JOHN MENERICK

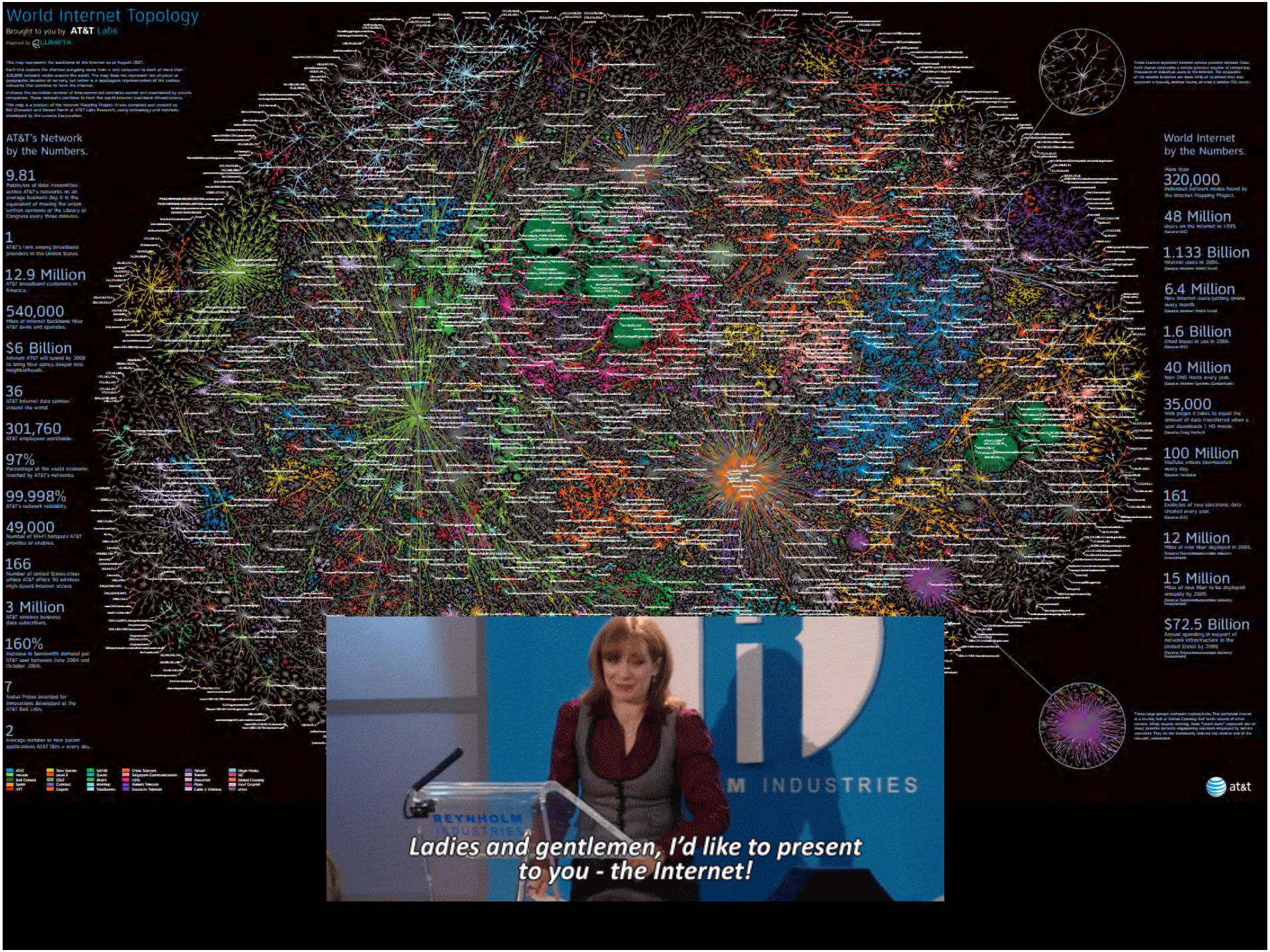
# OPEN SOURCE FAIRY DUST

# SECURITY DRAGON @ NETSUITE

THE VIEWS AND OPINIONS EXPRESSED HERE ARE MY OWN ONLY AND IN NO WAY REPRESENT THE VIEWS, POSITIONS OR OPINIONS - EXPRESSED OR IMPLIED - OF MY EMPLOYER (PRESENT AND PAST) OR ANYONE ELSE. MY THOUGHTS AND OPINIONS CHANGE FROM TIME TO TIME; THIS IS A NATURAL OFFSHOOT OF HAVING AN OPEN AND INQUISITIVE MIND.

WHAT WE ARE NOT TALKING ABOUT

# WHAT WE ARE TALKING ABOUT


World Internet Topology
Brought to you by AT&T Labs
Powered by LUMETA
This map represents the backbone of the Internet as of August 2007.
Each line depicts the shortest outgoing route from a test computer to each of more than 320,000 network nodes around the world. The map does not represent the physical or geographic location of servers, but rather is a topological representation of the various networks that combine to form the Internet.
It shows the incredible number of interconnected networks owned and maintained by private companies. These networks combine to form the real-life Internet backbone infrastructure.
This map is a product of the Internet Mapping Project. It was compiled and created by Bill Cheswick and Steven Hardy at AT&T Labs Research, using technology and methods developed by the Lumeta Corporation.
AT&T's Network by the Numbers.
9.81
Petabytes of data transmitted across AT&T's networks on an average business day. It is the equivalent of moving the entire written contents of the Library of Congress every three minutes.
1
AT&T's rank among broadband providers in the United States.
12.9 Million
AT&T broadband customers in America.
540,000
Miles of Internet backbone fiber AT&T owns and operates.
$6 Billion
Amount AT&T will spend by 2008 to bring fiber optics deeper into neighborhoods.
36
AT&T Internet data centers around the world.
301,760
AT&T employees worldwide.
97%
Percentage of the world economy reached by AT&T's networks.
99.998%
AT&T's network reliability.
49,000
Number of Wi-Fi hotspots AT&T provides or enables.
166
Number of United States cities where AT&T offers 3G wireless high-speed Internet access.
3 Million
AT&T wireless business data subscribers.
160%
Increase in bandwidth demand per AT&T user between June 2004 and October 2006.
7
Nobel Prizes awarded for innovations developed at the AT&T Bell Labs.
2
Average number of new patent applications AT&T files – every day.
AT&T
Verizon
Bell Canada
Sprint
NTT
Time Warner
Level 3
CW
Comcast
Cogent
SAVVIS
Qwest
Sharp
Worldcom
TeleGlobe
China Telecom
Singapore Communications
USA
Hanaro Telecom
Deutsche Telekom
Yahoo!
Telemar
Abovenet
Pipex
Cable & Wireless
Virgin Media
KD
Global Crossing
Tata/ Teleglobe
Level 3
Sprint
Global Crossing
Cogent
Verizon
Qwest
AT&T
Time Warner
Comcast
Cable & Wireless
Deutsche Telekom
Hanaro Telecom
NTT
Singapore Communications
China Telecom
Tata/ Teleglobe
Yahoo!
Telemar
Abovenet
Pipex
Virgin Media
KD
Global Crossing
Tata/ Teleglobe
World Internet by the Numbers.
More than
320,000
Individual network nodes found by the Internet Mapping Project.
48 Million
Users on the Internet in 1995.
1.133 Billion
Internet users in 2006.
6.4 Million
New Internet users getting online every month.
1.6 Billion
Email boxes in use in 2006.
40 Million
New DNS Hosts every year.
35,000
Web pages it takes to equal the amount of data transferred when a user downloads 1 HD movie.
100 Million
YouTube videos downloaded every day.
161
Exabytes of new electronic data created every year.
12 Million
Miles of new fiber deployed in 2005.
15 Million
Miles of new fiber to be deployed annually by 2009.
$72.5 Billion
Annual spending in support of network infrastructure in the United States by 2010.
M INDUSTRIES
REYNHOLM INDUSTRIES
Ladies and gentlemen, I'd like to present to you - the Internet!
at&t

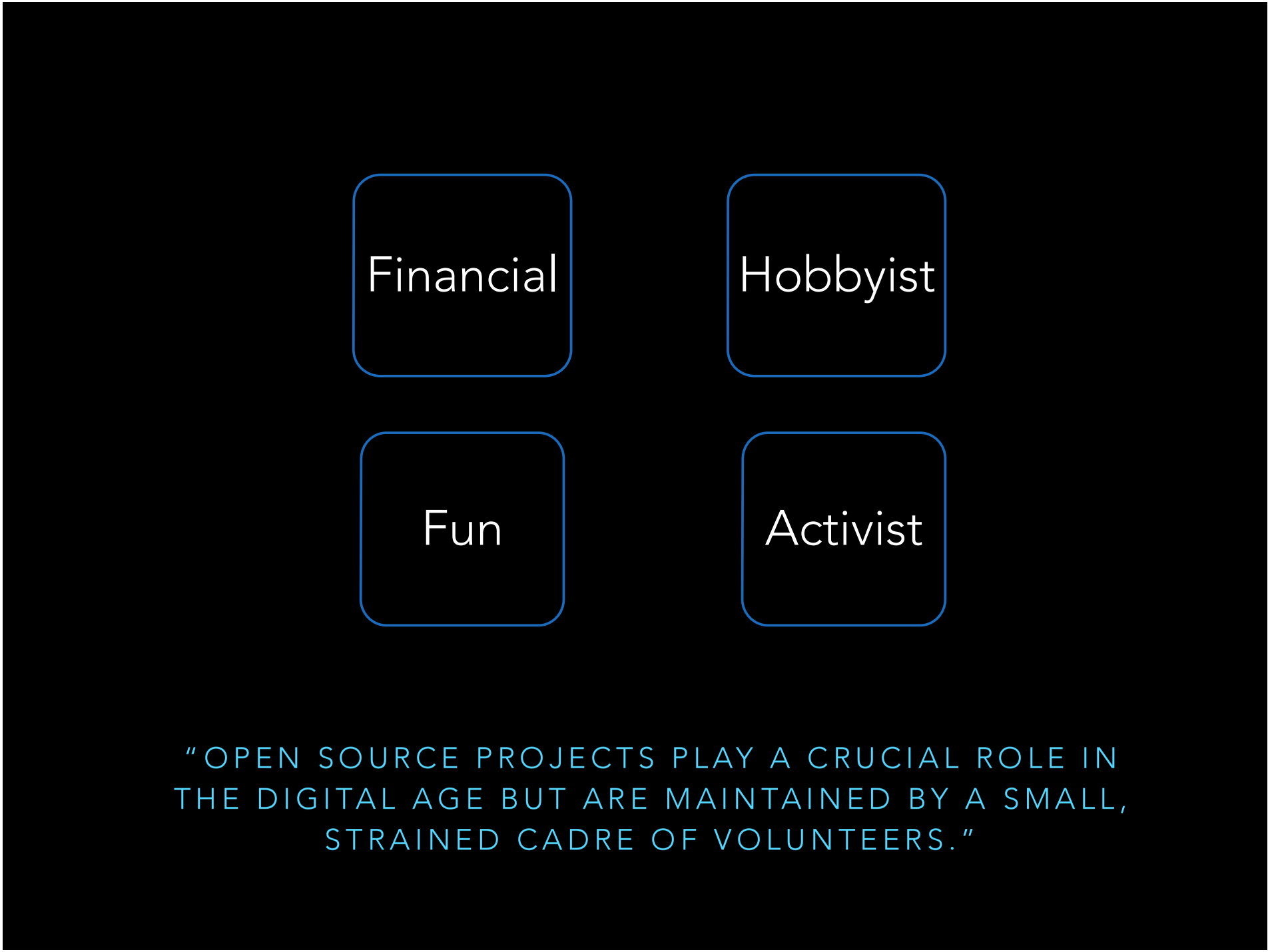
www.globalteckz.com
OPEN
SOURCE
SOFTWARE
FREE
WORK
COPYRIGHT
SYSTEM
INNOVATION
CONCEPT
CREATED
NEW
USING
LICENSE
FORMAT
LAW
PRODUCTS
CASE
ECONOMIC
ONE
SCIENTIFIC
DEVELOPMENT
FILE
STANDARDS
AVAILABLE
MEDIA
PROPERTY
ORGANIZATIONS
CULTURE
INTERNATIONAL
MOVEMENT
MAKING
COST
COMPANY
NOW
EDIT
COMMONS
ISBN
MODEL
USE
ONLINE
SYSTEMS
MADE
POTENTIAL
INITIATIVE
ETHICS
DESCRIBE
COMMUNITIES
COMPANIES
EXAMPLE
TECHNOLOGIES
PRODUCTION
EXPRESSION
CONTENT
PROCESS
BUSINESS
PRESS
PDF
BEER
MANY
CALLED
HARDWARE
CODE
MOVIE
LICENSES
USED
BEGAN
WEB
VOL
LIMITED
AUDIO
BASED
LIKE
OTHERS
FILM
IDEA
ERIC
CENTURY
RESEARCH
TERM
COMMUNITY
CULTURAL
PLATFORM
TECHNOLOGY
OPEN-SOURCE
COMPUTER
CREATIVE
INTERNET
SOCIETY
PUBLIC
EXAMPLES
PUBLISHING
ALSO
INFORMATION
NETWORK
SHARING
ECONOMICS
SIMILAR
DIGITAL
POLITICAL
PHARMACEUTICALS
MESSAGEBOARDS
BLOGS
RAYMOND
INCLUDING

NO ONE SAID IT WAS SECURE

"This is a story about four people named Everybody, Somebody, Anybody, and Nobody. There was an important job to be done and Everybody was asked to do it. Everybody was sure Somebody would do it. Anybody could have done it, but Nobody did it. Somebody got angry about that, because it was Everybody's job. Everybody thought Anybody could do it but Nobody realized that Everybody wouldn't do it.

It ended up that Everybody blamed Somebody when Nobody did what Anybody could have done."

EVERYBODY'S JOB IS NOBODY'S JOB


Financial
Hobbyist
Fun
Activist
"OPEN SOURCE PROJECTS PLAY A CRUCIAL ROLE IN THE DIGITAL AGE BUT ARE MAINTAINED BY A SMALL, STRAINED CADRE OF VOLUNTEERS."

Functionality

Stability

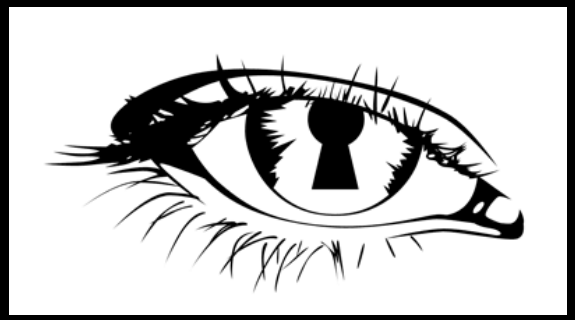
Compliance

Performance

Usability

Security

"THERE ARE LOTS OF CRITICAL LIBRARIES MAINTAINED BY VOLUNTEERS THAT ARE NOT GIVEN ENOUGH ATTENTION"



" The system must not require secrecy and can be stolen by the enemy without causing trouble. "

"MEMORY LIFECYCLE AND BOUNDARY MANAGEMENT IS A BITCH IN APPLICATION LOGIC"

C / C++

"IT IS NOT LIKE JAVA GOT INSECURE ALL OF A SUDDEN. IT HAS BEEN INSECURE FOR YEARS."

JAVA

# PHP 0DAY FOR EVERYONE

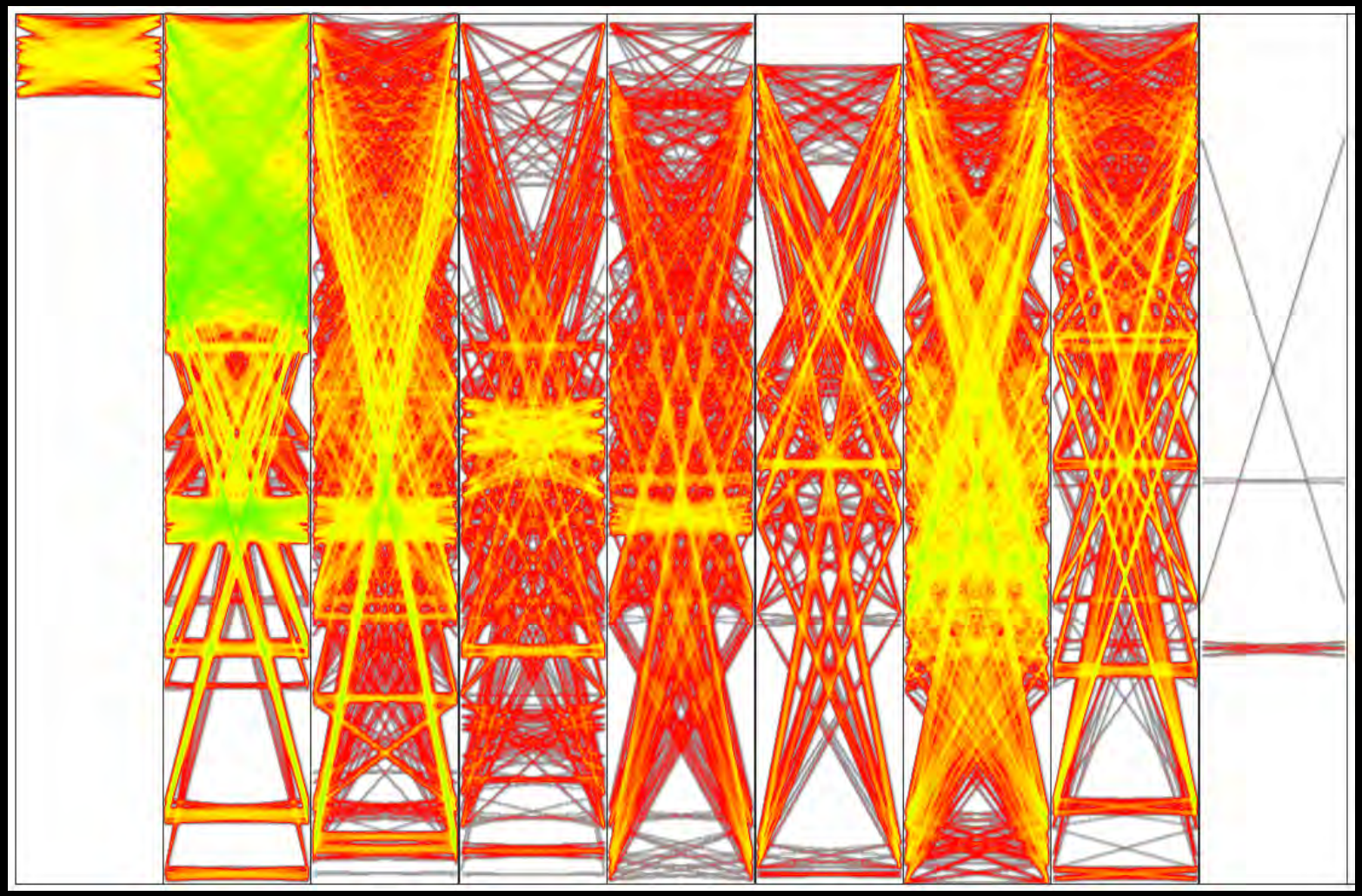
PHP

SOMETHING'S FUCKY
quickmeme.com

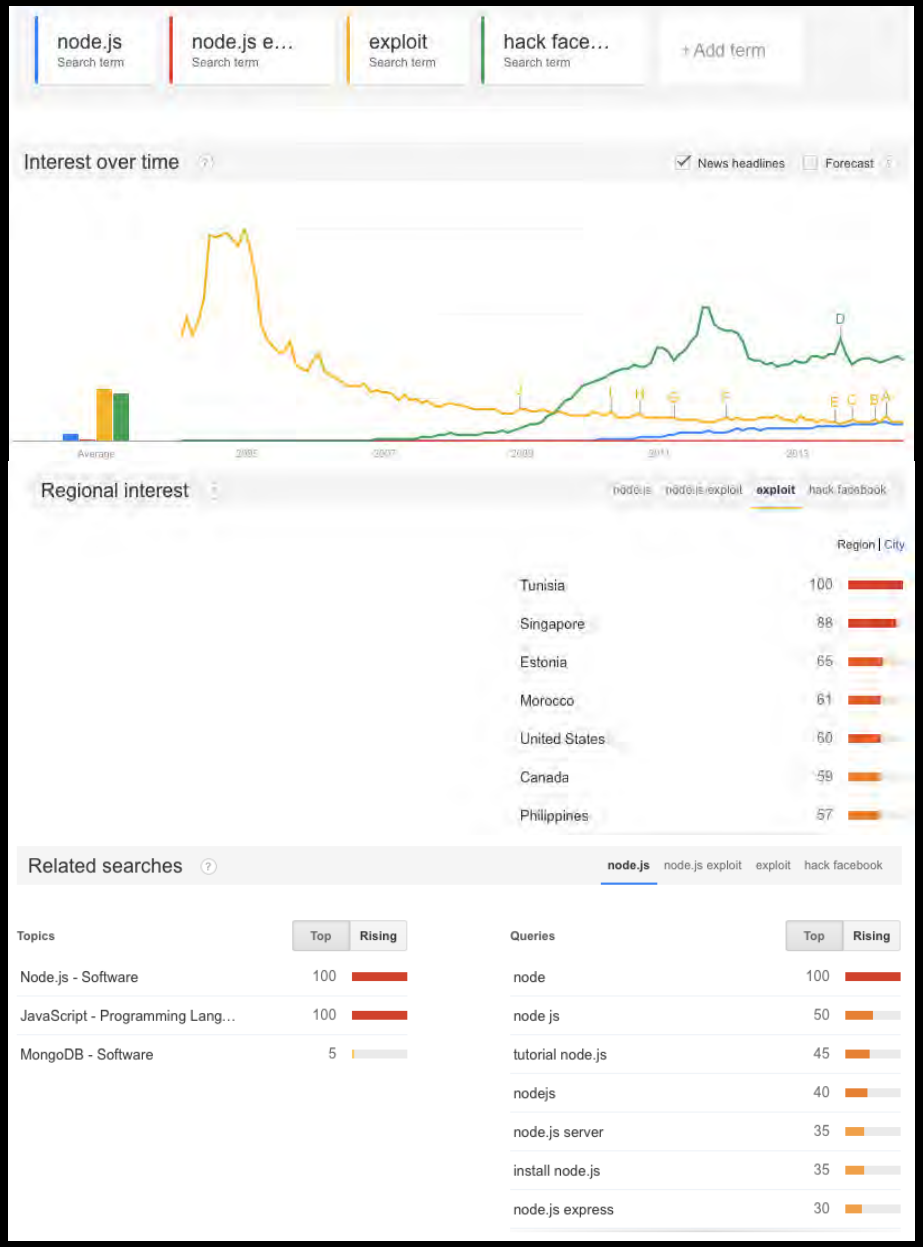
LOST
CONFUSED
UNSURE
UNCLEAR
PERPLEXED
DISORIENTED
BEWILDERED

NO STRATEGY

NO SECURITY CONTACT OR REPORTING DEFINED



Inconsistent coding styles, usage, or complex code




TRENDING UPWARD VS LOW MATURITY

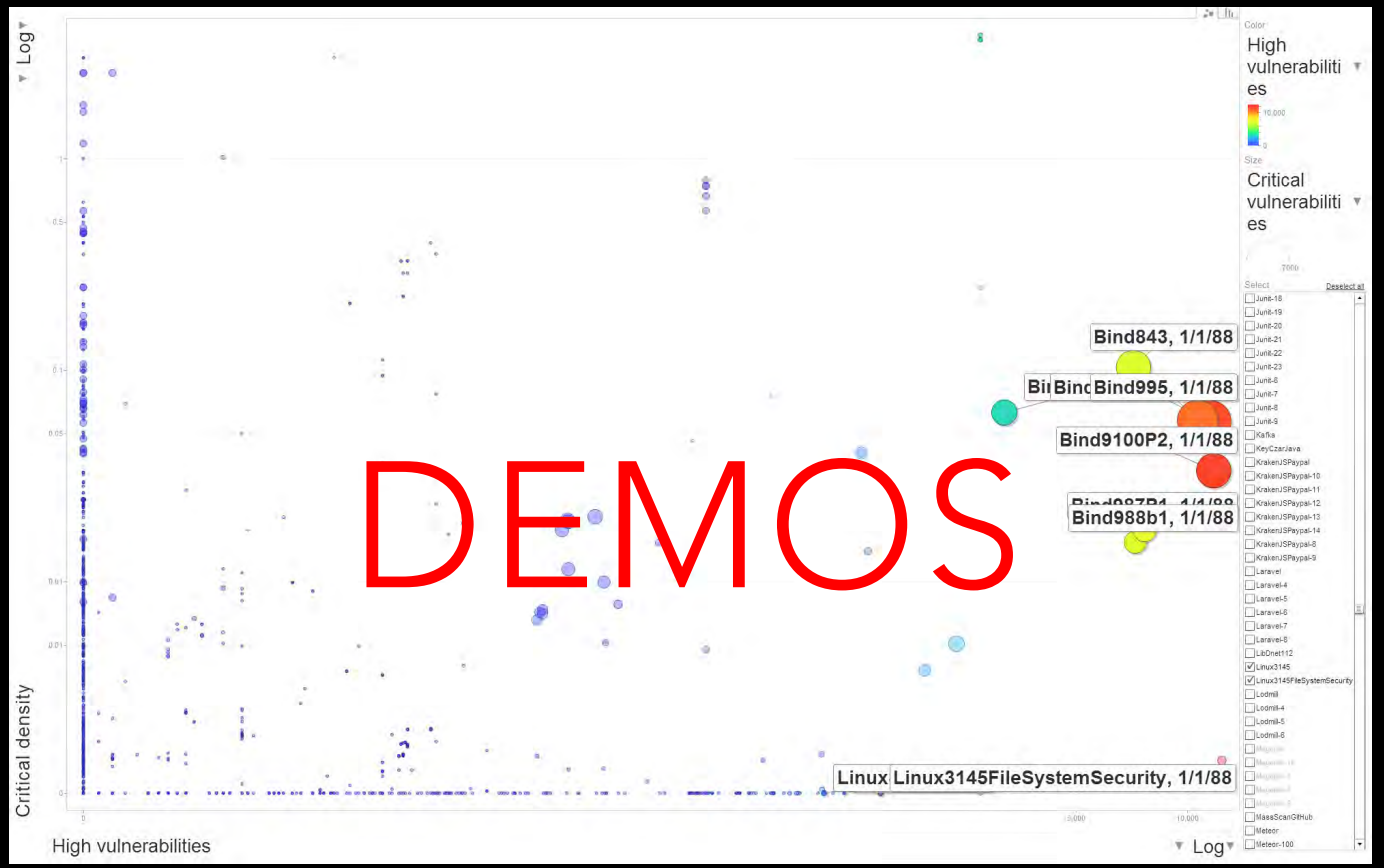
"System administrators hate change when they have to bear the brunt of adverse effects of change."

CHANGE IS HARD

where are we now?

Vulnerability
Just Ahead

50
FEDERAL RESERVE NOTE
50
EE 00000000 T
E5
SPECIMEN
THE UNITED STATES OF AMERICA
SPECIMEN
EE 00000000 T
50
50
FIFTY
DOLLARS


Log
Critical density
High vulnerabilities
Log
Color
High vulnerabilities
Size
Critical vulnerabilities
Bind843, 1/1/88
Bind995, 1/1/88
Bind9100P2, 1/1/88
Bind988b1, 1/1/88
Linux3145FileSystemSecurity, 1/1/88
DEMOS

# I AM LEGION

(AND SO CAN YOU!)

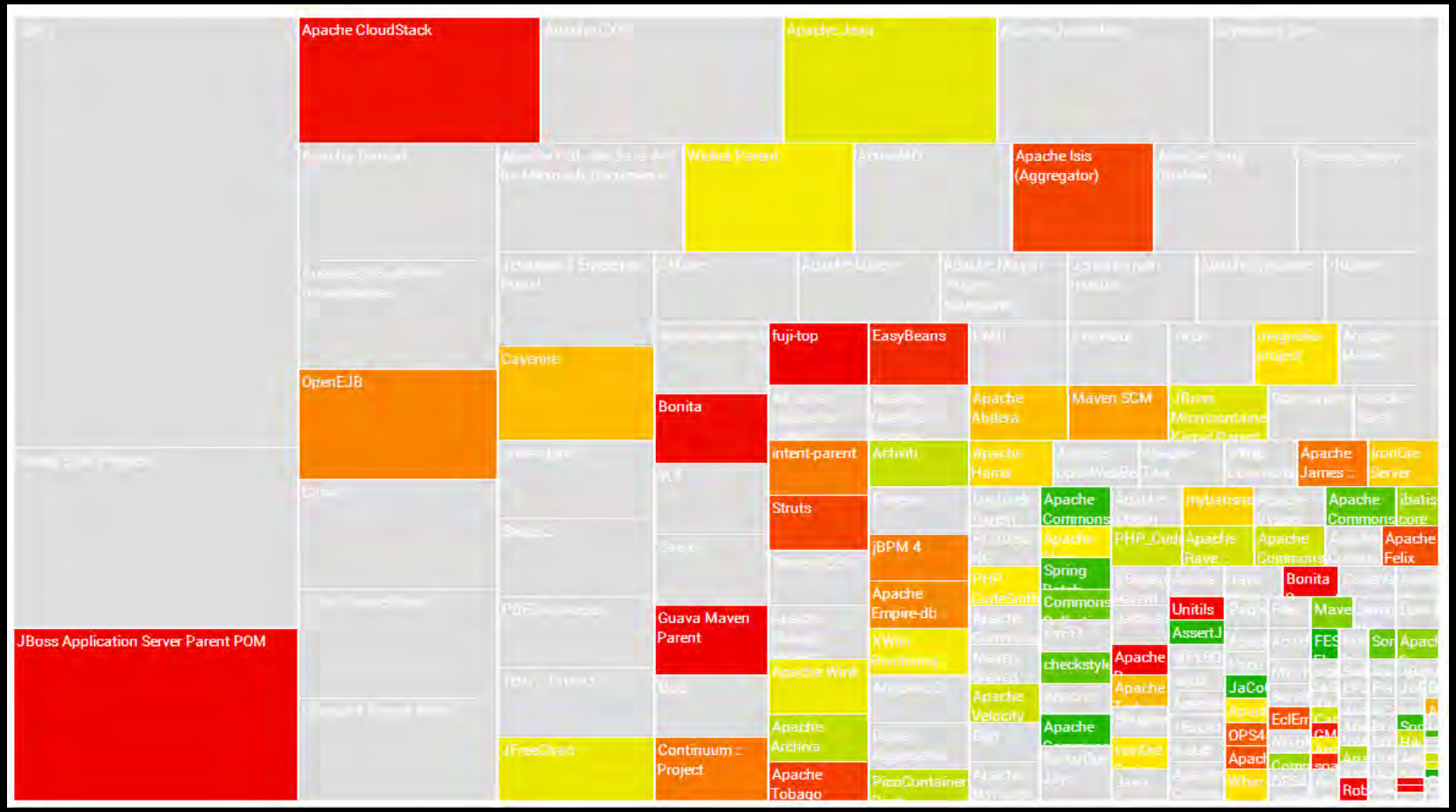
WHAT DO WE DO NOW?

FULL DISCLOSURE

STREET CRED

LULZ

WHAT IS YOUR INCENTIVE?


Apache CloudStack
Apache Isis (Aggregator)
fuji-top
EasyBeans
OpenEJB
Cayenne
Bonita
Apache Abdera
Maven SCM
intent-parent
Activiti
Apache Hama
Apache James
IronOre Server
Struts
Apache Commons
jBPM 4
Apache Rave
Apache Commons
Apache Felix
Spring
Apache Empire-db
Commons
Unitils
AssertJ
Bonita
Guava Maven Parent
JBoss Application Server Parent POM
checkstyle
Apache Velocity
Apache Archiva
Apache Tobago
Continuum :: Project
JFreeChart
PicoContainer

OBSTACLES

git

BRAKEMAN

amazon web services

FORTIFY

LLVM

COMPILER INFRASTRUCTURE

dtrace

VERACODE

National Vulnerability Database
nvd.nist.gov

Inspected with sonarqube

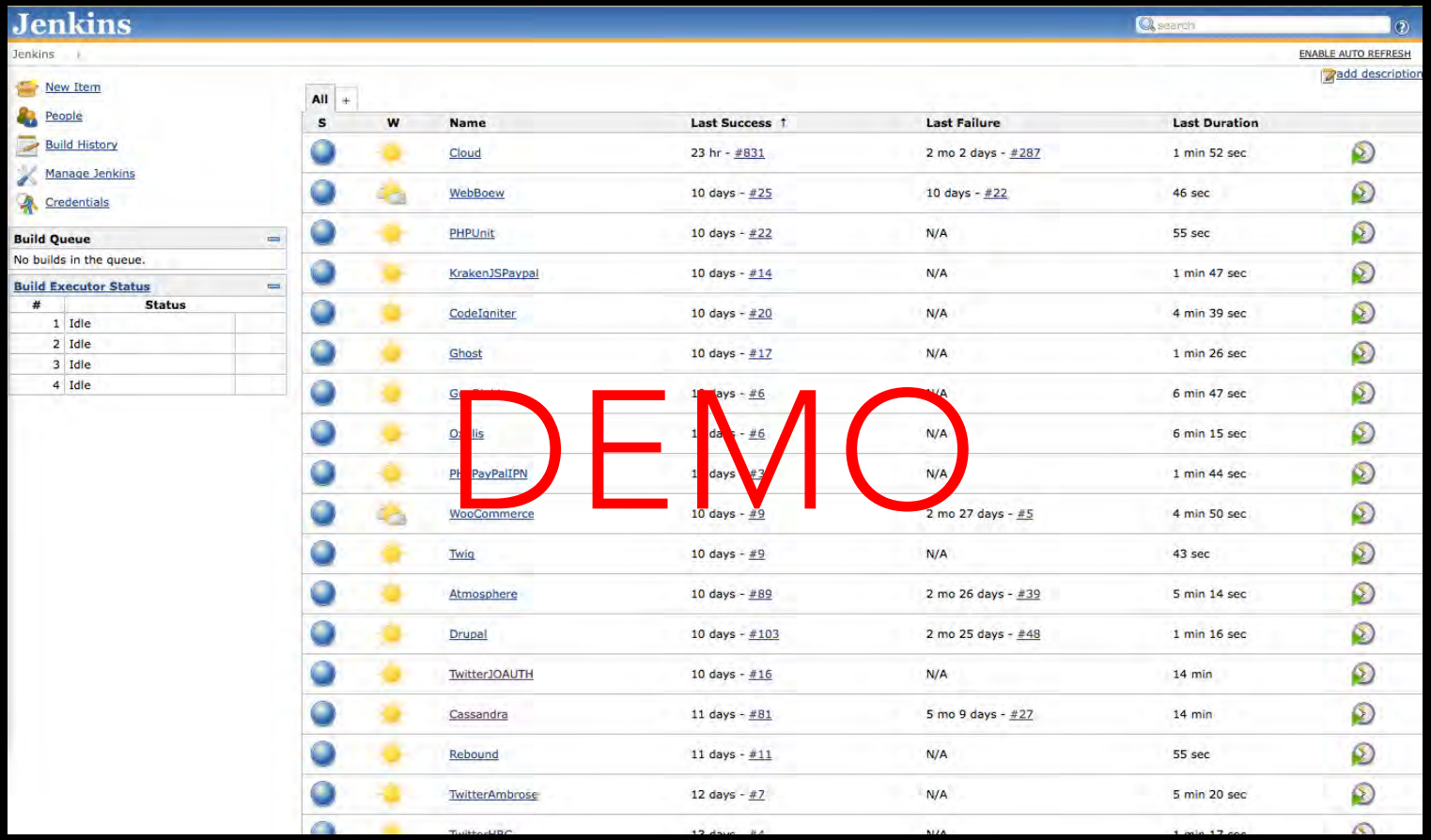
PEACH FUZZER

TOOLING

1: APPLY: $\mathcal{G}$ to $\mathcal{P}$ to create subpopulations: $\{\mathcal{P}_{\mathcal{G}_1}, \ldots, \mathcal{P}_{\mathcal{G}_m}\}$
2: **for all** $\mathcal{P}_{\mathcal{G}_i}$ **do**
3: $\quad \mathcal{P}_{\mathcal{G}_i}.\hat{p} \leftarrow \mathcal{P}_{\mathcal{G}_i}.s / \mathcal{P}_{\mathcal{G}_i}.n$
4: **if** $\max_{\mathcal{P}_{\mathcal{G}_i}} \mathcal{P}_{\mathcal{G}_i}.n < 51$ **then**
5: $\quad p_0 \leftarrow \left(\frac{1}{m}\right) \sum_{i=1}^{m} \mathcal{P}_{\mathcal{G}_i}.\hat{p}$
6: **else**
7: $\quad p_0 \leftarrow 0.85$
8: **for all** $\mathcal{P}_{\mathcal{G}_i}$ **do**
9: $\quad$ **if** $\mathcal{P}_{\mathcal{G}_i}.s = 0$ and using *NO-SUCCESS HEURISTIC* **then**
10: $\quad\quad$ Discard $\mathcal{P}_{\mathcal{G}_i}$
11: $\quad$ **else**
12: $\quad\quad \mathcal{P}_{\mathcal{G}_i}.z \leftarrow (\mathcal{P}_{\mathcal{G}_i}.\hat{p} - p_0)/\sqrt{p_0(1-p_0)/\mathcal{P}_{\mathcal{G}_i}.n}$
13: CREATE equivalence classes $\{E_{z_1}, \ldots, E_{z_k}\}$: $E_{z_i} \leftarrow \{\mathcal{P}_{\mathcal{G}_j} \cap \mathcal{E} | \mathcal{P}_{\mathcal{G}_j}.z = z_i\}$
14: SORT $\{E_{z_1}, \ldots, E_{z_k}\}$ by $z_i$ in descending order. Designate that order as $\{E_{z_{(1)}}, \ldots, E_{z_{(k)}}\}$.
15: **for all** $i = 1, \ldots, k$ **do**
16: $\quad$ Inspect error reports in $E_{z_{(i)}}$ using an auxiliary ranking scheme

```
1  I ← H
2  while U ≠ ∅
       do
3          for each r in U
               do
4                  r.prob ← UPDATEPROBABILITY(r, I, M)
5                  r.info ← INFOGAIN(r, U, I, M)
6          r_best ← FIND-MAX-BY-PROB-THEN-INFO(U, ε)
7          r_best.value ← USER-INSPECT-REPORT(r_best)
8          I ← I ∪ {r_best}
9          U ← U − {r_best}
```

TUNING AND CORRELATION


Jenkins
Jenkins
ENABLE AUTO REFRESH
add description
New Item
People
Build History
Manage Jenkins
Credentials
Build Queue
No builds in the queue.
Build Executor Status
# Status
1 Idle
2 Idle
3 Idle
4 Idle
All
S W Name Last Success Last Failure Last Duration
Cloud 23 hr - #831 2 mo 2 days - #287 1 min 52 sec
WebBoew 10 days - #25 10 days - #22 46 sec
PHPUnit 10 days - #22 N/A 55 sec
KrakenJSPaypal 10 days - #14 N/A 1 min 47 sec
CodeIgniter 10 days - #20 N/A 4 min 39 sec
Ghost 10 days - #17 N/A 1 min 26 sec
6 min 47 sec
6 min 15 sec
1 min 44 sec
WooCommerce 10 days - #9 2 mo 27 days - #5 4 min 50 sec
Twig 10 days - #9 N/A 43 sec
Atmosphere 10 days - #89 2 mo 26 days - #39 5 min 14 sec
Drupal 10 days - #103 2 mo 25 days - #48 1 min 16 sec
TwitterJOAUTH 10 days - #16 N/A 14 min
Cassandra 11 days - #81 5 mo 9 days - #27 14 min
Rebound 11 days - #11 N/A 55 sec
TwitterAmbrose 12 days - #7 N/A 5 min 20 sec
DEMO

AUTOMATION

- hacktheplanet.ninja

# ONE MORE THING...

VIM 0DAY FOR EVERYONE

VIM