NORTHERN ILLINOIS UNIVERSITY

The Importance of DevSecOps

A Thesis Submitted to the

University Honors Program

In Partial Fulfillment of the

Requirements of the Baccalaureate Degree

With Upper Division Honors

Department Of

Computer Science

By

Katia Gomes

DeKalb, Illinois

May 2018
University Honors Program

Capstone Approval Page

Capstone Title (print or type)

The Importance of DevSecOps

Student Name (print or type)   Katia Gomes

Faculty Supervisor (print or type)   Daniel Rogness

Faculty Approval Signature

Department of (print or type)   Computer Science

Date of Approval (print or type)   5/2/18
HONORS THESIS ABSTRACT
THESIS SUBMISSION FORM

AUTHOR: Katia Gomes

THESIS TITLE: The Importance of DevSecOps

ADVISOR: Daniel Rogness

ADVISOR’S DEPARTMENT: Computer Science

DISCIPLINE: Computer Science

YEAR: 2018

PAGE LENGTH: 16

BIBLIOGRAPHY: Included

ILLUSTRATED: Yes

PUBLISHED (YES OR NO): No

LIST PUBLICATION: N/A

COPIES AVAILABLE: Online

ABSTRACT (100-200 WORDS):

With the rapid growth of technology, the potential for data to be stolen has grown exponentially. Therefore, security needs to become a higher priority in applications. DevSecOps is a concept which seeks to do just that. With this presentation, I seek to create a means to inform IT professionals why security is a rising concern and methods to improve the security of applications through DevSecOps. With reports on data breaches, this presentation first emphasizes how security is a growing concern. Then, through articles written by IT professionals, it focuses on how DevSecOps can transform the application development cycle to create more secure applications. Through this practice, companies can have faster response times and fend off more attacks, leading to an overall more protected system.
Why is security important?

- **Generic Login**

- **Basic SQL Injection**
  
  ```sql
  select Password from Users where UserName='$user' and Password='$password'
  
  select Password from Users where UserName='' or ''='' and Password='' or ''=''
  
  - The query will return true – valid user
  ```

To demonstrate why security is such a big topic, let’s go through a basic example I created at http://students.cs.niu.edu/~z1730089/honors/. It is a basic login connected to a database of users and their password. It works as you would accept, allowing a login with correct credentials and failing otherwise. However, with some simple SQL Injection (‘ or ‘=’ in Username and Password), a malicious user could fake a successful login, gaining access to data they shouldn’t have.
Open Web Application Security Project

- **Injection**
  - Untrusted data is sent to an interpreter and is executed, allowing a malicious user to access data without proper authorization (like my example)

- **Broken Authentication**
  - Authentication and session management are incorrectly implemented, allowing attackers to compromise passwords, keys or session tokens. They can then assume other users’ identities temporarily or permanently

- **Sensitive Data Exposure**
  - Sensitive data such as financial or healthcare are not properly protected.
  Attackers can steal or modify such data to conduct credit card fraud, identity theft, or other crimes.
# Data Breaches

## BIGGEST

<table>
<thead>
<tr>
<th>Name</th>
<th>Year</th>
<th>Number of Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahoo</td>
<td>2013</td>
<td>3 billion accounts</td>
</tr>
<tr>
<td>Adult Friend Finder</td>
<td>2016</td>
<td>400+ million accounts</td>
</tr>
<tr>
<td>eBay</td>
<td>2014</td>
<td>145 million users</td>
</tr>
<tr>
<td>Equifax</td>
<td>2017</td>
<td>143 million consumers</td>
</tr>
</tbody>
</table>

## 2018

- Best Buy – April 5
- Sears – April 4
- Delta – April 4
- Saks Fifth Ave/Lord & Taylor – April 1
- Under Armour – March 29
- Hack Sponsored by Iran – March 23
- FedEx – February 15

There have also been many data breaches over the years. These are the top 4, by number of records stolen:

- **Yahoo**
  - 3 billion user accounts, including user names, email addresses, dates of birth and passwords

- **Adult Friend Finder**
  - 400+ million accounts including names, email addresses and passwords (encryption easily cracked)

- **eBay**
  - 145 million accounts, including names, addresses, dates of birth and encrypted passwords.

- The hackers got in via credentials of 3 corporate employees
• Equifax

  • 143 million consumers, including SSN, birth dates, addresses plus potentially
    drivers’ license numbers and credit card data

  • They are one of the largest credit bureaus in the U.S.

In 2018 alone, these companies have been hacked and user information, typically including
customer information and even payment information.

  • Specifically, an Iranian hacker ring hacked into computer networks of 144 U.S.
    universities and sent a phishing scan, breaching the email accounts of roughly
    4,000 professors. This resulted in 31 terabytes of data stolen, totaling $3.4 billion
    worth of damages.
As a whole, data breaches are on the rise. And those are just a few examples of the number of data breaches that have occurred. As a whole, data breaches have been on the rise.

Now, how can we go about reducing the number of data breaches? Of course, we need to make applications more secure. But how would a company go about doing that?
This is where the concept DevSecOps comes into play. It stands for Development, Security and Operations. This is basically a guideline for how to weave security into DevOps – a practice companies have already started using. To fully understand DevSecOps, we need to make sure we understand DevOps.
Basically, DevOps restructures the traditional application lifecycle. It weaves together Development and Operations to create flexibility in the application. It outlines a set of guidelines to implement through tools, technology and process. The core principles are …

DevOps encourages faster delivery, defect resolutions and creates an overall collaborative environment. However, this process fails to include security.
DevSecOps is, simply put, DevOps with security baked into it. It once again restructures the application lifecycle to make it so that security is something considered at every stage. The goal is to shift security to the left of the development cycle, adding security checks after each development phase.
So what?

By shifting security to the left of the development cycle, it ensures that security is thoroughly built into the application. Security checks after each phase add a level of automation. It also allows developers to notice potential vulnerabilities faster. And, one of the most important things, in my opinion, is that it allows for faster response times to vulnerabilities found in the live software.
Integration

• Developers need to learn security
• Add security checks for each small code release
• Use tools to both monitor and identify security issues

Clearly this concept is something beneficial for companies to use, but with any new methodology, a company would need to figure out how to implement it into their work flow. With DevSecOps, this means changing the development process from start to finish so that it incorporates security. So, first off developers need to learn about security.
One very helpful software companies can use is called Jenkins. It is a software that can help with automation. Specifically, it is used to assist with continuous integration. With DevSecOps, there should be frequent releases. This means there will be daily code changes and merging with repositories. If code is not tested frequently, it could lead to a pile of defects by the time it is. Jenkins assists with automatically testing code when it is integrated, helping to ensure that the code contains no defects.
Another useful software is called Nessus. It is a vulnerability scanner software. It scans the application and will search for security defects that a hacker could exploit. Nessus alerts the developer of these defects, ordering them by severity. Then these potential exploits can be fixed before the software is released, leading to less vulnerabilities in the deployed code.
Another tool used for finding security defects is Metasploit. Specifically, Metasploit is used for penetration testing. This is where the company has a person test their application to see if there are any security vulnerabilities in the software. They are trying to see if they can find a way to break through the security of the software. So, Metasploit allows the tester to facilitate the attacks hacker run. This way different types of security vulnerabilities can be tested. This ability to run penetration tests on the software adds another way to make sure that an application doesn’t have any security defects.
One more very useful tool for companies to use is Splunk. This is a monitoring software that identifies potentially malicious attacks on the application. This application makes it very easy to not only identify malicious attacks, but automating the incident response procedures. This leads to faster response times to vulnerabilities.
With all of that said, here are a few final thoughts. Obviously, security is important for the fact that technology is constantly being developed and it is only being released faster. Given how many security breaches there have been, the need for secure applications is only increasing. So, thoughts of security need to be generated towards the start of development.

DevSecOps is a framework with the goal to bake security into an application. It makes it so that security is everyone's responsibility, not just the security team. And there are already many tools available to assist with the integration of DevSecOps. Though it seems like a simple concept, it is something that will help increase the overall application security and would help prevent data breaches.
Bibliography


“DevSecOps Bootcamp.” GitHub, github.com/devsecops/bootcamp.


Reklaitis, Victor. “How the Number of Data Breaches Is Soaring - in One Chart.” *MarketWatch*,