

API Blindspots: Why Experienced Developers Write Vulnerable Code

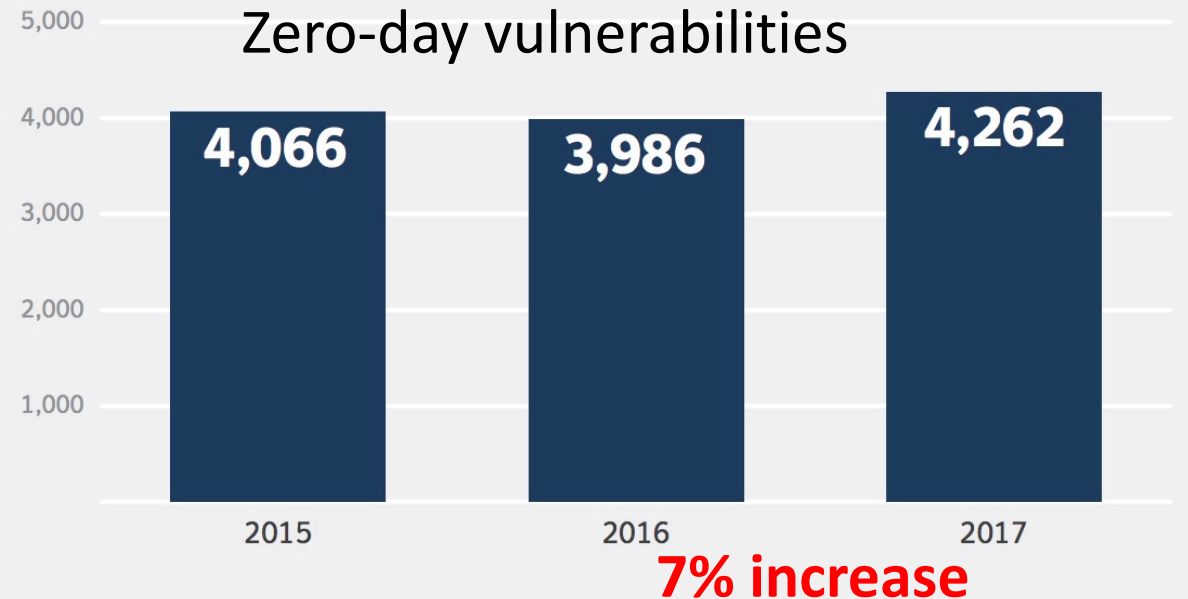
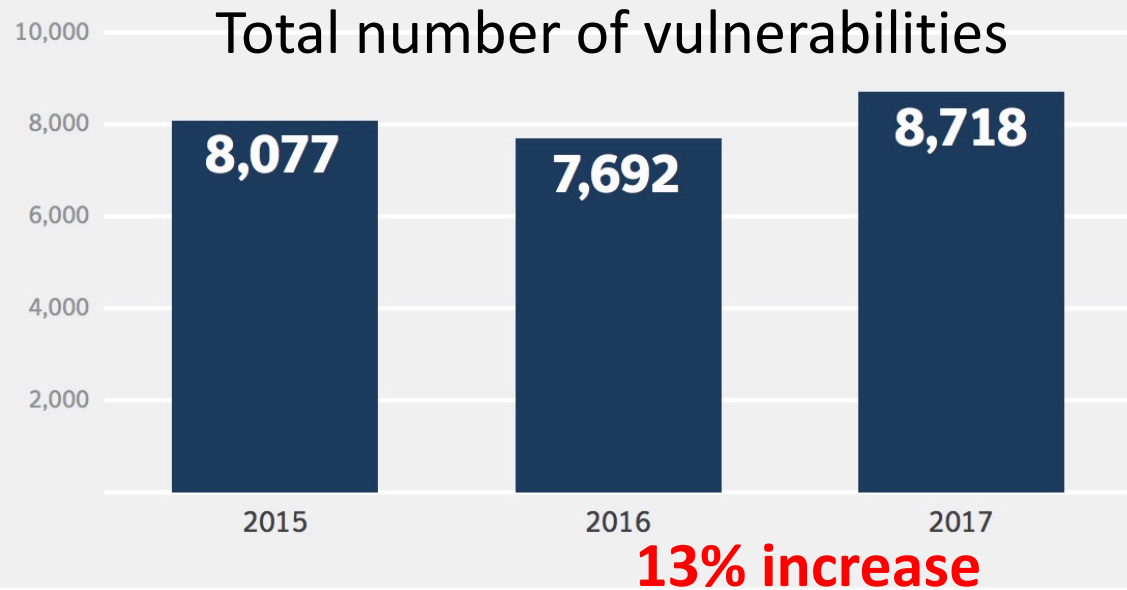
Daniela Seabra Oliveira, Tian Lin, Muhammad Sajidur Rahman, Rad Akefirad, Donovan Ellis, Eliany Perez, Rahul Bobhate, Lois A. DeLong, Justin Cappos, Yuriy Brun, Natalie C. Ebner



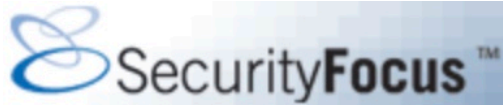
@dseabraoliveira
daniela@ece.ufl.edu

Vulnerabilities keep increasing...

From Symantec Security Report 2018!



The same old vulnerabilities again and again



✦ About ✦ Contact

Symantec Connect

A technical community for Symantec customers, end-users, developers, and partners.

Join the conversation ▶

Vulnerabilities

Linux Kernel 'tcp_input.c' Remote Denial of Service Vulnerability

2018-08-07

<http://www.securityfocus.com/bid/104976>

Mozilla Firefox and Firefox ESR Multiple Unspecified Memory Corruption Vulnerabilities

2018-08-07

<http://www.securityfocus.com/bid/104556>

Mozilla Firefox and Firefox ESR Multiple Security Vulnerabilities

2018-08-07

<http://www.securityfocus.com/bid/104561>

Mozilla Firefox and Firefox ESR Multiple Security Vulnerabilities

2018-08-07

Mozilla Firefox and Firefox ESR Multiple Security Vulnerabilities

2018-08-07

<http://www.securityfocus.com/bid/104555>

August 2018!

PHP Multiple Heap Buffer Overflow Vulnerabilities

2018-08-06

<http://www.securityfocus.com/bid/104871>

Microsoft Edge CVE-2018-0871 Information Disclosure Vulnerability

2018-08-06

<http://www.securityfocus.com/bid/104339>

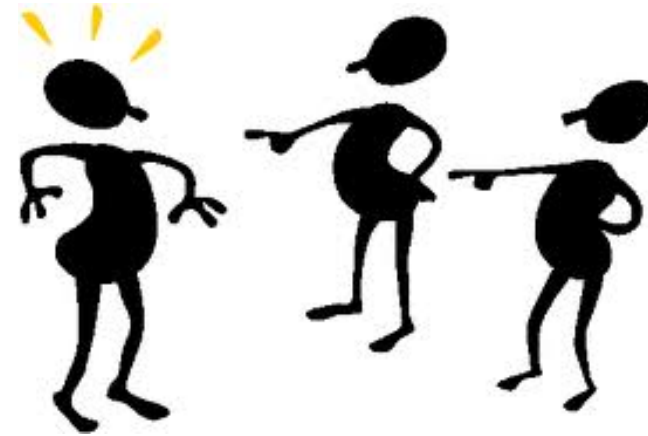
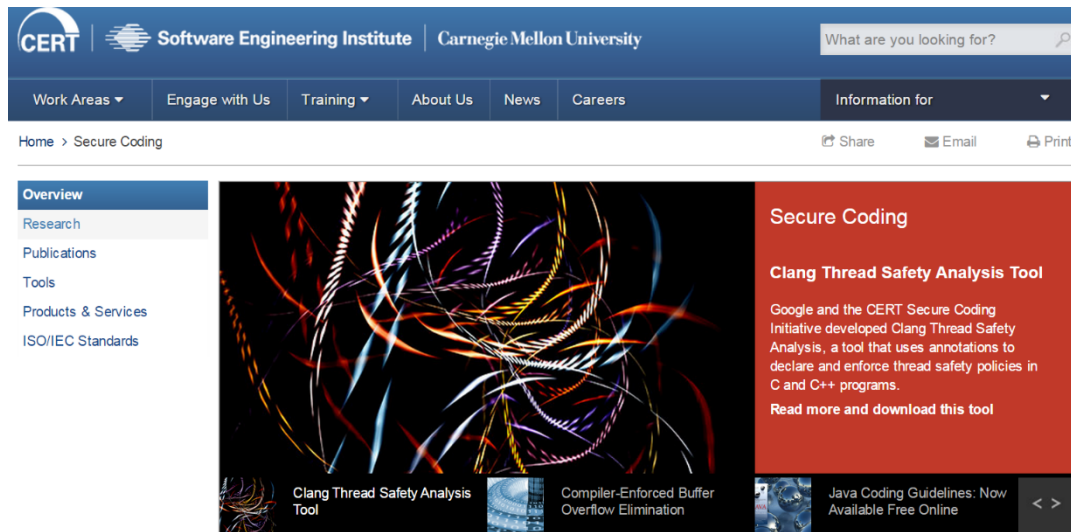
Multiple Dell EMC Products CVE-2018-1244 Remote Command Injection Vulnerability

2018-08-06

<http://www.securityfocus.com/bid/104964>

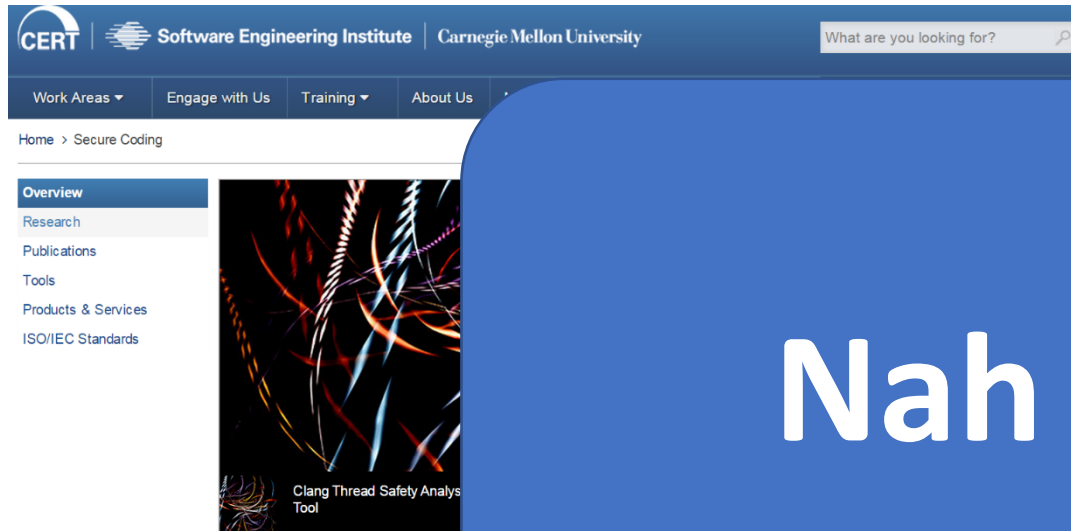
Security Community Response 1

Blame the developer for lack of security education



Security Community Response 1

Blame the developer for lack of security education



Nah

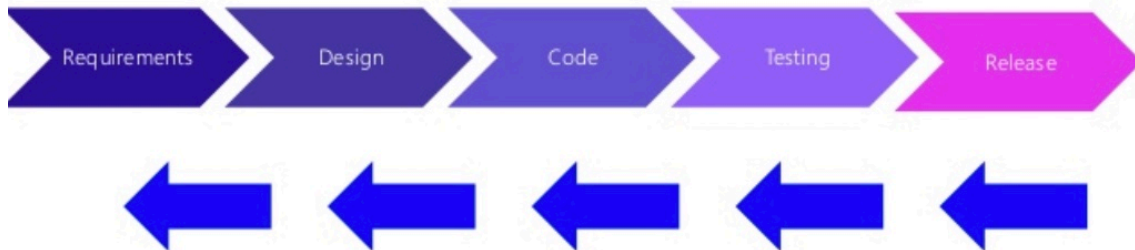


Security Community Response 2

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

Pushing Left

If you imagine the SDLC written out on a piece of paper, the further 'left' you go, the earlier you are.



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

@SheHacksPurple



OWASP

The Open Web Application Security Project

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.

Security Community Response 2

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

Pushing Left

If you imagine the SDLC written a piece of paper, the further you go, the earlier you are.



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

@SheHacksPurple



WASP
Web Application Security Project

ry:

port dev and sec team with processes, ing, and resources so they can idently get the job done.

2. Repair relationship.
3. Do not accept 'bad' behavior anymore.

Security Community Response 3

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
Rennes 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

Developer-centered security and the symmetry of ignorance

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

Developers Are Not The Enemy

Matthew Green,
Matthew Smith, Unive

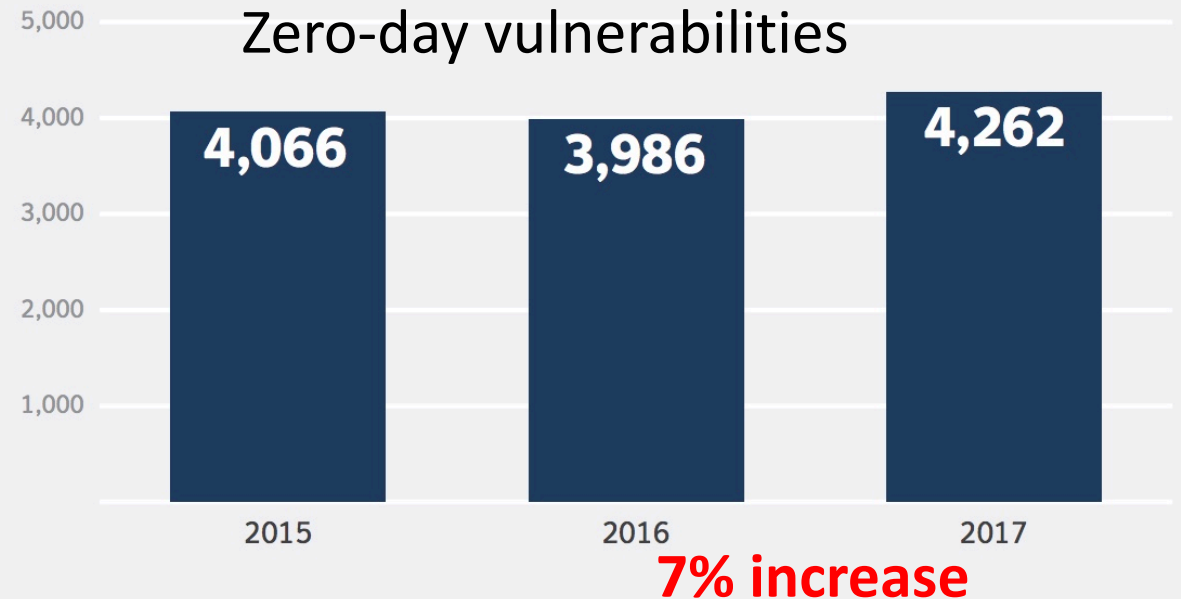
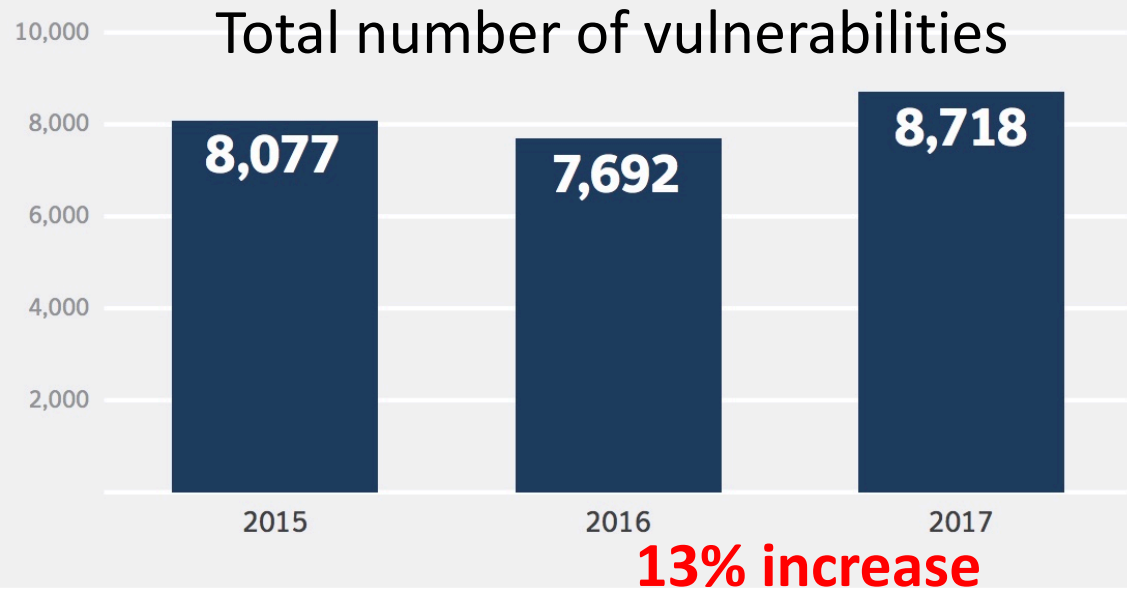
Developers Need Support for Software Developers

Yes!

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

But...Vulnerabilities keep increasing...

From Symantec Security Report 2018!



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)



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



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 3: Professional
Experience and
Expertise

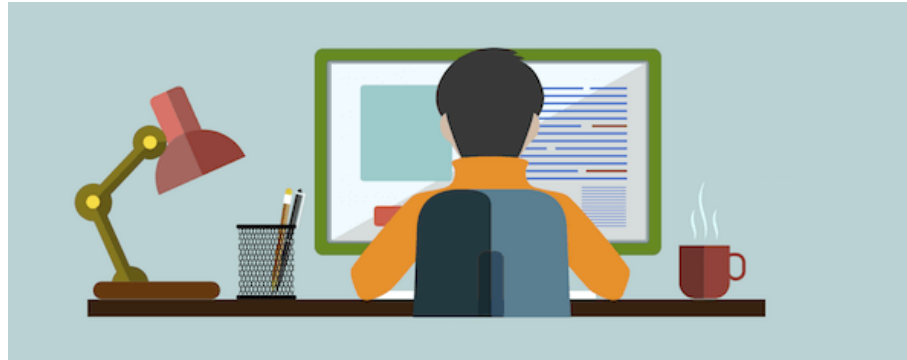
Part 2: Demographics

Part 5: Personality
Assessment (Big 5)

Part 4: Cognitive
Assessment

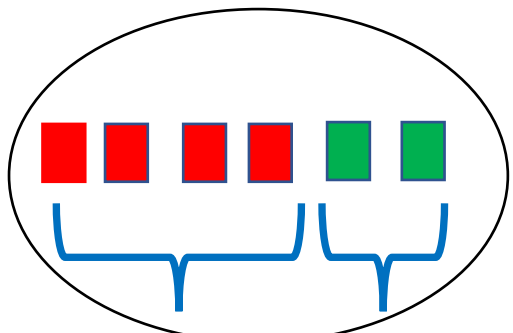
Part 1: Programming Puzzles

US
Brazil



India, Bangladesh

Set 1



BS

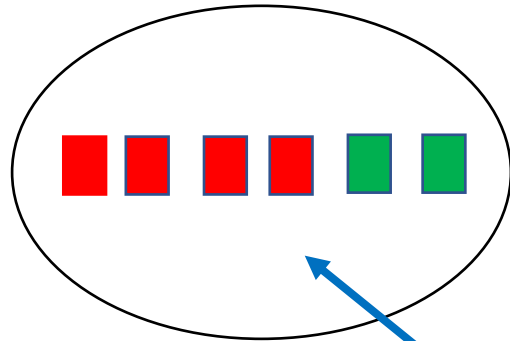
Non-BS

I/O

String

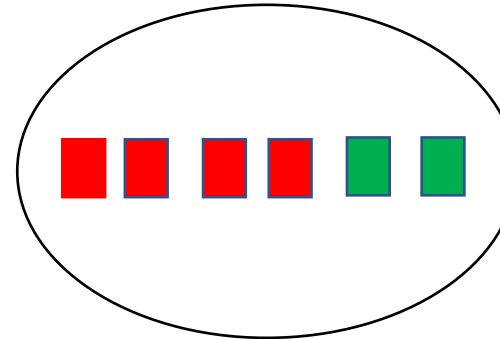
Crypto

Set 2

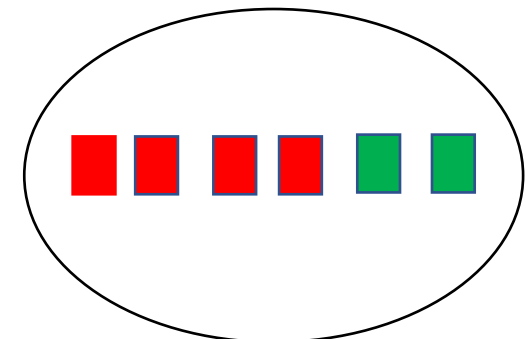


Random assignment

Set 3



Set 4



Programming puzzles

Part 1: Puzzles – BS on String API

```
01  // OMITTED: Import whatever is needed
02  public final class SystemUtils {
03      public static boolean setDate (String date)
04          throws Exception {
05          return run("DATE " + date);
06      }
07
08      private static boolean run (String cmd)
09          throws Exception {
10          Process process = Runtime.getRuntime().exec("CMD /C " + cmd);
11          int exit = process.waitFor();
12
13          if (exit == 0)
14              return true;
15          else
16              return false;
17      }
18  }
```


Part 1: Puzzles - BS on String API

```
01  // OMITTED: Import whatever is needed
02  public final class SystemUtils {
03      public static boolean setDate (String date)
04          throws Exception {
05          return run("DATE " + date);
06      }
07
08      private static boolean run (String cmd)
09          throws Exception {
10          Process process = Runtime.getRuntime().exec("CMD /C " + cmd);
11          int exit = process.waitFor();
12
13          if (exit == 0)
14              return true;
15          else
16              return false;
17      }
18  }
```

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 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)

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

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

BTACT Word list recall

Processing speed and working memory

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.

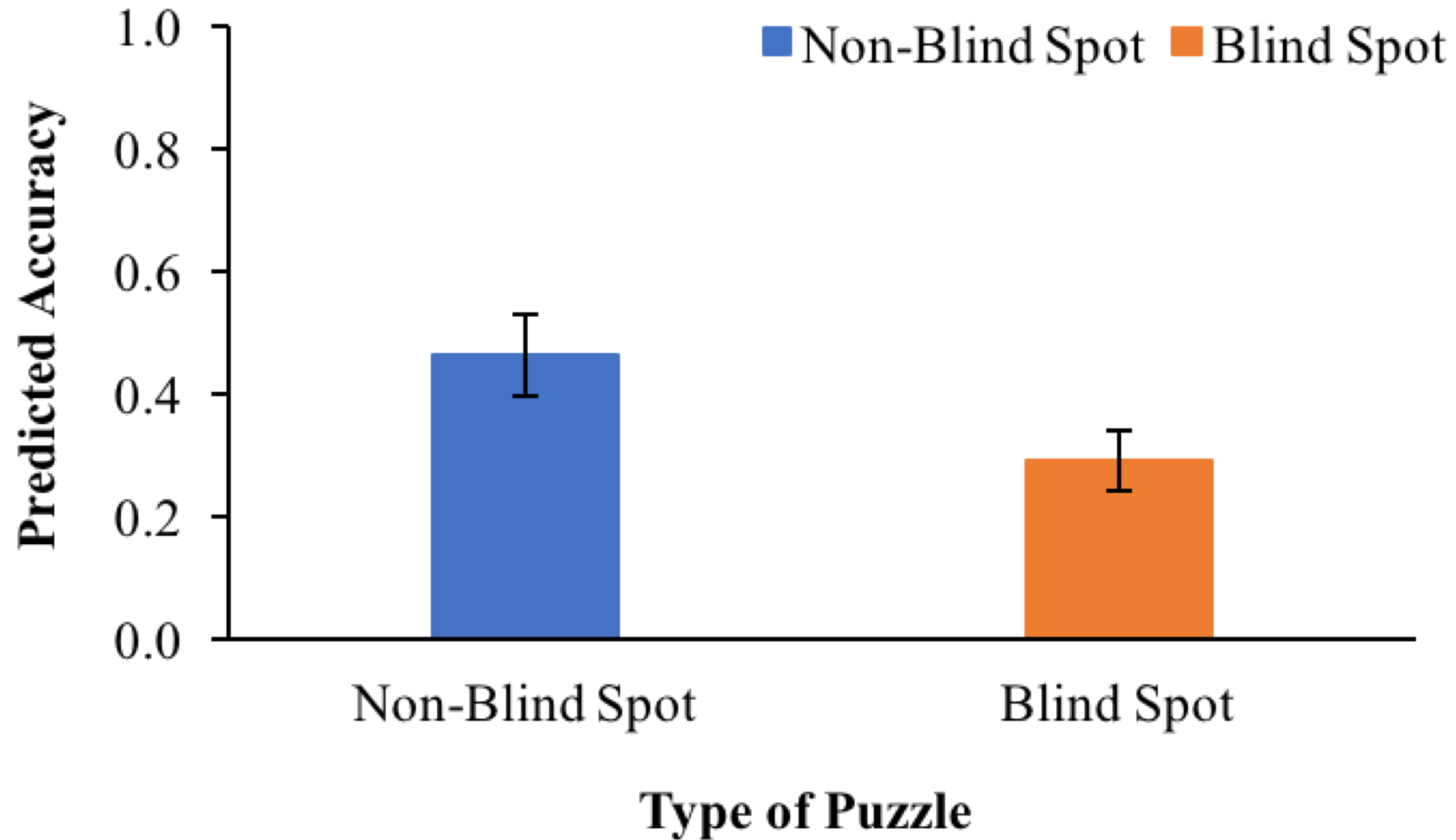
Play

Part 5: Personality Assessment (Big 5)



Data Analysis and Results

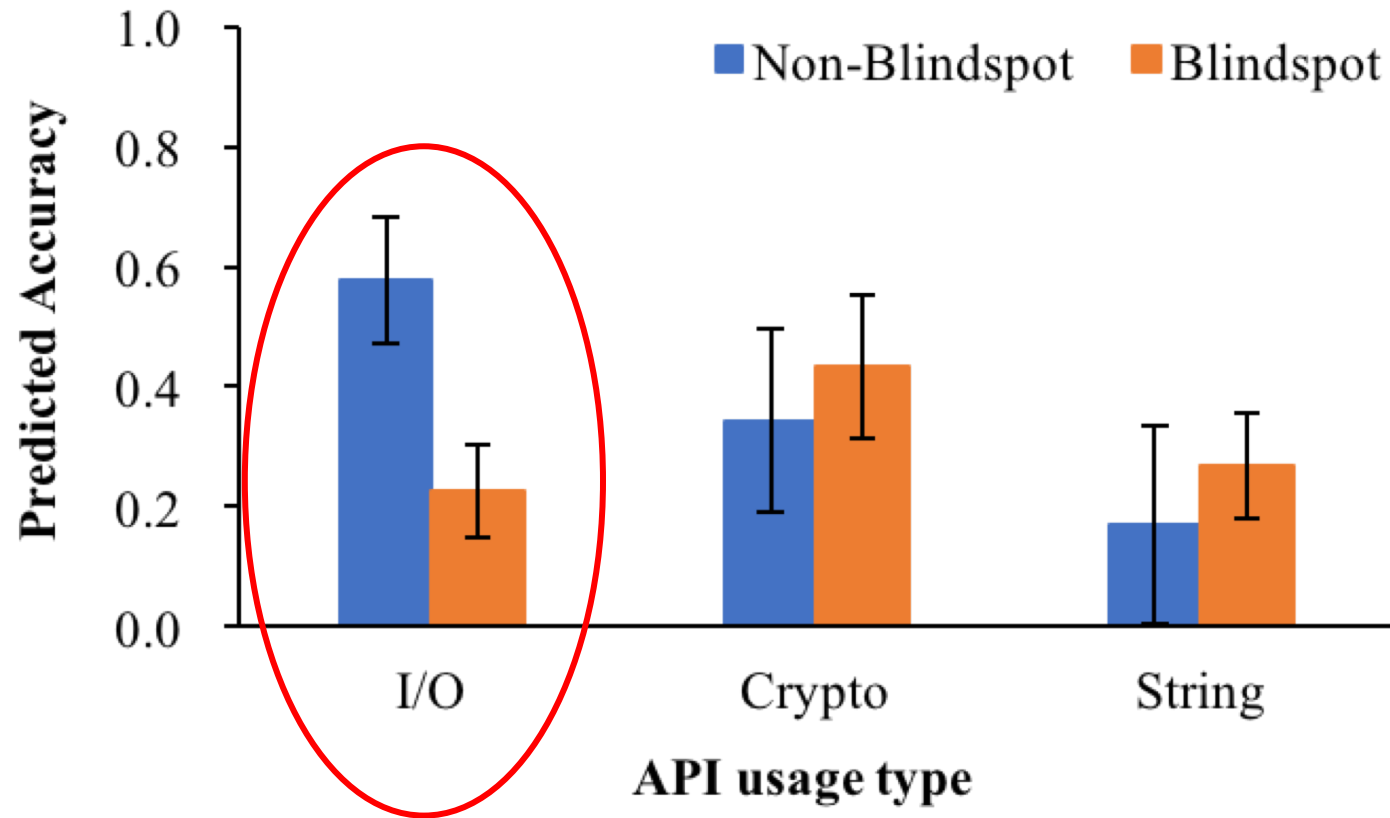
H1: Developers are less likely to solve puzzles with API functions containing BS than puzzles with innocuous functions.



Presence of blindspot had a significant effect on puzzle accuracy

Multilevel logistic regression. (Wald $\chi^2(2) = 20.60, p < .001$)

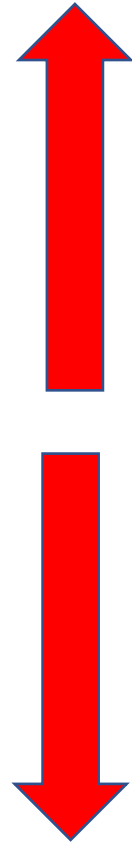
API Usage Type and Blindspots



Blindspot effect more pronounced for I/O API

.(Wald $\chi^2(2) = 24.81, p < .001$)

Cyclomatic Complexity and Blindposts



Complexity

Security accuracy
in puzzles with BS

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***

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***

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



CONSCIENTIOUSNESS



NEUROTICISM



EXTRAVERSION



AGREEABLENESS

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

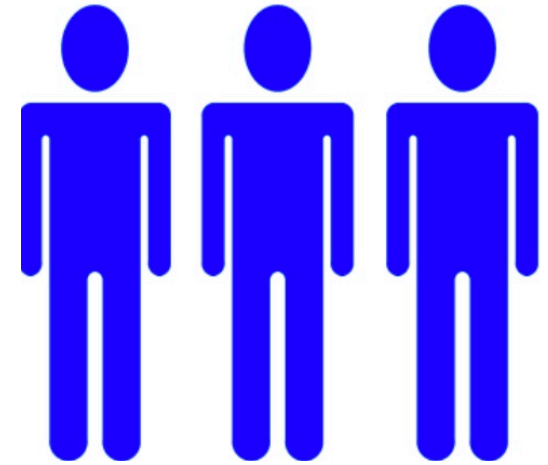
- Even expert, experienced, and highly intelligent developers will experience blindspots when using APIs
- Perceptions and gut feelings might be misleading
- More reliance on diagnostics tools

Software development process



VS

Functionality



Security



Openness

Thank you!

daniela@ece.ufl.edu
@dseabraoliveira