API Blindspots:
Why Experienced Developers Write Vulnerable Code

Daniela Seabra Oliveira, Tian Lin, Muhammad Sajidur Rahman, Rad Akefirad, Donovan Ellis, Eliany Perez, Rahul Bobhate, Lois A. DeLong, Justin Cappos, Yuriy Brun, Natalie C. Ebner

@dseabraoliveira
daniela@ece.ufl.edu
Vulnerabilities keep increasing...

From Symantec Security Report 2018!

**Total number of vulnerabilities**
- 2015: 8,077
- 2016: 7,692
- 2017: 8,718

13% increase

**Zero-day vulnerabilities**
- 2015: 4,066
- 2016: 3,986
- 2017: 4,262

7% increase
The same old vulnerabilities again and again

<table>
<thead>
<tr>
<th>Vulnerabilities</th>
<th>Date</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux Kernel 'tcp_input.c' Remote Denial of Service Vulnerability</td>
<td>2018-08-07</td>
<td><a href="http://www.securityfocus.com/bid/104976">http://www.securityfocus.com/bid/104976</a></td>
</tr>
<tr>
<td>Mozilla Firefox and Firefox ESR Multiple Unspecified Memory Corruption Vulnerabilities</td>
<td>2018-08-07</td>
<td><a href="http://www.securityfocus.com/bid/104556">http://www.securityfocus.com/bid/104556</a></td>
</tr>
<tr>
<td>Mozilla Firefox and Firefox ESR Multiple Security Vulnerabilities</td>
<td>2018-08-07</td>
<td><a href="http://www.securityfocus.com/bid/104561">http://www.securityfocus.com/bid/104561</a></td>
</tr>
<tr>
<td>Mozilla Firefox and Firefox ESR Multiple Security Vulnerabilities</td>
<td>2018-08-07</td>
<td><a href="http://www.securityfocus.com/bid/104561">http://www.securityfocus.com/bid/104561</a></td>
</tr>
<tr>
<td>Mozilla Firefox and Firefox ESR Multiple Security Vulnerabilities</td>
<td>2018-08-07</td>
<td><a href="http://www.securityfocus.com/bid/104561">http://www.securityfocus.com/bid/104561</a></td>
</tr>
<tr>
<td>Mozilla Firefox and Firefox ESR Multiple Security Vulnerabilities</td>
<td>2018-08-07</td>
<td><a href="http://www.securityfocus.com/bid/104561">http://www.securityfocus.com/bid/104561</a></td>
</tr>
<tr>
<td>PHP Multiple Heap Buffer Overflow Vulnerabilities</td>
<td>2018-08-06</td>
<td><a href="http://www.securityfocus.com/bid/104871">http://www.securityfocus.com/bid/104871</a></td>
</tr>
</tbody>
</table>
Security Community Response 1

Blame the developer for lack of security education
Security Community Response 1

Blame the developer for lack of security education

Nah
Security Community Response 2

Security should be required from the beginning, developers can write secure code if provided with resources.

Summary:
1. Support dev and sec team with processes, training, and resources so they can confidently get the job done.
2. Repair relationship.
3. Do not accept ‘bad’ behavior anymore.

'Pushing Left' means doing security from the start, and continuing the whole way through.
Security Community Response 2

Security should be required from the beginning, developers can write secure code if provided with resources.

'Pushing Left' means doing security from the start, and continuing the whole way through.
Developers need *usable* resources to write secure code

Developer-centered security and the symmetry of ignorance

Olgierd Pieczul
IBM
Dublin, Ireland

Simon Foley
IMT Atlantique, Lab-STICC,
Université Bretagne Loire
Brest, France

Mary Ellen Zurko
MIT Lincoln Laboratory
Massachusetts Institute of Technology
Lexington, USA

Developers Are Not The Enemy! The need for usable security APIs

Matthew Green, Johns Hopkins University
Matthew Smith, University of Bonn, Fraunhofer FKIE

Developers Need Support, Too: A Survey of Security Advice for Software Developers

Yasemin Acar, Christian Stransky,* Dominik Wermke, Charles Weir,† Michelle L. Mazurek,‡ and Sascha Fahl
Leibniz University Hannover, *CISPA, Saarland University, †Security Lancaster, ‡University of Maryland
{acar,wermke,fahl}@sec.uni-hannover.de; stransky@cs.uni-saarland.de; c.weir1@lancaster.ac.uk; mmazurek@umd.edu
Security Community Response 3

Developers need *usable* resources to write security code.

Yes!
But...Vulnerabilities keep increasing...

From Symantec Security Report 2018!

Total number of vulnerabilities

<table>
<thead>
<tr>
<th>Year</th>
<th>Total Number of Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>8,077</td>
</tr>
<tr>
<td>2016</td>
<td>7,692</td>
</tr>
<tr>
<td>2017</td>
<td>8,718</td>
</tr>
</tbody>
</table>

13% increase

Zero-day vulnerabilities

<table>
<thead>
<tr>
<th>Year</th>
<th>Zero-day Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>4,066</td>
</tr>
<tr>
<td>2016</td>
<td>3,986</td>
</tr>
<tr>
<td>2017</td>
<td>4,262</td>
</tr>
</tbody>
</table>

7% increase
What if there is something else? Like some missing ingredient for the recipe of secure code?
Hypothesis: Even with usable resources to write secure code, developers might still experience blindspots, especially when using APIs...
API blindspot: a developer misunderstanding or oversight when using an API function, which can lead to a violation of the recommended API usage with possible introduction of vulnerabilities.
Donnie Brasco 1976-1981 (Joe Pistone)

Source: FBI archives
Donnie Brasco 1976-1981 (Joe Pistone)

Source: FBI archives
Donnie Brasco 1976-1981 (Joe Pistone)

Impact:
- 200 indictments
- 100 convictions
- Bonnano family almost destroyed
- NY Mafia instituting new rules
- $500,000 contract on his life forever
Undetected Donnie’s Vulnerabilities

• Met with FBI contact agent twice a month

• Called contact agent every few days and even FBI headquarters

• Wore “wires” on several occasions

• Every 3 weeks he visited his wife and daughters.
Weren’t the Mafia guys experienced?

• “When you talk on the phone...“you don’t talk direct about what’s going on ... Because all the phones are tapped...” Like most mobsters, he [Lefty] was paranoid. “There’s agents everywhere”.

• “Because of their paranoia that there are bugs planted everywhere, mob guys, ..., always turn on the TV or radio to cover the conversation.”

Aren’t Mafia guys “experts”?

• “Lefty was Mafia twenty-four hours a day. He would never let his guard down.”

• “Sonny [cappo] was good at what he did.”

What about developers’ blindspots?
Understand API blindspots from a developer’s perspective

Experience/Expertise
Perceptions
Cognition
Personality
Study Goals

1. Determine developers’ ability to detect API blindspots in code.

2. Examine how developer’s characteristics affect this capability.

3. Explore how API function or programming scenario characteristics affect this capability.
Study design
Part 1: Programming Puzzles (Java)

Part 2: Demographics

Part 3: Professional Experience and Expertise

Part 4: Cognitive Assessment

Part 5: Personality Assessment (Big 5)
Part 1: Programming Puzzles

Set 1

Set 2

Set 3

Set 4

I/O

String

Crypto

Source: http://www.techreviewer.club/why-hire-wordpress-developers/
```java
    // OMITTED: Import whatever is needed
    public final class SystemUtils {
        public static boolean setDate(String date) throws Exception {
            return run("DATE "+ date);
        }

        private static boolean run(String cmd) throws Exception {
            Process process = Runtime.getRuntime().exec("CMD /C "+ cmd);
            int exit = process.waitFor();

            if (exit == 0)
                return true;
            else
                return false;
        }
    }
```
Part 1: Puzzles - BS on String API

```java
public final class SystemUtils {
    public static boolean setDate(String date) throws Exception {
        return run("DATE " + date);
    }

    private static boolean run(String cmd) throws Exception {
        Process process = Runtime.getRuntime().exec("CMD /C " + cmd);
        int exit = process.waitFor();

        if (exit == 0) {
            return true;
        } else {
            return false;
        }
    }
}
```
Which of the following statements would be correct if the `setDate()` method was invoked with an arbitrary String value as the new date:

a. If the given String value does not conform to the “dd-mm-yyyy” format, an exception is thrown.
b. The `setDate()` method cannot change the date.
c. The `setDate()` method might do more than change the date.
d. The return value of the `waitFor()` method is not interpreted correctly (lines 14–17).
e. The web application will crash.
Part 1: Puzzles - BS on String API

Which of the following statements would be correct if the `setDate()` method was invoked with an arbitrary String value as the new date:

a. If the given String value does not conform to the “dd-mm-yyyy” format, an exception is thrown.
b. The `setDate()` method cannot change the date.
c. The `setDate()` method might do more than change the date.
d. The return value of the `waitFor()` method is not interpreted correctly (lines 14–17).
e. The web application will crash.
## Part 2: Participants Demographics (n = 109)

<table>
<thead>
<tr>
<th></th>
<th>Professionals (n = 70)</th>
<th>Students (n = 39)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gender</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male (88)</td>
<td>81.4</td>
<td>79.5</td>
</tr>
<tr>
<td>Female (21)</td>
<td>18.6</td>
<td>20.5</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male (88)</td>
<td>28.0 (6.0)</td>
<td>24.4 (2.1)</td>
</tr>
<tr>
<td>Female (21)</td>
<td>27.8 (6.2)</td>
<td>24.4 (2.2)</td>
</tr>
<tr>
<td><strong>Years of Programming</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.3 (3.5)</td>
<td>5.8 (3.8)</td>
</tr>
<tr>
<td><strong>Highest Degree Earned</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High School</td>
<td>1.4</td>
<td>0.0</td>
</tr>
<tr>
<td>Some College</td>
<td>0.0</td>
<td>2.6</td>
</tr>
<tr>
<td>Associates</td>
<td>1.4</td>
<td>2.6</td>
</tr>
<tr>
<td>Bachelor’s</td>
<td>40.0</td>
<td>56.4</td>
</tr>
<tr>
<td>Some Graduate School</td>
<td>11.4</td>
<td>5.1</td>
</tr>
<tr>
<td>Graduate-Level Degree</td>
<td>45.7</td>
<td>33.3</td>
</tr>
<tr>
<td><strong>Annual Income</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0–$39,999</td>
<td>45.7</td>
<td>69.2</td>
</tr>
<tr>
<td>$40,000–$70,000</td>
<td>22.9</td>
<td>15.4</td>
</tr>
<tr>
<td>$70,001–$100,000</td>
<td>20.0</td>
<td>12.8</td>
</tr>
<tr>
<td>$100,001–$200,000</td>
<td>11.4</td>
<td>2.6</td>
</tr>
<tr>
<td>&gt;$200,000</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td><strong>Race/Ethnicity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>American Indian/Alaskan</td>
<td>1.4</td>
<td>2.6</td>
</tr>
<tr>
<td>Asian</td>
<td>81.4</td>
<td>92.3</td>
</tr>
<tr>
<td>African American</td>
<td>2.9</td>
<td>0.0</td>
</tr>
<tr>
<td>Hawaiian/Pacific Islander</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>White</td>
<td>10.0</td>
<td>2.6</td>
</tr>
<tr>
<td>Other/Multi-racial</td>
<td>4.3</td>
<td>2.6</td>
</tr>
<tr>
<td><strong>Country of Residence</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>United States</td>
<td>72.3</td>
<td>94.9</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>15.7</td>
<td>2.6</td>
</tr>
<tr>
<td>Brazil</td>
<td>8.6</td>
<td>2.6</td>
</tr>
<tr>
<td>Malaysia</td>
<td>1.4</td>
<td>0.0</td>
</tr>
</tbody>
</table>
Part 3: Professional Experience and Expertise

• Programming languages:
  • Java, Python, C/C++, PHP, Visual Basic, .Net, and JavaScript

• Programming concepts and technologies:
  • SQL, Cryptography, File compression, Networking, HTTP/HTTPS, I/O operations, etc.
Part 4: Cognitive Assessment

- **BTACT** (Brief Test of Adult Cognition by Telephone) and the NIH Toolbox
  - Processing speed
  - Memory span
  - Verbal fluency
  - Short- and long-term episodic verbal memory
  - Inductive reasoning
You are going to hear a list of 15 words. Listen carefully. When the list is finished, you are to repeat as many of the words as you can remember. It doesn’t matter in what order you repeat them. Just try to remember as many as you can. You will hear each word only one time. You will have up to one and a half minutes (90 seconds).

Please press "Play" below to hear the audio. When the audio has finished, click the "Next" button to proceed to the next page where the recording for your responses will begin after 1 second.

We suggest that you close your eyes while you are listening to the audio to help you concentrate.

NOTE: On the pages where your audio response is being recorded, the page will automatically progress after the allotted time has finished.

Please do not refresh/reload the page after the recording has begun.
Part 5: Personality Assessment (Big 5)

https://www.enkimd.com/big-five-personality-traits.html
Data Analysis and Results
H1: Developers are less likely to solve puzzles with API functions containing BS than puzzles with innocuous functions.
Presence of blindspot had a significant effect on puzzle accuracy.

Multilevel logistic regression. \( \text{Wald } \chi^2(2) = 20.60, p < .001 \)
API Usage Type and Blindspots

Blindspot effect more pronounced for I/O API

(Wald $\chi^2(2) = 24.81$, $p < .001$)
Cyclomatic Complexity and Blindposts

Wald $\chi^2(2) = 24.81, p < .001$
H2a-d: Developers perceive puzzles with BS as more difficult, less clear, less familiar, and with less confidence than puzzles without BS.
Developer’s perceptions did not differ as a function of presence of BS

Multilevel modeling, all ps > 0.1
H3: Higher cognitive functioning in developers is associated with greater accuracy in solving puzzles with BS
Higher cognitive functioning did not predict higher ability in finding vulnerabilities in puzzles with BS.

Multilevel modeling, all ps > 0.1
H4: Higher levels of professional experience and expertise in developers are associated with greater accuracy in solving puzzles with BS.
More experience and expertise did not predict higher ability in finding vulnerabilities in puzzles with BS.
H5: Higher levels of openness and conscientiousness, and lower levels of neuroticism and agreeableness in developers are associated with greater accuracy in solving puzzles with BS
Ability to detect vulnerabilities

Multilevel modeling, all $p < 0.001$

https://www.enkimd.com/big-five-personality-traits.html
Summary
• Developers experience blindspots while using certain API functions
  • Effect more pronounced for I/O APIs and complex code

• Characteristics **NOT** predicting higher ability in finding vulnerabilities:
  • Perceptions of code difficulty, clarity, familiarity, and confidence
  • Experience and expertise
  • Level of cognitive functioning

• Openness **associated** with developers’ ability in finding vulnerabilities.
Now what?

Recommendations
API Functions

• Should be simple

• Functions should be designed assuming developers will **NOT** handle security issues
  • Especially I/O related

• Design of new functions should leverage developer studies

• Documentation of legacy functions should address blindspots
Software Security Training and Awareness

• Even expert, experienced, and highly intelligent developers will experience blindspots when using APIs

• Perceptions and gut feelings might be misleading

• More reliance on diagnostics tools
Software development process

Functionality vs Security

VS

Functionality

Security

Openness
Thank you!

daniela@ece.ufl.edu
@dseabraoliveira