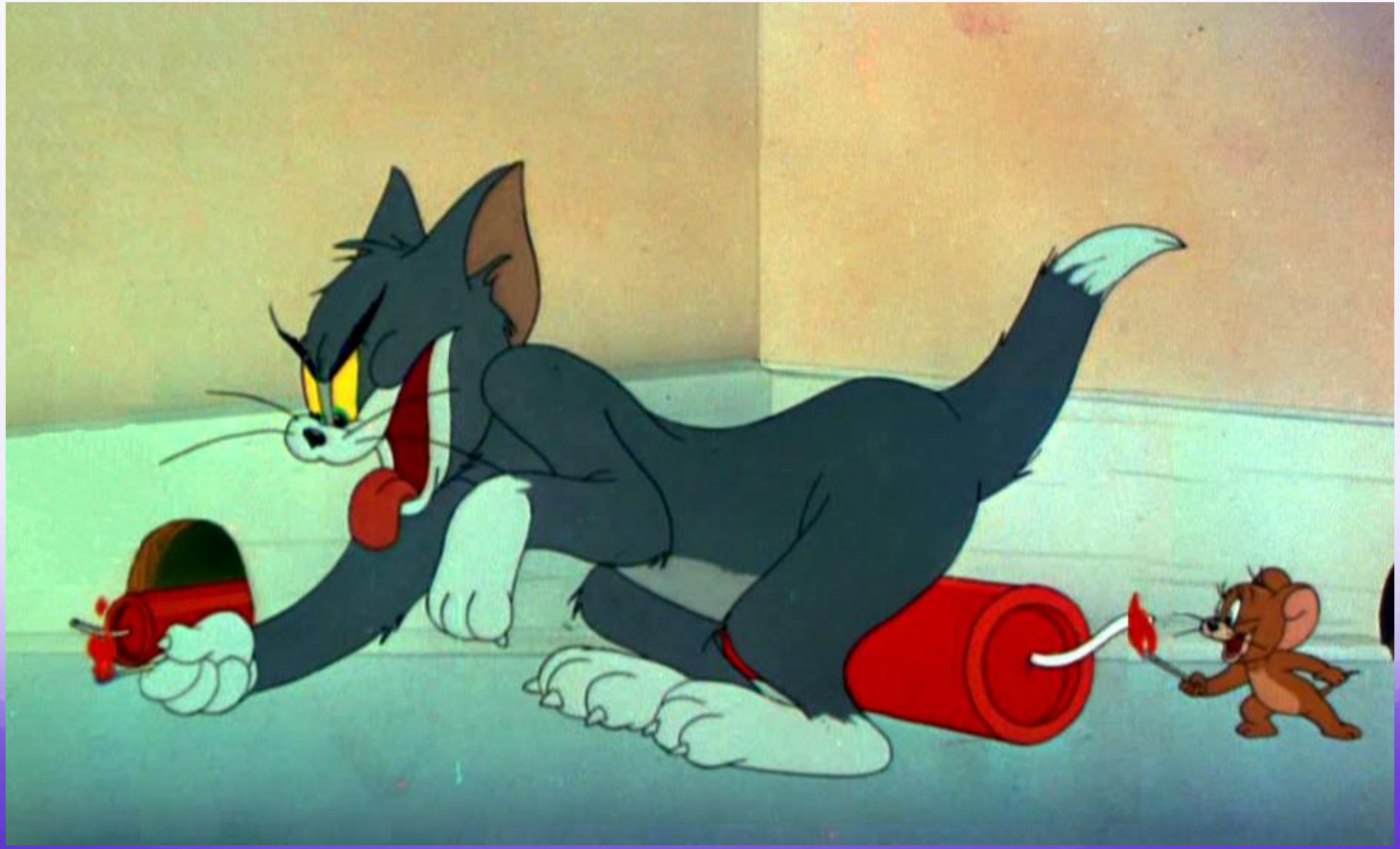
The Advancement of Science in Cybersecurity



Laurie Williams
North Carolina State University
#metoosecurity

A game of cat and mouse ...



Why the Science of Security?

- "… nagging perception that too much of the research is opportunistic, lacks rigor, has weak methodology, and fails to produce material advances on underlying hard problems."

(NSA BAA Industry Day, 2013)



THE THREE MUSKETEERS

2011 Release



Carnegie Mellon University

NC STATE UNIVERSITY

ILLINOIS

2014 Re-release



The three missions of the Science of Security Lablets

- **Build a science of security community**
- Advance research methods in the context of cybersecurity to build a sound science of security
- "Solve" hard security problems through the application of scientific research

Through diversity of opinion, creativity and unity is born.



Focus areas



THE THREE MUSKETEERS



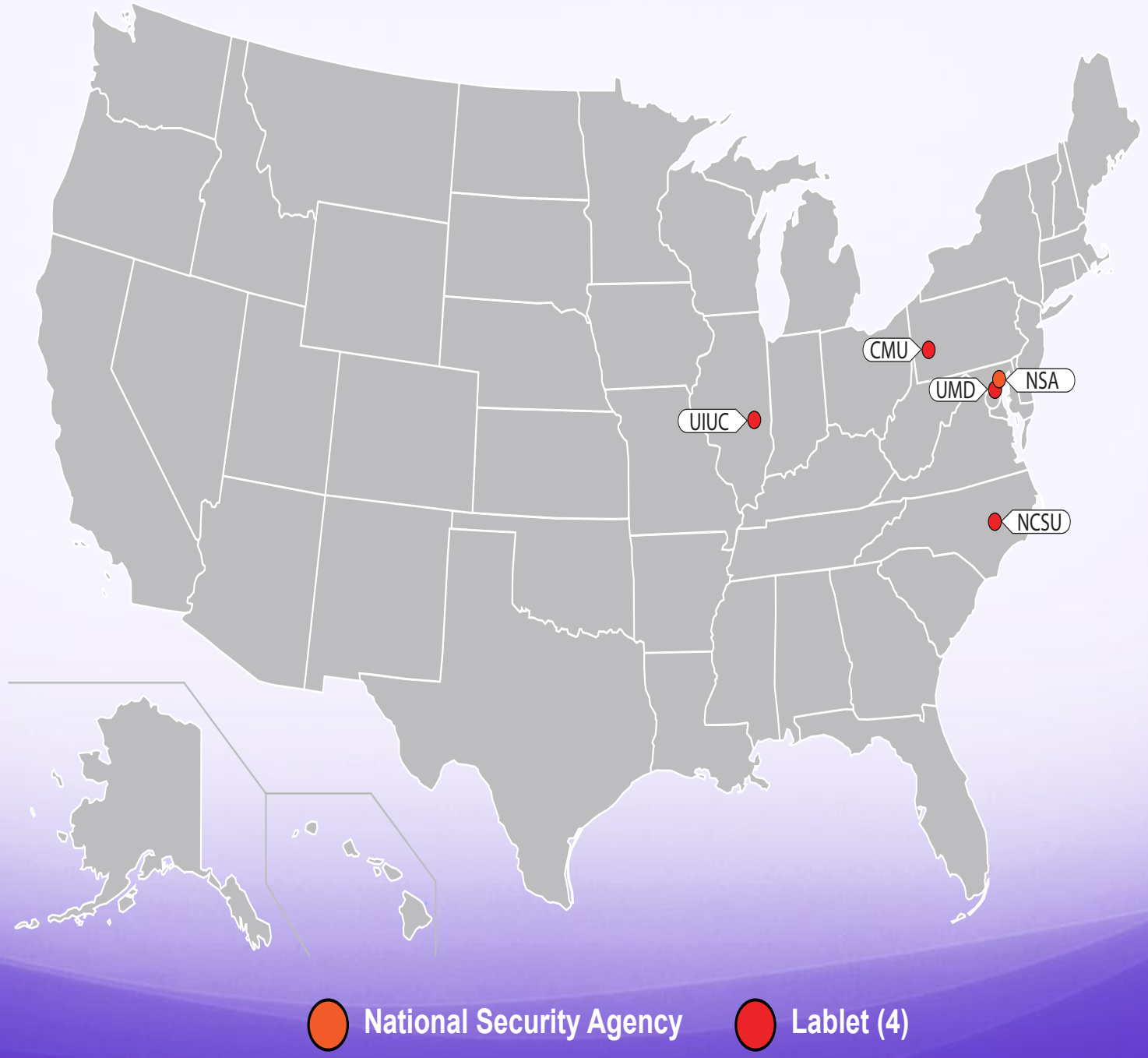
Through collaboration and unity, we can accelerate change on a larger scale.



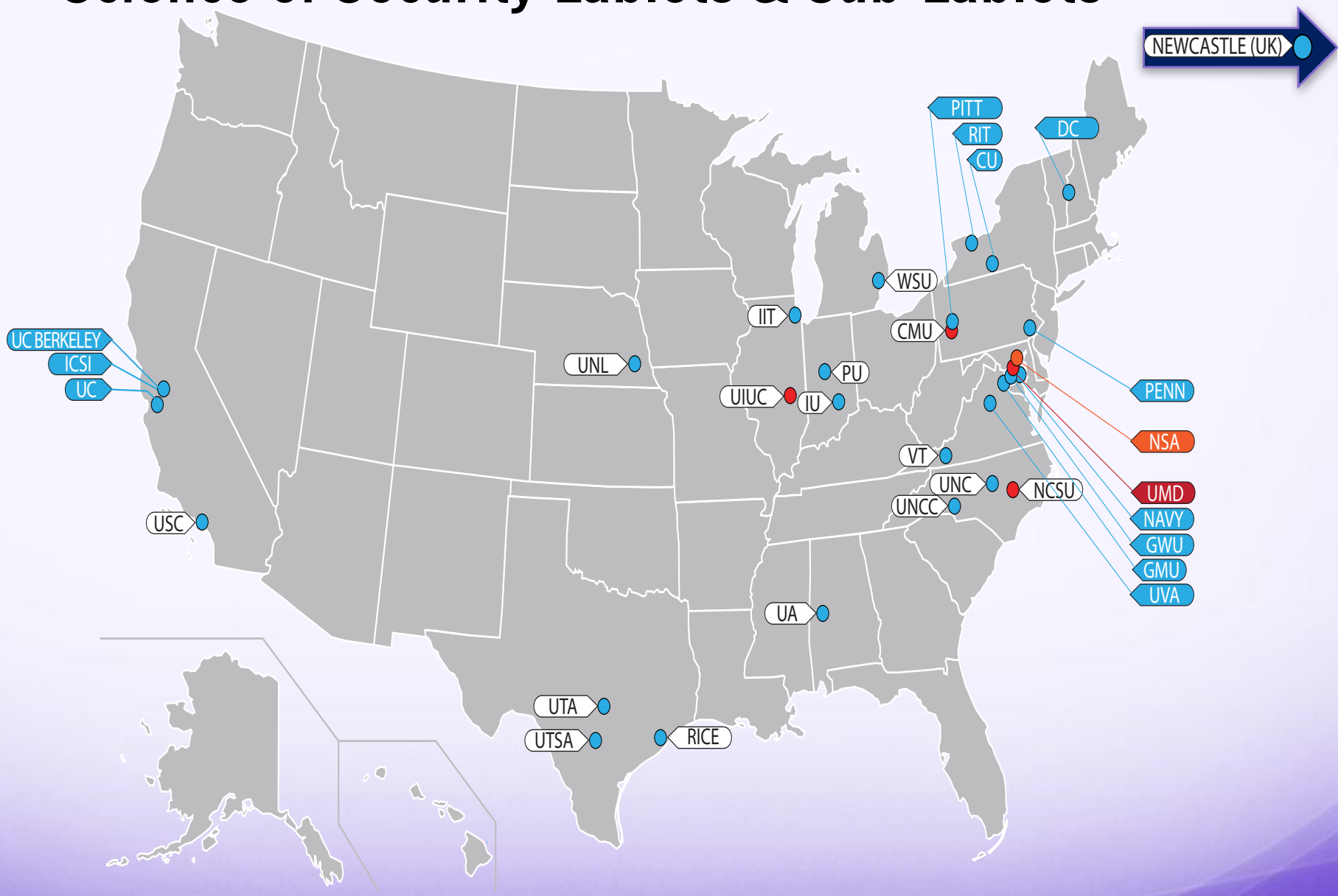
Competition-free zone



Science of Security Lablets



Science of Security Lablets & Sub-Lablets

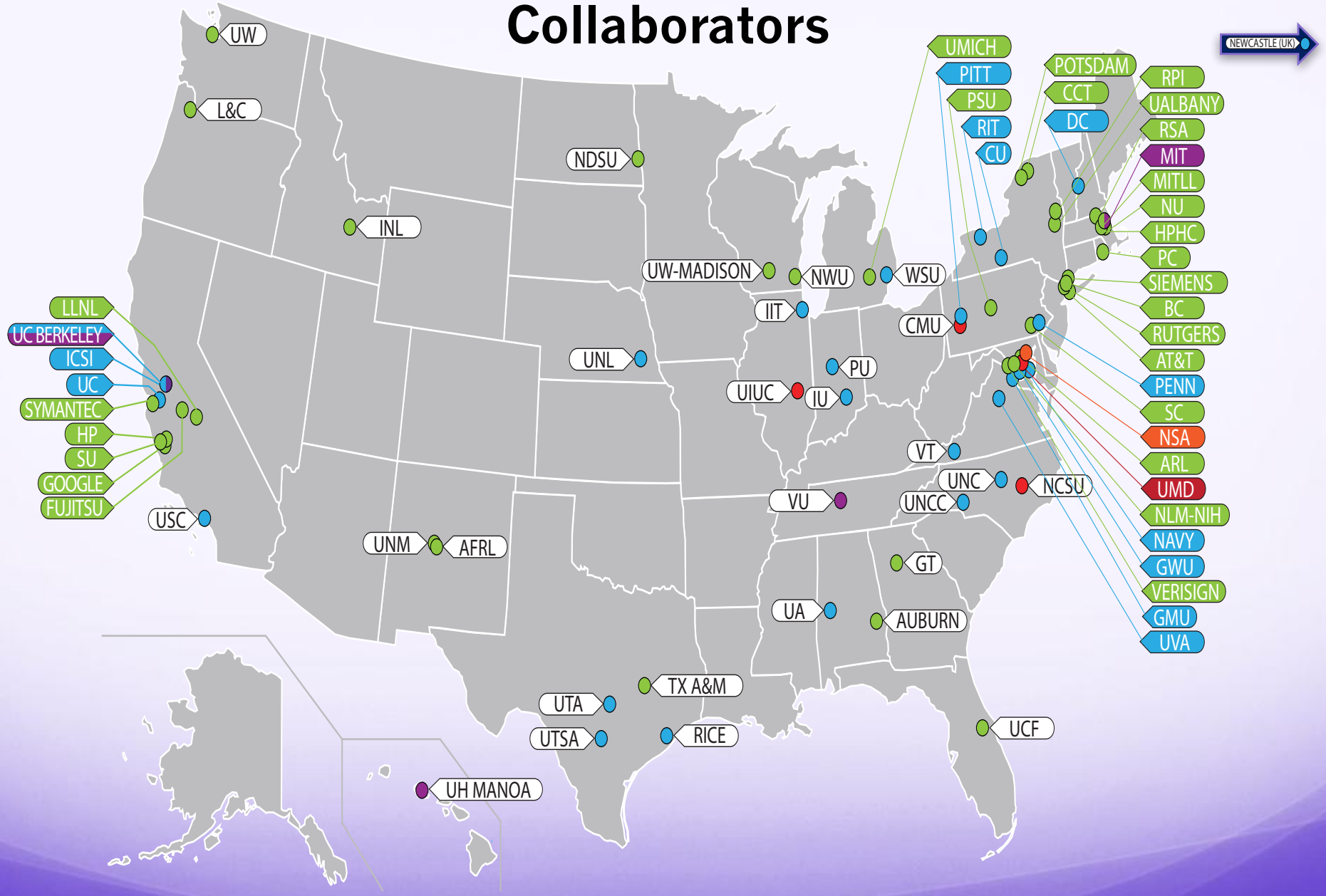


National Security Agency

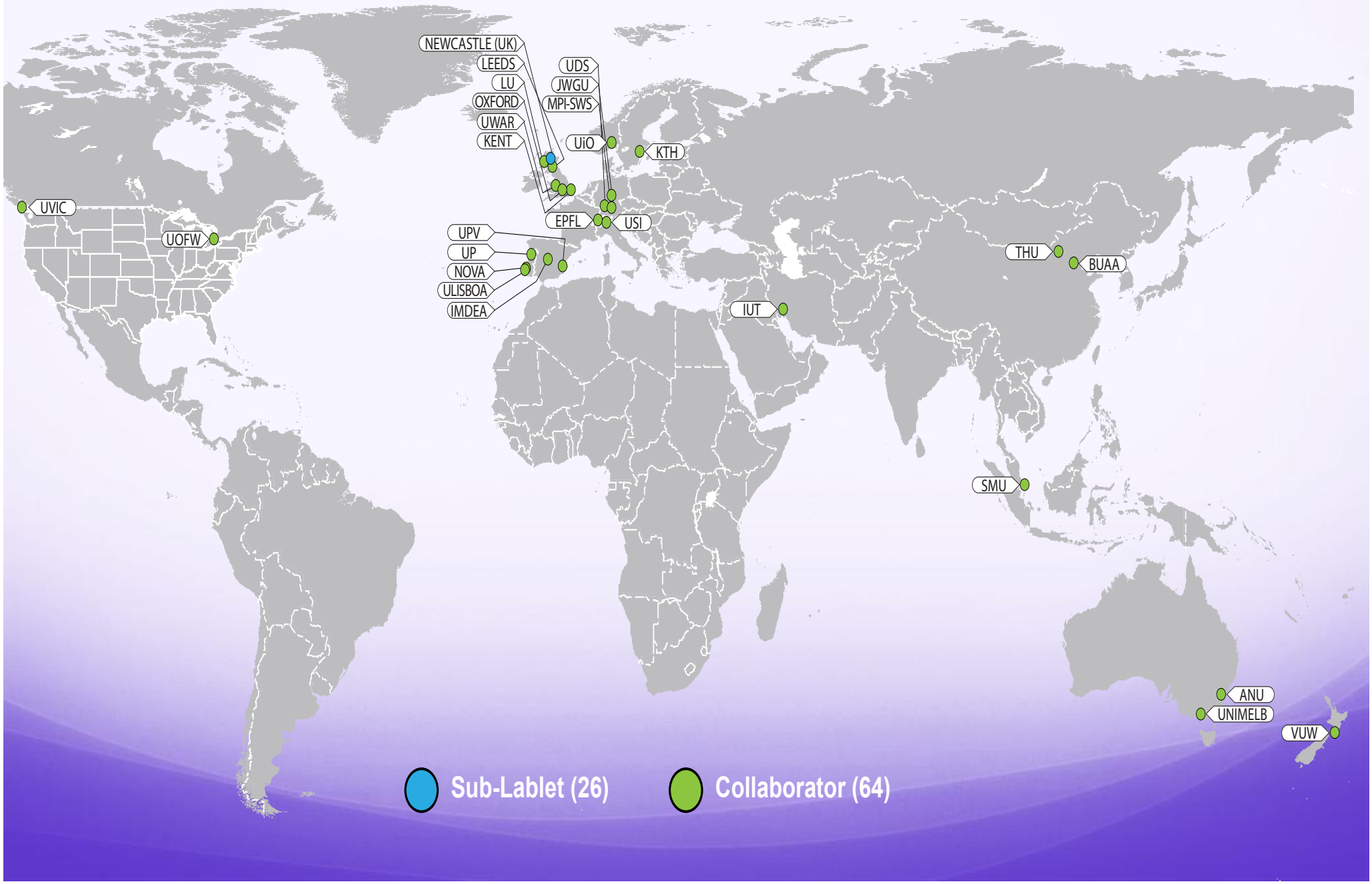
Lablet (4)

Sub-Lablet (26)

Science of Security Lablets, Sub-Lablets, and Collaborators



Science of Security International Sub-Lablets and Collaborators




mology
ABBREVIATIONS

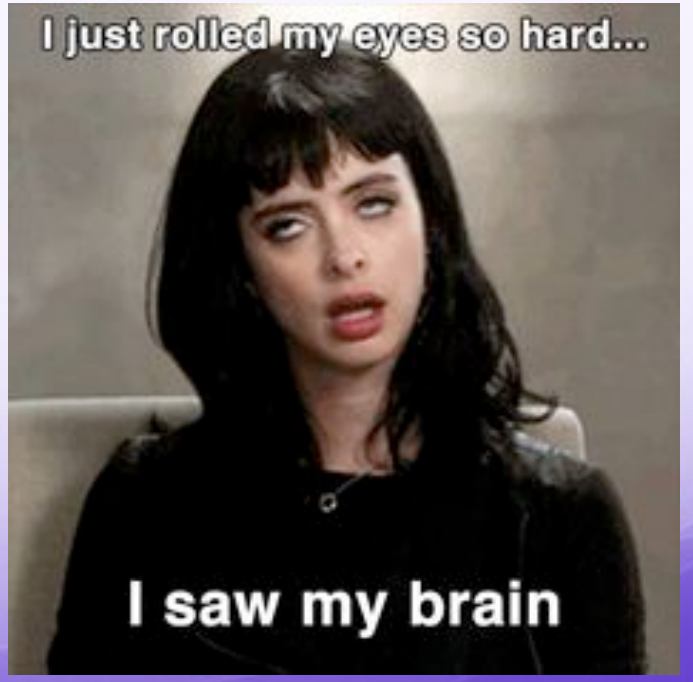
The three missions of the Science of Security Lablets

- Build a science of security community
- **Advance research methods in the context of cybersecurity to build a sound science of security**
- "Solve" hard security problems through the application of scientific research

Those “pesky” and ever-present tough questions

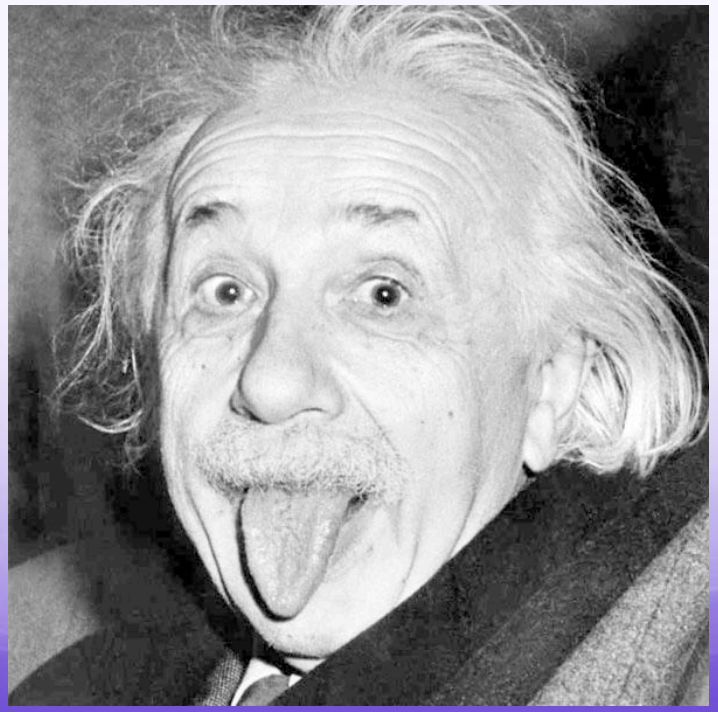
Where’s the ~~beef~~ . . . . science?





Tough questions lead to great(er) insight.

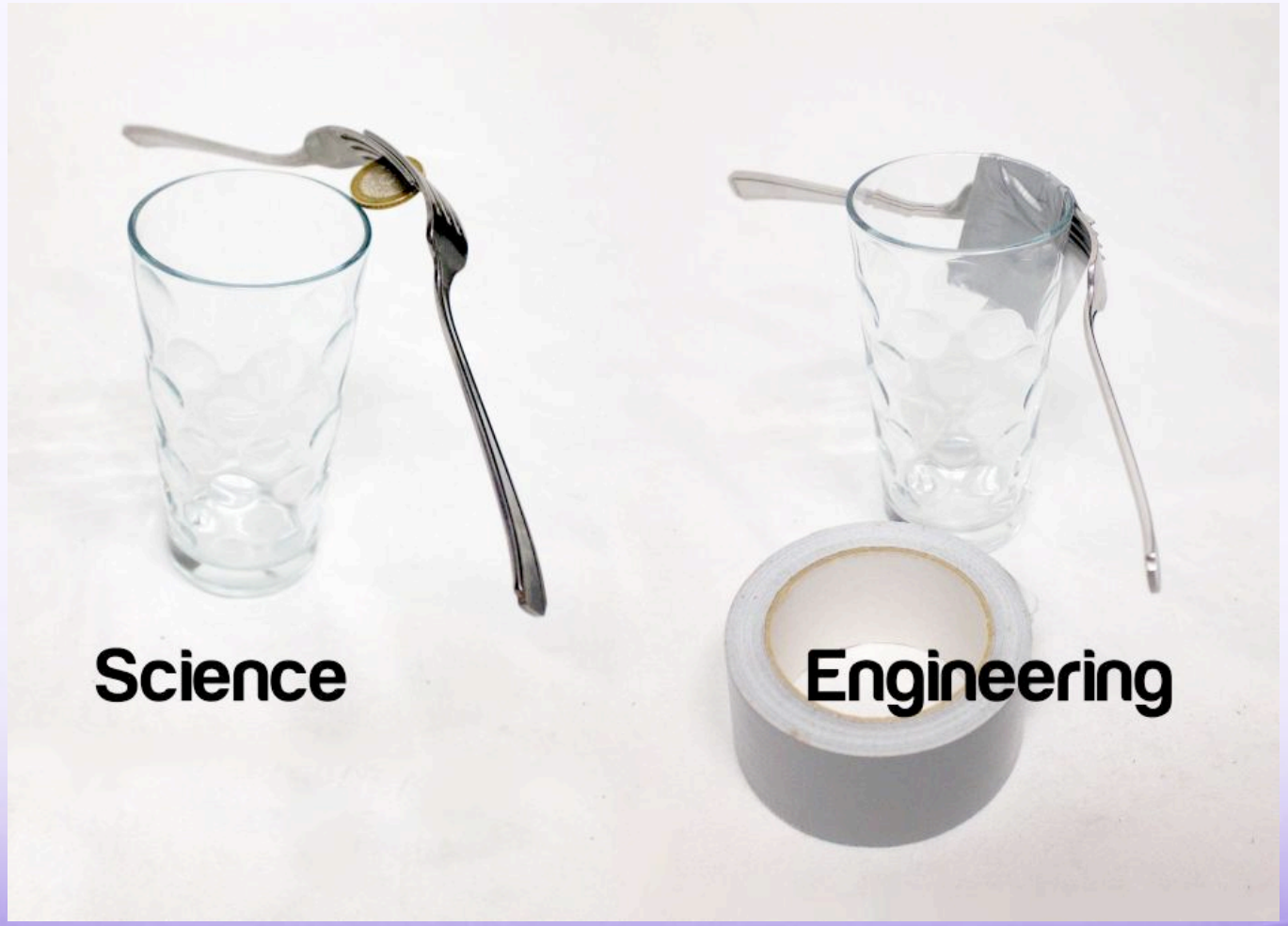
"The quality of your answers is in direct proportion to the quality of your questions."
--Albert Einstein



It's so easy to fall back to "engineering-ish" research.



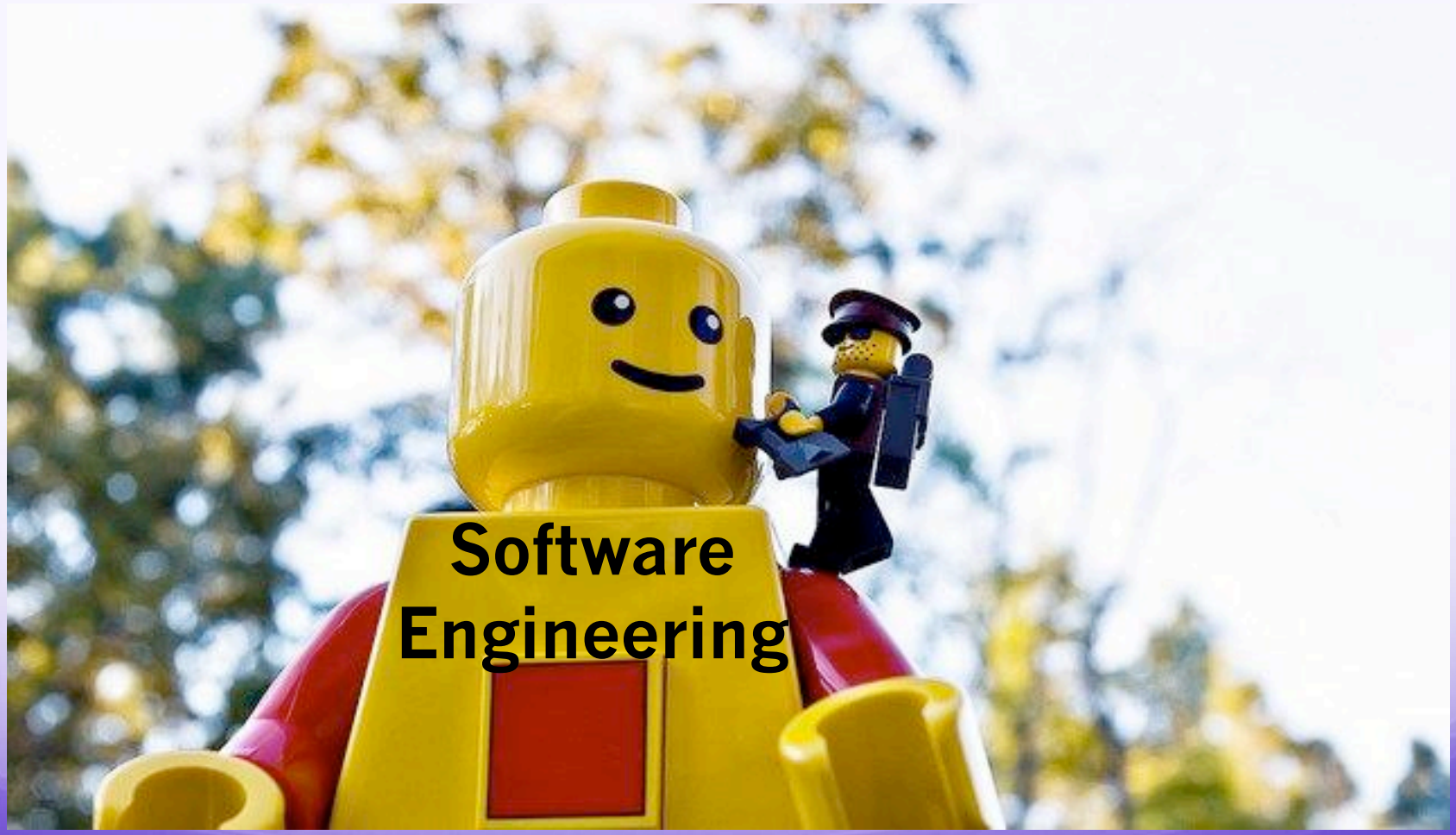
Principles, Theories, Laws, Hypotheses … Science



May be just a “subtle change”



Stand on the shoulders of giants.



Types of Validation

Type of result	Accepted (ICSE 2002)	Accepted (ICSE 2016)
Analysis	…	…
Evaluation	…	…
Experience	**8 (19%)**	**4 (4%)**
Example	16 (37%)	1 (1%)
Persuasion	0 (0%)	1 (1%)
Underspecified	…	…
No validation mentioned	6 (14%)	0 (0%)

Types of Validation

Type of result	Accepted (ICSE 2002)	Accepted (ICSE 2016)
Analysis	…	…
Evaluation	…	…
Experience	8 (19%)	4 (4%)
Example	**16 (37%)**	**1 (1%)**
Persuasion	0 (0%)	1 (1%)
Underspecified	…	…
No validation mentioned	6 (14%)	0 (0%)

Types of Validation

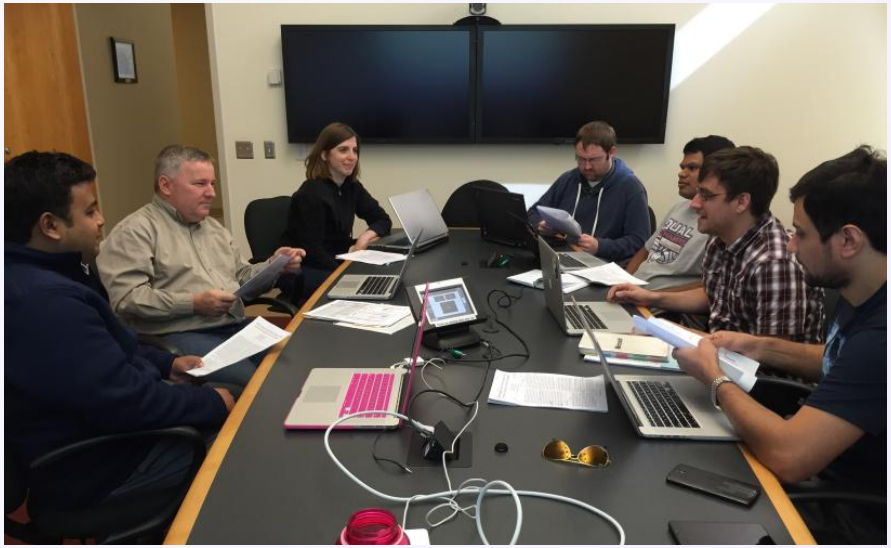
Type of result	Accepted (ICSE 2002)	Accepted (ICSE 2016)
Analysis	…	…
Evaluation	…	…
Experience	8 (19%)	4 (4%)
Example	16 (37%)	1 (1%)
Persuasion	**0 (0%)**	**1 (1%)**
Underspecified	…	…
No validation mentioned	6 (14%)	0 (0%)

Types of Validation

Type of result	Accepted (ICSE 2002)	Accepted (ICSE 2016)
Analysis	…	…
Evaluation	…	…
Experience	8 (19%)	4 (4%)
Example	16 (37%)	1 (1%)
Persuasion	0 (0%)	1 (1%)
Underspecified	…	…
No validation mentioned	**6 (14%)**	**0 (0%)**

Science of Security Copycats

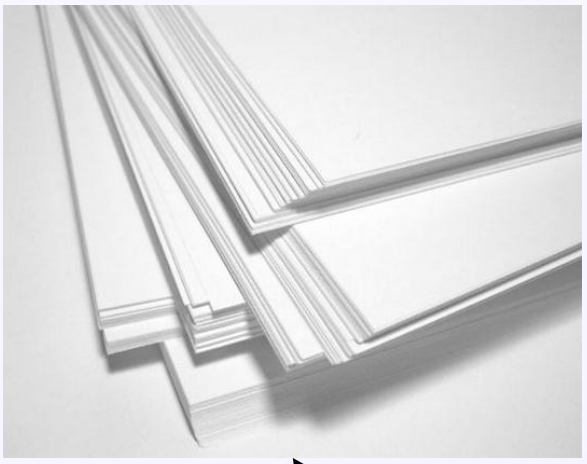
- Guidelines
- Seminars
- Research plan reviews
- Workshops
- Conference (Hot SoS)





Security Paper Study

128 Papers (CCS)
55 Papers (S&P)

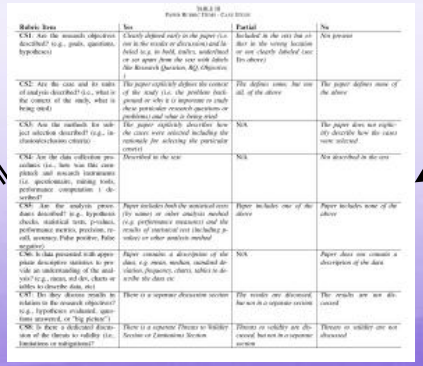


7 Reviewers





Author

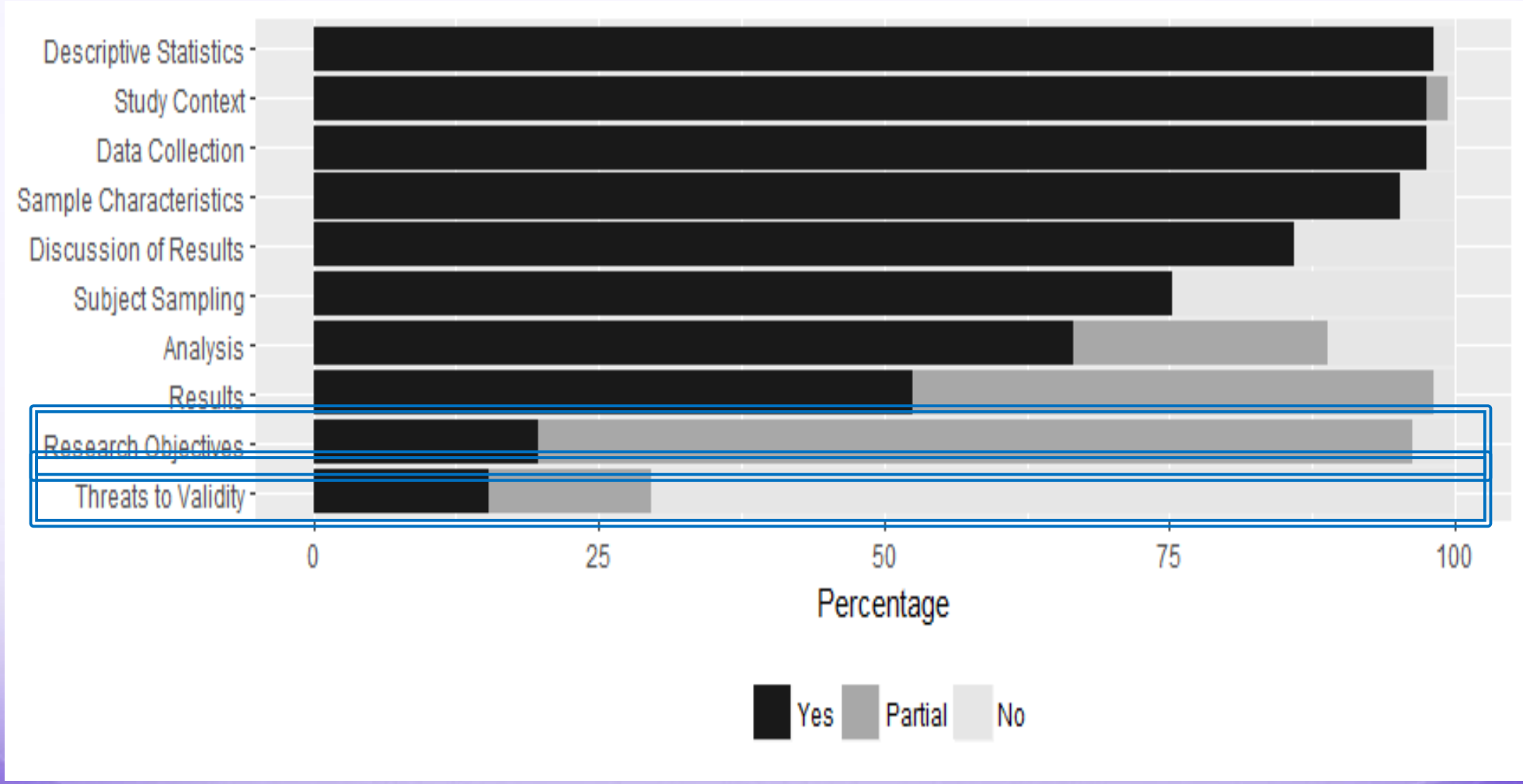




Paper Characteristics

	Empirical	Proof	Discussion
Process	27	9	2
Tool	104	3	3
Model	23	18	0
Protocol	21	20	5
Theory	7	0	0

Paper Completeness



The three missions of the Science of Security Lablets

- Build a science of security community
- Advance research methods in the context of cybersecurity to build a sound science of security
- **"Solve" hard security problems through the application of scientific research**

Through focus, progress is made.

1. Thing 1
2. Thing 2
3. Thing 3
4. Thing 4
5. Thing 5
6. Thing 6
7. Thing 7
8. Thing 8

Do This!

DON'T DO THIS!

You wouldn't do it anyway.

Science of Security **Focus**

1. Scalability and composability
2. Policy-governed secure collaboration
3. Encryption algorithms
4. Predictive security metrics
5. Intrusion Detection
6. Resilient architectures
7. Human behavior

Do This!

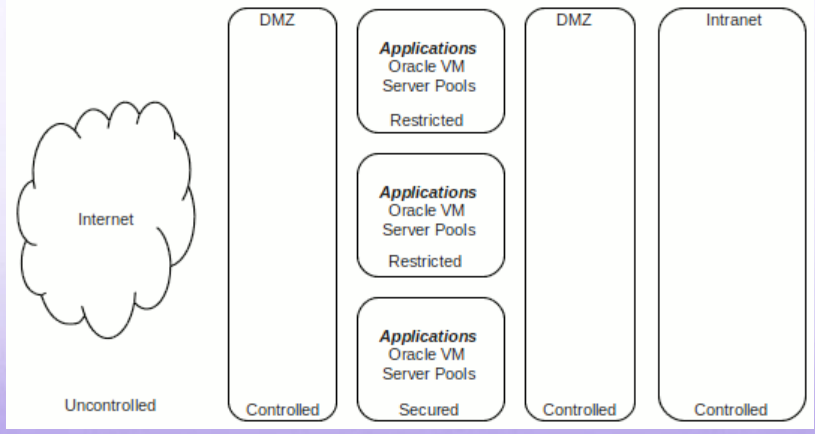
DON'T DO THIS!



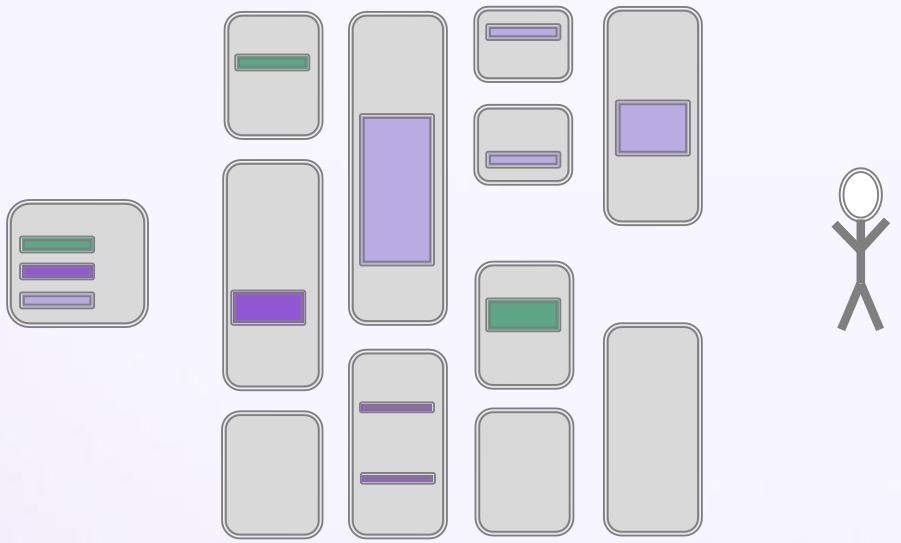
Hard Problem 1: **Scalability and Composability**

Challenge

- Develop methods to enable the construction of secure systems with **known security properties**.

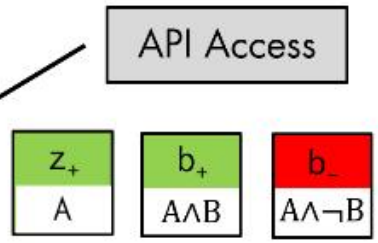


Component and Configuration Change



Configuration Map

true	`boolean z = hasA();`
true	`if(z) {`
A	`method1();`
A	`boolean b = hasB();`
	`if(z && !b) {`
	`method2();`
	`}`
	`} else {`
	`method3();`
	`}`



$A \wedge \neg A \Longrightarrow$ unsatisfiable

$A \wedge A \Longrightarrow A$

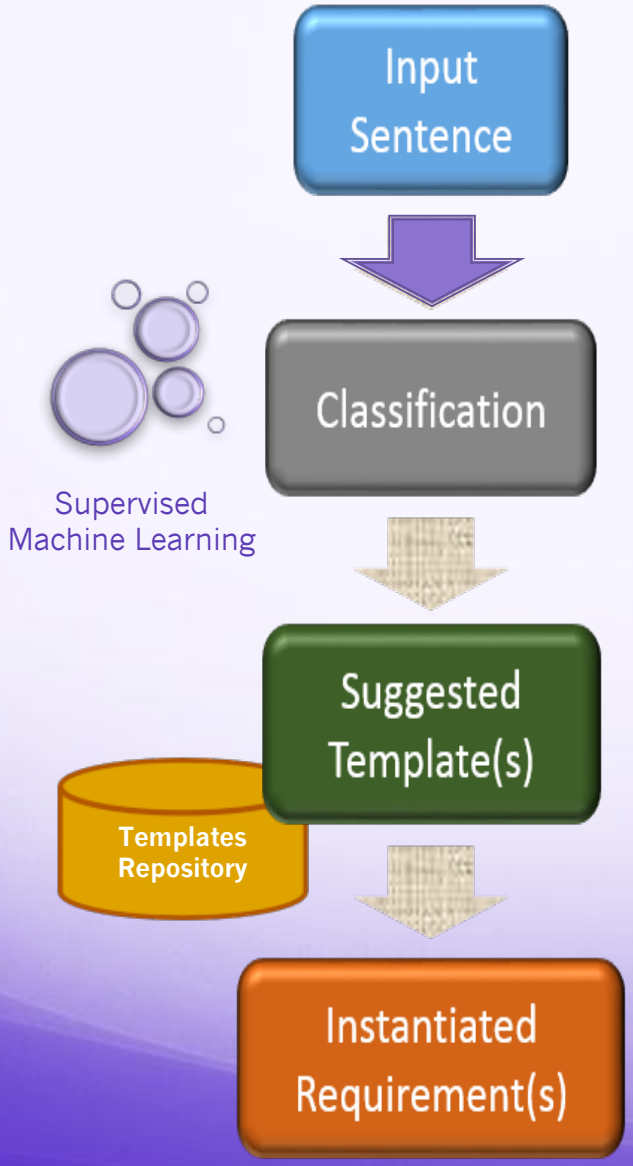
Hard Problem 2: **Policy-Governed Secure Collaboration**

Challenge

- Develop methods to express and enforce normative requirements and policies for handling data with **differing usage needs** and among users in **different authority domains**



Implied security and privacy requirements



*The system shall provide a means to **edit** discharge **instructions** for a particular patient.*

(a) Confidentiality (*of patient's discharge instructions*);
(b) Integrity (*when editing*);
(c) Accountability (*who performed the edit*);

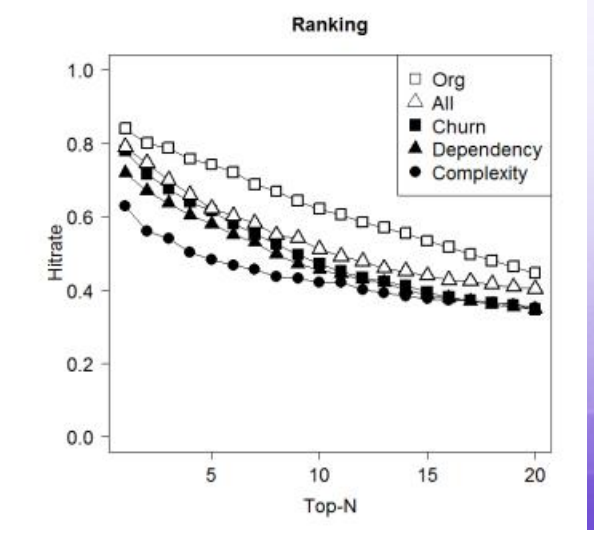
Confidentiality:
"The system shall enforce access privileges that **<enable | prevent> <subject>** to **<action> <resource>**.
"The system shall encrypt **<resource>** and store **<resource>** …."

Confidentiality:
"The system shall enforce access privileges that **enable authorized users** to **edit discharge instructions**. …"

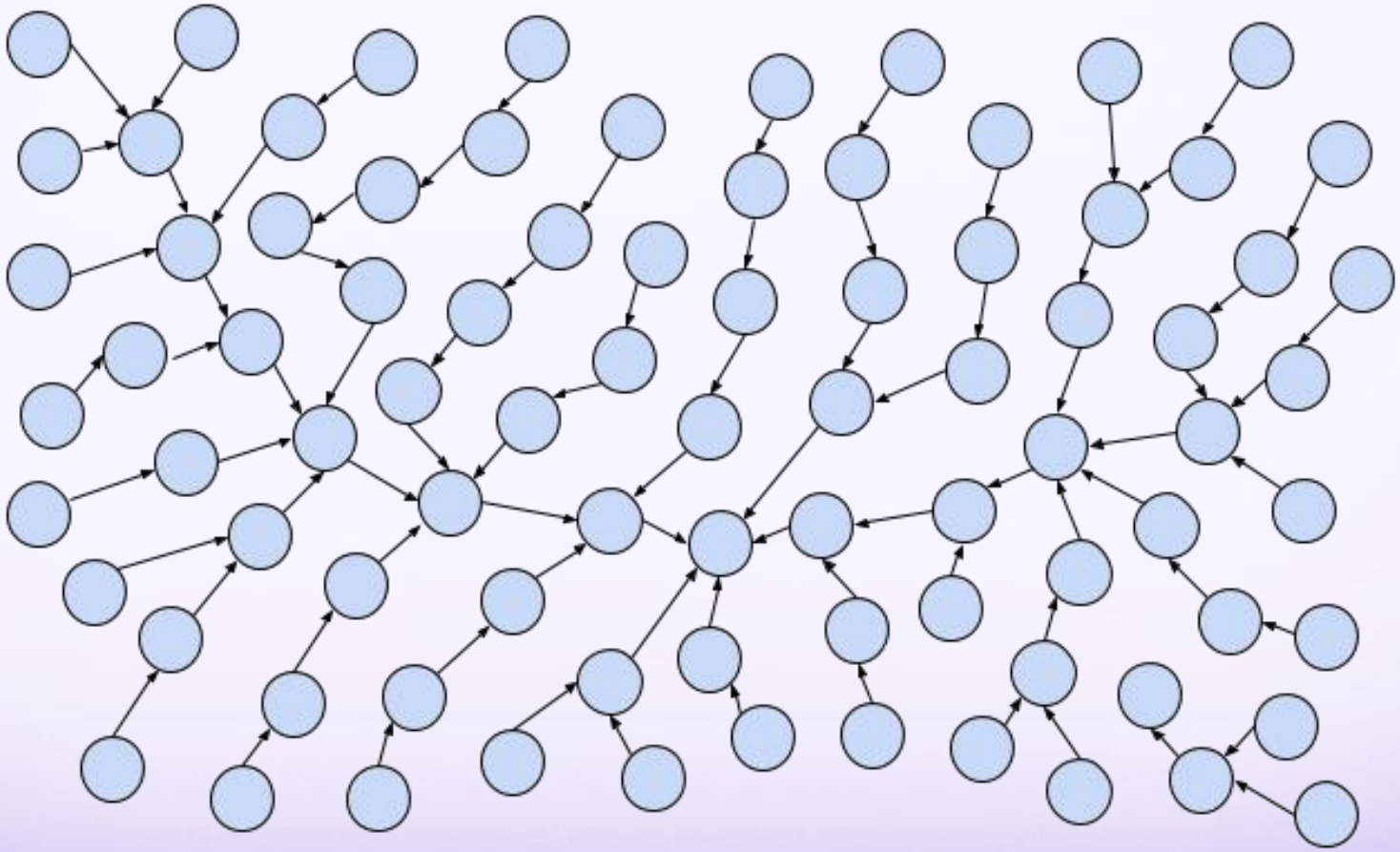
Hard Problem 3: **Predictive Security Metrics**

Challenge

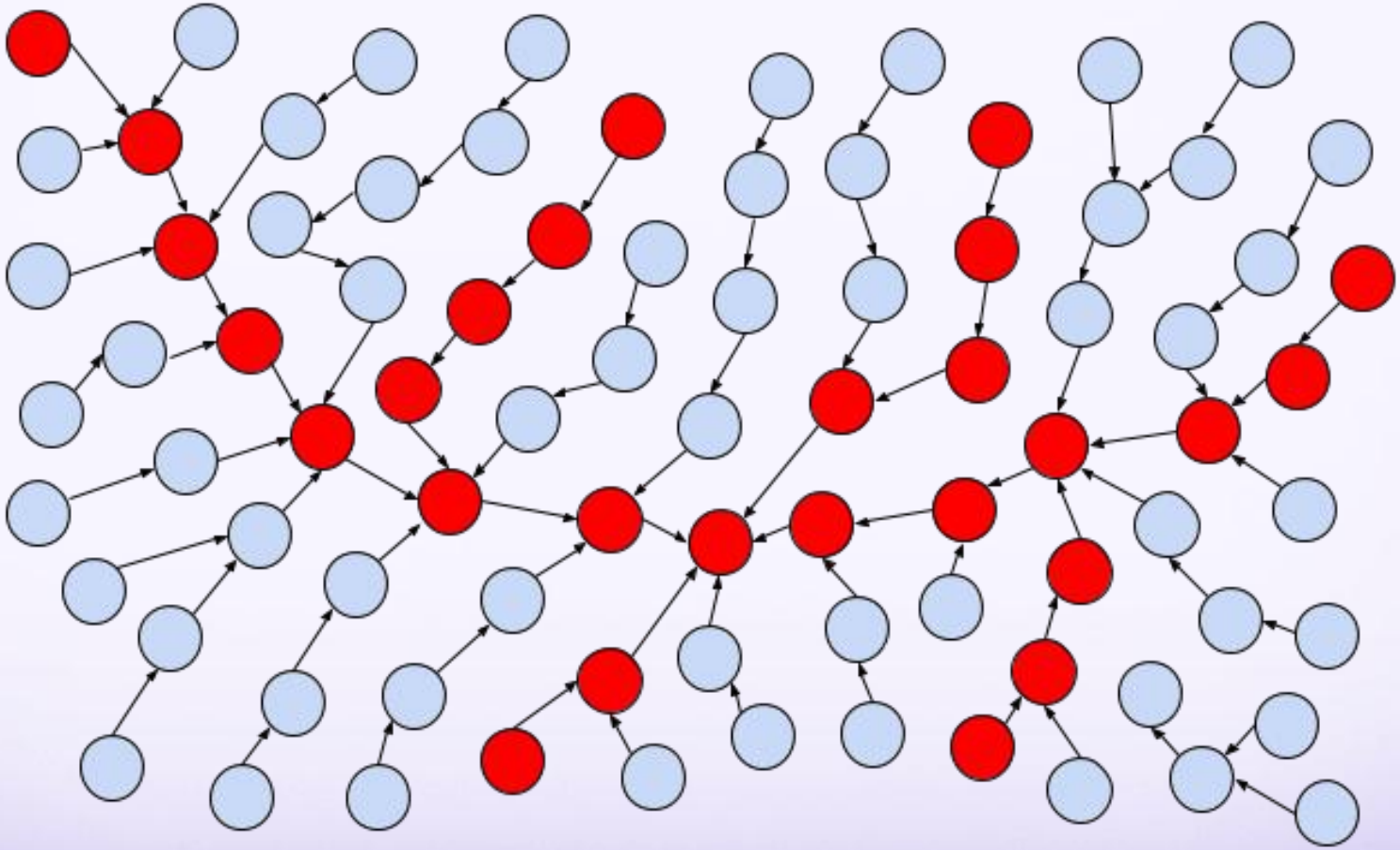
- Develop **security metrics and models** capable of predicting whether or confirming that a given cyber system preserves a given set of security properties (deterministically or probabilistically), in a given context.



Leveraging stack traces from crash dumps



Risk-based attack surface approximation

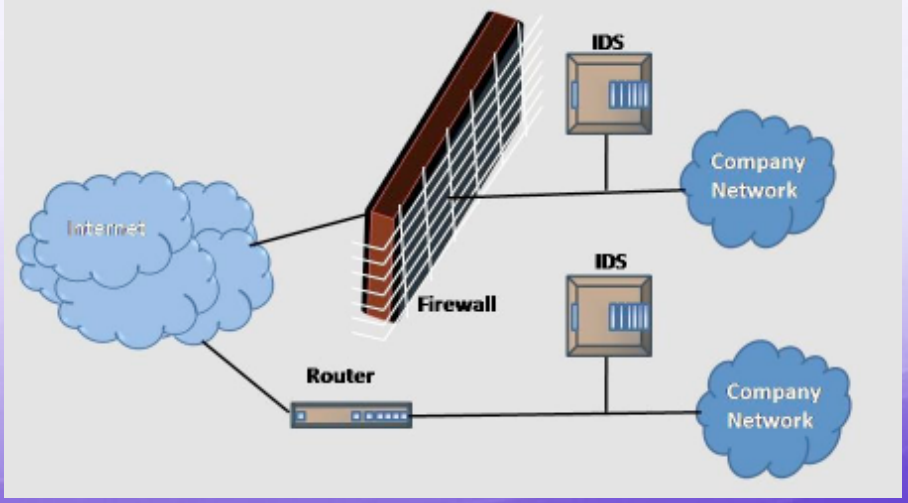


Windows: 48% of **all** binaries crash, 95% of **vulnerable** binaries crash.
Firefox: 16% of **all** files crash, 74% of **vulnerable** files crash.
Fedora: 8% of **all** packages crash, 60% of **vulnerable** packages crash.

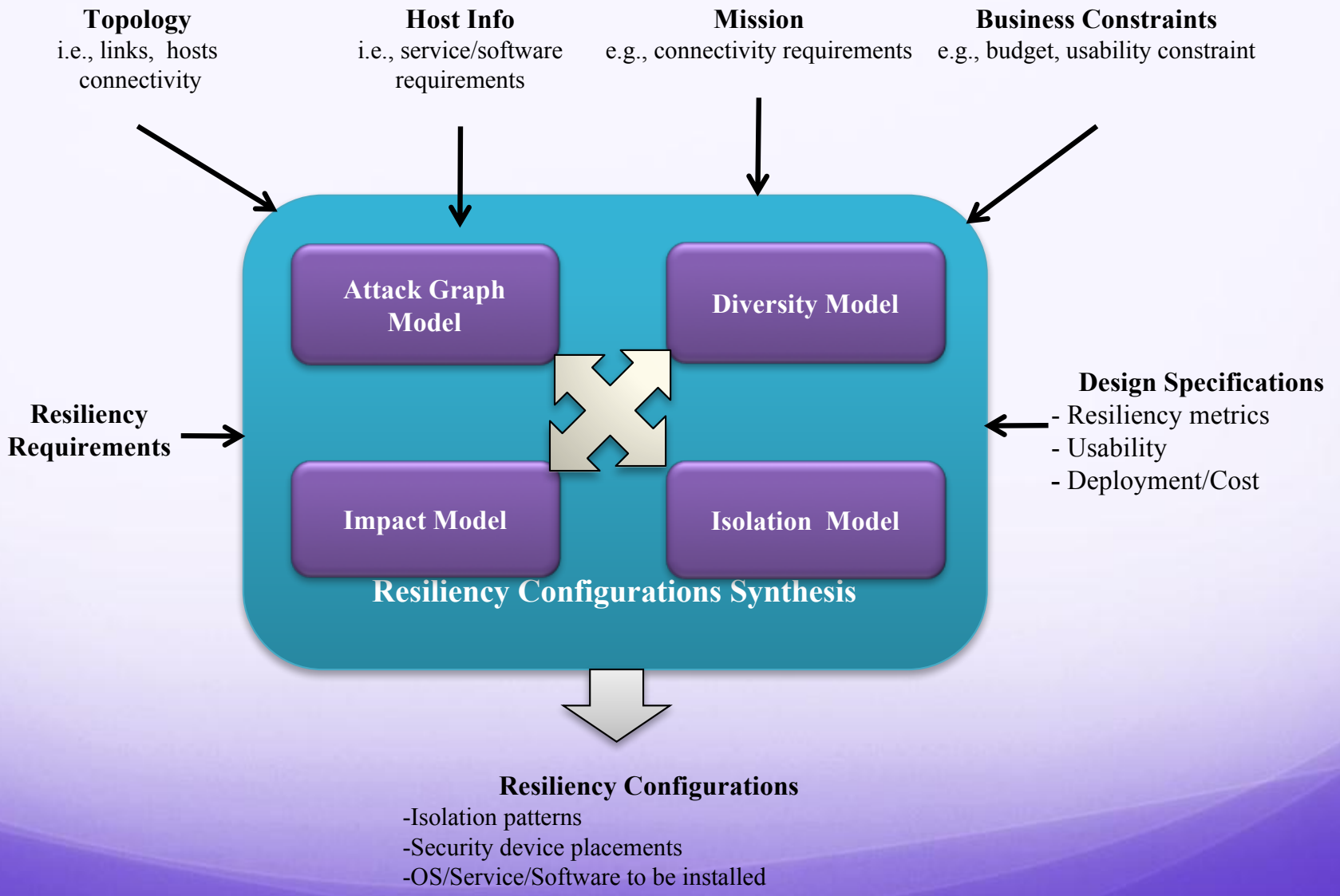
Hard Problem 4: **Resilient Architectures**

Challenge

- Develop means to design and analyze system architectures that deliver required service in the **face of compromised components**

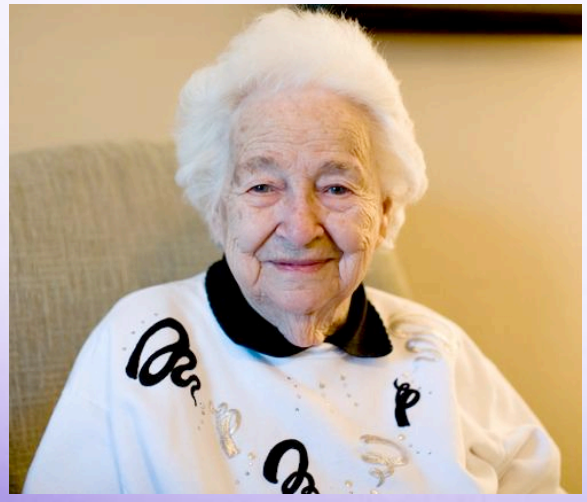


Synthesizing Network Security Configurations

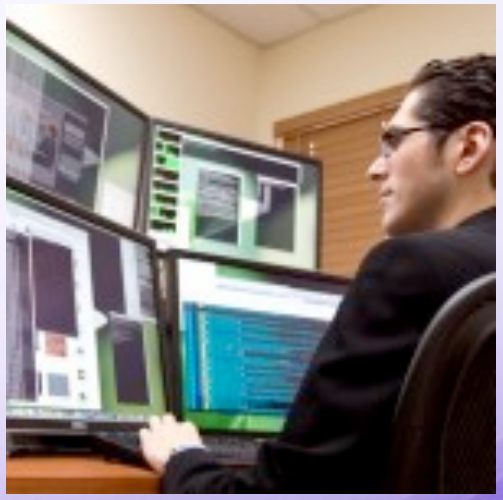


Hard Problem 5: **Human Behavior**

Develop models of human behavior (of both users and adversaries) that enable the design, modeling, and analysis of systems with specified security properties







Phishing: Personality & Persuasion




YOU BETTER WATCH
YOURSELF.....



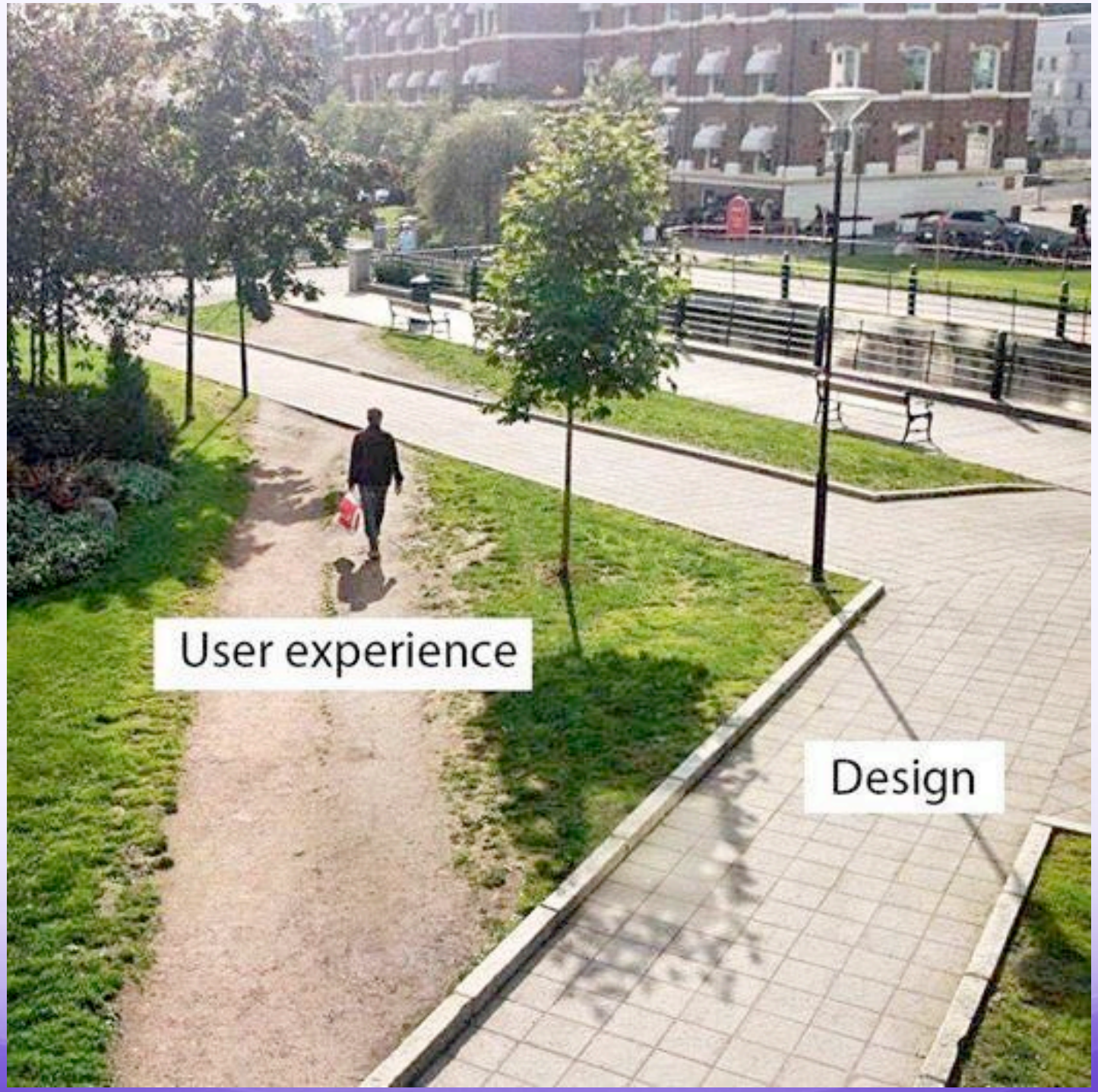
MAY 18, 2016 @ 12:23 PM 78,122

12 Stocks to

LinkedIn Resets Passwords As 117M Logins For Sale On Dark Web - UPDATED

LinkedIn Passwords

Rank	Password	Frequency
1	123456	753,305
2	linkedin	172,523
3	password	144,458
4	123456789	94,314
5	12345678	63,769
6	111111	57,210
7	1234567	49,652
8	sunshine	39,118
9	qwerty	37,538
10	654321	33,854
11	000000	32,490
12	password1	30,981
13	abc123	30,398
14	charlie	28,049
15	linked	25,334


User experience
Design

As Seen at NC State



Protect users from themselves … easily!



My Intentions

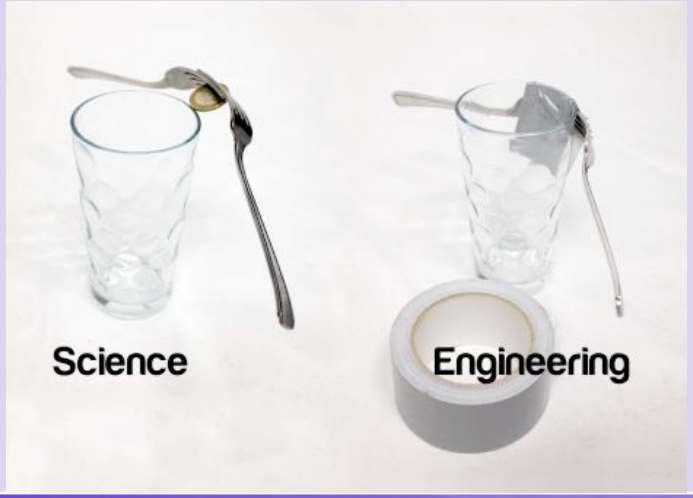
Security



Collaborative Research



Science



Life



Attackers Unceasing



Slide photos -1

- http://www.foxbusiness.com/markets/2017/07/13/verizon-customer-information-exposed-in-data-breach.html
- http://www.tomandjerryonline.com/images/TrapHappy1.jpg
- http://www.leftlion.co.uk/articles.cfm/title/the-three-musketeers/id/1539
- http://www.dailymail.co.uk/tvshowbiz/article-1085791/Free-DVD-The-Four-Musketeers-todays-Mail-Sunday.html
- https://www.reddit.com/r/pics/comments/1aw3f3/pathway/; http://www.bbc.co.uk/bristol/content/image_galleries/tunnel_gallery.shtml
- http://www.thomthom.net/gallery/everything/tunnel-vision/
- http://davemeehan.com/cycling/ojos-negros-tunnel-vision
- http://www.techsangam.com/wp33/wp-content/uploads/2011/05/1221_jargon-boil-the-ocean_485x340_forbes_com.jpg
- https://upload.wikimedia.org/wikipedia/en/3/33/Silicon_valley_title.png
- http://www.hindustantimes.com/india-news/tirupati-temple-andhra-pradesh-secretariat-hit-by-wannacry-ransomware-attack/story-UJorivWJKEe2CL2tTaDusK.html
- https://www.popxo.com/2016/12/stereotypes-about-introverts-and-extroverts-broken/
- http://www.[illegible]/images/pissed-off-obama/you-better-watch-yourself-[illegible].jpg

Slide photos - 2

- https://bizpsycho.files.wordpress.com/2015/05/colored_puzzle_connection_1600_wht_9893.png
- https://scottmccown.wordpress.com/category/competition/
- https://www.linkedin.com/pulse/standing-shoulders-giants-6-apis-instant-saas-success-nick-boucart
- http://thebsblog.com/2015/10/09/oops-wrong-diagnosis/#prettyPhoto/0/
- http://www.findmemes.com/eye-roll-memes
- http://user47329.vs.easily.co.uk/wp-content/uploads/2014/08/Science-v-Engineering-Wordpress3.jpg
- http://memegenerator.net/instance/59256035
- http://www.pxleyes.com/photoshop-contest/20606/makeover.html
- http://lorettalovehuffblog.com/
- http://itnewscast.com/book/export/html/62241
- http://www.jenningswire.com/book-coaches/searching-for-the-needle-in-the-haystack/
- https://www.bing.com/images/search?view=detailV2&ccid=Y%2bfsSC%2b6&id=00072BAC4D3C77ECF8E4AFFA13CCBFE0EC8E8A12&thid=OIP.Y-fsSC-6cSVEL_8ECb-wlgEsC7&q=capability+brown++bridges&simid=608050771047878264&selectedIndex=7&ajaxhist=0

Slide photos - 3

- http://1000awesomethings.com/2011/02/23/302-grandma-hair
- http://garysreflections.blogspot.com/2011/02/chinese-hackers-now-hitting-major.html
- http://www.my-programming.com/2011/10/how-to-become-a-programmer/
- http://www.govconexecutive.com/2011/02/executive-spotlight-joseph-cormier-of-gtec
- https://cdn.psychologytoday.com/sites/default/files/field_blog_entry_images/ext.jpg
- http://www.keywordsblogger.com/wp-content/uploads/2009/05/persuading.jpg
- http://www.zdnet.com/pictures/biggest-hacks-security-data-breaches-2016
- http://www.zdnet.com/article/these-are-the-worst-passwords-from-the-linkedin-hack/
- https://www.iii.com/sites/default/files/imce/Elizabeth_Image_for_Blog_July_2015.png
- https://www.magzter.com/news/488/1242/032017/er0pk
- http://www.youngwebbuilder.com/how-to-get-listed-on-justtweetit-directory/
- https://alisonhinksyoga.wordpress.com/2013/09/09/a-rising-tide-lifts-all-boats/

http://thecybersaviours.com/intrusion-detection-system-ids