2015-Jan-27

Monoculture – is it working?

Gaus <gausix@gmail.com>

Panasonic PSIRT

Monoculture

The cultivation or exploitation of a single crop, or the maintenance of a single kind of animal, to the exclusion of others.

(source: Oxford Dictionary)

It is generally considered a bad practice.

The term is borrowed for use in the computer security arena.

Monoculture In The Computer Security Arena

Single product can ‘amplify’ adverse effects of an attack.

The commonly argued solution is to deploy product from different vendors.

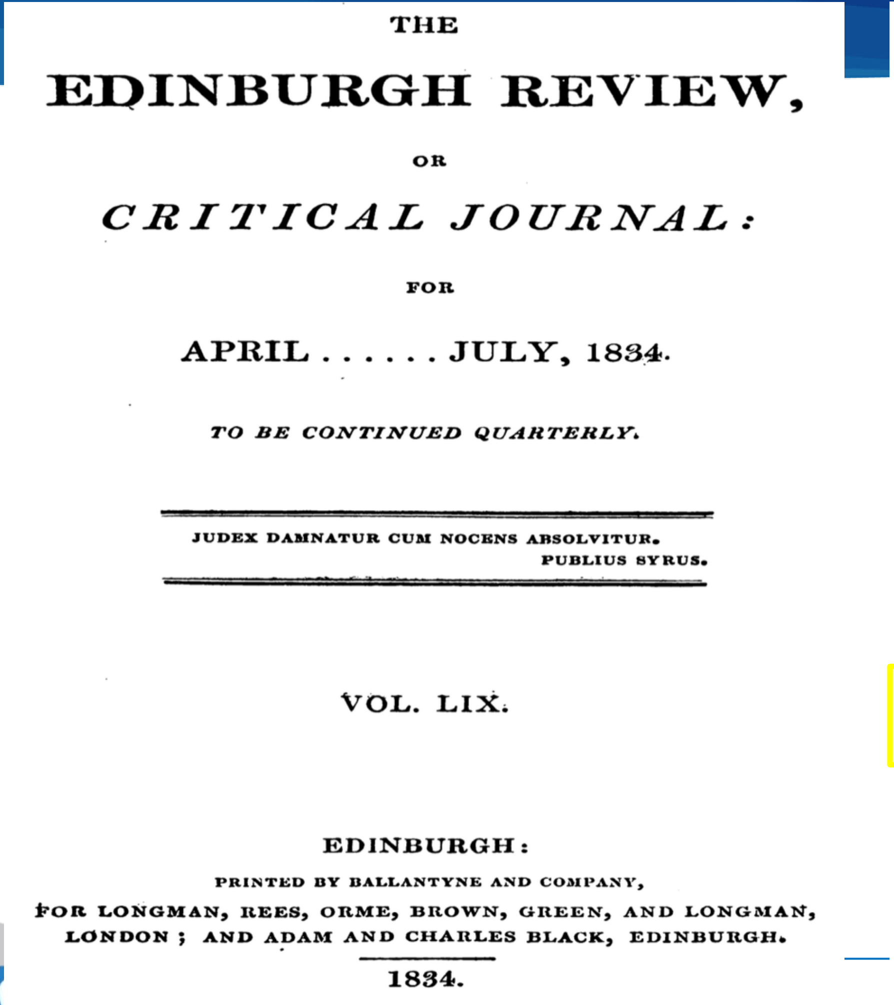
But is that solution effective?

Organization of this talk

- Principle on which product diversification idea is based on
- How effective diversification is in theory and practice?
- Monoculture revisited
- Why we do not see more bad things happening?

“The most certain and effectual check upon errors which arise in the process of computation, is to cause the same computations to be made by separate and independent computers; and this check is rendered still more decisive if they make their computations by different methods.”

IBM



THE

EDINBURGH REVIEW,

OR

CRITICAL JOURNAL:

FOR

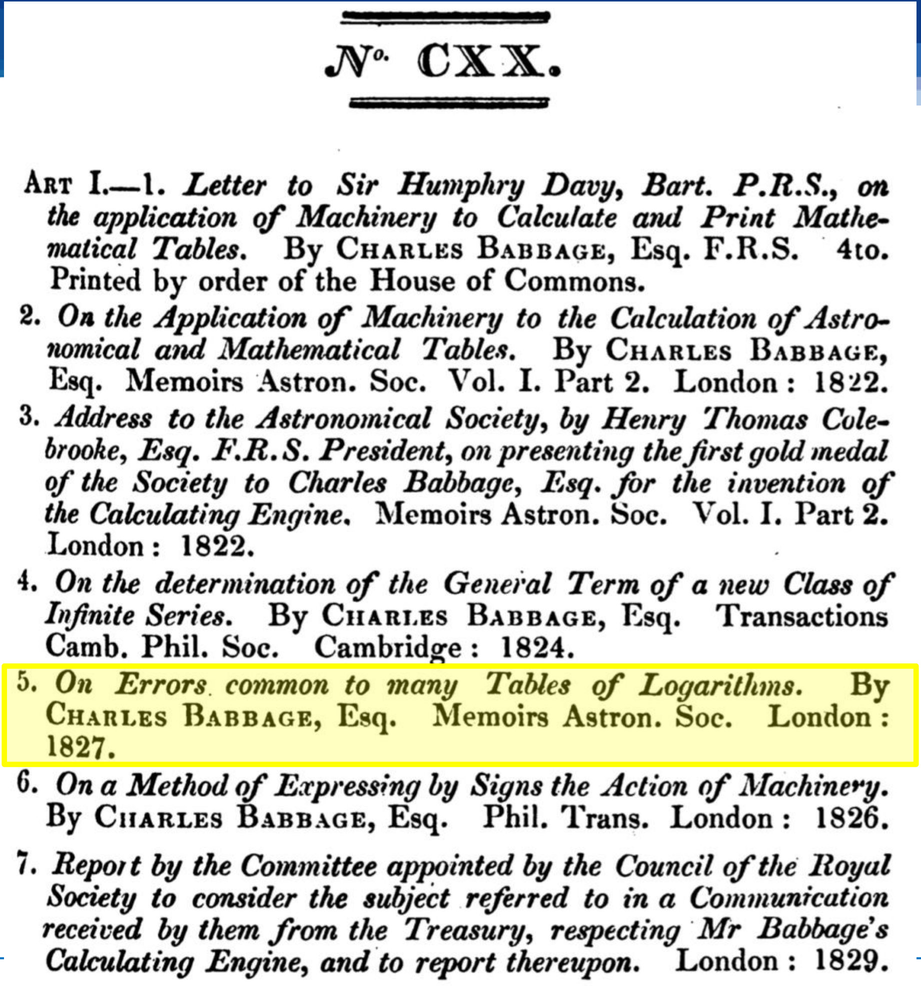
APRIL . . . . . . JULY, 1834.

TO BE CONTINUED QUARTERLY.

> JUDEX DAMNATUR CUM NOCENS ABSOLVITUR.
> PUBLIUS SYRUS.

VOL. LIX.

EDINBURGH:
PRINTED BY BALLANTYNE AND COMPANY,
FOR LONGMAN, REES, ORME, BROWN, GREEN, AND LONGMAN,
LONDON; AND ADAM AND CHARLES BLACK, EDINBURGH.
1834.



No. CXX.

ART I.—1. *Letter to Sir Humphry Davy, Bart. P.R.S., on the application of Machinery to Calculate and Print Mathematical Tables.* By CHARLES BABBAGE, Esq. F.R.S. 4to. Printed by order of the House of Commons.

2. *On the Application of Machinery to the Calculation of Astronomical and Mathematical Tables.* By CHARLES BABBAGE, Esq. Memoirs Astron. Soc. Vol. I. Part 2. London: 1822.

3. *Address to the Astronomical Society, by Henry Thomas Colebrooke, Esq. F.R.S. President, on presenting the first gold medal of the Society to Charles Babbage, Esq. for the invention of the Calculating Engine.* Memoirs Astron. Soc. Vol. I. Part 2. London: 1822.

4. *On the determination of the General Term of a new Class of Infinite Series.* By CHARLES BABBAGE, Esq. Transactions Camb. Phil. Soc. Cambridge: 1824.

5. *On Errors common to many Tables of Logarithms.* By CHARLES BABBAGE, Esq. Memoirs Astron. Soc. London: 1827.

6. *On a Method of Expressing by Signs the Action of Machinery.* By CHARLES BABBAGE, Esq. Phil. Trans. London: 1826.

7. *Report by the Committee appointed by the Council of the Royal Society to consider the subject referred to in a Communication received by them from the Treasury, respecting Mr Babbage's Calculating Engine, and to report thereupon.* London: 1829.

N-Version Programming (NVP)

- Used heavily in mission critical environments to achieve fault tolerance
- Multiple teams are developing from the same specifications
- It tends to be expensive

NVP By Another Means

- Use products from different vendors
- Products are developed by different groups
- Groups did not cooperate while developing the products
- It is much cheaper than the NVP proper

Organization of this talk

- Principle on which product diversification idea is based on
- How effective diversification is in theory and practice?
- Monoculture revisited
- Why we do not see more bad things happening?

Putting Diversification To The Test

- We will use two sources:
  - A study made in 1986 by Knight, J.C. and Leveson, N.G
  - CERT/CC / US-CERT Vulnerability Notes

Knight & Leveson Study

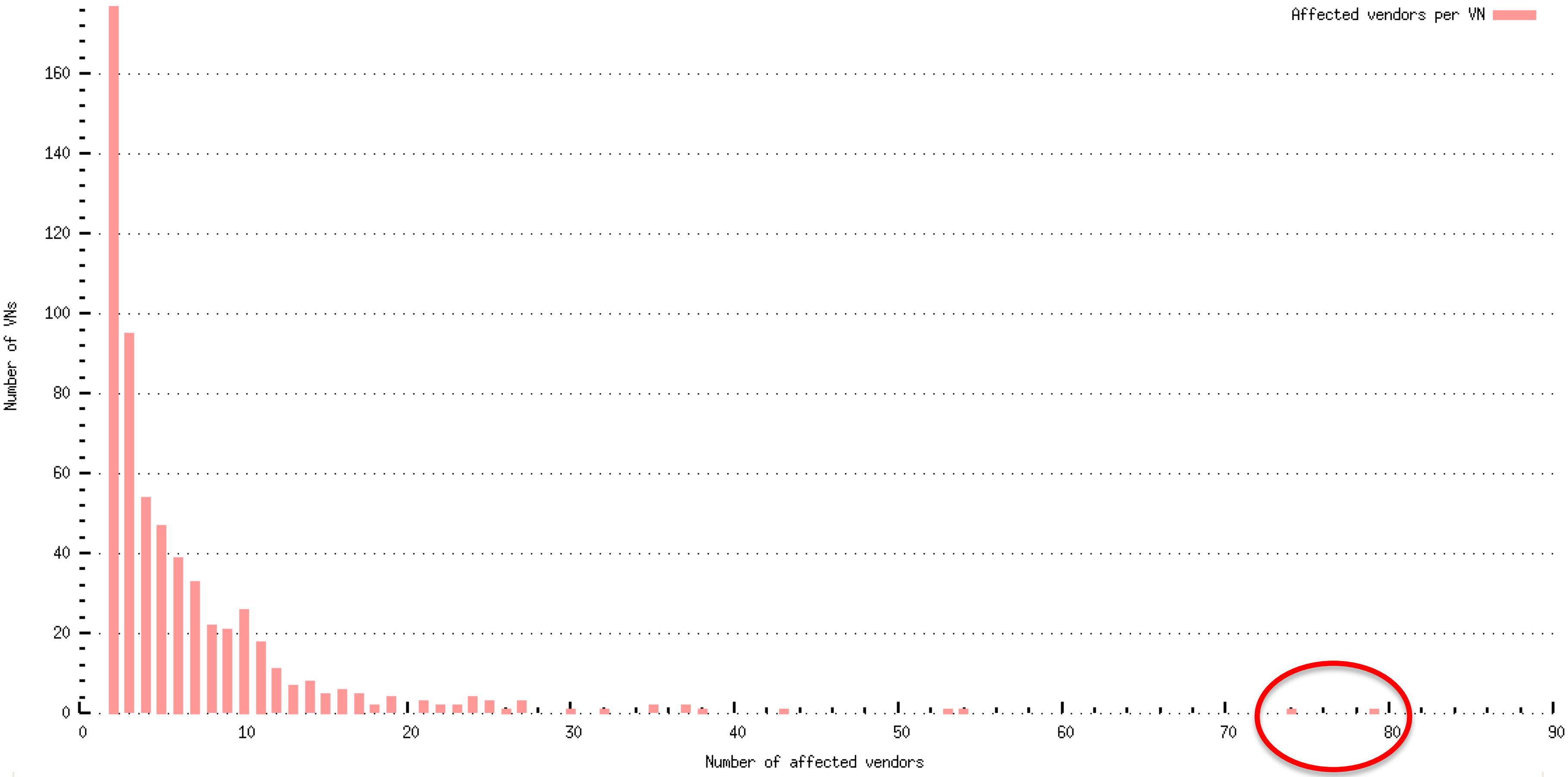
- Students from two universities are given the same specification
- They were instructed to code the solution
- Students were forbidden to collaborate with other students included in the study
- Each developer was given an identical set of tests to verify the correctness of the solution
- Acceptance test consisted of 200 randomly generated tests unique for each solution
- 27 solutions have been accepted

“For the particular problem that was programmed for this experiment, we conclude that the assumption of independence of errors that is fundamental to the analysis of N-version programming *does not hold*.”

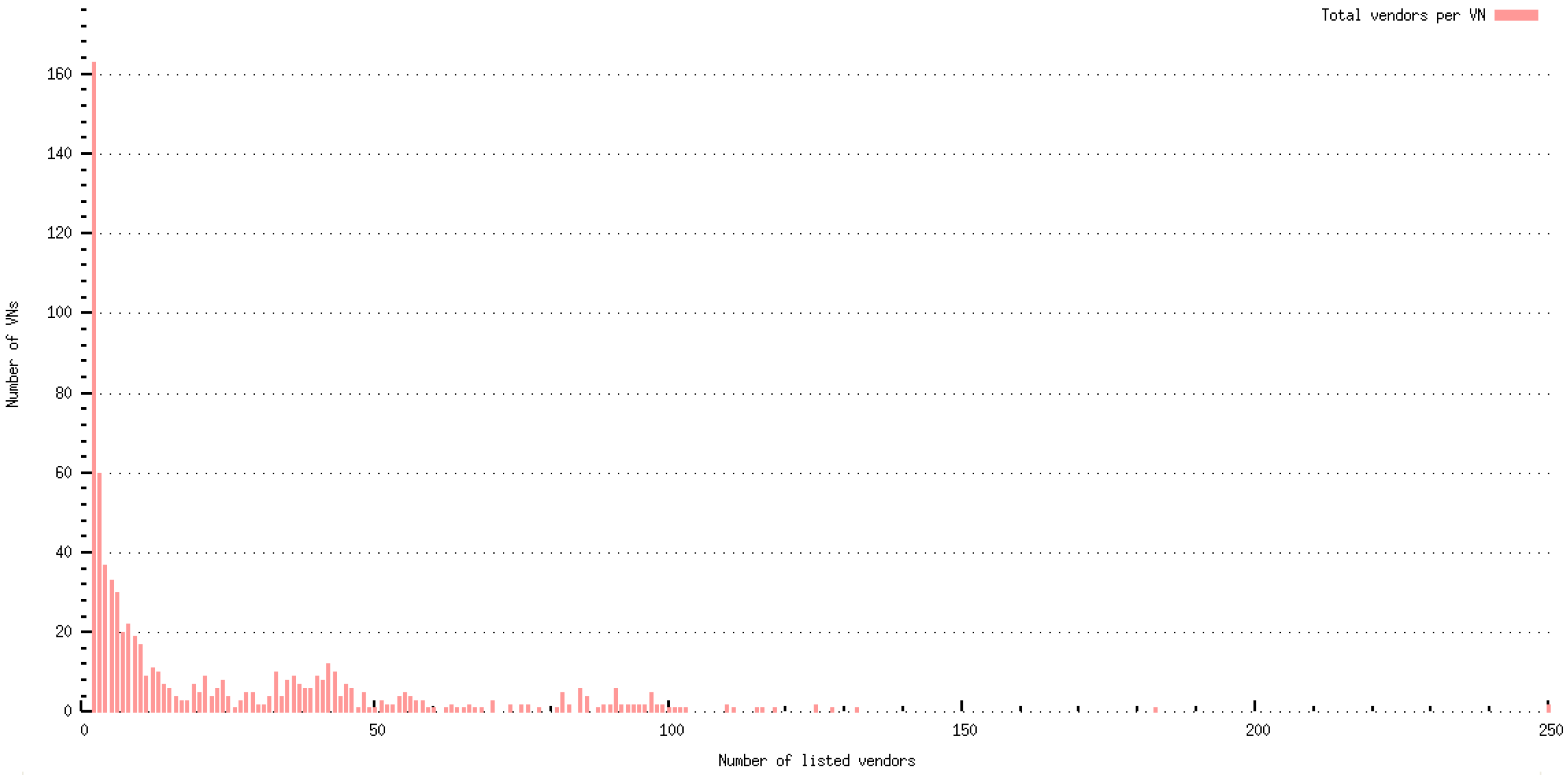
“An Experimental Evaluation of the Assumption of Independence in Multi-Version Programming”, John Knight and Nancy Leveson, IEEE 1986.

Analysis Of Vulnerability Notes

- Analyzed VNs in the period from Sep-2000 to Jan-2015 (available at http://www.kb.cert.org/vuls)
- 3158 VNs have been published in that period
- Each VN tend to cover a single vulnerability
- We were looking for instances where multiple vendors were listed as ‘vulnerable’ in the same Vulnerability Note

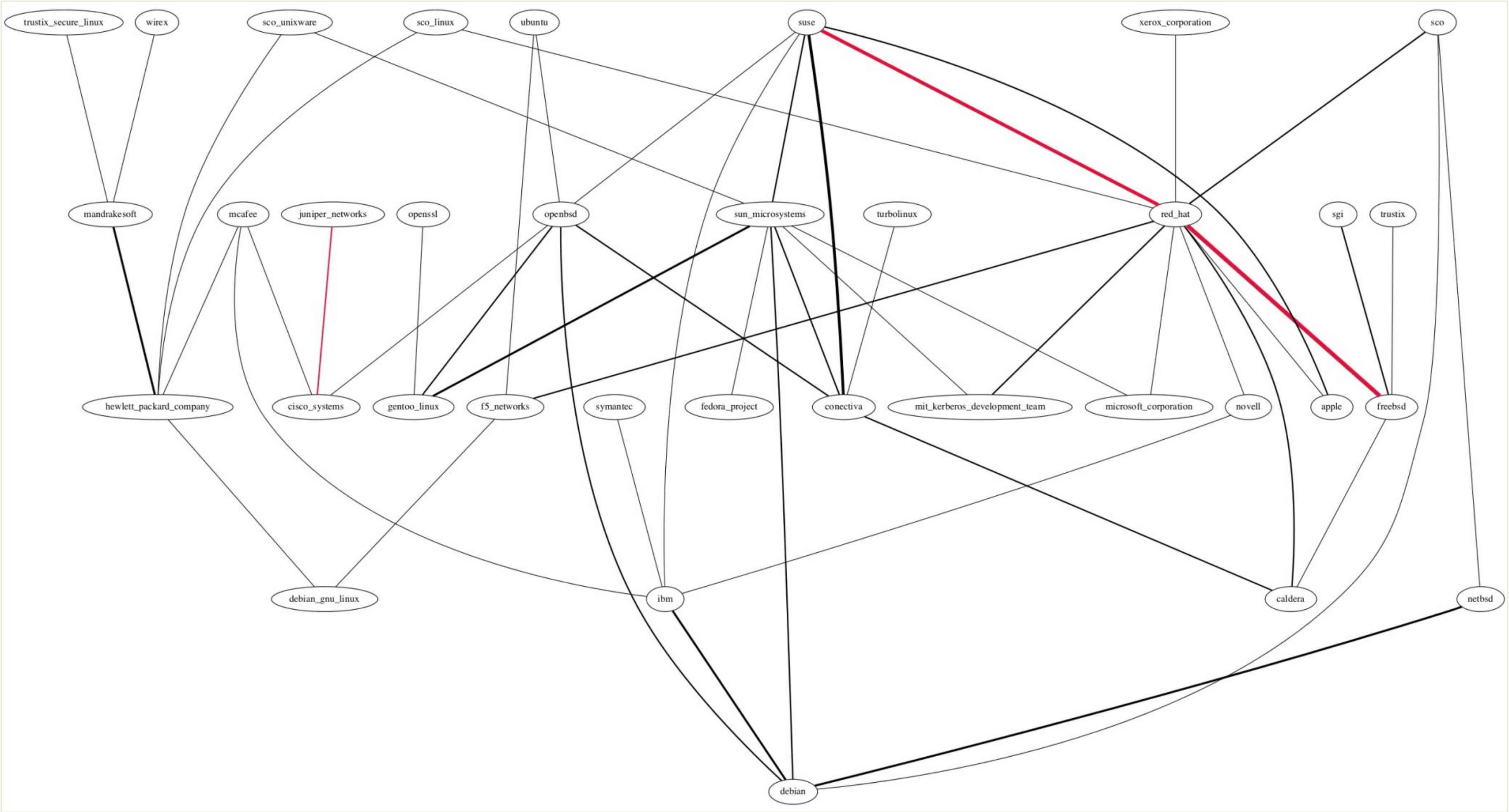


© Panasonic 2015


Total vendors per VN
Number of VNs
0
20
40
60
80
100
120
140
160
0
50
100
150
200
250
Number of listed vendors

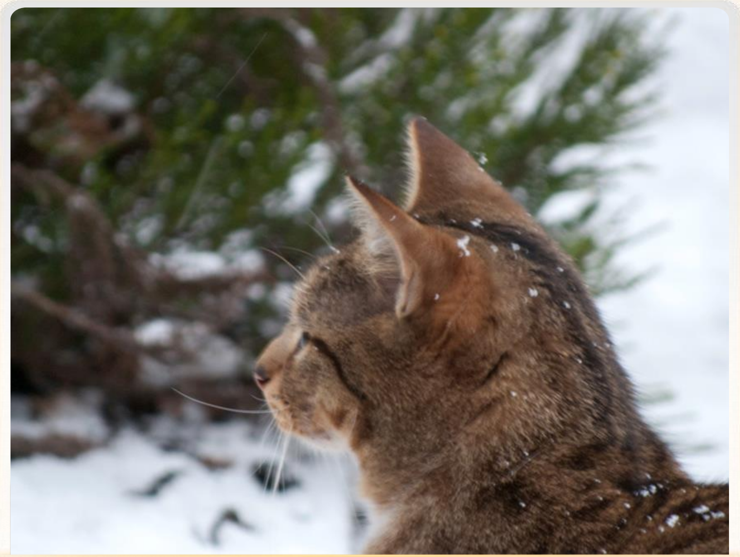
Vendor Pairs Analysis

- Are there any vendors that appear together more often than others?
- That would indicate tight product coupling
- Application level analysis has not been done


trustix_secure_linux
wirex
sco_unixware
sco_linux
ubuntu
suse
xerox_corporation
sco
mandrakesoft
mcafee
juniper_networks
openssl
openbsd
sun_microsystems
turbolinux
red_hat
sgi
trustix
hewlett_packard_company
cisco_systems
gentoo_linux
f5_networks
symantec
fedora_project
conectiva
mit_kerberos_development_team
microsoft_corporation
novell
apple
freebsd
debian_gnu_linux
ibm
caldera
netbsd
debian

Organization of this talk

- Principle on which product diversification idea is based on
- How effective diversification is in theory and practice?
- Monoculture revisited
- Why we do not see more bad things happening?



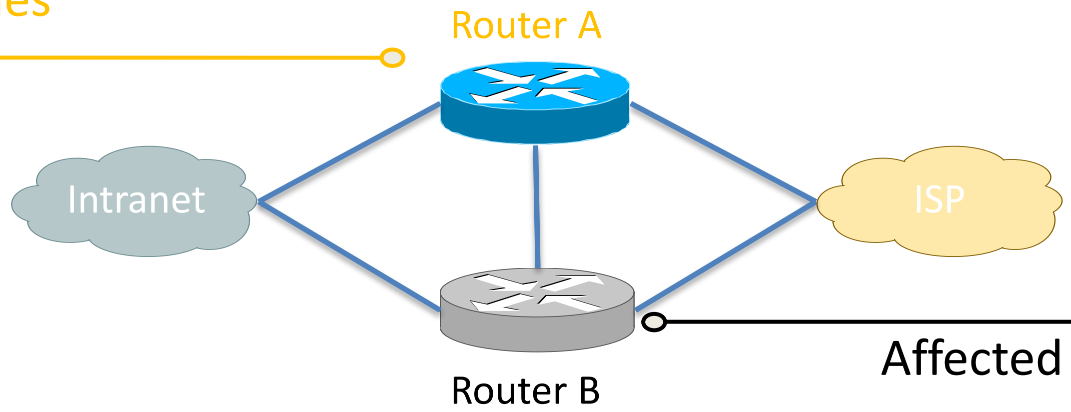
© Panasonic 2015

Diversification Revisited

- Products from different vendors are *not* substitute for NVP
- They have too many interdependencies
- Deploying products from different vendors is not much different than deploying products from a single vendor

Affected by

n vulnerabilities



Affected by

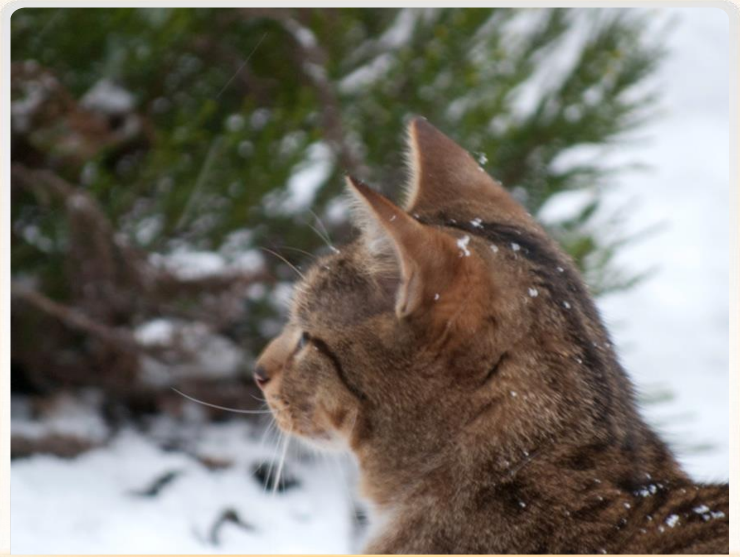
m vulnerabilities

“It is, nevertheless, a remarkable fact, that several computers, working separately and independently, do frequently commit precisely the same error; so that falsehood in this case assumes that character of consistency, which is regarded as the exclusive attribute of truth.”

Edinburgh Review, July 1834

Organization of this talk

- Principle on which product diversification idea is based on
- How effective diversification is in theory and practice?
- Monoculture revisited
- Why we do not see more bad things happening?



Uniformity Is Not a Norm

- Cisco IOS or JunOS does not mean that all releases are exactly the same
- Not all devices are configured exactly the same
- Vendors may introduce changes in third-party components that remove the vulnerability or the trigger

Third Party Library Use

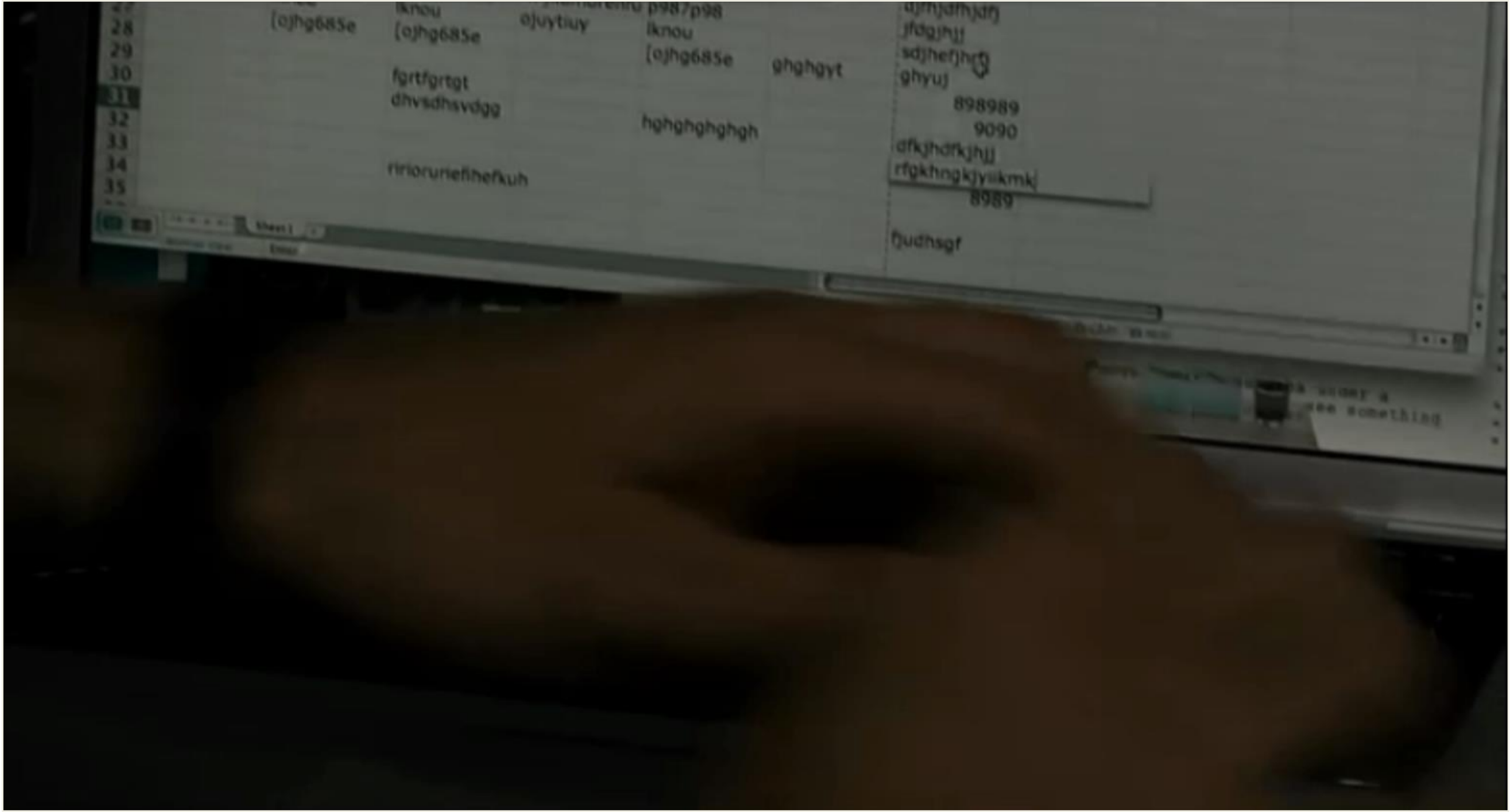
Product Version	OpenSSL Version
1.0	0.9.8g
1.1	0.9.8h
1.2	0.9.8k

A vulnerability is discovered in 0.9.8i

Do your homework and investigate Cves and VNs for vendors you are putting into your networks

We need a framework detailing how to build resilient systems out of components that have an unknown number and type of common points of failure.

Thank you!


28
29
30
31
32
33
34
35
[ojhg685e
lknou
[ojhg685e
ojuytiuy
p987p98
lknou
[ojhg685e
ghghgyt
fgrtfgrtgt
dhvsdhsvdgg
hghghghghgh
ririorurieflhefkuh
djfhjdfhjdfj
jfdgjhjj
sdjhefjhrfj
ghyuj
898989
9090
dfkjhdfkjhjj
rfgkhngkjyiikmk
8989
fjudhsgf
Sheet1