One Time Pad

CoreVUE

High Level Description

www.TunnelVUE.com

What Does CoreVUE Do?

Imagine having a network of communication devices where each device could only communicate with each other or to the outer world in this manner:

- Assume that you have a secure "Core" server that is physically accessible only by your own trusted technicians, which has great firewalls to protect it from the outside.
- Your Core has a relationship established with each of its connected devices such that the relationship is only between the two parties, and the Core recognizes each device separately.
- Your Core shares an infinitely large pad of cypher codes with each of its devices, but has a different pad for each device connected to the network. Each device has one cypher pad exactly matching the one the Core has for it, and they can only communicate with each other by using a new page from that single pair of pads for encoding and decoding their messages every time they need to communicate. When that communication session is ended, both parties burn that sheet from the pad.
  - Each session using a new page also issues a *new* shared page for *every single word* of information in that session! Again, the Core and the device have the same page each time, using a new page for each word which is used to encode and decode each word as it moves from one end to the other.
  - Every word only travels from one end to the other (no matter how far it must travel or how many switches it must pass through) fully encoded. Once the word is received the page for encoding and decoding that word is burned automatically at both ends.
  - The Core knows exactly what device is sending what information—every time, all the time because it only shares a single pair of pads with each device. Devices cannot talk to each other, or talk to the outside world without going through the Core.
- It is impossible to decode/decipher *any* word unless one can simultaneously use both the session page and the word page (which are each destroyed after each single use) from the shared pads.

Now imagine a small library (about 60Kb) of software that can be inserted below the internet layer of practically any device that has a processor that can manage that entire process above within your own network - *even if you have thousands of devices in your network*. Every transaction is double-wrapped with encryption with a process that creates and destroys the keys automatically, on-the-fly using about as much processing power as 10 percent of a single core Intel processor. It goes through the same process digitally of issuing a new key for every transaction between Core and device, and for every packet within that transaction. Same result.

What you have is an extremely difficult problem for any kind of would-be malicious intruder! The word "impossible" comes to mind, even for quantum computing power. What you have is the most secure form of encryption available economically to practically any application and any network. You have power that will protect data in transit or at rest, industrial controls, infrastructure, and operations. While significantly increasing entropy, it reduces the attack vector for a network to a single site – the "Core" which is much easier protected than all the other connected devices. What you have is CoreVUE.

If you are interested, contact Rick Plaskett, Director of Communications, Tunnel VUE, Inc.
Email is richardplaskett@tunnelvue.com. Text or voice is 334-657-9986.