ARCHITECTURAL RISK ANALYSIS

ILYA VERBITSKIY

@ILICH_X86

INTRODUCTION

- ILYA VERBITSKIY
- “ON CALL” CTO
- SDLC & ARCHITECTURE CONSULTANT
- 15 YEARS IN FINANCE AND E-COMMERCE INDUSTRIES
- HTTPS://VERBITSKIY.CO/

SECURITY BUGS VS. DESIGN FLAWS

- ISSUE IN SOURCE CODE
- ONE COMPONENT AFFECTED
- NO IMPACT ON SYSTEM ARCHITECTURE
- AUTOMATION
- EASY TO FIX

- MULTIPLE COMPONENTS AFFECTED
- IMPACT ON SYSTEM ARCHITECTURE
- NO AUTOMATION
- HARD TO DISCOVER AND FIX

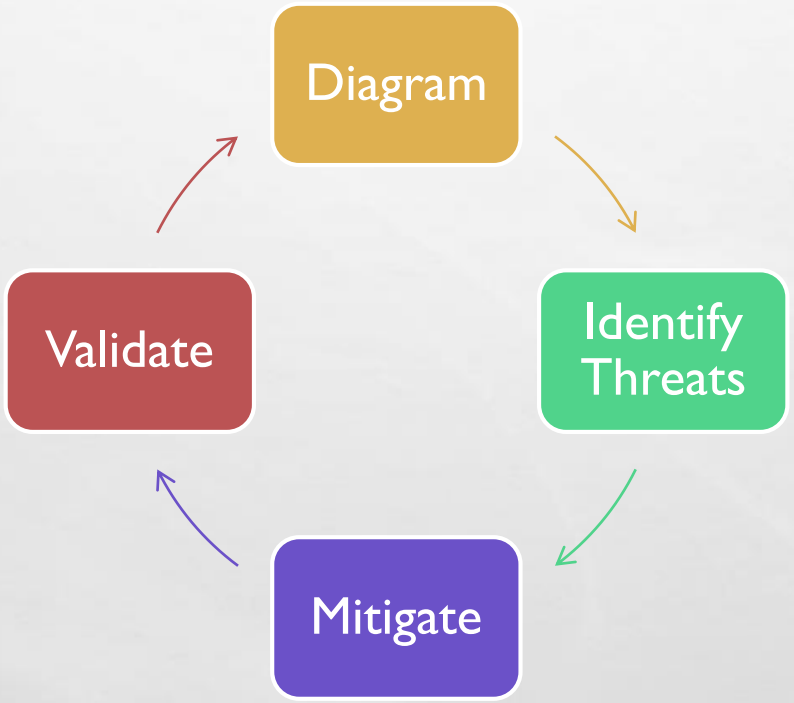
OWASP TOP 10 2017

- A1 – INJECTION
- A3 – CROSS-SITE SCRIPTING (XSS)
- A5 – SECURITY MISCONFIGURATION
- A7 – INSUFFICIENT ATTACK PROTECTION
- A8 – CROSS-SITE REQUEST FORGERY (CSRF)
- A9 – USING COMPONENTS WITH KNOWN VULNERABILITIES
- A2 – BROKEN AUTHENTICATION AND SESSION MANAGEMENT
- A4 – BROKEN ACCESS CONTROL
- A6 – SENSITIVE DATA EXPOSURE
- A10 – UNDERPROTECTED APIS

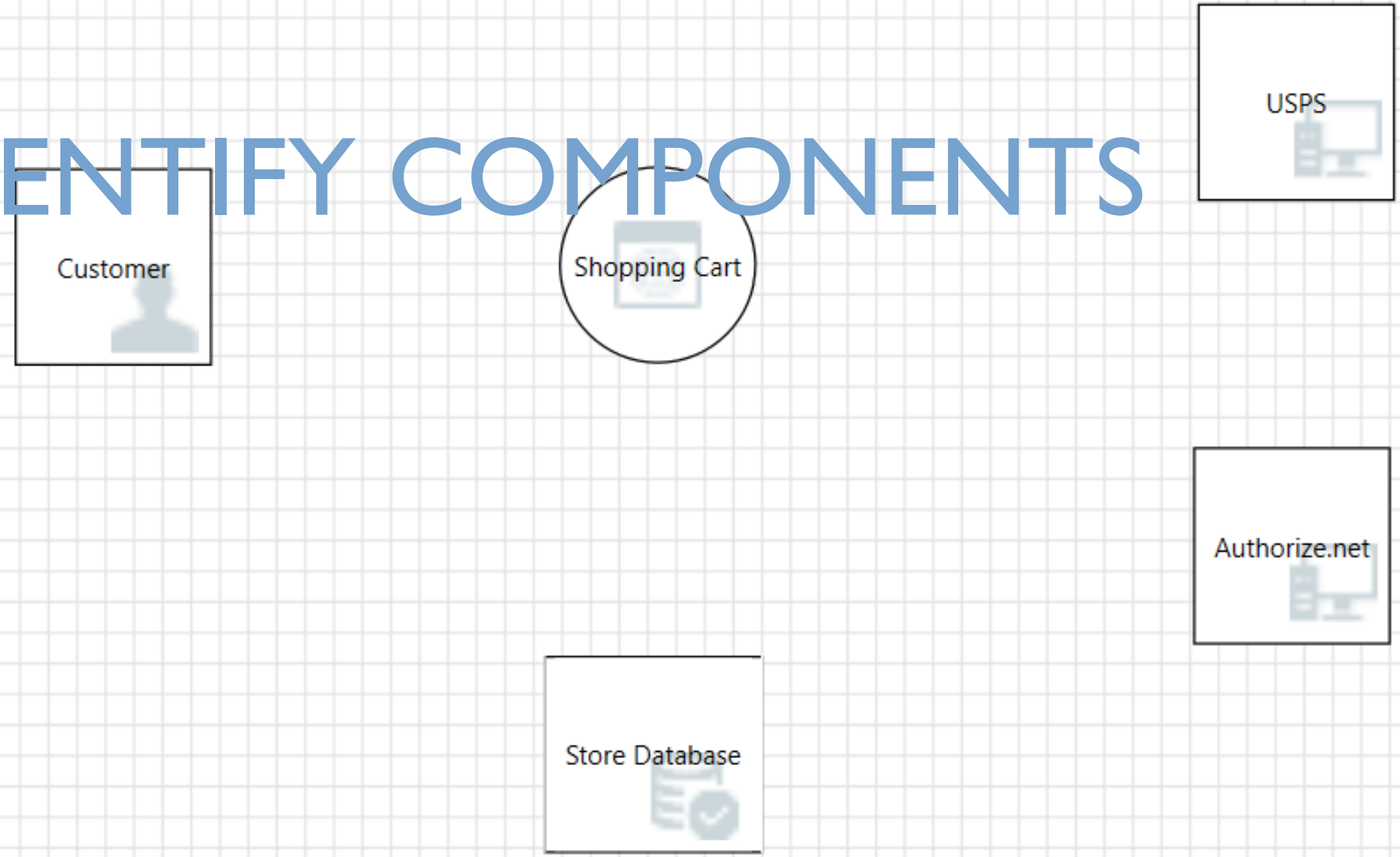
BUGS VS. FLAWS

50% / 50%

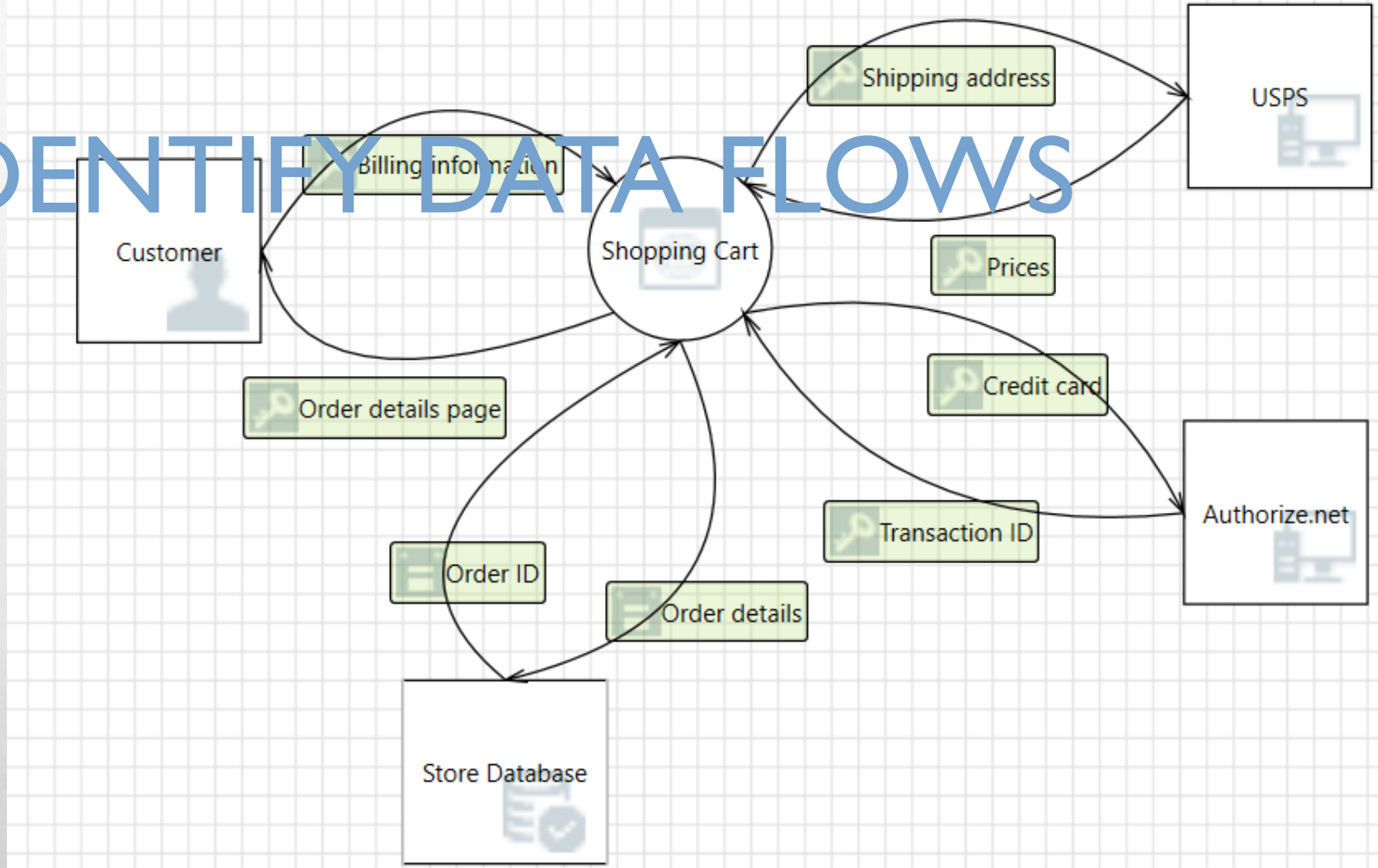
SDL THREAT MODELING



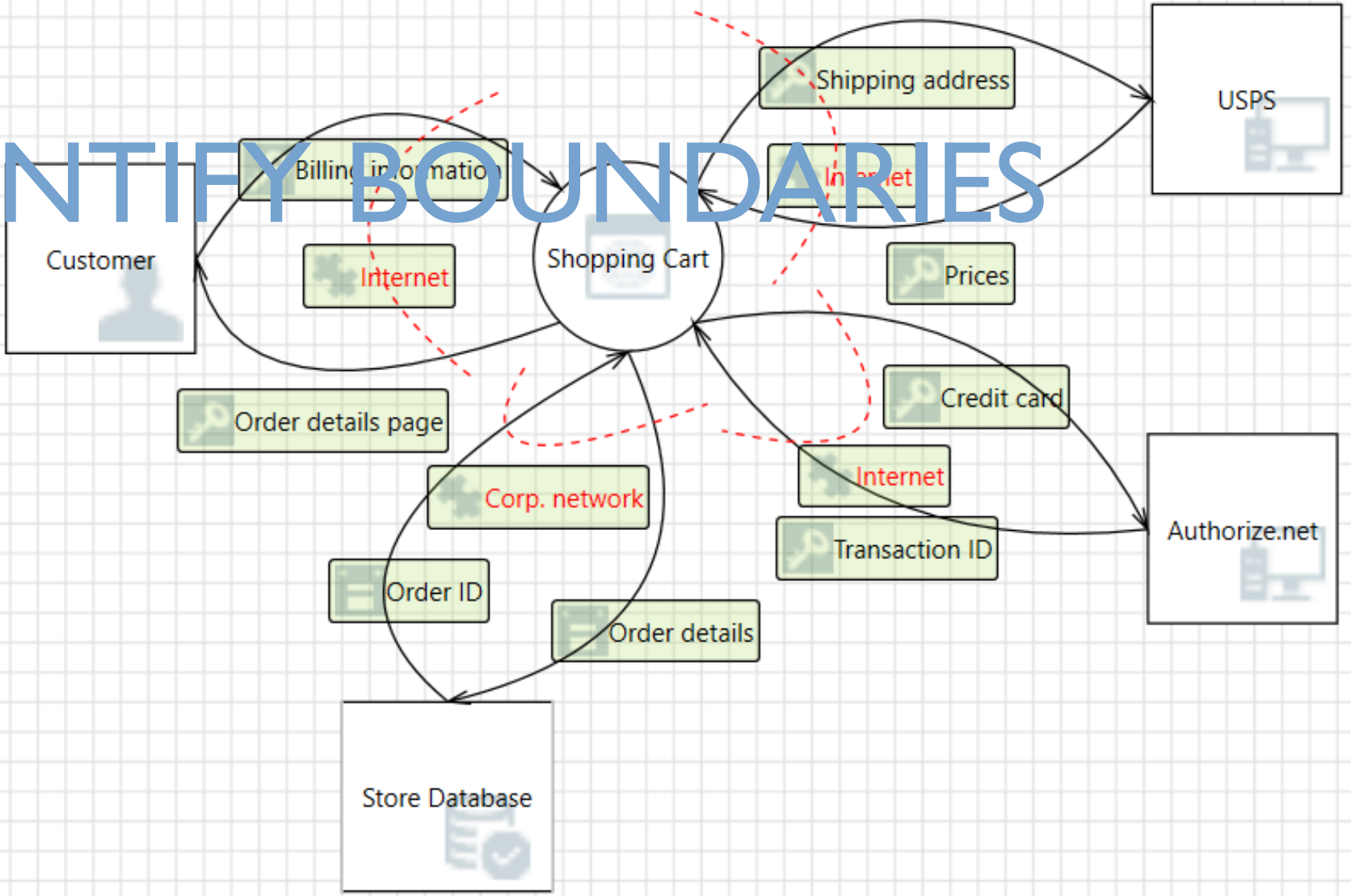
IDENTIFY COMPONENTS



IDENTIFY DATA FLOWS



IDENTIFY BOUNDARIES



THE STRIDE THREAT MODEL

- SPOOFING IDENTITY
- TAMPERING WITH DATA
- REPUDIATION
- INFORMATION DISCLOSURE
- DENIAL OF SERVICE
- ELEVATION OF PRIVILEGE

THREAT MODELING

WHO WILL USE WHAT ATTACK AGAINST WHICH VECTOR IN ORDER TO ACCESS WHAT ASSET.

RISK ASSESSMENT

NIST 800-300 RISK MODEL

- LIKELIHOOD (HIGH, MEDIUM, LOW)
- IMPACT (HIGH, MEDIUM, LOW)
- RISK = LIKELIHOOD X IMPACT

MS DREAD RISK MODEL

- DAMAGE POTENTIAL (1- 10)
- REPRODUCIBILITY (1- 10)
- EXPLOITABILITY (1- 10)
- AFFECTED USERS (1- 10)
- DISCOVERABILITY (1- 10)
- RISK = (D + R + E + A + D) / 5

LIMITED TIME?

- SECURING WEB APPLICATION TECHNOLOGIES (SWAT) CHECK LIST BY SANS
- WEB APPLICATION SECURITY TESTING CHEAT SHEET BY OWASP
- SEI SECURITY TACTICS
- CHECKLIST: ARCHITECTURE AND DESIGN REVIEW BY MICROSOFT

QUESTIONS?