ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

International Vulnerability Purchase Program (IVPP)

What would it mean and cost to outbid cyber criminals?

Dr. Stefan Frei
@stefan_frei
frei@techzoom.net

AREA41 DC4131

Zurich, June 2nd, 2014

Throughout history, new technologies have revolutionized crime and warfare alike

- Chariot ..
- Gunpowder ..
- Tanks ..

Criminals proofed repeatedly to be very fast adopters of new technology

The last two decades saw an incredible rise in importance of information systems for the economy and for society ..

accompanied by increased interest in the way in which

vulnerability information is managed and traded

information about

security vulnerabilities

has become a

valuable asset

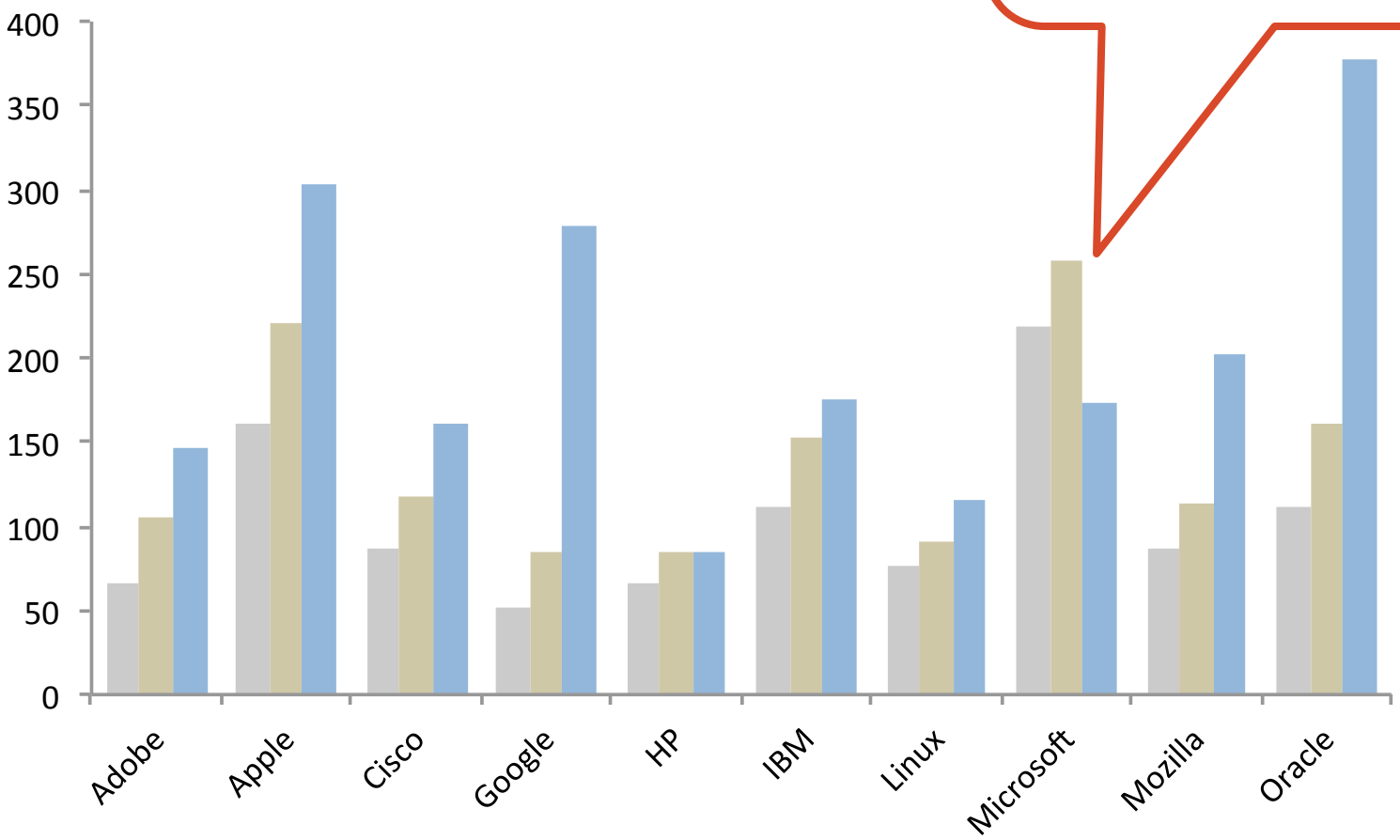
Vulnerability commercialization remains a contentious issue
(linked to the concept of vulnerability disclosure)

However, a market for vulnerabilities & exploits has developed, and is exploding

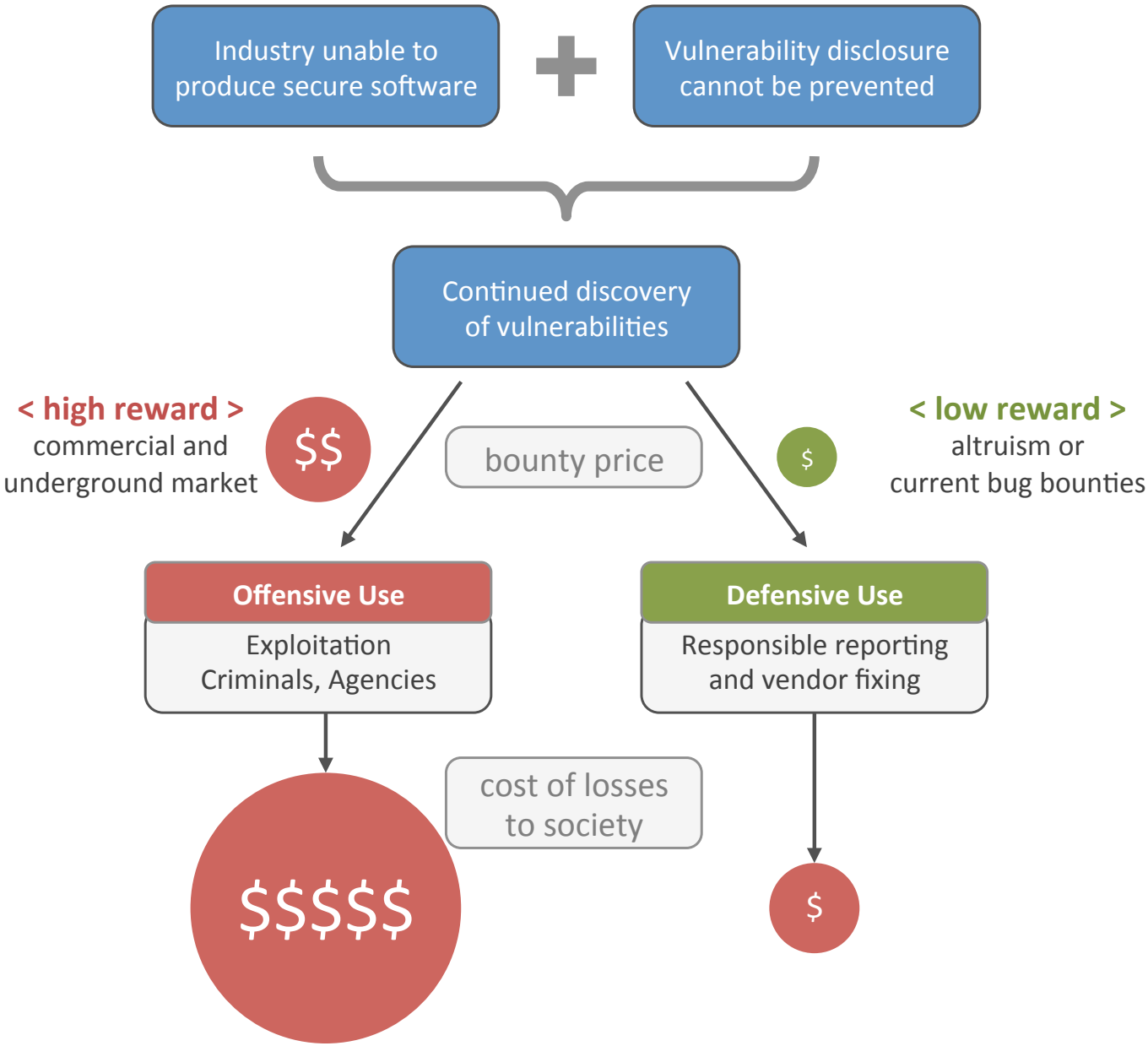
Vulnerabilities are abundant

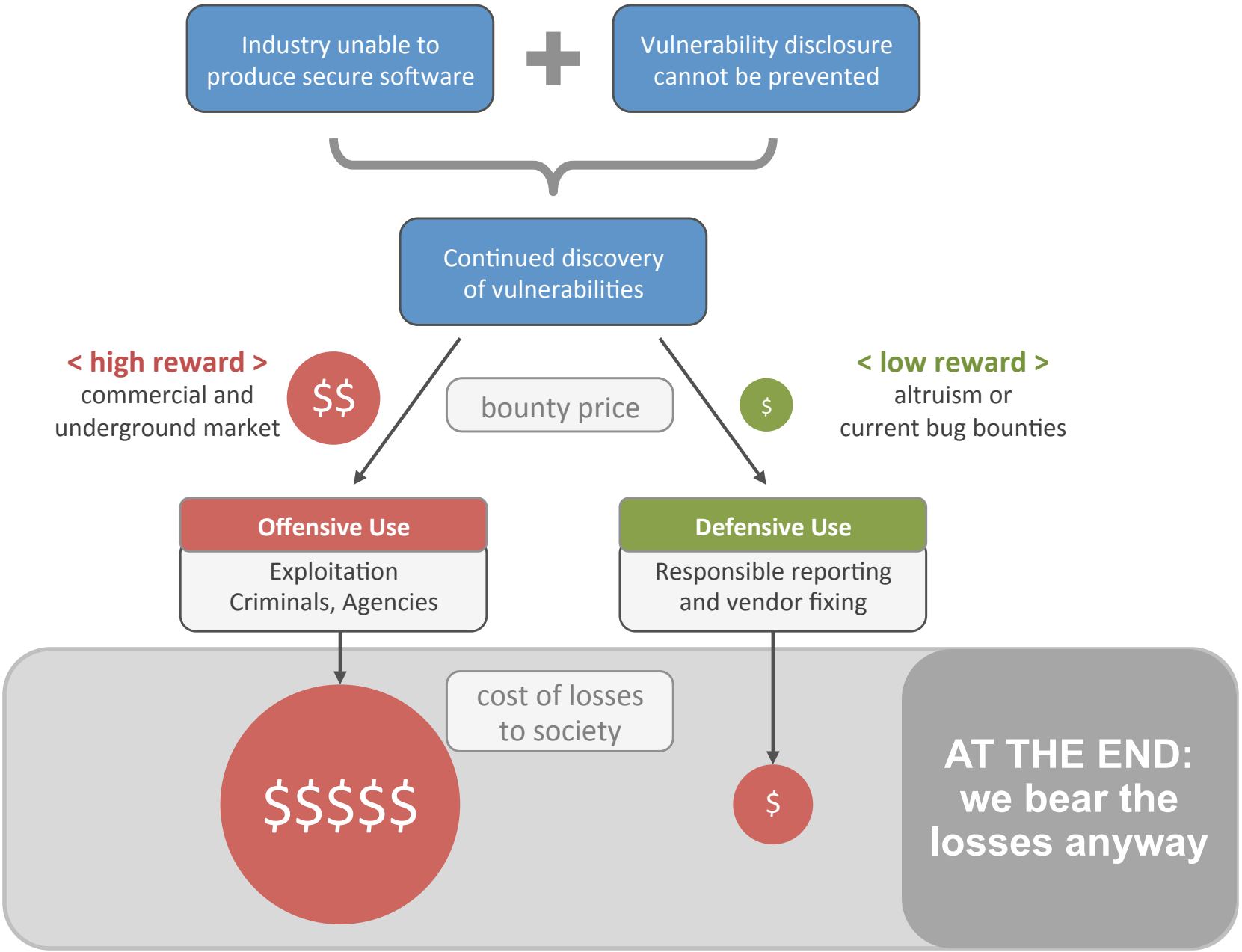
only
1 of 10
software vendors

reduced vulnerabilities
in 2012 vs. previous 10 years



Source: The evolution of vulnerability disclosures by software vendor for 2012 - http://youtu.be/IjWTVGo6ol0


Industry unable to produce secure software
+
Vulnerability disclosure cannot be prevented
Continued discovery of vulnerabilities
< high reward >
commercial and underground market
$$
bounty price
$
< low reward >
altruism or current bug bounties
Offensive Use
Exploitation
Criminals, Agencies
Defensive Use
Responsible reporting and vendor fixing
cost of losses to society
$$$$$
$


Industry unable to produce secure software
+
Vulnerability disclosure cannot be prevented
Continued discovery of vulnerabilities
< high reward >
commercial and underground market
$$
bounty price
$
< low reward >
altruism or current bug bounties
Offensive Use
Exploitation
Criminals, Agencies
Defensive Use
Responsible reporting and vendor fixing
cost of losses to society
$$$$$
$
AT THE END:
we bear the losses anyway

Vulnerabilities known only to
privileged closed groups
such as ..

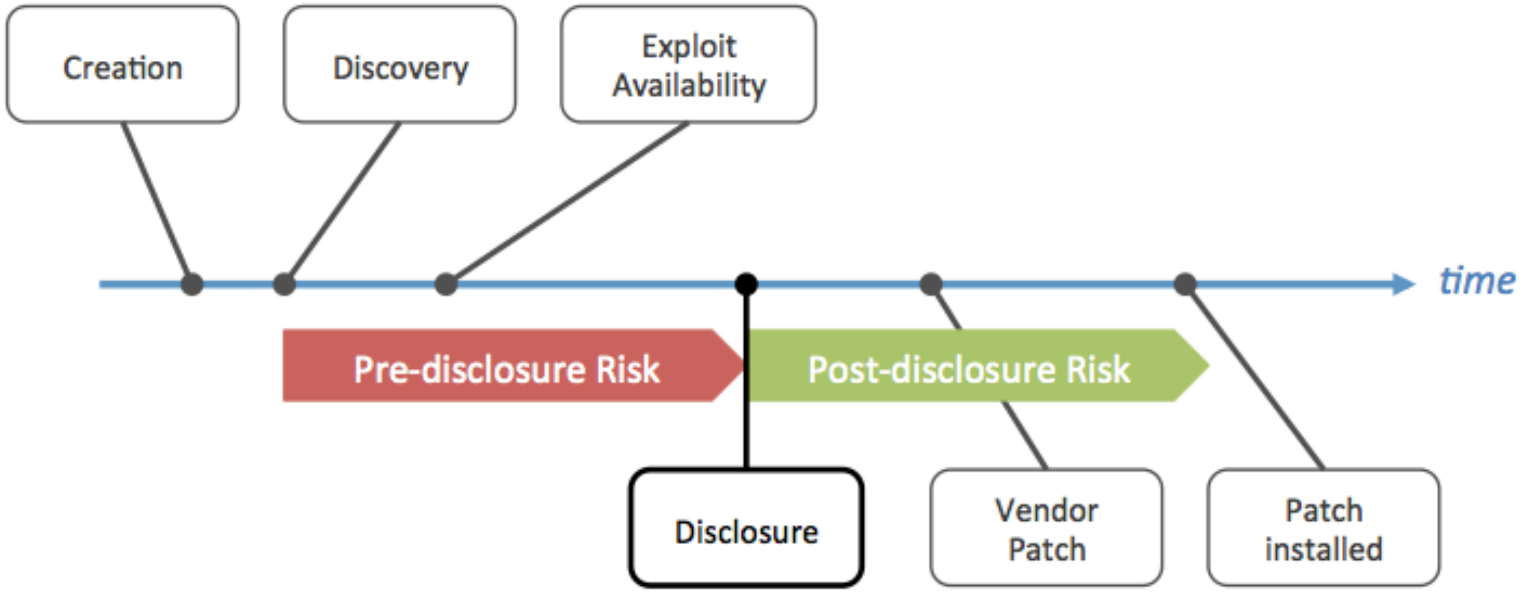
Cyber Criminals

Brokers

Government Agencies

.. pose a real and present risk to all who use the affected software

Lifecycle of a Vulnerability



The

Known Unknowns

vulnerabilities known to privileged groups only

How many?

Unknown for how long?

How to measure?

Vulnerability Purchase Programs

Data of two vulnerability purchase programs covering 1,855 vulnerabilities from 2002 - 2013 allow the reconstruction of the vulnerability lifecycle after publication

Program	Program Inception	Total Purchases	Targeted Vendors	Time To Disclosure
iDefense VCP	2002	969	195	133 days
TippingPoint ZDI	2005	1,423	92	174 days

Pre-disclosure risk

These programs coordinate vulnerability information with the software vendor!

iDefense Vulnerability Contributor Program (VCP)

TippingPoint Zero Day Initiative (ZDI)

Relevant targets, considerable exposure

#	Vendor Affected	Total Purchases VCP	ZDI	VCP+ZDI	Days Private	Vendor Share
1	Microsoft	153	237	390	181	14%
2	Apple	38	171	209	129	10%
3	HP	17	157	174	233	19%
4	Adobe	59	102	161	119	17%
5	Oracle	29	114	143	166	8%
6	Novell	30	112	142	142	10%
7	IBM	58	67	125	226	8%
8	RealNetworks	19	73	92	262	49%
9	Sun	34	26	60	159	5%
10	Symantec	20	39	59	198	18%
11	Mozilla	8	51	59	80	5%
12	CA	23	30	53	151	29%
13	EMC	11	35	46	131	38%
14	Cisco	10	20	30	229	2%
15	WebKit	13	14	27	138	5%
16	Trend Micro	15	10	25	94	24%
17	Samba	9	14	23	65	28%
18	Ipswitch	15	8	23	58	25%
19	SAP	4	10	14	143	13%
Total		**565**	**1290**	**1855**		
Average					**153**	**17%**

14%

of all Microsoft vulnerabilities reported through a purchase program

153 days

from purchase to patch availability

Purchase programs …

- cover a considerable share of a vendors' vulnerabilities
- despite offering low prices compared to the "black market"

Exposure to "Known Unknowns"

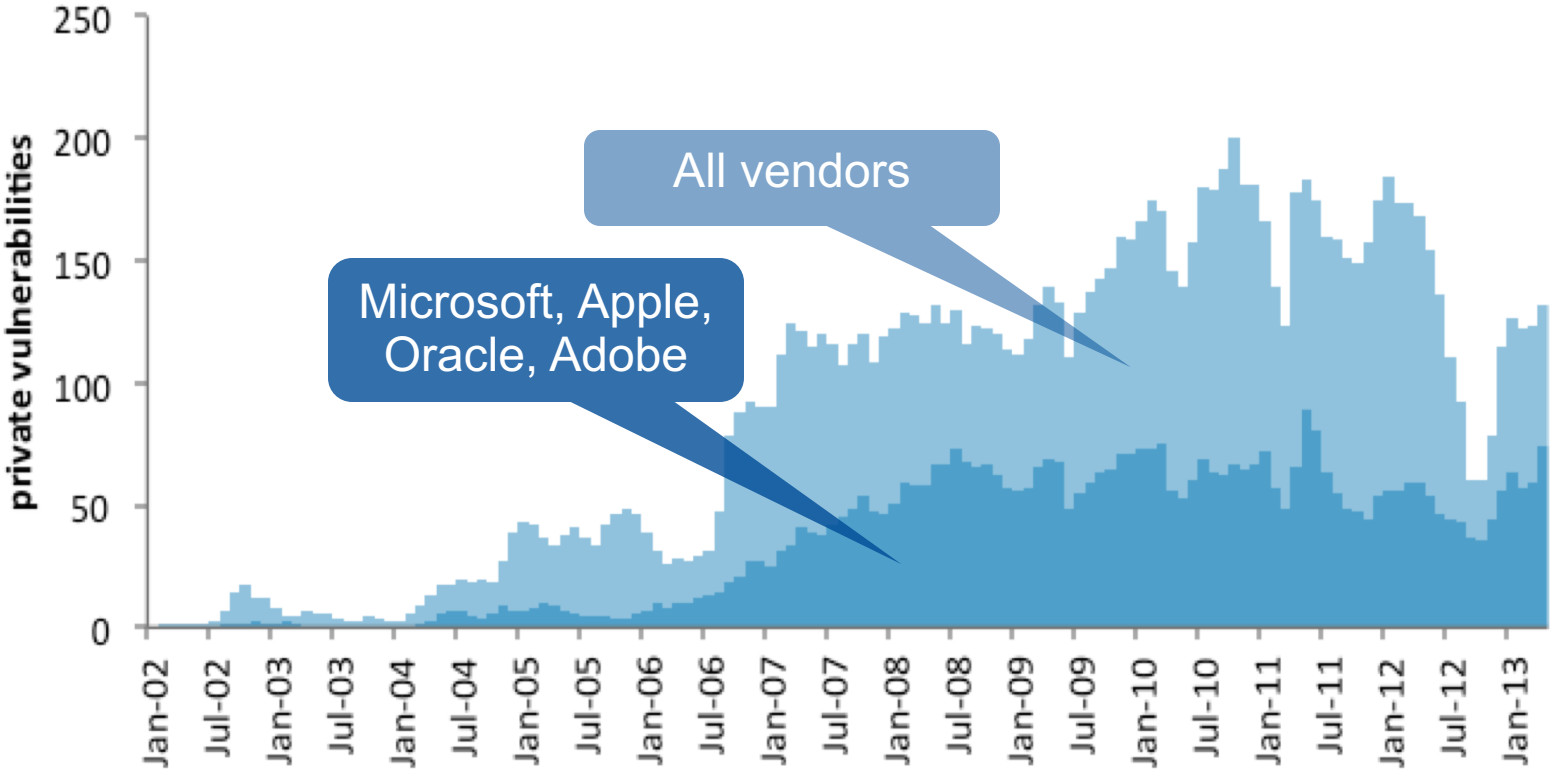
How many yet unpublished vulnerabilities are known to purchase programs exclusively ..

at any given day in the last years?

153 vulnerabilities known only to VCP and ZDI on any given day between 2010 and 2013

# of known unknowns, average per day

58 of which target Microsoft, Apple, Oracle, and Adobe



Source: The Known Unknowns - http://bit.ly/1x52Fce

VCP & ZDI inform the vendor in order to release a patch

average exposure time: 153 days

Critical vulnerabilities are available

- in considerable quantities for private groups, for extended periods

and for a relatively low price

When the vendor is not informed about new vulnerabilities

average zero-day attack persists 312 days

The average zero-day attack persists for almost a year before it is detected

Source: Symantec Research
http://www.symantec.com/connect/blogs/zero-day-world

More Unknowns

Our measurement provides a minimum estimate of the known unknowns
(… criminals and government agencies don't share data)

What about vulnerabilities and exploits that are not publicly traded, and are definitively not coordinated with the software vendor?

- Boutique Exploit Providers
- Governments & Defense Contractors
- Commercial Security Consulting

ENDGAME. [Re]Vuln VUPEN security EXODUS INTELLIGENCE

Vulnerability & Exploit Providers

An increasing number of commercial players offer zero-day exploits for their subscribers:

- they do not reveal their clients
  (big buyers reportedly include government agencies)
- have a keen interest in a long pre-disclosure time
  (keep the zero-day private as long as possible)
- some firms restrict their clientele
  (by country, specific agencies)
- price for exploits between USD $40k and $160k

Shopping List

Maui – Zero-Day Vulnerability and CNE/CNA Program

Maui	$2,500,000 per contract year	• Minimum of 25 deliverables per year
		• Deliverable contents - Software
		  • Software CNE/CNA
		  • Metasploit module
		  • VMware image for testing
		• Deliverable contents - Documentation
		  • Vulnerability information
		  • CNE/CNA information
		  • Demo instructions
		  • Revision history

USD $2.5 million for 25 zero-day exploits per year

Software Vulnerability Packages

- Development of general and custom tools for IA and IO
- Productization for use by trained and untrained operators

.. for use by trained and untrained operators

Challenge to society (I)

The discovery and subsequent abuse of vulnerabilities by external researchers or organizations can not be prevented

Yearly losses due to cyber crime are estimated between

10 to 400 billion USD

Vulnerabilities are the root cause of considerable part of these losses

Source: International Vulnerability Purchase Program (IVPP) - http://bit.ly/1x51RUP

Challenge to society (II)

Our security depends largely:

- on the ethics and altruism of the discoverer to follow coordinated disclosure
- a few vendor-operated bug bounty programs with moderate-to-low rewards

At the same time, the black market is expanding rapidly and offering large rewards for the same information

Challenge to society (III)

"Never was so much owed by so many to so few."

Winston Churchill's famous 1940 wartime speech

Follow the money ...

The experience of past decades has shown that traditional approaches based on "more of the same" did not deliver adequate security

The question to ask is this:

"How much are those that bear the costs willing to pay to reduce their losses incurred as a result of cyber crime?"

Risk Management

spending

USD 10.-

on measures to prevent losses of

USD 100.-

is a sound proposal

Follow the money ...

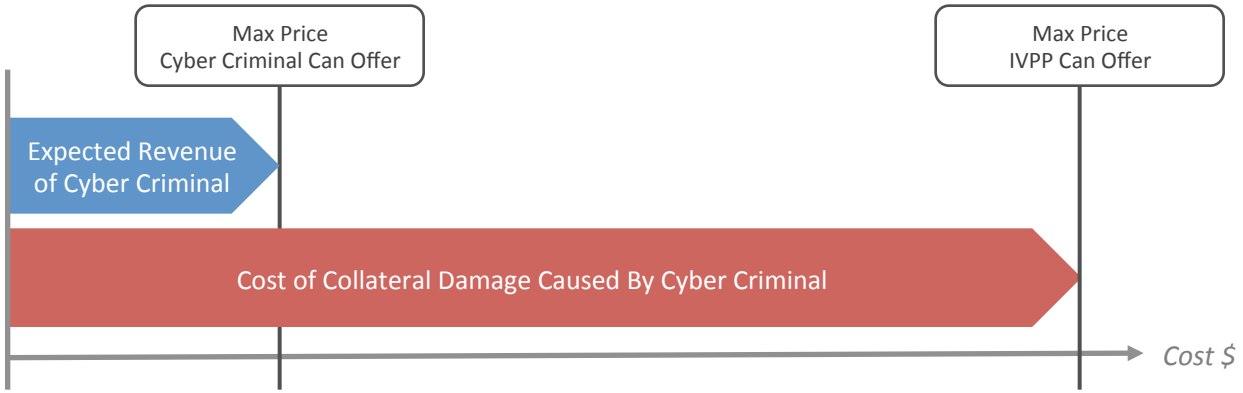
What would be the cost to society, the software industry, or individual software vendors if we would offer

USD 150,000 per vulnerability ?

- buying all vulnerabilities (irrespective of risk or affected software) in a given year
- kind of an overkill to buy all, but OK to validate the model

Yes we can - outbid criminals!

Buying vulnerabilities makes sense as long as the purchase cost is less than the cost of the prevented losses



Vulnerability abuse incurs large collateral damage, by far exceeding criminals revenue

International Vulnerability Purchase Program

What would it cost society to buy all vulnerabilities from all vendors for USD 150,000 each?

This includes buying all non-critical vulnerabilites

Cost of buying all vulnerabilities in 2012

		Cost in Million $				Percentage Cost of			Percentage Cost of	
	Vuln.	Cost by Risk				GDP	GDP	Revenue	Cyber Crime Estimates	
Vendors	Total	High	Med	Low	Total	US	EU	SW Ind.	10 Billion	100 Billion
All	**5,218**	265	441	76	**783**	0.005%	0.005%	0.268%	7.827%	0.783%
Top 100	**3,332**	192	257	51	**500**	0.003%	0.003%	0.171%	4.998%	0.500%
Top 50	**2,959**	176	224	44	**444**	0.003%	0.003%	0.152%	4.439%	0.444%
Top 10	**2,065**	147	134	29	**310**	0.002%	0.002%	0.106%	3.098%	0.310%

less than **0.01%** of the **GDP** of the **US** or the **European Union**

less than **0.8%** of the yearly cost of **cyber crime**

Program Cost

On average, buying all 5,000 to 6,000 vulnerabilities published in a given year costs ..

- less than 0.01% of the GDP of the US or EU
- less than 1.0% of the revenue of the software industry
- less than 0.8% of cyber crime losses (at 100 Billon/year)

Program Cost

Buying all vulnerabilities irrespective of risk and affected product is an overkill:

- buy only high risk vulnerabilities: ~ 33% of cost

Most relevant vulnerabilities are concentrated in the products of a few major vendors:

- top 10 vendors only: ~ 39% of cost
- top 50 vendors only: ~ 56% of cost
- top 100 vendors only: ~ 63% of cost

Software Vendors

There is no product liability for software vendors.

Have major software vendors pay for their own vulnerabilities:

Argument:

> “Oh no, .. this would break the software vendors business model ..”

Data:

See next slide

Software vendors buying their vulnerabilities

What would it cost software vendors to buy all their vulnerabilities for USD 150,000 each?

This includes buying all non-critical vulnerabilites

		Cost in Million $				Revenue in Million $	
	Vuln.	Cost by Risk					
Vendor	Total	High	Med	Low	Total	Revenue	Cost in %
Oracle	427	9.8	37.4	17.0	64.1	37,120	0.173%
Apple	303	25.1	18.3	2.1	45.5	164,700	0.028%
Google	279	24.9	16.2	0.8	41.9	49,770	0.084%
Mozilla	202	18.0	11.6	0.8	30.3	n/a	
IBM	175	6.9	16.5	2.9	26.3	104,500	0.025%
Microsoft	173	18.2	7.2	0.6	26.0	72,930	0.036%
Cisco	160	13.8	9.5	0.8	24.0	46,680	0.051%
Adobe	146	19.8	2.1	0.0	21.9	4,404	0.497%
Linux	116	3.5	10.5	3.5	17.4	n/a	
HP	84	6.8	5.0	0.9	12.6	120,400	0.010%
Total w/o Mozilla, Linux	(Open Source, No Revenue)				**262.1**	**600,504.0**	**0.044%**

less than
1%
of the software vendors' **revenue**

International Vulnerability Purchase Program

The benefits of such a program include:

- Inclusion of products that are not currently covered by existing bug bounty programs
- Vulnerabilities that otherwise would be acquired for illicit use are reported to the vendor

International Vulnerability Purchase Program

The benefits of such a program include:

- Competitive pricing increases vulnerability research, thereby increasing the chance of the independent discovery and reporting of vulnerabilities that are already privately used by criminals or for cyber espionage
- Long term effect: more secure software firsthand

Purchasing Vulnerabilities

Over the past decades "more of the same" did not solve our security problems

- It is time to think out of the box
- An economic approach could be effective to reduce the risk, and instill incentives that favor security

Conclusion
Recommendations

Conclusion

The industry as a whole needs to assess current trends and possible nontechnical solutions, and evaluate new approaches to handling vulnerabilities at large

– failing to take action is not an option

Conclusion

Governments must evaluate the idea of an international vulnerability purchase program (IVPP) that could reduce losses occurring as a result of cyber crime.

Governments should establish incentives for the creation of more secure software.

Conclusion

Governments and the industry as a whole should aim to assign the liability or costs of purchasing vulnerabilities to the parties that are best equipped to manage the risk.

Conclusion

All software vendors must establish a process for coordinated disclosure of vulnerabilities and communication with researchers (including bug bounties).

Software vendors must invest in mechanisms that allow for the simple, automatic patching of their installed software

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

REFERENCES

References

- The Known Unknowns in Cyber Security
  http://www.techzoom.net/papers/nss_the_known_unknowns_2013.pdf
- International Vulnerability Purchase Program (IVPP)
  http://www.techzoom.net/papers/nss_international_vulnerability_purchase_program_ivpp_2013.pdf
- Cybercrime Kill Chain & Defense Layer Effectiveness
  http://bit.ly/VQJJsY
- Modeling Evasions in Layered Security
  www.nsslabs.com/reports/modeling-evasions-layered-security
- Correlation of Detection Failures
  www.nsslabs.com/reports/correlation-detection-failures