Towards an Approach for Improved Security in Wireless Networks

T Senthil Kumar
Department of Computer Science Engineering, Amrita School of Engineering
Ettimadai, Coimbatore

Uppu Sree Priyanka
Department of Computer Science Engineering, Amrita School of Engineering
Ettimadai, Coimbatore

K Abinaya
Department of Computer Science Engineering, Amrita School of Engineering
Ettimadai, Coimbatore

ABSTRACT
For high security transmission over a network, high randomness is required in the seed used for generating a key. This paper deals with two phenomena/methods (a) Bio-metric method (b) Hardware and Software method that possess randomness. Comparison tables have been tabulated with respect to each of the methods. Comparing each source a conclusion is derived at a set of sources that can contribute to the entropy pool.

Keywords
Entropy, Randomness, Random number Generator, Biometrics, Seed.

1. INTRODUCTION
With increase in the use of internet there has been an increased opportunity in identity fraud, organized crime and various other forms of cyber-crime [1]. Thereby, a need arises to secure the information which is being transferred across any network. The method to secure the data to be transmitted is to encrypt the data using a key and send it across the network. The receiver can decrypt the data with the help of the same key or a derived key. The key which is being used plays an important role. Hence, a need arises to generate a key which is highly random so that it cannot be guessed by an intruder who tries to steal the data from the network.

2. Random Numbers and Random Number Generator (RNG) [2]
For transfer of data in a secure manner, secure encryption standard is required. Most of the high level encryption algorithms require a seed. A seed is a numerical value which leads to the generation of a sequence of random numbers when given as an input to a random number generator. A seed is required in various applications such as:

i. Random passwords
ii. Session keys for encrypted data exchange
iii. HTTP cookies
iv. One-time passwords
v. TCP initial sequence numbers

A sequence is said to be random if you cannot predict the $(n+1)^{th}$term of the sequence even if you know first n elements of the sequence. This sequence is generated by a RANDOM NUMBER GENERATOR (RNG-computational device) based on the input seed given.
Real time applications of RNG are as follows:

i. Encryption of data using algorithms like, Advanced Encryption Standard (AES), Diffie Hellman, etc.
ii. In digital signatures
iii. Generation of code numbers or transaction numbers
iv. Creation of lottery number

3. ENTROPY
The quantitative measure of the randomness of a RNG is entropy.

The following criteria can be used to determine best entropy methods: Time complexity, accuracy, error rate, randomness, cost.

i. Time complexity involved in the computation should be less.
ii. The accuracy should be high with low error rate.
iii. The randomness of each source should be equally high.
iv. The cost involved with system should be low.

4. CLASSIFICATION OF ENTROPY
Entropy can be studied under the following methods:

4.1 Biometric entropy methods:

Biometric entropy deals with the generation of seed value depending on the measurement and statistical analysis of human body characteristics such as fingerprints, eye retinas and irises, facial patterns and hand measurements for authentication purposes [3].

4.2 Hardware and software entropy methods:
It deals with the generation of seed value depending on the measurement and statistical analysis of system or device characteristics such as -

i. Hardware: Mouse-Movement start/end, Scroll direction, Button press/release; Sound card, Received bit-errors, CPU temperature, Clock and Videos
ii. Software: magnetic hard disk (fetching time etc.)

5. COMPARISON

5.1 Biometric Entropy Methods
Table I gives the various techinques and the measurement parameters used in Biometric methods.

Table 1: Bimoetric Methods

TECHNIQUES	MEASUREMENT PARAMETERS
Keystroke Dynamics[4],[8]	1.Elapsed time between release of first key and depression of the second key 2.Duration of each key stroke(time for which it is held down) 3.Pressure applied on keys 4.Overall typing speed 5. Finger placement
Voice Biometrics [8]	1.Physiological component(voice tract) 2.Behavioural component(accent)
Fingerprint [6],[7],[8]	1. Minutia matching compares specific details within the fingerprint ridges. 2.Pattern matching compares the overall characteristics of the fingerprints such as sub-areas of ridge thickness, curvature, or density.
Iris Recognition [5],[8]	An iris scan will analyze over 200 points of the iris, such as rings, furrows, freckles, the corona and will compare it with a previously recorded template.
Retina Recognition [8]	The blood vessels patterns of a human eye.
Face Recognition [6],[7],[8]	1.Shape and proportions of the face 2.Distance between the eyes, nose, mouth, and jaw edges; upper outlines of the eye sockets, the sides of the mouth, the location of the nose and eyes, the area surrounding the cheekbones.

The merits, demerits and cross over rates of the techniques are elaborated below.

1. Keystroke Dynamics[4],[8]:
   Merit:
   1.1 No additional hardware is required.
   1.2 Minimal training.
   1.3 Natural authentication for computer system and network security.
   1.4 Non-intrusive and wide user acceptance.
   Demerit:
   1.1 High false reject rate (FAR).
   1.2 Sensitive to changes in keyboard, user's physical condition (illness, drowsy) and other operational conditions.
   1.3 Need to account for problems like typing errors.
   1.4 Narrow range of applications.
   Crossover error rate: 2.54%

2. Voice Biometrics[8]:
   Merit:
   2.1 Ability to use existing telephones.
   2.2 Low perceived invasiveness.
   Demerit:
   2.1 High false non-matching rates.
   Crossover error rate: 2%

3. Fingerprint [6],[7],[8]:
   Merit:
   3.1 Easy to use.
   3.2 Cost effective
   3.3 Small size
   3.4 Low power
   3.5 Non-intrusive
   3.6 Large database already available to store the fingerprints.
   Demerit:
   3.1 Acquiring high-quality images of distinctive fingerprint ridges and minutiae is a complicated task.
   3.2 There have been controversial issues regarding the uniqueness of the fingerprints.
   3.2 As the number of definite points decreases the degree of certainty also decreases.
   Crossover error rate: 0.2%

4. Iris Recognition [5],[8]:
   Merit:
   4.1 Highly accurate, i.e, no case of false acceptance for iris recognition.
   False Acceptance Rate (FAR) = 0.096%
   False Reject Rate (FRR) = 0.76%
   4.2 Based on the entropy of iris it generates a seed consisting of 42 bits.
   Demerit:
   4.1 User must hold still while the scan is taking place.
   4.2 Many commercial Iris scanners can be easily fooled by a high quality image of an iris or face in place of the real thing.
   4.3 Iris scanners are significantly more expensive than some other forms of biometrics.
   4.4 The accuracy of scanners can be affected by changes in lighting.
   Crossover error rate: 0.000763%

5. Retina Recognition:
   Merit:
   5.1 Highly accurate
   5.2 It is impossible to forge a human retina.
   5.3 Based on the entropy of iris it generates a seed consisting of 42 bits.
   Demerits:
   5.1 Enrollment and scanning are intrusive and slow.
   5.2 High equipment cost.
   5.3 Subject being scanned must be close to the camera optics.
   5.4 Measurement accuracy can be affected by diseases such as cataracts.
   Crossover error rate: 0.0000001%

6. Face Recognition [6],[7],[8]:
   Merit:
   6.1 Not intrusive, can be done from a distance, even without the user being aware of it
   6.2 A seed of 20 bits can be generated using this method.
   Demerit:
   6.1 Face biometric systems are more suited for authentication than for identification purposes, as it is easy to change the proportion of one's face by wearing a mask, a nose extension, etc.

7. Signature Recognition [8]:
   Merit:
   7.1 Low false acceptance rate(FAR)
   7.2 While, it is easy to copy the image of a signature, it is extremely difficult to mimic the behaviour of signing.
   Demerit:
   7.1 People may not always sign in a consistent manner.

The performance of biometric sources of entropy can be measured in terms of various error rates:

(a.) False Acceptance Rate (FAR) or False Match Rate (FMR) is the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.

(b.) False Rejection Rate (FRR) or False Non-Matching Rate (FNR) is the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

(c.) Equal Error Rate (EER) or Crossover Error Rate (CER) is the error rate at which the false acceptance rate (FAR) equals the false rejection rate (FRR). As, an identification device becomes more sensitive or accurate, its FAR decreases while its FRR increases. The CER is the point at which these two rates are equal, or cross over.

From the analysis of the above table, the best secure key-generator is, keystroke dynamics. Though this system has high FRR, this is compensated by the fact that additional hardware requirement for this system is nil and also the user's typing behaviour is inferred to be unique. Hence, it can generate highly secure keys. Currently it is in the research stage and has not been implemented in any web site due to latencies.
The next best seed-generator is, signature recognition though user dependent but, has low FAR and is highly secure because it measures the signing behaviour of the user.

The merits and demerits of the techniques are elaborated below.

1. Mouse[10]:
   1.1 Merit:
   1.1.1. The least 4 significant bits of the (x, y) coordinates of [w.r.t display resolution]: 0–
   1.1.2. 640/480 bits (15'), 0–1280/1024 bits (19') provide true randomness.
   1.1.3. No test has proved that this data is non-usable
   1.2 Demerit:

5.2 Hardware and Software Entropy Methods

Table 2 gives the various techniques and the measurement parameters used in Hardware and Software entropy methods.

Table 2:

Hardware and Software Methods

TECHNIQUE	**MEASUREMENT/PARAMETER**
Mouse[10]	Cursor position i. Movement start/end ii. Scroll direction iii. Button press/release
Sound card[10]	16-bit sample recorded across the microphone of the soundcard.
Network bit-errors[11]	Value of the error bit
Magnetic hard disk[12]	Variations in response time: Two modes of operation: 1. Paranoid- i. Speed of rotation of a disk(rotational latency) ii. Chaotic air turbulence 2. Utility- Randomness from disk access time
CPU temperature	Sensor measures the CPU temperature
Clock	Gathers entropy from-timing-differences between different physical high-frequency clocks in the computer:the drift between the processor clock and the rate at which interval timer interrupts
Video[13]	1. Fetches 2 images from a video (with a random delay in between) 2. calculates the difference between those two images and then calculates the number of information-bits in that data. 3. After that, the data with the number-of-entropy-bits is submitted.

1.2.1 The general position of the cursor at any instance of time can be estimated by an attacker, and will most likely have a pattern.

1.2.2 Only 8-10 bits of variability per event can be achieved while the expected is 20 or more.

1.2.3 If the mouse is not moved for a long period, it cannot be sampled to be included in the pool i.e presence of user is essential.

1.2.4 Attacker can gain control of these sources and force them to behave in a predictable way.

2 Sound card[10]:

2.1 Merit:

2.1.1 Entropy pool has a continuous source for random seeds even without user's presence.

2.1.2 The least significant bit has true random data.

2.2 Demerit:

2.2.1 Only the least significant bit is truly random hence high sampling rate with random wrapping of the bits into a byte is essential.

3 Network-bit error[11]:

3.1 Merit:

3.1.1 10.6% error bits is unique to the user and is not predictable by the attacker. Error bit cannot be easily modified either.

3.1.2 When LQI (Link Quality Indicator) is less than 45 the error bits cannot be controlled and hence attacker is unable to observe. Even if the attacker sends malicious packets he'll have to reduce the power of emission at which additional transmission errors will occur in the received packet. Hence provides high security.

3.2 Demerit:

3.2.1 If quality of the signal reception is more than 45, then the generated errors can be controlled and hence observed by the attacker.

4 Magnetic Hard disk[12]:

4.1 Merit:

4.1.1 2^-80 is the correct guessing probability of a bit if each output bit is taken from 1494 readings.

4.1.2 Timing measurements are from the noise hence randomness is maintained.

4.2 Demerit:

4.2.1 Although the components are deterministic, we 'assume' that the complexity and their interaction renders them randomness.

5 CPU Temperature:

5.1 Merit:

5.1.1 No new hardware required for sourcing entropy.

5.2 Demerit:

5.2.1 The variation of the temperature may not be too high in an interval, they will fall into a small range hence proving to be a weak entropy source.

6 Clock:

6.1 Merit:

6.1.1 Every value passes through a test of FIPS (Federal Information Processing Standards) only on passing through this test it is included in the entropy pool, hence true randomness is ensured.

6.1.2 4-bits of entropy per interrupt

6.1.3 Randomness does not depend on external events

6.2 Demerit:

6.2.1 Clock random generator delivers entropy only every 3 minutes, hence not suitable for desktop or server usage.

6.2.2 This not applicable for processors that use a single clock for interval timing and CPU clocking.

7 Video[13]:

7.1 Merit:

7.1.1 It is highly useful when there is lot of demand for entropy data and maximum random data is required in the entropy pool.

7.2 Demerit:

7.2.1 It may sometimes report that it could not access the video device.

From the above comparisons it is concluded that, for a system to send data securely over a network, the high random seed that can generate a secure key is network bit-error. The demerit of this source is, if the reception power is more than 45, then it can be controlled and hence observed by the attacker. But, because transmission of bits is the most energy-consuming operation, each node tends to minimise the transmission power and therefore increase the erroneous bits. Hence, high entropy can be gathered in a short interval of time and hence fill the entropy pool.

The other efficient entropy source from which high entropy can be gathered is sound card. Sound card is an external device attached to the system and requires high sampling rate because only its least significant bit is purely random. But, it can function independently without user's presence and provide a continuous source to the entropy pool.

While the others like, in mouse-it has higher susceptibility problems, magnetic hard disk lacks assured indeterministic components, in CPU temperature and clock -variation is not high over a short interval and hence too slow at filling the entropy pool, and though video is a relatively better option because of its high entropy, the major problem faced is that sometimes video may be inaccessible. All these sources can fill the entropy pool though their use as a seed for key-generation is only more than seldom.

6. CONCLUSION

We have presented a comparison of entropy sources available to an average PC user. The table has been verified and evaluated. The best entropy sources chosen from each table considering every criteria for comparison is, keystroke dynamics and network bit-error. They have been classified to have maximum randomness among all the others in the table. Hence enable very high secure key-generation by a RNG.

7. REFERENCES

[1] Chris Roberts: PDF: Biometrics 2005

[2] George Landon, Chao Shen, Chengdong Li: PPT: Random number generators.

[3] UmutUludag,SalilPrabhakar: PPT: Biometric Cryptosystems: Issues and Challenges

[4] Anil K. Jain: PPT: Biometric Authentication based on Keystroke Dynamics.

[5] Sanjay Kanade, Danielle Camara, DijanaPetrovska-Delacretaz, and Bernadette Dorizzi:Application of Biometrics to Obtain High Entropy Cryptographic Keys, World Academy of Science,Engineering and Technology 51 2009.

[6] Andy Adler, Richard Youmaran, Sergey Loyka: PPT: Towards a Measure of Biometric Feature Information.

[7] Andy Adler, Richard Youmaran, Sergey Loyka: PPT: Information Content of Biometric Features.

[8] Biometric Newsportal.com,www.biometricnewsportal.com

[9] Biometrics Wikipedia: en.wikipedia.org/wiki/Biometrics/

[10] Robert McEvoy,JamesCurran,PaulCotter,ColinMurphy:Fortuna: Cryptographically Secure Pseudo-Random Number Generation In Software And Hardware.

[11] AurélienFrancillon, Claude Castelluccia: TinyRNG: A Cryptographic Random Number Generator for Wireless Sensors Network Nodes.

[12] Markus Jakobsson, Elizabeth Shriver, Bruce K. Hillyer, Ari Juels:A Practical Secure Physical Random Bit Generator.

[13] vanheusden.com software development,www.vanheusden.com/ved/