Introspective Networks Streaming Transmission One-time-pad Protocol (STOP) Technology: Cyber Encryption Defensive Capabilities and Benefits

Authors: Introspective Networks:
Anthony Scott Thompson
Dr. Nicole Nemer
Brig Gen Ian R. Dickinson, USAF (Ret.)
Brian Mielke
Steven Cummings
Editor: Monisha Merchant

Abstract: Over the last several years, there has been a marked increase in distributed automation and control that requires wide area networking (WAN) communication cybersecurity solutions, especially when the communication system relies on public Internet or shared IP networks. This includes increasing automation in logistics and supply chain management. Moreover, there has been a need for more secure communications across radio frequencies and network Layer 1 communications. Current encryption techniques do not address security shortcomings with WAN communications and introduce network latency that impede real-time response to wide area events in a given technological ecosystem.

To address these and other issues being faced by distributed automation and control, Introspective Networks has developed and patented the Streaming Transmission One-time-pad Protocol (STOP). STOP removes all network facing attack vectors including Man in the Middle, Injection, IP Header and DoS/DDos port based attacks.

This paper provides details around the benefits of STOP technology. Its aim is to educate on the technique and why network bandwidth is abundant resource that can be used to protect our data much more effectively than encryption alone.

Disclaimer and Intellectual Property Statement

This report has been created by Introspective Power, Inc. dba Introspective Networks for the purpose of furthering the understanding of Introspective Power, Inc. intellectual property. The additional purpose of the paper is to explore potential future business activities. Accepting this report and/or reading it signifies that the recipient/reader agrees that all ideas and concepts that may constitute intellectual property, whether trade secret, trademark, copyright or patent, remain the property of Introspective Power, Inc. This report in no way grant rights to any other party, including the recipient and/or reader including but not limited to license to or transference of any of the aforementioned property.

Both the recipient of this report and Introspective Power, Inc. agree that this report in no way commits either party to future work or contracts and is no guarantee of future business.

By accepting this report and/or reading it, the recipient/reader agrees to keep all information contained in this report confidential and not to release it to any third party without the consent of Introspective Power, Inc.

Table of Contents

Introspective Networks STOP Technology

Introduction

Introspective Networks Streaming Transmission One-time-pad Protocol (STOP), is a cyber security technique to protect data in motion like no other available today. STOP uses multiple layers of techniques moving uncrackable data in both time and space in a way that is unpredictable. If an unauthorized user comes across part of the data, it would have no idea how to crack it and, moreover, would have no means to know which part of the data this represents.

One of the key parts of STOP is the use of a Vernam Cipher also called the One Time Pad (OTP). The technique is quite simple: there is a message along with a series of random characters derived from naturally occurring entropy. The message and the random characters are combined using an operator that has an inverse and does not break the bounds of the character set. The output is encrypted data. The pad[1] book of random data and the encrypted data are then provided to the receiver by separate couriers and, once received, the inverse operator is used one character at a time to produce the results. If the random data is not calculated and both the pad book and encrypted data are kept separate and safe, this method is mathematically proven unbreakable[2].

The OTP proof is based on a simple algebraic equation: x + y = z. Even if z is known, if x and y are not, you cannot solve the problem as there is not enough information. So, intercepting one of the couriers does not provide a solution. This uncrackable property is the key to allowing STOP to create the most secure network transmission protocol known.

To simulate the “two couriers” in a network, we need two separate communications channels (at a minimum). In this way, the OTP and the ciphertext are separated in the network in some distinct way. The key at this point is to ensure that the random data can never be discovered while traveling across a network. Figure 1 shows at a high level a diverse path network example of STOP with two end point devices.

[1] While the term Pad actually harkens back to days when random data was kept in a pad book, the term is still used today to refer to a random set of data used for the purpose of encryption.
[2] "Communication Theory of Secrecy Systems - Network Research Lab." http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf. Accessed 29 Dec. 2016.

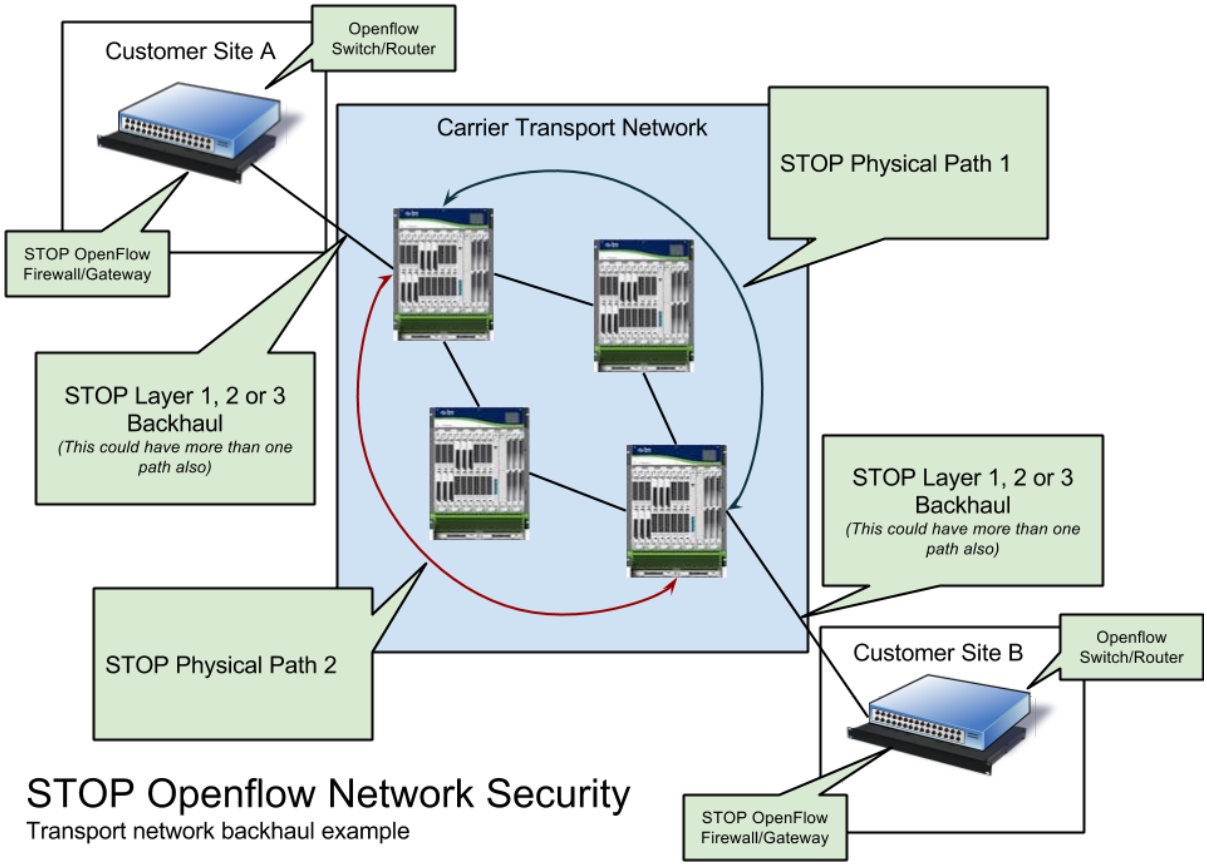

Figure 1: Openflow/NFV example of STOP with diverse path networking. In this example, data is moved at both layer 1 and 2 and also at layer 3's virtual ports.

Using an OTP directly in a network defies conventional thinking. The classic belief is that an OTP, the only uncrackable form of encryption with a mathematical proof, can not be used directly in a network. The belief falls on two notions:

1) The use of OTP will double the size of the network bandwidth making it impractical.
2) The second problem revolves around getting the metaphorical pad book or "Pad", as it's come to be known, across the network securely. The common myth is that even if you encrypt the Pad using existing techniques, the Pad is no more secure than simply sending the data across directly using that same encryption. In short, only a single step is added to the process of decrypting once you have both the OTP encrypted data and the encrypted Pad.

With all technology, there is a system cost. STOP is no different. With current encryption, the cost is processing time and the latency created in execution of data encryption/decryption. With STOP, this cost is network bandwidth. As a resource, you can actually gain more protection as you add more bandwidth as we will see later. The fact is advances in technology and infrastructure have made bandwidth inexpensive and abundant, reducing bandwidth to a fairly

insignificant issue for most types of data in most digital ecosystems. What once was a taboo system cost because of monetary consideration is now readily available and, monetarily, cheap. Moreover, data compression can potentially reduce the payload keeping the overall network bandwidth increase to a minimum. This reduction in payload size is a function of the data to be sent. Some data compresses well while other types do not and while others yet might already be compressed like a compressed jpg or png image. In short, effectiveness of reducing bandwidth via compression will vary but, if bandwidth is a constraint, compression should alleviate that concern in most general cases.

On further study, perceived insecurity or lack of improvement to security when encrypting a Pad for transmission turns out to be somewhat misleading and overly simplistic. Simple deductive reasoning can be utilized to explain. First, let's assume we are encrypting the pad for network transmission using AES256; the current standard for top secret data encryption in the US. Let us also assume certain entities have the capability to crack the key to AES256 in a reasonable amount of time. To know the attack has worked, the attacker would need to verify the success by inspecting the output of AES256 with the cracked key - a requirement to validate any encryption crack. Since a Pad's data is random, there is no way for an attacker to know the values; there is nothing to validate with any confidence. Unless they have the OTP encrypted data channel readily available to test this against and can align the two channels perfectly, this becomes a trial and error process.

Another way to look at this is the Pad itself is creating a double encryption that in turn creates an unsolvable problem. Because the Pad stream can not be discovered in this arrangement, it provides an adequate vehicle to transport the entropy securely across a network. This relationship has always been true so the old argument that the encryption is no more secure than the encryption that is used to transmit the Pad is fundamentally flawed when the pad is delivered as a streaming key. This statement would only hold true if there was a weakness that allowed the key(s) to be discovered but, even then, with proper random entropy, there would still be no method to validate the crack's success with any confidence. As we'll see later, STOP does not simply rely on this deductive reasoning but utilizes Polymorphic Encryption to change out keys and ciphers to further obfuscate the data from cracking.

With all that, STOP takes things even a step further and rotates the network locations, either physically, virtually or both, to ensure would be hackers are completely unaware of which channel is ciphertext and which is the encrypted Pad being transmitted. To a would be attacker, it only looks like gibberish in random locations in the network. The data can also be moved physically across any combination of differing waves of light, radio frequencies, wires, wire frequencies, geographic routes and/or carriers for the data. In this physical juggling of encrypted data, it becomes virtually impossible to collect all the pieces to successfully crack.

In short, there are five (5) main components that would all need to be defeated to obtain data:

1) Existing, conventional polymorphic encryption with a random payload (the Pad);
2) That information sets sent at random time intervals with offsets;

3) Channels that are moving physically and/or virtually in the network in a way that is unpredictable;
4) Intentional disorder and misalignment of all aforementioned channels (entropy and ciphertext are not sent at the same time).
5) Decoy channels.

Taking all of these components together provides a would be perpetrator with not only greater complexity in cracking data, but an almost insurmountable problem of finding and aligning all the channels in the first place.

MTD - Moving Target Defense

Recently, some of the techniques used in STOP have been quantified by various groups involved in national cyber security and are being referred to as Moving Target Defense[3]. The technique was successfully used in the 2015-2016 DNC hack[4] of email messages but was used as a Moving Target Attack instead of defense[5] (or, better put, in defense of the attack).

Polymorphic Networking

The concept of Polymorphic Networking, a set of techniques defined by Moving Target Defense[6] (MTD), is a concept of moving around or changing the characteristics of a network connection to hide the data being transmitted.

Polymorphism is a concept in Computer Science where one thing or object can take on many forms. In polymorphic networking, this is exactly what is happening. In this system, a network connection can be viewed simply as a channel and can move or change over the lifetime of a network transmission. The system only sees “send” and “receive” and is unaware of the changes happening to the network itself.

This change can be physical and/or logical in nature. This hides the information being transmitted as there is no way of knowing where this information is in the network at any given time. The starting point is quickly changed and will never transmit valuable information across the network itself.

---

[3] "CSD-MTD | Homeland Security." https://www.dhs.gov/science-and-technology/csd-mtd. Accessed 28 Dec. 2016.
[4] "Bears in the Midst: Intrusion into the Democratic National ... - Crowdstrike." 15 Jun. 2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. Accessed 28 Dec. 2016.
[5] "Moving target defense vs. moving target attacks: The two faces of ...." 4 Jan. 2016, http://www.networkworld.com/article/3018881/tech-primers/moving-target-defense-vs-moving-target-attacks-the-two-faces-of-deception.html. Accessed 28 Dec. 2016.
[6] "CSD-MTD | Homeland Security." https://www.dhs.gov/science-and-technology/csd-mtd. Accessed 27 Dec. 2016.

For a simple example in an IP network, let's start with an SSH session on its given listen port of 22. A polymorphic approach may immediately hop to initiate a new connection on another port of let's say 12,304. The listen socket, which can be detected by a port scan, is never open that long. It is dropped immediately after the single connection is made in subsecond time. What this means is it's highly improbable, nearly impossible, for a port scan to detect this port, leaving the subsequent starting port hidden from detection. Even if one hop was detected, this hopping will continue to happen. To detect the specific communications channel after each switch makes the detection of an entire transmission more and more improbable.

The Polymorphic and MTD concepts are core parts of STOP patents. Introspective Networks is the inventor not only of these techniques, but also a working implementation making STOP likely the first secure Polymorphic Networking technique.

Polymorphic Encryption

Similar to Polymorphic Networking, Polymorphic Encryption is constantly changing some aspect of the encryption in a way that makes it increasingly more difficult to decipher. In the classic code definition, an algorithm is used to constantly change the encryption/decryption key so that it can not be easily guessed[7]. To do this, the key and decryption method must also always be changing. This can be handled by outputting the decryption as an ever changing OTP or having an algorithm both sides agree on that constantly rotates. There are also notions of Polymorphic Encryption Algorithm (PEA) for quantum computing[8] and Polymorphic Encryption and Pseudonymisation (PEP) which is used to distribute access to data without giving access to the actual holder of the data.[9] These are both interesting and the latter can easily be incorporated into the STOP stack but, for this conversation, we will deal specifically with Polymorphic Encryption which, at it's base, is the same definition provided for Polymorphic Networking: one code object that can take on many different characteristics without the user or system knowing or needing to know the changes to the implementation details. Moreover, what we will describe is very much in line with MTD principles in general as encryption also will become a moving target.

With this fundamental definition, Polymorphic Encryption can be as simple as changing the keys in a symmetric encryption scheme. It could also mean the changing of the underlying encryption cipher algorithm. For example, we may rotate our keys for AES256 periodically and then, without letting an eavesdropper know, switch to another strong symmetric algorithm like Blowfish[10]. By constantly changing keys and cipher algorithms, it becomes very difficult to

---

[7] "Polymorphic code - Wikipedia." https://en.wikipedia.org/wiki/Polymorphic_code. Accessed 28 Dec. 2016.
[8] "PEA: Polymorphic Encryption Algorithm based on quantum computation." http://openaccess.city.ac.uk/2509/. Accessed 28 Dec. 2016.
[9] "Polymorphic Encryption and Pseudonymisation for Personalised ...." 30 Sep. 2016, https://eprint.iacr.org/2016/411.pdf. Accessed 28 Dec. 2016.
[10] "Schneier on Security: The Blowfish Encryption Algorithm." https://www.schneier.com/academic/blowfish/. Accessed 4 Jan. 2017.

determine how to even start to decrypt discovered data. Even if data is captured, the key or the cipher algorithm are not easily discovered because this information is encrypted using an OTP. To make this work, transmitting the change in key and/or algorithm to the other side in secrecy is the critical step.

Research into Polymorphic Encryption will reveal many different implementation variants. While each one is Polymorphic in nature, they are all, including simply rotating keys, a form of Polymorphism[11]. In fact, an OTP system itself is Polymorphic by design simply based on the fact the key is always changing for the length of the data being sent. In a stream, it goes on until that stream is discontinued. Used to secure an entire network, it's ever changing and never predictably repeating until that network is no longer needed..

Putting the Pieces Together: How STOP Works

So, the question is, what makes STOP special? The most critical thing is, as of today, it is the only known MTD technique available that improves data encryption. That is accomplished by using, among other things, an OTP directly in the network and also using the network itself to provide MTD capabilities. It is the use of two or more channels that adds a time component on top of the spacial movement that makes the would be perpetrator not only have to get multiple parts in the right order, but also aligned to the exact bit.

One of the most crucial elements to make any MTD really work is starting with at least one streaming channel of directly uncrackable, encrypted data. This channel, on its own, provides a method for the two sides to communicate without fear that the messages can be intercepted and cracked. The only method known that is provably uncrackable by itself is an OTP. This channel not only contains the data to be transmitted, but all the messages that are required to make the MTD work in a deterministic manner without shared calculations on both ends of a data connection. This also comes into play during the first communication as the system is "primed" with two sets of Pads. This happens one time only at initiation. These sets of Pads lets the system connect the first time to a known port without fear that the data will be intercepted or cracked. This Pad needs to be large enough to encrypt the first port hop away from the well known port for Channel 0 and also share the key the Channel 0 symetric or asymetric encryption. Once Channel 0 is established, the process of sending Pad across the network starts and subsequent channels can be brought up using Pad to encrypt the data. This initial pad can also be large. This will increase the amount of time buffered before the system entropy is used to encrypt data. This makes the time dimension much more powerful because observers, even if they can record everything, will never know when the system entropy utilization starts.

[11] "Polymorphism (computer science) - Wikipedia." https://en.wikipedia.org/wiki/Polymorphism_(computer_science). Accessed 28 Dec. 2016.

To get this first Pad for priming the system to each side of the connection, a variety of techniques can be used. The easiest is to simply send it from a third system that brokers this exchange. Another method is manually priming each side holding the pads on removable media like a USB Stick or using Cyrptokeys. The two can be combined so that the manual method is used to prime the connection to the central broker system. In this scenario, the clients would only be primed once and then would receive subsequent priming pads from the centralized broker service that is already transmitting messages over a STOP enabled connection. A third method would be to put the priming pads in a message or reasonably secured remote file storage system but have an expiration for use. This method would send the priming pad directly in an email or store it in a cloud storage location. Again, this technique can be used with a centralized broker to prime that specific connection.

To protect the data further, we want to ensure it's difficult to find. We know for a fact that, without a compromise to the system on either end, using STOP there is no way this information can be directly recorded and later decrypted using the current state of the art. As we laid out earlier, the reason for this is the Polymorphic Networking that's been employed. Current "man in the middle" (MitM) recording methods require knowing not just the IP address, but, to understand what the data is related to, also the port to be recorded. Without these two pieces of information, there is no way to understand what the data stream is. STOP uses unknown ports so, for almost all network attacks including MitM, most DoS/DDoS and Injection attacks, there is no starting point for the perpetrator.

The question probably being contemplated is, how does one get truly random entropy for the Pad and random number generation? The answer to that is simple and all around you. Taking any measurement from the analog world and measuring it to a high enough fidelity produces random, unpredictable fluctuations in readings. For example, the ambient temperature of any area, enclosed or otherwise, measured to a Pico reading or 10^{-12}, even in an extremely controlled environment, is going to be fluctuating wildly in an unpredictable manner. Many other measurements taken to a similar level of fidelity, such as a voltage measurement or the reading from a gyroscope or accelerometer will produce similar results. The key to using analog sources is to ensure you have a measurement capability to handle the desired level of fidelity where readings start to enter entropy. Before moving forward, to ensure the high fidelity of readings, a test should be performed that takes in a large sample set of data from the source of entropy and validates that the readings have good, valid number frequency across all possibilities within the desired numeric range being captured. This is a critical step in validating the measurement source is providing real, accurate high fidelity readings and not providing some kind of approximation with a limited numeric set.

Taking this concept to the next level, several high fidelity, analog entropy readings can be combined using binary operators to further ensure that someone cannot guess one analog source or the other. This ensures the most secure Pad possible making a true OTP system actually live up to its mathematical proof.

Now that we have viable Pad, we need a way of transmitting that pad from the sender to the receiver in a reliable manner. This is where Introspective Networks STOP's seminal network Cyber MTD inventions really starts to take shape. STOP can use both Polymorphic Networking and Polymorphic Encryption to provide secure key transmission that transcends simple symetric or asymetric encryption itself. That said, if we think about how brute force attacks are conducted, if our keys are not compromised and we send nothing but non-repeating entropy across that channel, it would still be impervious to brute force techniques because, as we discussed in the introduction, the underlying data can never be guessed. For brute force to work, you have to know something about the data being sent at a given point in time. In the case of sending entropy derived from the analog world that never has two repeating bytes, brute force techniques, very logically, become impossible. Even with all that, it is better to leave nothing to chance and, using Polymorphic Networking and Encryption, add MTD to the security provided by STOP.

Another concept we've mentioned that might be worth explaining is how does this work in Time and Space. Space should be obvious as we are moving the channels in physical or virtual space as it relates to the network(s) used. The time dimension is another story altogether. This is done by sending data at different intervals. In the simplest implementation, only two channels are used: 1) for the OTP stream and 2) containing ciphertext. The time dimension comes into play as the OTP channel will be cached on the far end so, the key stream needed to decrypt the data is never sent at the same time as the data itself. If we were to have more than two channels, subsequent channels used for encryption would have a completely new OTP stream. This stream would be encrypted with the prior OTP stream. What this adds is more complexity to the variables in the time and space dimensions. Caching, if able to stay consistently ahead of data decryption needs, can have random temporal offsets to create further randomness in the timing. We also account for possible decoy streams that have nothing to do with anything but add noise and complexity to both the time and space aspects of STOP. Figure 4 shows how this data is sent across the network. With a little imagination, you can depict how each of these streams could be sent at vastly different times.

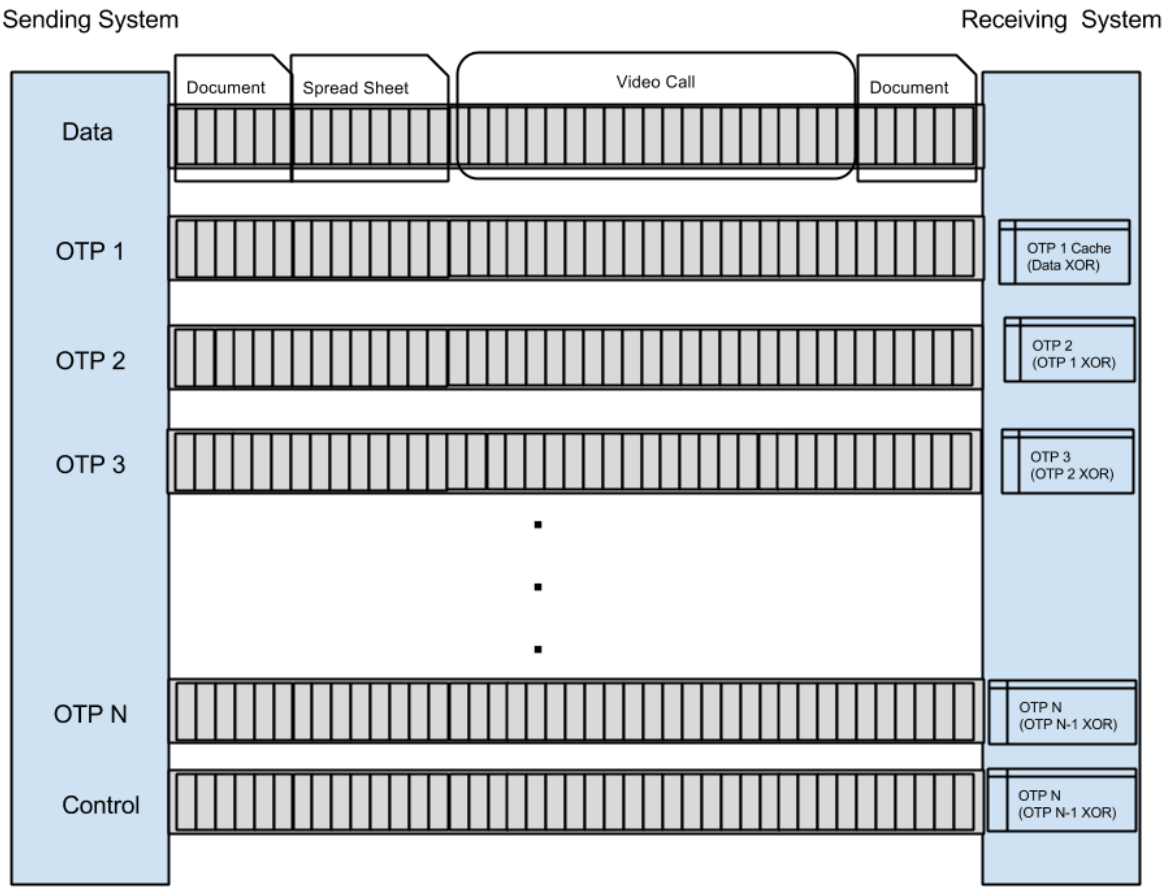

Figure 4 - OTP caching example diagram. For channels, the numbers are the inverse of the OTP numbering and zero based. So, the Control with OTP N is actually Channel 0. The real thing to take away from this is the OTP can and must be cached ahead of the data channel. This caching can be done at any time and should have a randomness to it. The key is to have the network speed to stay well ahead of the data itself.

Figure 5 provides a further example of how this rotation works with multiple ports. This figure emphasizes the rotation which, as we've discussed, also can contain a random time component along with its inherent space movement.

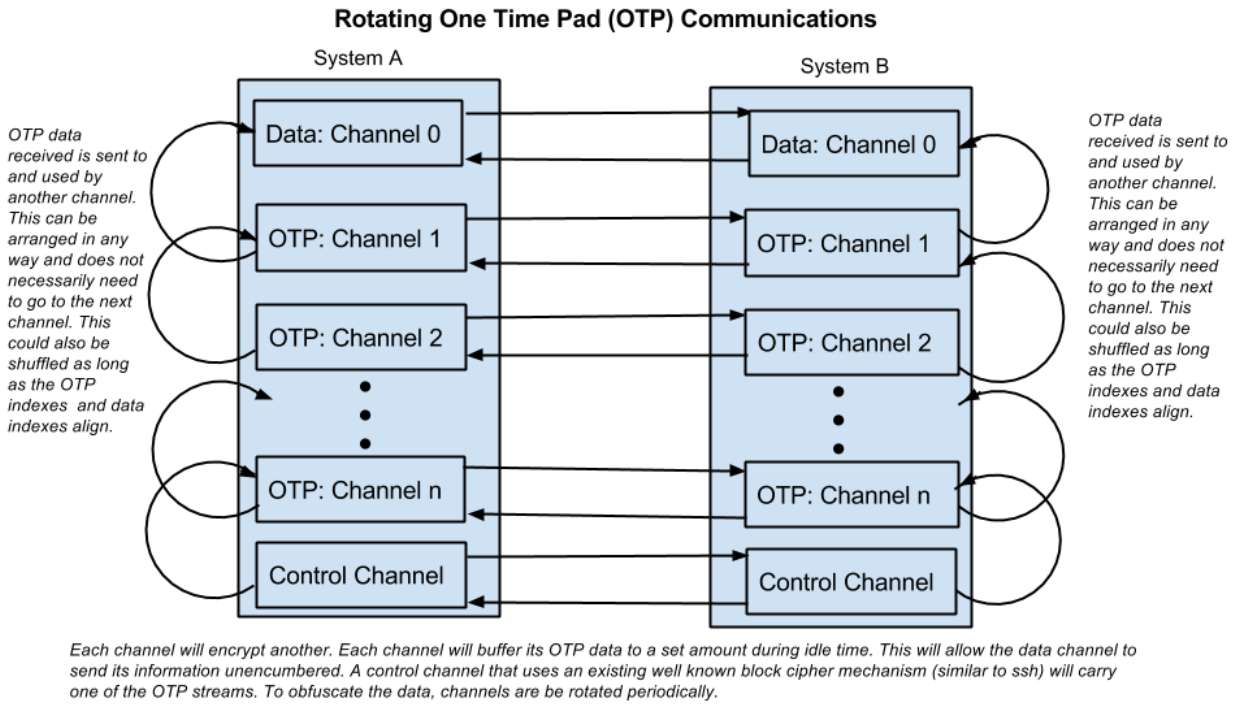

Figure 5 - Rotating One Time Pad Communications

The last and final thing that truly separates STOP from all other forms of communication/data encryption and obfuscation is all system MTD changes are deterministic. There are no calculations on either end to guess or crack. Data is moved, as we've discussed, in both space (across the network) and time (pertaining to the frequency of these changes) in a random manner that, while it may be bound, cannot be guessed with any certainty. The bound set of possibilities is too large to make discovery practical. This determinism can only be performed if the messages are guaranteed to be secure which is made possible by analog sources of entropy and following all the rules of the OTP.

Appendix A - STOP Applicability Examples

There are numerous requirements for secure communications in the military that STOP technology could meet or assist in meeting. This section will highlight some of those potential candidate requirements.

BlockChain

Block Chain is a technology that is quickly being seen as a way to track and record transactions. This technology can service a number of industries including Manufacturing, IoT and Logistics. Used for these purposes, it becomes the glue in modern supply chain management. It also takes on a “Triple A” security role with accounting taking on a larger role with the BlockChain Ledger. The issue is, as we have seen with BitCoin heists, BlockChain systems on a public or shared network infrastructure is only secured by encryption that is likely crackable by the right entities and, with Quantum Computing looming, soon to be anyone able to afford Quantum Computing resources. The other issue is, if you want to disrupt the system, what’s to stop Injection, DoS or Message based (bad blocks) attacks? There is also the problem of securing the ledger which, by design, is relatively open and exposed.

To fix this issue, STOP can be employed either across a VPN or embedded directly in the BlockChain system. In short, the BlockChain becomes a closed system on an open network. This provides all the goodness of a shared resource across a shared network with the security of a private line network.

The Cloud

Cloud computing is pervasive and the economy of scale derived from it outweighs security concerns. For critical, secure usage though, Cloud resources by themselves are not even remotely secure. They run into the same issues as described in BlockChain.

STOP can be embedded directly into Cloud processes providing a very secure, no touch method for securing data from the client back to the cloud service. Network attack vectors evaporate and the mechanics of STOP are even hidden from system administrators.

Additive Manufacturing

The latest market change starting to take shape is Additive Manufacturing. This is where parts are ordered from a 3-D printer and manufactured as needed, where they are needed. This radically changes supply chain logistics speeding up delivery and removing shipping and other related handling costs. This, like most other systems, relies on an open network to connecting people to the printer.

The issue with this newfound convenience is the potential for industrial sabotage. What if someone changes the way the part is built? What if a competitor, a rogue state, or other adversary wants a critical system to fail? To mitigate those issues, we need STOP creating a closed system on an open network. This will stop network borne attacks that may allow things to be maladjusted remotely. STOP will provide that same level of protection as it does for other, similar network services.

The Internet of Things (IoT)

IoT is likely the most exposed and vulnerable new technology on the Internet. We saw first hand in 2016 how these devices can be co-opted to participate in massive Distributed Denial of Service attacks. Moreover, packet injection, URL spoofing and IP spoofing can all be used to create fake data. This data does not have to be real; it simply has to cause errors to disable or degrade IoT elements and systems. STOP prevents all these issues and allows private, hidden networks to be created across the public Internet and shared networks alike. The devices communicating in a STOP network are not only secure - perpetrators can not even validate they exist.

Securing Communications From Private Devices

There are often times when senior leaders or small operational teams may be in locations where unsecured, private devices are the only reliable method of communications. As a currently available fee-based application for any iOS or Android capable device, STOP applied to secure chat communications, can immediately meet this requirement. Appropriate senior leaders or operational members can download and secure SMS-like chat communications to other similar personnel or to their home headquarters; using either similar mobile devices or the chrome-browser configuration of the application on a government workstation (laptop or desktop). This is the simplest initial application of STOP technology to secure sensitive communications.

Truly Secure VPN

Utilizing STOP technology as applied to the security of VPN communications will provide greater protection to current attack vectors applied to these types of communications. Our testing and assessment of STOP security will confirm that it provides an improvement over prevalent current methodologies to secure VPN solutions. The ability to eradicate MiTM attack vectors and obfuscate packet streams from adversaries attempting to compromise VPN communications will add greater security to these important methods of securing the extensive applications protected by VPN today.

Appendix B - STOP Usages

STOP MTD network protection technology has many usages and can also be implemented in many ways. While it can be embedded directly in applications, likely providing the highest level of protection, it can also be implemented in more generic ways to provide network level defense at a port or edge device level.

STOP For Point to Point

Point to Point protection will provide security between two computers - say a workstation and a server, two or more databases for secure replication or between a site and a cloud service . This can also create a tunnel between two systems, a STOP enabled shell or maybe even a bridge/gateway between networks. There are many usages for Point to Point connectivity and adding STOP security will remove the MiTM relay and injection attacks and also hide information from all conventional means of discovering a VPN tunnel. Figure 6 shows an example of a point to point setup between two devices.

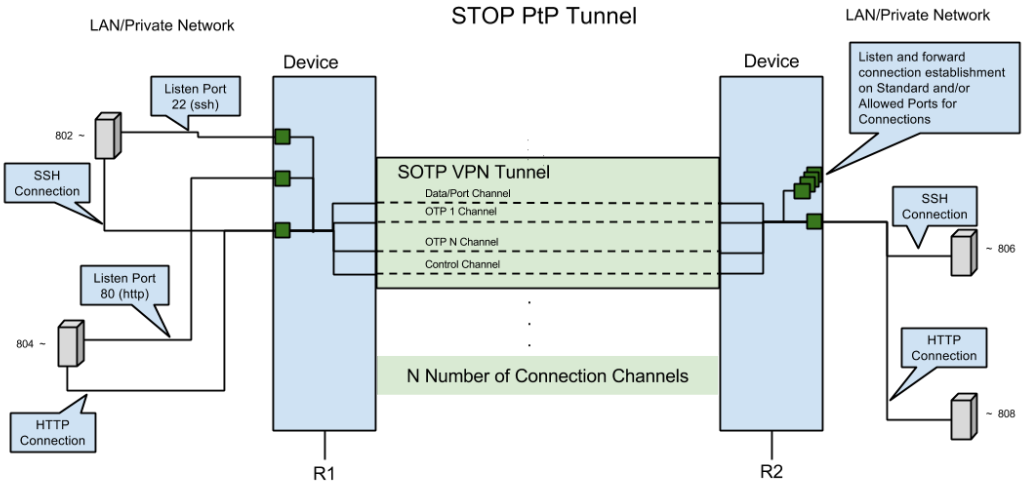

Figure 6: This shows a point to point tunnel using STOP. This behaves like a normal Point to Point VPN tunnel masking the fact that STOP even exists. Networking applications are none the wiser that they are using STOP behind the scenes. More importantly, network traffic is completely hidden from the network itself. In this case, you can send something across the public Internet and there would be no indications where the traffic is.

Applications for this kind of tunnel include bridging networks, private communications channel between systems and, probably of most interest, backhauling data to cloud service providers. This last usage is the final piece needed to bring the cloud to larger enterprises as well as military and government services. It's the security of the communications and the prohibitive cost of private line backhaul that is preventing these final entities embracing cloud solutions.

STOP VPN

Right now, AES256 is or likely will be soon rendered irrelevant by quantum computing or some other technology like massive graphic processing unit (GPU - vector processing[12]) or field-programmable gate arrays (FPGA[13]) clusters. This will leave a large number of networks protected by VPNs exposed. STOP VPN provides an efficient way to protect an entire network of systems quickly and easily. The end users are completely unaware STOP is present. The network behaves exactly like it does today and STOP technology is executed behind the scenes. This means STOP becomes a drop-in solution to replace current VPN solutions.

Moreover, the configuration for a STOP VPN is much lower. For low risk setups like a small business, priming can be automated over the web. Once implemented, MTD renders the VPN nearly invisible with regards to purpose.

STOP VPN can also be embedded in edge systems including firewalls and NFV[14] enabled network elements. This allows full control over the STOP VPN implementation and is more suited to large operations where full control is desired.

STOP for Communications

Introspective Networks has developed an entire suite of STOP tools that specifically deal with communications. Currently, there is a Messaging client with File Transfer soon to follow. STOP can also be applied to voice, video and radio communications. STOP makes a great drop-in replacement for frequency hopping over radio frequencies. As mentioned, because STOP is deterministic, there is no algorithm to predict. Also, crypto keys become a thing of the past as true entropy is used in the network in a way that makes it as close to impossible to penetrate as is currently feasible.

STOP Embedded in Applications

When embedding STOP in an application at a software source level, you get two or more applications that can only talk to each other. This locks down communications directly at the app. While this definitely requires the most work for both development and application installation, this is by far the most secure and restrictive way to run STOP.

---

[12] "Graphics processing unit - Wikipedia." https://en.wikipedia.org/wiki/Graphics_processing_unit. Accessed 10 Jan. 2017.
[13] "Field-programmable gate array - Wikipedia." https://en.wikipedia.org/wiki/Field-programmable_gate_array. Accessed 10 Jan. 2017.
[14] "What's Network Functions Virtualization (NFV)? - SDxCentral." https://www.sdxcentral.com/nfv/definitions/whats-network-functions-virtualization-nfv/. Accessed 10 Jan. 2017.

Appendix C - Acronyms

AES	Advanced Encryption Standard
CPU	Central Processing Unit
DDos	Distributed Denial of Service
DNC	Democratic National Committee
DoS	Denial of Service
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standards
FPGA	Field-Programming Gate Arrays
GPU	Graphic Processing Unit
IP	Internet Protocol
MitM	Man in the Middle
MTD	Moving Target Defense
NFV	Network Function Virtualization
NSA	National Security Agency
OTP	One Time Pad
P2P	Point to Point
PEA	Polymorphic Encryption Algorithm
PEP	Polymorphic Encryption Pseudonymisation
SSH	Secure Shell
STOP	Streaming Transmission One-time-pad Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

Appendix D - Intellectual Property

Introspective Networks holds several granted patents, along with other patents pending, related to STOP technology. Patents granted as of this writing are:

US9,584,313 - Streaming one time pad cipher using rotating ports for data encryption
US9,584,488 - Data encryption cipher using rotating ports
US8,995,652 - Streaming one time pad cipher using rotating ports for data encryption
US9,569,289 - Generic distributed processing for multi-agent systems
US9,378,070 - Generic distributed processing unit for multi-agent systems
US8,898,218 - Generic distributed processing for multi-agent systems