DevSecOps = DevOps + Secure Coding
Who are we?

Rajiv Malkan, Ph.D.
Lonestar College – Montgomery
Professor – Business and Computer Science (Computer Information Technologies)
rajiv.malkan@lonestar.edu

Bruce Caraway
Lonestar College – University Park
Assistant Professor – Computer Information Technologies
bruce.caraway@lonestar.edu
Agenda

- Introduction
- DevOps and DevSecOps
- Software Development Life Cycle
- Secure Coding
- Incorporating Skills
- Tools Availability
- Best Practices
- Questions
Introduction

- Industrial Revolution is over
- Information/Digital Revolution is now leading the way
- Convergence of Cloud Computing, IoT, Big Data – opportunity for software development and integration
Introduction

Digital Economy – Top 10 public companies by market capital (2019)

Introduction

- Cisco is transforming into a software company
  - Engineer–Hardware (Area of Interest)–43 Openings
  - Engineer – Software (Area of Interest) – 462 Openings
  - Indeed – DevOps (25,000+)
  - Indeed – DevSecOps (1,700+)
DevOps

DevOps Developer – Position Requirements

Entry Level DevOps Developer - Austin, TX
Full-time, Contract

What You’ll Do:

You’ll work in an Agile, collaborative environment to understand requirements, design, code and test innovative applications, and support those applications for our highly valued customers.

You’ll employ IBM’s Design Thinking and Agile methodologies to create products that provide a great user experience along with high performance, security, quality, and stability.
**DevOps**

As a DevOps Engineer you will:

Manage a portfolio of cloud-based web applications (Azure).

Design, implement, and document CICD (Continuous Integration/Continuous Development) pipelines using Azure DevOps tools.

Take ownership of code release processes for multiple projects.

Participate in architecture and implementation of infrastructure monitoring, security, scaling, and disaster recovery solutions.

Collaborate with engineers, testers, and business analysts to consistently deliver quality software to end users.
DevSecOps

As a DevSecOps Leader responsibilities:

Maintain cloud infrastructure architecture aligning security, compliance, performance and resilience with cost
Maintain a good understanding on the latest secure development practices and tools that help increase awareness around secure code practices
Develop and maintain IT policies and procedures, especially those for quality and productivity standards that enable the team to meet established client service levels
Develop and maintain Information Security policies and procedures, and verifies deliverables meet Information Security requirements
DevOps - DevSecOps

Source: https://jaxenter.com/wp-content/uploads/2019/03/1.png
Shifting Paradigm

- Software-Enabled Products
- Security Risks in Application Software
  - Data Breaches
  - Software Vulnerabilities
  - Software Security Flaws
Software Development Cycle

- Waterfall
- Agile
- Continuous Integration/Continuous Deployment
Software Development Cycle

Traditional - Waterfall Development Style

- Requirements
  - Product requirements document
- Design
  - Software architecture
- Implementation
  - Software
- Verification
- Maintenance

Source: https://en.wikipedia.org/wiki/Waterfall_model
Windows Software Updates

Software Development Cycle

Agile Development Style

- Uses short iterations to build software
  - 1-4 weeks in length
- Iteration begins with short planning meeting
- Every iteration involves building shippable software
- Quick responses to change
- Continuous Improvement
- Testing is completed in same iteration as coding
Software Development Cycle

Agile Development Style

Source: https://www.pinterest.com/pin/24136547979068985
Previous monthly updates to Power BI Desktop

06/09/2019 • 75 minutes to read • 🗣️ _PB  🗣️ +10

This article describes previous updates to Power BI Desktop. For the most current month’s release, check out Power BI Desktop latest updates.

You can always download the latest version of Power BI Desktop. If you’re running Windows 10, you can also get Power BI Desktop from the Windows Store. The monthly versions are the same even though the version numbering may differ between the two, regardless of which way you install Power BI Desktop. See this article for more information.

The links beside each update mean the following:

- [video] excerpts play in a new browser tab, when the feature is being discussed.
- Some features have an [article] that provides more detail.

Source: https://docs.microsoft.com/en-us/power-bi/desktop/latest-update-archive
Software Development Cycle

Agile Development Style

- Popular Frameworks
  - Scrum
  - Kanban
Software Development Cycle

Scrum Process

- Product Owner
- Development Team
- Scrum Master
- Stakeholder liaison
- Sprint Planning
  - Team forecasts work needed to achieve Sprint Goal
- Sprint Backlog
  - Topic 1: forecast PBI's
  - Topic 2: plan work (e.g. tasks)
Software - DevOps

Software Development and Software Operations are unified (DevOps) – merging together.

Software – disrupting traditional industries
- Automobile
- Manufacturing
- Construction
- Medical/Health
- Shipping
- Education
Software Development

Increasing Complexity

- U.S. military drone uses 3.5 million lines of code.
- A Boeing 787 has 6.5 million lines behind its avionics and online support systems.
- Google Chrome (browser) runs on 6.7 million lines of code.
- A Chevy Volt uses 10 million lines.
- The Android operating system runs on 12-15 million lines.

Source: http://www.visualcapitalist.com/millions-lines-of-code/
Software Development

Increasing Complexity

- Not including backend code, Facebook runs on 62 million lines of code.
- With the advent of sophisticated, cloud-connected infotainment systems, the car software in a modern vehicle apparently uses 100 million lines of code.
- All Google services combine for a whopping 2 billion lines.

Source: http://www.visualcapitalist.com/millions-lines-of-code/
Are we teaching to develop secure software?

2018 DevSecOps Global Skills Survey

- Nearly 40% of organizations have difficulty finding employees with sufficient knowledge about security testing.
- 70% of developers said their organizations don’t provide them with adequate training in security.
- Over 64% of Professionals Surveyed said they learned their most relevant skills on the job.
Are we teaching to develop secure software?

2018 DevSecOps Global Skills Survey

- A miniscule 3% said they learned their most relevant skills for their profession through their college education.
- More than 76% of college educated respondents said – they weren’t required to complete any courses focused on security during higher education.
- Most recent graduates receive little to no instruction about secure coding, cryptography and other cybersecurity issues.
- While the business world is merging software development and security, the academic world is separating the two fields and even creating greater stratification among college graduates.
Security Breach – Loophole Exploited

https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices
Loophole Patched
Are we teaching to develop secure software?

Moving from DevOps to DevSecOps

• In today’s software development environment – both computing security professionals and software development professionals need to be responsible for security.

• Unlike more traditional models, where systems were built by developers and then scrutinized to uncover vulnerabilities, DevSecOps builds security in at the code level.
Why Secured Software Development is Needed?

- Defect prevention reduces software production time by 3-10 hours/employee
- Rework on post released software costs 50-200 times
- About 60% defects arise in design phase itself
- A defect of $1 in design phase grows to $60-$100 after it is shipped.

Source: EC-Council Certified Secure Programmer Courseware
Why Secured Software Development is Needed?

According to Gartner Report

- Gartner predicts that, through 2020, 99% of vulnerabilities exploited will continue to be the ones known by security and IT professionals for at least one year.
- Organizations must invest in people and process, such as by adopting a DevSecOps workstyle.
- Train All Developers on the Basics of Secure Coding, but Don't Expect Them to Become Security Experts

Source: https://www.gartner.com/smarterwithgartner/how-to-address-threats-in-todays-security-landscape/
Why Secured Software Development is Needed?

According to Gartner Report

- Adapt Your Security Testing Tools and Processes to the Developers, Not the Other Way Around
- By 2021, DevSecOps processes will be used by 80% of development teams, growing from just 15% in 2017.
- Security breaches have the potential to cause serious financial and reputational damage, with regulations such as the EU’s General Data Protection Regulation -GDPR.

Source: https://www.gartner.com/smarterwithgartner/how-to-address-threats-in-todays-security-landscape/
Why Secured Software Development is Needed?

- Top 10 Application Risk - 2017
  - https://www.owasp.org/index.php/ASVS_V5_Input_validation_and_output_encoding
Integrating Security Concepts in Teaching Software Development

Current Standards for Secure Coding Practices

- The Open Web Application Security Project (OWASP)
- Secure Coding Guidelines
- Developers Guide
  https://github.com/OWASP/DevGuide/tree/dc5a2977a4797d9b98486417a5527b9f15d8a251/DevGuide2.0.1
- Code Review Guide
Integrating Security Concepts in Teaching Software Development

Current Standards for Secure Coding Practices

- CERT (Carnegie Mellon University – Software Engineering Institute)
  https://www.cert.org/secure-coding/index.cfm

- Java Coding Standards
  https://wiki.sei.cmu.edu/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java

- C++ Coding Standards
  https://wiki.sei.cmu.edu/confluence/display/cplusplus
Integrating Security Concepts in Teaching Software Development

Current Standards for Secure Coding Practices

- Microsoft – Security Development Life Cycle
Integrating Security Concepts in Teaching Software Development
Integrating Security Concepts in Teaching Software Development

Current Textbook – 2019 Copyright

- No concepts of SDLC and Agile Software Development Life Cycle
- No concept of Secure Coding
Integrating Security Concepts in Teaching Software Development

Best Practices:

- Textbooks used in today’s classroom – does not cover SDLC and Secure Concepts

- SDLC (Software Development Life Cycle) – does not touch on Security Aspect of Software Development

- SSDLC (Secure Software Development Life Cycle)
Integrating Security Concepts in Teaching Software Development

Best Practices:

- SSDLC (Secure Software Development Life Cycle)
- Project Design Phase
  - Incorporate –Security Features
    - (Think Like a Hacker – Concept)
  - Data Input Validation Check
  - Variable Data Types
  - File Input/OutPut Error Handling
  - Detailed Documentation
public class Chandler_Timothy_Chpt4_Slot {

    /**
     * @param args the command line arguments
     */

    public static void main(String[] args) {

        String[] images = {"Cherries","Oranges","Plums","Bells","Melons","Bars"}; //images for the slots of the machine
        double amountEntered, totalEntered=0, earnings=0; //variables to keep track of spendings and earnings
        int result1, result2, result3; //variables to determine which image to display on the slots
        String playAgain; //takes user input to see if they want to play again
        Scanner input = new Scanner(System.in); //set up user input
        Random rand = new Random(); //set up something to randomly select slots

        //slot machine
        System.out.println("Welcome to the slot machine");
        do{
            amountEntered=inputCheck(); //checks to see if the input is valid
            while (amountEntered<0){ //this stuff happens if the value entered is not positive
                System.out.println("Please input a valid number");
                amountEntered=inputCheck();
            }
            totalEntered+=amountEntered; //keep track of how much money was spent
            result1=rand.nextInt(5); //spin the slots
            result2=rand.nextInt(5);
            result3=rand.nextInt(5);
            System.out.println("|"+images[result1]+" |"+images[result2]+" |"+images[result3]+" |"); //output the slot result
            if (result1==result2 || result2==result3 || result3==result1){ //check if any two or them match
                if(result1==result2 && result2==result3){ //check if all three match
                    System.out.println("Congratulations! You won:\n")+
                }
            }
        }
    }
}
Best Practices

```java
public static double inputCheck() { // this method checks if they input a valid number
    try {
        double enteredAmount; // variable for the input that may or may not be wrong
        Scanner input = new Scanner(System.in); // set up input
        System.out.print("How much money would you like to insert? \n"); // ask how much money to give the machine
        enteredAmount = input.nextDouble(); // get cash input
        return (enteredAmount); // happens if the value entered is a number
    } catch (java.util.InputMismatchException e) { // this happens if they don’t input a valid number
        System.out.println("Nice try. Input a number this time"); // tell user to input a number
        inputCheck(); // try again
    }
    return 0;
}
```
Best Practices

```java
//@package swinglinkedlistmodified;

class LinkedList1 {
    **// The Node class stores a list element 
       and a reference to the next node.**

    private class Node {
        String value;
        Node next;

        **// Constructor.**
        @param val The element to store in the node.
        @param n The reference to the successor node.

        Node(String val, Node n)
    }
}
```
Best Practices

https://wiki.sei.cmu.edu/confluence/display/java/NUM02-J.+Ensure+that+division+and+remainder+operations+do+not+result+in+divide-by-zero+errors
Best Practices

Division and Remainder – divide by zero error handling

Typical Code for divide one number by another:

```c
int num1, num2, result;

/* Initialize num1 and num2 */

result = num1 / num2;
```
Best Practices

Division and Remainder – divide by zero error handling

Typical Code for divide one number by another with error handling:

double num1, num2, result;
/* Initialize num1 and num2 */
if (num2 == 0) {
    // Handle error message
} else {
    result = num1 / num2;
}
Best Practices

Division and Remainder – divide by zero error handling

What is the Risk Assessment if Error Handling is not addressed at code level?

Program may terminate abruptly if the numerator is 0 and thus may be vulnerable for Denial of Service (DoS) attack.
Tools for Secure Coding

- NetBeans – Integrated Development Environment (IDE)
- Eclipse - Integrated Development Environment (IDE)
- IntelliJ IDEA
- FindBugs – Static Code Analysis (Check for Inconsistences in the code)
  - https://netbeans.org/kb/docs/java/code-inspect.html
Tools for Secure Coding

- Source Code Analysis Laboratory (SCALe)
  - SCALe can refer to one or more of the following three artifacts, all of which evaluate source code for adherence to secure coding standards: SCALe auditing framework, SCALe research prototype, and SCALe code Conformance Testing
  - [http://www.cert.org/secure-coding/products-servicesSCALE.cfm](http://www.cert.org/secure-coding/products-servicesSCALE.cfm)
Tools for Secure Coding

- [http://cis1.towson.edu/~cyber4all/modules/nanomodules/Input.Validation-CS0_Java.html](http://cis1.towson.edu/~cyber4all/modules/nanomodules/Input.Validation-CS0_Java.html)
Summary

- Digital Economy
- SDLC – Traditional
- Agile – Development
- DevOps and DevSecOps
- Secure Coding Implementation
- Implement secure coding in Fall 2019 semester......
Questions
Contacts

Rajiv Malkan, Ph.D.
Lonestar College – Montgomery
Professor – Business and Computer Science (Computer Information Technologies)
rajiv.malkan@lonestar.edu

Bruce Caraway
Lonestar College – University Park
Assistant Professor – Computer Information Technologies
bruce.caraway@lonestar.edu