

Virus Writing Techniques

How lessons from the past can help us change the
direction of the malware arms race.

Tim Sally

tss@timsally.com

My Background

CS Undergrad



Past Intern

LOCKHEED MARTIN



Future Intern



Cyber Security Scholar



Undergrad RA

Center for Simulation of Advanced Rockets



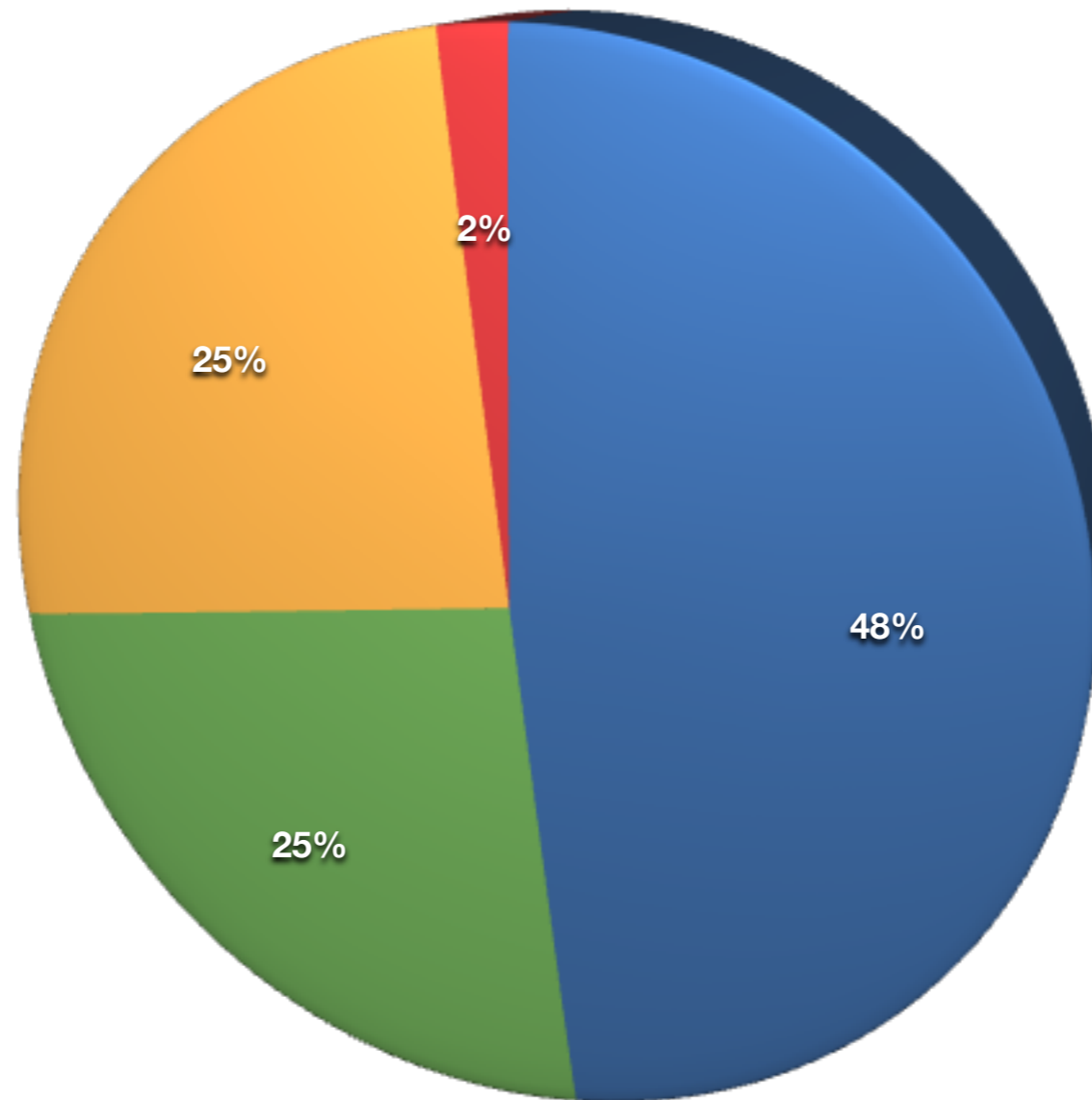
University of Illinois at Urbana-Champaign

The Next 45 Minutes

- ▶ Motivation
- ▶ Virus Writing 101
- ▶ New Tools!
- ▶ Evading AV (Demo)
- ▶ Wrap up

Motivation

Hate Chart



What's the Problem?

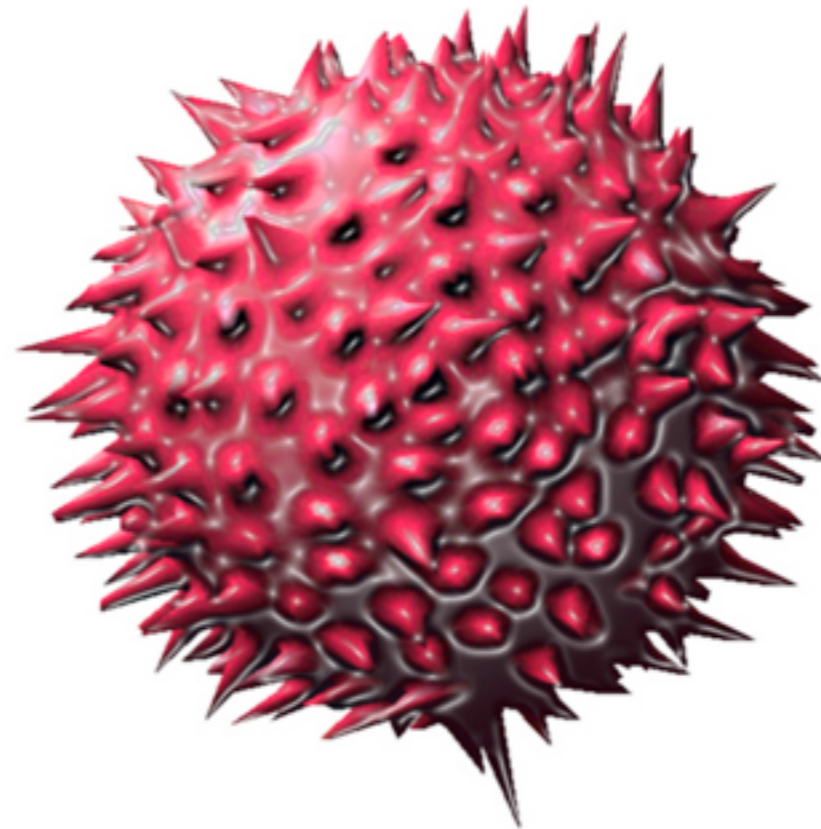
- ▶ AV marketing prevents average customers from making informed choices.
- ▶ Signatures are a Cold War approach to fighting malware.
- ▶ There is no “full disclosure” for AV.

AV Marketing

Bullets and Viruses: Serious Business



(C)2009 Daniel Austin Hoherd




<http://www.flickr.com/photos/warzauwynn/4191357929/>

<http://www.flickr.com/photos/ringai/3911794367/>

Protection: Body Armor and AV

Protection: Body Armor and AV



Body armor (chalecos blindados, chaleco antibalas) comes in all sorts of shapes and designs to fit your individual requirements and the level of protection you need. To understand the level of protection please refer to the bulletproof chart which details bullet calibers, speed per second etc.

Protection: Body Armor and AV

Body armor (chalecos blindados, chaleco antibalas) comes in all sorts of shapes and designs to fit your individual requirements and the level of protection you need. To understand the level of protection please refer to the bulletproof chart which details bullet calibers, speed per second etc.



AVG Internet Security 9.0

Complete protection for everything you do

We know when you go online you want to be able to surf, shop safely. With AVG Internet Security, our most advanced worry-free online experience every time. Internet Security's

Protection: Body

Armor and AV Part 2

Protection: Body Armor and AV Part 2

BODYARMOR.COM

No one bullet resistant vest works for everyone. There are a number of issues to consider when selecting body armor:

1. Ballistic resistance materials
2. Threat levels
3. Vest type (concealable vs. tactical body armor)

The information below will guide you in the process for choosing the right armor protection for your needs. For specific information, please visit one of

<http://www.bodyarmor.com/>

Protection: Body Armor and AV Part 2

BODYARMOR.COM

No one bullet resistant vest works for everyone. There are a number of issues to consider when selecting body armor:

1. Ballistic resistance materials
2. Threat levels
3. Vest type (concealable vs. tactical body armor)

The information below will guide you in the process for choosing the right armor protection for your needs. For specific information, please visit one of

<http://www.bodyarmor.com/>



Total Protection Advanced Service

- 1 Year Subscription
(from \$59.85 / License)
- 2 Year Subscription

Complete Desktop Protection
Website Protection
Risk and Compliance
Email Protection

<http://shop.mcafee.com/Products/TotalProtectionForSmallBusinessAdvanced.aspx>

This Is A Market Failure

If customers can't understand the
merits of products, the best product
will not win.

Lessons From The Cold War

Cold War: Build More Missiles



Growth of Malware: 2002-2008

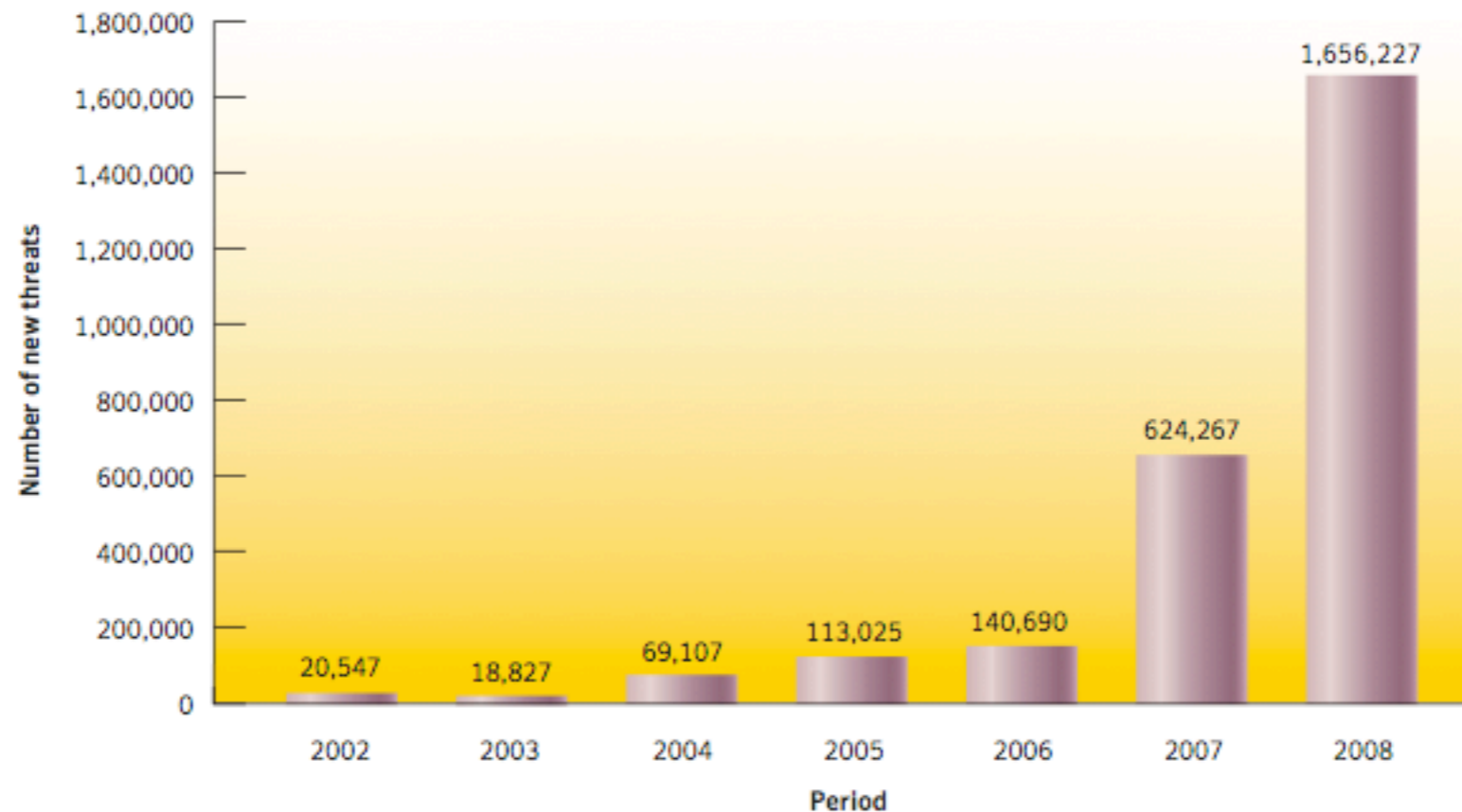


Figure 3. New malicious code threats
Source: Symantec

Growth of Malware:

~~2002-2008~~ ICBMS

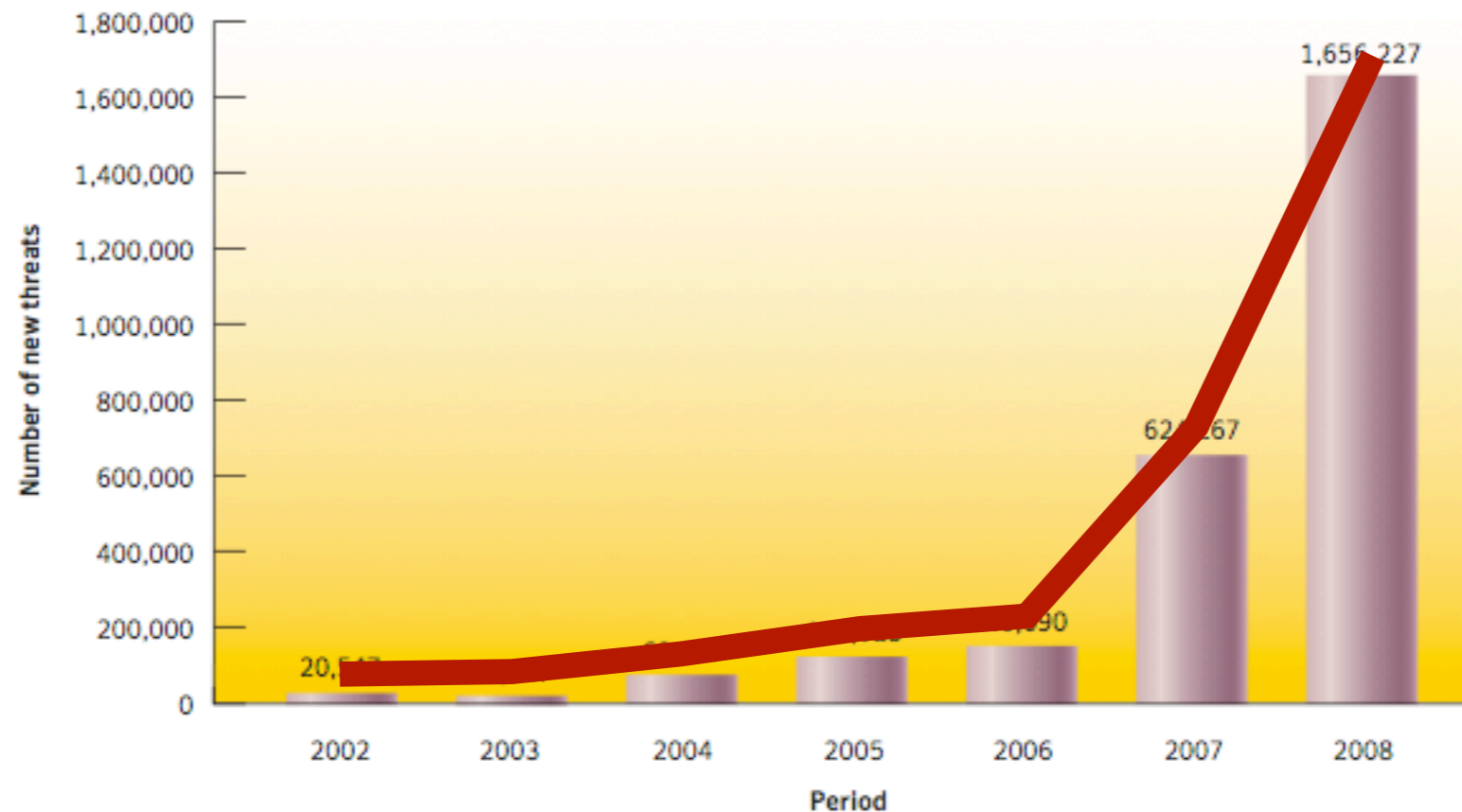


Figure 3. New malicious code threats
Source: Symantec

Cold War: How Did They Fix It?



Failed Solution: “Star Wars”



Successful Solution:

INF



How Can We Adjust
Our AV Approach?

Failed Solution: Malware Signatures

- ▶ One-for-one approach never works.
- ▶ The defensive tech is an order of magnitude harder than offensive tech.
- ▶ Historical track record of failure.

McAfee Incident

- ▶ “At 11 AM today, 4/21, McAfee released an update to its customers that improperly identified a critical component of Windows as having a virus.”

McAfee Incident

- ▶ “Roughly 800,000 PCs ... are not experiences repetitive reboots.”

McAfee Incident

- ▶ “NOTE: Your computer does not have a virus, but McAfee VirusScan incorrectly believes it does.”

∴ (

New (Old?) Solution:

Full Disclosure

- ▶ In part responsible for the gains in network and OS security since the 90's.
- ▶ Vendors can't afford to employ enough people, must involve public.
- ▶ In turn, vendors are held accountable.

Involving the Community Works

<input type="checkbox"/> ☆ Secunia Research (2)	Full Disclosure	Bugtraq	[Full-disclosure] Secunia Research: Bournal insecure temporary Files Security Issue - Secunia Res
<input type="checkbox"/> ☆ Secunia Research (2)	Full Disclosure	Bugtraq	[Full-disclosure] Secunia Research: Bournal ccrypt Information Disclosure Security Issue - Secunia I
<input type="checkbox"/> ☆ Ramos, Rohit (2)	Full Disclosure		[Full-disclosure] Nmap5 cheatsheet - Well, the Spanish translation is nice, but what does the English version I
<input type="checkbox"/> ☆ Kotas, Kevin J (2)	Full Disclosure	Bugtraq	[Full-disclosure] CA20100222-01: Security Notice for CA Service Desk - BEGIN PGP SIGNED MES:
<input type="checkbox"/> ☆ Karn Ganeshen	Full Disclosure		Re: [Full-disclosure] Oracle eBusiness Suite 11i - Cross Site Scripting - All Parameters - Hi, Specific to 11i, I h
<input type="checkbox"/> ☆ Jonathan .. T (13)	Full Disclosure		Re: [Full-disclosure] Why - Kafka's The *Trial. My sincere apologies. On Mon, Feb 22, 2010 at 12:51 PM, T Bi
<input type="checkbox"/> ☆ Marc Deslauriers	Full Disclosure		[Full-disclosure] [USN-902-1] Pidgin vulnerabilities - Ubuntu Security Notice USN-902-1 February 22, 2010 pi
<input type="checkbox"/> ☆ Major Malfunction	Full Disclosure		[Full-disclosure] London DEFCON February meet - DC4420 - Wed 24th Feb 2010 - I think we can safely say I
<input type="checkbox"/> ☆ Stephan Gerling	Full Disclosure		[Full-disclosure] Some nice code yust captured - Dear all, I just get a information by a scared user about some
<input type="checkbox"/> ☆ John .. Adam (6)	Full Disclosure		[Full-disclosure] How I become Vice President of Security at Yahoo! 1999-2005. - Let us not forget that this is
<input type="checkbox"/> ☆ Ofer Maor (2)	Full Disclosure	Bugtraq	[Full-disclosure] Hacktics Advisory Feb10: Persistent XSS in Microsoft SharePoint Portal - Hacktics I
<input type="checkbox"/> ☆ SEC Consult Research	Full Disclosure		[Full-disclosure] SEC Consult SA-20100208-0 :: Backdoor and Vulnerabilities in Xerox Wo... - SEC Consult S
<input type="checkbox"/> ☆ Roberto Suggi Liverani (2)	Full Disclosure	Bugtraq	[Full-disclosure] Multiple Adobe Products - XML External Entity And XML Injection Vulne... - _) .'),)
<input type="checkbox"/> ☆ Georgi, Jeff, Pavel (3)	Full Disclosure		[Full-disclosure] help fuzzing/finding Horn CNF formula - On Fri, 19 Feb 2010, Georgi Guninski wrote: > i am I
<input type="checkbox"/> ☆ Fernando Gont (2)	Full Disclosure	Bugtraq	[Full-disclosure] Request for feedback on TCP security (IETF effort) - Hello, folks, I've just posted a r
<input type="checkbox"/> ☆ security (2)	Full Disclosure	Bugtraq	[Full-disclosure] [MDVSA-2010:044] mysql - BEGIN PGP SIGNED MESSAGE Hash: SHA1 ...

There's No Public Red Team for AV!

- ▶ We have cryptanalysts.
- ▶ We have penetration testers.
- ▶ We have public disclosure of vulns.
- ▶ We DON'T have anything public for AV.

FD Implementation?

- ▶ Security community needs to help AV vendors.
- ▶ Produce open source tools to evaluate the effectiveness of existing AV.
- ▶ Good guys need to study virus writing techniques and publish results.

Virus Writing 101

Clumsy Evasion

- ▶ Encryption
- ▶ Anti-disassembly/Anti-debugging
- ▶ Virtualization detection
- ▶ Anti-anti-virus

Elegant Evasion

- ▶ Metamorphic techniques
- ▶ Binary \rightarrow Intermediate Representation (IR)
- ▶ Add/subtract from IR
- ▶ Perform transformations on IR
- ▶ IR \rightarrow Binary

Why It's Scary

- ▶ Takes some expertise to implement, but very difficult to detect.
- ▶ “Theoretically” accurate signatures are impossible.
- ▶ Bonus prize: better cross platform support than your average enterprise application!

Tools

Introducing **Parable**: A
Tool To Help The
Development of AV

Overview

- ▶ Based on Alessandro Warth's OMeta.
- ▶ Parser/transformer for assembly (currently only x86).
- ▶ Can be extended in an OO way.
- ▶ Extremely fast and flexible development.

Parser/Transformer

- ▶ Takes ASCII assembly in, writes ASCII assembly out.
- ▶ Disassembly and assembly of binaries are scripted.
- ▶ Transformations written in Ruby!

Extending With OO

- ▶ Parsing: random garbage instruction

```
meta x86++ <: x86 {  
    stmt ::= <space>* 'rand_garbage' => ...  
           | <super stmt>;  
}
```

Extending With OO

- ▶ Parsing: pluggable code modules

```
meta x86++ <: x86 {  
    stmt ::= <space>* 'encrypt_func' => ...  
           | <super stmt>;  
}
```

Extending With OO

- ▶ Transformation: pluggable code modules

```
'encrypt_func' => { gen_rand_encrypt()  
                    # just code normal Ruby!  
                    }
```

Current Capabilities

- ▶ Entry point obscuring.
- ▶ Instruction and method permutation.
- ▶ Attempt at data structure permutation and mimicking system binaries.

Demo

Caveats

- ▶ Not a true metamorphic engine.
- ▶ Could be implemented in C/x86....
- ▶ Ruby implementation deters plug and play script kiddies.

Caveats II

- ▶ Complete evasion is not the goal.
- ▶ Just need to make signature based detection completely impractical.
- ▶ Provide a testbed for experimentation for AV vendors and security professionals.

Wrapping Up

Related Tool: SLIPFEST

- ▶ SLIPFEST (<http://slipfest.cro.org/>)
- ▶ HIPS Evaluation, similar motivation
- ▶ Difference: *AV* isn't a strict target

Related Tool: Metasm

- ▶ Metasm (<http://metasm.cro.org/>)
- ▶ Binary file manipulation
- ▶ Pure Ruby!
- ▶ Difference: Parable focuses on rapid development and offensive testing.

Final Thoughts

- ▶ Security community at large can help make *AV* stronger.
- ▶ We need to adopt the same standards for *AV* that we have in every other area.

Thanks!

[http://www.timsally.com/talks/
thotcon0x1.html](http://www.timsally.com/talks/thotcon0x1.html)

Code, slides, notes, links, papers, etc!