# Étude du générateur d'aléa du noyau Linux

Andrea Röck [*], Vincent Strubel[†], Marion Videau [‡]

Générateur d'aléa aussi répandu que l'est le noyau qui l'embarque, le générateur d'aléa du noyau Linux [MT05] mérite bien qu'on s'y intéresse en détail. Des détails qui se révèlent très nombreux, de la structure aux critères de conception sous-jacents ainsi qu'à l'évaluation de sécurité. Nous présentons ici une étude en cours.

Le générateur d'aléa du noyau Linux utilise l'entropie provenant de l'environnement du système (frappe clavier, déplacement de la souris, interruption réseau ou disque) ou de sources d'entropie extérieures pour alimenter une structure composée de deux blocs successifs : {registre à décalage, insertion par rebouclage, extraction par hachage}. Cette structure est en fait dédoublée afin de mettre à disposition d'une part un générateur bloquant, `/dev/random`, qui fournit un nombre de bits limité par la valeur du compteur d'entropie, et d'autre part un générateur pseudo-aléatoire non-bloquant plus classique, `/dev/urandom`, qui fournit autant de bits que demandés.

Bien que le générateur ait déjà fait l'objet d'études antérieures (voir par exemple [BH05], [GPR06]), de nombreux points restent à préciser, que ce soit sur la place du générateur dans le noyau et son interaction avec les autres applications, les divers contextes d'utilisation plus ou moins nominaux, sur les détails de sa structure (registre à décalage, hachage) et des critères de conception qui ont été utilisés ainsi que sur l'estimation d'entropie — est-elle plus ou moins conservative, avec quelle autre estimation la comparer, peut-on présenter des résultats expérimentaux ? — et l'évaluation de sécurité de manière plus générale.

## Références

[BH05] Boaz Barak et Shai Halevi. An architecture for robust pseudo-random generation and applications to /dev/random. In ACM, editor, *Proc. Computing and Communication Security (CCS)*, 2005.

[GPR06] Zvi Gutterman, Benny Pinkas et Tzachy Reinman. Analysis of the linux random number generator. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy (S& P 2006)*, pages 371–385, Washington DC, USA, 2006. IEEE Computer Society.

[MT05] Matt Mackall et Theodore Ts'o. `random.c` — a strong number generator. `/drivers/char/random.c` in Linux Kernel 2.6, `http://www.kernel.org`, 1994, 2005.

[*]Helsinki University of Technology, Department of Information and Computer Science, P.O. Box 5400, FI-02015 TKK, Finland. `andrea.roeck@inria.fr`

[†]Agence Nationale de la Sécurité des Systèmes d'Information, Laboratoire architecture et réseaux, 51 boulevard de La Tour-Maubourg, 75007 Paris, France. `vincent.strubel@sgdn.gouv.fr`

[‡]Université Henri Poincaré, Nancy 1 / LORIA et Agence Nationale de la Sécurité des Systèmes d'Information, Laboratoire cryptographie et composants, 51 boulevard de La Tour-Maubourg, 75007 Paris, France. `marion.videau@loria.`