

**Katitza Rodríguez**  
International Rights Director  
Electronic Frontier Foundation  
@txitua ~ [katitza@eff.org](mailto:katitza@eff.org)



# ¿Qué es EFF?

LITIGATION • TECHNOLOGY • ACTIVISM



# EFF25

MEMBER SUPPORTED SINCE 1990: [EFF.ORG/EFF25](http://EFF.ORG/EFF25)



ELECTRONIC FRONTIER FOUNDATION [eff.org](http://eff.org)

Colombia, Agosto, 2015

# Scriptkitty Dreams

Electronic Frontier Foundation



VOL83UGJ2RUDKGDJDPWZL8RUD7S2I VAD  
D3KJNJ2NW2AP9LKM7L07GRCZJ2NW2APRUD  
M70E5V7S2FVADKND3DYBH48VHDHNVDA4GD  
UVT2APE83UC0D3J1S0SP33CHDPW28RUDKJ  
GRCZJ2NW2AP9LKM70E5V7S2FVADKND3DYB  
HDHNVDA4GDJMNDUV0E83UGJG04J17W96RU  
L07GRCZJ2RUDKAP9LKM70E5V7S2FVADKND  
H48VHDHNVDA4GDJMNDUV0E83UGJG07DPW2







# PROBLEMS WITH VOTING MACHINES

## SHARE



SHARE  
28



TWEET



PIN



COMMENT  
0

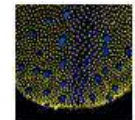


EMAIL



A SECURITY RESEARCHER in India has been arrested after he refused to provide authorities with the name of a person who supplied him with an electronic voting machine that was

## LATEST NEWS



BIOLOGY  
Sucking on M...  
to Understan...  
Buds Work  
1 HOUR



AUTONOMOUS  
Oddly Addicti...  
Shows That Y...  
Driving  
2 HOURS

MORE NEWS



## AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

Miller, one of the two researchers who developed the Uconnect-hacking technique, said he was happy to see the company respond. “I was surprised they hadn’t before and I’m glad they did,” he told WIRED in a phone call. He particularly praised the move to work with Sprint to prevent attacks through its network.

“Blocking the Sprint network is a huge thing,” Miller adds. “The biggest problem before was that cars would never get fixed or fixed way down the road. Assuming that they did [the Sprint network fix] correctly...you don’t have to worry about that tail-end of cars that won’t get fixed.”





MAIN MENU MY STORIES: 25 FORUMS SUBSCRIBE JOBS ARS CONSORTIUM

RISK ASSESSMENT / SECURITY & HACKTIVISM

Fiat Chrysler recalls 1.4 million cars over remote hack vulnerability

Uconnect bug can shut down engine and brakes, take over steering.

PATCH YOUR CHRYSLER NOW AGAINST A WIRELESS HACKING ATTACK



Forbes

New Posts Most Popular Lists Video 10 Stocks to Buy Now

Sell us your Honda

Top prices for your used Honda. Fast, fair & free market appraisal.



SECURITY 7/21/2015 @ 9:24AM | 23,826 views

Jeep Owners Urged To Update Cars To Stop Hackers Taking Them Off The Road

Thomas Fox-Brewster Forbes Staff



TRENDING NOW

How to upgrade to Windows 10 without waiting in line

TECH SCIENCE ENTERTAINMENT CARS DESIGN US & WORLD FORUMS

NEXT STORY

One of the PlayStation 2's best-looking games is getting an HD remake

CULTURE TRANSPORTATION WEB EDITORIAL

The scariest thing about the Chrysler hack is how hard it was to patch

By Russell Brandom on July 24, 2015 03:01 pm Email @russellbrandom



# Judge orders halt to Defcon speech on subway card hacking

Federal judge grants the state of Massachusetts' request to prevent three MIT students from giving a presentation about hacking smartcards used in the Boston subway system.

MIT Students Get Top Marks for Hacking Boston Subway

CHARLIE SORREL GEAR 08.20.08 4:04 AM

## MIT STUDENTS GET TOP MARKS FOR HACKING BOSTON SUBWAY



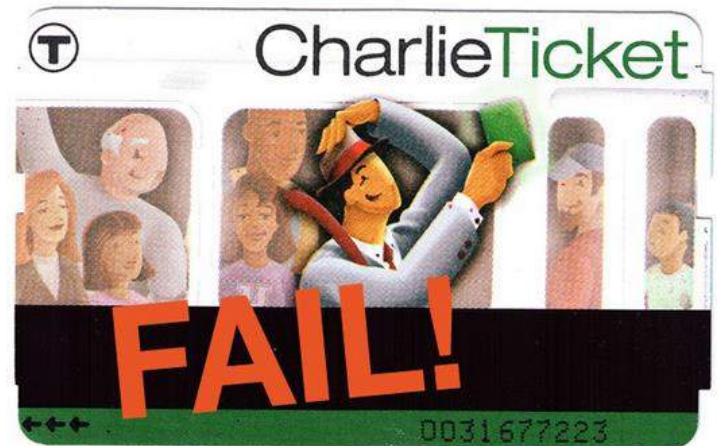
Search

Home

[HOME](#) » [CRIME](#) » MIT KIDS: PLEASE COME HACK US!

### MIT Kids: Please come hack us!

Posted on August 11th, 2008 by The SUBWAYblogger in Crime, Transit Failures

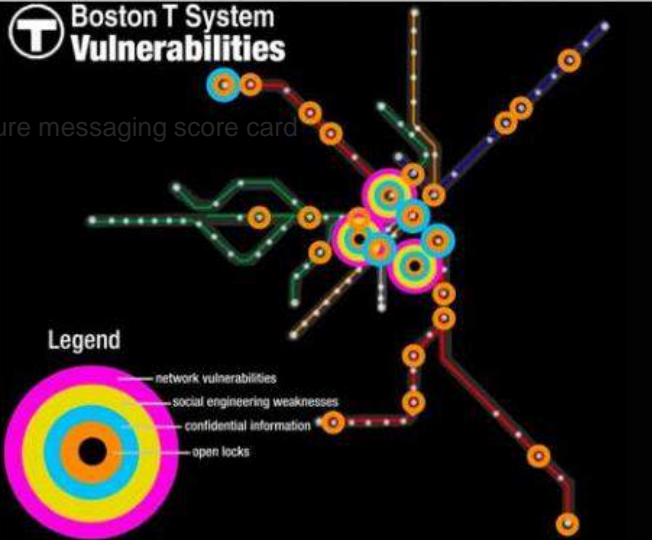






### T Boston T System Vulnerabilities

secure messaging score card



### MBTA Suit Against MIT Charlie Card Hackers May Perpetuate Vulnerabilities

15 August 2008 - 5:22pm | Jesse K-S

## MIT Subway Hack Paper Published on the Web

BY [CHLOE ALBANESIUS](#) AUGUST 12, 2008 11:47AM EST 0 COMMENTS

*Massachusetts transit officials were skeptical that three MIT students were providing them with their complete presentation prior to Defcon, but an analysis by a security consultant said that the conference presentation alone was not enough to help someone hack the Boston subway system.*

## MIT Students Who Hacked Boston Subway Silenced; Report Gets Out Anyway

By Andrew Moseman | August 11, 2008 1:36 pm



A group of eleven professional security researchers have written a letter to Judge George O'Toole, the judge overseeing the case, asking that the temporary restraining order be removed. They wrote that "Preventing researchers from discussing a technology's vulnerabilities does not make them go away - in fact, it may exacerbate them as more people and institutions use and come to rely upon the illusory protection. Yet the commercial purveyors of such technologies often do not want truthful discussions of their products' flaws, and will likely withhold the prior approval or deny researchers access for testing if the law supports that effort." They provide as examples of responsible hacking, cases in which security researchers discovered vulnerabilities in encryption used by banking systems, and one in which a plot to attack the White House's web server was revealed by reverse engineering. In each of these cases, security researchers provided evidence that helped eliminate vulnerabilities in systems the public uses.



# Watch the ATM Hacker At Work

See hacker Barnaby Jack, who died last week, trick an ATM into spewing out all its cash





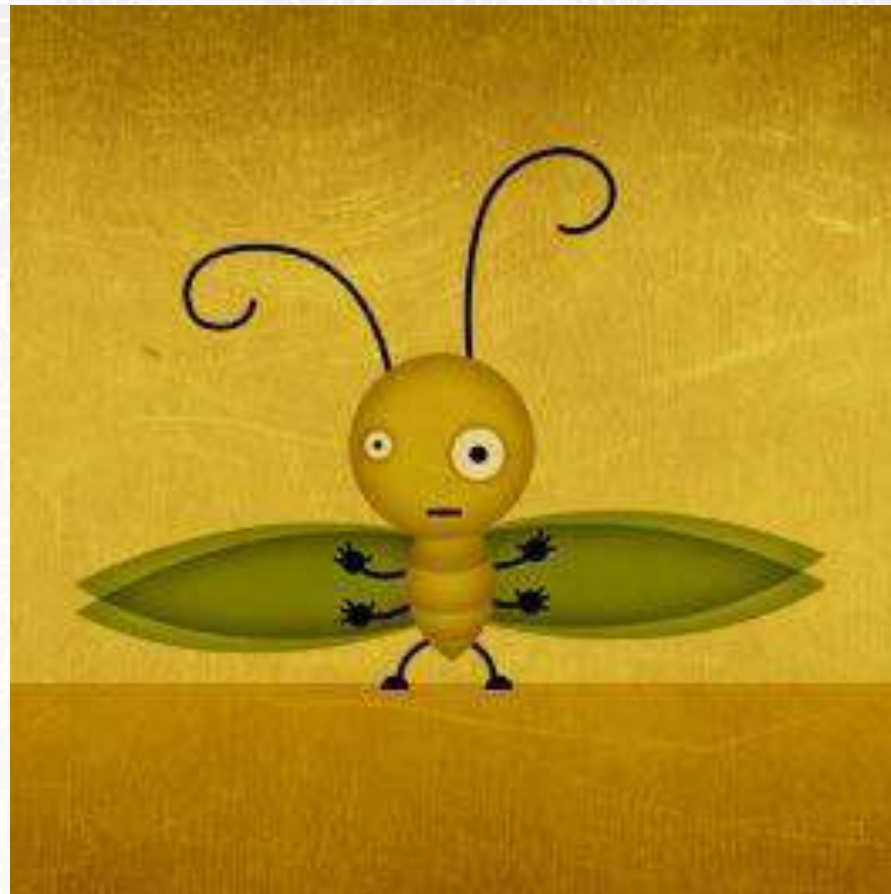
# **I. Invertir en investigación y herramientas de seguridad: Más cifrado punto a punto**





# La inseguridad en Tecnología

## *It's a bug, not a feature*





TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

# Why are we interested in HTTP?

facebook

YAHOO!

twitter

myspace.com  
a place for friends

Because nearly everything a typical user does on the Internet uses HTTP

CNN.com

Google  
Earth

@mail.ru



Gmail





## Official Gmail Blog

News, tips and tricks from Google's Gmail team and friends.

### Default https access for Gmail

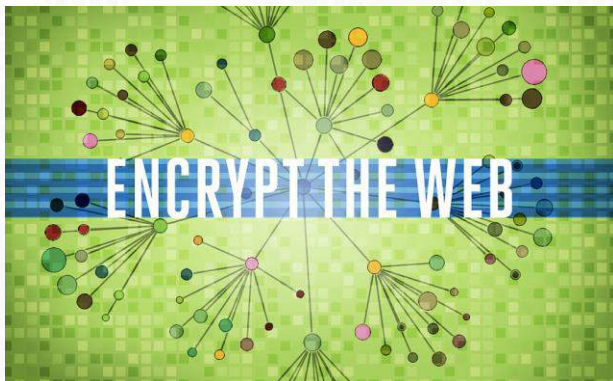


# HTTPS EVERYWHERE

<https://www.eff.org/https-everywhere>

## Facebook Adopts Secure Web Pages By Default

Facebook has finally started using HTTPS by default, following a 2010 FTC demand and in the distant footsteps of Google, Twitter, and Hotmail.



YAHOO!

2014

January February March April  
 May June July August  
 September October November December

YAHOO!

Yahoo ID  
 Password  
 Keep me signed in  
 Sign In

I can't access my account  
 Help

Google

**LAST TO THE PARTY, YAHOO TURNS ON SSL BY DEFAULT**





# Top messaging apps flat-out flunk EFF's security review

Lucian Constantin

IDG News Service

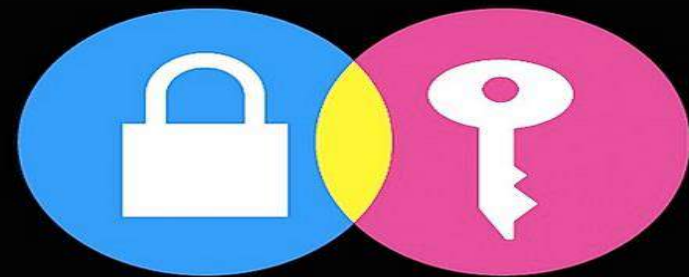
Nov 5, 2014 5:45 AM | |

Some of the most widely used messaging apps in the world, including Google Hangouts, Facebook chat, Yahoo Messenger, and Snapchat, flunked a best-practices security test by advocacy group the Electronic Frontier Foundation (EFF).




































## EFF ranks Apple's iMessage, FaceTime "best mass market options" for secure messaging, ahead of BlackBerry Messenger, Google Hangouts, Facebook, Microsoft Skype

By Daniel Eran Dilger  
Wednesday, November 05, 2014, 11:20 am PT (02:20 pm ET)

In its ranking of electronic messaging systems for safety and security, the Electronic Frontier Foundation said no mainstream products passed all of its criteria, but that Apple's iMessage and FaceTime "stood out as the best of the mass-market options."



**SECURE MESSAGING SCORECARD**

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
Facebook chat							
Google Hangouts/Chat "off the record"							
iMessage							
Jitsi + Ostel							
Off-The-Record Messaging for Mac (Adium)							



# **II. Remover las barreras legales para la investigación en seguridad la información**





**III. Crear incentivos para los investigadores**

**IV. Mantener concursos para los programadores que reportan vulnerabilidades**



NEWS

# Google lays \$2.7M on the line for Pwnium hacking contest

After last year's semi-washout, will again try to draw out exploits of Chrome OS at March security conference

**MORE LIKE THIS**

Pwn2Own hack contest puts record \$645K on prize table

## Facebook awards \$50,000 Internet Defense Prize for security research



21/08/2014

By Barclay Ballard, CONTRIBUTOR

SECURITY NEWS

## The new bounty hunters chasing the Internet's 'most wanted'

Kryisia Lenzo | @KryisiaLenzo

Sunday, 26 Jul 2015 | 1:00 PM ET





# Internet Bug Bounty plans rewards for new tools to find vulnerabilities

Jeremy Kirk

IDG News Service

Apr 15, 2015 6:55 AM



A program that pays researchers for information on software vulnerabilities, the [Internet Bug Bounty \(IBB\)](#), will now also reward those who develop tools and techniques to spot bugs.

The idea is to expand the range of tools organizations can use to find security flaws in their software before hackers do and sell that valuable information, wrote Katie Moussouris, chief policy officer for HackerOne, one of IBB's sponsors, along with Facebook and Microsoft.

"In the end, the tug of war between attackers and defenders will always exist," Moussouris wrote in a [blog post](#) Tuesday. "How we structure incentives toward making offense more expensive for attackers and giving more defenders and advantage is the question."





## Internet Bug Bounty

How it works

The Panel

Software

Bounty sponsors

FAQ

### The Panel

The Internet Bug Bounty is managed by a panel of volunteers selected from the security community. These security experts are responsible for defining the rules of the program, allocating bounties to where additional security research is needed most, and mediating any disagreements that might arise.

- [Alex Rice](#), HackerOne
- [Chris Evans](#), Google Project Zero
- [Katie Moussouris](#), HackerOne
- [Zane Lackey](#), Signal Sciences
- Jesse Burns, NCC Group
- [Collin Greene](#), Uber
- Matt Miller, Microsoft
- Roman Porter, Microsoft
- [Neal Poole](#), Facebook
- [Kostya Kortchinsky](#), Google
- [Peleus Uhley](#), Adobe

*Panelists represent their own opinions and not their employers.*



## Frequently Asked Questions

### **Why run an Internet Bug Bounty program?**

Our collective safety is only possible when public security research is allowed to flourish. Some of the most critical vulnerabilities in the internet's history have been resolved thanks to efforts of researchers fueled entirely by curiosity and altruism. We owe these individuals an enormous debt and believe it is our duty to do everything in our power to cultivate a safe, rewarding environment for past, present, and future researchers.

### **Who is running the Internet Bug Bounty?**

The Internet Bug Bounty is a California non-profit public benefit corporation. The program itself is administered by an independent panel of security experts from the community. The Panel is responsible for defining the rules of the program, allocating bounties to where additional security research is needed most, and mediating any disagreements that might arise.

### **How is the program funded?**

The Internet Bug Bounty program is sponsored by individuals and organizations who genuinely care about our collective security. Their contributions directly fund the bounties paid to researchers with no portion going to The Panel or administration: 100% goes to researchers. Sponsors do not have any special access or rights to bug data. If you'd like to sponsor security research, let us know!



# V. Crear Incentivos para Desarrollo de Software Seguro





# Capturan a funcionarios que vendían información de víctimas

Entre ellos está el actual personero de Chigorodó y un funcionario de la Alcaldía de Medellín.

Por: MEDELLÍN |

© 11:04 p.m. | 5 de agosto de 2014

# Día cero, talón de Aquiles para los sistemas informáticos

Los cibercriminales pueden usar esta falla en software para crear ataques más avanzados, más eficientes y difíciles de detectar



2/01/2015 01:46 Aura Hernández



COMPARTIR

## Hackers' top six database attacks:

- 1. Brute-force (or not) cracking of weak or default usernames/passwords
- 2. Privilege escalation
- 3. Exploiting unused and unnecessary database services and functionality
- 4. Targeting unpatched database vulnerabilities
- 5. SQL injection
- 6. Stolen backup (unencrypted) tapes



**¡Muchas gracias!**  
¿Preguntas?

[katitza@eff.org](mailto:katitza@eff.org) ~ @txitua