How to spend $3.6M on one coding mistake and other fun stuff you can do with $3.6M

Matias Madou Ph.D., Secure Code Warrior
Matias Madou, Ph.D.

CTO and Co-Founder

• Ph.D. in Computer Engineering from Ghent University
• Over 15 years hands-on software security experience
• Led multiple application security research projects for HPE Fortify which have led to commercial products
• Instructor for advanced application security training courses
• Speaker at global conferences including RSA Conference, Black Hat, DefCon, BSIMM, OWASP AppSec and BruCon
What we believe...

... that developers can become the first line of defense against cyber attacks.
What can coding mistakes lead to?

INTRODUCTION
Coding failure costs money

Ariane 5 rocket
• $7 billion
• 10 years of work

Technical:
• Velocity: 64-bit float
• Convert to 16-bit int
• Overflow
• Error handling suppressed (performance)
Coding failure brand damage
C-Level people get fired
What's in the name?

APPSEC
Why visibility matters—the Ariane 5 crash

- Velocity was represented as a 64-bit float
- A conversion into a 16-bit signed integer caused an overflow
- The current velocity of Ariane 5 was too high to be represented as a 16-bit integer
- Error handling was suppressed for performance reasons

-- Vertical velocity bias as measured by sensor
L_M_BV_32 :=
  TBD.T_ENTIER_32S ((1.0/C_M_LSB_BV) *
  G_M_INFO_DERIVE(T_ALG.E_BV));
-- Check, if measured vertical velocity bias can be
-- converted to a 16 bit int. If so, then convert
if L_M_BV_32 > 32767 then
  P_M_DERIVE(T_ALG.E_BV) := 16#7FFF#
elsif L_M_BV_32 < -32768 then
  P_M_DERIVE(T_ALG.E_BV) := 16#8000#
else
  P_M_DERIVE(T_ALG.E_BV) :=
    UC_16S_EN_16NS(TDB.T_ENTIER_16S(L_M_BV_32));
end if;
-- Horizontal velocity bias as measured by sensor
-- is converted to a 16 bit int without checking
P_M_DERIVE(T_ALG.E_BH) :=
  UC_16S_EN_16NS (TDB.T_ENTIER_16S ((1.0/C_M_LSB_BH) *
  G_M_INFO_DERIVE(T_ALG.E_BH));

*Source: http://moscova.inria.fr/~levy/talks/10enslongo/enslongo.pdf
```java
/**
 * Method will save the payment details into the database.
 */

public boolean savePaymentDetails(PaymentDetails paymentDetails) {
    Session session = HibernateUtil.getCurrentSession();
    Session session = null;
    Transaction tx = null;
    boolean isSuccess = true;
    try {
        session = sessionFactory.getCurrentSession();
        tx = session.beginTransaction();
        String dml = "insert into paymentDetails (orderId, cardNumber, card Owner, totalAmount) values (?,?,?,?)";
        String orderId = paymentDetails.getOrderId();
        String cardNumber = paymentDetails.getCardNumber();
        String cardOwner = paymentDetails.getCardOwner();
        String totalAmount = paymentDetails.getTotalAmount();
        tx.commit();
    } catch (Exception e) {
        logger.error("Error at saving Payment Details information ", e);
        if (tx != null) {
            tx.rollback();
            throw new ApplicationException(1111, "Database Exception.");
        }
        isSuccess = false;
    }
```
HI. THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.

OH DEAR - DID HE BREAK SOMETHING? IN A WAY -

OH YES. BOBBY BROKE THE TABLE.

DID YOU REALLY NAME YOUR SON ROBERT 3: DROP TABLE STUDENTS;

- OH, YES. WE CAN NOT SELL HIM.

MERRY CHRISTMAS MATIAS!

- JACOB
  2008
Why is this not resolved yet?

Security knows about issues in code

1) Fix known security issues
2) Do not introduce new issues

Scale of AppSec team?
Ton of overhead!
700+ categories of problems!

∞ Never ending story…
Flying a plane: simulator vs flying for real

Time spend in training

Time spending doing it for real

Beginner Master
Software Development Lifecycle

WHERE DO MISTAKES HAPPEN
Software development lifecycle

Waterfall, agile, ...

1. Security, where?
2. Developer view?
Secure Software Development Lifecycle

Microsoft SSDLC

Cigital Touchpoints
How does a developer look at this?

1. Developer
2. Write
3. Repository
4. Build
5. Deploy
6. Production
How does a developer look at this?

Developers can do something

No idea what’s happening over there

SECURITY...
Developers can do something. No idea what's happening over there.

How does a developer look at this?

<table>
<thead>
<tr>
<th>DEVELOPERS</th>
<th>DESIGNERS</th>
<th>PROJECT MANAGERS</th>
<th>QA</th>
<th>SYSADMINS</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Developer" /></td>
<td><img src="image2" alt="Designer" /></td>
<td><img src="image3" alt="Project Manager" /></td>
<td><img src="image4" alt="QA" /></td>
<td><img src="image5" alt="SysAdmin" /></td>
</tr>
</tbody>
</table>

---

Developer

Production
Developers can do something

No idea what’s happening over there

Developer: total control
Security: no control

Developer: no control
Security: can access it...
Developers can do something

No idea what’s happening over there

**How does a developer look at this?**

- **Developer** → **Write**
- **Repository** → **Build** → **Deploy** → **Production**

**Training** → **SAST**

**In IDE help** → **IAST**

**SECURITY**...

**DAST** → **RASP**
WHERE DO WE SPEND THE MONEY
How do companies spend their money?
How do companies spend their money?

- **Developer**: Training
- **Write**: In IDE help
- **Repository**
  - SAST
  - IAST
- **Build**
- **Deploy**
  - DAST
  - RASP
- **Production**
How do we spend the AppSec budget in the most optimal way? Nobody knows.
What we see in the field? Is there a pattern?

ACTUAL SPENDING
What type of company is this?

“All is good”-company

Or, we are not hacked company

... yet
“Ow s***, we need to do something” - company

Ow s***, we need to do “pen-testing” and hackers and the like
What type of company is this?

Company maturing over time... but it’s very reactive and baseless.

- Developer
- Write
- Repository
- Build
- Deploy
- Production

- Training
- In IDE help
- SAST
- IAST
- DAST
- RASP

Good sales people, lot of traction

PCI Compliance sticker

Gartner says it’s the latest good stuff
WHERE DO WE HAVE TO SPEND?

Pros and cons on the technology
What does the BSIMM say?

Developer
- Training
- (T) Training Practice

Write
- In IDE help

Repository
- SAST
- (CR) Code Review
- (ST) Security Testing
- (PT) Penetration Testing

Build
- IAST

Deploy
- DAST

Production
- RASP

(? CMVM: Maybe CMVM1.1: Create interface with incident response ?)
What does the BSIMM say?

T1.1: Provide awareness training
T2.6: Include security resources in onboarding
T3.4: Require annual refresher
CR1.4: Use automated tools with manual code review
CR2.6: Use automated tools with tailored rules
CR3.5: Enforce coding standards
What does the BSIMM say?

Developer → Write → Repository → Build → Deploy → Production

- PT1.3: Use penetration testing tools internally
- ST2.5: Include security tests in QA automation
- PT2.3: Schedule periodic penetration tests for application coverage
- PT3.2: Have the SSG customize penetration testing tools and scripts
End result: all solutions have their pros and cons

Cool ... but we cannot call this progress

All this is saying: Yes, there is a valid case to spend money
Finding problems vs. coding right

WHAT DO WE DO IN APPSEC?
What do we do?

Write Secure code: Coding guidelines

• OWASP Secure coding guidelines
• Android Secure development (JSSA)
• ...

Find the bad stuff: talk about vulnerabilities

• SQL Injection
• OWASP Top 10
• ...

Developer

Write

Repository

Build

Deploy

Production

Training

In IDE help

SAST

IAST

DAST

RASP
AppSec approach today

“SELECT * FROM database WHERE
param1 = ‘ " + param1 + " ’ and
param2 = ‘ " + param2 + " ’ and
param3 = ‘ " + param3 + " ’ and
param4 = ‘ " + param4 + " ’;”

“SELECT * FROM database WHERE
param1 = ? and
param2 = ? and
param3 = ????????????????? and
param4 = ‘ " + param4 + " ’;”

Ask QA to find an exploit?
What’s the difference?

Vulnerability

• SQL injection
• Command injection
• ...

Write coding guideline

• Use parameterized queries
• Command line execution is forbidden
• ...

Badness-ometer

Courtesy of Gary McGraw, Cigital
Best ROI and value for money?

Write Secure code: Coding guidelines

Find the bad stuff: talk about vulnerabilities

Developer → Write → Repository → Build → Deploy → Production

Training → In IDE help → SAST → IAST → DAST → RASP

Prevention → Detection

Badness-ometer

Courtesy of Gary McGraw, Cigital
What type of company is this?

Write Secure code: Coding guidelines

Developer → Write → Repository → Build → Deploy → Production

Training → In IDE help

Find the bad stuff: talk about vulnerabilities

SAST → IAST → DAST → RASP

80% NOT introduced

20% detected and fixed
WHERE DO WE HAVE TO SPEND?
Let’s throw numbers in there

General consensus: the earlier you find it, the less it costs to fix

Cost/Defect during Phases of Software Development

Actual data from Jim Routh, Aetna
Should we care?

3.6 million, average cost of a breach

You can fix more than 1 problem!

Cost/Defect during Phases of Software Development

<table>
<thead>
<tr>
<th>Phase</th>
<th>Cost</th>
<th>Defects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>$139</td>
<td>25,899</td>
</tr>
<tr>
<td>Design</td>
<td>$455</td>
<td>7,912</td>
</tr>
<tr>
<td>Code</td>
<td>$977</td>
<td>3,685</td>
</tr>
<tr>
<td>Test</td>
<td>$7,136</td>
<td>504</td>
</tr>
<tr>
<td>Maintain</td>
<td>$14,102</td>
<td>255</td>
</tr>
</tbody>
</table>

Actual data from Jim Routh, Aetna
<table>
<thead>
<tr>
<th>The numbers:</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10D @ $$/day</td>
<td>Xxxx</td>
<td>$20,000</td>
<td></td>
</tr>
<tr>
<td>Issues found</td>
<td>Yyyy</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Developer cost(fix)</td>
<td>Zzzz</td>
<td>No time</td>
<td></td>
</tr>
<tr>
<td>COST</td>
<td>Pretty big number</td>
<td>Waste of money</td>
<td></td>
</tr>
<tr>
<td>COST/issue</td>
<td>Still a big number</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Penetration testing: Consulting services

<table>
<thead>
<tr>
<th>The numbers:</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10D @ $$/day</td>
<td>Xxxx</td>
<td>$20,000</td>
</tr>
<tr>
<td>Issues found</td>
<td>Yyyy</td>
<td>10</td>
</tr>
<tr>
<td>Developer cost (fix)</td>
<td>Zzzz</td>
<td>$2,000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COST</th>
<th>Pretty big number</th>
<th>$40,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>COST/issue</td>
<td>Still a big number</td>
<td>$4,000</td>
</tr>
</tbody>
</table>

Fill in your own numbers! This is an example. Do the exercise internally.
Penetration testing: Consulting services

<table>
<thead>
<tr>
<th>The numbers:</th>
<th>Xxxx</th>
<th>$20,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>10D @ $$/day</td>
<td>Xxxx</td>
<td>$20,000</td>
</tr>
<tr>
<td>Issues found</td>
<td>Yyyy</td>
<td>10</td>
</tr>
<tr>
<td>Developer cost(fix)</td>
<td>Zzzz</td>
<td>$2,000</td>
</tr>
<tr>
<td>COST</td>
<td>Pretty big number</td>
<td>$40,000</td>
</tr>
<tr>
<td><strong>COST/issue</strong></td>
<td>Still a big number</td>
<td><strong>$4,000</strong></td>
</tr>
</tbody>
</table>

Bear in mind that these are real issues!
Likability of an adversary exploiting these is high
<table>
<thead>
<tr>
<th>The numbers:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost of SAST solution</td>
<td>Xxxx</td>
</tr>
<tr>
<td>Issues found</td>
<td>Yyyy</td>
</tr>
<tr>
<td>Developer cost (fix)</td>
<td>Zzzz</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COST</th>
<th>Pretty big number</th>
</tr>
</thead>
<tbody>
<tr>
<td>COST/issue</td>
<td></td>
</tr>
</tbody>
</table>

Bear in mind that these are theoretical problems.
The numbers:
Cost of training
??
??

COST

COST/issue

Effect of training on coding: Less mistakes introduced + issues fixed
Conclusion on where to spend money

Write Secure code: Coding guidelines

Find the bad stuff: talk about vulnerabilities

Developer

Write

Repository

Build

Deploy

Production

1. Measure! Security is measurable
2. Calculate ROI
3. Optimize your budget

Developer introduces $45.18/day on security problems in the code
Solution 1: Get rid of all developers

Write Secure code: Coding guidelines

Find the bad stuff: talk about vulnerabilities

1. Measure
2. Calculate
3. Optimize

Developer introduces $45.18/day on security problems in the code
Solution 2: Do the numbers and optimize budget

1. Measure! Security is measurable
2. Calculate ROI
3. Optimize your budget

Developer introduces $45.18/day on security problems in the code
Try it out yourself

TOURNAMENT
Join the Tournament: Play and win
ACCOUNT & TOURNAMENT REGISTRATION

1. GO TO: https://portal.securecodewarrior.com/#/register

2. CLICK ‘REGISTER’, FILL IN YOUR EMAIL AND USE THE FOLLOWING TOKEN KEY: 947 273 385 338

3. Click on the Tournaments Tab, and then Click BENELUX2017

THE TOURNAMENT WILL GO LIVE AT 10.30AM and stop at 4:00PM

Follow us on Twitter and be in with a chance to win some more cool prizes @Seccodewarrior #securecodewarrior
ARE YOU A SECURE CODE WARRIOR?

Join Secure Code Warrior's live tournament to prove your web application security knowledge of the OWASP Top 10 or if you simply want to learn more about secure coding.

Players will be presented with a series of vulnerable code challenges that will ask them to identify the problem, locate the insecure code, and fix the vulnerability. Select from various software languages to complete the tournament, including: Java EE, Java Spring, C# MVC, C# WebForms, Ruby on Rails, Python Django, Scala Play, Java Struts & Node JS.

Watch as you climb to the top of the leaderboard and be crowned the 'Secure Code Warrior.' Prizes will be provided to the top three winners.

Instructions:
1. Visit https://portal.securecodewarrior.com/#/register
2. Enter invitation token: 947 273 385 338
3. Update your details and go to the Tournaments tab and enter join code: BENELUX2017
4. Follow us on social media and use hashtag #securecodewarrior for a chance to win extra prizes

Connect with us:
- Twitter: @seccodewarrior
- Facebook: facebook.com/securecodewarrior
- LinkedIn: linkedin.com/company/secure-code-warrior
- Website: securecodewarrior.com
Matias Madou, Ph.D.
CTO and Co-Founder
Secure Code Warrior

+32 495 25 49 78
mmadou@securecodewarrior.com
@mmadou
www.linkedin.com/in/matiasmadou/
Follow us on social media and use the hashtag #securecodewarrior for a chance to win prizes!

- APPLICATIONSECURITYINSIGHTS.SECURECODEWARRIOR.COM
- SECURECODEWARRIOR.COM
- @SECCODEWARRIOR
- LINKEDIN.COM/COMPANY/SECURE-CODE-WARRIOR
- FACEBOOK.COM/SECURECODEWARRIOR/