Feline Entropy Project



Defcon XV

Nick Kryptr
nkryptr@classful.net

What this is NOT:

A discussion of political reality:

-Any eg. Trusted Computing Initiative will necessarily involve key escrow or similar sophomoric attempt to subvert user security and privacy.

-That a large telco recently admitted to transporting wheelbarrowloads of data snarfed with span ports onto magnetic tape directly into the waiting arms of a well-known TLA says more about user apathy than cryptographic insecurity.

What this is NOT:

A criticism of ex machina randomness:

-With the publication of RFC4086/BCP106, randomness has become a standard.

-Little attention has been paid to the black art of entropy of late, as ever-greater CPU clock speed has brought us measurement of hardware noise with seemingly quantum granularity.

-Given the audience's particular penchant for system security (or lack thereof), it is incumbent upon the hacker community to punch holes in the basic premise, namely that hardware under the control of a potentially compromised operating system can be trusted.

-"Law RNG-2: Anyone who uses software to produce random numbers is in a "state of sin". [John von Neumann]" (Wagner, pp. 99)

What this is NOT:

A reference Design:

-Nothing presented here should prompt anyone to try this at home, or to trust entropy bits thusly generated, as being cryptographically secure.

-(Patent pending.)

-((Hey, if that laser pointer guy can get away with it...))

What this IS:

-An examination of the considerations and challenges inherent in solving the problem of reliable cryptographic entropy

-extra machina

-on a relatively low budget

-using COTS materials

Why?

-extant methods use hardware intrinsic to the system, in theory, all systems are pwned, therefore these entropy methods suck.

-extant methods are insufficiently complicated.

-no amount of legislation a la Patriot Act, or rubber-hose cryptanalysis, can persuade a cat to confess.

-cat /dev/cat - how postmodern.

Entropy:

Traditionally accepted definitions:

-Shannon's Equation (Shannon)

-Comparison of binary data to statistically typical binary data, or testing to see if data compresses ("Maurer's Test")

Project Goals:

1) Produce data to be subjected to tests of randomness.

2) Move entropy study from the theoretical to the practical.

3) Embrace the Heisenberg Effect.

4) Explore attack scenarios using a real-world example not implemented in software.

Methodology:

Equipment:

1) Cat

2) RFID tag - model EM4102 - using a Read-Only chip during Phase 1 solves some of the issues outlined in : www.rfidvirus.org

3) RFID readers - Trossen Robotics Phidget USB reader (www.trossenrobotics.com)

4) Data collection equipment - Assembly A (see appendix A)

ITEM #1



"Random Packette - Feline experimental subject"

ITEM #2



ITEM #3



ITEM #4

[not shown]

Methodology:

Process:

-Item #1 (Cat) to be implanted with Item #2 (EM4102). This may require replacement of existing Avid chip, which is proprietary, and for which readers are prohibitively expensive, given that neither of these chips supports anti-collision. Special care must be taken if this is the case, since EM4102 is not supported by local shelters and Veterinarian offices, to prevent the escape of Item #1.

-Item #3 works with Item #4 in several strategic locations around Item #1's abode and surrounding environs. In the initial test phase, Item #4 is wireless, using an 802.11 interface and USB reading from the Phidget to transmit RFID tag data onto the 802.11 network, with a timestamp.

-Data so transmitted will be intercepted from the network using tcpdump, snort, or similar mechanism, and used to populate a relational database.

Methodology:

Process:

-Item #4 are distributed at areas of frequent transit for Item #1, as opposed to areas of frequent rest. In Phase 1, these areas are determined using experimentation. For example, feeding/watering areas, litterbox, cat tree, would normally be characterized as areas of relatively static activity, but experiment may determine suitability.

-Initial observation of entropy will use time interval 't' between observances of 'Intercepted Packet' or Tagged Cat Presentations. This is similar in principle to the current methodology used in numerous programs with user input from keyboards.



[Static Activity in cat tree.]

Methodology:

IKEA toy department - item "SPEJA" provides an enticing environment for cats. Taking advantage of the long RFID reader range, readers can be mounted at either end of each tube, with tubes running between typical cat destinations.



[Packets move in tubes, not dumptrucks.]

Methodology:

Considerations: Security

-802.11 - 'nuff said. Obviously the project must balance the use of this technology with the issues inherent in clock variances among several distinct electronic assemblies with autonomous data storage, and the inherent cost (and potential Tempest vulnerability) of cabling the distinct assemblies together using 802.3.

- In each of the Ethernet cases, the obvious advantage in clock synchronization is the use of NTP, but this itself is potentially a liability, as special care must be taken to secure the network against the introduction of spurious NTP messages. Also, the use of crypto on the wire (or lack of wire) will necessarily introduce latency, although this may or may not prove significant.

Methodology:

Considerations: Security (continued)

-Read-only RFID chips, such as the EM4102, are subject to spoofing or replay attacks.

-Read-Write RFID chips are subject to additional types of attack: www.rfidvirus.org

-RFID - range can be an issue. Proximity limits mean designs must incorporate architectural features designed to assure proper distance and orientation of tag with reader.

Methodology:

Considerations: Security (continued)

-Potential vectors of observation:

--Frequency analysis against vulnerable points - food dish, water bowl, litter box

--Is the Veterinarian a confederate of the Observer?

--Is it possible for the Observer to introduce non-random data via such means as releasing birds near a window?

--Do Felines engage in stereotopy? (Yes. See Appendix for references)

Methodology:

Considerations: Security (continued)

-Potential factors influencing randomness:

--Catnip

--Heisenberg Effect - does the cat know she's being observed?

--Heisenberg Effect - given the difficulty of conducting double-blind research in this area, will the people involved affect the outcome by their own behaviors? Does this affect the randomness of the data? Further experimentation is necessary.

Methodology:

Considerations: Security (continued)

-Potential factors influencing randomness:

--Play-time - cats will often invent hallucinatory prey creatures ("invisible energy monsters") in the absence of actual play with people or other cats. See also - stereotopy.

--Increasingly sedentary behavior with age, diet, or other factors



[Sloth is a factor.]

Full Text and ongoing notes at:

http://fep.classful.net

Questions?

5A57 7E68 A6E6 5E2B 4E30 3B50 B000 D6BA D2AC C0F7

Partial List of References:

IKEA - http://www.ikea.com/us/en/catalog/products/80078877

Maurer, Ueli - "A Universal Statistical Test for Random Bit Generators." Lecture Notes In Computer Science; Vol. 537 - Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology - ISBN:3-540-54508-5

Schneier, B: Applied Cryptography, Second edition, page 234. John Wiley and Sons.

Shannon, Claude E. A mathematical theory of communication. Bell System Technical Journal, 27:379–423 and 623–656, July and October 1948.

Wagner, Neal R. The Laws of Cryptography with Java Code. 2003.