When Malware Attacks (anything but Windows)!(?)

Adam J. O'Donnell, Ph.D.
Cloudmark, Inc.
adam@cloudmark.com
http://np-incomplete.com

CLOUDMARK®

or... Modeling the Security Attack/Defense Game.

Adam J. O'Donnell, Ph.D.
Cloudmark, Inc.
adam@cloudmark.com
http://np-incomplete.com

CLOUDMARK®

- Windows malware: around 250k samples by the end of 2006, 500k by the end of 2007.

- Macintosh Malware: under 100, including pre-OSX

1. Mac users are just fundamentally more intelligent than PC users

2. Macs are harder to attack, and therefore less malware exists

3. Mac market share is too small to be of interest to malware writers

1. ~~Mac users are just fundamentally more intelligent than PC users~~

2. Macs are harder to attack, and therefore less malware exists

3. Mac market share is too small to be of interest to malware writers

Dino Dai Zovi

ex-Matasano, ex-@Stake

CLOUDMARK®

1. ~~Mac users are just fundamentally more intelligent than PC users~~

2. Macs are harder to attack, and therefore less malware exists

3. Mac market share is too small to be of interest to malware writers

1. ~~Mac users are just fundamentally more intelligent than PC users~~

2. ~~Macs are harder to attack, and therefore less malware exists~~

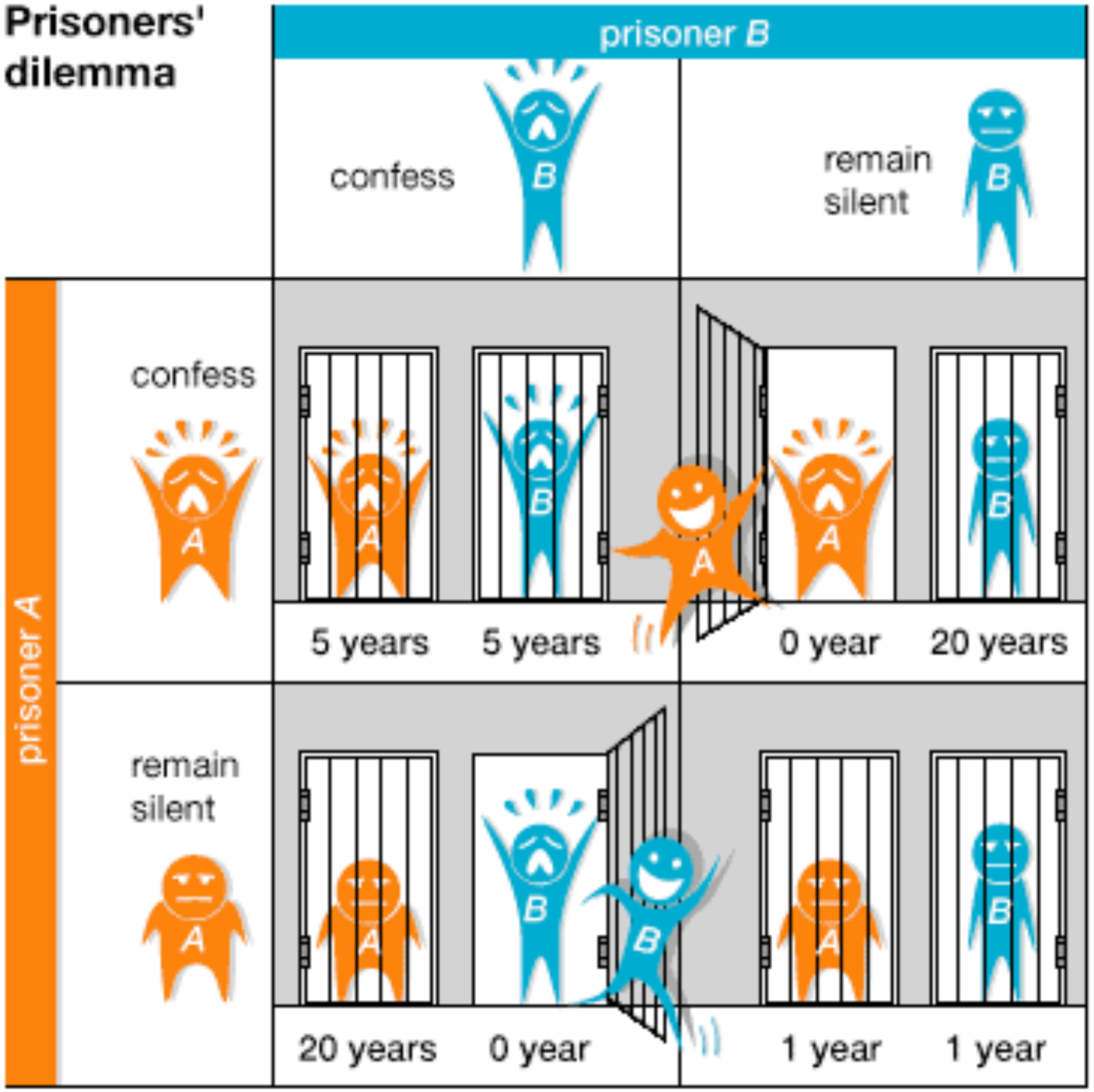
3. Mac market share is too small to be of interest to malware writers

If not now, when?

CLOUDMARK®

Game Theory!

Prisoners' dilemma



Dr. Strangelove

Or:
How
I Learned
To
Stop
Worrying
And
Love
The
Bomb

- Players: Actors who can make decisions
- Strategies: Decisions the actors can take
- Payoffs: Economic cost/benefit of taking said action

- Players: *Users* and *Attackers*

- Strategies: *Users* can either defend *A* or *B*; *Attackers* can either attack *A* or *B*

- Payoffs: Zero-Sum game; *Attackers* compromise all systems if they are undefended, but only fraction if they are defended

f	Market size of majority systems
p	Accuracy of security mechanisms
v	Value of a compromised host

Normal Form

		Defend	
		A	B
Attack	A	$(1-p)fv$	fv
	B	$(1-f)v$	$(1-p)(1-f)v$

Normal Form

		Defend	
		A	B
Attack	A	$(1-p)fv$	fv
	B	$(1-f)v$	$(1-p)(1-f)v$

- If the ratio $f/(1-f)$ is greater than $1/(1-p)$, then there is no rational point to attacking system *B*.

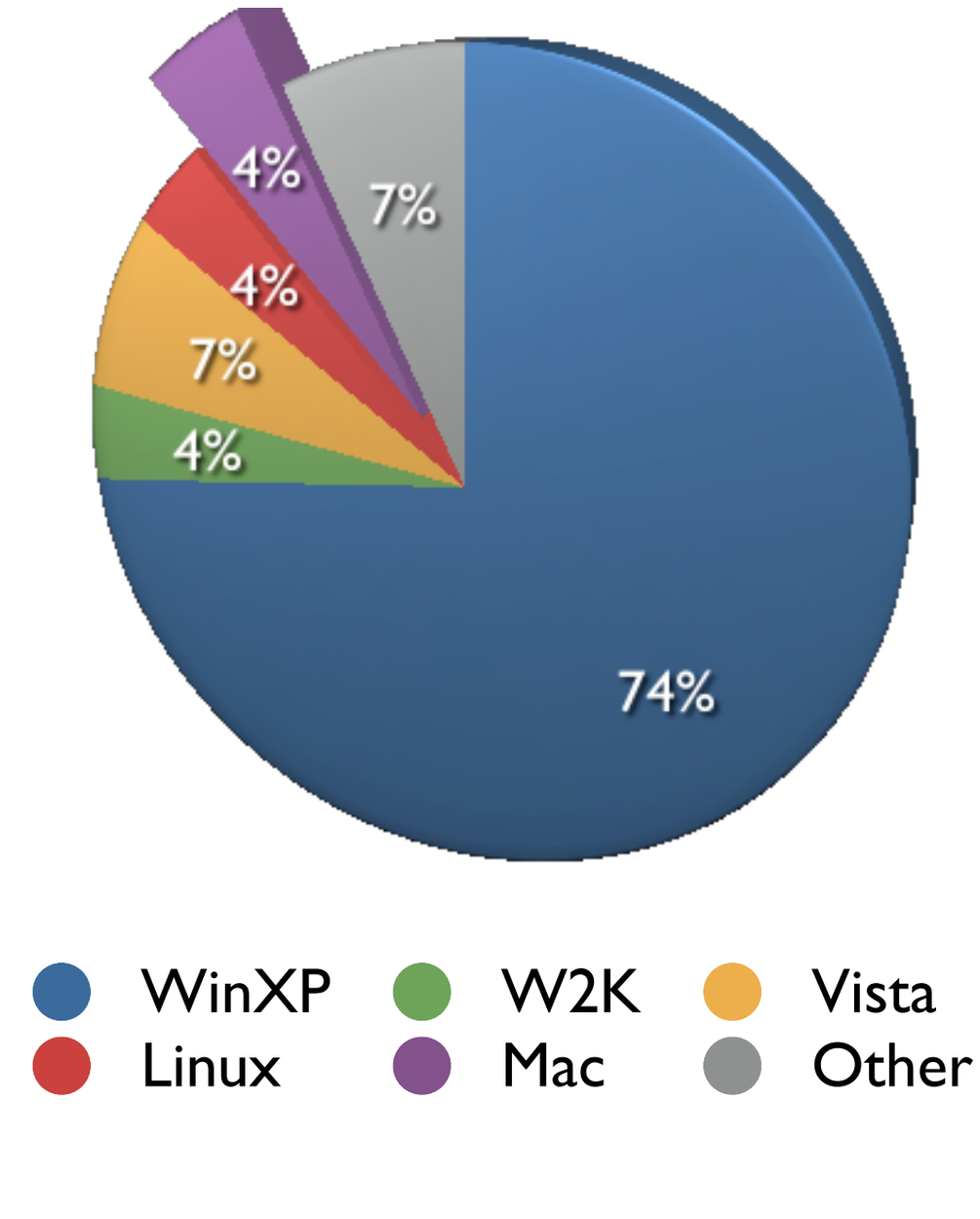
- Translation: Protection methods have to have effectiveness rates around the same level as the market penetration of *A* to make attacking *B* viable.

- Translation: Protection methods have to have effectiveness rates around the same level as the market penetration of PC to make attacking Macs viable.

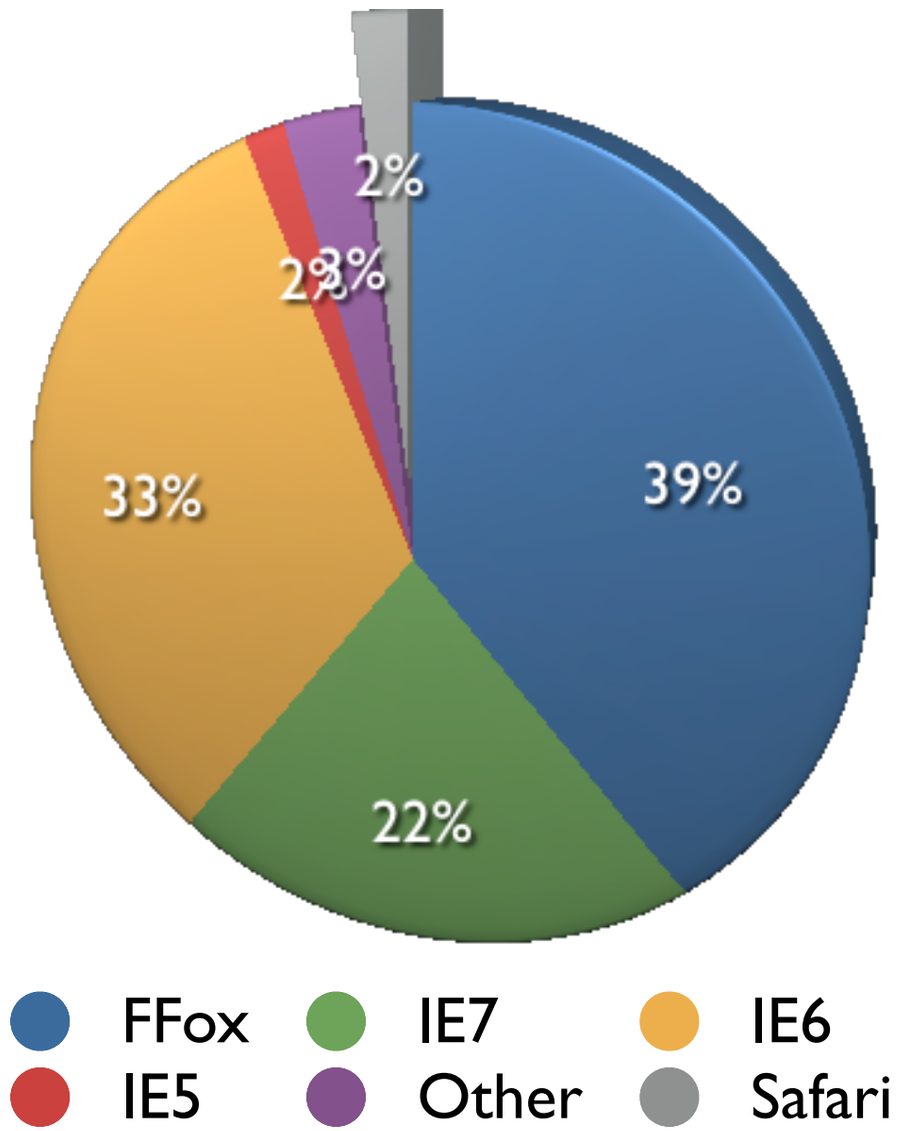
Real Data!

CLOUDMARK®

OS Share



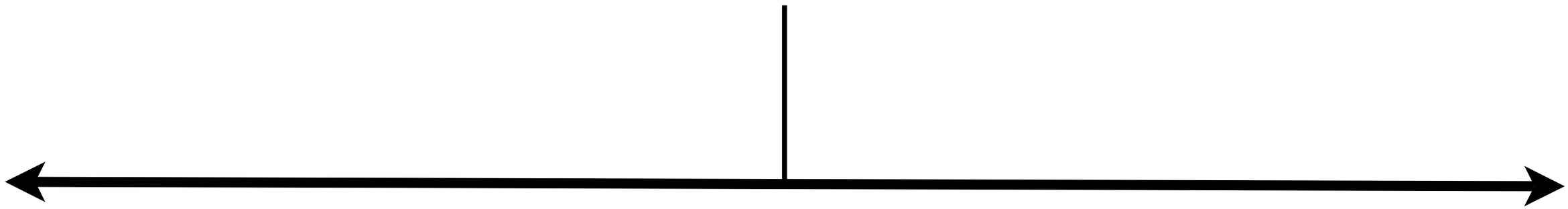
Browser Share



- PCs outnumber Macs 20, 25 to 1
- At that rate, protection mechanisms focused on PCs need to be better than 95% effective to make it worthwhile to attack Macs en-masse

Bottom Line?

I expect relatively wide-spread, monetized Mac malware when we see around 5-10% of the Internet population using Macs.



CLOUDMARK®

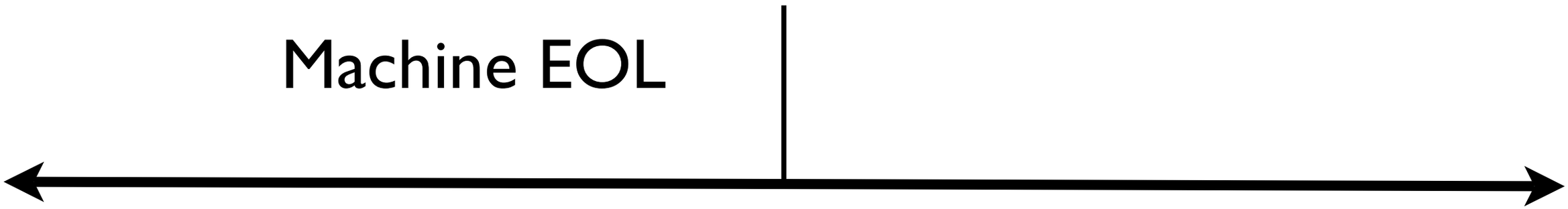
Cleanup Services

Better AV

More Macs

Competitive Malware

Machine EOL



More likely...

Less likely...

CLOUDMARK®

Cleanup Services

Efficient Malware Market

Better AV

More Macs

Recession

Competitive Malware

Machine EOL

Targeted & Zero Day Attack Effectiveness

More likely...

Less likely...

CLOUDMARK®

Predicting Emerging Threats

CLOUDMARK®

		Defend	
		A	B
Attack	A	$(1-p)fv$	fv
	B	$(1-f)v$	$(1-p)(1-f)v$

		Defend	
		E-Mail	Social Networks
Attack	E-Mail	$(1-p)fv$	fv
	Social Networks	$(1-f)v$	$(1-p)(1-f)v$

CLOUDMARK®

		Defend	
		E-Mail	SMS
Attack	E-Mail	$(1-p)fv$	fv
	SMS	$(1-f)v$	$(1-p)(1-f)v$

CLOUDMARK®

		Defend	
		MySpace	Facebook
Attack	MySpace	$(1-p)fv$	fv
	Facebook	$(1-f)v$	$(1-p)(1-f)v$

		Defend	
		Twitter	Qwigibo
Attack	Twitter	$(1-p)fv$	fv
	Qwidgibo	$(1-f)v$	$(1-p)(1-f)v$

CLOUDMARK®

		Defend	
		Twitter	Qwigibo
Attack	Twitter	$(1-p)fv$	fv
	Qwidgibo	$(1-f)v$	$(1-p)(1-f)v$

CLOUDMARK®

What is "*v*"?

The value of a given target is defined by how much value an attacker can extract over time

CLOUDMARK®

“*v*” defined by rate of...

CLOUDMARK®

“*v*” defined by rate of...

User response

Message generation

"*v*" defined by rate of...

User response

Message generation

Account creation/cost

Target market

CLOUDMARK®

“*v*” defined by rate of...

Network size

User response

Message generation

Account creation/cost

Target market

Number of contactable users

CLOUDMARK®

Will making these factors less appealing to attackers kill the business growth?

What is the proper balance between utility and security in an emergent technology?

What is the next target?

When Malware Attacks (anything but Windows)!(?)

Adam J. O'Donnell, Ph.D.
Cloudmark, Inc.
adam@cloudmark.com
http://np-incomplete.com

CLOUDMARK®