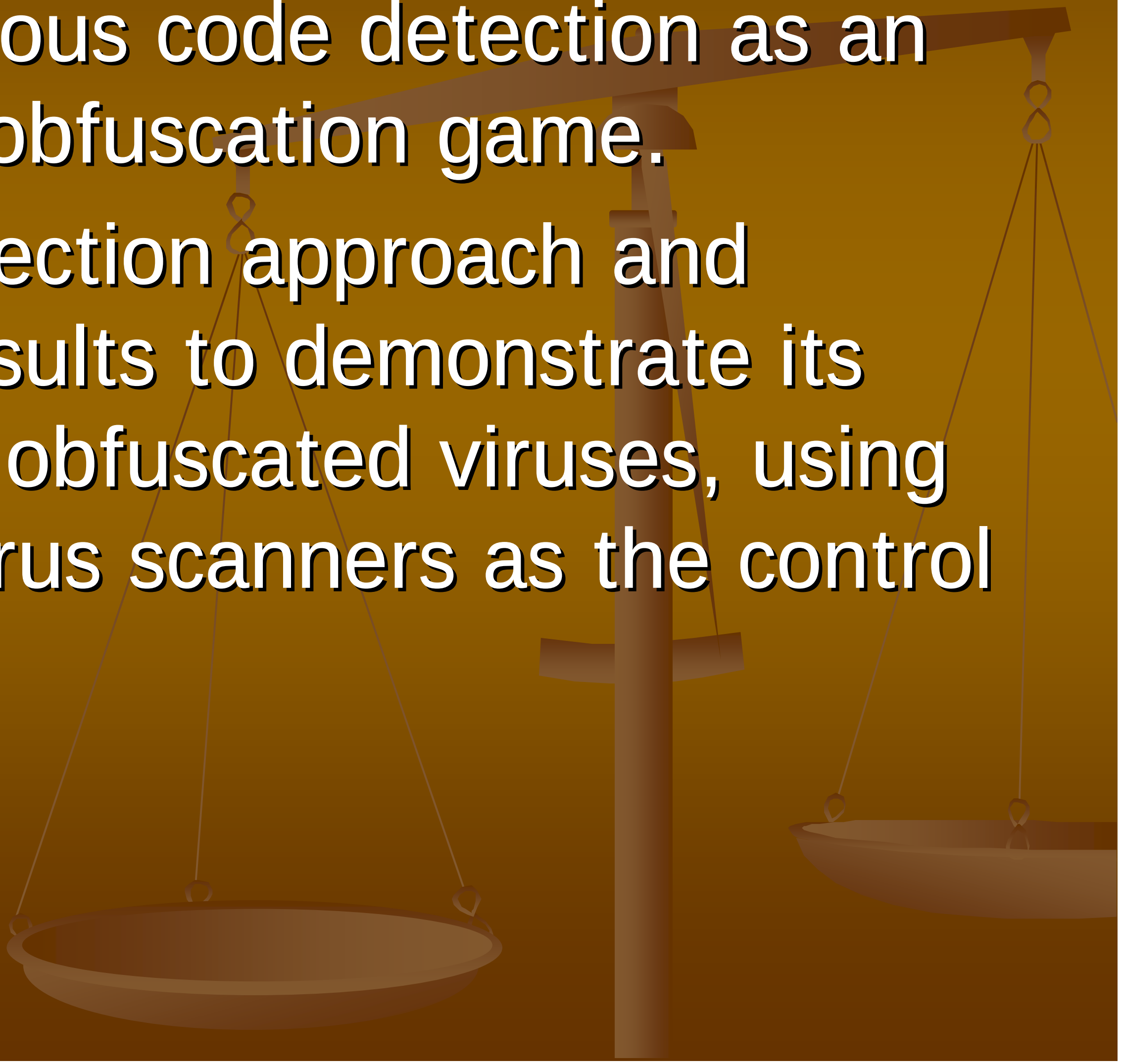
"Static Analysis of Executables to Detect Malicious Patterns", in *12th USENIX Security Symposium*, pp. 169-186, August 2003.

Christodorescu, M., Jha, S.
University of Wisconsin

Presented by
Gilbert Notoatmodjo
Auckland University

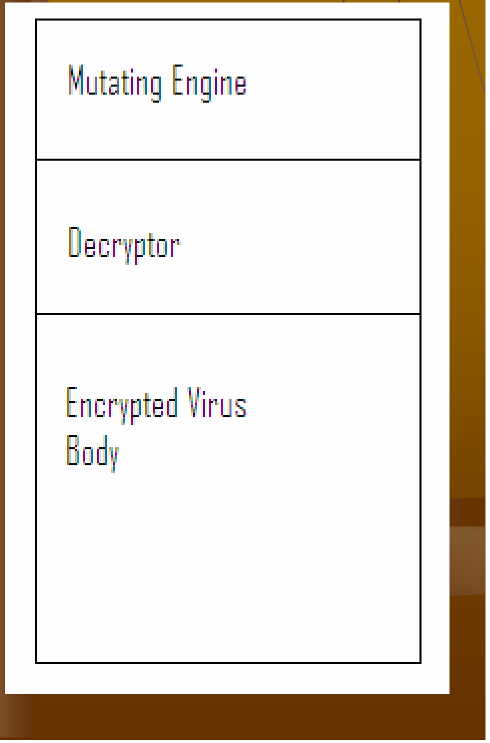
Summary

- Regarded malicious code detection as an obfuscation/ deobfuscation game.
- Presented a detection approach and experimental results to demonstrate its viability against obfuscated viruses, using 3 commercial virus scanners as the control group.



Polymorphic Virus

- Capable of changing its encryption key and obfuscating its decryptor using simple techniques (junk insertion, code transposition, etc) without any human interference.
- Uses mutating engines. There are many of these engines available. Every engine behaves differently.



Mutating Engine

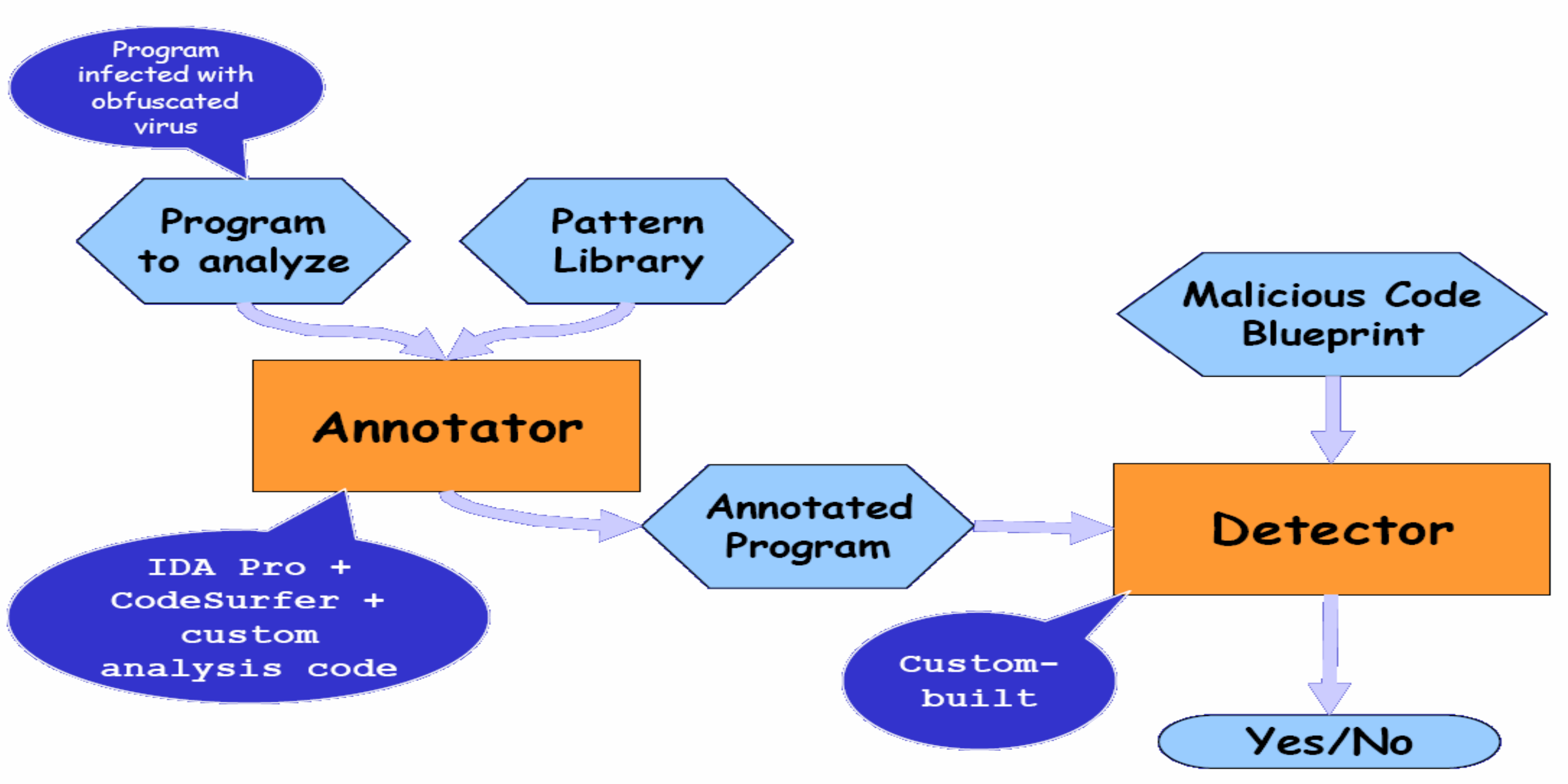
Decryptor

Encrypted Virus Body

How Do Virus Scanners Detect Polymorphic Viruses?

- Regular expression, heuristic analyses, emulation.
- Virus scanners normally rely on a database of known polymorphic viruses and their corresponding engines to perform the detection.
- Some of the methods used are not generic, since different engines have different weaknesses.

SAFE (Static Analyzer For Executables)

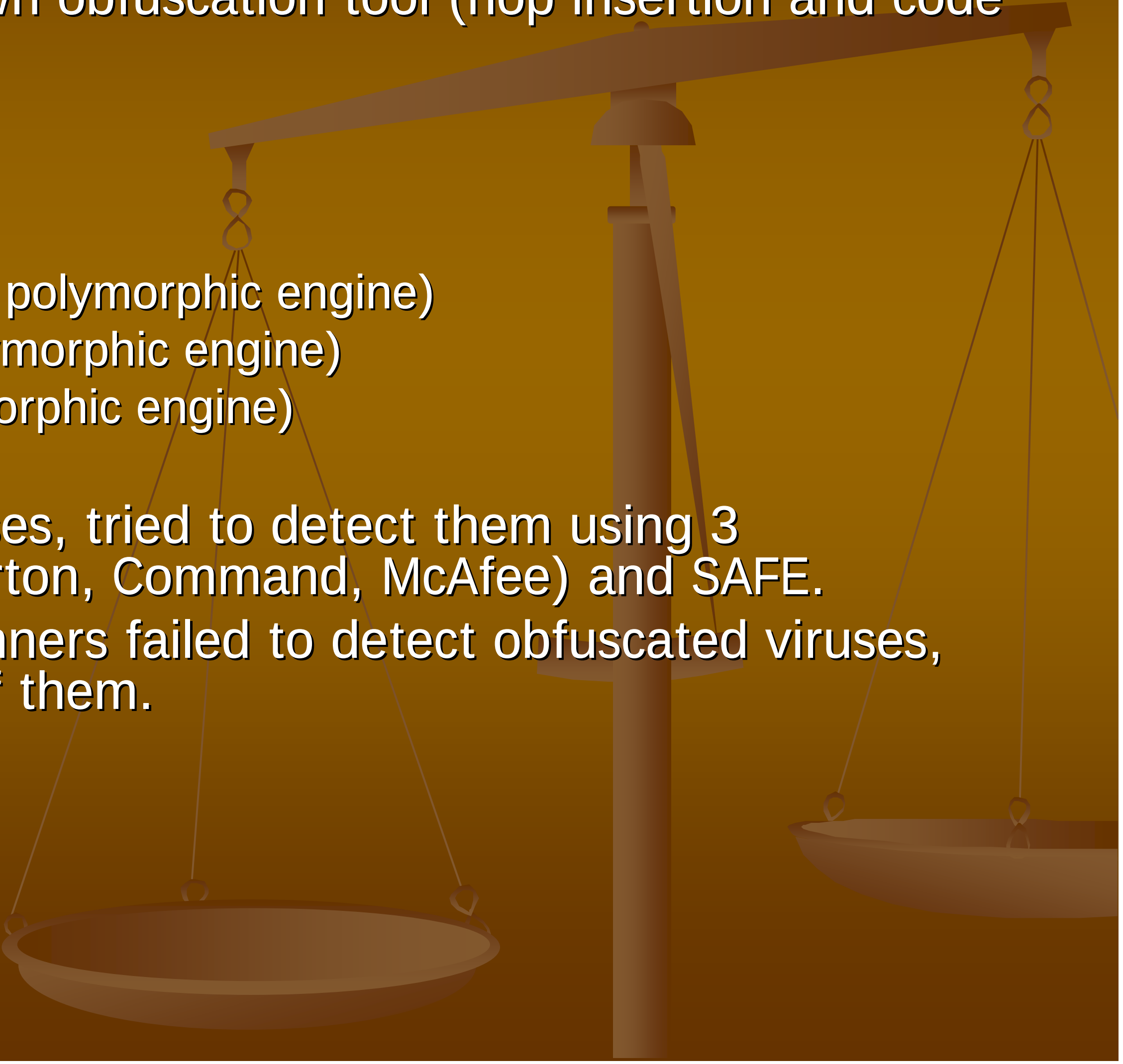


Taken from Static Analysis of Executables to Detect Malicious Patterns-USENIX Security'03 Presentation by Mihai Christodorescu. http://www.cs.wisc.edu/wisa/Presentations/2003/0807/mihai/safe-USENIX-sec03.pdf

Note that it also needs a blueprint for each virus

Experiment

- The authors used their own obfuscation tool (nop insertion and code transposition).
- 4 viruses were used:
  - Chernobyl/CIH
  - Zombie-6.b (has its own polymorphic engine)
  - f0sf0r0 (has its own polymorphic engine)
  - Hare (has its own polymorphic engine)
- They obfuscated the viruses, tried to detect them using 3 commercial scanners (Norton, Command, McAfee) and SAFE.
- Result: 3 commercial scanners failed to detect obfuscated viruses, while SAFE detected all of them.



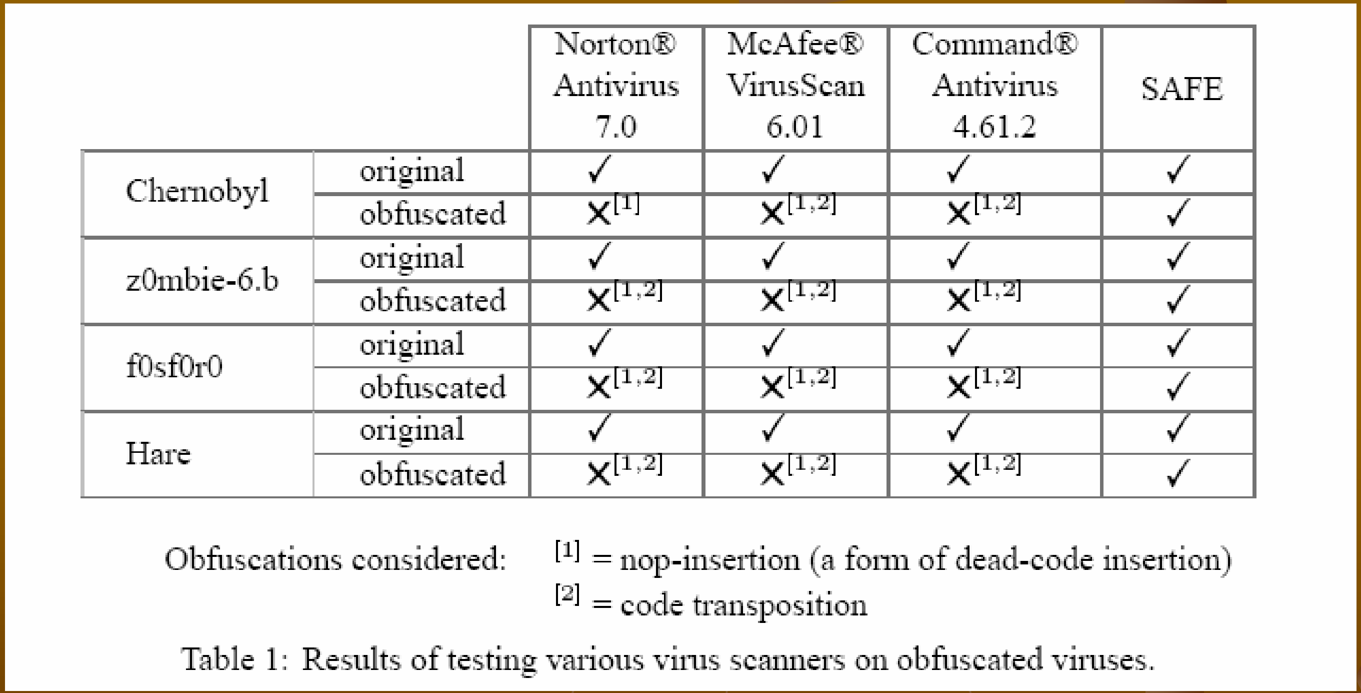
Appreciative Comments

- The paper presented a brief, yet thorough information on viruses, detection and obfuscation techniques, providing good background knowledge for the readers.

- The paper also pointed out the limitations of commercial virus scanners – caveat emptor.

Critical Comments

- Result presentation



		Norton® Antivirus 7.0	McAfee® VirusScan 6.01	Command® Antivirus 4.61.2	SAFE
Chernobyl	original	✓	✓	✓	✓
	obfuscated	✗[1]	✗[1,2]	✗[1,2]	✓
z0mbie-6.b	original	✓	✓	✓	✓
	obfuscated	✗[1,2]	✗[1,2]	✗[1,2]	✓
f0sf0r0	original	✓	✓	✓	✓
	obfuscated	✗[1,2]	✗[1,2]	✗[1,2]	✓
Hare	original	✓	✓	✓	✓
	obfuscated	✗[1,2]	✗[1,2]	✗[1,2]	✓

Obfuscations considered: [1] = nop-insertion (a form of dead-code insertion)
[2] = code transposition

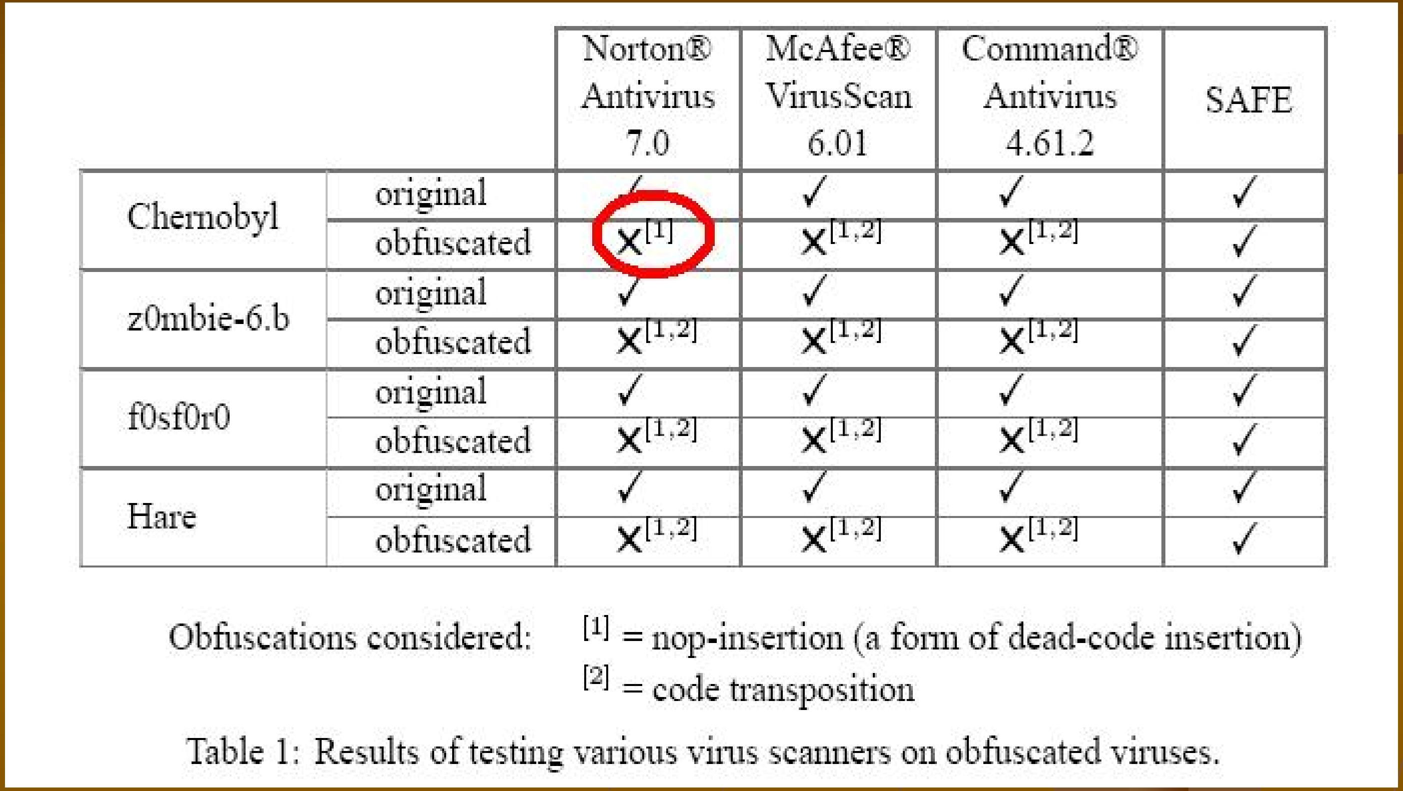
Table 1: Results of testing various virus scanners on obfuscated viruses.

Commercial antivirus can’t do anything against obfuscated viruses!

- "…The results were quite surprising: *a combination of nop-insertion and code transposition was enough to create obfuscated versions of the viruses that the commercial virus scanners could not detect*…Norton antivirus software could not detect an obfuscated version of the Chernobyl virus using just nop insertions. …Note that unobfuscated versions of all four viruses were detected by all the tools."

- Perception : commercial virus scanners are vulnerable to **any kind of obfuscation**, even the simple ones. In other words: "OH WOW this is CONTROVERSIAL, so these softwares are actually useless?!"

Try to look at the results from a different angle:



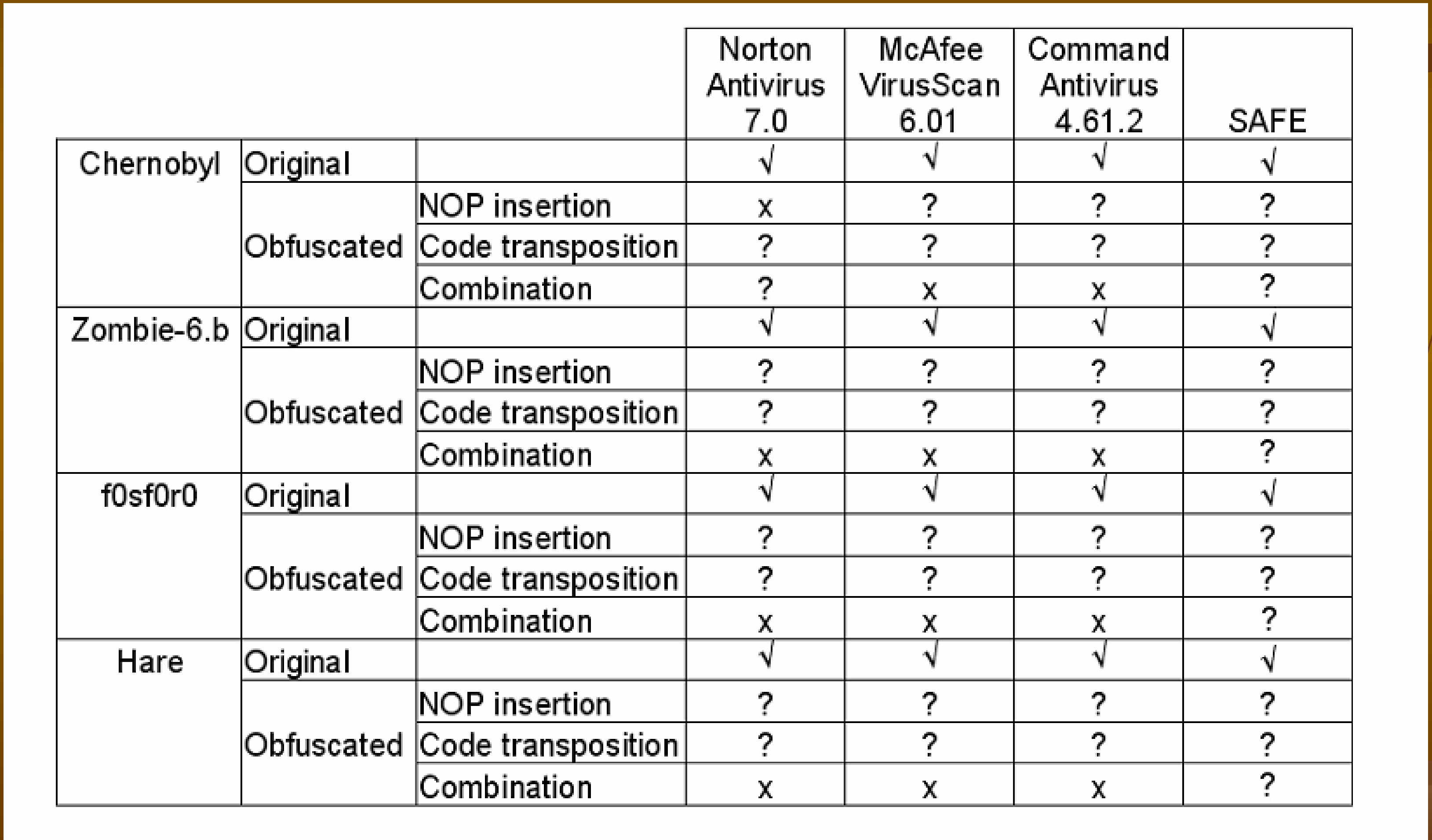
		Norton® Antivirus 7.0	McAfee® VirusScan 6.01	Command® Antivirus 4.61.2	SAFE
Chernobyl	original	✓	✓	✓	✓
	obfuscated	✗[1]	✗[1,2]	✗[1,2]	✓
z0mbie-6.b	original	✓	✓	✓	✓
	obfuscated	✗[1,2]	✗[1,2]	✗[1,2]	✓
f0sf0r0	original	✓	✓	✓	✓
	obfuscated	✗[1,2]	✗[1,2]	✗[1,2]	✓
Hare	original	✓	✓	✓	✓
	obfuscated	✗[1,2]	✗[1,2]	✗[1,2]	✓

Obfuscations considered: [1] = nop-insertion (a form of dead-code insertion)
[2] = code transposition

Table 1: Results of testing various virus scanners on obfuscated viruses.

Did they mention anything about using only nop insertion on the other commercial scanners? Did they actually try that?

The actual dataset?



			Norton Antivirus 7.0	McAfee VirusScan 6.01	Command Antivirus 4.61.2	SAFE
Chernobyl	Original		√	√	√	√
	Obfuscated	NOP insertion	x	?	?	?
		Code transposition	?	?	?	?
		Combination	?	x	x	?
Zombie-6.b	Original		√	√	√	√
	Obfuscated	NOP insertion	?	?	?	?
		Code transposition	?	?	?	?
		Combination	x	x	x	?
f0sf0r0	Original		√	√	√	√
	Obfuscated	NOP insertion	?	?	?	?
		Code transposition	?	?	?	?
		Combination	x	x	x	?
Hare	Original		√	√	√	√
	Obfuscated	NOP insertion	?	?	?	?
		Code transposition	?	?	?	?
		Combination	x	x	x	?

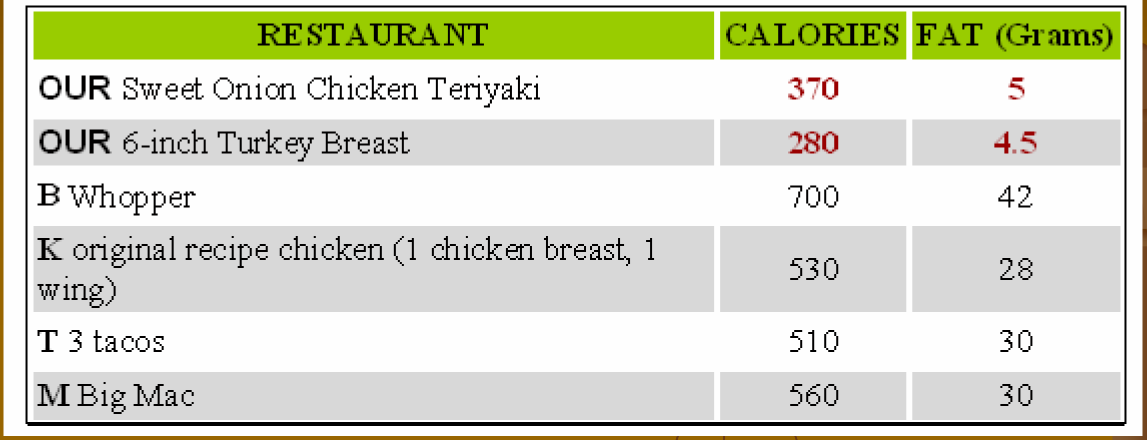
- “…The results were quite surprising: *a **combination** of nop-insertion and code transposition was enough to create obfuscated versions of the viruses that the commercial virus scanners could not detect*…Norton antivirus software could not detect an obfuscated version of the Chernobyl virus using just nop insertions. …Note that unobfuscated versions of all four viruses were detected by all the tools.”

- Didn’t say anything about ONE transformation.

- Did the antivirus softwares (except Norton) actually detect viruses that were obfuscated using ONLY nop insertion and ONLY code transposition?

Compare with:

- “Our sandwiches contain 6g of fat or less.”



RESTAURANT	CALORIES	FAT (Grams)
OUR Sweet Onion Chicken Teriyaki	370	5
OUR 6-inch Turkey Breast	280	4.5
B Whopper	700	42
K original recipe chicken (1 chicken breast, 1 wing)	530	28
T 3 tacos	510	30
M Big Mac	560	30

- (in almost illegible font) *"6 grams of fat or less“ only applies to 6-inch sandwiches, deli style sandwiches, and salads – a small fraction of their range of products. How about their footlong meatball sandwiches?

- ‘Partial truth’ might work for this advertising campaign, but would you expect this from an academic paper?

- Experiment Design

Commercial virus scanners rely on a list of polymorphic viruses and the corresponding engines to determine if a virus is polymorphic and therefore should be treated as a polymorphic.

The authors used their own obfuscation tool (engine, shall we say), whose behavior is obviously **unknown** to the scanners. REMEMBER, every engine behaves differently – three of the viruses have their own polymorphic engines.

SAFE was loaded with all blueprints that it needs to perform the detection successfully.

Given these facts, is it reasonable (in this scenario) to expect the antivirus softwares to match the performance of SAFE?