Top 10 Reasons Why Unbreakable Matters

I know what you're thinking: 'All this cybercrime stuff is terrible…but they don't actually break the encryption – they get in other ways, so what we've got is good!' This is like saying a restaurant is 'good' because it has food. There's good, better, best ingredients…and good, better, *unbreakable* encryption. Using the best matters.

Here's how:

10. Which car do you want to drive?

So there's a crash fatality test for two different cars. One of them passes the test 95% of the time; the other, 100% of the time. You choose. Out of, say, everyone on the planet, how many are choosing the fatal one? Right: when it comes to an absolute, unbreakable is it. It exists – there *is* a 100% safe secure communication method, it is unbreakable; and all of the ones in use today are those 95s…they are *less than safe*. The funny thing is, of course, that safety is an absolute too: you either have it, or you don't. 95 ain't 100.

9. Here's a list of *eleven cryptographic attacks*. None of them – zero – exist for unbreakable

Whether you're a crypto-geek and 'know this stuff' or not, there's a set of fundamentals for attacking cryptographic schemes. Those who write algorithms (less than unbreakable), they categorize those attacks. Here's an interesting thing: *none of them exist for unbreakable*. Not *some* of them, under this or that scenario – **none of them**. And the assumptions? Just these: you've got the ciphertext, each and every single unique bit of it (literally, in digital terms – every *1 or 0, every bit*) is available, there is no 'cipher' (it's just a key added to the plaintext message), and every key bit is only used once. Go ahead – attack! You won't get anywhere – unbreakable is *unbreakable.* Now, if you're like me, you're thinking the same thing: *What are all those attacks for then?* Yup: the stuff *less than unbreakable*.

So: we make less-than-unbreakable…have to categorize all the ways it can be broken…can't think of them all, so they keep appearing over time…then we make new, still less than unbreakable to 'fix' those…then we…*are lost down the rabbit hole!* Attack scenarios don't exist with Unbreakable. Rabbit Hole…Shut It Down!

8. Unbreakable is a whole lot faster

You've heard of that 'order of magnitude' saying, yes? Like 'Today's politics are an order of magnitude worse than in previous generations.' Ugh. There's actually a real, math definition – and it's when you change the exponent, like from 10^2 to 10^3. Computing these less-than-unbreakable encryption methods, like the AES standard you've heard of, takes in the hundreds of computer cycles per byte to accomplish on regular machines. Unbreakable, just adding a key to the plaintext, can be done in a less than 10 cycles per byte. Now think about your computer session…add mine…now all of us using the same ISP…throw in everyone in America…don't forget China…*WOW*! Order of magnitude speed improvement is World Changing. **World Changing**. Because I know that when things can be done *faster*, we all get *more done*. And then, we can get *new things done* using the same networks. OMG. No wonder they advertise 'Better, *FASTER*, Cheaper'. It's what changes the world.

7. Because it's faster, it can be done more often and in more places

Here's the first thing about digital networks: there's a whole bunch of parts. Web servers, backbone switches, routers, commercial switches, wires, wireless, more switches…oh my! Been on a road trip lately? Network Encryption is like taking all the kids in the neighborhood on a long distance drive: Let's Stop At Every Place! Every. Single. Place. The performance degradation (much like the frying of your brain while driving those kids!) can't be solved because *you have to stop*. The different owners, different laws, different content, etc. all demand a part. The *only way* to speed up the trip, is to *make all the stops quicker*. Unbreakable – fast – can be done everywhere, without adding any total time. Oh – and some of those places have a specific timing that must be met…you have to manage your whole trip around them: and if you take longer, Big Problems. Since unbreakable is so much faster, you can meet any timing schedule, at any point along the trip. More Often, In Every Place.

6. Because it's more efficient, it can be done with a whole lot less…energy, footprint, devices, etc.

So speed – performance – is a kind of efficiency. But there are others, all having to do with encryption: bandwidth (the number of messages related to setting up the encryption, and the actual amount of 'stuff' in those messages); footprint (the amount of software and/or hardware code required to do the encryption (setup and execution), where it needs to be, how often it needs to be executed (memory requirements, etc.)); devices (the specs for the minimum device capability in order to store and operate); energy (how much power does it take to 'do' the encryption, based on how much is available, how long it has to operate, etc.). *When all of these are more than something else that is also more secure, there is* ***so much less room for doing the real purpose of the network communications!*** Efficiency is the true benchmark of 'Cheaper'. And Less Is More.

5. When everything's unbreakable, communication is finally like everything in person

You and I know just what to do, expect, and operate in order to communicate in person. We know what to say, when to say it, how to say it privately – everything is known. Now – imagine if when we were talking out loud to each other in a restaurant, suddenly, we changed to talking in code. Every person in there knows we just 'went secure'. Same with encrypted traffic – only the good stuff is encrypted. It's like putting a Big Neon Sign on the back door of the Bank: *"This Entrance FOR CRIMINALS ONLY!"*

20 years after SSL's introduction into Internet traffic, only 75% of the traffic is secure (it's TLS now). This is due, *exclusively*, to the encryption (and authentication) methods used – for less-than-perfect stuff – because they take too long, and are incredibly inefficient. Unbreakable, in terms of the above efficiencies and speed order of magnitude improvements, could easily be put everywhere. And every message has the same perfect security: everyone in the restaurant is having their own, personal, private conversations – and everyone knows that it is *all* secure. This is the goal of digital networks: in person communication replication – and it *must* include, and play by, the exact same rules.

4. Legally, everything that isn't unbreakable is liable

A friend of mine asked me what I thought would be the outcome of all the Equifax attack lawsuits. I told her nothing. I had to explain that it wasn't because they won't pay $Millions, and fire people, and maybe even send a few through the Criminal courts. I had to explain that I meant that nothing will happen to stop the next one. She asked why – and I said because the Legal standard for digital cybercrimes aren't the same as they are for physical crimes. Oh they use the same *terms*, but they don't mean the same thing. Therefore, there won't be any need/pressure/law that brings about any change.

Take 'non-repudiation', for example – in person, this means that after someone has witnessed you signing a document, you have no means to challenge. In security, 'non-repudiation' means something less: it means there is a guarantee that it was you who signed. Yes, you read that correctly and understood it – in cryptography, the term is what the witness's purpose is in physical interactions. In person, it is the *recourse of challenging the event* – challenging the witness is something else entirely, and has a separate set of legal standards to pass in order to 'remove the credibility of the event.'

These two definitions are not the same thing. This is why anything less than unbreakable, if it were something that was used in the above restaurant communications, wouldn't ever be able to be used as a *witness* – its credibility simply doesn't exist, since it can be forged, changed, tampered with, etc. Those above cryptographic properties that are attempted to be implemented in today's encryption are trying to raise the level of 'Witness Credibility' – *and anything less than unbreakable is fraudulently being passed as capable.* Wouldn't it be nice, if instead of just waiting for the next Equifax, we did something about it?

3. If lawyers knew that all encryption was liable, there'd be negligence lawsuits everywhere

As we sadly watch the follow-on of the recent fatal bridge collapse, the first place any investigator will look: was the bridge built correctly; and if not, was it knowingly made inferior in some fashion. This is exactly the *Best Practices* that we hear so much about in digital security: we've got you covered, because We Do The Best Available. U'mmm…no, they don't. They do what they do because it's the only thing they think is possible. But it's not – unbreakable, which is **The Best Practice**, isn't done; it is defined, and most certainly is possible. And 'they' know that what they do doesn't meet that standard. This, if digital security was properly treated the same as a physical bridge, would meet the standard of criminal liability. After that's established…then it's on to negligence, for purposely using inferior products. All that's needed to remove all of these future legal issues, is to establish the proper Best Practice: Unbreakable.

2. Quantum Computers don't matter

Quantum Computers are coming…and they're going to wake the dead! You know what I'm talking about – you hear all these things about *The Future*; and, especially with new tech, you can't quite tell the hype from the kernel of truth (that is, *if there is one!*) So here's the truth: Quantum Computers will be a Quantum Leap in *speed* (get it?!) When they arrive, one of the things they absolutely *can do,* is compute an order (or ten) of magnitude faster, more, better. This means that certain types of calculating can be improved from today's value (a lifetime) to 'instantly' (like 5 minutes). As you might have heard, current encryption security is based on really big keys that take a really long time to compute – so when a Universe's amount of time becomes an hour long lunch break, encryption is *toast!* Uh-oh. But – **don't worry** – cuz The Security Boys are working on…(wait for it…)…"Quantum Safe" techniques! These are new types of algorithms that will *still* take a Big Old Time using a Quantum Computer!! OMG!

Want to hear something funny (sad, actually)? *Unbreakable is already Quantum Safe*! Because **Unbreakable isn't based on how long it takes to compute it: *It is always Unbreakable – forever***! The Security Boys are, again, feverishly trying to protect you…in the same ways they have been before: The Luddite Way! Unbreakable exists, it is independent of computing power, it is available now – and will be *AnyComputer Safe Forever*. Jeez…hopefully someday soon those folks will come out of their cave…

1. Network attacks are because the encryption isn't end-to-end

Well – here it is. All of the above are a great collection of reasons why unbreakable encryption matters, and why it should be The Holy Grail of cryptography. And I had fun articulating all of those things…but there is a short-cut Plain As Day reason: All of the network attacks that occur – *every single one of them* – is because whatever communication is being made, whatever content is being shared, whatever network is performing the messaging, however the data is stored – it doesn't start encrypted…and end the exact same way. It wouldn't make a single bit of difference what anyone tried to do, how they tried to do it, where they do it, when they do it, with whatever special magic they possess to do it, *if I encrypted my message…and no matter how it got to you…you were the only one on the planet that could decrypt it.* While this ***seems*** to be hard to do…it isn't. Unbreakable Encryption exists…it's simply a matter of implementing it. That's not hard…it just takes desire.

Thanks for listening…and learning about why Unbreakable Matters. I'll leave you with a sobering thought:

There are 5 new LPWA (Low Power Wide Area) security protocols being proposed to the various 'digital authorities' as the *future standard*. These are crucial to the next-world, Internet of Things future…the one you're being promised and the one you've watched in Star Wars movies for 50 years. But…

Not A Single One Can Perform End-To-End Security. None. Not a one uses unbreakable encryption.

What does this mean? Oh you'll get your networked Future, all right. It just won't look anything like what you want it to…it'll look just like it does now: Broken…still in need of repair.