From Microsoft with <3

A New Security Research Incentive – Not at All What You Were Expecting

Katie Moussouris
Senior Security Strategist Lead, Microsoft Security Response Center
Microsoft Corporation

Agenda

- Intro – Who, Why, What
- Researcher Motivations
- The Vulnerability Economy and You (and Us)
- ???
- Profit!!!
- <3
- Questions

Who Mom Loves

- Joined Microsoft in April 2007
- Now I run Microsoft Security Community Outreach & Strategy, MSVR, and BlueHat ☺
- My (Security*) Work in Bullet Points:
  - Linux Dev and Security Tzarina - TurboLinux, circa 2000
  - Pen Tester - Artist formerly known as @stake
  - Founder - Symantec Vulnerability Research (SVR)
  - Founder - Microsoft Vulnerability Research (MSVR)
  - Policy Maker
    - Editor for draft ISO standard on Vulnerability Handling (30111)
    - Lead SME for US National Body on Vulnerability Disclosure (29147)

* Was a molecular biologist in a past professional life, worked on the Human Genome Project

The Vulnerability Economy and You (and Us)

Researchers in general	• Have other motivations besides money
Researchers who report vulnerabilities to Microsoft	• Over 90% of private reports are made directly to Microsoft

- We respect researchers' right to earn a living from their work
- We hope researchers who sell vulnerabilities choose the white market
- We try to hire talented researchers to help us improve our security

BlueHat Prize Announcement

- **First BlueHat Prize Challenge:**
  - Design a novel runtime mitigation technology that is capable of preventing the exploitation of memory safety vulnerabilities
- **Entry Period:** Aug 3, 2011 – Apr 1, 2012
- **Winners announced:** BlackHat USA August 2012
- **IP remains the property of the inventor**, with a license for Microsoft to use the technology

Grand Prize:	• **$200,000** in cash
Second Prize:	• **$50,000** in cash
Third Prize:	• MSDN subscription ($10,000 value)

Examples of Mitigation Technology

Data Execution Prevention (DEP)

- Sets non executable memory pages

Address Space Layout Randomization (ASLR)

- Randomizes memory in which apps load

Structured Exception Handler Overwrite Protection (SEHOP)

- Verifies exception handler lists have not been corrupted

Mitigation tools from Microsoft:

Enhanced Mitigation Experience Toolkit (EMET)

- Download EMET:
  http://www.microsoft.com/download/en/details.aspx?id=1677

BlueHat Prize Judging Criteria

Practicality – 30%

- Can the solution be implemented and deployed at a large scale on Windows?
- Overhead must be low (e.g. CPU and memory cost no more than 5%).
- No application compatibility regressions should occur.
- No usability regressions should occur.
- Reasonable to develop, test, and deploy.

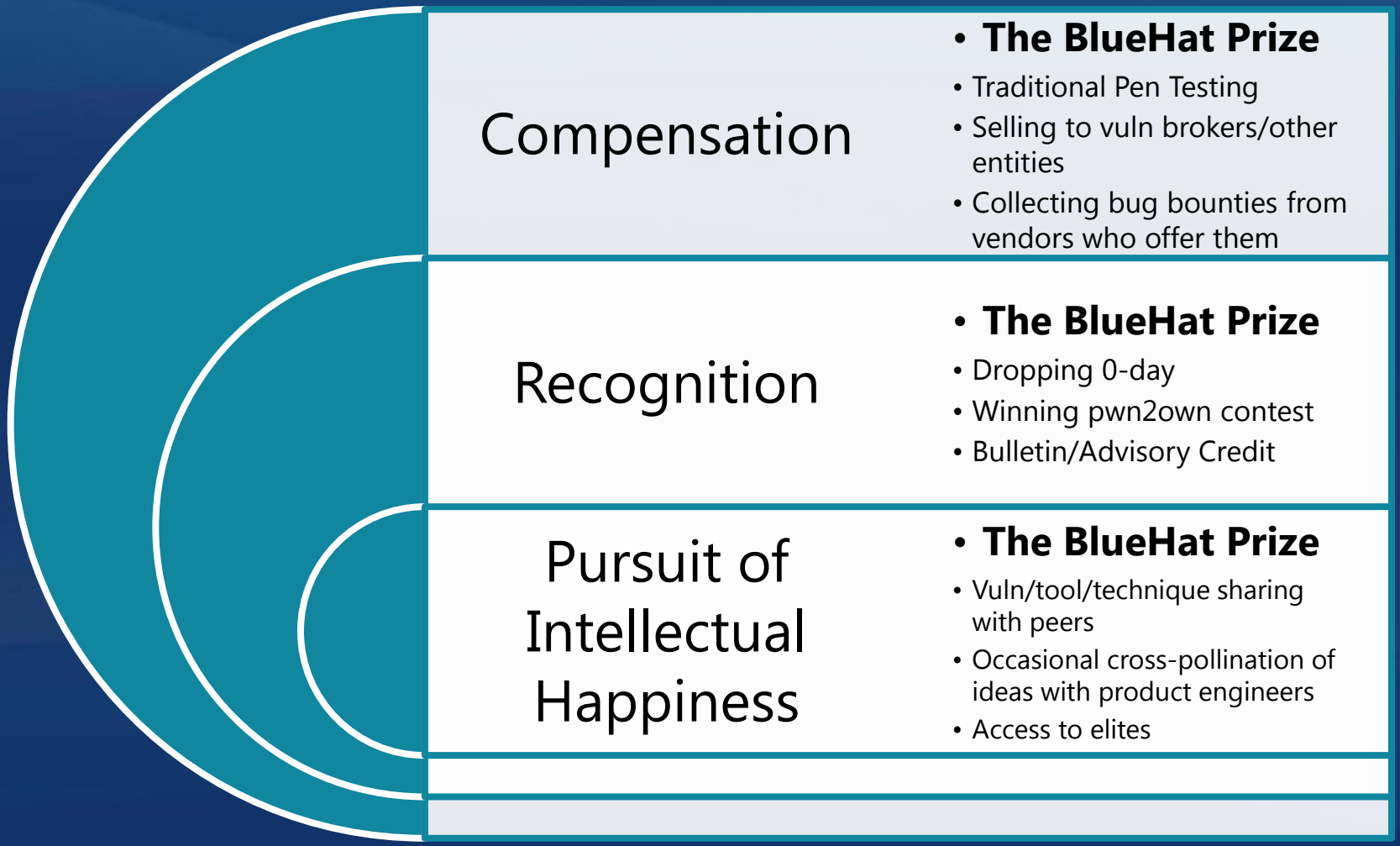
Robustness – 30%

- How easy would it be to bypass the proposed solution?

Impact – 40%

- Does the solution strongly address key open problems or significantly refine an existing approach?
- Would the solution strongly mitigate modern exploits above and beyond our current arsenal?

New Researcher Motivations/Fulfillment



Help Us Secure the Planet

- Microsoft values the security community and their work
  - In fact, we <3 u!
- New incentive for DEFENSIVE Security – The BlueHat Prize
  - Over a quarter million dollars in cash and prizes for the best runtime mitigation technology
- Platform providers like Microsoft help the ecosystem by investing in mitigating entire classes of vulnerabilities
- Some of the best defenders come from the offense side
  - The other side of the security coin awaits you!

- Now you know what a Security Strategist at Microsoft Does

For More Information…

- BlueHat Prize Web site: www.bluehatprize.com
  - Questions? bluehatprize@microsoft.com

- MSRC Blog: http://blogs.technet.com/msrc
- EcoStrat Blog: http://blogs.technet.com/ecostrat/
- Help Defend the Planet: http://careers.microsoft.com
- Follow us on Twitter:

Microsoft®

Your potential. Our passion.™