

Never lose your Luggage again!

bluesmart



SAVE \$100

PRE ORDER NOW ▶



DATA CENTRE

SOFTWARE

NETWORKS

SECURITY

INFRASTRUCTURE

BUSINESS

HARDWARE

SCIENCE

BOOTNOTES

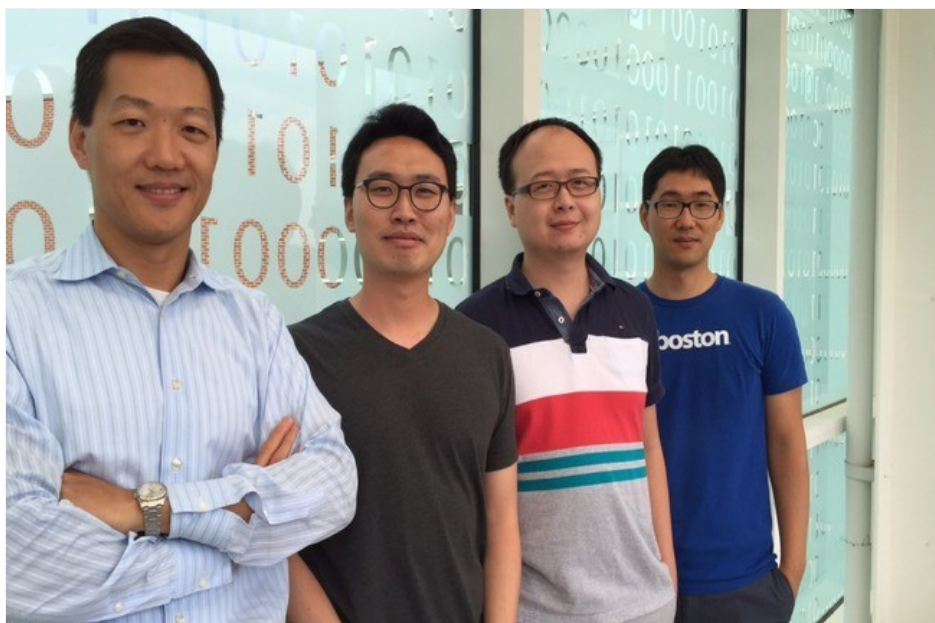
FORUMS

WEEKEND

**Security**

Facebook hands hackers \$100k for breaking browsers

Internet Defense Prize™ handed out, bugs broken. Hello Oracle?

14 Aug 2015 at 05:03, [Darren Pauli](#)

149

22



Four researchers have scored US\$100,000 from Facebook for revealing 11 bugs affecting platforms including the Chrome and Firefox browsers using novel vulnerability discovery methods.

The Georgia Institute of Technology team of PhD students Byoungyoung Lee and Chengyu Song, and professors Taesoo Kim and Wenke Lee discovered the holes affecting C++ programs.

The Social Network™, together with Usenix, offer up a pool of US\$300,000 under the [Internet Defense Prize™](#) first created last year.

The hacks are detailed in the paper *Type Casting Verification: Stopping an Emerging Attack Vector* ([PDF](#)) in which the quartet offered a tool to help detect the *bad-casting* and *type-confusion* holes.

Quoth the researchers:

Type casting, which converts one type of an object to another, plays an essential role in enabling polymorphism in C++ because it allows a program to utilize certain general or specific implementations in the class hierarchies. However, if not correctly used, it may return unsafe and incorrectly casted values, leading to so-called bad-casting or type-confusion vulnerabilities.

Since a bad-casted pointer violates a programmer's intended pointer semantics and enables an attacker to corrupt memory, bad-casting has critical security implications similar to those of other memory corruption vulnerabilities. Despite the increasing number of bad-casting vulnerabilities, the bad-casting detection problem has not been addressed by the security community.

The authors' CaVER vulnerability detection tool found two unknown browser bugs and nine in

More like this[Vulnerabilities](#)[Facebook](#)[Security](#)**Most read**

The Raspberry Pi is succeeding in ways its makers *almost* imagined



Google makes it official: Chrome will freeze Flash ads on sight from Sept 1



Malware menaces poison ads as Google, Yahoo! look away



Krebs: I know who hacked Ashley Madison



The most tragic thing about the Ashley Madison hack? It was really 1% actual women

Spotlight

Malware menaces poison ads as Google, Yahoo! look away



Want security? Next-gen startups show how old practices don't cut it

libstdc++ which have since been pinched.

The team says the dynamic analysis checks cause between a 7.6 percent and whopping 64.6 percent overhead on performance-intensive Chromium and Firefox benchmarks respectively.

A US\$50,000 award went to a pair of German researchers who used static analysis to find second-order vulnerabilities in web applications. Facebook says the team used the cash to bring in new researchers and build new features.

Facebook security engineering manager Ioannis Papagiannis says such defensive security research needs to be more common in the academic world.

"We all benefit from this kind of work—a large part of why Facebook has been successful in serving nearly 1.5 billion people is because we have been quick to introduce and adopt categories of systems and frameworks that prevent whole classes of vulnerabilities at once," Papagiannis says in a statement.

"As an industry, we need to invest in those kinds of solutions that scale."

Might that statement be a subtle swipe at [Oracle](#), which this week declared bug bounty programs expensive and ineffectual? There's a comment field down there and you know how to use it. ®

Tips and corrections

4 Comments

More from The Register



Holy Zuck! Facebook fraud suspect VANISHES

Lawyer: I 'haven't got a clue' where he's gone

14 Comments



Judge greenlights class-action suit accusing AMD of securities fraud

Plaintiffs claim chipmaker misled investors about supply-chain woes

8 Comments



PEAK TECHNOLOGY? Facebook, Amazon, Netflix, Google, Apple stocks hit the deck

Billions wiped off the charts – and Twitter falls below its stock-market debut

7 Comments



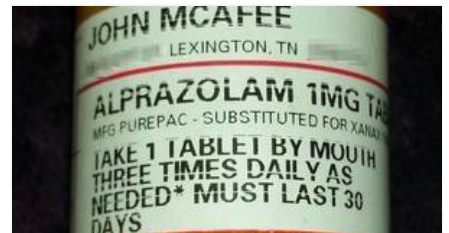
Rise up against Oracle class stupidity and join the infosec strike



Patching a fragmented, Stagefrightened Android isn't easy



Junior defence staffer on trial for 'posting secret dossier to 4chan'



John McAfee cuffed by Tennessee cops, faces drug-driving, gun rap



Hacktivists congratulate Daily Show's Jon Stewart via Donald Trump's website



Facebook slurps 'paste sites' for STOLEN passwords, sprinkles on hash and salt

Zuck's ad empire DOESN'T see details in plain text. Phew!

9 Comments



Facebook and Twitter queen Taylor Swift: Facebook and Twitter are RUBBISH

Refuses even to Tweet or Facebook her opinion of them

38 Comments



Small change to Medium takes large axe to passwords

'This login will self-destruct in 15 minutes'

6 Comments

Whitepapers



Governance takes a central role as enterprises shift to mobile

The findings in this report are the result of an Forrester Consulting survey commissioned by Druva to evaluate governance and eDiscovery amid enterprise companies.



2015 Cost of data breach study

Ponemon Institute's latest study of 350 organizations around the globe details both the cost and impact of data breaches, with breakdowns by industry and country.



Five fundamentals of virtual server protection

Outlining the top 5 challenges to overcome in order to take advantage of the benefits of virtualisation for your organisation.



The rising value, and falling cost, of desktop virtualisation

When vendors compete, desktop virtualization customers win. Moore's Law and market forces lead to better solutions at a lower cost.

Global spy system ECHELON confirmed at last – by leaked Snowden files



Telstra's bush broadband boxes bugged, bashed, bottled

HONG KONG

YOU BELONG HERE.
Book now from
\$49/night.

airbnb

Sponsored links

[Sign up to The Register to receive newsletters and alerts](#)

Good Idea? Bad Idea?

STOP THE DEBATES.
MAKE DECISIONS WITH CONFIDENCE.
TEST & LEARN™

APT
Test & Learn®

CLICK HERE
to Read Our Case Studies

The Register

Biting the hand that feeds IT © 1998–2015

Independent news, views, opinions and reviews on the latest in the IT industry. Offices in London, Edinburgh, San Francisco and Sydney.

About us

[Privacy](#)
[Company info](#)
[Advertise with us](#)
[Syndication](#)
[Send us news tips](#)

More content

[Newsletters](#)
[Top 20 stories](#)
[Week's headlines](#)
[Archive](#)
[eBooks](#)
[Webcasts](#)

Follow us