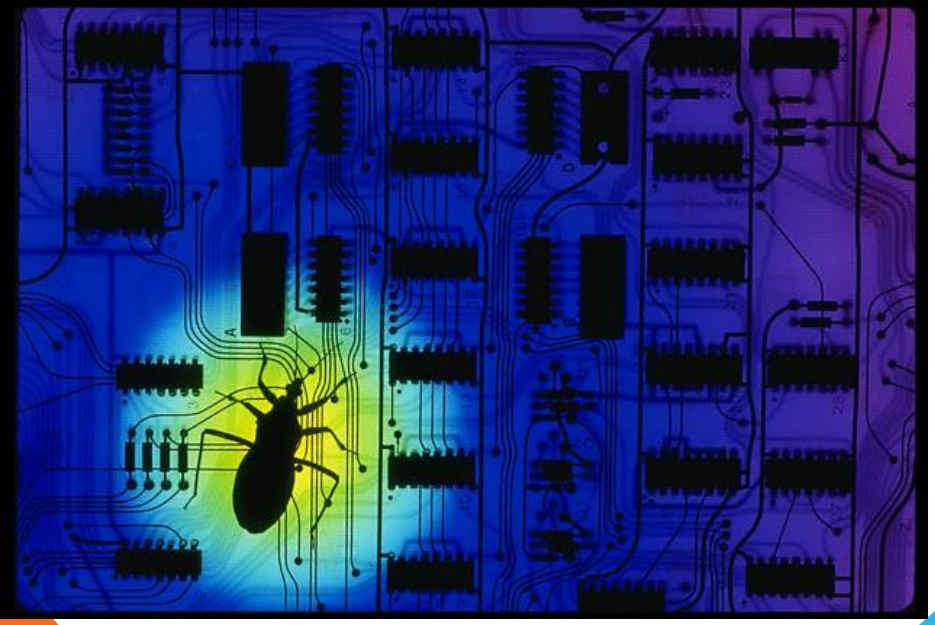


# *Imagineering an Internet of "Anything"*

JEFFREY VOAS, PHD, FIEEE, FAAAS
NIST

SERE'14, July 1, 2014

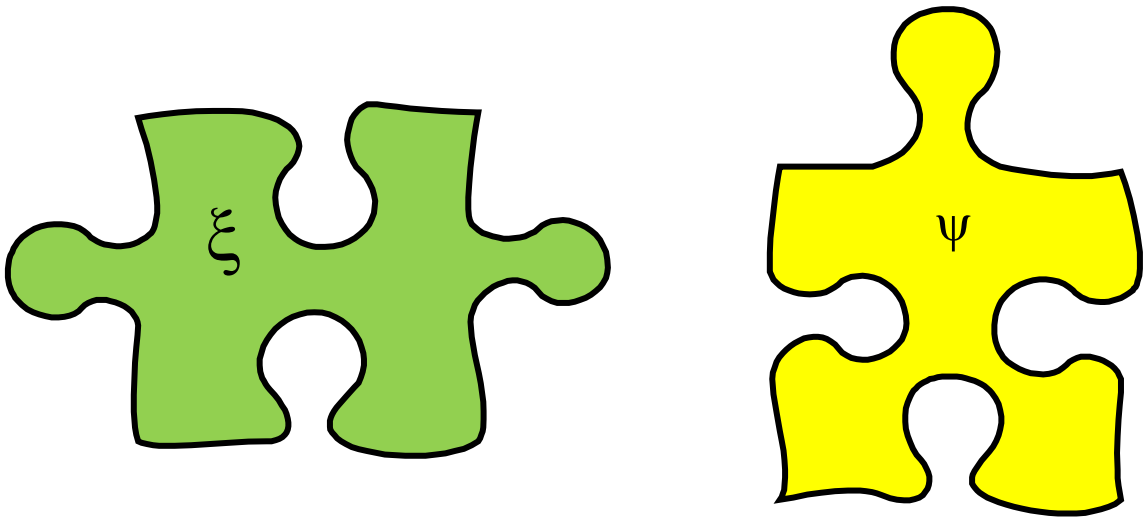
(Disclaimer: These Are Not The Official Positions of NIST on Topic)

# BACKGROUND

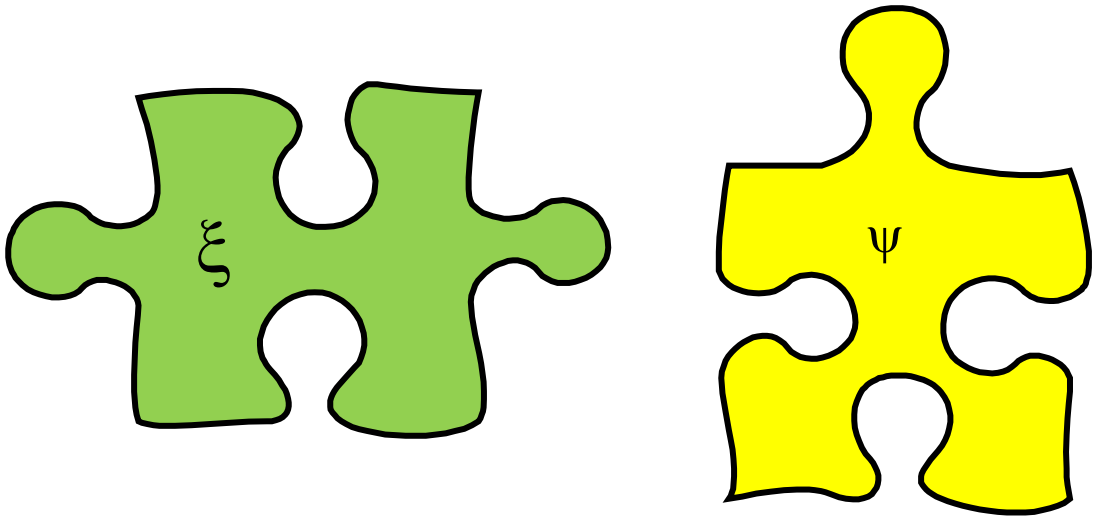
System-of-Systems Assurance (a type of Trust) is a function of, and minimally:

1. The degree to which *functional* system requirements are met,
2. The degree to which *inherited component behaviors* interoperate, i.e., cooperate and do not induce interference, and
3. The degree to which the "*shall not*" requirements are defined, and met, if at all.

# CONSIDER TWO COMPONENTS



# INHERITED COMPONENT BEHAVIORS



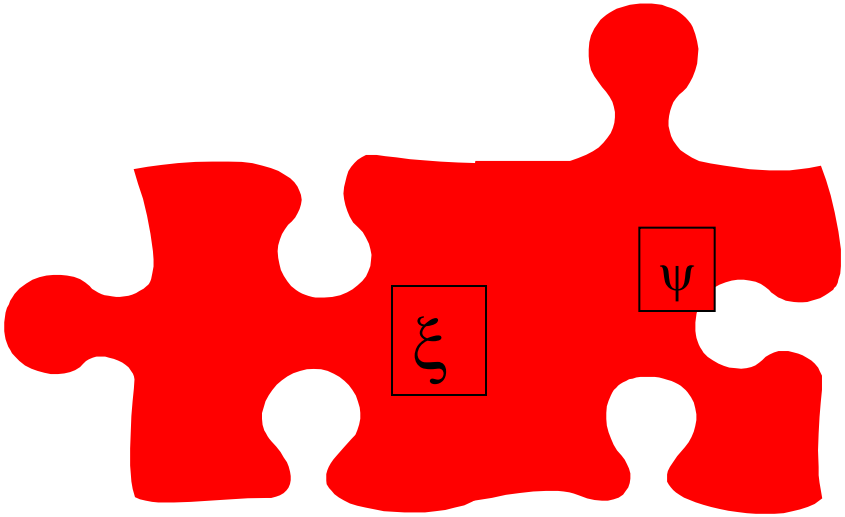

Component $\xi$ has inherited behaviors:

($a$R, $b$P, $c$F, $d$Sa, $e$Se, $f$A, $g$T, $h$M)

Component $\psi$ has inherited behaviors:

($i$R, $j$P, $k$F, $l$Sa, $m$Se, $n$A, $o$T, $p$M)

# COMPOSING PRE-INHERITED PROPERTIES




- $F(\xi \circ \psi)$ (“the marriage”) will inherit the Component’s Inherited Behaviors
- Same as genetics
- *A priori* knowledge of $F(\xi \circ \psi)$ preferred

# ATTRIBUTES NEED TO BE PRE-DEFINED

- Requirements should prescribe at some level of granularity as to what the weights are for various “ilities”, as well as how much of each “ility” is desired.

- But HOW?

- Ignoring the  attributes is not an option for achieving high assurance and trustworthy systems!

# WEIGHTING IS IMPORTANT

$w_1$R $w_2$P $w_3$F $w_4$Sa
$w_5$Se $w_6$A $w_7$T $w_8$M

in order to not over-design any attribute into the system.

For example, for an web-based transaction processing application, $w_4$ would probably equal 0.0 and $w_7$ would also be less than something like $w_2$

# TRADEOFFS

How much will you spend for increased reliability knowing that doing so will take needed, financial resources away from security or performance or …?

# EXAMPLES

- Security *vs.* Performance
- Fault tolerance *vs.* Testability
- Fault tolerance *vs.* Performance

etc.

# COUNTERINTUITIVE REALITIES

- 100% safety and 0% reliability
- 100% reliability and 0% safety
- 0% functionality/reliability and 100% security
- 100% availability and 0% reliability
- 100% availability and 0% performance
- 0% performance and 100% safety

# CULPRIT?

YES


Systems can remain static, but environments are dynamic due to time (e.g, they have a nasty temporal side to them).

# IoT (1)

We, as researchers, have a unique opportunity to get in early and create a compass that defines and measures the “so-called” Internet-of-Things (IoT). The business case is that IoT is a reported $19T business [REF: slide 14]. The research case is to define: (1) What are the needed IoT measures?, (2) What are the defining attributes of IoTs?, and (3) What are the lingering trust concerns of this loosely defined and likely unbounded infrastructure that is composed from differing entities? Understand that these entities are likely unfriendly, and supply-chain issues will play a key role. And are expecting specific environments.

In public discourse, big data is often discussed in terms of "meta data." In IoT, there is a similar concept: meta-ilities, and in particular, (1) Scalability, and (2) Heterogeneity. These 2 meta-ilities are unique due to complexity, and exemplify why IoT is a different problem than past efforts for distributed systems, communication networks, and systems-of-systems. This may be, ultimately, a sensors and algorithms problem with abundant wireless security concerns. Note that all of the classical "ility” concerns still apply (i.e., reliability, performance, fault tolerance), but they are sub-ilities, somewhat dwarfed to the meta-ilities.

I prefer the term of Internet of Anything (IoA). I accept the fact that all I can control would be a private network of things (PNoT).

# IoA (2)

The tenets of IoA are: (1) Things communicate, (2) Things may also sense, (3) Things should be physical (or some argue that software component should be tagged as 'things'), (4) Communications will be mostly wireless due to scale and limitations of wired infrastructure, (5) On board algorithms and software implementations own and control sensor I/O, (6) Things are almost certainly heterogeneous, (7) Are people things?

Why state "Internet of Anything" ? The answer is distributed automation; it creates identity control and management issues such as: (1) Are you a thing or human? (2) Who are you if you are human? (3) Where is where (geo-location )? (4) When is when (time is tamper-able)? (5) The unknowns of unknowns of future things, These all play into an IoA trust story. The key points dissolve down to the fact that truth is not malleable, trust is, and in IoA, that malleability is dis-concerning. It also begs the question as to whether we need an IoA separated from an Internet of Humans (IoH).

# IoA (3)

We, as computer scientists, have a unique opportunity to bound and define security and privacy IoA issues. Without doing this, we will be tackling isolated IoA problems of smaller consequence after others have informally defined the space, and we will likely wind up with *de facto* standards/definitions that make standards and measurement difficult, and certainly if they are closed/proprietary.

Based on the above, I argue that: (1) Trust in IoA is minimally a function of: wireless, security, privacy, sensors, algorithms, interfaces, and interoperability/composability, (2) Scalability fuels complexity, (3) Heterogeneity exacerbates interoperability problems, (4) Privacy falls victim to sensors and wireless communications, (5) Malicious code and associated algorithms will abound (no doubt), (6) Testing techniques such as combinatorial testing might be a chance to address the aforementioned scalability and heterogeneity concerns, (7) Traditional reliability testing is near useless due to scale in a timely manner, and (8) Millions of new things are being attached every day.

http://www.washingtonpost.com/business/on-it/cisco-ceo-at-ces-2014-internet-of-things-is-a-19-trillion-opportunity/2014/01/08/8d456fba-789b-11e3-8963-b4b654bcc9b2_story.html

# BASED ON THIS .....

System-of-Systems Assurance (a type of Trust) is a function of, and minimally:

1. What could ever be believable *functional* system requirements for the IoA or PNoT? and,

2. The degree to which *inherited component behaviors* interoperate, i.e., cooperate and do not induce interference. What does that even mean in IoA?

# AND BASED ON THIS .....

We have people (and orgs) that are creating definitions and policies for which they appear to have no evidence.

Our small group at NIST is planning a PNoT lab to better understand the problem space before giving guidance or recommendations, let alone definitions and policies.

We hope to have preliminary results in early 2015 that offer insights into the security and performance issues of a PNoT. (Possibly reliability insights as well.)

We also intend to publish use cases for testing an IoT solution (commercial or open) for orgs before they adopt it.