Progression and Forecast of a Curated Web-of-Trust: A Study on the Debian Project's Cryptographic Keyring

Gunnar Wolf, Víctor González Quiroga

OSS2017, Buenos Aires, Argentina, May 22-23 2017

Contenidos

The Debian keyrings: a *curated Web of Trust*

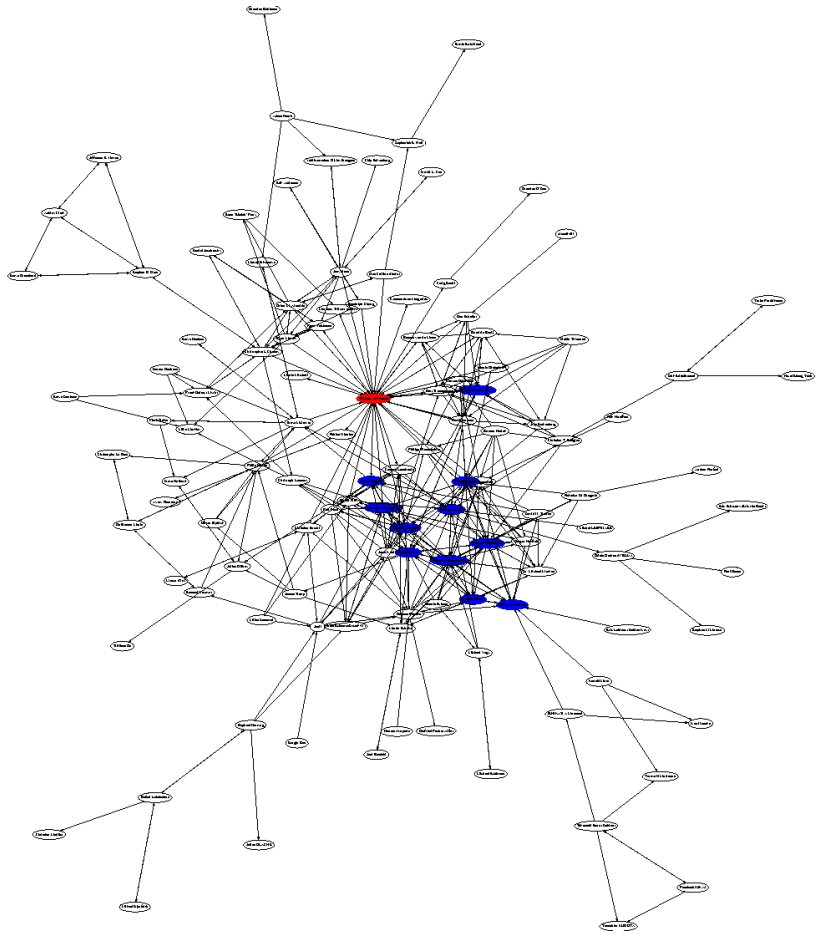
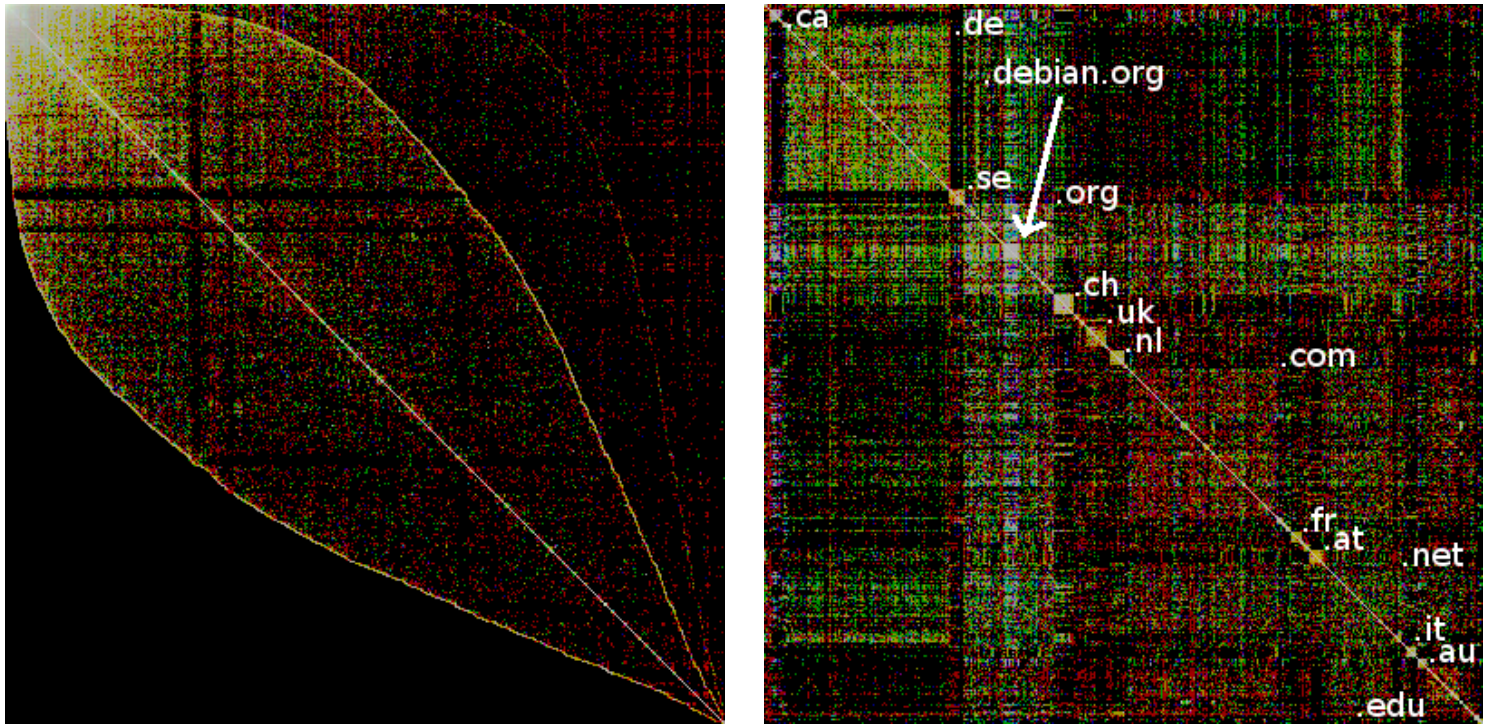


Figure: Graphical representation of the *strong set* of the Debian keyring back in 2000

Social studies from transitive trust graphs — And Debian's relative weight



(a) Whole "leaf"

(b) Sorted by TLD

Figure: Webs of Trust can teach us quite a bit - *Dissecting the Leaf of Trust* (Cederlöf 2008)

Work started after a big migration...

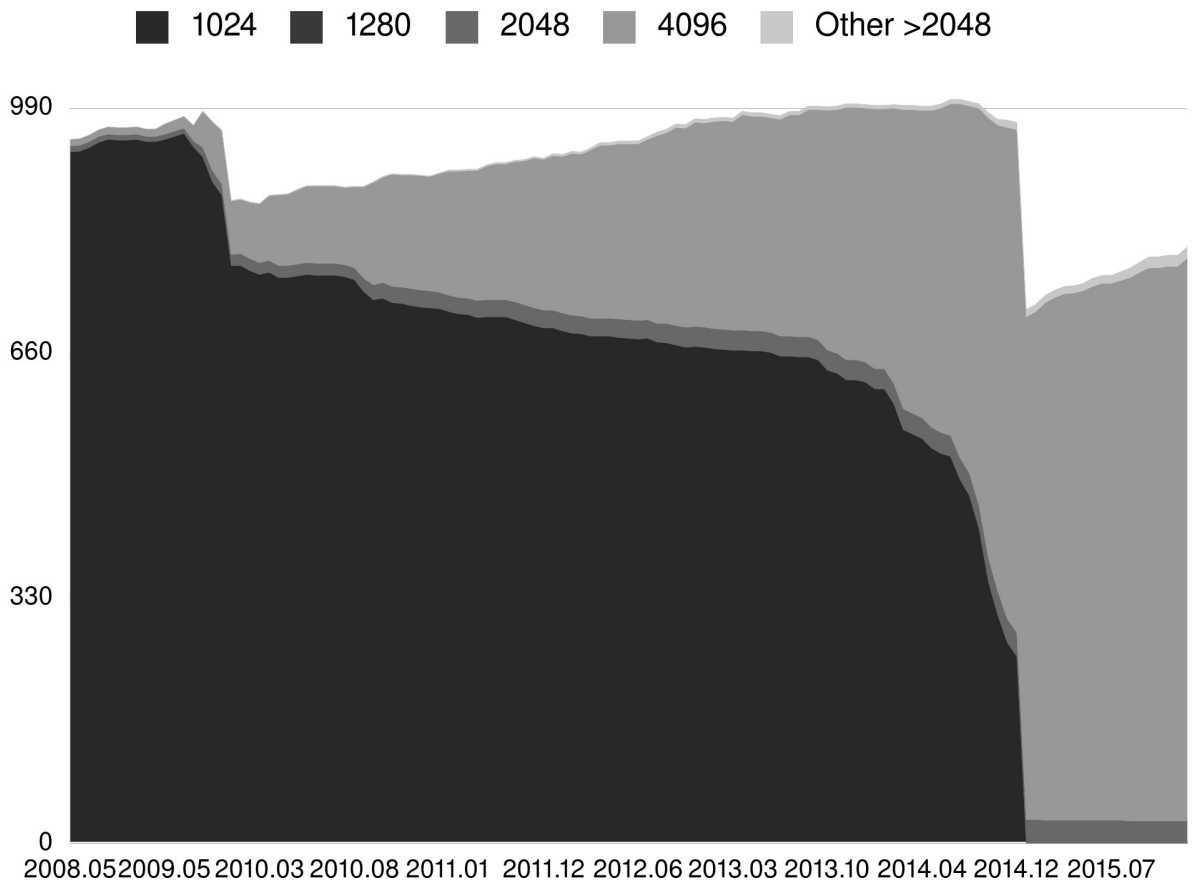


Figure: Breakdown of the Debian keyrings by key length, showing the migration away from short keys (<2048 bits)

Out of curiosity, the shape of the keyring

- Played with giving the keyring to `graphviz`
  - Might not be the best tool
  - Graph orientation and general shape is not *stable*
  - . . . But the results are interesting nonetheless!
- Keys are nodes, signatures are edges
- Of course, it looks like a simple, useless blob. . .

Just a simple, boring blob: Debian Developers, 2015.01.01

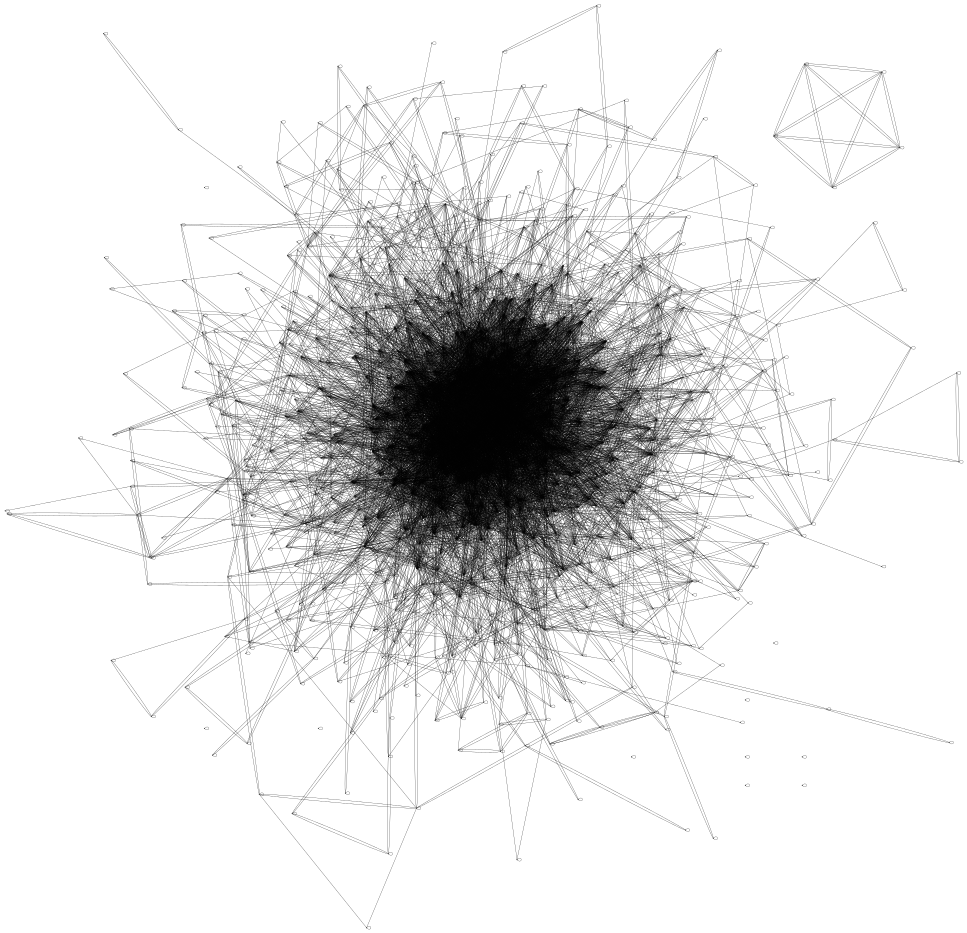


Figure: Our WoT — A maze of twisty passages, all alike

A *fun* blob: Debian Developers, January 2014

Thanks to having everything under Git (version control), we have a handy window to the past...

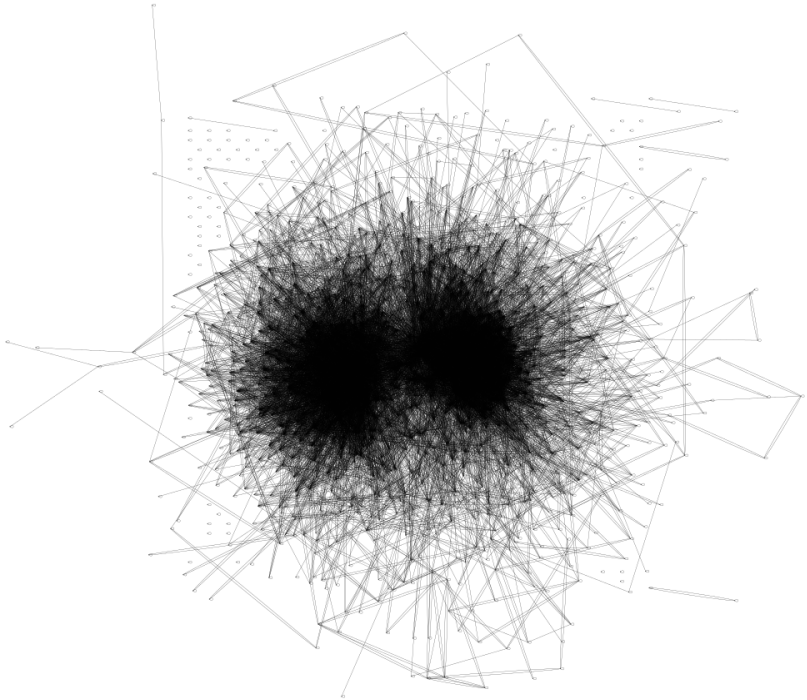
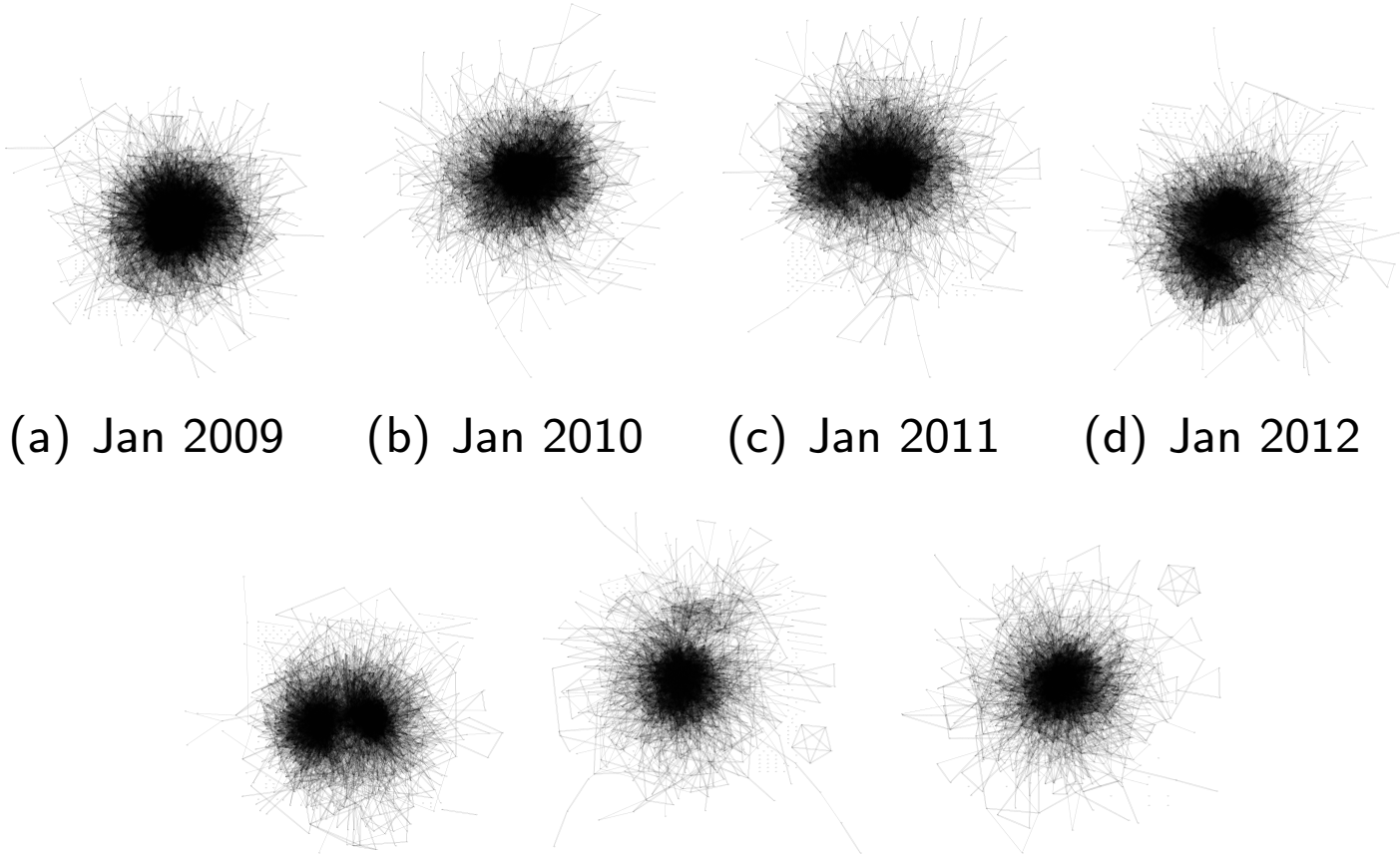


Figure: It's ALIVE!!!

- What does this split mean?
- Why did it appear?
- Where does it come from?
- How did it get there?
- When did it appear?

Evolution of the keyring



(a) Jan 2009 (b) Jan 2010 (c) Jan 2011 (d) Jan 2012

(e) Jan 2014 (f) Dec 2014 (g) Jan 2015

Figure: Snapshots of the Debian keyring evolution at different points in time

Contenidos

Hypothesis: Keyring aging?

- Leading to, and mostly during 2014, a huge portion of our keyring was replaced
  - One of the "blobs" marks older keys, the other new replacements?
  - But why the split began as early as 2011?
  - Note that nodes are grouped by their *cross-signatures* not by the key age (hence a 1024D key could be in the "younger" group and be expired!)
- Or it marks a *generation* of Debian Developers, slowly reducing their involvement?

Lets add some color!

- Nodes are irrelevant (`point`), only edges are important
- Edges represent key signatures; color denotes signature age WRT the point in time the snapshot was *taken*

Table: Color key for the resulting graphs

Blue	Less than one year
Green	1 to 2 years
Yellow	2 to 3 years
Orange	3 to 4 years
Red	over 4 years old

Same old keyrings: 2014.01.12

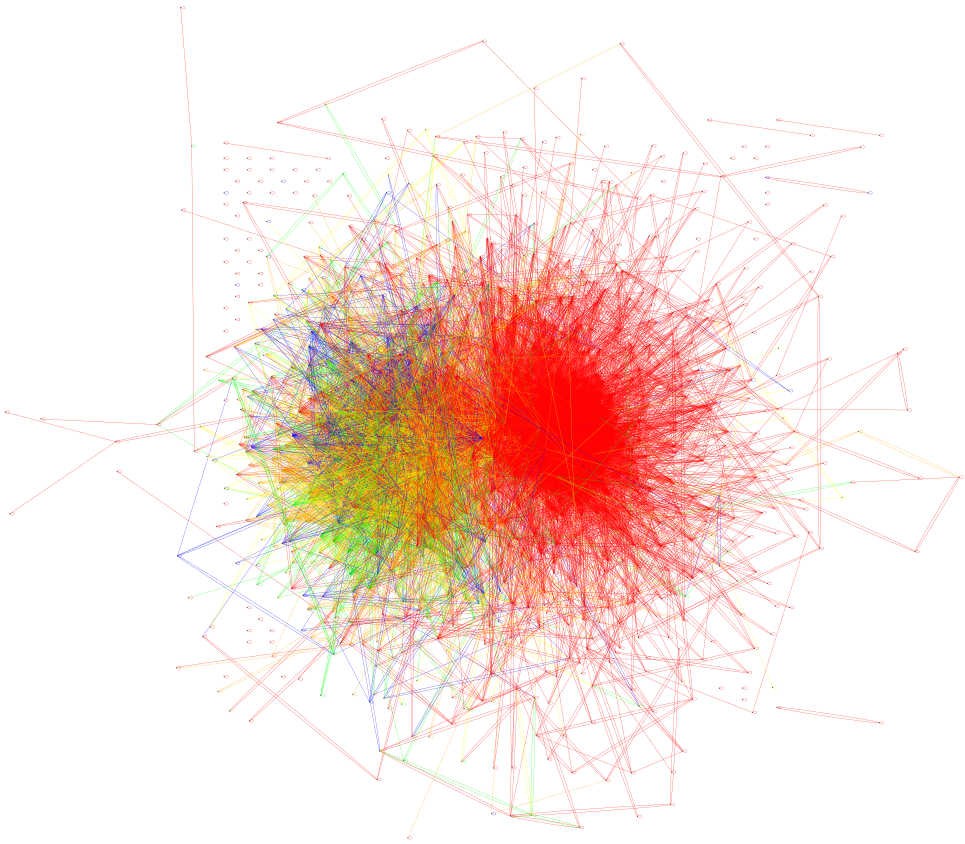


Figure: Big, red, disconnected blob

Same old keyrings: 2015.01.01

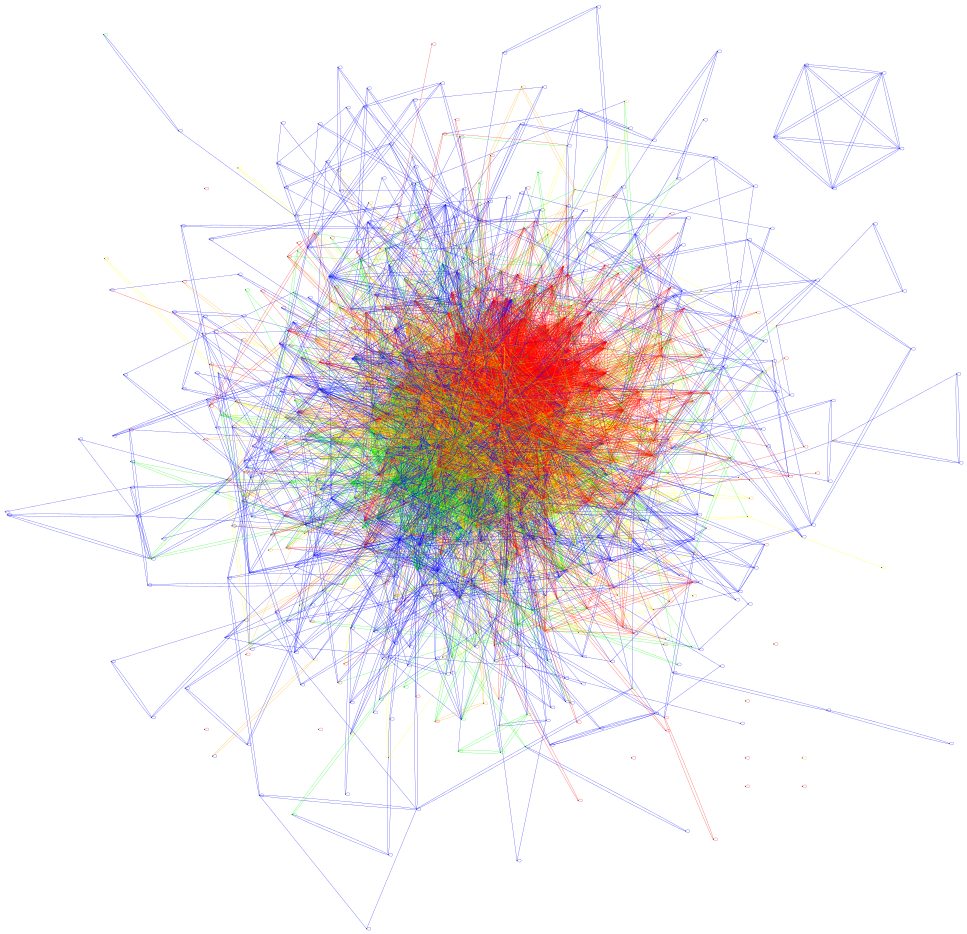
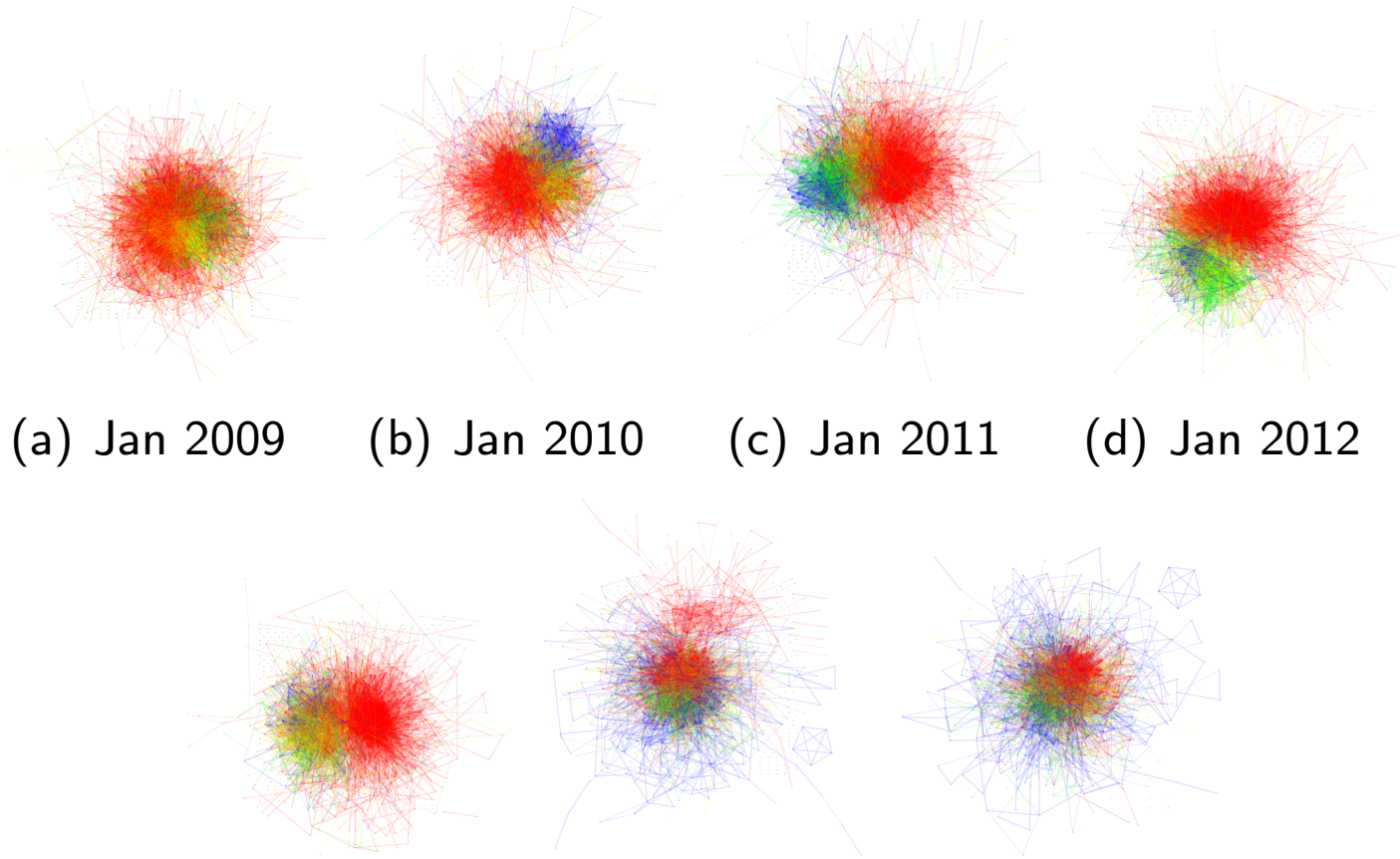


Figure: Big, red, disconnected blob

Same ten-keyring snapshot



(a) Jan 2009 (b) Jan 2010 (c) Jan 2011 (d) Jan 2012

(e) Jan 2014 (f) Dec 2014 (g) Jan 2015

Figure: Snapshots of the Debian keyring evolution at different points in time, showing signature age. Signature coloring is relative to each of the snapshots.

Contenidos

Measuring permanency

- A first closeup to answer How many keys are reliable per se?
- Survival implies Reliability, which implies Trust
- How many keys keep participating in the project?

Proportion of keys in keyring

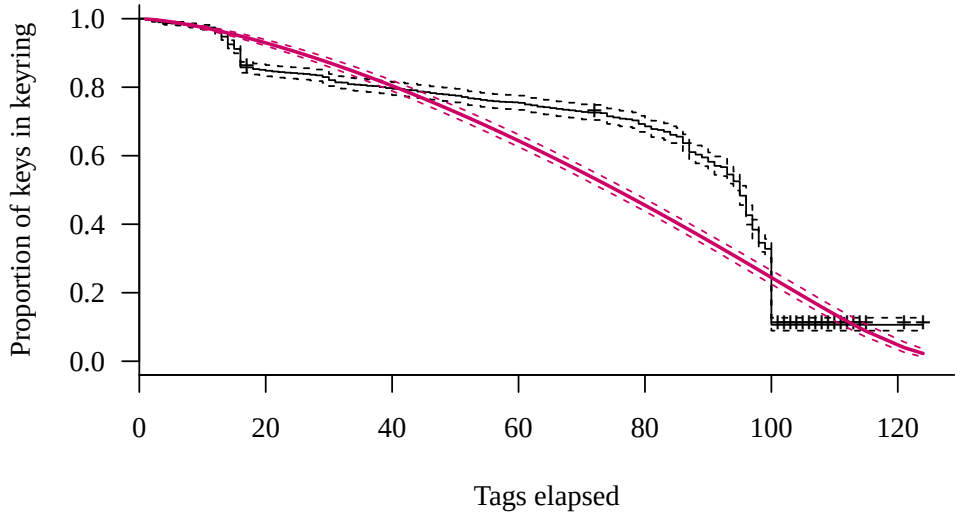


Figure: Probability of key permanency.

- Passing 40 tags (4 years) keys aren't likely to leave that much.
- Passing 95 tags (6 years) key exit is a coin flip.

Expected exits per key

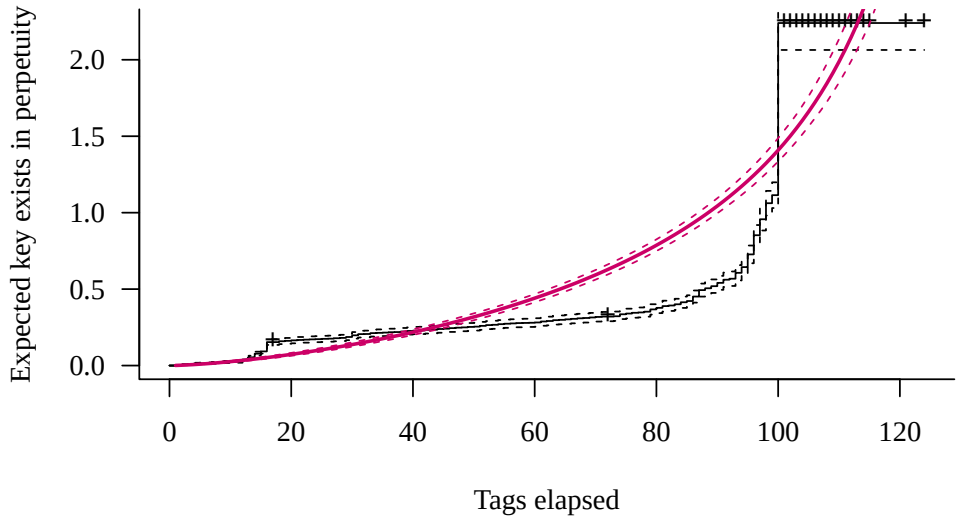


Figure: Cumulated hazard of key exits.

- If a key would leave around tag 100 (6 years).
- If it didn't, then it will leave passing 3 tags (2 months).

Departure Rate

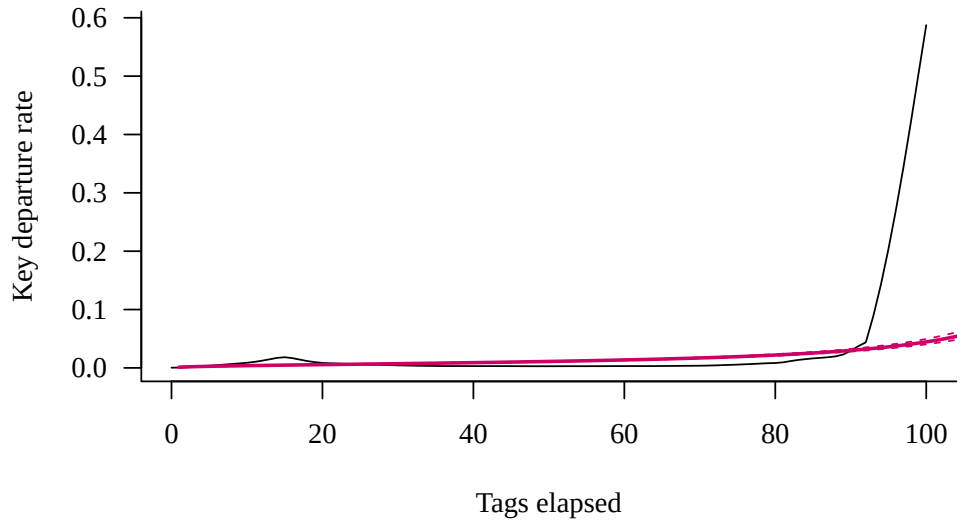


Figure: Hazard rate of key exits.

- Keys "wear out" coming of age at tag 90 (6 years).
- 5/1000 keys will leave "any time now" consistently in the lifetime.

Contenidos

Future work

- Assess the impact of *expiring* signatures
- Revise key survival — But *folding* different keys into personal identities
- Go beyond *Developers* to the other active keyrings (*Non-uploading*, *Maintainers*)
  - Compare patterns
  - Migrations between active keyrings
- Applicability to other free software projects?
  - Correlate with events and trends spanning a wider population
  - Issue: Do we have a similar data source?

Thanks!

Thanks for your attention!

Gunnar Wolf • gwolf@debian.org
AB41 C1C6 8AFD 668C A045 EBF8 673A 03E4 C1DB 921F

Víctor González Quiroga • masterquiroga@protonmail.com
066B F460 3199 5DF2 37CB EA44 149E 8316 4E64 6572

Instituto de Investigaciones Económicas / Facultad de Ciencias
Universidad Nacional Autónoma de México