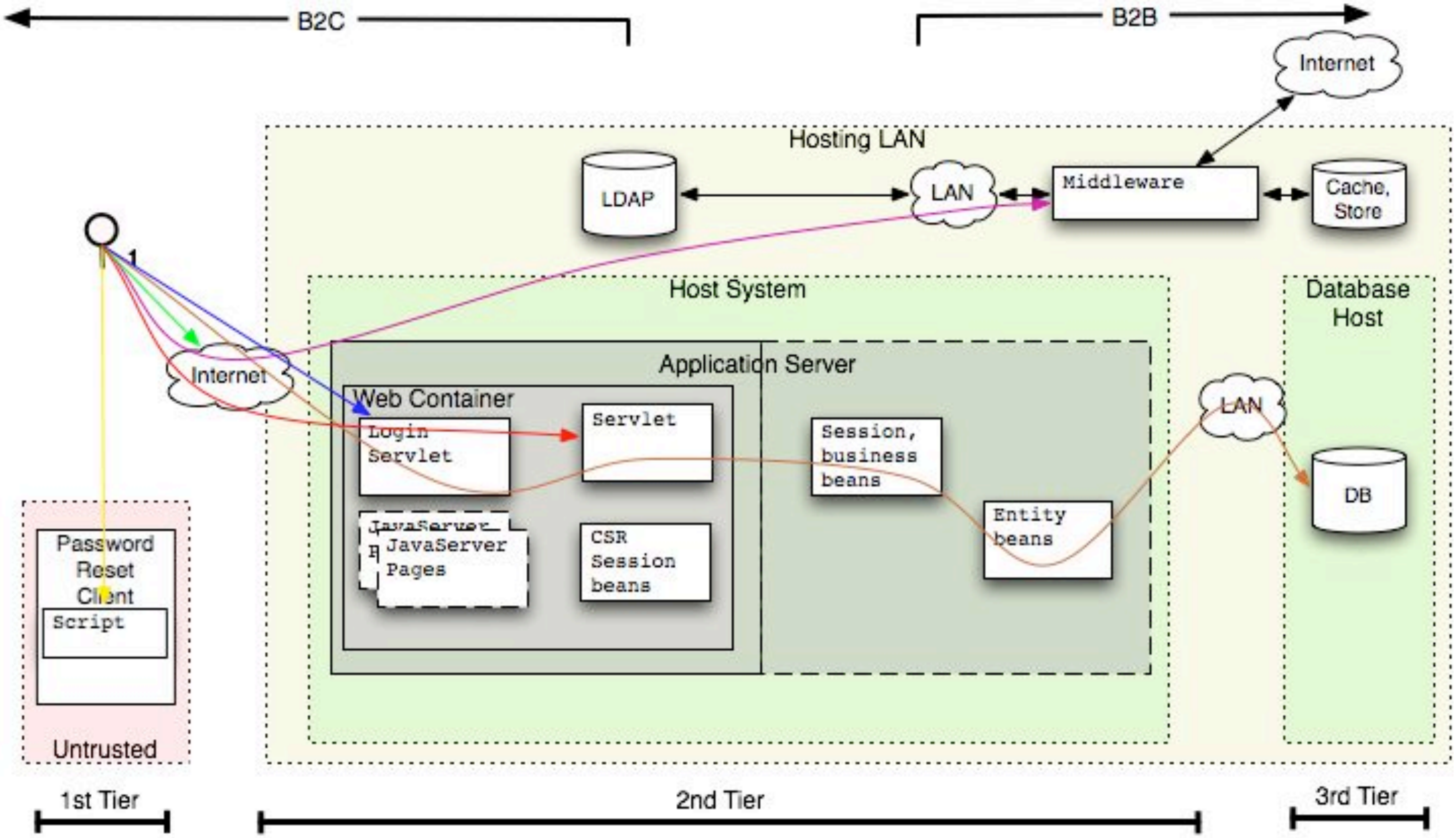
- Conceive properties an unknown attack might have

Look for:

- Assets close to surface
- Shortest paths
- Attacks that target tiers



Example #1: Threats Facing Web Authentication



Attack Vectors →

- Access w/o authentication →
- Sniff, reuses existing credentials →
- Password guessing (dictionary, etc.) →
- Log into downstream EIS →
- Lift credentials through injection →
- Lift credentials from client →

System/Net Arch. ⬚

- Untrusted ▨
- Hosting LAN ▨
- Application Host ▨
- Database Host ▨
- High-trust (App.) ▨

Threats

1 - Internet-based Attacker (unauthorized)

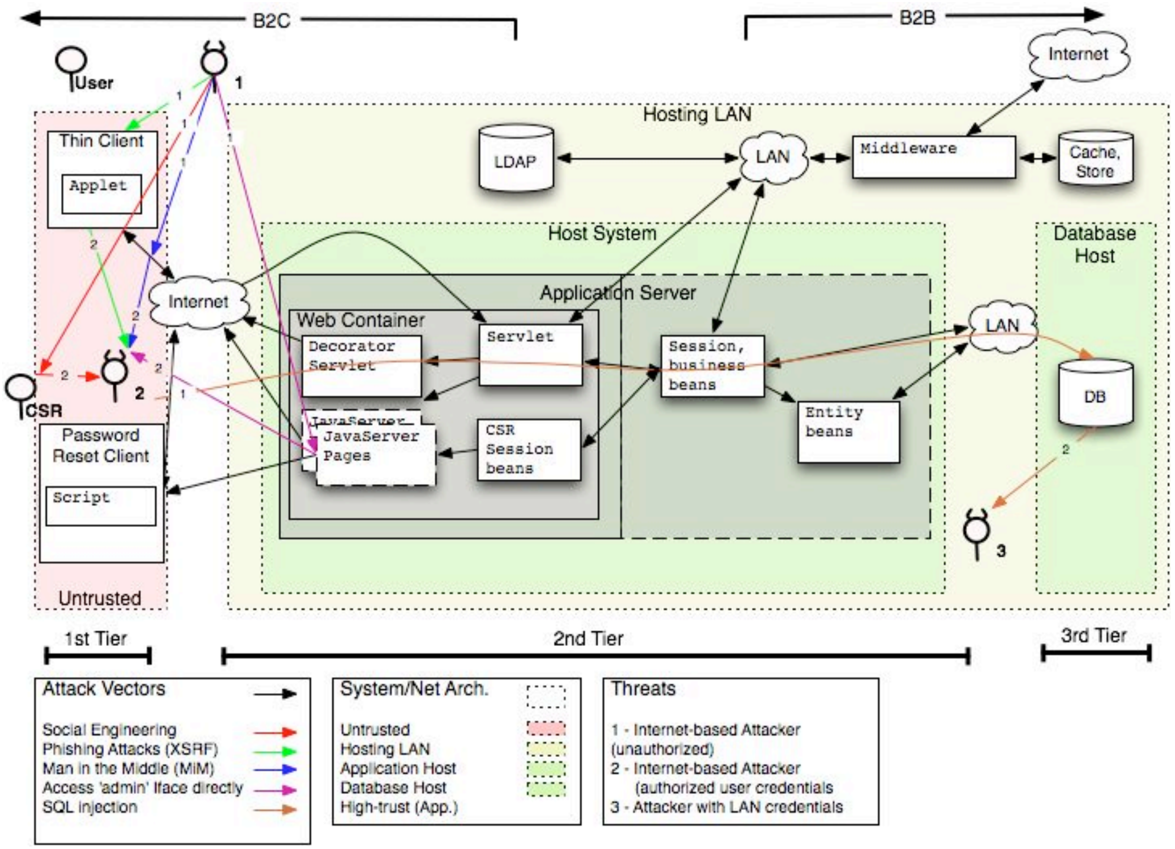
2 - Internet-based Attacker (authorized user credentials

3 - Attacker with LAN credentials

More Advanced Threat Modeling Techniques

cigital

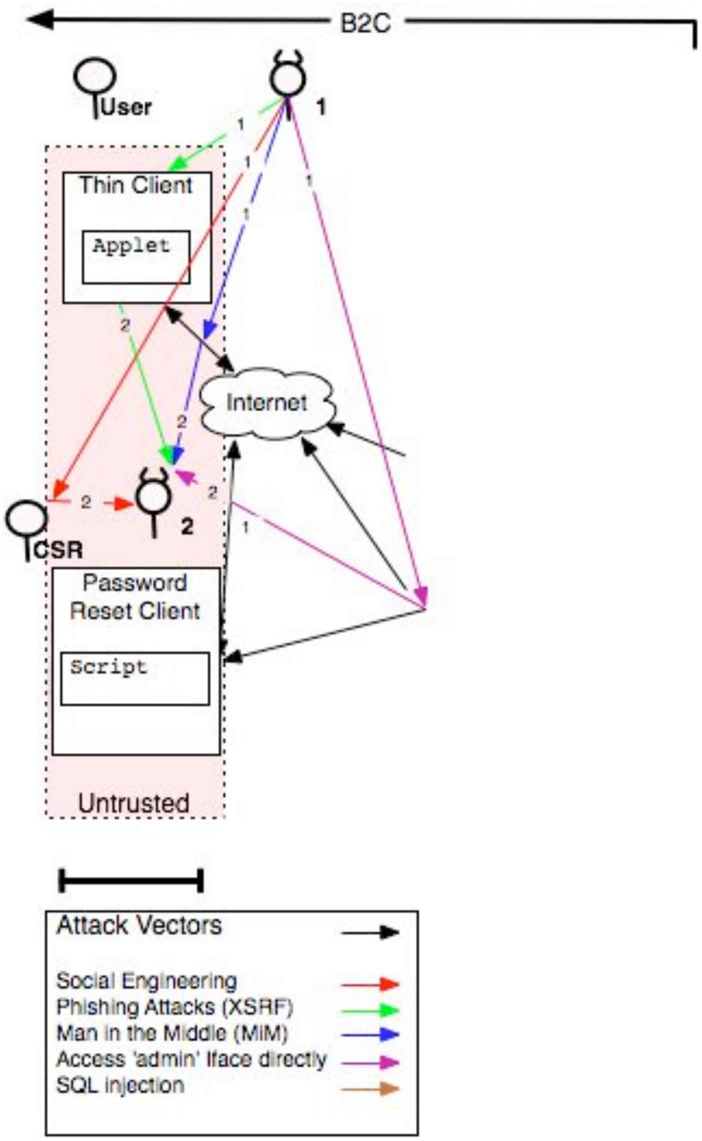
Tips & Tricks #1: Threat Privilege Escalation



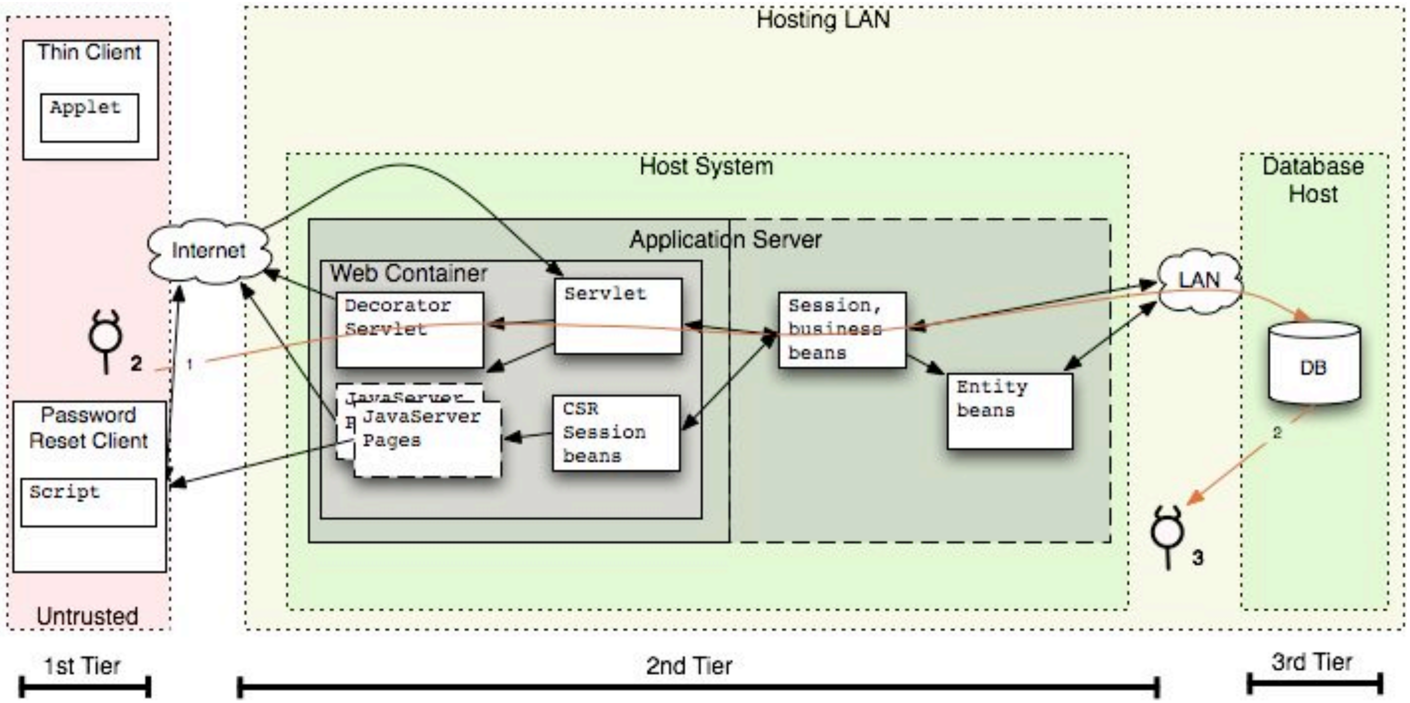
- Integrate with entitlement specification
  - Show escalation of privilege
  - Motivate probability of ‘insider’ attack

Privilege Escalation: How to do it.

- Tackle each escalation separately
- Don't duplicate work
  - Steal this escalation for your T.M. "cookbook"
  - Ignore escalation through esoteric means at first
- Consider social, physical means where simpler than software-based attacks
  - Password reset
  - Stolen fobs
  - Phishing

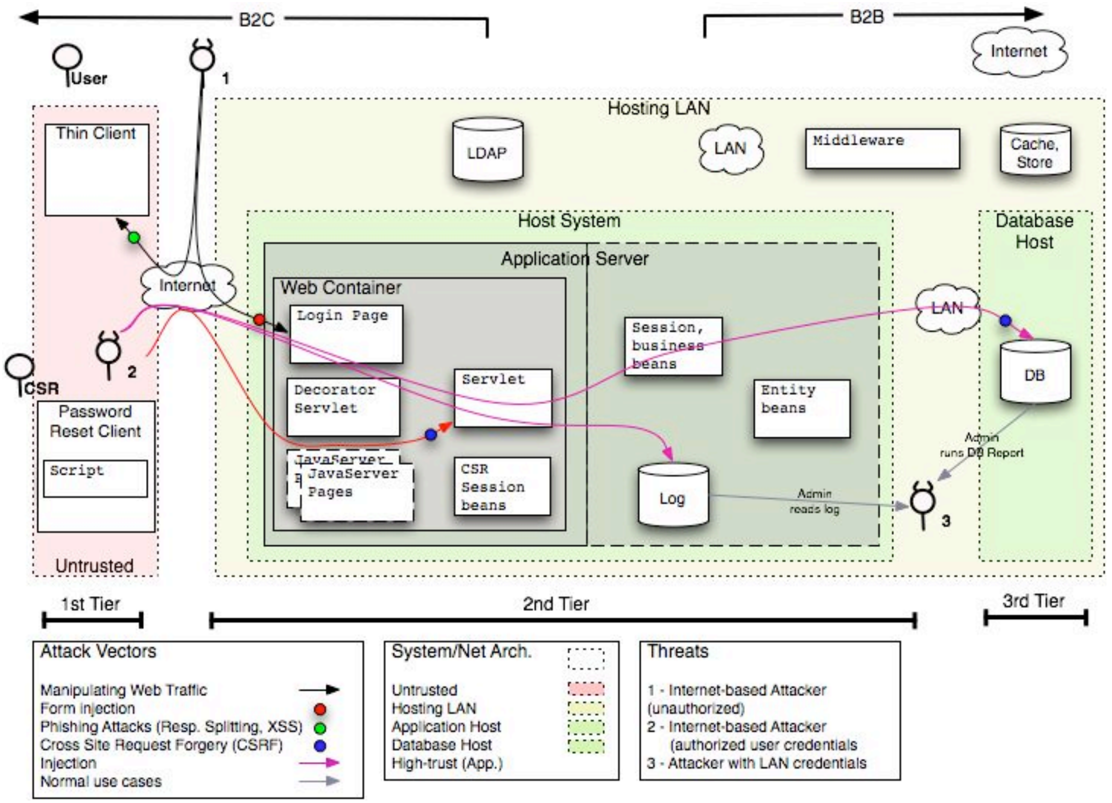


Overcoming Objections



- Remember:
  - Focus on common, simple attacks
  - Escalation to admin/LAN credential possible where credential stores reside in site database
  - ‘insiders’ need not be

Tips #2: Target Using Layered Attacks



Attack Vectors

- Manipulating Web Traffic →
- Form injection ●
- Phishing Attacks (Resp. Splitting, XSS) ●
- Cross Site Request Forgery (CSRF) ●
- Injection →
- Normal use cases →

System/Net Arch.

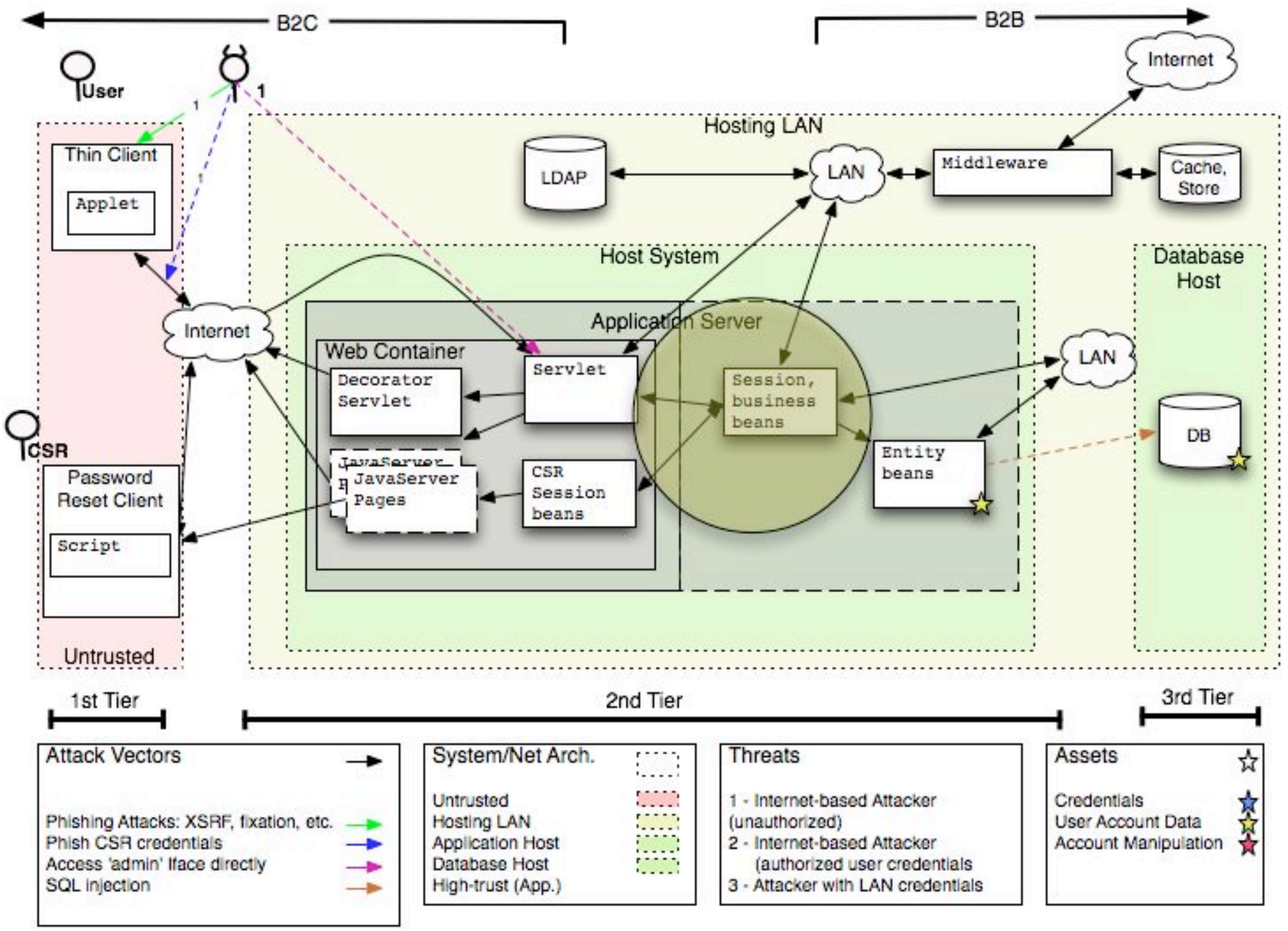
- Untrusted
- Hosting LAN
- Application Host
- Database Host
- High-trust (App.)

Threats

1 - Internet-based Attacker (unauthorized)
2 - Internet-based Attacker (authorized user credentials)
3 - Attacker with LAN credentials

- Bootstrap later attacks with those that ‘deliver’
  - Use one layer to exploit another (net, app)
  - Combine attacks to reach desired target

Tips #3: Filling the Gaps…



- How do we design tests to fill this gap?

cigital

Take Homes

- Base Threat Model in *software architecture*
- When specific *use (cases)* and high-level architecture are defined:
  - Inventory roles, entitlements, if one doesn't exist
  - Inventory assets: sensitive data, privileged components
- Enumerate initial *attack vectors*
  - Use common 'low-hanging' fruit
- Elaborate more attacks
  - Find opportunities for privilege escalation
  - Layer attacks to target or 'hop' to assets
  - Fill in gaps by 'inventing' attacks
- Use Threat Modeling to drive security testing:

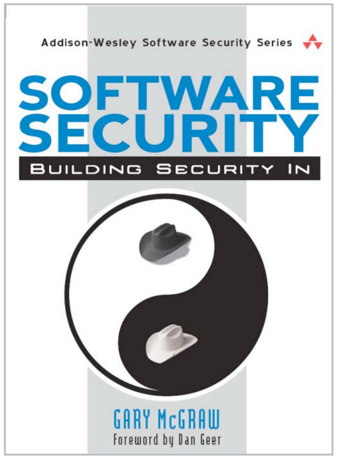
cigital

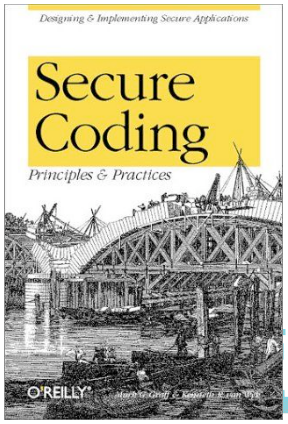
For More

- Cigital's Software Security Group invents and delivers Software Quality Management
- See the Addison-Wesley Software Security series
- What areas are you interested in?

"So now, when we face a choice between adding features and resolving security issues, we need to choose security."

-Bill Gates




Designing & Implementing Secure Applications
Secure Coding
Principles & Practices
O'REILLY
Mark G. Graff & Kenneth R. van Wyk

Thank you for your time

John Steven

jsteven@cigital.com

cigital

Software Confidence. Achieved.

www.cigital.com
info@cigital.com
+1.703.404.9293