CPA
Practice Advisor

from sound to SMS texting to Internet web pages: but none of them use Gilbert's OTP! So why doesn't cryptography use this perfect Unbreakable cipher?

Feb. 14, 2018

Cryptography, in the dictionary, is the art of writing or solving codes. In the security world, it's the practice and study of techniques for secure communication in the presence of third parties called adversaries. I call it sharing a secret.

And the perfect, **unbreakable** way to do it was invented over 100 years ago by an engineer named Gilbert Vernam. All it took for anyone to send an Unbreakable

message was to pre-share a one-time-only encryption key, which is known as a **One-**

this **Key Distribution Problem** (KDP) was quite a problem!

In the 1970s, large networks were envisioned and created. Cryptography's luminaries at the time arrived at a dual-key approach as their attempted solution to the KDP – and this way everyone only needed one key (a public key) and anyone could talk to them. The problem with their idea: it didn't work as an encryption capability since it was way too slow, so it was only an authentication mechanism.

Not only did their new approach not work for encryption, it was so slow that it couldn't do more than the very beginning of any messaging session. The "tag-along" encryption mechanisms had to be different than the already perfect OTP, so Unbreakable was lost.

And to add insult to injury, both of the new approaches – for authentication and encryption – are not really based on fact, like the Unbreakable OTP. They are based on theory. And leaving a secret "theoretically" safe isn't a good idea – just ask any gossip columnist!

But as luck would have it, there is a solution to the Key Distribution Problem that uses the 100-year-old Unbreakable cipher. It's all about distributing those OTP keys, every time, for every use, to anyone who wants to message securely.

Here's how: Everyone gets one authentication key that verifies their identity. It mathematically – not theoretically – creates (but never sends) a one-time encryption key. Now we are back to Unbreakable encryption. As part of the process, the authentication key mathematically – again, not theoretically – changes every time it is used without being sent! Now we have Unbreakable key distribution as well.

Combination technology from OTP encryption and one-key authentication yields Unbreakable in any communication system and will in the near future have massive implications for all global networks. With that, let's examine how.

IoT:

flexible enough to apply, broad enough to encompass, uniform enough to limit required customization, and capable enough to actually perform within usability requirements.

That's why the current system just doesn't work—and Unbreakable will. When applied, it will finally deliver universal security to this market, transforming offerings to meet the consumer's vision.

There you have it, a Secure, Smart, and Interconnected Home.

Internet:

For over 20 years, HTTPS – the Secure Internet – still only gets used less than 75% of the time. This privacy void is directly related to the methods used by the current protocol that provides authentication and encryption—that locked, secure browser. HTTPS is terrifying slow, cumbersome, complex, full of one-off extensions and at its last chance ability to provide the next generation of Cloud-based, content rich, ever-present secure, private Internet.

What is required, then, is the Unbreakable OTP: order of magnitude performance improvement, streamlined efficiency, easy end-user participation, and universal application. A model for individual, secure connectivity to global content – whether provided by a Mom-n-Pop underpowered website or a processing-rich Web presence —is the future of the Internet Everywhere.

Ta-da!

Finance:

There has been a promised explosion in P2P financial applications…for…ever. The only problem is, there isn't any way to actually be certain that the security is

complete and end-to-end. And until those required properties appear for the back-

———————

Paul McGough is co-founder and CTO of **Qwyit**, created the first unbreakable crypto system, bringing universal connectivity for unbreakable communications to any network, application, or device.

Digital Currency • Small Business • Technology

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.