



Rugged Software Development

Joshua Corman, David Rice, Jeff Williams

12th Semi-Annual Software Assurance Forum

March 11, 2010

Who am I?

- **Research Director for Enterprise Security, The 451 Group**

Joined The 451 Group on Oct 2009

12 years in Networking and Security

- Former Principal Security Strategist [IBM ISS]
- Sold stealth start-up vCIS to ISS in 2002

Industry Leadership

- Expert Faculty - The Institute for Applied Network Security (IANS)
- Co-Founder: “Rugged” www.ruggedsoftware.org

Things I’ve been researching:

Compliance vs Security

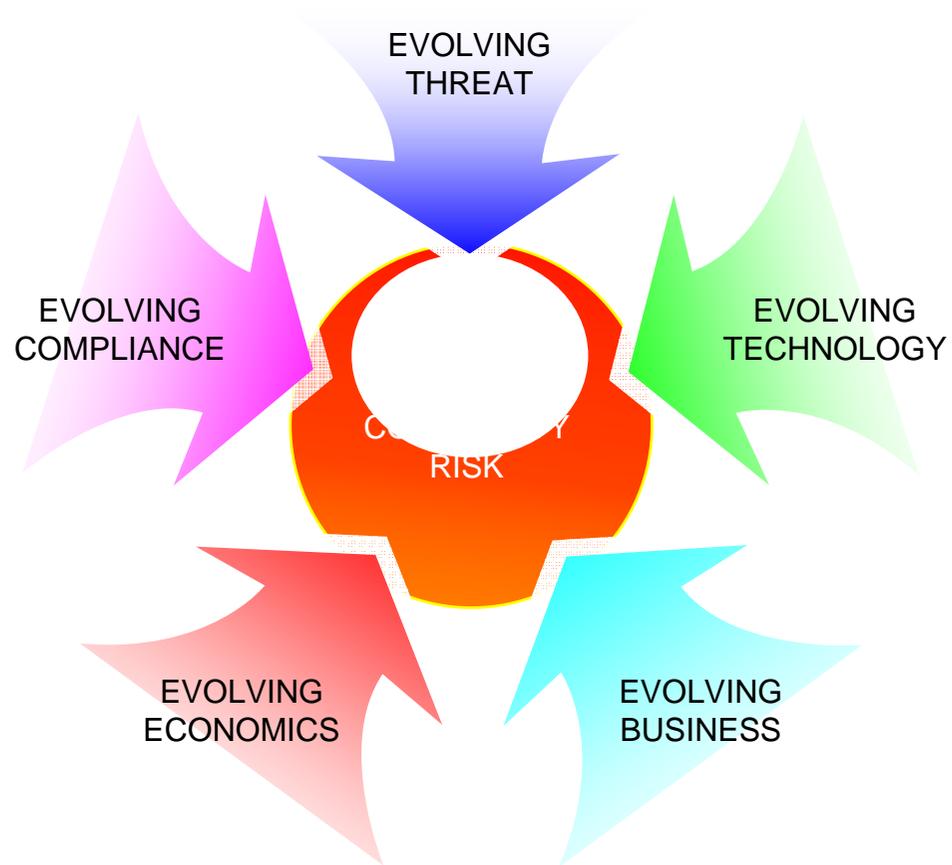
Virtualization and Cloud Computing

The Economics of Security

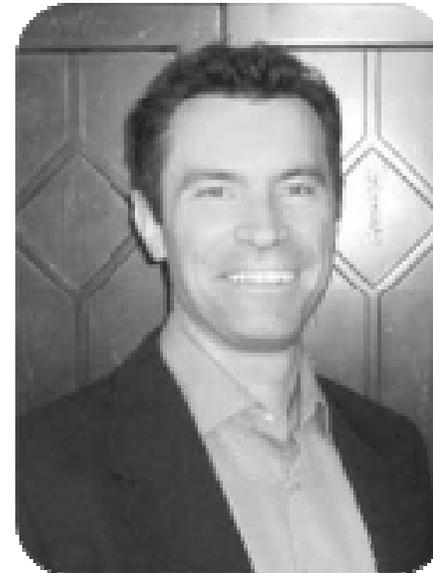
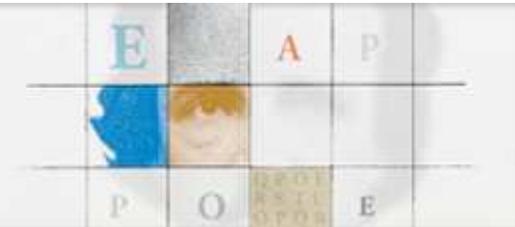
Politically Motivated Cyber (APT/APA/SMT)

Comprehensive Data Security

Context



USA 2009 20-24 April | Moscone Center | San Francisco





“What is missing from software security?”

CULTURAL INFORMATION

PRACTICE OR **IDEA** OR CONCEPT

THEORIES PRACTICES HABITS SONGS

NATURAL SELECTION

EXAMPLES MIGHT INCLUDE THOUGHTS IDEAS

CHARLES DARWIN'S IDEAS

SELF-PROPAGATING

SURVIVAL AND COMPETITION INFLUENCE THEM

MEME



PIRATES ARE ATTACKING U.S. SHIPS OFF THE COAST OF AFRICA. THEY'VE BROKEN THE 100 YEAR TRUCE.

WHO, THE PIRATES?

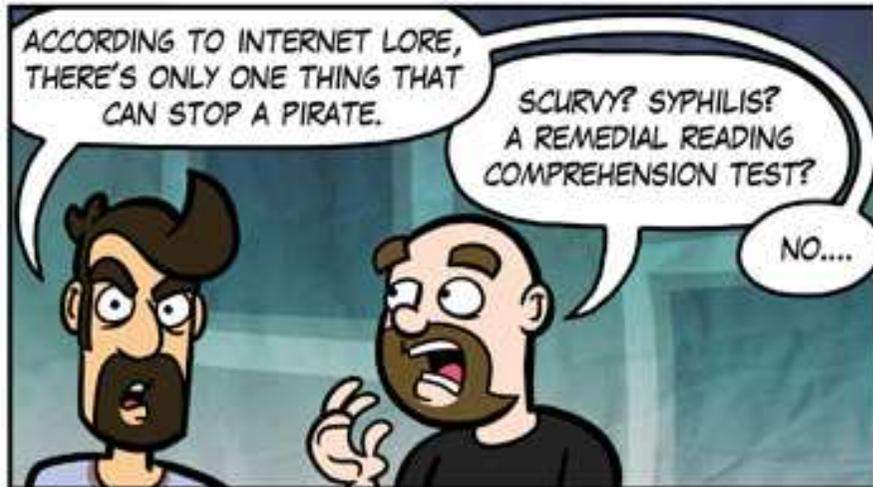
NO, THE INTERNET MEMES.



IT STARTS WITH PIRATES. THEN THE ZOMBIES AND THE UNICORN RIDING ROBOTS.

THE NEXT THING YOU KNOW, BLOOD THIRSTY LOLCATS ARE JUMPING OUT OF ROFLCOPTERS AND OM NOMNOMING OUR TRACHEAS.

DO NOT WANT!



ACCORDING TO INTERNET LORE, THERE'S ONLY ONE THING THAT CAN STOP A PIRATE.

SCURVY? SYPHILIS? A REMEDIAL READING COMPREHENSION TEST?

NO....



NINJAS!

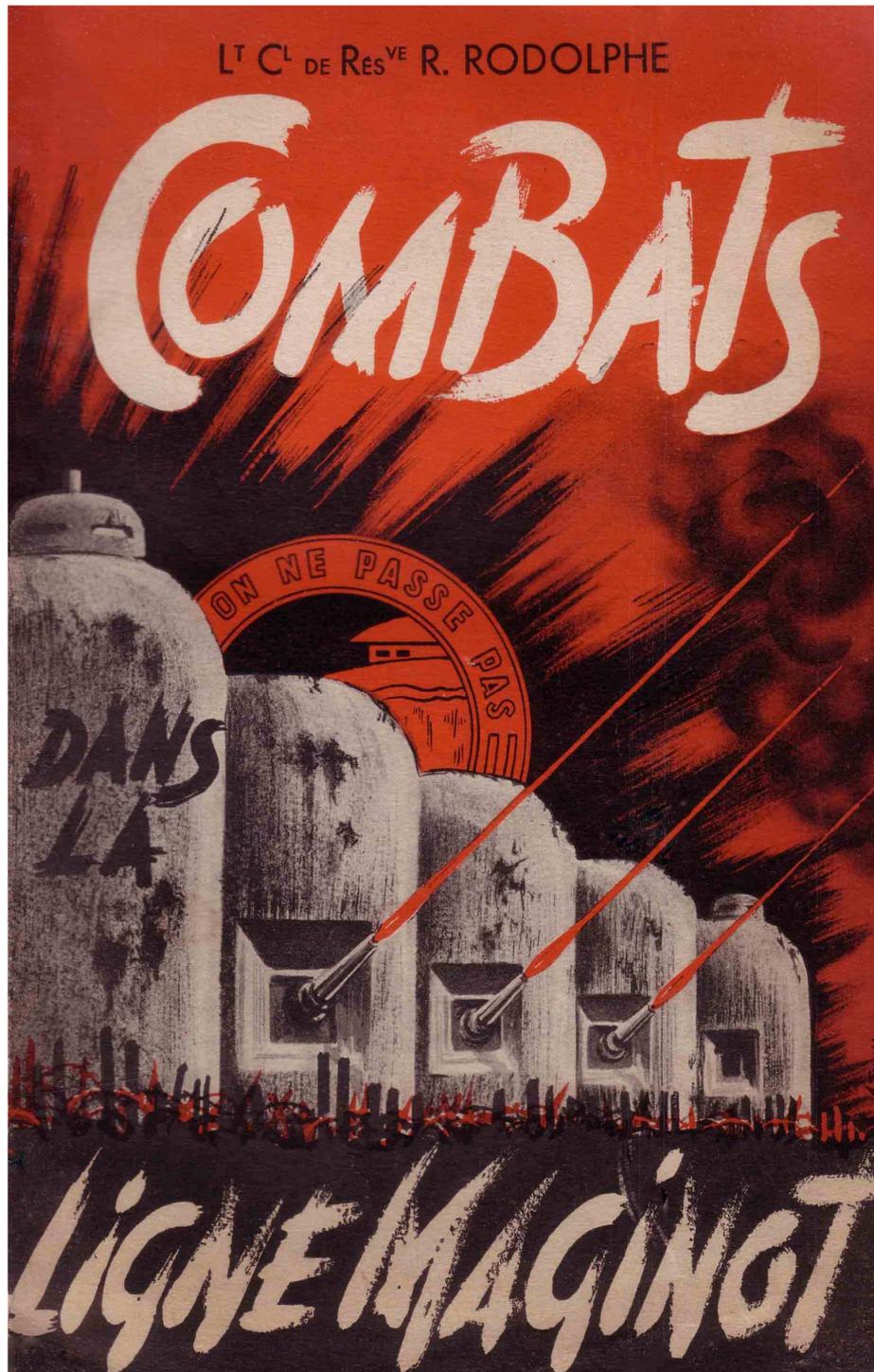
MY THROWING STARS, LET ME SHOW YOU THEM.

I WAS LATE. WHY ARE WE DOING THIS?



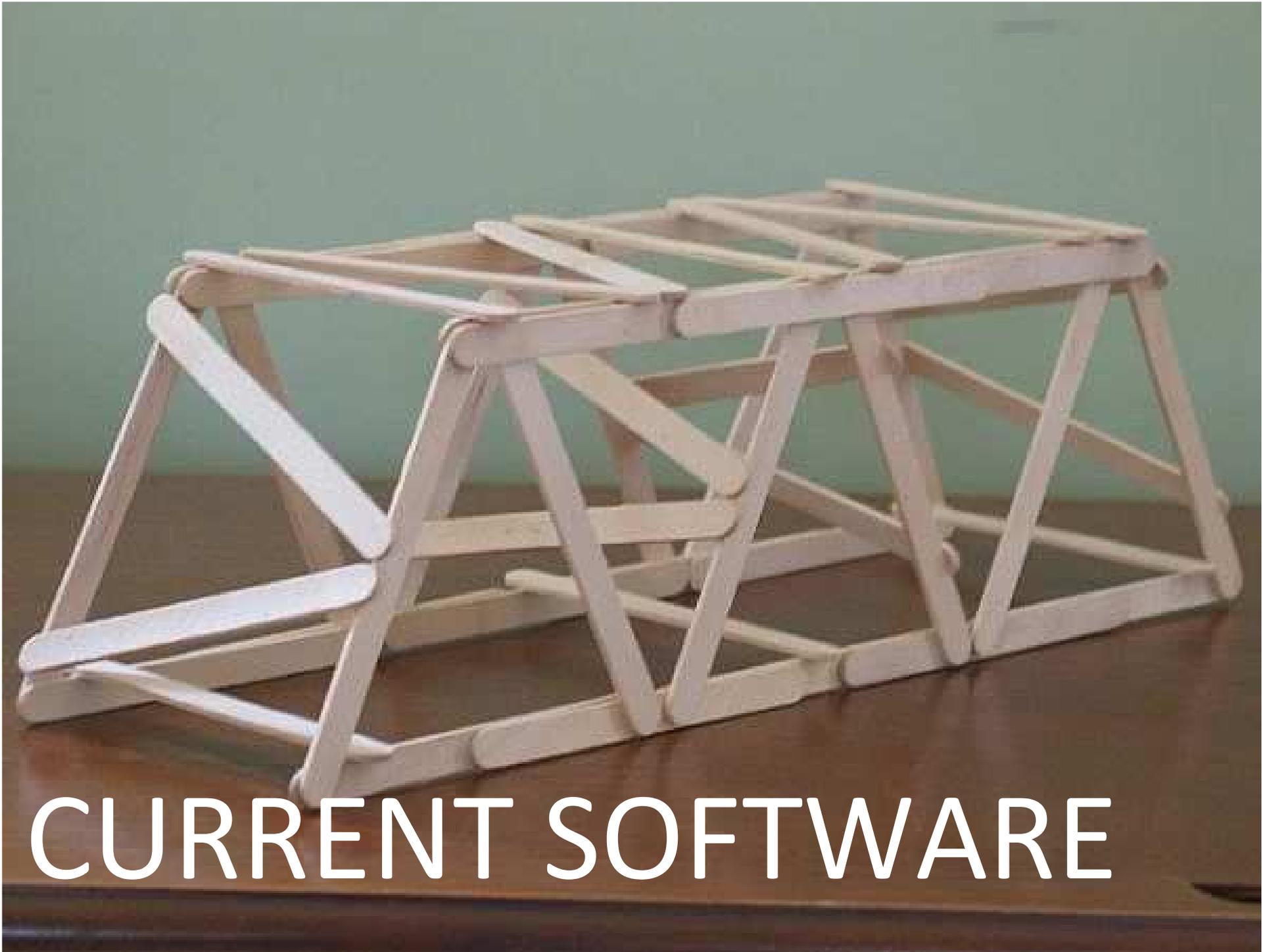
Secure software is critically important to almost every aspect of life.





“A fortress mentality will not work in cyber. **We cannot retreat behind a Maginot Line of firewalls...**If we stand still for a minute, our adversaries will overtake us.”

-William Lynn, U.S. Deputy Secretary of Defense
January 2010





RUGGED SOFTWARE

CURRENT SOFTWARE



Boulanger



RUGGED SOFTWARE



CURRENT SOFTWARE



RUGGED SOFTWARE

...so software not only needs to
be...



FAST

AGILE



AAI

ELITE™ VISA



Are You Rugged?



HARSH



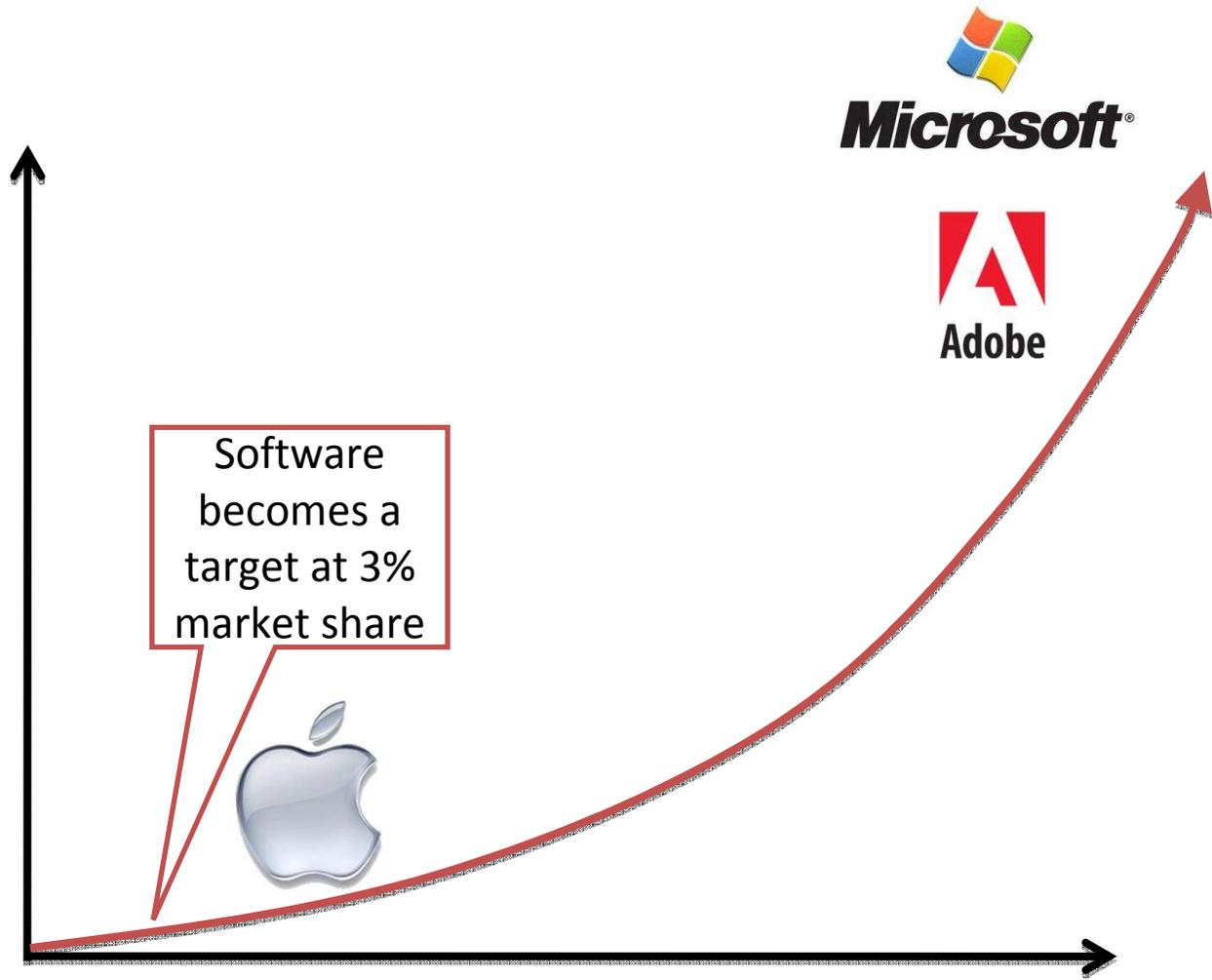
There is no such thing
as “toy” software.

ATTACKER'S
INTEREST

Software
becomes a
target at 3%
market share



Market Share



THE MANIFESTO

I am rugged - and more importantly, my code is rugged.

I recognize that software has become a
foundation of our modern world.

I recognize the awesome responsibility that comes with this foundational role.

I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.

I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic, and national security.

I recognize these things - and I choose to be
rugged.

I am rugged because I refuse to be a source of vulnerability or weakness.

I am rugged because I assure my code will
support its mission.

I am rugged because my code can face these challenges and persist in spite of them.

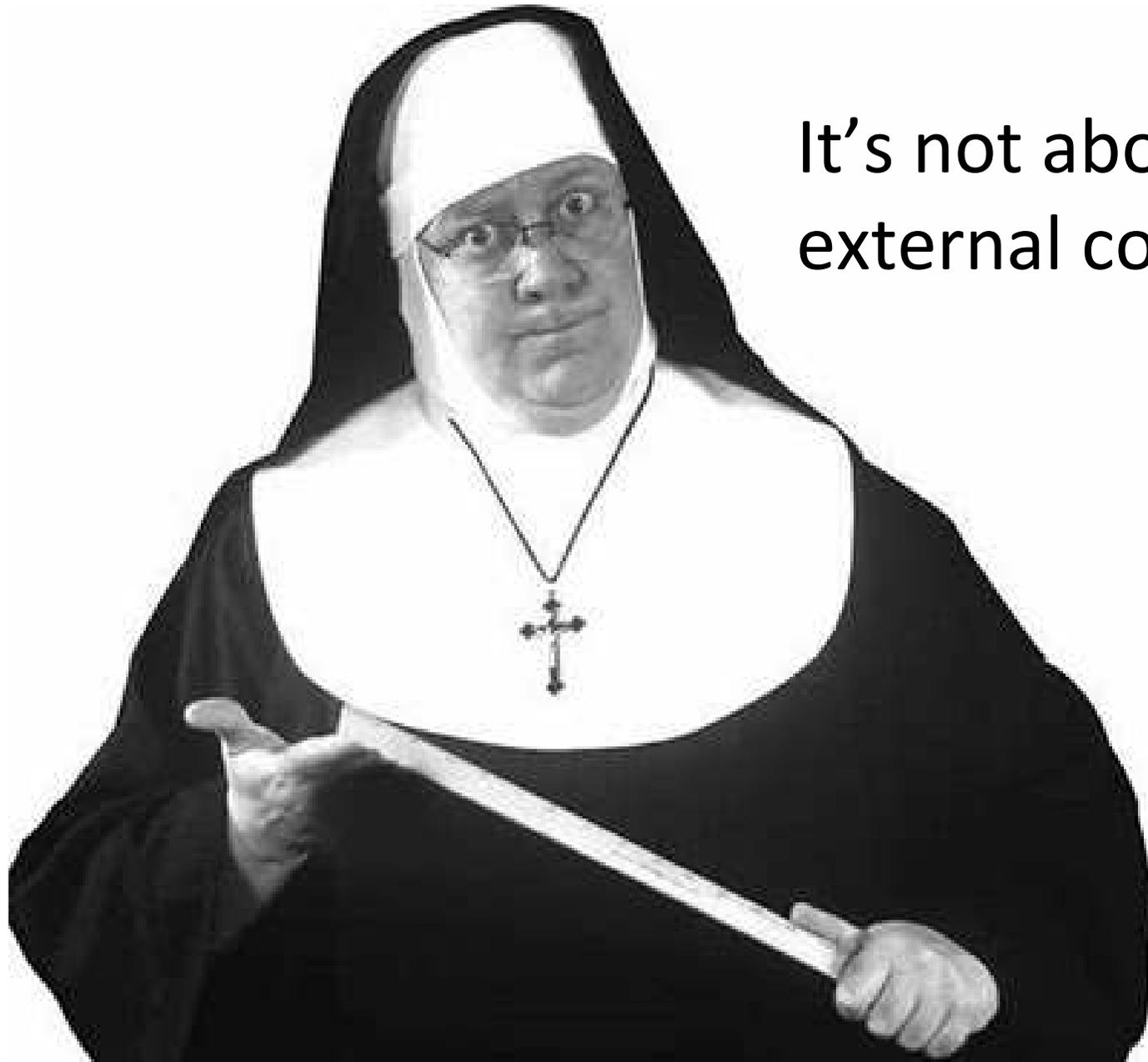
I am rugged, not because it is easy, but because it is necessary... and I am up for the challenge.

Rugged?

WHAT IS RUGGED?



It's not about style, it's about the result.



It's not about
external compliance...

RULES

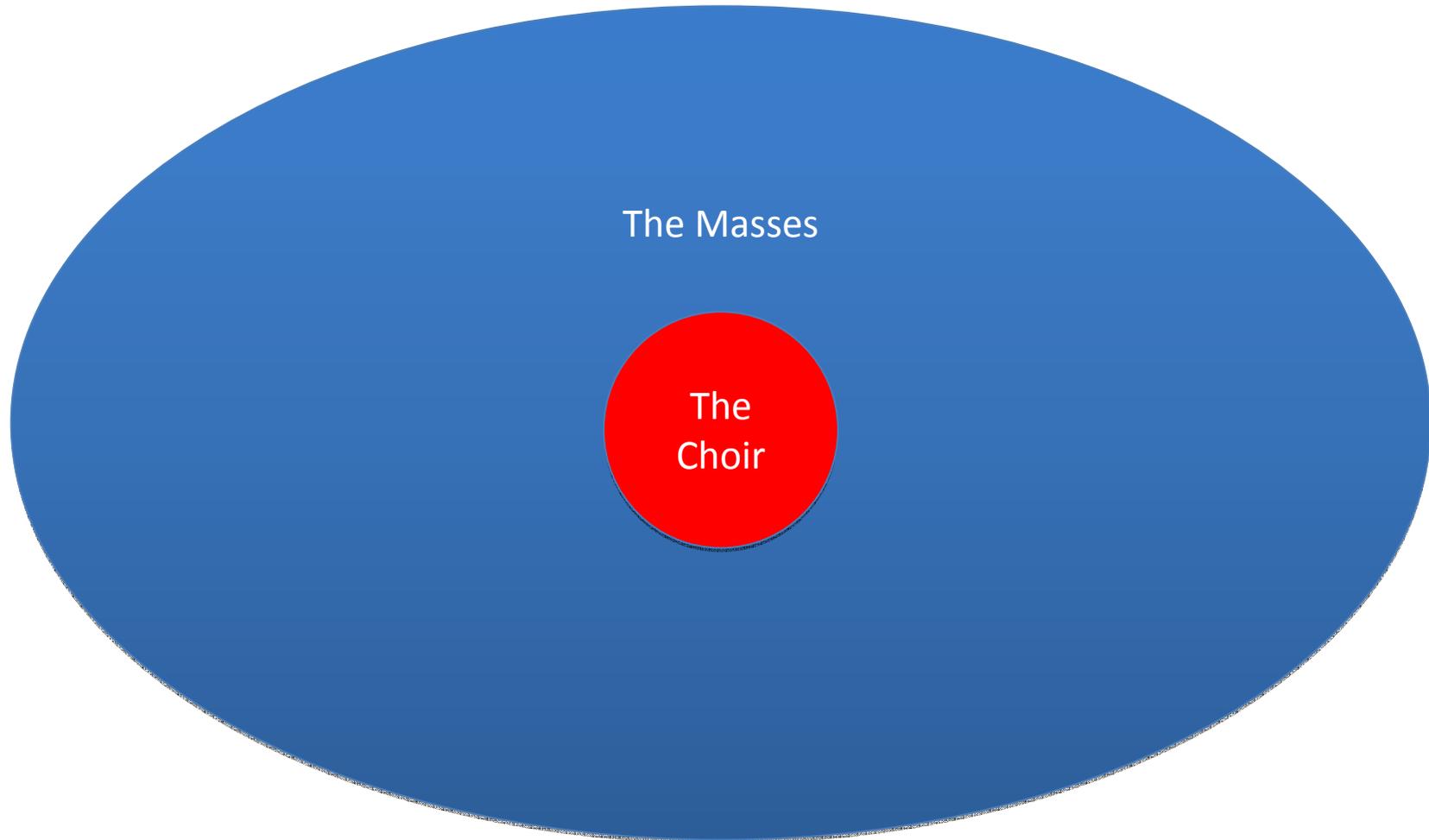
1. YOU CAN....

2. YOU CAN'T...

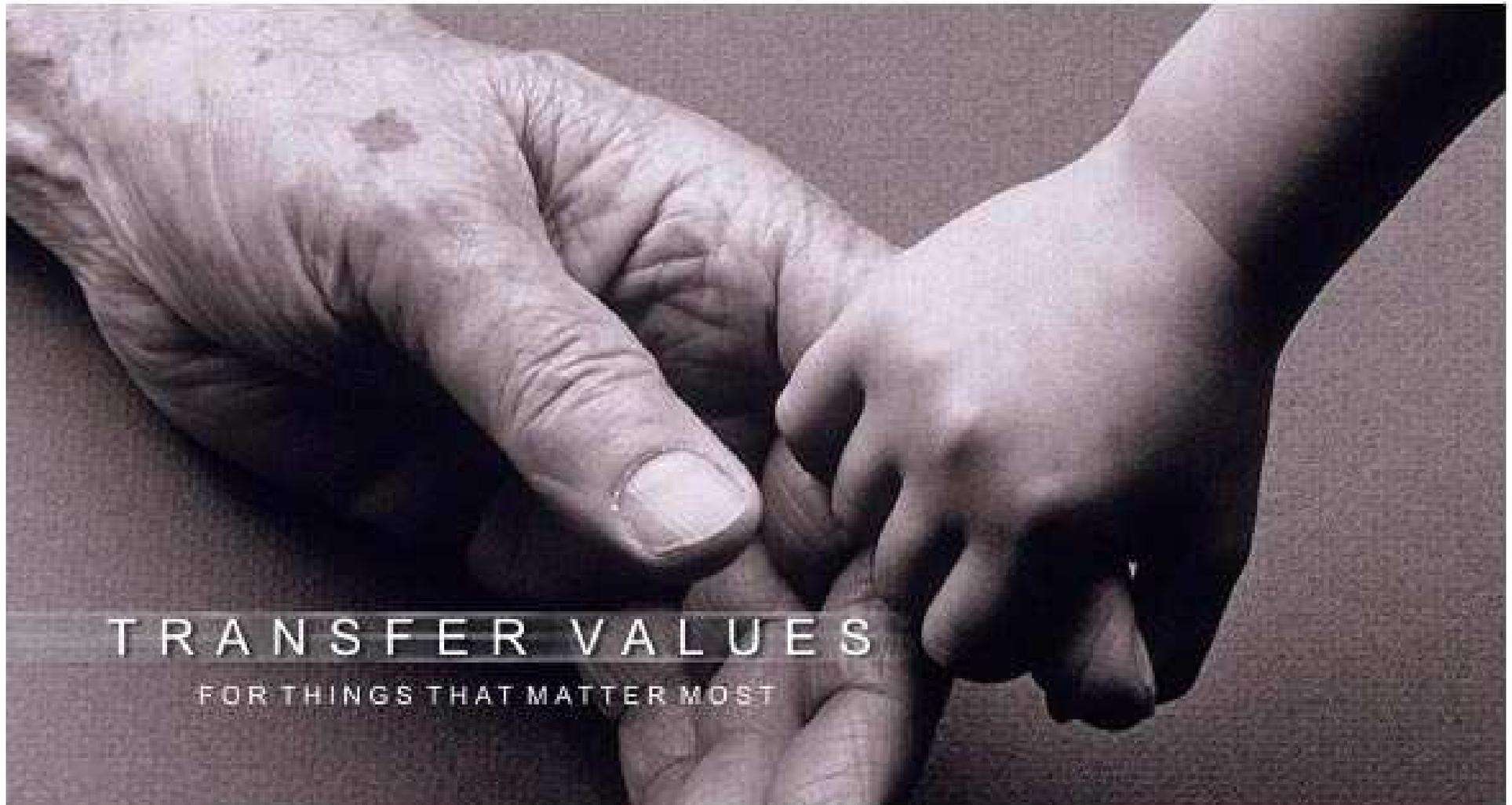
3. YOU CAN....

4. YOU CAN'T

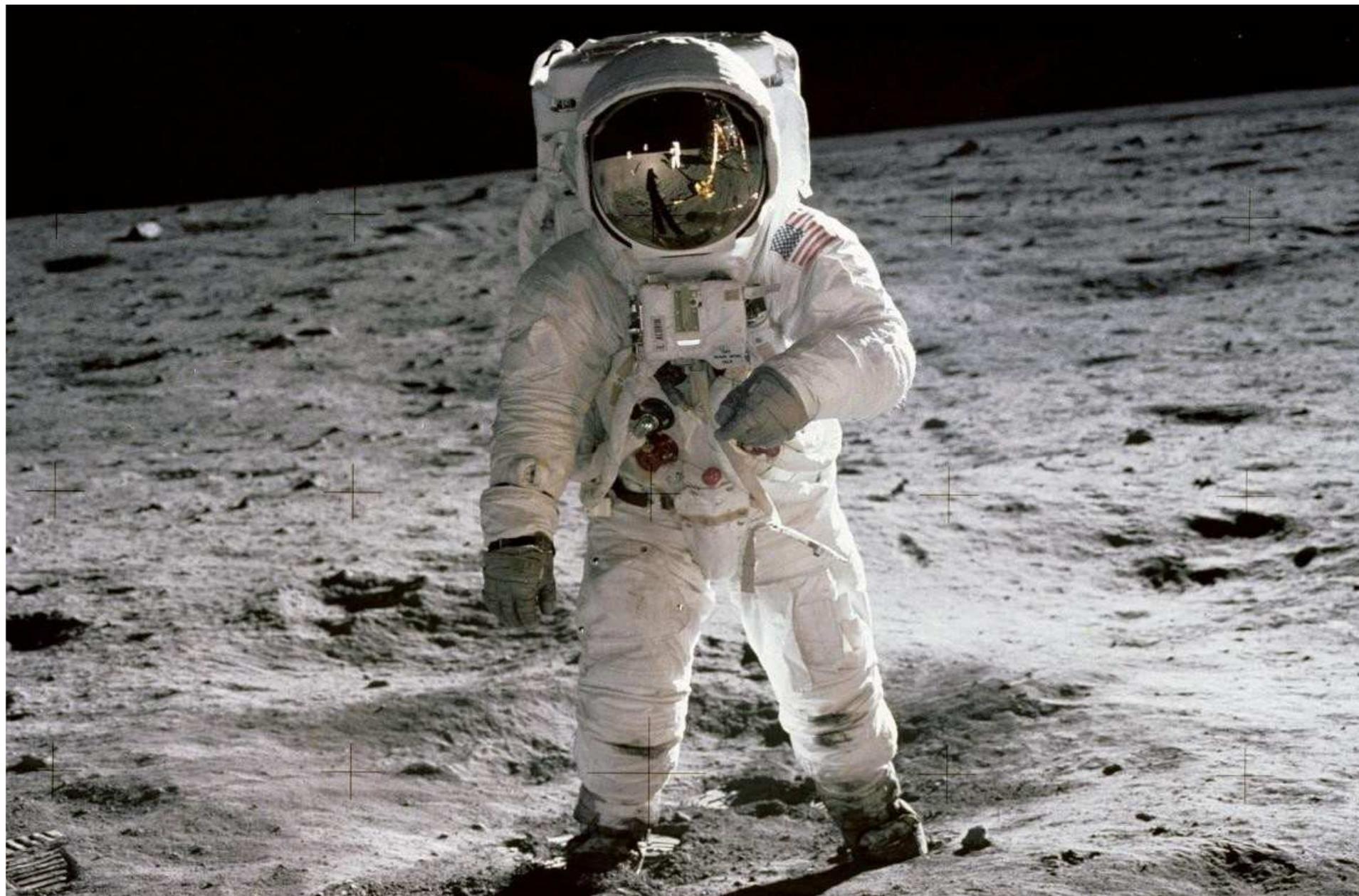
1) Beyond the choir



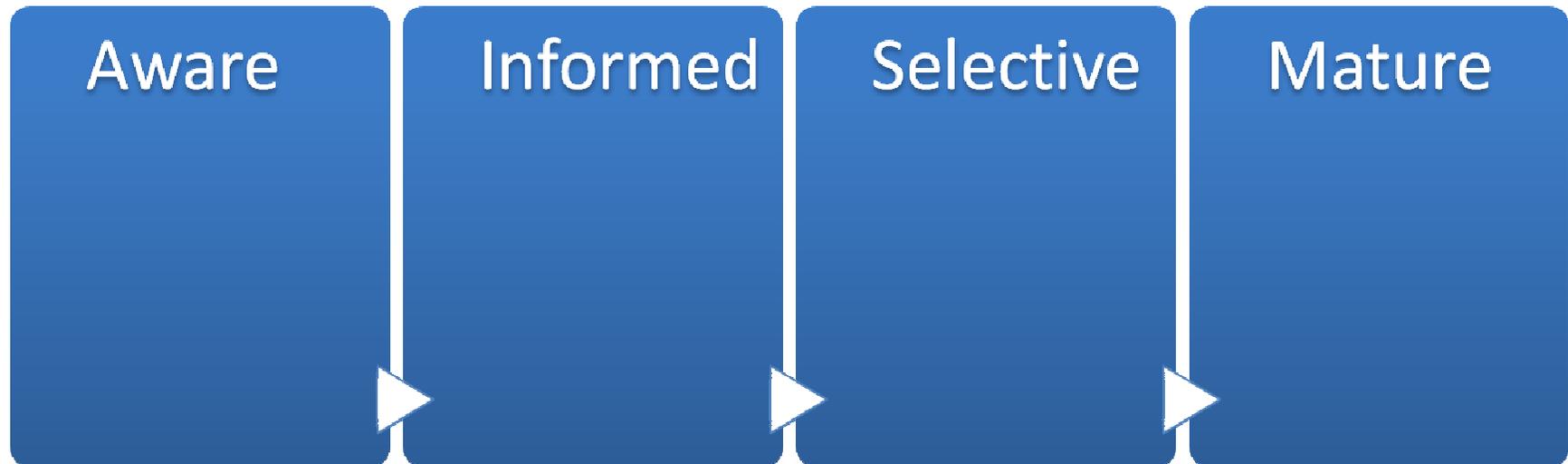
2) Beyond technology



3) Aspirational



The Journey



GETTING INVOLVED

Folks Who Helped Shape This

- Dan Geer, In-Q-Tel
- Chris Hoff, Cisco
- Chris Wysopal, Veracode
- Scott Crawford, EMA
- Pete Lindstrom, Spire Security
- Andrew Hay
- Tom Kellermann, Core Security
- Will Gragido, Cassandra Security
- Eric Hanselman, LeoStream
- Marisa Fagan, Errata Security
- Anton Chuvakin, Security Warrior
- Joe Jarzombek, DHS
- Barmak Meftah, Fortify
- Nick Selby, Trident Risk Mngt
- David Etue, Fidelis
- Rich Mogull, Securosis
- Adrian Lane, Securosis
- Tim Greene, NetworkWorld
- Dan Guido, NYU: Poly
- Caleb Sima, Armorize
- Ryan Barnett, Breach Security
- Jack Daniel, Astaro
- Jennifer Jabbusch, CAD, Inc.

Next Steps...

- Charter Members
- Introductions to University CS Programs
- Chair and Co-Chair Working Groups
 - Welcome Package: Getting Started
 - Business Cases



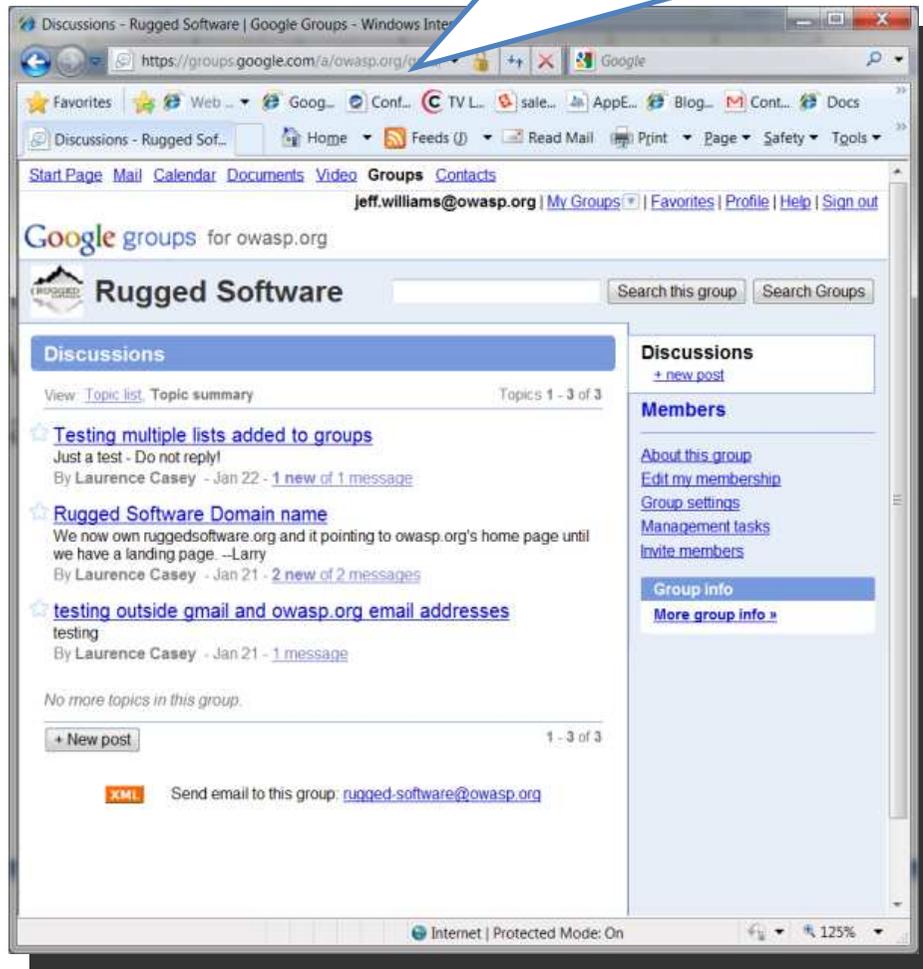
How to find
out more...



<http://ruggedsoftware.org>

Twitter: @RuggedSoftware

<https://groups.google.com/a/owasp.org/group/rugged-software>



Google Groups

“What does Rugged mean
to you?”

ruggedsoftware.org

The Rugged Software Manifesto

I am rugged... and more importantly, my code is rugged.

I recognize that software has become a foundation of our modern world.

I recognize the awesome responsibility that comes with this foundational role.

I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.

I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic, and national security.

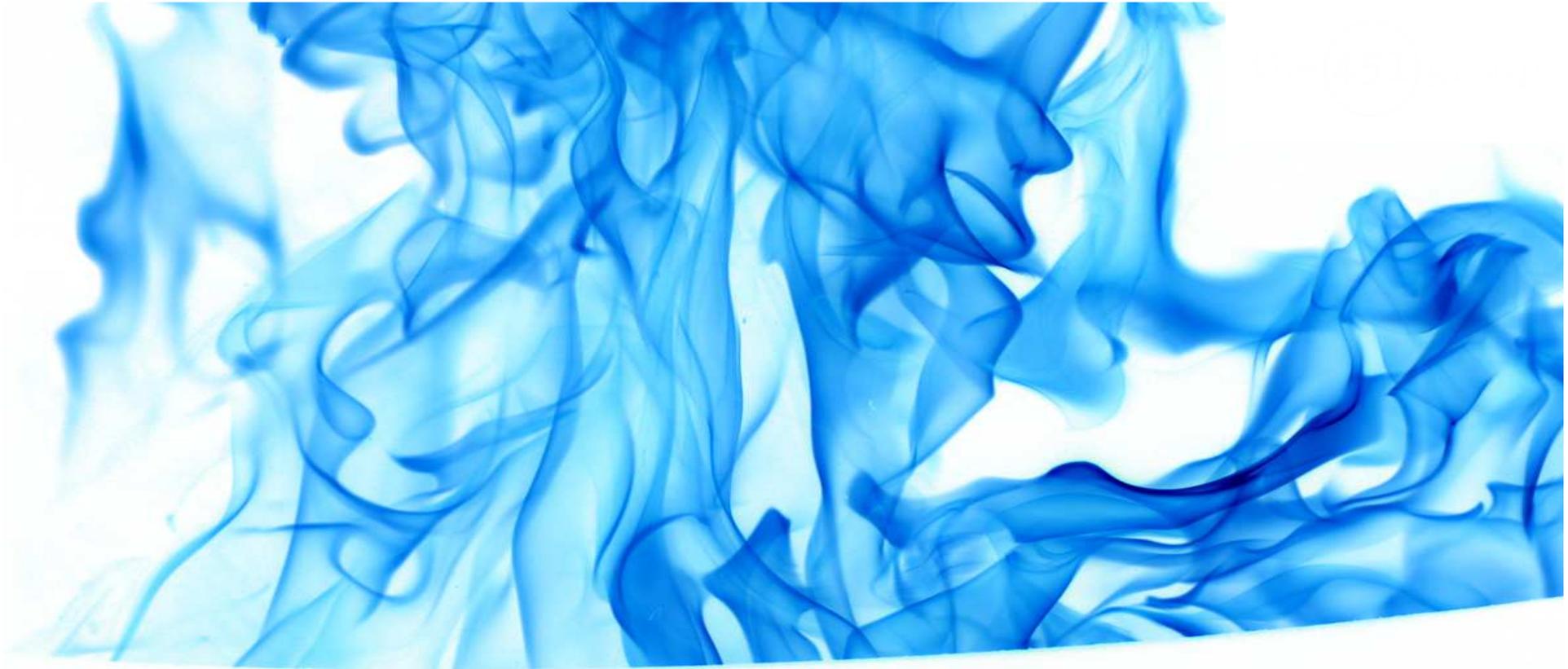
I recognize these things - and I choose to be rugged.

I am rugged because I refuse to be a source of vulnerability or weakness.

I am rugged because I assure my code will support its mission.

I am rugged because my code can face these challenges and persist in spite of them.

I am rugged, not because it is easy, but because it is necessary... and I am up for the challenge.



I just published:

The Beginning of the End: Driving and Era of Rugged Software

<http://www.the451group.com/intake/rugged/>

Joshua Corman
Research Director, Enterprise Security
The 451 Group

jcorman@the451group.com
twitter @joshcorman