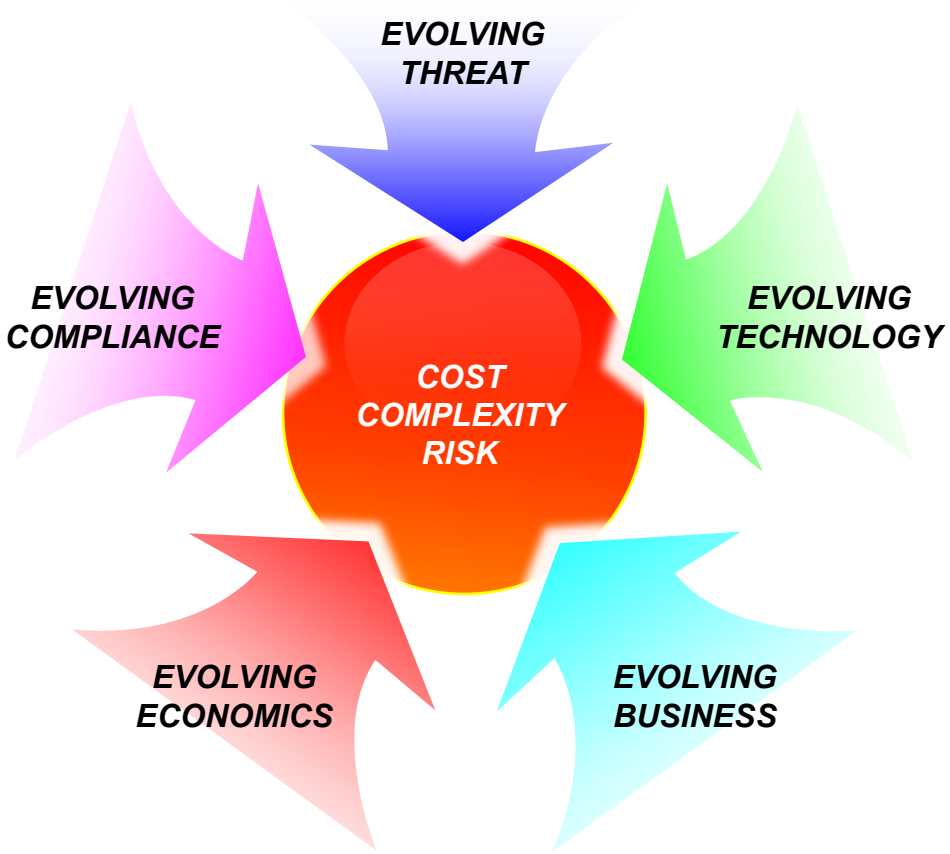
Rugged Software Development

Joshua Corman, David Rice, Jeff Williams

SANS Application Security Summit

February 5, 2010

Context


EVOLVING THREAT
EVOLVING COMPLIANCE
EVOLVING TECHNOLOGY
COST COMPLEXITY RISK
EVOLVING ECONOMICS
EVOLVING BUSINESS

RSA CONFERENCE | Where The World Talks Security

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

GREYLOCK PARTNERS

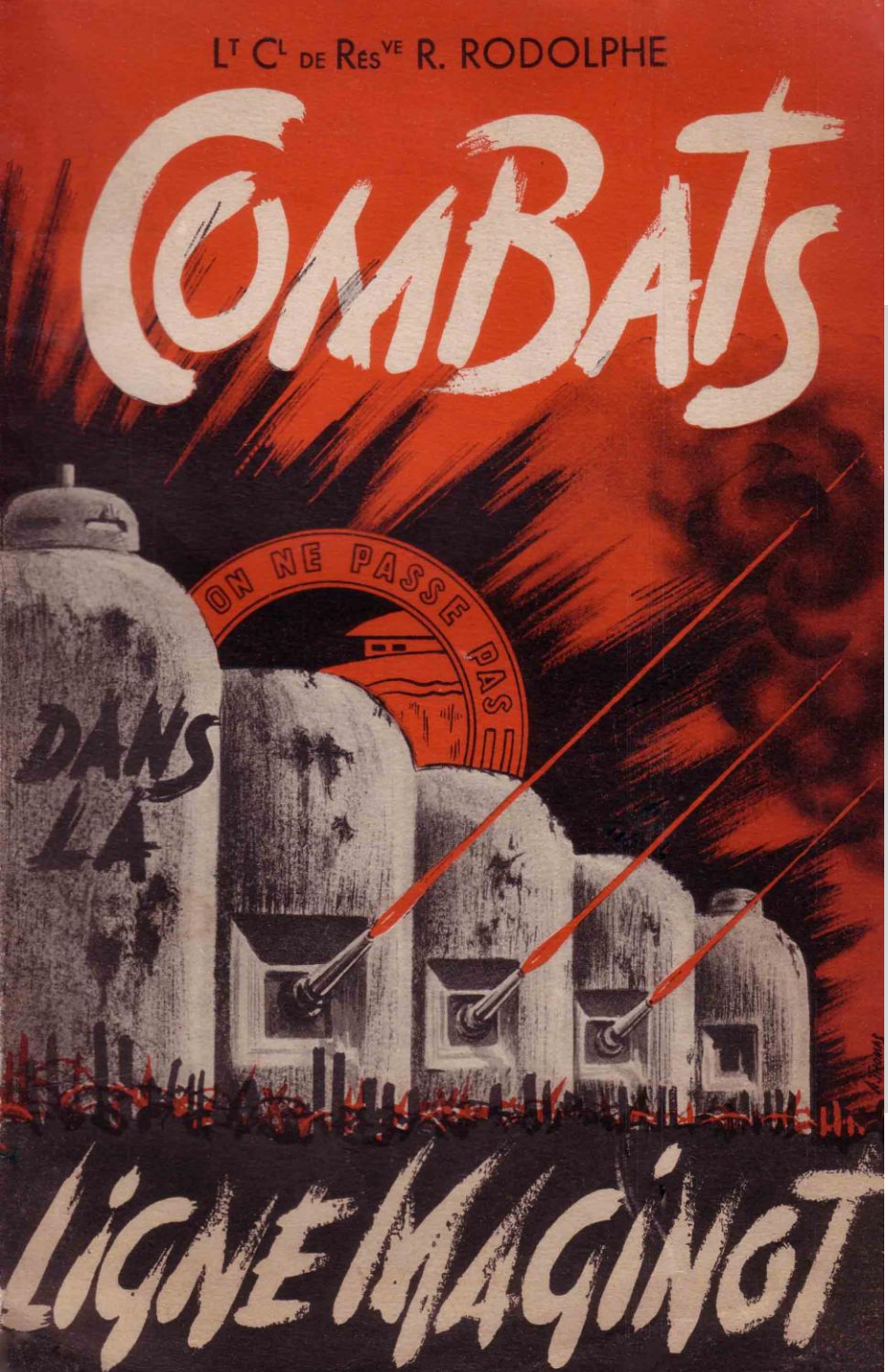
“What is missing from software security?”


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


DANGER
MEMES
AHEAD

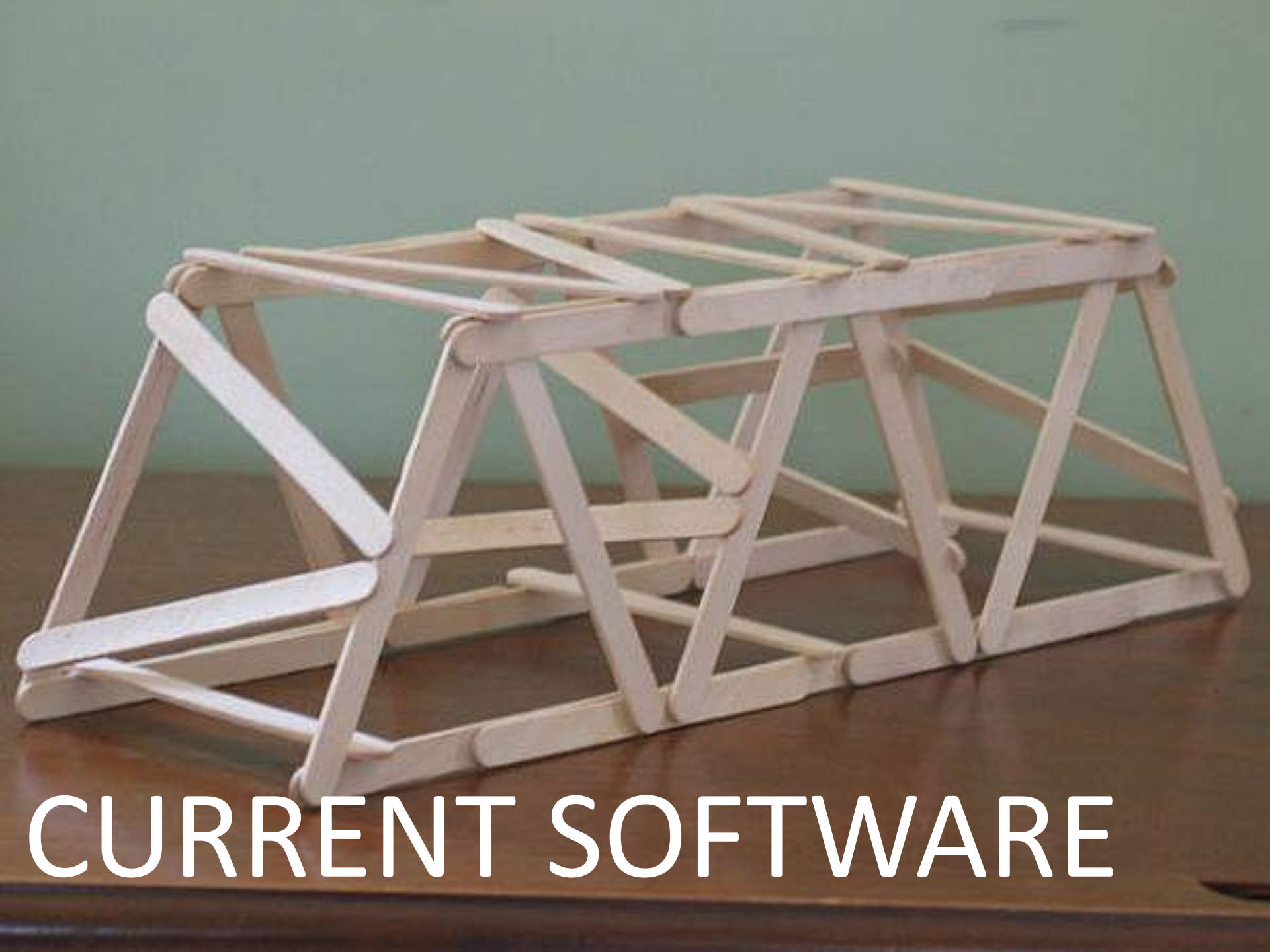
 WWW.HIJINKSENSUE.COM

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


CURRENT SOFTWARE

RUGGED SOFTWARE

CURRENT SOFTWARE

RUGGED SOFTWARE

CURRENT SOFTWARE

RUGGED SOFTWARE

…so software not only needs to be…


FAST
Coca-Cola
Radisson SAS
SIEMENS
hydrolift
fly without wings
Koenigsegg
Spirit of NORWAY
offshore RACING
ColorLine
projectiondesign

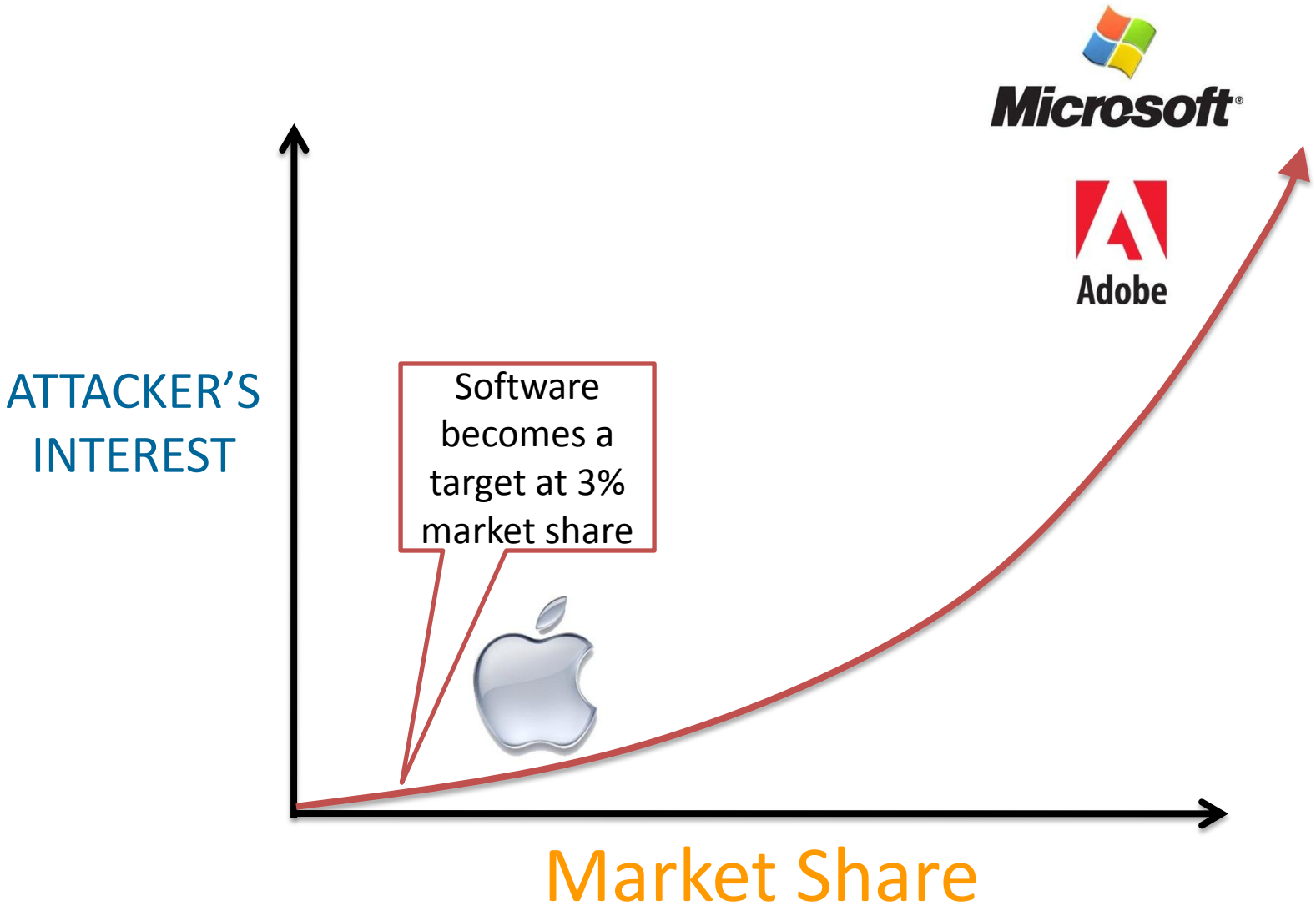
AGILE

Are You Rugged?


HARSH


UNFRIENDLY

There is no such thing as “toy” software.


Microsoft
Adobe
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 the modern world.

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

I recognize that may code may 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.

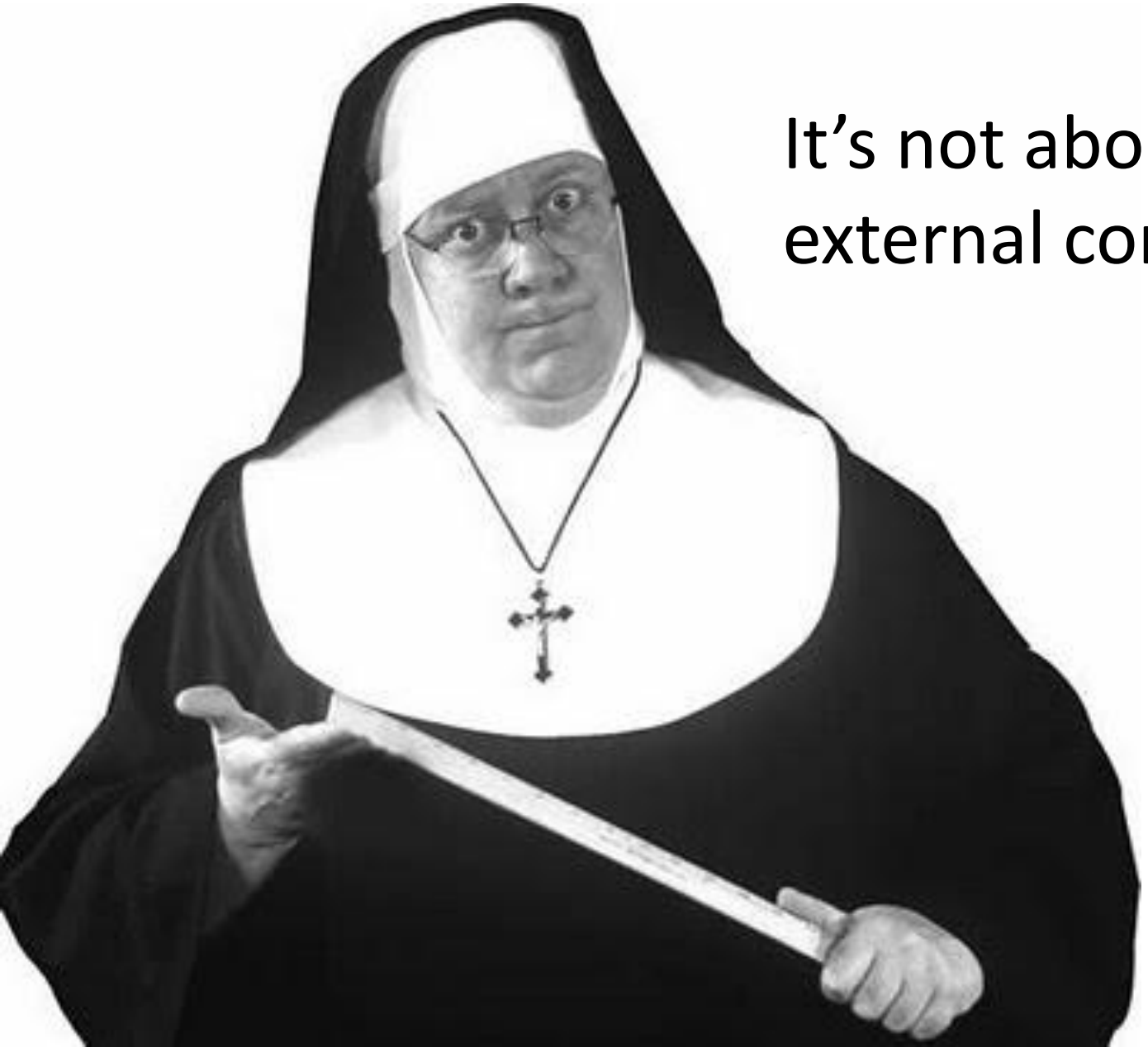
I am rugged because my code can face these challenges and persist in spite of them.

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


Rugged?

WHAT IS RUGGED?

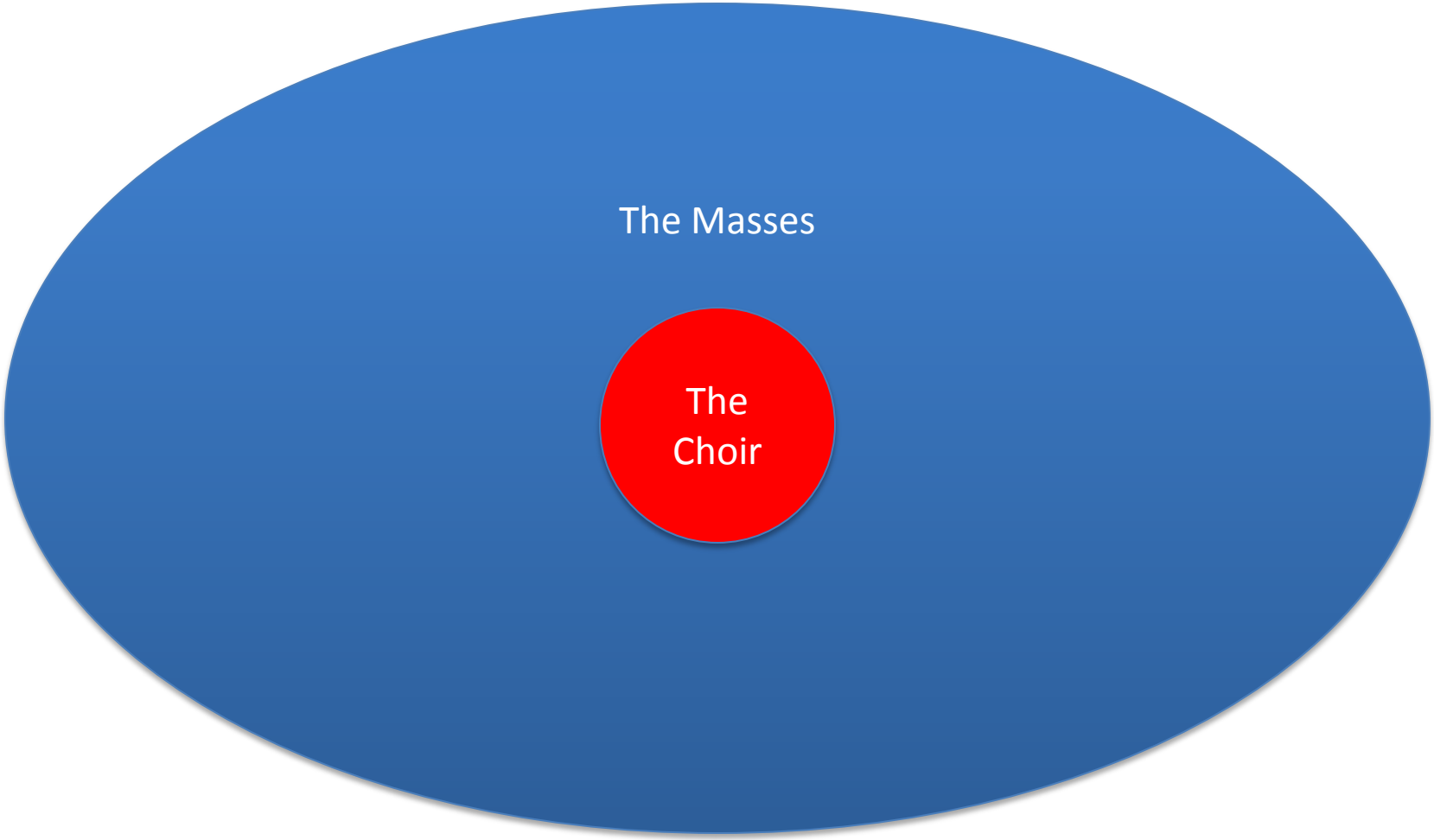
It’s not about style, it’s about the result.



It’s not about external compliance…

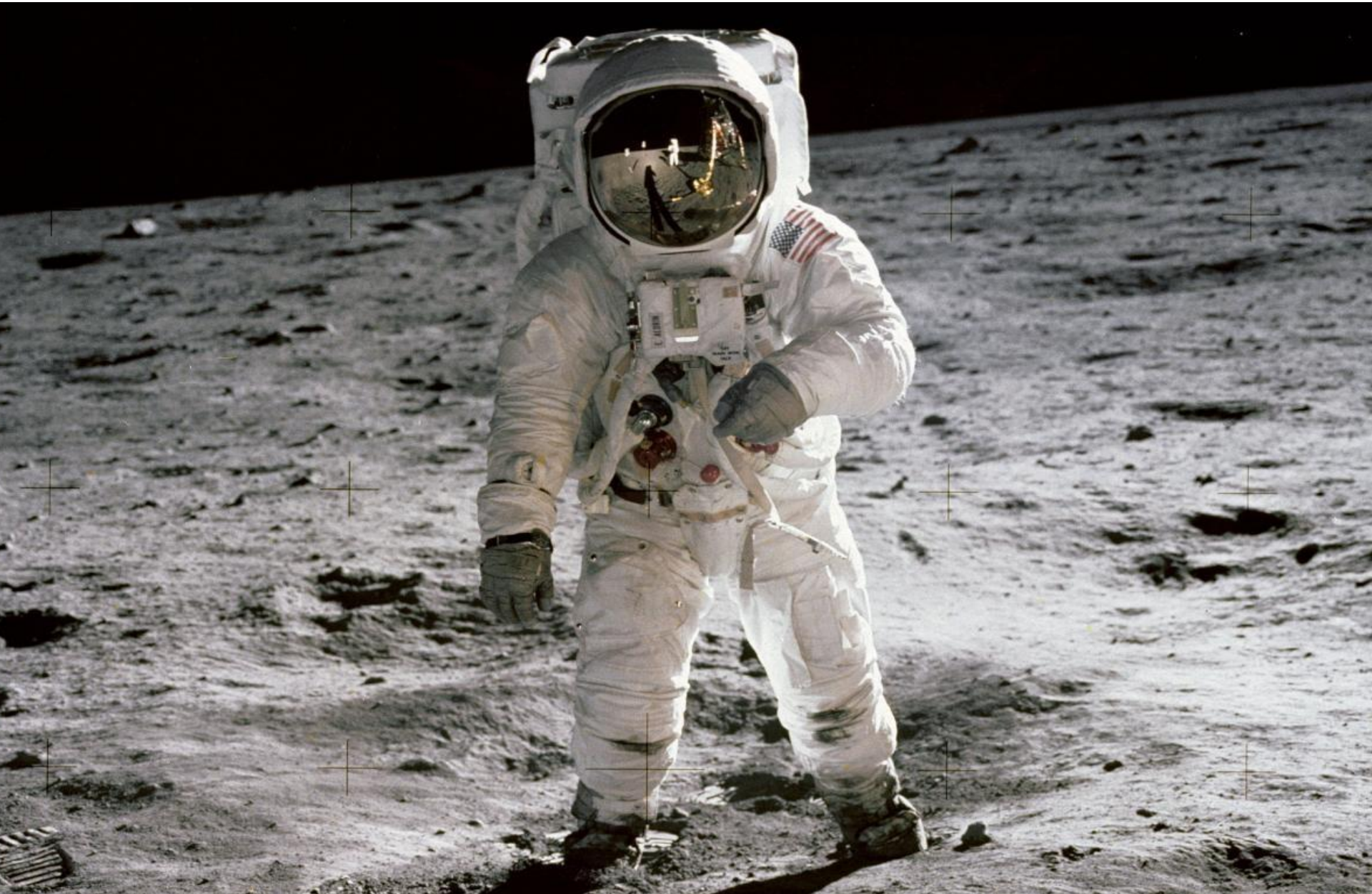

RULES
1. YOU CAN....
2. YOU CAN'T...
3. YOU CAN....
4. YOU CAN'T

1) Beyond the choir



2) Beyond technology

3) Aspirational



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 Kellerman, 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, TRG
- David Etue, Fidelis
- Rich Mogull, Securosis
- Adrian Lane, Securosis
- Tim Greene, NetworkWorld
- Dan Guido, NYU: Poly
- Caleb Sima, HP
- Ryan Barnett, Breach Security
- Jack Daniel, Astaro
- Jennifer Jabbusch, CAD, Inc.

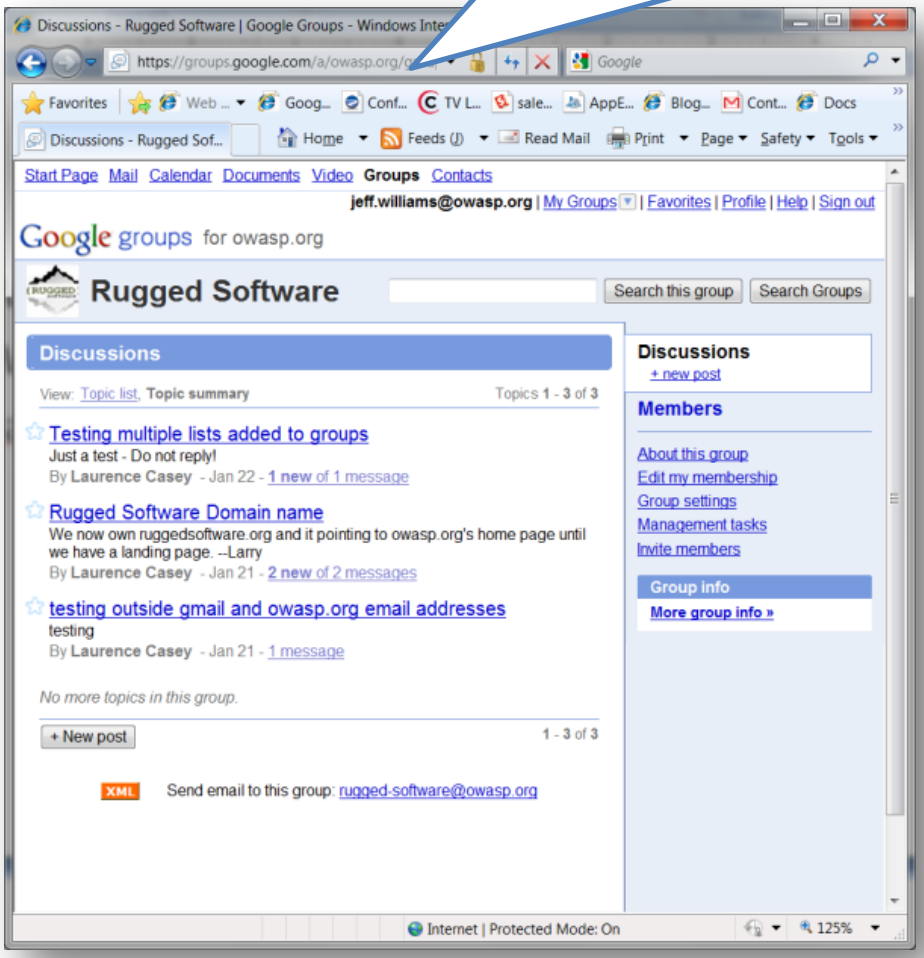
Next Steps…

- 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

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



Google Groups

“What does Rugged mean to you?”