Qwyit – An Engineering Story

I'm constantly asked to review new security technologies. Someone sends me a website, and wants me to tell them what's new, special, different, superior, or lacking about the company, their products and/or technology. And it's such a shame, that I always have to say the same thing, over and over again:

They are just rearranging deck chairs on the Titanic.

Now don't get me wrong…these companies are some of the best new thinking available. And they are backed by some of the smartest money in all of technology. Which, of course, is why I keep my distance from sharp knives and medicine cabinets; otherwise I'd off myself at every review!

Look: 'Digital Security' means only one thing – that life online is the same as it is in person. There isn't a technology in the universe that will stop people from cheating each other, stealing stuff, causing harm for the thrill – and this happens about 2-6% of the time. Just check out the FBI's yearly stats on physical crime, and it's fairly static. "The Best" online could do, would be to get to that 2-6%. Online treachery is well over that, and growing – depending on what stat you look up, it can be as high as 50%!

So what are these companies doing? They are making a fundamental, egregious error: Symptom fighting. Not disease curing. They take something that 'worked' as a solution to some problem, and misapply it on another problem. So not only have they gone astray, they never really even looked to see if the original 'worked' still applies, was correct, the best fit, etc. So the 'solutions' they tout are nothing more than another pass at some part of The Total Problem, without any merit in the ingredients:

There isn't a Chef on the planet that can make a gourmet meal out of garbage.

One can certainly make Art out of garbage; and these companies, their products, their marketing departments, their investors, their customers even, are gloriously painting the Security Technology canvas brilliantly – without a single bit of actual, measurable, systematic reduction in the constant, growing Digital Security Problem: life online isn't secure, it isn't the same as personal interaction.

…

So what *would* actually reduce digital crime, bringing it in line with personal conduct? The sobering reality is that it's quite simple – nothing like the complexity espoused by 'The Experts' in the field: cryptographers, mathematicians, computer systems gurus:

Just like the simplicity of solving The Climate Change Problem by electrifying *everything* and then cleanly generating that electricity not from fossil fuels but from renewable energy sources, the simplicity of solving The Digital Security Problem is nothing more than encrypting *everything* and unbreakably generating that universal ciphertext not from broken/slow/incompetent algorithms, but from the only provably secure cipher, the One Time Pad (OTP).

And…as you surmised with your smirk at the correctness, yet seeming implausibility of solving a HUGE human problem like Climate Change with such a simple method, the exact same 'implausibility' exists for solving a HUGE human problem like Digital Security. But…whereas the first problem requires human cooperation, which in and of itself involves a miracle (!); luckily, the second problem only requires a technological advancement:

Unique Key Generation for all those OTP messages. Once that method arrives – and it incorporates the necessary properties (speed, efficiency, flexibility and maintains the provable security of the OTP) – then all we need to do is put out the software, the firmware, the hardware…and Encrypt Everything, Everywhere, for Everybody. Then digital crime will be 2-6%, insider jobs, bad people, humanity's bane. Problem Solved!

…

This relegates all of the misdirected effort of the current corps of companies to meaningless shenanigans, as none of them are, or have ever, worked on the ***only*** Cryptographic Problem: Since there is a 100 year old, simple, provably secure cipher, the OTP, that has only one key requirement where every bit must be unique, *the only problem to solve is how to generate and share those keys!*

This is an engineering problem: lots of people, lots of messages, and lots of unique keys that seemingly are impossible to distribute and pre-share. The solution to this, of course, is exactly like the solution to all engineering problems – there is a principle, somewhere, that can be, should be, and will be relied on to deliver the solution. Engineers discover or bring about these principles, and they gain the necessary understanding, by doing what they always do:

Define The Real Problem!

In the Digital Security case, the problem can be succinctly summarized:

Since it is impossible to pre-share endless keys for endless messages, what **single keys** *can be* pre-shared and acted upon by a *method that will render them endless*?

Turns out there's a simple one, and it has all of the required properties – it's the same one used for centuries, when one needs a unique series of continual inputs but some small way to encapsulate their creation: Dice.

Why didn't anyone think of that? If you and I share 2 small little cubes, we can create an endless series of numbers between 1 and 12 without having to pre-share a series of values, like 6, then 2, then 9, etc.

Using that metaphor and example, the solution to the endless keys problem is to provide 2 numeric keys (just like the dice), and 'throw them' (just like the dice!). Where 'throwing' is the simple technique of using one of the keys to point into the other one, and select out individual digits, add them together, and use the result. This 'dice throwing' can actually be done endlessly, without any loss in the randomness and uniqueness of the 2 starting keys. This principle has been named 'Random Rearrangement' and the technique called a Position Digit Algebra Function (PDAF) by the inventor…me! ☺

So the first part of the solution has been delivered: we can provide single keys (in 2 parts) to everyone, and they can use them for at least one message endlessly – so all those messages meet the requirements of the OTP, and they are *provably secure* (which means *unbreakable* in lay terms!) Now all we need to do is update the keys endlessly, so we don't have to re-deliver them every time (certainly, re-delivering them every now and again is feasible, and desirable – so that isn't a part of the Digital Problem – it's using them over and over and over again, uniquely, endlessly.)

It turns out the solution to this second part is sitting right in the first part! All we need to have everyone/anyone do after they have finished their first endless, unbreakable message, is 'throw the keys' individually, alone without having to send anything to each other – as long as they both know how to 'throw them' in exactly the same way, where the pointed and added results are exactly the same size as the starting keys but now uniquely

updated – everyone has new keys to use endlessly once again! And because this engineering solution is wonderfully elegant, they did this *without having to communicate with each other!*

Now…the only remaining engineering obstacle to implementing this solution, is to 'share' each other's single key with multiple people. Because each person will, of course, need/want to communicate securely 'throwing their dice' with lots of people – so how does everyone get/know our individual keys? Luckily, plenty of other smart engineers have already solved this problem – because it is the fundamental human privacy problem: Who Do You Trust?

And that solution varies dependent on the 'network of people' who are communicating. Banks do it one way, stores do it another, countries do it yet again – and all of them, collectively, rely on a principle called 'Federated Trust'. You get a driver's license by showing your birth certificate – each now relying on the place you were born. So this portion of the Digital Security solution is easy to implement, easy to configure, easy to *solve – because the owners of those networks fundamentally rely on a trust network*. This is how it works in person, so digitally implementing the trusted sharing of individual endless keys can simply mirror those 'networks'.

…

Whew…I don't know about you, but I'm exhausted. Both from telling that story over and over, and from wondering just exactly when the world will accept such an elegant, simple engineering implementation of Gilbert Vernam's 100 year old genius One Time Pad. He already solved The Digital Security Problem, he just needed 'the engineers down the hall' to build it. And implement it everywhere. No cryptographers needed.

Unfortunately, it seems that 'Down the hall' stopped working on the problem before lunch on the very first day…since all cryptography does today is sloppily re-invent existing Perfection by making it worse, breakable, slower…dumber. The Digital Security Problem is solved – the answer exists. All we've got to do is proliferate it…everywhere, for everyone to use every time. And all those new companies can re-direct their efforts into the implementation of a Perfect Solution, across all the varying hardware and software of today's ever increasing, interconnected communications networks, instead of polishing their marketing so everyone continues to suffer.

…

Okay…I've got to run…seems I've just received a new request to review yet another Security company…I need to take my Valium first…