Analyzing Malware Detection Effectiveness with Multiple Anti-Malware Programs

Jose A. Morales
SEI @ CMU

Shouhuai Xu
CS @ UTSA

Ravi Sandhu
ICS @ UTSA

Roadmap

- ❑ Motivation
- ❑ Experimental Methodology
- ❑ Experimental Results
- ❑ Summary

Motivation

- We all are victims of computer malware.
- We all use anti-malware programs.
- Most of us, if not all, use a single anti-malware program (for economic reason).

Motivation (cont.)

- Is one anti-malware program sufficient?
- If not, how many?
- How critical is it to install anti-malware program in clean state?

The Ideal

- Ideally, an anti-malware program can detect and clean all malwares in a system (undecidability!)
- An anti-malware program C_1 is competent if for every input $S=S_0$ it holds that after applying C_1, no others can detect any more malware.

$$(\mathrm{DT}(C_1(S_0))=T)\wedge(\mathrm{DT}(C_2(S_1))=F)\wedge\ldots\wedge(\mathrm{DT}(C_n(S_{n-1})=F)$$

- Caveat: What is the ground truth?

The Reality

- The above idea can be extended to multiple programs that work collectively.
- Incompetence can be caused by
  - Incompetent detection
  - Incompetent cleaning up

Experiment 1: Install Anti-Malware Programs in Clean State

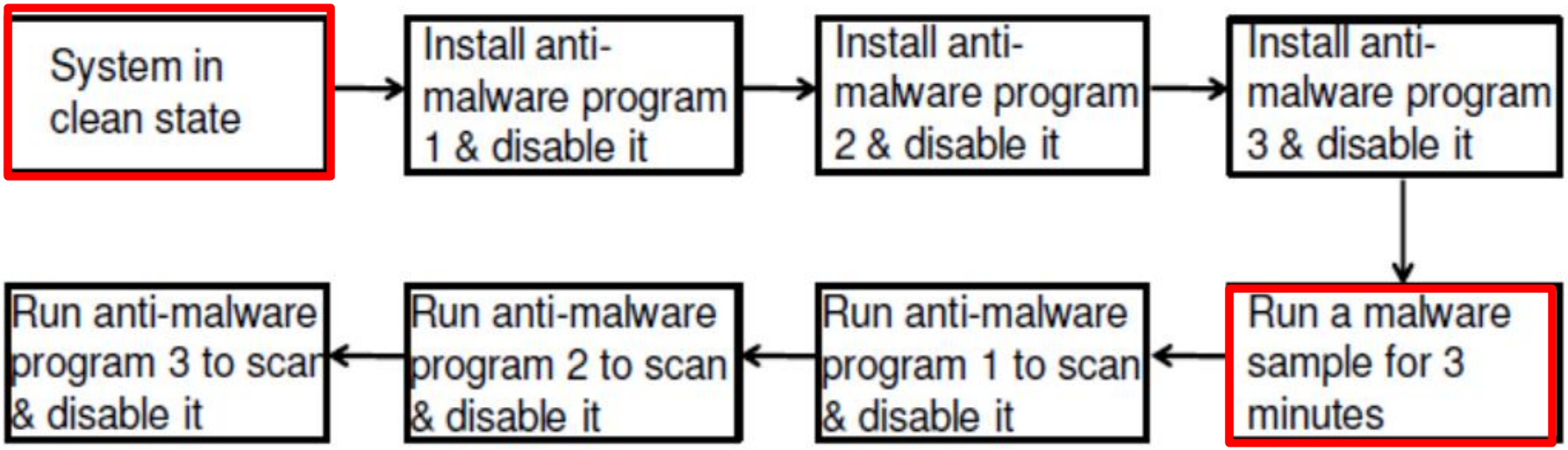

Fig. 2: Experiment 1 steps

Caveat: some malware may not do bad things until after running for more than 3 minutes or upon detecting the presence of VM

Experiment 2: Install Anti-Malware Programs in Possibly Compromised State

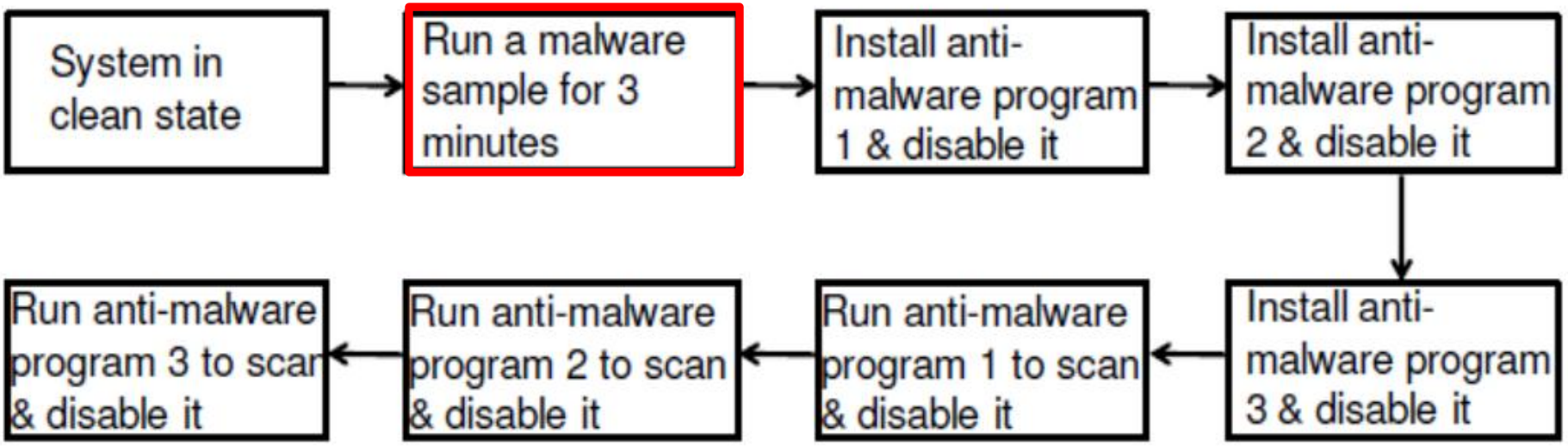

Fig. 3: Experiment 2 steps

Caveat: some malware may not do bad things until after running for more than 3 minutes or upon detecting the presence of VM

Experiments Setup

- Tested two sets of 3 anti-malware programs:
  - 1st set: ESET, AVG, Zonealarm
  - 2nd set: Kaspersky, G-data, Bitdefender
- Tested all permutations of each set: 3!=6
- Experiments carried out in Vmware
  - Running Windows 7 OS freshly installed to assure clean-state environment

Experiments Setup (cont.)

- 500 malware samples
  - worms, rootkits, bots, backdoors, password stealers, malware downloaders

Experimental Results

Scanning permutation	SDT($C_1(\cdot)$)	SDT($C_1 \wedge C_2$)	SDT($C_1 \wedge C_2 \wedge C_3$)
EAZ	487	13	0
EZA	488	8	4
ZEA	500	0	0
ZAE	500	0	0
AEZ	494	6	0
AZE	493	5	2
KGB	500	0	0
KBG	500	0	0
GBK	497	0	3
GKB	494	6	0
BKG	493	6	1
BGK	494	2	4

Table 3: Experiment 1 results for SDT($C_1 \wedge ... \wedge C_n$)

- Using multiple anti-malware programs does increase detection and cleaning up capability, despite some kind of diminishing return
- Sometimes 3 anti-malware programs may not be sufficient (need to be verified by 4th anti-malware program)

Among the 500 malwares, the numbers of malwares detected & cleaned by the anti-malware programs.

Experimental Results

Scanning permutation	SDT($C_1(\cdot)$)	SDT($C_1 \wedge C_2$)	SDT($C_1 \wedge C_2 \wedge C_3$)
EAZ	180	64	128
EZA	190	43	161
ZEA	86	157	102
ZAE	106	71	251
AEZ	251	98	31
AZE	207	49	126
KGB	403	57	21
KBG	412	38	9
GBK	302	76	57
GKB	239	146	102
BKG	298	104	31
BGK	287	116	92

Table 5: Experiment 2 results for SDT($C_1 \wedge ... \wedge C_n$)

- Make sure anti-malware program installed in clean state
- Anti-malware program installed in already compromised systems have high false-negatives
- Tested anti-malware progams seem to lack a self-defense mechanisms
- Malware running in a system may block access to resources needed by anti-malware

Among the 500 malwares, the numbers of malwares detected & cleaned by the anti-malware programs.

How Many Anti-Malware Tools Are Sufficient?

- Based on experimental results (based on 500 malware samples only):
  - 1 is occasionally ok
  - 2 minimum for low protection
  - 3+ for medium+ protection

Summary

- Current individual anti-malware programs do not provide sufficient protection
  - Despite some anti-malware programs worked well with the 500 malware samples
- Using multiple anti-malware programs together can improve protection
  - Need to test with much larger malware sets

The Challenge

- Implication: Current anti-malware technology is not sufficient
- We need revolutionary technology in combating malware
- We have to
- How?
- Things can be worse: Our another study showed that there are malwares that can evade perhaps all anti-malware programs

Thanks!

Questions or Comments?