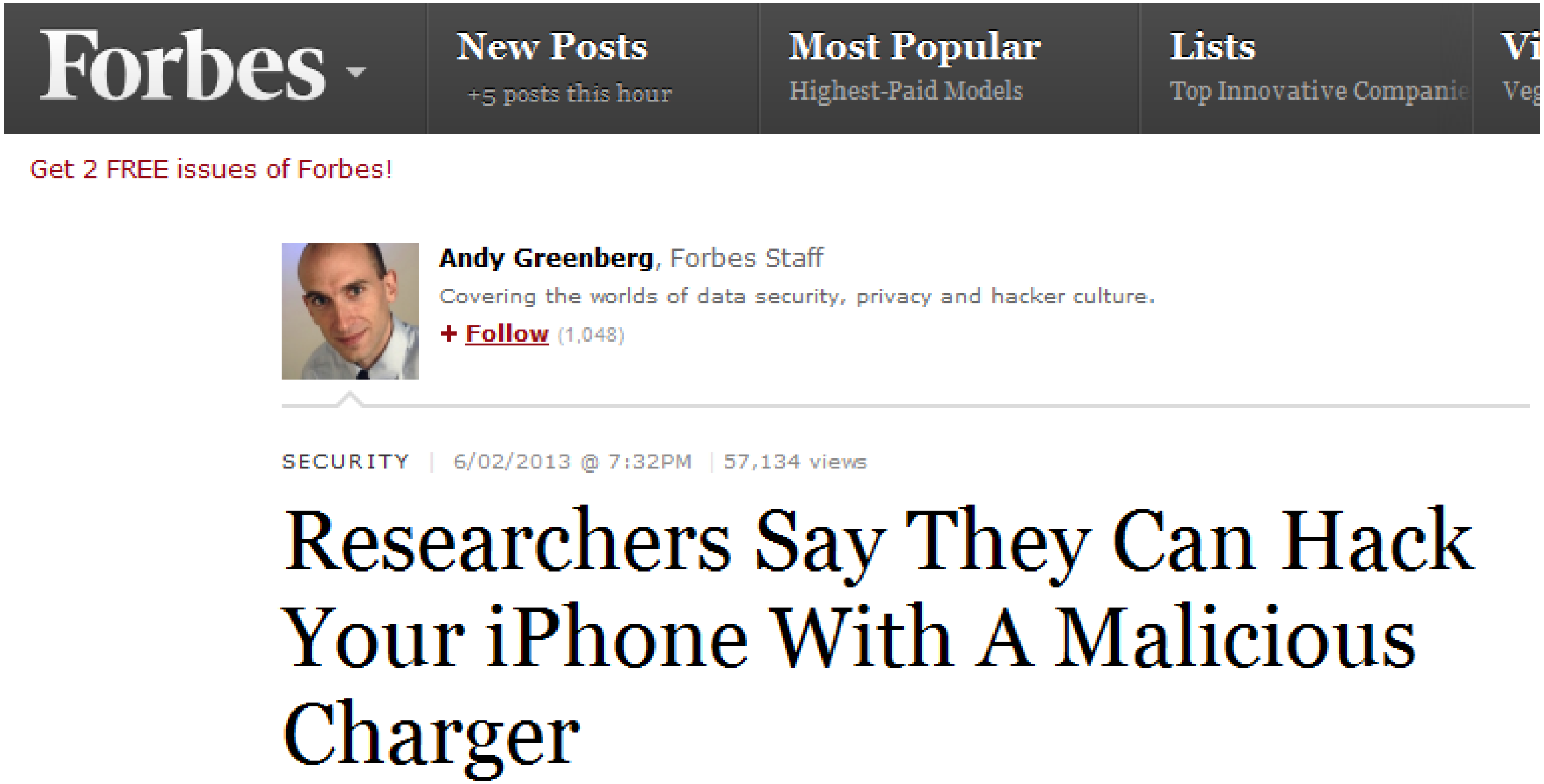
CS 858 – Mobile Privacy and Security (MoPS)

Fall 2013

Introduction

WATERLOO
CHERITON SCHOOL OF
COMPUTER SCIENCE

CrySP

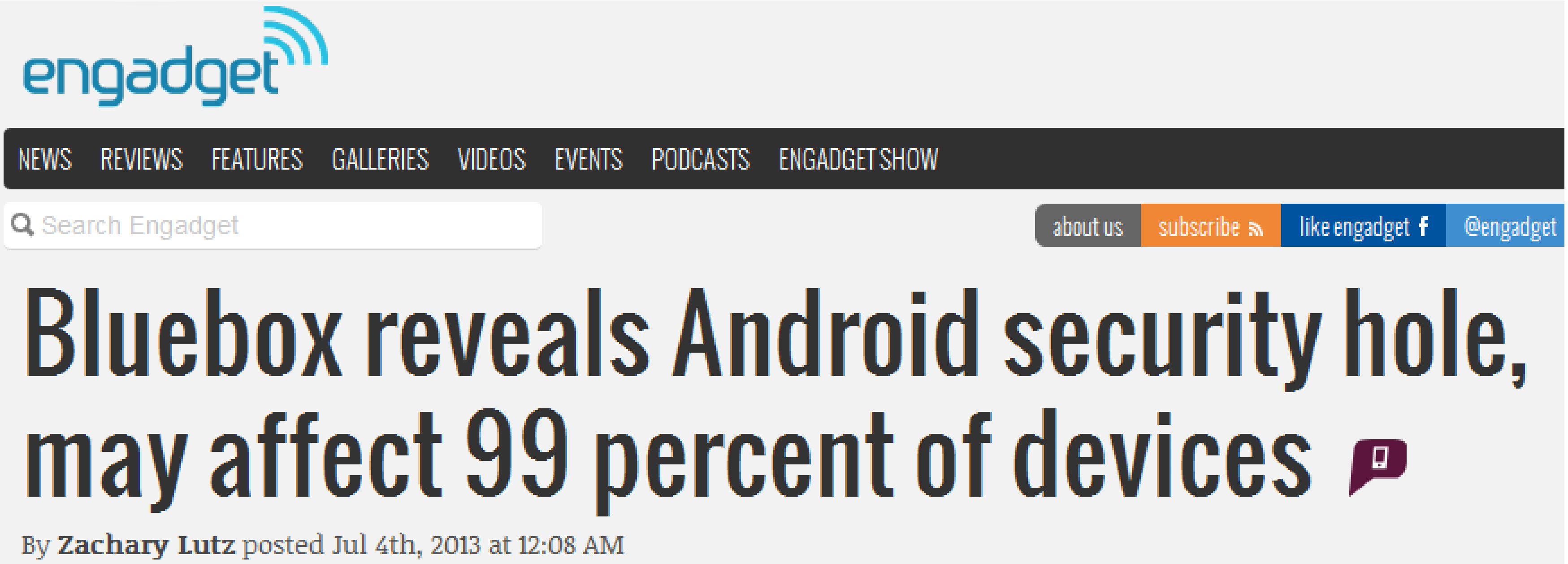


Andy Greenberg, Forbes Staff

Covering the worlds of data security, privacy and hacker culture.

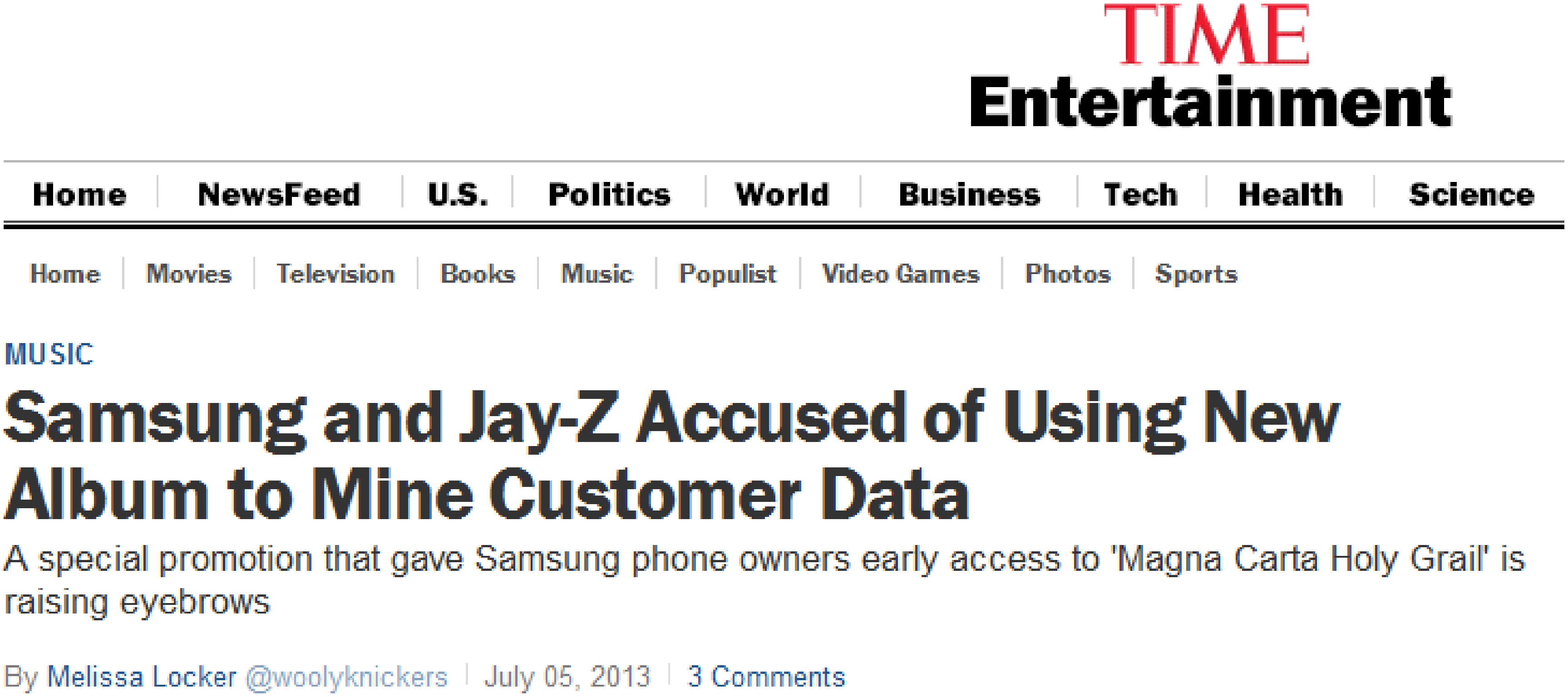
SECURITY | 6/02/2013 @ 7:32PM | 57,134 views

Researchers Say They Can Hack Your iPhone With A Malicious Charger



Bluebox reveals Android security hole, may affect 99 percent of devices

By **Zachary Lutz** posted Jul 4th, 2013 at 12:08 AM



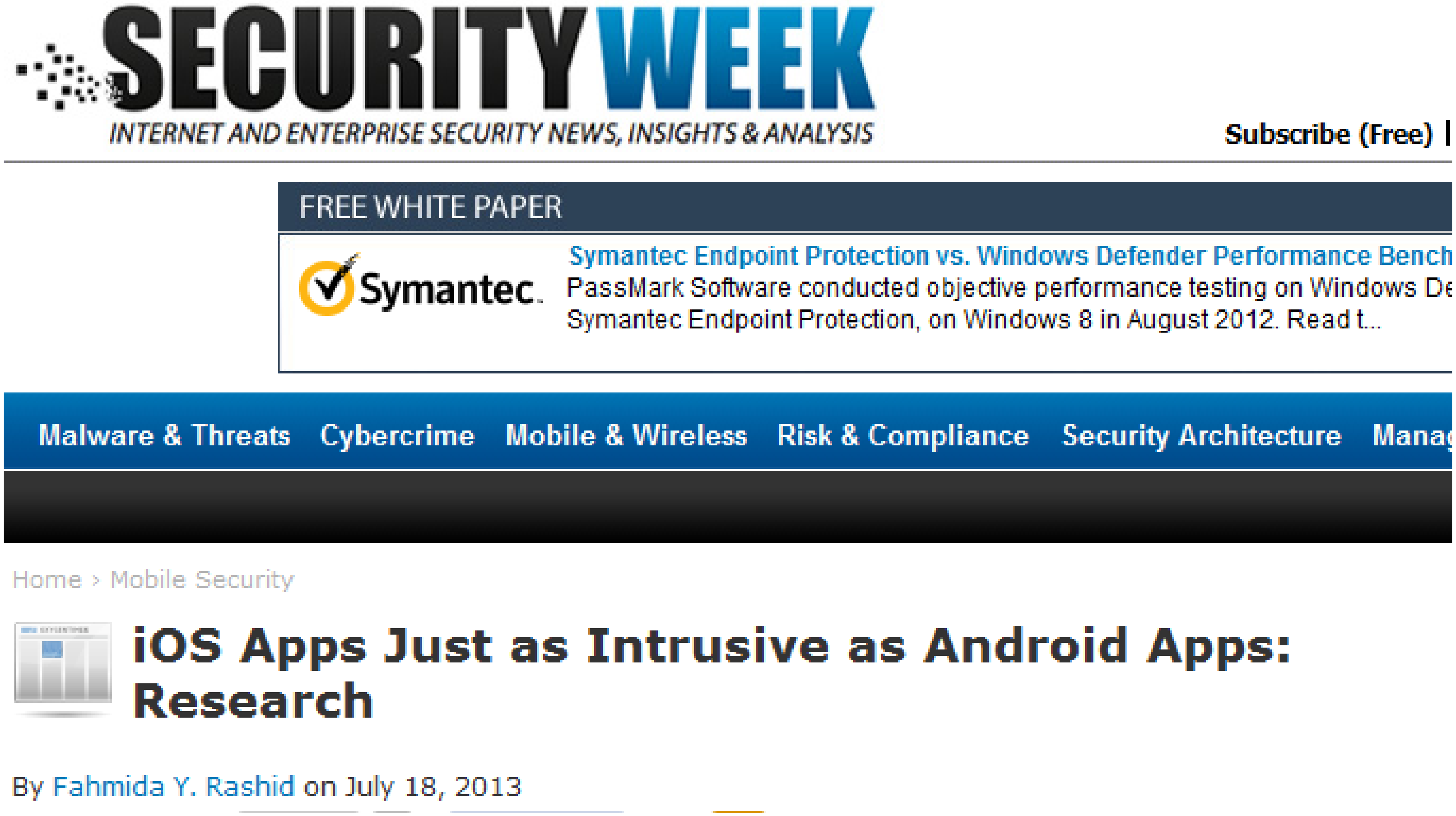
TIME
Entertainment
Home | NewsFeed | U.S. | Politics | World | Business | Tech | Health | Science
Home | Movies | Television | Books | Music | Populist | Video Games | Photos | Sports

MUSIC

Samsung and Jay-Z Accused of Using New Album to Mine Customer Data

A special promotion that gave Samsung phone owners early access to 'Magna Carta Holy Grail' is raising eyebrows

By Melissa Locker @woolyknickers | July 05, 2013 | 3 Comments



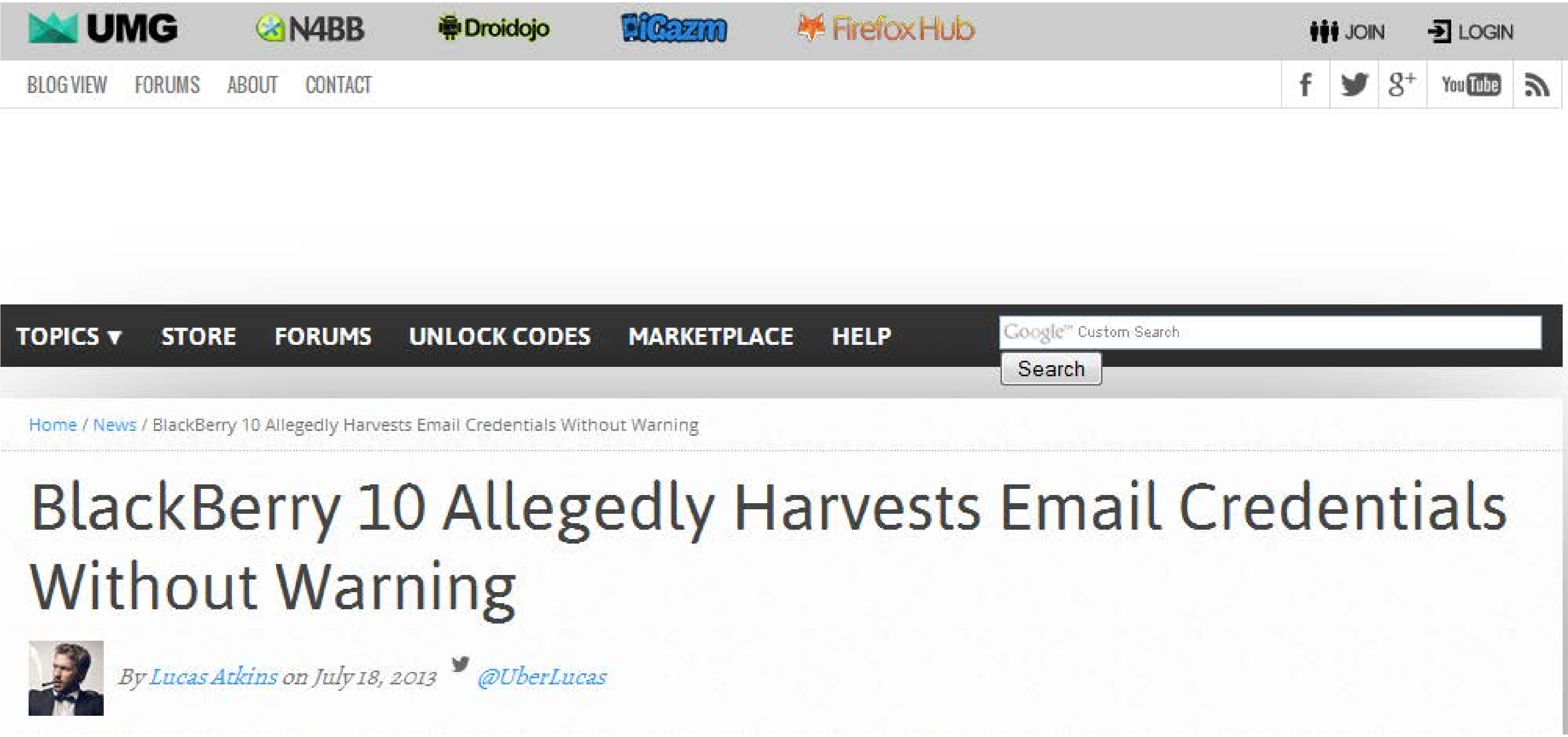
SECURITY WEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) |

iOS Apps Just as Intrusive as Android Apps: Research

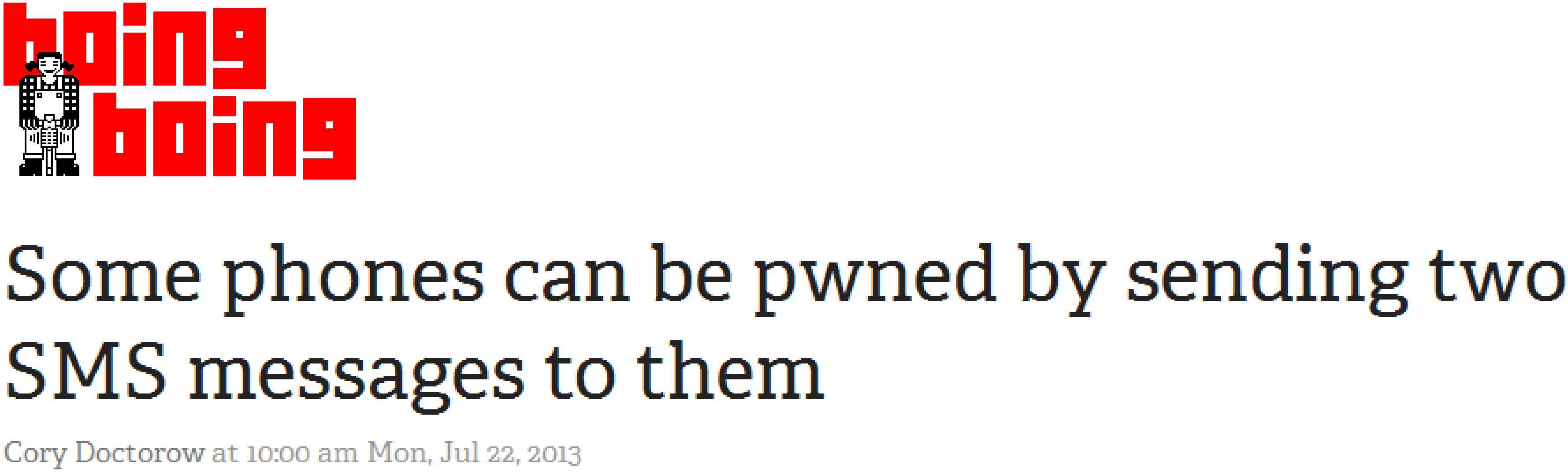
By Fahmida Y. Rashid on July 18, 2013



Home / News / BlackBerry 10 Allegedly Harvests Email Credentials Without Warning

BlackBerry 10 Allegedly Harvests Email Credentials Without Warning

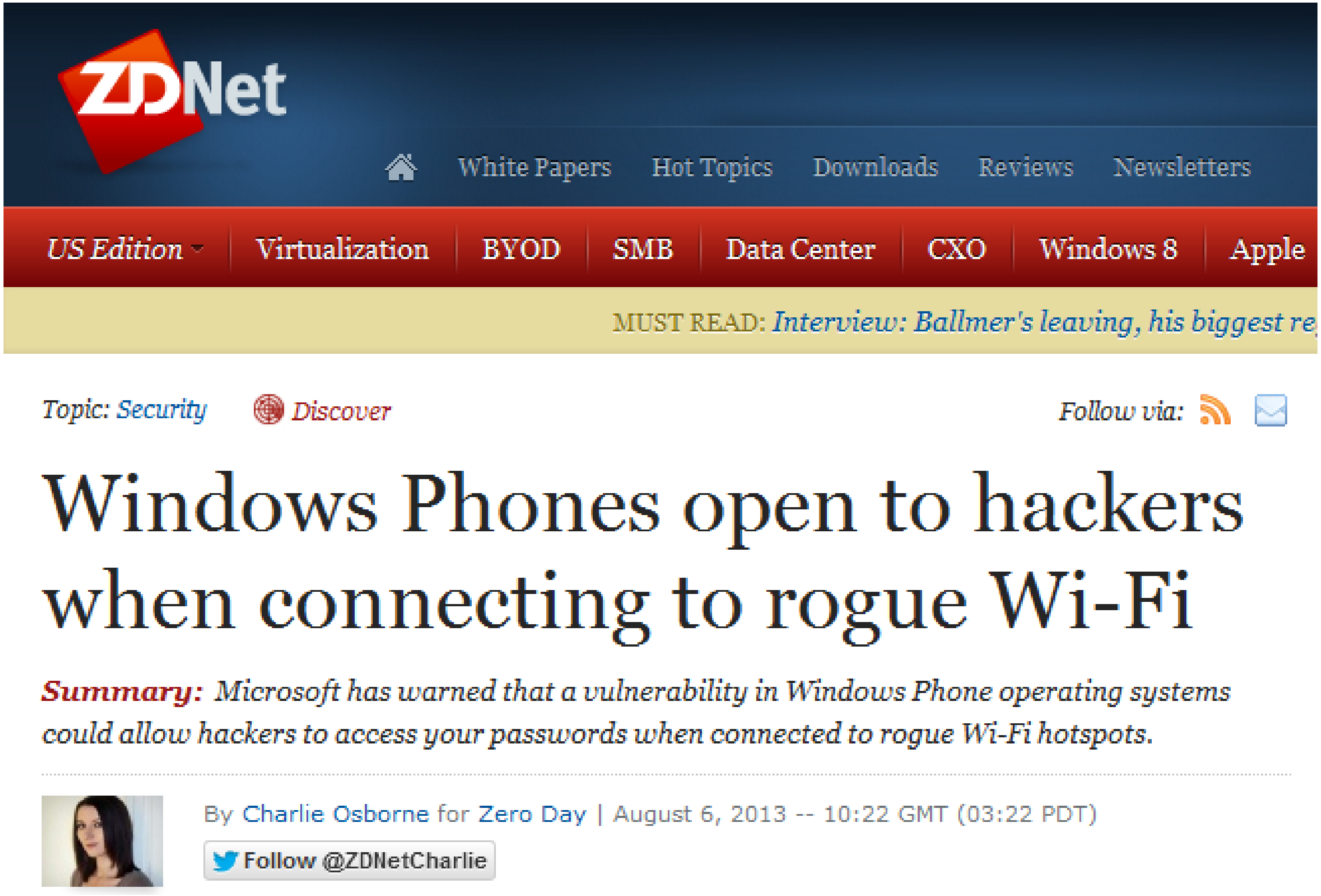
By Lucas Atkins on July 18, 2013 *@UberLucas*



boing boing

Some phones can be pwned by sending two SMS messages to them

Cory Doctorow at 10:00 am Mon, Jul 22, 2013

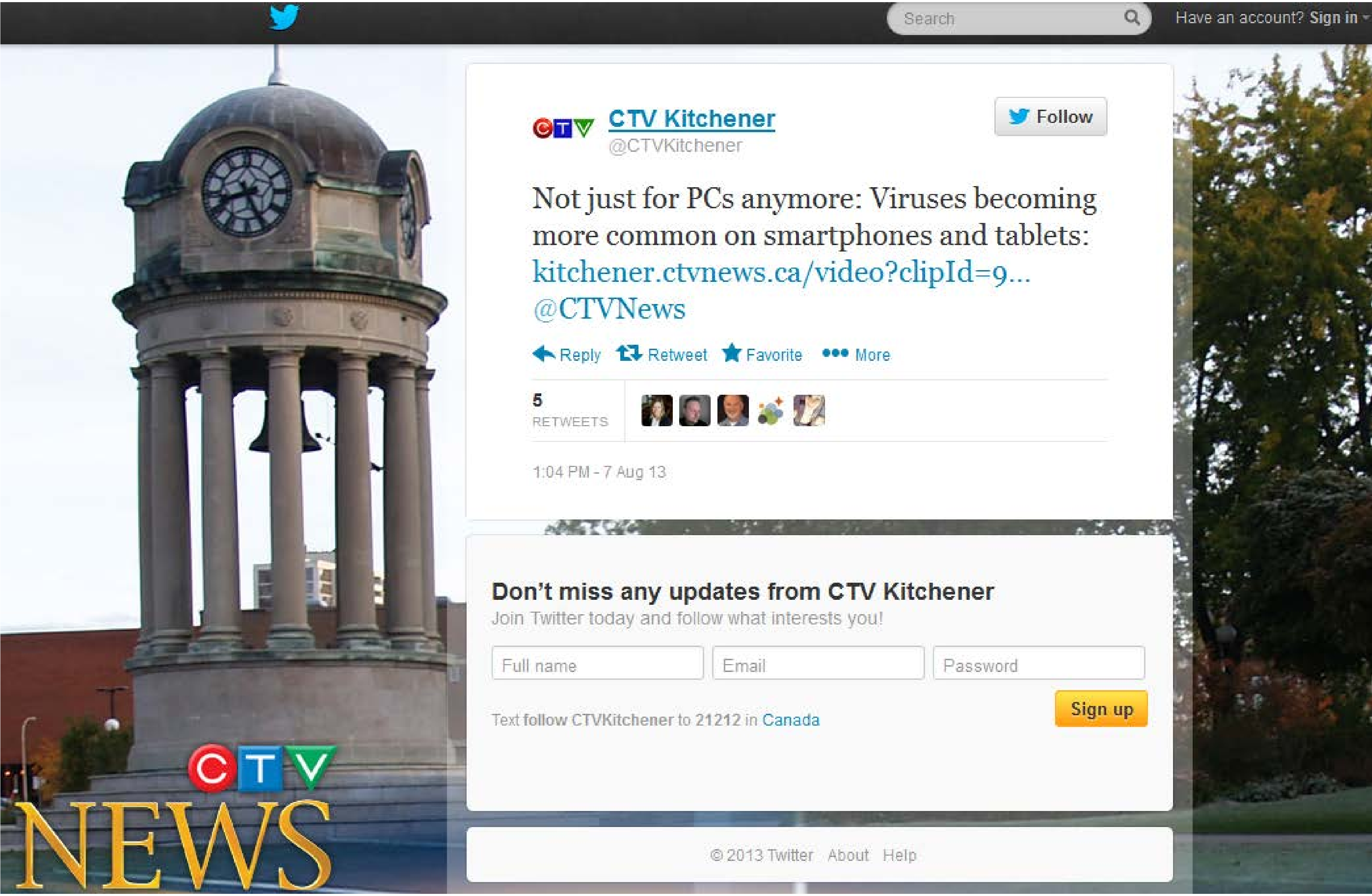


MUST READ: *Interview: Ballmer's leaving, his biggest re*

Windows Phones open to hackers when connecting to rogue Wi-Fi

Summary: *Microsoft has warned that a vulnerability in Windows Phone operating systems could allow hackers to access your passwords when connected to rogue Wi-Fi hotspots.*

By Charlie Osborne for Zero Day | August 6, 2013 -- 10:22 GMT (03:22 PDT)



CTV Kitchener
@CTVKitchener

Not just for PCs anymore: Viruses becoming more common on smartphones and tablets: kitchener.ctvnews.ca/video?clipId=9... @CTVNews

5 RETWEETS

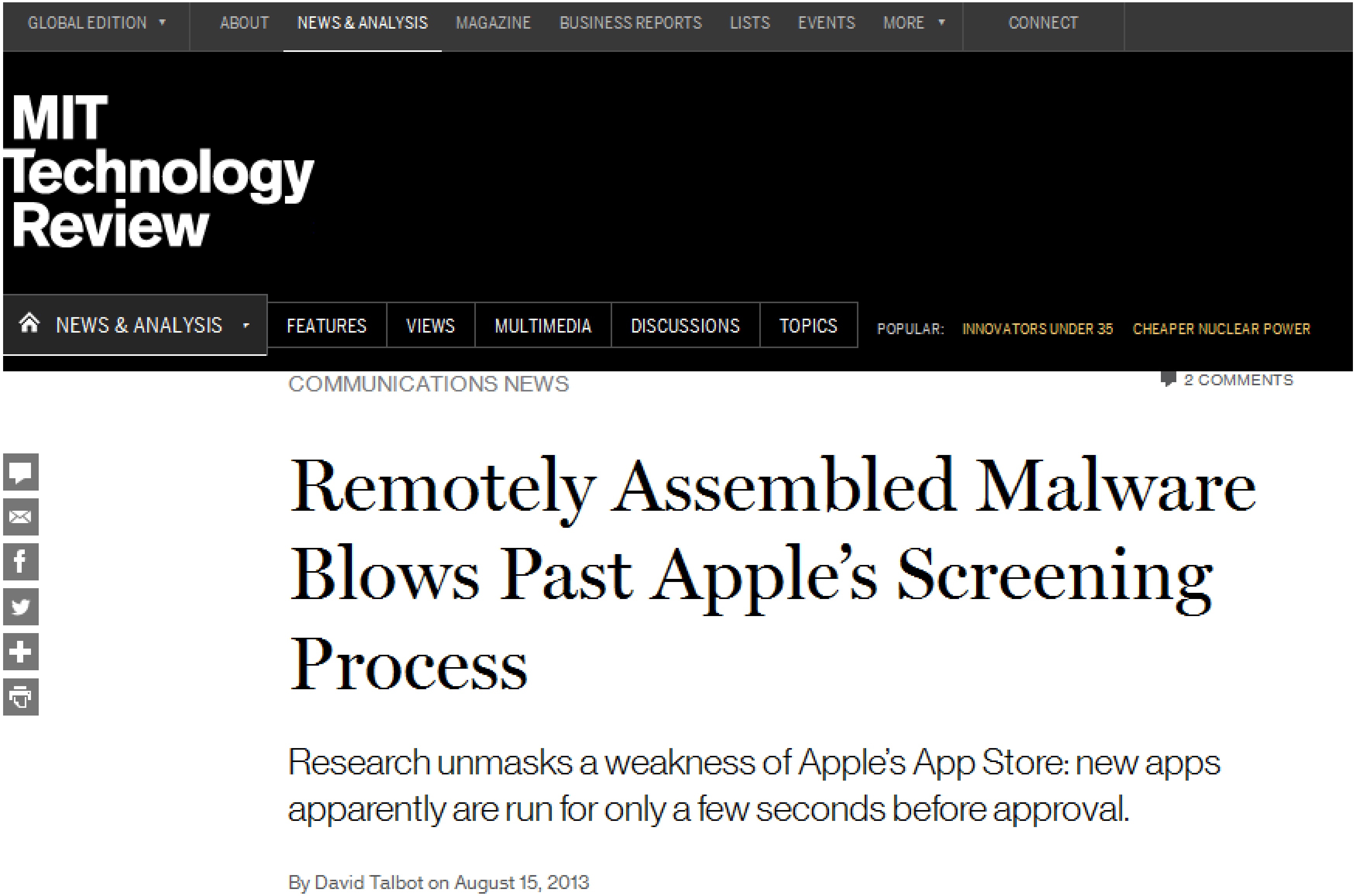
1:04 PM - 7 Aug 13

Don’t miss any updates from CTV Kitchener

Join Twitter today and follow what interests you!

Text follow CTVKitchener to 21212 in Canada

© 2013 Twitter About Help

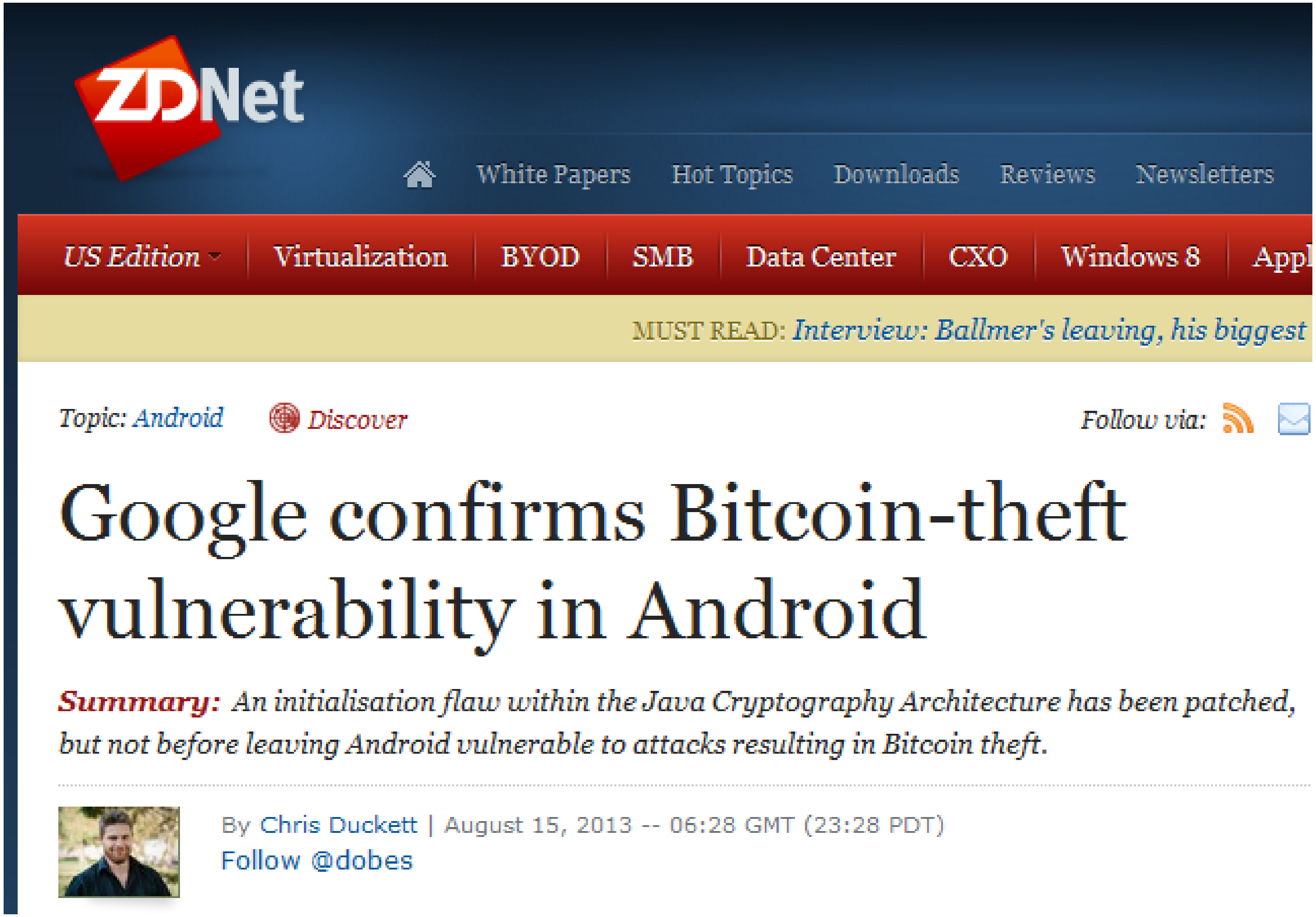


COMMUNICATIONS NEWS

Remotely Assembled Malware Blows Past Apple's Screening Process

Research unmasks a weakness of Apple's App Store: new apps apparently are run for only a few seconds before approval.

By David Talbot on August 15, 2013



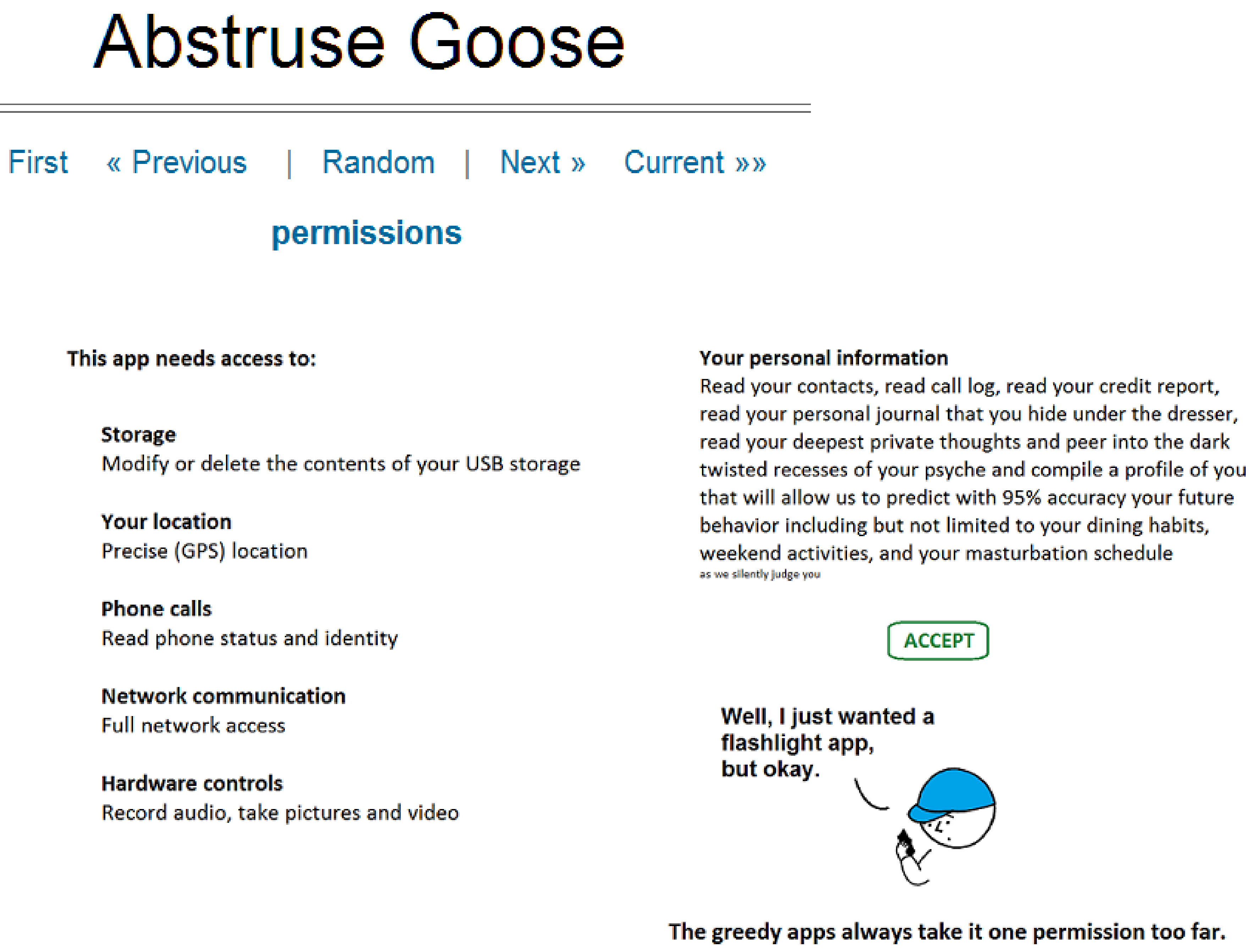
MUST READ: *Interview: Ballmer's leaving, his biggest*

Topic: Android

Google confirms Bitcoin-theft vulnerability in Android

Summary: *An initialisation flaw within the Java Cryptography Architecture has been patched, but not before leaving Android vulnerable to attacks resulting in Bitcoin theft.*

By Chris Duckett | August 15, 2013 -- 06:28 GMT (23:28 PDT)
Follow @dobes



Abstruse Goose

First « Previous | Random | Next » Current »»

permissions

This app needs access to:

Storage
Modify or delete the contents of your USB storage

Your location
Precise (GPS) location

Phone calls
Read phone status and identity

Network communication
Full network access

Hardware controls
Record audio, take pictures and video

Your personal information
Read your contacts, read call log, read your credit report, read your personal journal that you hide under the dresser, read your deepest private thoughts and peer into the dark twisted recesses of your psyche and compile a profile of you that will allow us to predict with 95% accuracy your future behavior including but not limited to your dining habits, weekend activities, and your masturbation schedule
as we silently judge you

ACCEPT

The greedy apps always take it one permission too far.

Overview

Goals

Organization

Survey of Topics

Goals

Becoming familiar with current research problems in mobile privacy and security

Studying some proposed solutions

Developing new solutions in course project

Learning to read and review papers

Learning to give good presentations

Organization

Goals

Organization

Survey of Topics

Meetings

Time: Tuesdays and Thursdays 10:00-11:20am

Location: DC 2568

Office hour: Mondays 3-4pm or by appointment

Prerequisites

No formal prerequisites

No familiarity with security or cryptography required

Basic knowledge of computer systems and networks helpful

Wide range of papers (applied cryptography, economics, human computer interaction, machine learning, networking, programming languages, systems)

Course Website

Reachable from my own website

Has reading list, schedule, policies,...

Keep track of announcements posted there

Lectures

First four lectures:

Given by me and my postdoc Bisheng Liu

Introduction, advice on giving presentations, sample research projects, Android Security

Following lectures:

Two students will each present and lead a discussion on a research paper

Course project presentations at the very end

Grading

Paper presentations:	25%
Paper reviews:	20%
Class participation:	15%
Includes presentation feedback	
Research project :	40%

Paper Reviews

Goal: learn what makes a good paper
So that you can write your own good papers ☺

Every student should read the two mandatory papers before each lecture

See Keshav's How to Read a Paper

Every student should submit a review for one of the two papers before class

Using submission system, see later

You will see each others' (anonymized) reviews

Paper Presentations

Goal: practice your presentation skills

Every student should present two research papers during the term

Workshop/conference-style presentation

Present the paper as it is your own

You can re-use figures and animations (with attribution)

Carefully prepare your slides (Advice on Thursday)

About 25 minutes

Send me your slides before the lecture

Paper Discussion (Past Terms)

After each paper presentation, the presenter leads a discussion about the presented paper

Possible starting points for discussion:

- Presenter gives his/her opinion about the presented paper
- Presenter comes up with interesting questions (and possible answers to stimulate discussion if necessary)

About 15 minutes

Paper Discussion (This Term?)

There are several lectures where a joint discussion would make sense; for example, when both papers solve the same or a similar problem

Possible outline: Student A compares “his/her” paper to student B’s and argues why “his/hers” is better; followed by student B in the opposite role; followed by a joint discussion

It is up to you to decide what kind of discussion to have; talk to your co-presenter! We’ll revisit this issue after the first round of presentations is over

Presentation Feedback

Feedback is essential for training speaking skills

Every student should submit a review for each presentation by 12pm the day after a presentation
Using submission system, see later

Look at review form in system before preparing your presentation

Presenter will see (anonymized) feedback

HotCRP

We will use HotCRP, which is used by many CS workshops/conferences to manage the review of submitted papers

Three different instantiations of HotCRP, reachable from course website

1) Bidding for papers to present
2) Submitting paper reviews
3) Submitting presentation reviews

Bidding for Papers

I will create an account in the bidding system by the end of today for all students registered in the course

Go to the bidding system and retrieve your password

Log in, click on “Review Preferences”, and bid for papers; instructions are in the system

The bidding deadline is Sept 15, 11:59pm; students who submit their bids late will likely not get any papers assigned

Students not Registered in the Course

If you are not (yet) registered in the course, but are interested in taking it, send me an email explaining your situation ASAP

I will then create an account in the bidding system for you so that you can also submit bids

Paper Assignments

On Sept 16, I will assign papers to

1. Registered students who submitted a bid
2. Some of the not registered students who submitted a bid; these will also get a permission number to register if necessary

The students in the second group will be determined based on available course capacity and maybe other factors

Course Project

Goal: novel research in the area of mobile privacy and security

Might lead to workshop/conference submission

Typically in groups of two

Proposal: Oct 13

Presentation: Nov 26 and 28 (tentative)

Write-up: Dec 15 (tentative)

See course website for details

Overview

Goals

Organization

Survey of Topics

Survey of Topics

List of topics corresponds to topics on reading list

Examing Permissions:

Are there dangerous combinations of permissions, potentially used by malware?

Do apps actually use all the permissions that they ask for or are they overprivileged?

Survey of Topics (cont.)

Detecting Privacy Violations:

Tracing sensitive information from its source (e.g., GPS sensor) to its sink (e.g., network) using dynamic (Taintdroid) or static (PiOS) analysis

Managing Privacy Violations:

Avoid privacy leaks by replacing sensitive information with fake information or by blocking it, or by making access control more fine grained

Alert user of privacy leaks

Survey of Topics (cont.)

Studying Users and Permissions:

Do users pay attention to and understand permission screens?

Are there better ways to ask for permission?

Crowdsourcing Permission Expectations:

Can we use the crowd to provide useful information about required permissions to a user?

Survey of Topics (cont.)

Privilege Escalation:

How to avoid the “confused-deputy attack”, where a malicious, underprivileged app takes advantage of a benign, more privileged app

Advertising:

Advertising infrastructures that do not require each advertisement-supported ad to have all kinds of permissions (see flashlight example)

Survey of Topics (cont.)

Control-flow attacks:

Attacks and defenses against attacks that change the control flow of a program

Side-channel and Covert-channel Attacks:

Use the accelerometer to infer key presses

Use the microphone to retrieve credit card number and transfer it surreptitiously to attacker

Survey of Topics (cont.)

Device Theft:

How to prevent information stored on smartphone from becoming accessible to a thief stealing the phone

New Architectures:

Using smartphones to run virtual machines (Cells), sandbox cloud-based apps (пBox), build privacy-preserving location-based apps (Koi), or execute sophisticated cryptography (Opaak)

Survey of Topics (cont.)

Studying Users:

Is the All-Or-Nothing locking model sufficient?

Are users willing to pay more for less privacy-invasive apps?

Authentication:

Can we authenticate users based on their behaviour or biometrics?

Survey of Topics (cont.)

Privacy-preserving Data Processing:

How to release and learn from sensed data without revealing (all) this data

SSL:

How SSL is broken on smartphones and how to fix it

Survey of Topics (cont.)

Location Sharing:

Establish sharing preferences in a location-sharing app using machine learning or default privacy profiles