Why you need passwords – and how to make them strong

3 May 2023

Jacob Welsh
CTO, JWRD Computing
http://jfxpt.com/
sales@jwrd.net

IRC: jfw

0CBC 0594 1D03 FD95 C3A4
7654 AE0D F306 0255 94B3

Overview

- Who needs passwords and why?
- What makes a strong password?
- What is entropy?
- How can you obtain entropy?
- What toxins in the current environment are working against you?
- How can you remember strong passwords?

Why?

- To enforce ownership of your own information
- To be a trustworthy custodian of others' information

Not *everyone* needs passwords.

Common authentication devices

	Biometrics	Hardware tokens	Passwords
Source	Past developmental processes	Issuing authority	Generated by you, on demand
Information type	Public	Maybe private	Private
Available quantity	Low	High	High
Difficulty of stealing	Low	Low	High
Ease of concealing	Low	Low	High
Ease of replacement	Low	High	High (except when used as encryption key)
Implementation complexity	High	Moderate	Low
Ease of learning	High	High	Moderate

What makes a strong password?

- “The only way known, and the only way that can ever be or will ever be devised to transform *a computer* into *my computer*, as a matter of fact rather than an exercise in delusion -- relies on the use of entropy. There is not, nor could there ever be, any alternative.”
  - No Such lAbs (S.NSA), 2016

Cryptographic entropy

- Values selected from a set with full uncertainty
  - Can’t be predicted with any better odds than random guessing
- Measured in bits*: N* bits = choice from set of 2^N items
  - Equivalently, *N* choices from set of 2 items
- Cannot be obtained by mathematical means; must come from the physical world (nature)
  - "Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin." -John Von Neumann, 1949
- *Statistical* randomness is implied but it alone is not sufficient
  - It’s not enough to *look* random

Cryptographic vs Mathematical Entropy

- Random?
  - 652365236523652365236523652365236523652365236523652365236523652365236523652365236523652365236523652365
  - 89793238462643383279502884197169399375105820974944592307816406286208998628034825342117067 9
  - 50290311513578909777794133208102338438100824625282625299557865259335027642585324540529817 5

Cryptographic vs Mathematical Entropy

- Random?
  - (6523)(6523)(6523)...
    - No
  - (3.1415926535)8979323846264338327950288419716939937510582097494459230781640628620899862803482534211706 79
    - No
  - 5029031151357890977779413320810233843810082462528262529955786525933502764258532454052981 75
    - Maybe? (Until now!)

Cryptographic vs Mathematical Entropy

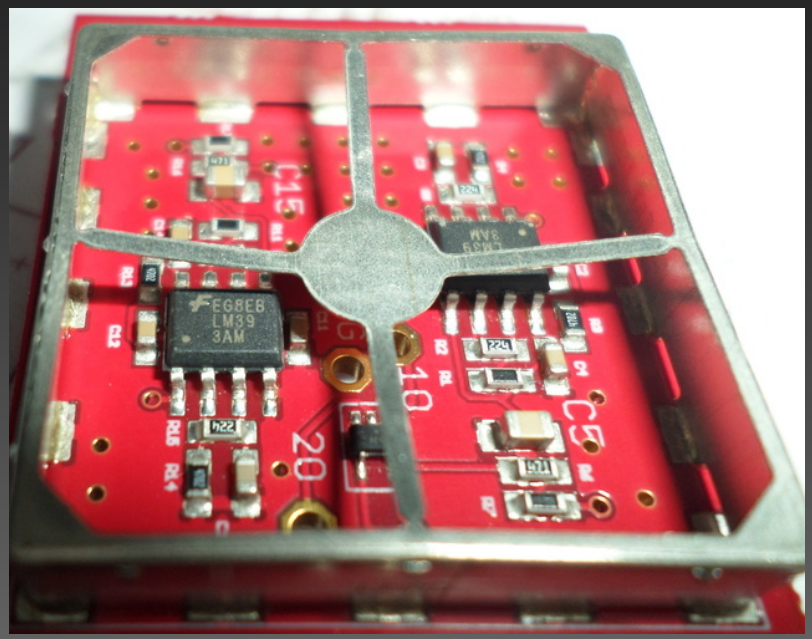
- Cryptography deals with systems which include *enemies.*
- What matters isn't whether a number "looks" random or "is" random (whatever that would mean) or even "was randomly generated", but rather the likelihood that a number produced by *your generator* can be deduced by *your enemy*.

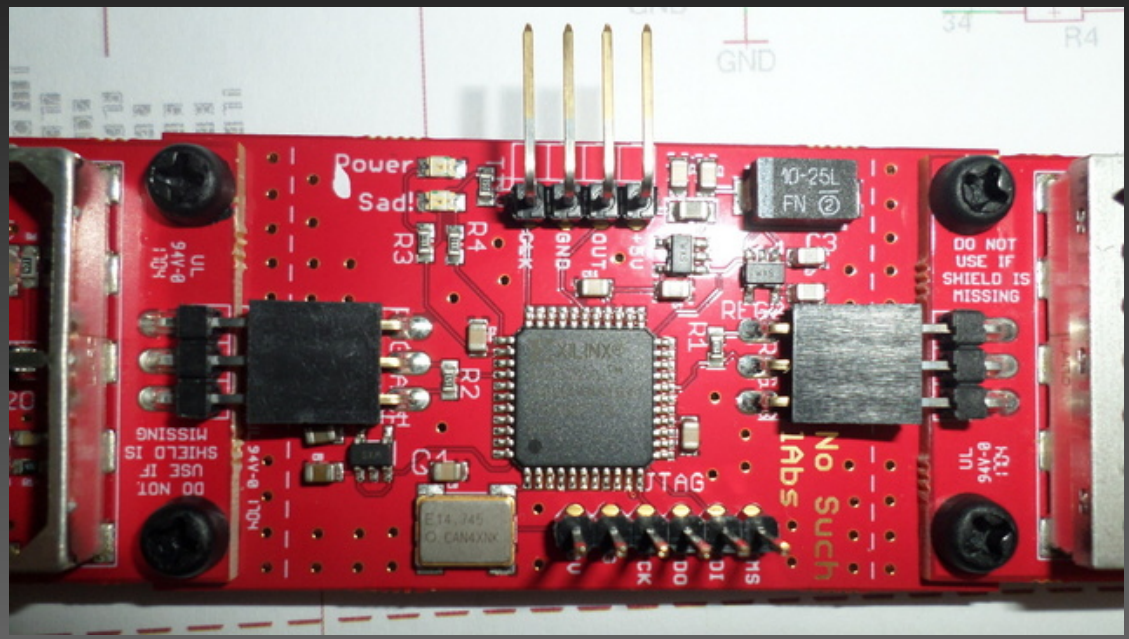
How much entropy is enough?

- Online vs. offline password cracking
  - Can the attacker bring all their computing resources to bear (having access to encrypted material) or are they rate-limited (querying an interactive system without access to its internals)?
- 1 GHz = 10^9 cycles/second
- 32 years ~ 10^9 seconds
- $10^{18} \sim 2^{60}$
- 32-symbol alphabet = 5 bits/symbol
- 60 bits = 12 symbols (characters)
  - Probably adequate for online scenarios
  - Otherwise stick with 128 bits ~ 25 symbols

How to get entropy?

- Digital computers are built to be deterministic; they are inherently entropy-poor
- Combine them with purpose-built circuitry for collecting environmental noise: a Hardware Random Number Generator





Cheapened RNG substitutes

- Pseudorandom functions
  - Garbage in, garbage out (at best!)
  - USG.NSA influence on cryptographic standards: Dual_EC_DRBG
- Hardware RNGs integrated in CPU
  - Unverifiable: “Just trust me!”
  - Intel RDRAND; ARM “security” features (phones, “hardware” wallets...)
  - Whitening: pass statistical tests by obscuring the physical noise

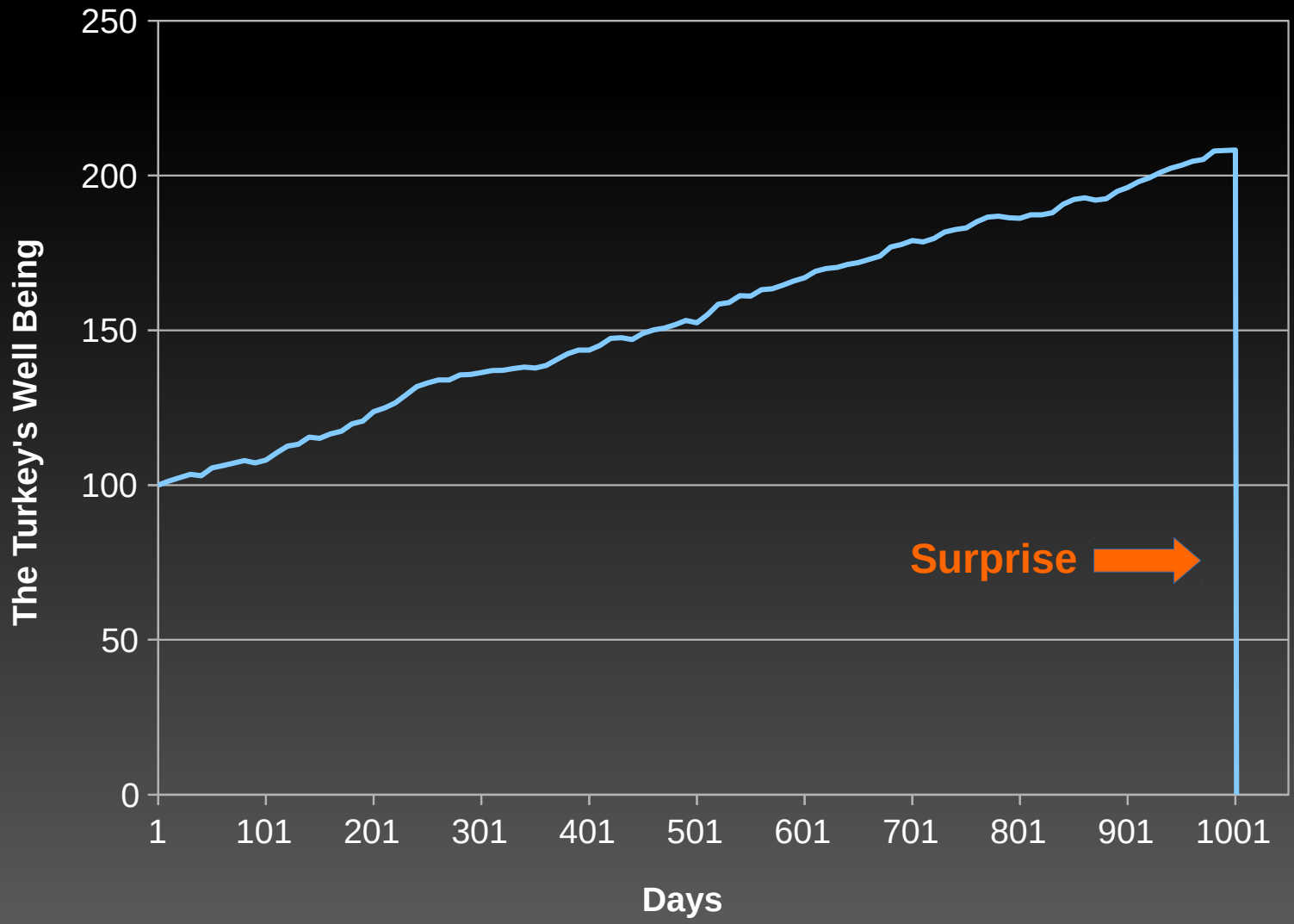
Cheapened RNG substitutes

- “Since 2011, the total spending on *Sigint enabling* has topped $800m. The program "actively engages US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs", the document states. None of the companies involved in such partnerships are named; these details are guarded by still higher levels of classification.
- “Among other things, the program is designed to "insert vulnerabilities into commercial encryption systems". These would be known to the NSA, but to no one else, including ordinary customers, who are tellingly referred to in the document as "adversaries".”
  - The Guardian, 2013

Do the risks matter?

- “What I’m doing has worked fine so far.”
- The problem of induction
  - Can you predict the future based on past observations?
  - Limitations of learning from experience
  - Illustrated through the worldview of a turkey (aka Russell’s chicken, adapted for a New World audience by Taleb)

1000 and 1 days in the life of a Thanksgiving turkey



Dice password generation

- 36 symbol alphabet ~ 5 bits per character (2^5 = 32)
- 25 characters > 128 bits

	1	2	3	4	5	6
1	a	b	c	d	e	f
2	g	h	i	j	k	l
3	m	n	o	p	q	r
4	s	t	u	v	w	x
5	y	z	0	1	2	3
6	4	5	6	7	8	9

Long-term memory

- Cryptographic entropy implies *mental* entropy
  - no such thing as “easy for you to remember but hard for others to guess”
- “Like so many aspects of the human brain, understanding of the capacity for long-term memory still eludes us, which sure, makes it a jerkoff move to suggest you memorize truly endless lists. This works both ways, however; it also makes it a jerkoff move to suggest you can't (or worse, "aren't meant to") memorize a handful or three. ... what's your limit? Nobody knows, but you sure as hell remember more than nine things from more than a few minutes ago.”
  - Hannah Wiggins, 2020

Long-term memory

- “The real problem at hand is that one's memory craves some *reason* to remember a given string. You need cause to get something transferred from your short-term, working memory to your long-term memory ... the information's got to be important, and not "because it's a password", but because it's a password for *something of personal or objective value*. Of course it's nigh on impossible to recall thirty and risin' distinct strings that grant access to things one doesn't care about, even if your personal brand of "because I said so" is especially strong. And *of course* every tool and service under the electric sun requires setting up an account for no ostensible reason. No ostensible reason, except to make you create and remember yet another password. Perhaps you'd like to store it somewhere? *It's so easy*.”
  - Hannah Wiggins, 2020
- Learn to “`gpg -aer`”
  - Learn one or a few strong passwords and use them to keep the rest in an encrypted text file.
- Hit the gym and get in the reps!

Recap

- Who needs passwords and why?
- What makes a strong password?
- What is entropy?
- How can you obtain entropy?
- What toxins in the current environment are working against you?
- How can you remember strong passwords?

http://jfxpt.com/

Resources

- http://jwrd.net/#training
- http://nosuchlabs.com/ (https://archive.is/hXB4r)
- http://jfxpt.com/2022/jwrd-rng-working-spec/
- http://thewhet.net/2020/02/manage-whats-important-to-you-with-rational-tools-when-you-join-humanity-or-fuck-mozilla/
- *Revealed: how US and UK spy agencies defeat internet privacy and security*, https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (https://archive.is/sgqnO)
- *On the Practical Exploitability of Dual EC in TLS Implementations*, http://dualec.org/ (https://archive.is/g3AuA)
- *Hopefully the last post I'll ever write on Dual EC DRBG*, https://blog.cryptographyengineering.com/2015/01/14/hopefully-last-post-ill-ever-write-on/ (https://archive.is/gXXYi)