



La difesa è figlia dell'offesa: il ruolo della *offensive security research*

Prof. Stefano Zanero

Ricercatore di Ruolo, Dip. Elettronica e Informazione
Politecnico di Milano



- **Associate professor @ POLIMI**
- **IEEE Computer Society**
 - Board of Governors member
 - Cybersecurity STC chair
- **Information Systems Security Association**
 - International Director
- **Black Hat**
 - Review board member



POLITECNICO
MILANO 1863



ISSA
Information Systems Security Association





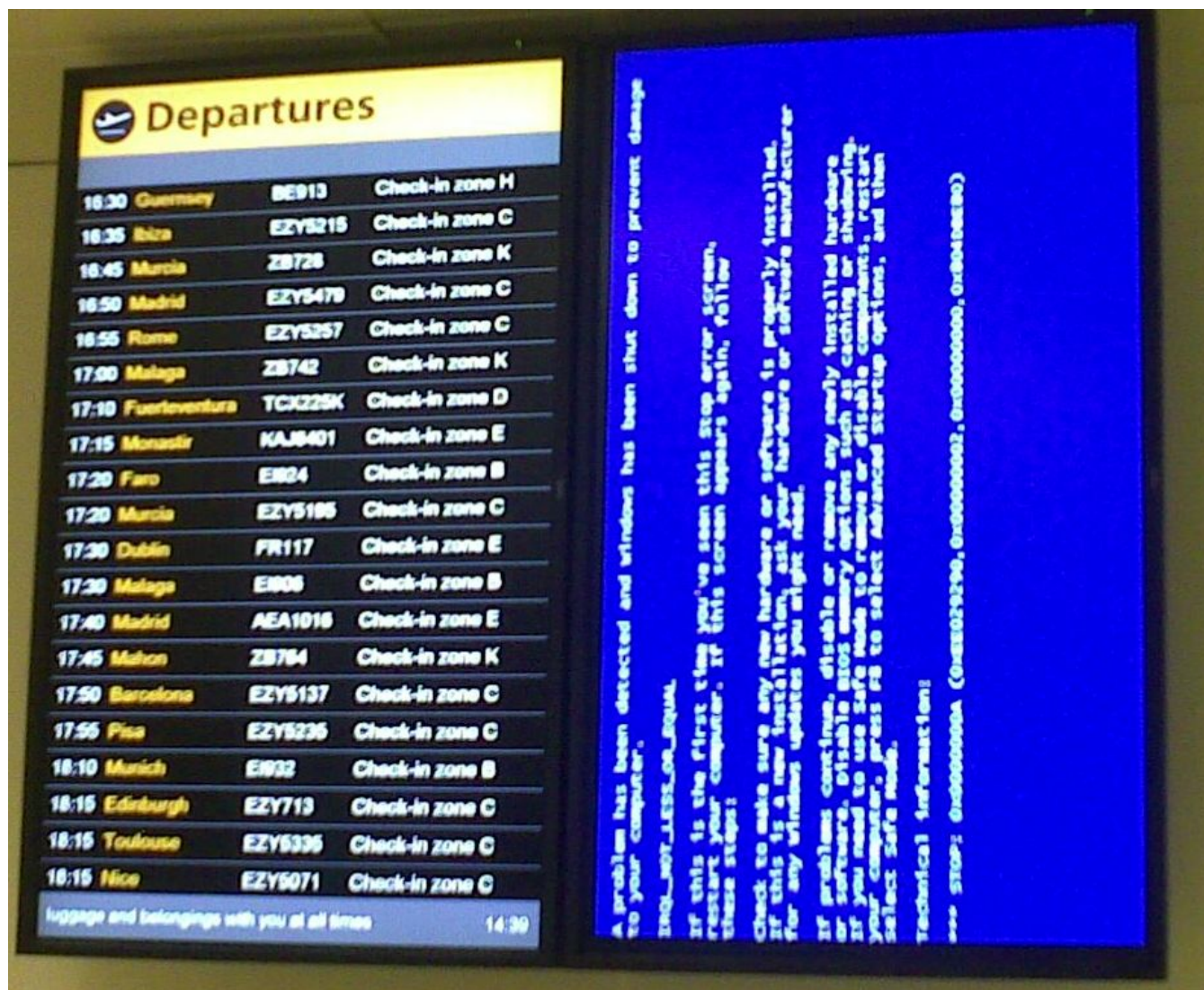
- Grandi trionfi dell'ingegneria
- Bancomat
- Montagne (americane)
- Montagne russe
- Cravatte e cappelli
- Insomma, parlerò di *offensive security* (chiaramente)







N.B. I fisici potrebbero sostenere di avere qualcosa a che vedere con l'LHC...







Grandi trionfi dell'ingegneria (molto grandi)

9





- **“A computer is secure if you can depend on it and its software to behave as you expect”**

Garfinkel and Spafford, “Practical UNIX and Internet Security”, 2nd Ed., O’Reilly & Associates, Inc., 1996

- **“Beware of bugs in the above code; I have only proved it correct, not tried it”**

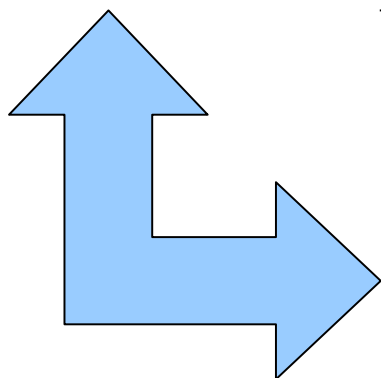
Donald Knuth, 1977











Photograph: Copyright Paul Shambrey

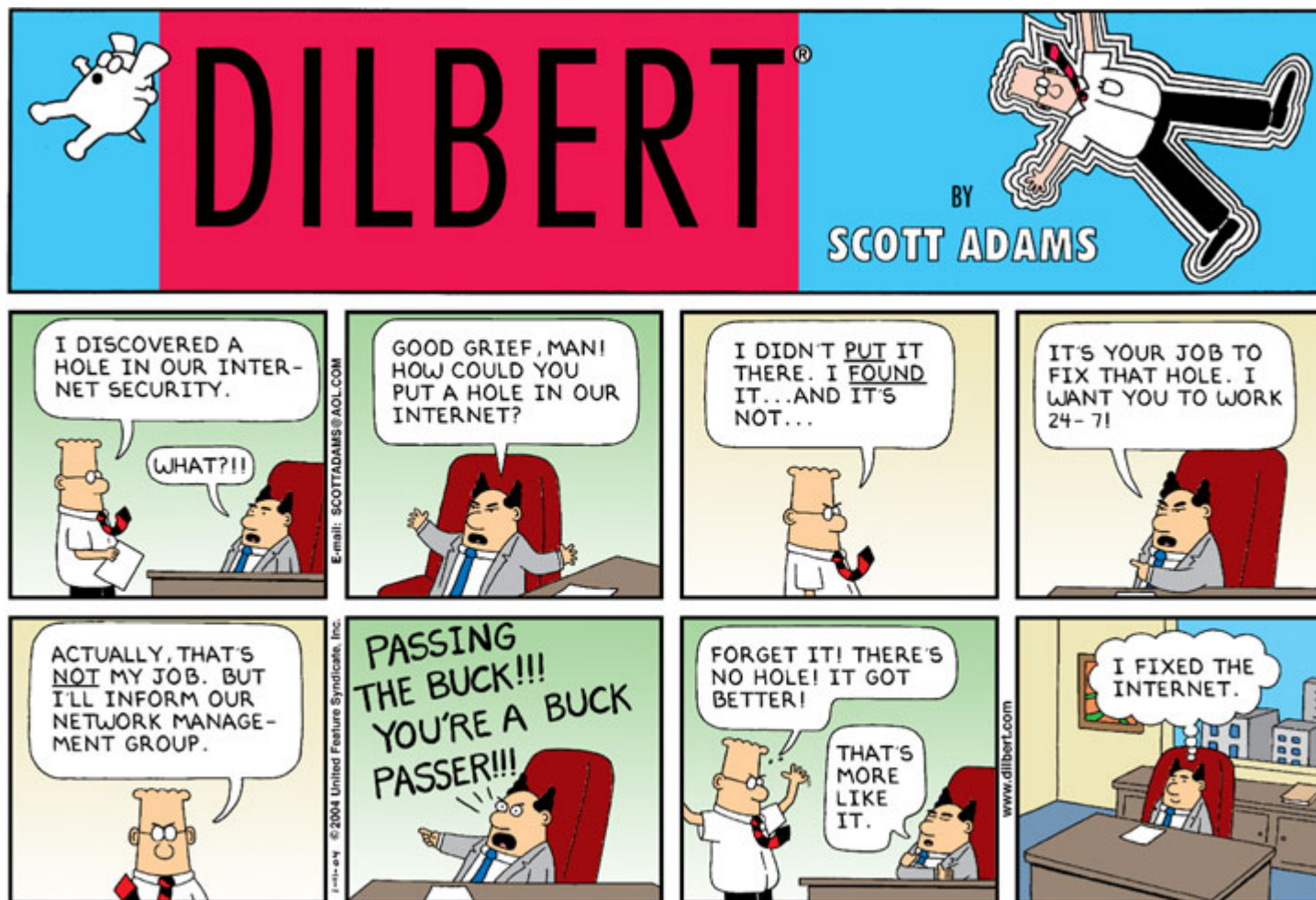


- **La sicurezza non è questione della quantità di difese ammassate di fronte a un sistema**
- Ma allora, come si valuta la sicurezza di un sistema?
- Risposta da hacker: “si valuta vedendo quanto è difficile comprometterlo”
 - Penetration testing / offensive security research
 - Se vi pare poco “ingegneristico”, è esattamente quello che si fa con le casseforti (standard EN 1143-1), e non molto diverso da quello che si fa con le prove dei materiali

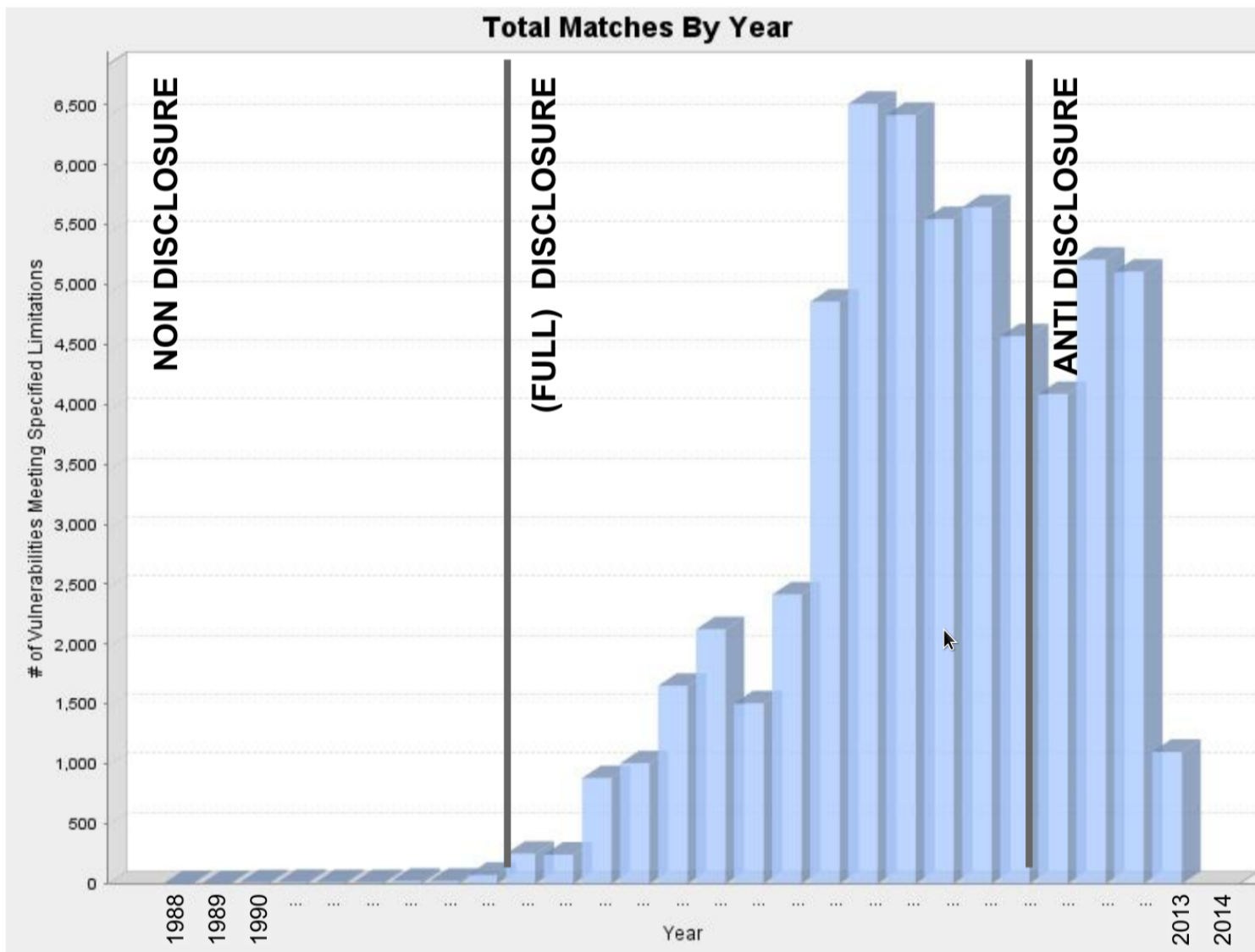


Alle volte la vita del *security engineer* è difficile...

17



© UFS, Inc.



Source: [NIST' National Vulnerability Database](#)



Subject: Comments on the dwssr.dll vulnerability threads

From: Iván Arce

Date: 2000-04-18 1:25:52

I do not intend to go further down the full disclosure vs. mediated release of information discussion here, however [Microsoft's handler's] post on NTBugtraq regarding CORE's work requires some clarifications on our side.

[...]

If someone yells 'FIRE' and that appears to be reasonable, I'd would be very careful in my methodology and editorial policies before yelling "NOT TRUE! NOT TRUE! EVERYTHING IS FINE!".

[...]

Excuse me if I'm being rude, but **I'm shocked by the fact that our company is being questioned because we found a bug.**

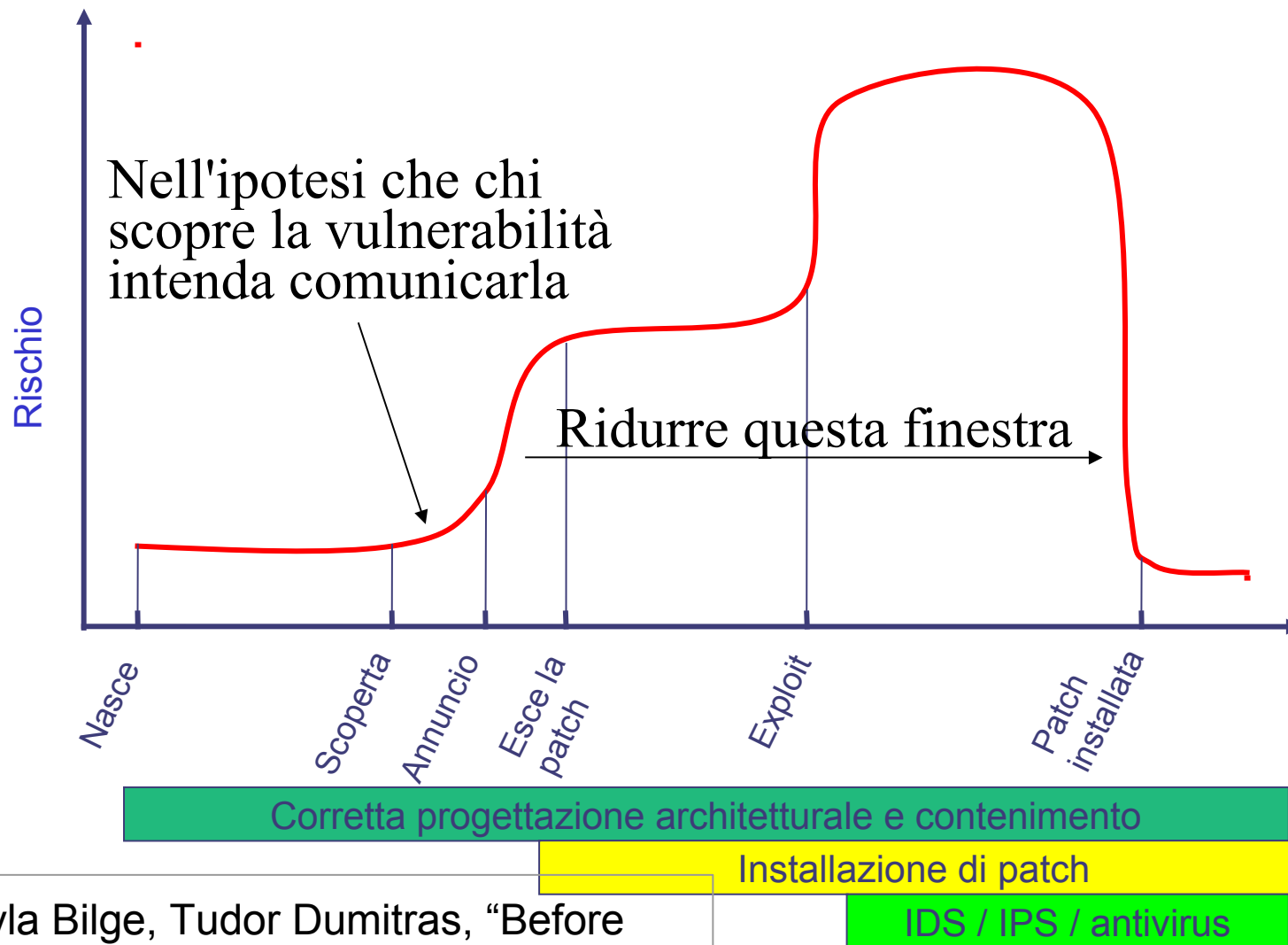
<http://www.s0ftpj.org/bfi/online/bfi10/BFi10-02.html>

<http://marc.info/?l=vuln-dev&m=95602682515862&w=2>



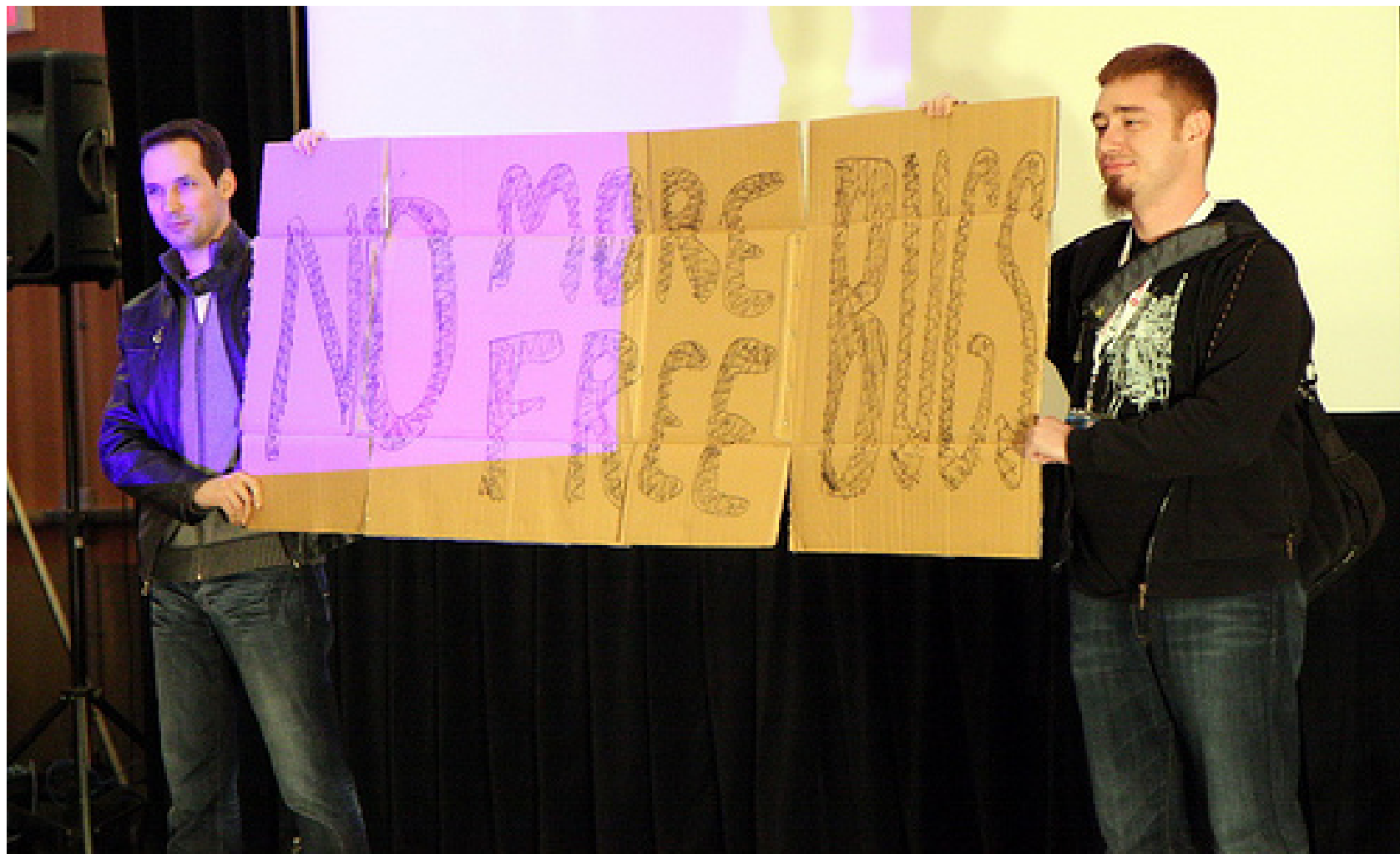
Rompi e ripara, rompi e ripara... (o: le montagne russe delle vulnerabilità)

20



See: Leyla Bilge, Tudor Dumitras, "Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World", ACM CCS 2012.









Build the Next Security Defense Technology and You Could Win \$200,000

WHY ARE WE DOING THIS?

The Microsoft BlueHat Prize contest is designed to generate new ideas for defensive approaches to support computer security. As part of our commitment to a more secure computing experience, we hope to inspire security researchers to develop innovative solutions intended to address serious security threats.

WHAT IS THE CONTEST?

The inaugural Microsoft BlueHat Prize contest challenges security researchers to design a novel runtime mitigation technology designed to prevent the exploitation of memory safety vulnerabilities. The solution considered to be the most innovative by the Microsoft BlueHat Prize board will be presented the grand prize of US \$200,000. Important information:

- Entries will be accepted and must be received by email to bluehatprize@microsoft.com between August 3rd 2011 to midnight Pacific Time on April 1st 2012.
- The winning entry will be announced at Black Hat USA 2012.
- For full details, see rules and regulations.

YOU COULD WIN

First prize: \$200,000 (USD)
Second prize: \$50,000 (USD)
Third prize: MSDN Universal subscription valued at \$10,000 (USD)

QUESTIONS?

Send your questions or comments to bluehatprize@microsoft.com.

HOW DO I ENTER?

To enter, send an email to bluehatprize@microsoft.com — include your technical description and prototype as outlined in the official rules.

The Microsoft BlueHat Prize board will reply with additional information applicants will need to submit a complete entry.



BlueHat Prize  150  Recommend  41



com/programs/q-reward		
	Dropbox Dropbox is a free service that lets you bring your photos, docs, and videos anywhere and share them easily. \$216 - \$4,913 Per Bug	Report Bug
	Barracuda Networks, Inc. Trusted Planet-Wide \$50 - \$3,133 Per Bug	Report Bug
	Jet.com The most brilliant way to shop. \$25 - \$2,500 Per Bug	Report Bug
	Pinterest Discover ideas for any project or interest, hand-picked by people like you. \$50 - \$1,000 Per Bug	Report Bug
	Simple Barter Banking \$50 - \$1,500 Per Bug	Report Bug
	Socrata Put your skills to the test! \$25 - \$5,000 Per Bug	Report Bug
	Hemku Cloud computing for developers \$100 - \$1,500 Per Bug	Report Bug
	Drupal The Drupal Open Source Content Management System \$50 - \$1,000 Per Bug	Report Bug



Domande?

- Grazie per l'attenzione
- Potete scrivermi a:
stefano.zanero@polimi.it
- Oppure twittare @raistolo

