Cryptography Landscape

Did you know that wallpaper was the great inspiration for…*Play-Doh* (originally a wall cleaner) and *Bubble Wrap* (originally a textured wallpaper)?! So what great things will come when there's an order of magnitude improvement in network security? Let's take a look at where we are…and how the future can be unleashed!

In 1994, Netscape invented the SSL protocol for securing Internet traffic. Since then, the protocol has been updated (6 times in total) and renamed **Transport Layer Security**, **TLS** – we're currently on V1.2. It is the only *global* secure communications protocol in use. The updates have focused, mainly, on removing/solving threats that became apparent through criminal and research attacks. The updates haven't been to the *principle* for performing TLS, just to some of the specific underlying methods – and keeping up with all of the growing list of *extensions*, which are needed in order to actually *use it!*

There is a current proposed new update, and it is exclusively for one reason: TLS just isn't cutting it anymore! It has reached the end of its usefulness as there simply isn't any way to perform the principle mission (authentication and encryption) within the performance and efficiency needs of new network communications. *The new version actually diminishes the security in order to enhance the performance!*

Whether or not the great advances in computer/device storage and bandwidth will continue unabated for the next 24 years to prop up TLS, one thing is absolutely certain: It is now limiting the ability of new, wonderful communication ideas from being implemented – and secured! For instance, there are 5 new Low Power, Wide Area (LPWA) communications technologies: **and not a single one of them can provide end-to-end security**. What's wrong with that picture?!

What's wrong is the same thing wrong with these:

- Why do I need a credit card anymore? Every current solution costs a $billion in device/reader upgrades!
- Why aren't all of my calls private – VoIP, cell, *whatever?!*
- Why on earth do I need to go to a silly movie theater to see the latest release?

The reason these 'data systems' haven't been upgraded – like you carry around a mobile phone super-computer in your pocket! – is because there isn't any way for the data *owners* to have a secure relationship with their data *users*: YOU! *TLS is the principle for what to do,* and not only is it limiting Internet security, it never had 'The Right Stuff' to allow brilliant new ideas to flourish anywhere else! Time for a change.

QwyitTalk™, Security as a Service, has exactly the right ingredients:

- Performs within network tolerances without degradation, without new processing power
- Is easily placed into existing software, hardware and any communication protocol
- Doesn't require the end-user to 'do stuff they don't understand'
- Small, so it doesn't impede or limit anything already accomplished
- Uses *unbreakable* mathematics
- QT™ Is TLS – Perfect Forward Secrecy (PFS), authentication, encryption, integrity and replay prevention

The future of secure communications is in dire need of improvement – how else is someone going to write a new phone app to turn down that darn street light that shines through their bedroom window…only to realize they've invented the missing ingredient in unleashing the Connected Smart Home! Wallpaper, indeed.