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

1 Introduction: Trust models

2 Trust aging

3 Key survival

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

Figure: It’s ALIVE!!!
Evolution of the keyring

Figure: Snapshots of the Debian keyring evolution at different points in time
1 Introduction: Trust models
2 Trust aging
3 Key survival
4 Future work
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?
Progression and Forecast of a Curated Web-of-Trust: A Study on the Debian Project’s Cryptographic Keyring

Gunnar Wolf, Víctor González Quiroga

Introduction: Trust models

- Trust aging
- Key survival
- Future work

Let's 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

<table>
<thead>
<tr>
<th>Color</th>
<th>Age Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>Less than one year</td>
</tr>
<tr>
<td>Green</td>
<td>1 to 2 years</td>
</tr>
<tr>
<td>Yellow</td>
<td>2 to 3 years</td>
</tr>
<tr>
<td>Orange</td>
<td>3 to 4 years</td>
</tr>
<tr>
<td>Red</td>
<td>over 4 years old</td>
</tr>
</tbody>
</table>
Progression and Forecast of a Curated Web-of-Trust: A Study on the Debian Project’s Cryptographic Keyring

Gunnar Wolf, Víctor González Quiroga

Introduction: Trust models

Trust aging

Key survival

Future work

Same old keyrings: 2014.01.12

Figure: Big, red, disconnected blob
Same old keyrings: 2015.01.01

Figure: Big, red, disconnected blob
Progression and Forecast of a Curated Web-of-Trust: A Study on the Debian Project’s Cryptographic Keyring

Gunnar Wolf, Víctor González Quiroga

Introduction:

Trust models
Trust aging
Key survival
Future work

Figure: Snapshots of the Debian keyring evolution at different points in time, showing signature age. Signature coloring is relative to each of the snapshots.
Progression and Forecast of a Curated Web-of-Trust: A Study on the Debian Project’s Cryptographic Keyring

Gunnar Wolf, Víctor González Quiroga

Introduction: Trust models

Trust aging

Key survival

Future work
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.
**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).
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.
Progression and Forecast of a Curated Web-of-Trust: A Study on the Debian Project’s Cryptographic Keyring

Gunnar Wolf, Víctor González Quiroga

Introduction: Trust models

Trust aging

Key survival

Future work
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 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