POLITECNICO DI MILANO





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

$whoami

- **Associate professor @ POLIMI**

- **IEEE Computer Society**
  - Board of Governors member
  - Cybersecurity STC chair

- **Information Systems Security Association**
  - International Director

- **Black Hat**
  - Review board member

Di cosa parlerò

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

Grandi trionfi dell'ingegneria

Grandi trionfi dell'ingegneria

Grandi trionfi dell'ingegneria

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

Grandi trionfi dell'ingegneria

Grandi trionfi dell'ingegneria

Grandi trionfi dell'ingegneria (molto grandi)

- **"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

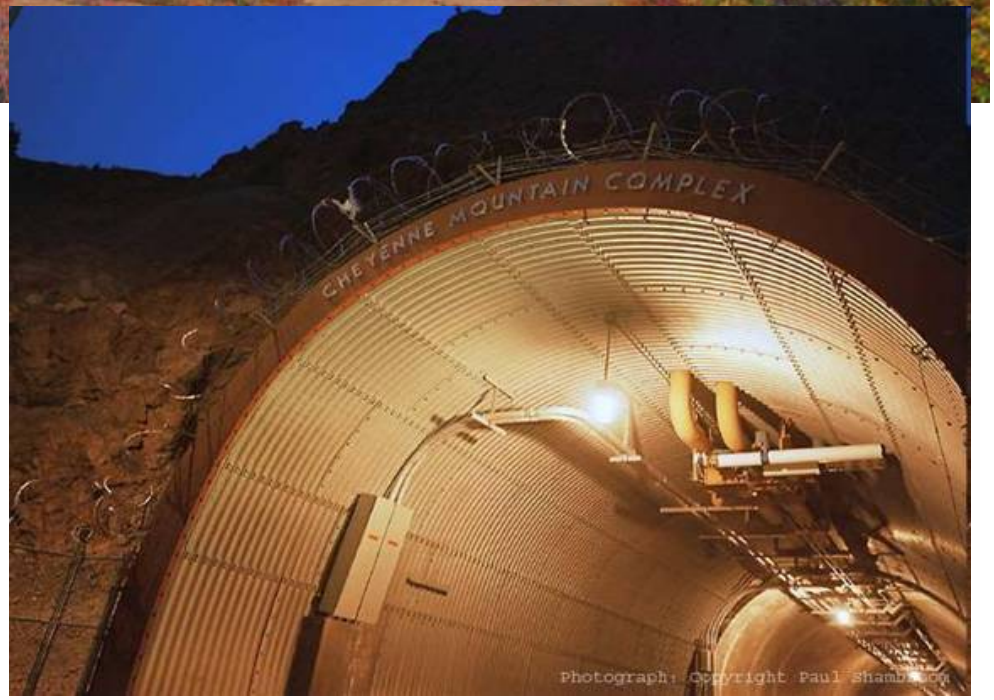
Cosa è “sicuro” ?

Cosa è “sicuro” ?

Cosa è “sicuro” ?

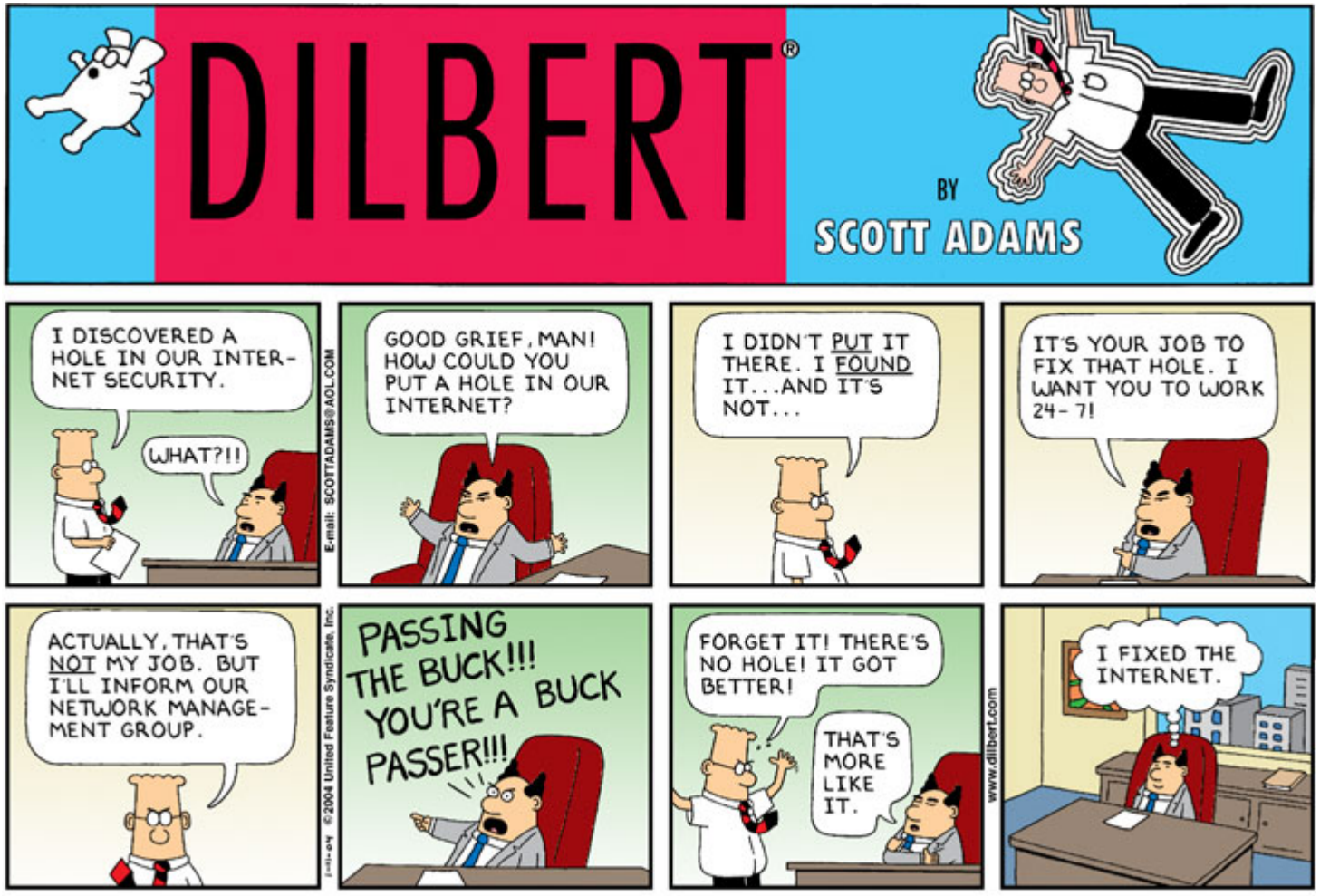
Cosa è “sicuro” ?

Cosa è “sicuro” ?

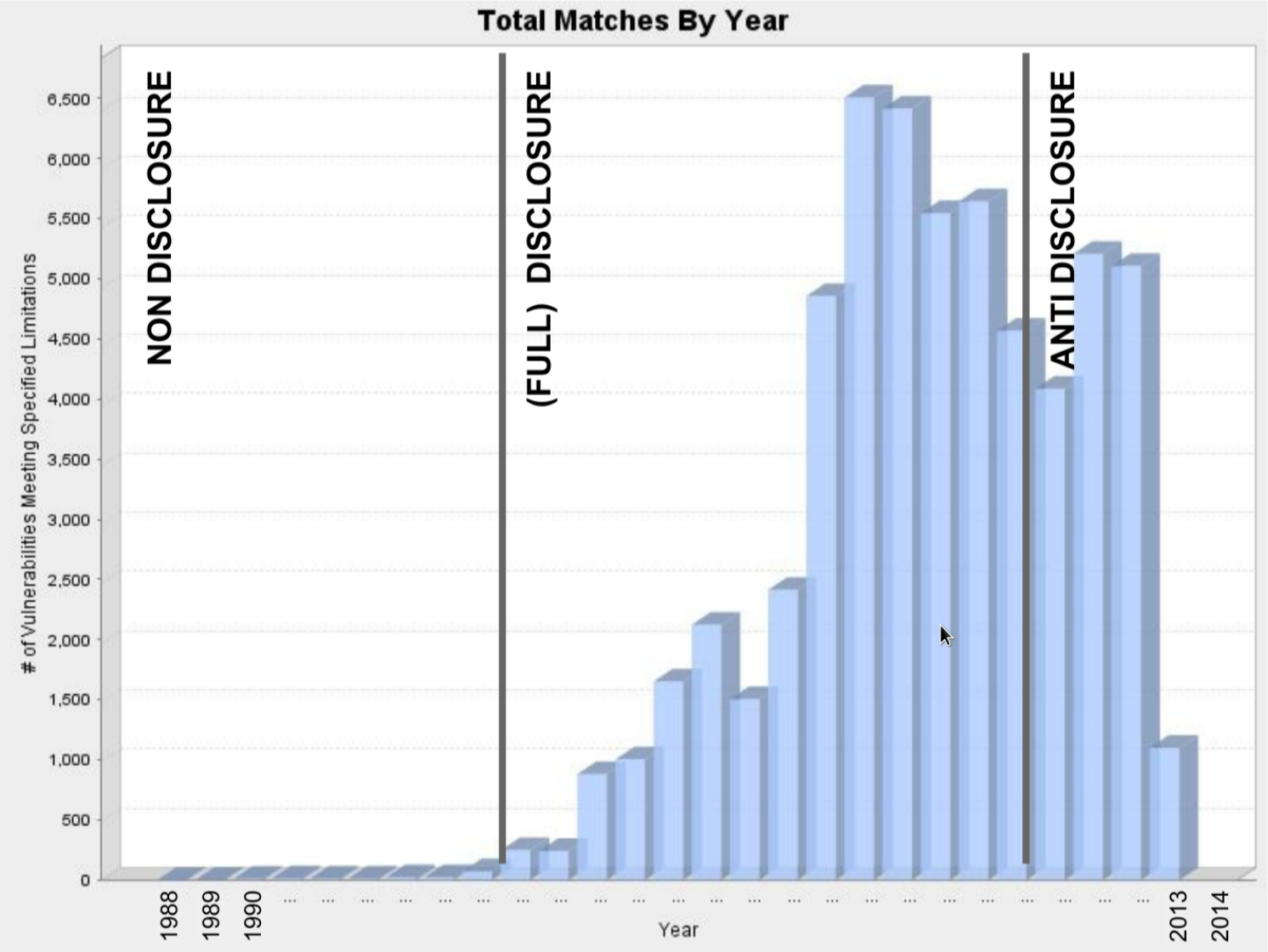


- **La sicurezza non è questione della quantità di difese ammassate di fronte a un sistema**
- Ma allora, come si valuta la sicurezza di un sistema?
- Risposta da hacker: “si valuta vedendo quanto è difficile comprometterlo”
  - Penetration testing / offensive security research
  - Se vi pare poco “ingegneristico”, 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...



Le vulnerabilità note



Source: NIST' National Vulnerability Database

I primi passi della disclosure

Subject: Comments on the dvwssr.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!".

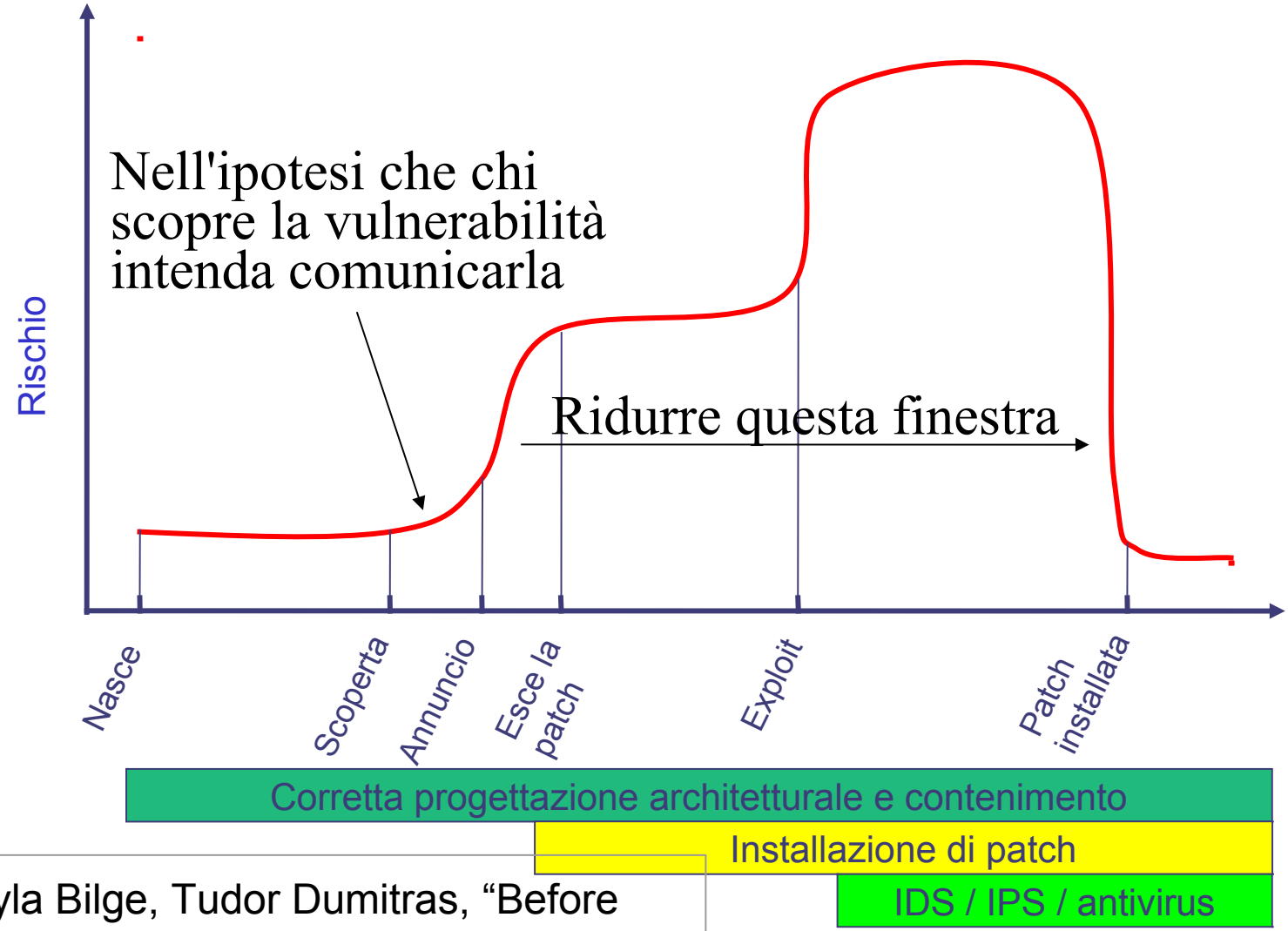
[...]

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

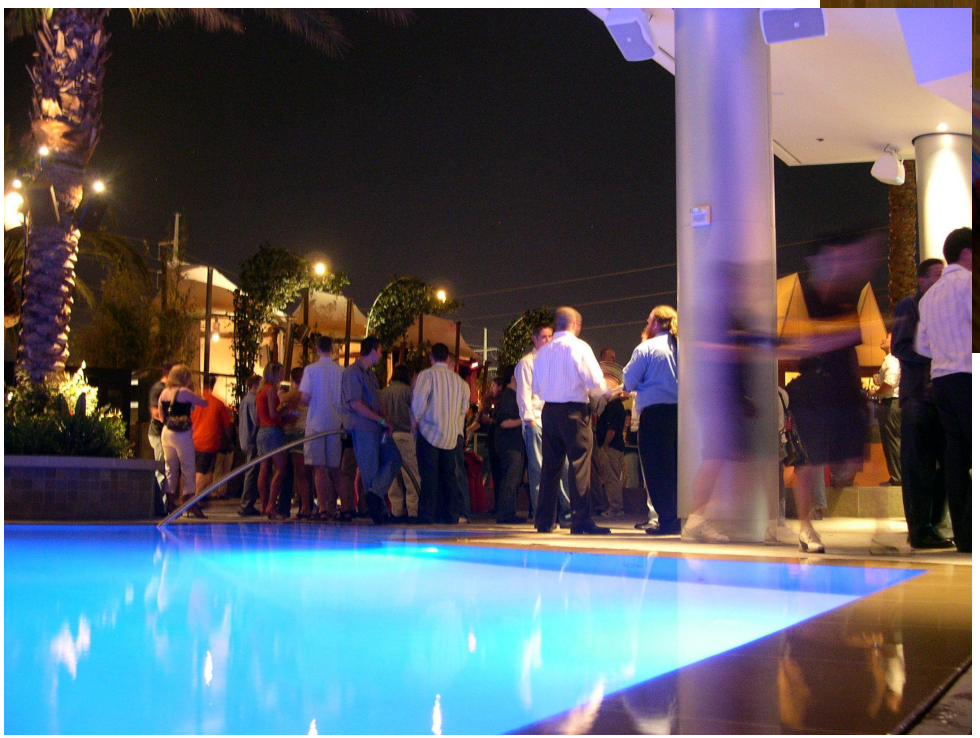
http://marc.info/?l=vuln-dev&m=95602682515862&w=2

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



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

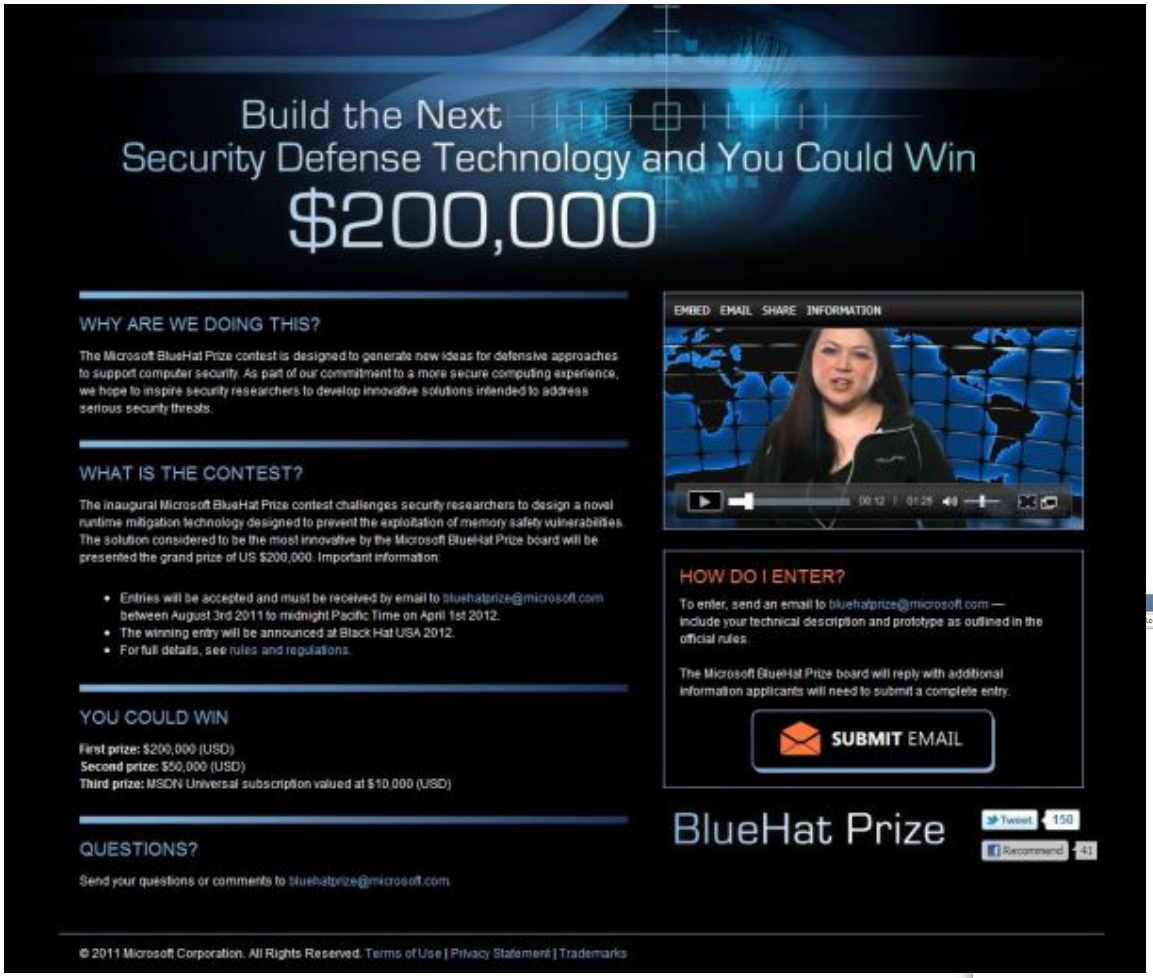
The Black Hat parties

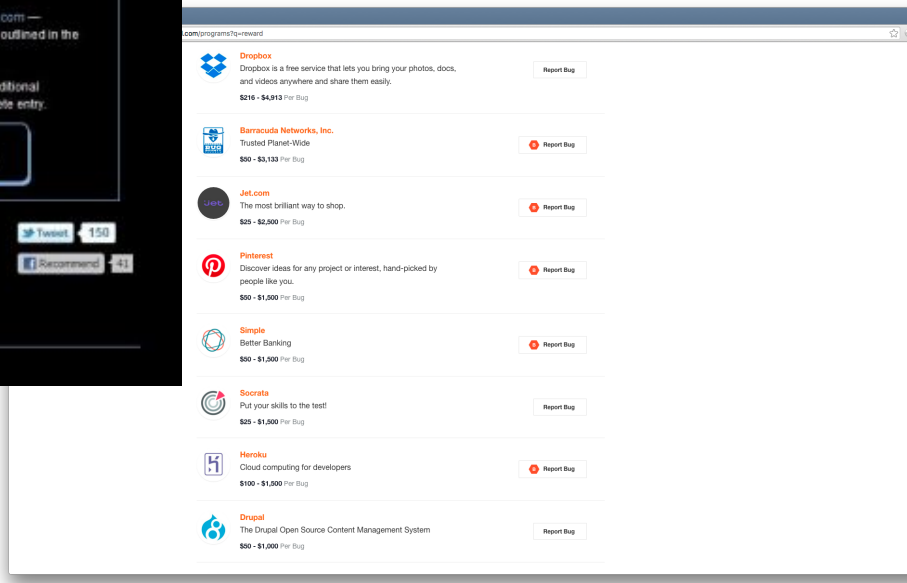


Non disclosure

Exploit black market

Bug bounties





Domande?

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