



Bad software is eating the world.

*Mark Felegyhazi*  
*CrySyS Lab / avatao*

# “Software is eating the world”



In short, software is eating the world

— *Marc Andreessen* —

AZ QUOTES

# Challenges of the software economy

need **skilled people**

to build **secure software**


# Internet of Things



Got a tip? [Let us know.](#)

[News](#) ▾ [Video](#) ▾ [Events](#) ▾ [CrunchBase](#)

Follow Us

 Message

**DISRUPT NY** Dave Cole, Co-Founder Of NextVR, To Discuss The Future Of VR At Disrupt NY [Get Your Tickets Now](#)

cybersecurity

Internet of Things

Gadgets

Popular Posts

CRUNCH NETWORK

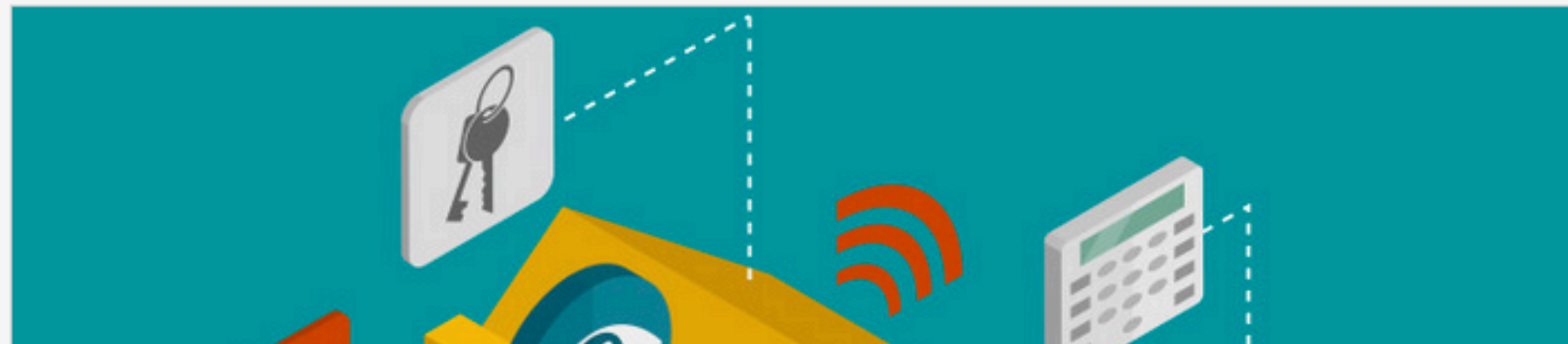
## Why IoT Security Is So Critical

Posted Oct 24, 2015 by [Ben Dickson](#) (@bendee983)

**10.2k**  
SHARES



Magic Instruments  
Replaces  
Traditional Guitar  
Strings With  
Buttons  
*6 days ago*







# Barnaby Jack pacemaker hack

Home > Security > Malware & Vulnerabilities

## NEWS

# Pacemaker hack can deliver deadly 830-volt jolt

Pacemakers and implantable cardioverter-defibrillators could be manipulated for an anonymous assassination



By Jeremy Kirk

IDG News Service | Oct 17, 2012 1:40 AM PT

## MORE LIKE THIS

Pacemaker hacker says worm could 'commit mass murder'

Top hacker dies days before scheduled execution  
Hat talk

Feds pressed to protect wireless medical devices from hackers

# Barnaby Jack pacemaker hack

1. Bedside transmitters sold with pacemakers (9-15m)
2. Ping to discover model and serial number of transmitter
3. Reprogram transmitter firmware
4. Reprogram the pacemaker remotely
5. Transmitters have access to remote servers
6. Upload specific firmware to remote servers and cause mass killing



# Self-driving cars



# CrySyS car hacking

PC running WinCC PLC management software

PLC controlling the uranium centrifuges

uranium centrifuges



PC running a vehicle diagnostic software

ECU controlling some function of the vehicle

vehicle





# Critical infrastructure





# Hungarian Lab found Stuxnet-like Duqu malware

By Ryan Naraine | October 21, 2011, 9:11am PDT

**Summary:** The Laboratory of Cryptography and confirmed its participation in the initial discovery



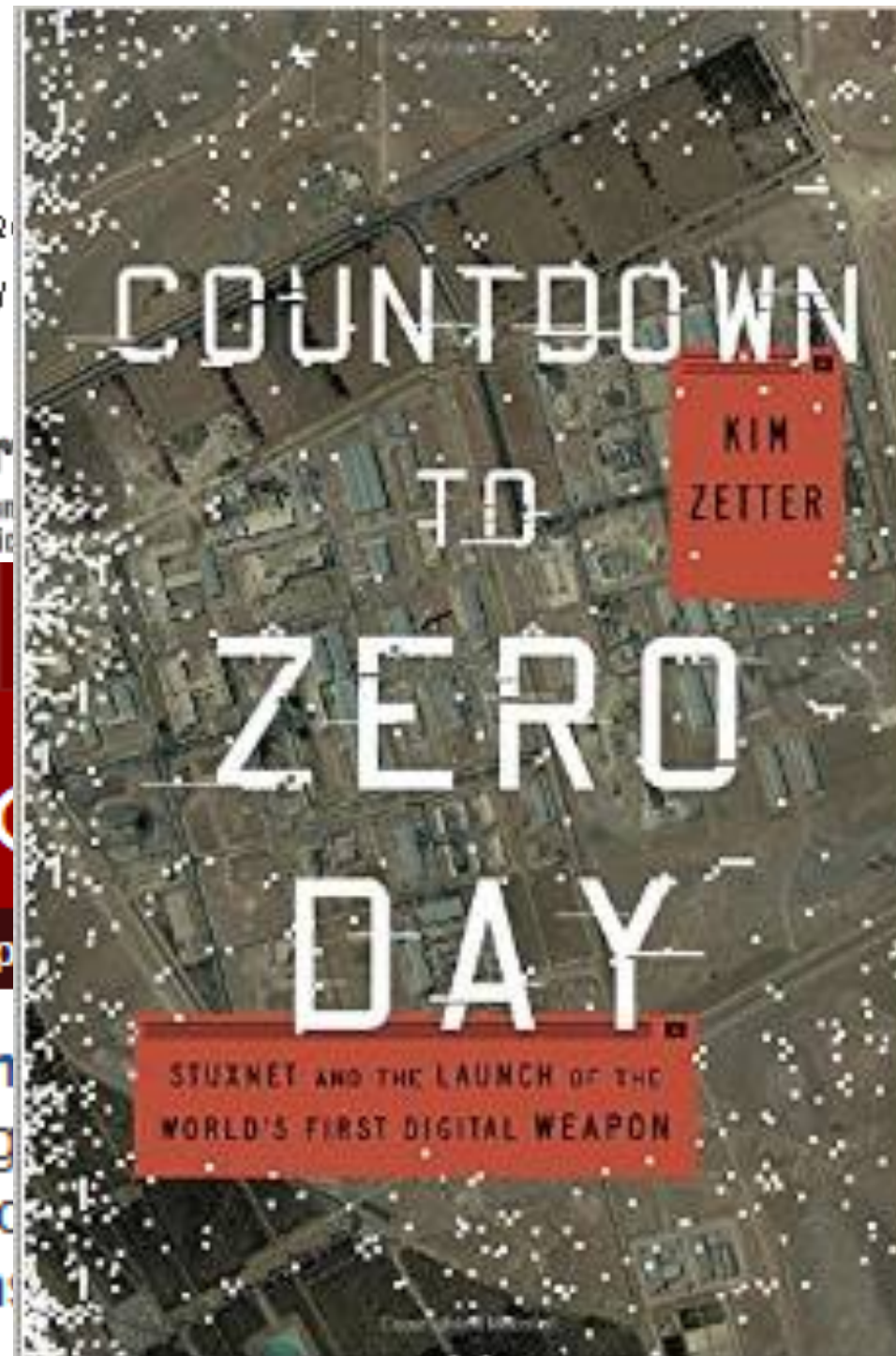
Laboratory of Cryptography  
Budapest University of Technology and Economics  
Department of Telecommunications

BBC

NEWS TECH

Home | UK | Africa | Asia | Europe

An in-depth look at Flan  
System Security at Hung  
in Budapest, said it stayed  
viruses, worms and trojan  
to catch.



Travel

Future

la | Business | Health

tography and  
and Economics  
rent to the  
s were designed

# Websites are the key target



Follow @ashleyrcarman

May 22, 2015

## Study: 86 percent of websites contain at least one 'serious' vulnerability

Share this content:



While high-profile vulnerabilities, including **Heartbleed** and **ShellShock**, might have garnered more press than most other vulnerabilities for putting websites at-risk, in reality, these flaws are being patched and addressed more than other pressing vulnerabilities in web application software.

Eighty-six percent of all websites have at least one serious vulnerability, and most of the time, they





# Apps are no better

**“90% of security incidents result from exploits against defects in software.”**

**ACCORDING TO THE U.S. DEPARTMENT OF HOMELAND SECURITY (DHS)**

**“3 out of 4 applications produced by software vendors fail to meet OWASP Top 10.”**

**ACCORDING TO VERACODE'S STATE OF SOFTWARE SECURITY REPORT**

# What can happen? – Advanced attack



**Target**

**HOW:** Sophisticated kill chain including exploitation of a vulnerable web application

**RESULT:** Hackers stole names, mailing addresses, phone numbers and email addresses from over 70 million shoppers

# What can happen? – Weak suppliers



**JP Morgan  
Chase**

**HOW: Vulnerability on  
website built and maintained  
by a third-party vendor in  
support of a charity**

**RESULT: Usernames and  
passwords for 76 million  
households and 7 million  
businesses accounts stolen**

# What can happen? – OpenSSL Heartbleed



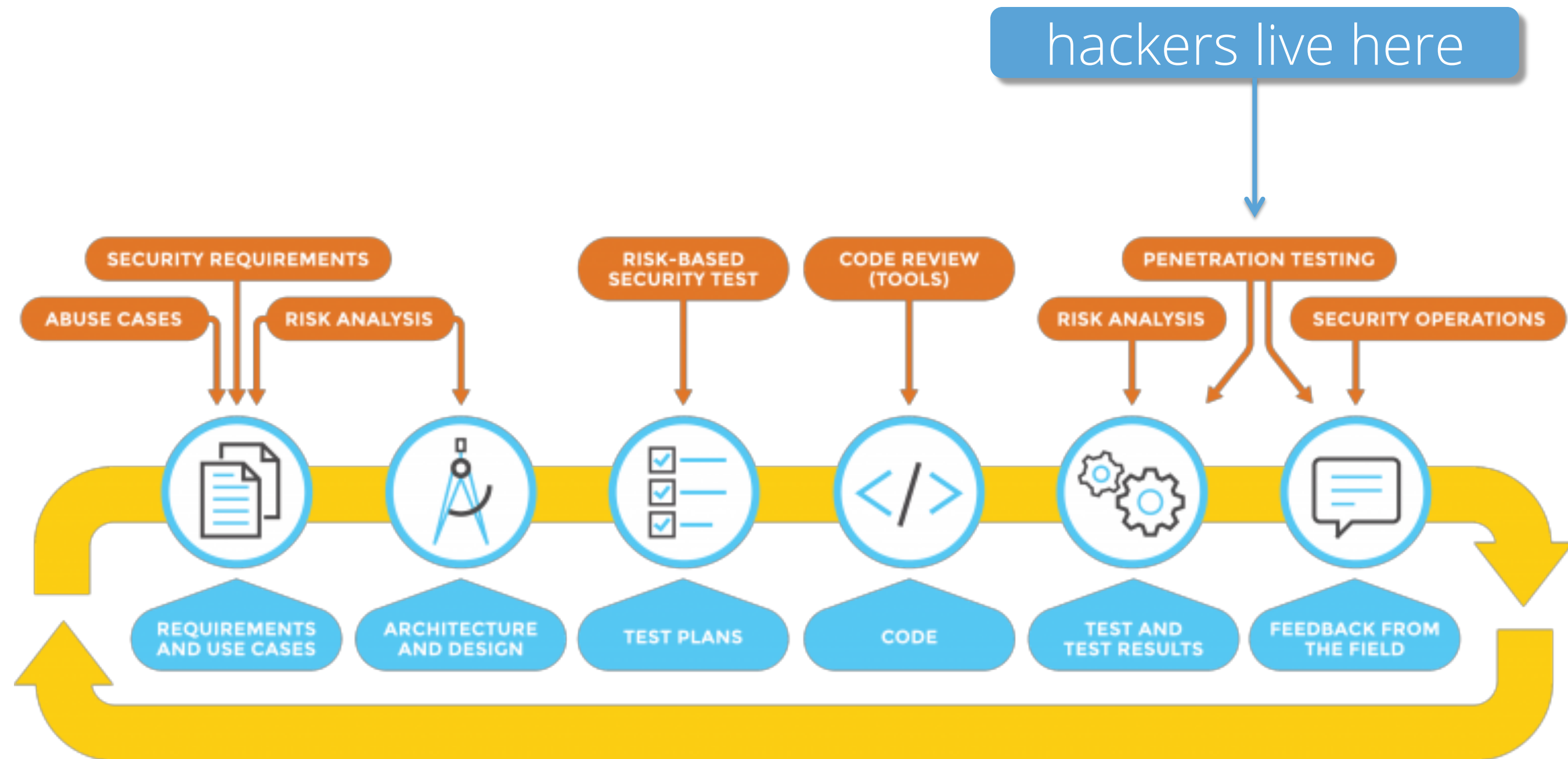
## Community Health

**HOW:** Targeted a flaw in OpenSSL, CVE-2014-0160, better known as Heartbleed

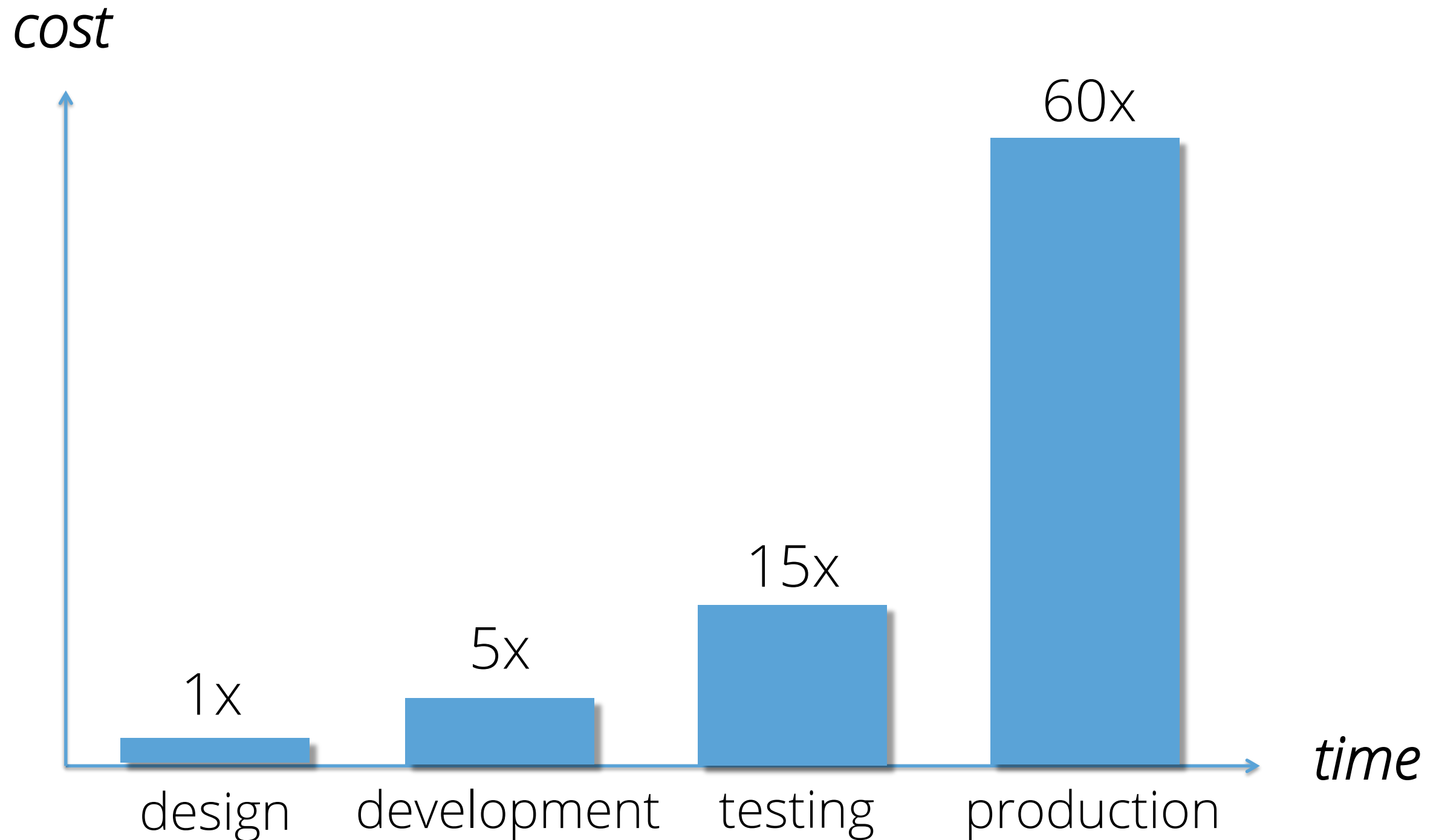
**RESULT:** The theft of Social Security numbers and other personal data belonging to 4.5 million patients

# How to write secure code?

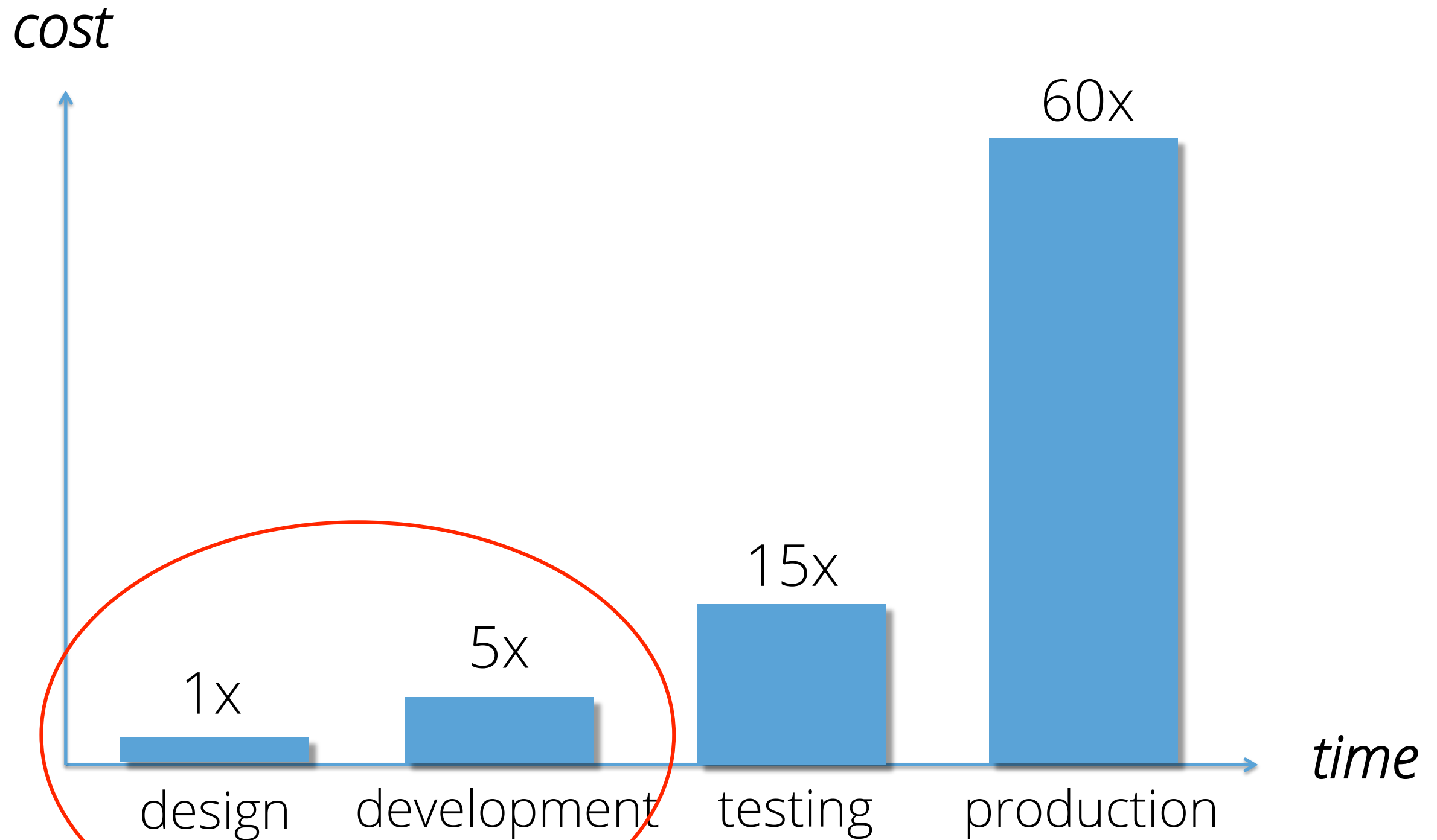
# Secure software development



# cost of security bugs



# cost of security bugs





# Code reuse

Code reuse is the Holy Grail  
of Software Engineering.

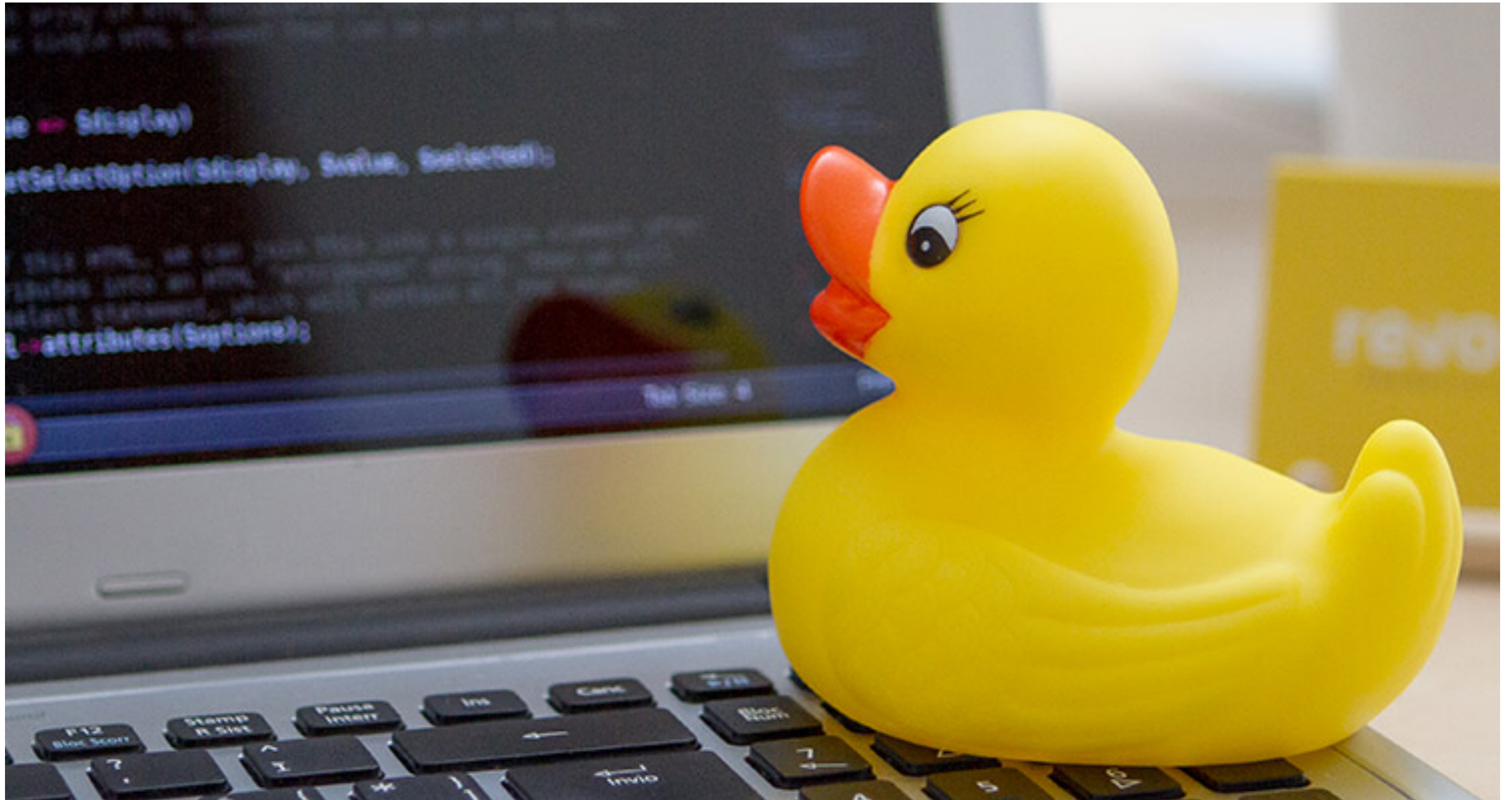
Douglas Crockford

quote fancy

# Debugging (for security)

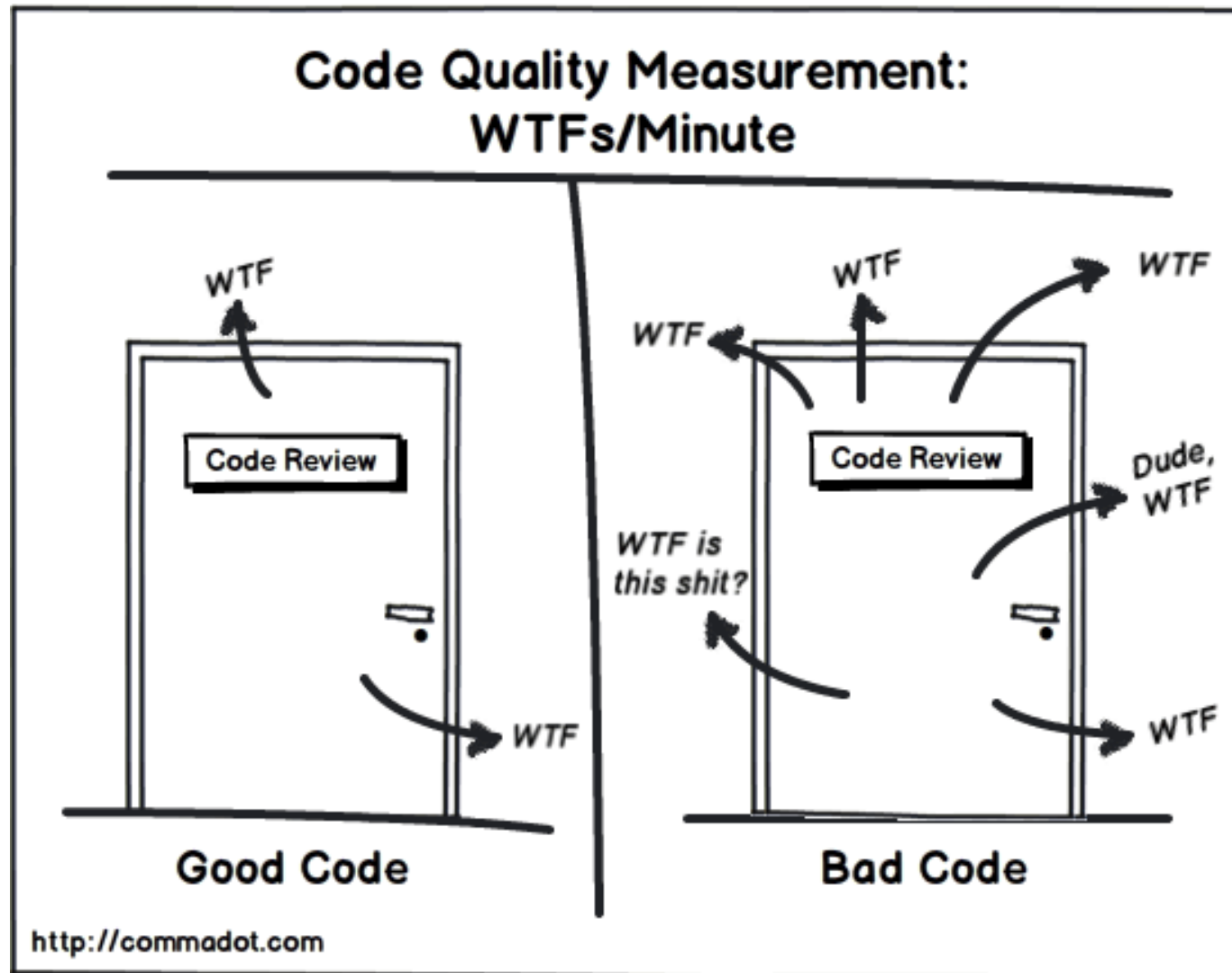


# Rubber-duck debugging





# Code review



# Pair programming



# Automated code testing

```
$ python sqlmap.py -u "http://target/vuln.php?id=1" --batch
```



**{1.0-dev-4512258}**

<http://sqlmap.org>

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

```
[*] starting at 15:02:07
```

```
[15:02:07] [INFO] testing connection to the target URL
```

```
[15:02:07] [INFO] heuristics detected web page charset 'ascii'
```

```
[15:02:07] [INFO] testing if the target URL is stable. This can take a couple of seconds
```

```
[15:02:08] [INFO] target URL is stable
```

```
[15:02:08] [INFO] testing if GET parameter 'id' is dynamic
```

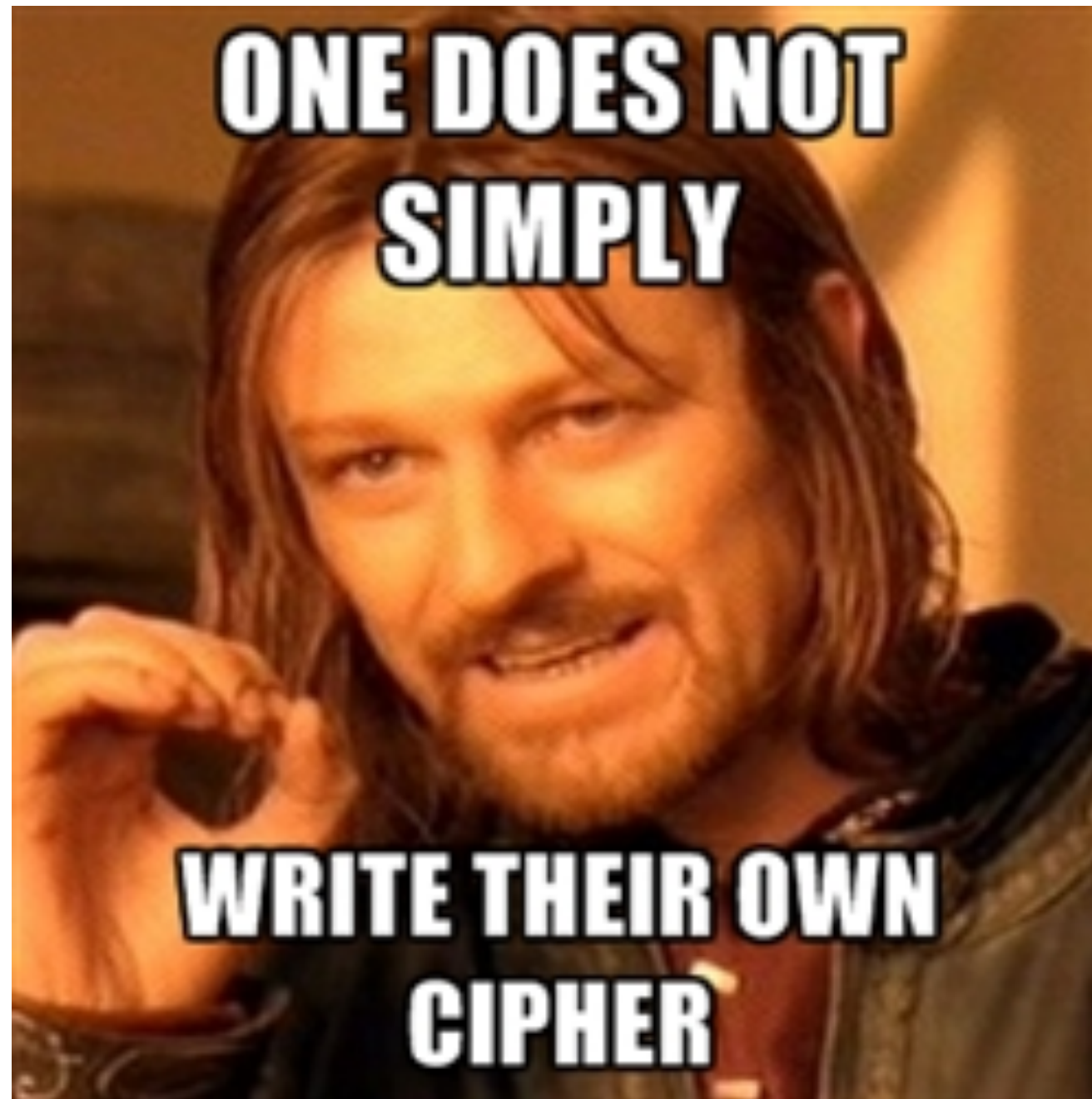
```
[15:02:08] [INFO] confirming that GET parameter 'id' is dynamic
```

```
[15:02:08] [INFO] GET parameter 'id' is dynamic
```

```
[15:02:08] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
```



Use reliable crypto protocols



Need people to **write secure code**



# Businesses need IT people



No bad developers, please



# Security is missing from education



## VULNERABILITIES / THREATS

4/7/2016  
11:00 AM



Kelly Jackson  
Higgins

## Top US Undergraduate Computer Science Programs Skip Cybersecurity Classes

**New study reveals that none of the top 10 US university computer science and engineering program degrees requires students take a cybersecurity course.**



# security @ universities?



SPOT





costly to build practice labs  
(infrastructure AND content)



it must be fun

Need practical, fun learning!



# Web Security Bootstrapping

Path description

Challenge list

Path statistics

## Challenges

Cookie Monster

BetterManager

Better Status

Let the Files be Include

Company Homepage

Company Homepage

PHP Sadness

Sadness 1

Sadness 2

Sadness 3

Sadness 4

Sadness 5

Sadness 6

Serial Killer

PHPUnserialize

PHPUnserialize2

DjangoCookie

## Challenge details

# Better Status

by Alex Badics



## Skill tags

Web Security

CGI

avatao

High-quality, up-to-date  
IT security exercises

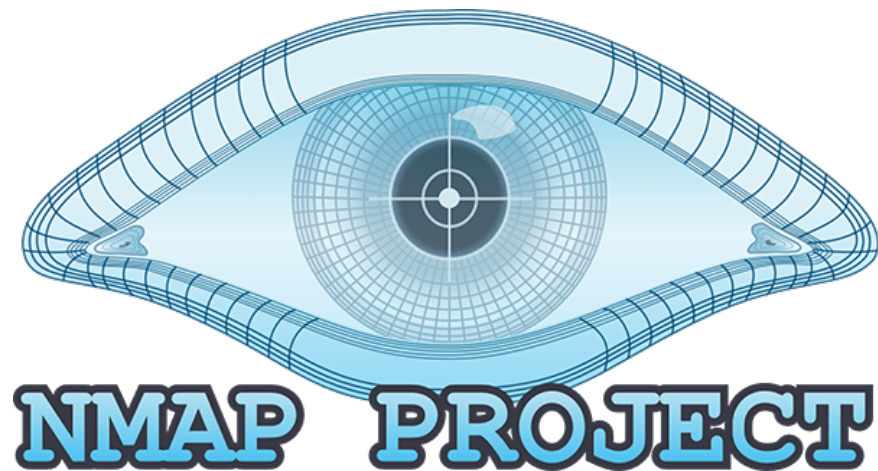
## Start your environment

Hey there! To start your enviroment, please click on the button below.

Start!



# Security tool tutorials





# Hacking events (created in 5 mins)





# Security for developers



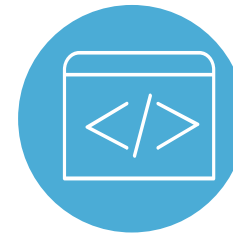
**Mark Felegyhazi** w: <http://avatao.com>  
e: [contact@avatao.com](mailto:contact@avatao.com)

Join our community  
to build secure software!

**<http://platform.avatao.com/defcamp2016>**  
(open until Sunday, Nov 13)

**avatao<sup>TM</sup>**

Cloud-based  
virtual platform



Hands-on IT  
security challenges

Expert community



Security tools and  
fun adventures

Hands-on exams  
proving true skills



Cost-effective training