Accelerometers as Sources of Randomness in Mobile Devices

Viliam Hromada, Juraj Varga

02. - 05.05.2013, ISCAMI 2013 in Malenovice

Outline

- Various sources of randomness.
- Camera picture as a source of randomness.
- Accelerometer as a source of randomness.
- Our tests and results.

Traditional sources of randomness

Guttermann - Linux kernel

- Keyboard & mouse input.
- HDD.
- Interruptions.
- Radio waves.

Traditional sources of randomness #2

- Repeatable, most of them automated.
- Either predictable or affectable by adversary.
- Microphone - audio file must be saved.
- Alternative sources - magnetometer, proximity sensor.

Camera as a source of randomness

- Bouda, Krhovják, Matyáš, Švenda - 2009.
- The goal: identify sources of randomness and estimate their min-entropy.
- Due to limited device resources authors focused on camera and microphone.
- Finally only camera was considered.
- Sensor output is not appropriate for cryptographic applications.
- Entropy extractor used - based on Carter-Wegman universal hash-function class.

Randomness extractor

Definition

Min-entropy of probability distribution X on $\{0,1\}^n$ is:

$$\textit{min-entropy}(X) = \min_{x \in 0,1^n} \{-\log_2 Pr(X = x)\}.$$

Randomness extractor

Definition

Function

$$e : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m,$$

is (non-deterministic) (k, ϵ) randomness extractor if for every input from distribution X on $\{0,1\}^n$ with min-entropy$(X) \geq k$ and for uniformly distributed d-tuple of bits is the probability distribution of the output ϵ-close to the uniform distribution of m-tuple of bits.

Camera as a source of randomness #2

- Data from each picture was cut and xored into 4 Bytes.
- Only 4 LSB are taken from each picture.
- Entropy of these bits was 3.984.
- Output was tested with NIST testing battery, 15/16 passed.

Accelerometer as a source of randomness

- Voris, Saxena, Halevi - 2011.
- RFID tag WISP with ADXL330 accelerometer (10b/c).
- Test its properties and possible adversary influence - different moves, temperature.
- Randomness extractor was used again.
- Device was moved for 10 minutes and the output was measured.

Accelerometer as a source of randomness #2

- From the output (50 samples) authors extracted 128 bits.
- NIST testing again (various success rate).
- Influence from environment can be mitigated by use of suspension materials.
- Sampling frequency has no effect on entropy.
- Temperature and a way of carrying can affect final results.

Accelerometer as a source of randomness #3

- Hromada, Varga - 2013.
- HTC EVO 3D with OS Android.
- Replication of test from Voris et. al.

Accelerometer as a source of randomness #4

Quite promising results:

Move	Min-entropy
Desk	5.5
During night	6.1
Shake	11.2
Hand	9.5
Arc swipe	12.6
Drop	9.2
Triangle	12.7
Alpha	13.4
Circle	12.5

Implemented PRNGs

- ISAAC
  - Published in 1996.
  - Uses ARX operations - very fast.
  - Only theoretical attack is known.
- Blum Blum Shub
  - Proven to be cryptographically secure.
  - Used as a reference generator.

Future work

- Work in progress (in beginning).
- Implement some chosen randomness extractor.
- Output from extractor will be used as a seed for our implementation of ISAAC.
- Try out other sources of randomness - gyroscope, magnetometer, test possible combinations.
- Test statistical properties of final output with various test suites (ParanoYa Academic).

References

Krhovják J., Matyáš V., Žižkovský J.: *Generating Random and Pseudorandom Sequences in Mobile Devices* Security and Privacy in Mobile Information and Communication Systems,First International ICST Conference, MobiSec 2009, Turin, Italy, June 3 – 5, 2009, Revised Selected Papers, published: Springer Verlag, Berlin, Germany, (2009) p. 122-133

Voris J., Saxena N., Halevi T.: *Accelerometers and Randomness: Perfect Together* WiSec '11 Proceedings of the fourth ACM conference on Wireless network security June 14 – 17, 2011, Hamburg, Germany, published: ACM New York, NY, USA (2011) p. 115-126

Thank you for your attention!