Whitenoise Telecom Pilot – IPSec/IPv6/WN – LDAP/CAS - SIMs

Telecom pilot scope and options

The telecom densification program

The telecom is currently well embarked upon its densification program which is targeting the addition of tens of thousands of cells with the specific goal of increasing speeds and quality of experience by using different bandwidths and aggregating them together.

We demonstrated our technology for them at the Telecom Council of Silicon Valley Showcase.

The telecom is “looking for new, disruptive players that bring a new thinking about how to architect networks."

Whitenoise Dynamic Distributed Key Infrastructures and the characteristics of Whitenoise bit independent keys provide a rational and simple way of scaling a secure infrastructure while achieving the goal of maximizing speeds.

Whitenoise can operate at top speed in any spectrum or context because it is as fast in software as it is in hardware, because keys can be parsed and operate in multiple spectrums simultaneously, and because it is the only security technology that creates a virtual secure framework without adding any appreciable overhead.

Deploying Whitenoise technologies and absorbing the new cells into that the telecom network is simply adding an additional tier to Dynamic Distributed Key Infrastructures that would utilize “link keys” that only need to be delivered once to identify their server and which enables secure communications between disparate cell and network servers.

Each cell or network will in turn act as a Key Vault and GateKeeper for their network and cells. Distributed key vaults also mean that all the eggs are not in one basket and that a cascading and complete breach of a secure network is not possible.

Background for Telecom/Whitenoise pilot

Currently security is a cost driver for telecoms. Telecoms have little choice but to use asymmetric RSA style technologies to provide a baseline level of security for their core and their clients which keeps them in compliance but which they also know is not only not 100% effective but continues to drive additional unrecoverable costs for the telecom. A myriad of additional security services and layers are required by the carriers, service providers and their clients alike to try to plug the fatal flaws of asymmetric security and minimize the escalating costs that result from cyber security failures.

An example of costs that result from asymmetric security includes centers that are heavily staffed that exist to try to identify inappropriate access and use of networks. And this detection can't be done in real time or instantly because of asymmetric technology algorithmic and architectural framework limitations. By the time Visa calls you in Los Angeles to see if you are in Prague where the card number has been used, the damage has already been done. Whitenoise technologies applied to those kind of financial transactions would prevent that scenario in the first place because, as the pilot will demonstrate, perfect identity and dynamic one-time-pad authentication, intrusion detection and automatic account revocation at the point of network access and throughout a session is inherent without human intervention.

Another interesting example of unanticipated costs and headaches is the spreading legislation requiring Google to eliminate internet footprints of persons and corporations who have used their service and request it. Using Whitenoise technologies for data provenance simplifies the search and scrubbing effort required to locate those footprints for compelled removal.

The telecoms need to protect their own networks and can protect the consumers it is servicing – and make a profit.

Security can be a ***protectable competitive advantage*** with Whitenoise patented technologies. Corporate and individual consumers worldwide spend enormous amounts of money for security that is inconvenient and less than 100% effective. They will not begrudge spending dollars instead on services that are simple and that work. They are already spending dearly on services that don't.

This is a significant revenue opportunity for telecoms that previously assumed a more limited role on security. Carriers have historically acted only as pipes and responsibility for security passed to their clients and service providers that rely on their backbone.

New legislation is changing that role. New technologies allow you to profitably empower your customers.

DoCoMo has proven that telecoms can monetize security by generating 25% of their profits on self-running, third party authentication services. They are providing the connection anyway. It is no additional effort.

You can easily add security services, provision them from the web and bill them out to your clients on a per-device, monthly basis along with your regular billing for ongoing annuitized revenue streams.

Currently the security market target tends to be B2B (except for antivirus applications and registry checkers). And generally it is vendors like EMC2/RSA, VeriSign, Intel and Cisco making the lion's share of the profits from security services and offerings based on obsolete cryptography.

You can turn security into a profit center since it is now possible to easily sell and configure security services remotely, virtually and directly without using vendors and other intermediaries.

Cyber security problems and risk are now tangible and painful for both service providers (and their decision makers) and their clients alike.

Cyber is high stakes and it is not a game.

Einstein's definition of insanity is appropriate for the prevalent approach to network and cyber security**: "Insanity – trying the same thing a thousand times and expecting a different result."**

What's the problem?

We have to become proactive on cyber security. We have to learn how to ask the correct questions when it comes to security so that we can choose solutions that actually work.

Last year Symantec announced all major US banks had been breached a year after they had already been compromised. 21 million records were stolen across all US government departments and the malware likely resided in those computers for a decade.

Recently it was announced 1 billion Android phones had been breached (or could be breached.)

That raises only two possibilities if we ask the right questions:

Why did it take a billion potentially compromised phones to discover the breach if heuristic, behavioral mapping and data analytic intrusion detection approaches are working?

If it is only a possible attack on the Stagefright utility then was the effort spent to find and create another possible problem, make a marketing announcement and then scare the market into action to use technologies that are probabilistic at best? That would be like releasing a virus to sell a solution?

Other recent cyber failures include:

- The US Joint Chiefs of Staff had been breached (likely by Russia).
- An airline had its flights grounded because of hackers. This is a chilling reminder that our enemies (both corporate competitors and nation states) and terrorists can do such things remotely with relative immunity.
- And, the US government announced in recent weeks that the Snowden files had been decrypted, presumably without keys, and Britain and the US began bringing foreign assets home for safety reasons.

The main problem is that we fail to address the main problem.

Security in networks and communications is a cryptographic issue. Anything that is not a cryptographic solution will never provide 100% security.

If we fail to address the underlying flaws in key strengths, asymmetric framework flaws, key exchange vulnerabilities, identity and data provenance than we will forever be adding layers on

top of the same problem and not solving it. Flawed solutions actually add more points of egress for mischief.

Currently markets are enamored with heuristics, behavioral modeling, big data analytics and a host of limited range solutions. While they can be useful for information gathering it means that the problem has already entered your phone, mobile, or network. They can never be 100% accurate.

Those are reactionary solutions and not proactive. The problem has already manifested itself.

The Solution

Whitenoise technologies prevent the vulnerability before it happens. There is no access to the network or device without proper identification and authentication of a user or device with unbreakable keys.

The use of keys in security is an objective approach. There is no guessing or probabilities. The keys are breakable or not. The keys can be delivered safely or not. The keys can be safely managed or not.

Whitenoise technologies are like pregnancy. A woman is pregnant or not. Whitenoise keys are synchronized or not.

If Whitenoise keys are not present to identify a user or data with constant, continuous, dynamic DIVA calls then there is never access to the network or device by criminals in the first place.

"Everything Should Be Made as Simple as Possible, But Not Simpler" *Albert Einstein*

And now we can be proactive without having to remove or change any existing security controls for seamless upgrading and transition. The fatal flaws of current asymmetric security protocols are fixed and the good parts of these frameworks are leveraged. There are no compliance issues (just regulatory export controls and permitting since Whitenoise technologies are national security level cryptography).

Pilot Goals

- We will satisfy the specific carrier's needs first.
- We will offer a pilot platform as a third party service that keeps the pilot away from the sponsor's core network but will still allow them visibility and control for a completely risk free evaluative process.
- We will implement, demonstrate and prove that Dynamic Distributed Key Infrastructure virtual frameworks are easily scalable and interoperable

- Implementation will be accomplished through a web based IPSec/IPv6 driver upgrade.

- In light of the July 8, 2015 shut down of the New York Stock Exchange and United Airlines, both the largest players in their specific critical infrastructures (finance and air transportation) we will also optionally pilot an implementation deploying an upgrade to Microsoft's Lightweight Director Access Protocol and Central Authentication Service (CAS) simultaneously to address problems inherent in Certificate Authorities.

- Pilot participants will be able to choose to upgrade either or both services through a secure web based process for their endpoint devices.

- We will construct the pilot in a manner that objective information and freely available information is available for analytics. This will facilitate informed decision making on strategies and how to market security as a protectable competitive advantage. The carrier sponsoring a pilot will tell us information that would be useful for them. This information will come from endpoints from your network that you want to participate. It will also include information about competitor networks and carriers that cannot prevent their subscribers from voluntary participation in the pilot. Tap into Google Analytics as well.

  This will allow **data analytics** based on perfect endpoint identity and data provenance with mining focused on information that will support future informed decision making for the monetization and prioritization of secure services. It will also identify appropriate target markets, their location and their particular vulnerabilities.

- We want to roll out the identical pilot for the rest of the telecoms and major service providers.

"If you are able to do it for us you will have done it for all telecoms." **Lyle Paczkowski**

It has been recognized that if we were able to implement Whitenoise technologies into the top 30 global telecoms that we will have enabled secure communications for at least 90% of the world. Everyone deserves security. Societies need it. You will see that security is a protectable competitive advantage with Whitenoise technologies. You will also experience how balancing security and privacy is simplified.

Scaling through telecoms is easily the simplest and most cost efficient channel for implementing a virtual framework with an unbreakable protocol to enable the online distribution of secure services and controls. Telecoms are a difficult but small target market universe. But because of their scale and reach, their adoption simplifies the harmonization of this virtual secure framework globally. Since networks are upgrading to IPv6 it is one of the logical places to piggy back.

This carrier channel also has various licensing/sublicensing opportunities where they can monopolize the use of Whitenoise technologies on a geographical basis and verticals basis since Whitenoise technologies are patented globally in countries with two thirds of the world's

population, economic activity and manufacturing. In this context exclusive licensers can sublicense even to their competitors and make revenue off their efforts.

We have the ability to identify which telecom is being used by a client (or end point) that has upgraded their IPv4 driver to the IPSec/IPv6/Whitenoise driver. This information can be gathered during enrollment, key distribution, authentication and activation or by other follow-up techniques targeted to an email address from their enrollment. Just getting their IP address which is benign and available will allow us to determine whether they are on ATT, Verizon, T-Mobile, Bell, Shaw, TELUS etc.

Regular commercial consumers from competitive carriers are demonstrating a lack of faith in the security of their carrier service provider by joining the pilot or competitive service in the first place. Properly constructed, and without violating any privacy issues, there is a lot of information that can be easily mined and used in marketing and decision making.

Our goal is really the one-time key distribution that will immediately provide identity, data provenance, secure network access, continuous dynamic one-time-pad authentication, inherent intrusion detection and revocation. This thwarts unauthorized network access and network use.

Once the single, unique, private, secret, identity management key is securely distributed, that device/client is able to purchase/access any additional secure services (i.e. streaming, file transfer, secure storage, secure data format translation, funds transfer and mobile payments, etc.) in the future without any further key distribution.

Pilot implementation, choices and time line

The pilot is targeted to selected or interested endpoints that need to upgrade to IPv6 compliance with an IPSec/IPv6/Whitenoise driver that will also deliver a Whitenoise Identity Management Key. Existing IPv6 enabled endpoints are do a routine maintenance driver upgrade.

We will enroll the telecom's participating devices online through a web page for the driver upgrade by a standard web based installer. *(Note: it is a logical technique for viral scaling by piggy backing on the upgrade process of other utilities.)* The sponsor telecom will have full access to the pilot host site for complete oversight and administration to the degree that they choose.

This pilot can also allow enrollment of competitor clients and devices for analytic purposes if the sponsor so desires.

Whitenoise and a sponsor-chosen-host site will manage the pilot, key management and distribution, logging of network use, and performing the continuous, dynamic one-time-pad authentication calls during a network session as a "Trusted Third Party".

The telecom pilot sponsor will identify their client devices that they want enrolled in the Pilot.

We will log all network use by these endpoints and generate ongoing statistics that will be useful to the pilot sponsor as a snapshot of their network security health.

Possible host sites:

- Sponsor telecom's own beta site
- Whitenoise Labs
- University of Victoria ECE
- The Group for Advanced Information Technology labs at the British Columbia Institute of Technology
- Tata Innovation Labs in Ohio

Possible consulting assistance on monetization of Whitenoise for telecoms

- MIT / CTA
- Tata Consultancy Services

Sponsor-chosen target pilot platforms, devices and contexts

- Android
- Windows
- iOS
- smart phones
- tablets
- desktops
- routers
- Internet of Things components
- sensors

Information available and used during the pilot

The telecom sponsor will determine which demographics, identifiers and network events they would like us to log for authentication, protection and analytics purposes. For example,

- IPv4 and IPv6 addresses
- Operating systems (this will also identify LDAP and CAS users for a pilot option)
- Carrier
- Location
- Unique device identifiers UID
    - MAC numbers
    - NAMs
    - Branded UIDs
    - Manufacturer numbers
    - Serial number
- Unauthorized access attempts

Note – this pilot will provide an IPv6 driver upgrade with an identity enabling application that will monitor identity and provide inherent intrusion detection and revocation against unauthorized network access attempts.

This pilot can also provide an LDAP/CAS upgrade with an identity enabling application that will monitor identity and provide inherent intrusion detection and revocation against unauthorized network access attempts. It will also protect against other vulnerabilities in Microsoft OS and applications using LDAP, CAS and certificate authorities.

As future services are tested, information acquired will be context specific and chosen based on the pilot sponsor's needs. For instance, in a subsequent phase an email filter can be provided that will only allow communications with a valid Whitenoise key (keyMail) to be delivered. All other emails will be stopped and can be quarantined. In that context we could collect information on the purveyors of malware and their locations.

The pilot leverages needed IPv6 upgrading as a viral approach to distributing Whitenoise keys and rapidly scaling secure, virtual network frameworks. The secure keyMail service suggested above provides another. A user of secure keyMail can rapidly increase their trusted circle and facilitate their enrollment and receipt of a one-time-delivered key.

If someone unknown tries to communicate with someone on secure keyMail they will be given the option of getting a Whitenoise identity management key. If they are legitimate there are various levels of identity proofing that can be used to bring legitimate (previously unknowns) into the secure network.

And, the LDAP/CAS upgrade provides yet another option for virtual and viral scaling for Microsoft service dependent applications.

Participating devices or components in any context only require connectivity, a tiny bit of storage space, and write-back capacity to track dynamic offsets.

Pilot Preparation Time Estimate

The pilot could be active in two months but we recommend 3-4 months so that the sponsor can provide input on their preferred configuration of the pilot that fits with their current Best Practices and goals. As well, an independent penetration test will be conducted by Deloitte prior to augment our collective penetration testing prior to the specific pilot launch.

Configuration and implementation choices

The pilot will provide a web based installer to upgrade IPv4 to IPv6 and to install a Whitenoise identity management key and the small endpoint application that will respond to the continuous, dynamic, one-time-pad DIVA authentication calls from the authentication server. The server will also be a key vault and manage, distribute, and resolve keys.

There will be separate platform installers for Android, Windows, and iOS devices.

The telecom sponsor will have access to a web based administrative dashboard similar to that seen in a file transfer application: http://sfi.wnlabs.com/help. This also shows a future premium service capability.

The telecom sponsor will be able to choose which authentication factors they want utilized for access to their network along with the DIVA authentication calls from the secure session manager.

For the purposes of the pilot we will leverage existing technologies for simplicity.

The IPSec/IPv6/Whitenoise driver upgrade **will use the currently prevalent SSL** for the distribution of the IPSec/IPv6/Whitenoise upgrade package.

Note: although we know that SSL is not completely secure it is the current standard. Thankfully, we can test for man-in-the-middle and DIVA requires synchronicity. Any unauthorized use will be detected and locked up regardless.

The pilot framework will be constructed in a virtual fashion similar for encrypted point-to-point tunneling utilizing Gatekeepers and a KeyVault. The pilot server will act as a KeyVault, third party endpoint authenticator, and will resolve the keys and offsets whether permanent private keys or server generated session keys are used for the chosen functions to be configured.

The key resides on endpoint device in an encrypted state

** Beyond the scope of this pilot, a long term goal will be hardware identity and trust implemented via tamper resistant chips or PICS during manufacturing of smart components. This will prevent any hackers from access to all key material required but will still allow rapid upgrading and customization by firmware.*

In this driver context, the endpoint, unique, private, secret key will live on the device file system. It could be compromised if someone steals the device (which can be deactivated), has physical access to the machine, can gain access to the machine remotely, or captures the key during key transfer in a man-in-the-middle context.
Man-in-the-middle attacks exploit the fundamental weakness of prevalent approaches. But, with DIVA, if a machine was physically compromised like this, the key will go out of sync with its relevant endpoints upon use, intrusion will be detected at that point, and network access will be revoked. The system administrator also has a definitive forensic universe.

Additional key security is provided by storing both the key and the current dynamic offsets in an encrypted state, in separate network locations. They are encrypted in storage with different distributed keys where possible (i.e. server).

For highest tier security, the keys should be physically installed on the machine in person, but initial key download on the fly is supported because as this pilot scenario will show the requisite offsets server-side are stored encrypted with the server Master Key which has been physically installed and which is NEVER transmitted…. period.

The installation package will install the driver and set it up for all of the devices IPv6 network interfaces.

There will also be the ability to monitor the driver status so appropriate authentication factors can be seen.

There will also be the ability to uninstall the utility.

Addendums

Background of the IPv6 problem

Problem – The internet ran out of unique addresses which are fundamental to directing all communications.

Solution - Using IPSec we can implement a unique WN identity management key with IPSec/IPv6 addresses and the internet infrastructure would never run out of unique addresses until the end of time. And everything would be able to use any Whitenoise Security as a Service capability because the single unique key has been safely delivered the one time. At any time in the future that device can be enrolled, authenticated, charged and activated for various security capabilities.

More importantly, our key is distributed with the IPSec/IPv6 driver one time as part of the overall system upgrade. Identification of every single endpoint and enrollment into secure networks thereafter becomes naturally viral and yet benign. Legitimate users and endpoints identifying themselves are then on the inside – criminals are on the outside.

IPSec/IPv6/ Whitenoise pilot proposal for the telecom

IPSec is a specification that supports IPv4 and IPv6. It is the security extension that allows for authentication and confidentiality. It's designed to support new crypto standards as they appear.

See:

- https://tools.ietf.org/html/rfc7321

- https://en.wikipedia.org/wiki/IPsec

- https://en.wikipedia.org/wiki/IPv6#Network-layer_security

The telecom/WN pilot will implement Dynamic Identity Verification and Authentication (DIVA) in an IPv6/IPSec driver context with pre-shared key(s) tied to each installation/device. These are then used to resolve more keys as needed. Windows, Linux/Android, and iOS/OSX are the main platforms we want to create driver support for in order to encapsulate most desktop/server/and mobile devices and components in the market.

In the future, this starting point can be extended to provide confidentiality through encryption and various other secure network services because the single key has been distributed. Initially the DIVA offset and one-time-pad tokens will be used for authentication and intrusion detection.

This approach is the most cost effective way to actually deploy a network security layer in an existing ecosystem with minimal or no hardware changes.

Note: to avoid hardware changes

- It is possible that your network infrastructure may not be 100% IPv6 compliant so potentially the telecom would need to update infrastructure that is IPv4 only. This could be done with the pilot.

- There may be instances where bottlenecked services would have to be upgraded for performance reasons.

- At this point, problematic areas will simply be avoided in the pilot and would be a point of planning consideration after a successful pilot.

Simply using the IPv6 Auth header MIGHT be enough: https://tools.ietf.org/html/rfc4302 .

Whether IPSec is required will depend on your specific requirements.

Hardware/firmware implications

We are aware that hardware based identity and trust are a particular area of interest. There are different ways to approach this.

One of the most secure approaches is deploying keys from tamper resistant chips and microprocessors. This is forward looking and presumes distribution of identity in part during the manufacturing process with a physical chip component.

The preferred method for the pilot and general scaling of secure networks to include legacy devices and components is using a software solution the binds identity to a device by means of unique device identifiers (and biometrics where applicable). This can be applied to different components and areas that have connectivity, a minute amount of storage for the key structure, and write-back capacity to track current dynamic offsets that are used in the one time pad authentication protocol of Dynamic Identity Verification and Authentication (DIVA).

Key distribution security and storage implications

For perfect security in key transfer, key setup and key use in a distributed key system at least one key, the Master Key is physically provisioned at system installation.

The keys in play are:

The host pilot service provider Master Key can make an infinite number of keys for the clients and network endpoints. The master key can be used to create session keys where needed or desired. And the master key can be used to encrypt the offsets in storage.

By using the physically distributed master key to encrypt the dynamic offsets in storage and encrypting the private key with the application key with SSL transfer for this pilot, the hacker will never have access to both keys and the required offsets which are stored in different network locations encrypted with different keys.

An application key is compiled in the end-user application that participates in the continuous, dynamic one-time pad authentication calls and is compiled in an endpoint executable, dll or driver.

The unique private, endpoint secret key is distributed along with an IPSec/IPv6 driver (even compiled into it), and the DIVA application over SSL. In the future other delivery techniques can be used to increase security even more.

The endpoint private key resides in an encrypted state on the device and at the server. Key materials are never moved in an unencrypted state.

- In majority of hacking contexts the hacker does not have the device and therefore does not have, or is not realistically going to have, the specific device identifiers that are associated with the encrypted key and need to be known for the compiled application key to decrypt the resident encrypted private key for use.

- While we have to assume that getting access to the application is not difficult accessing the application key by decompiling or reverse engineering adds an additional challenge layer.

Offset

The offset(s) is stored in a different location to keep it separate from the key structure and can be encrypted itself with a different key. Ideally the service provider master key is used for this. The master key HAS been delivered the one time at system setup physically and is never transferred otherwise.

- Additionally, any chance of stealing a key externally or internally would require circumventing or beating security layers in at least two separate areas. Accessing these areas internally require a minimum of two separate system administrators by design.

LDAP and CAS optional pilot addition

Yesterday, (July 8, 2015) the New York Stock Exchange, United Airlines and the Wall Street Journal were shut down for many hours. The NYSE and United Airlines both are the largest players in their critical infrastructures: finance and airline transportation.

The government is mum on the cause of yesterday's service outages even though recently they announced the Snowden tapes have been decrypted (apparently without keys). They announced complete breach of every single US government department.

Many will think yesterday's failure must be a significantly graver threat to our systems and national security exactly because no one is providing meaningful information.

If this outage occurred as NYSE claims because of software upgrade errors affecting time stamps from trading software then is it just coincidence that United Airlines and the Wall Street Journal went down at the exact same time?

How much revenue was lost with NYSE shutting down for hours in the middle of a trading day?

How much cost did United Airlines absorb yesterday with 800 delayed flights as has been reported?

Anonymous claimed it would happen before it happened.

How are these related?

The next day, (July 9, 2015), a military contractor requested a fix for Microsoft Certificate Authorities.

We have always considered the failure of certificate authorities. Public keys are always available and public keys can be factored. The government announcement of the Snowden files apparently being decrypted without keys acknowledges this. Because currently crypto standards are so poor, and computers are so fast, the Snowden files were likely decrypted with just brute force if this is true. Sadly asymmetric systems have many other vulnerabilities and limitations as well.

You have been presented with the IPSec/IPv6/Whitenoise driver update pilot. This is now updated to include fixing LDAP/CAS with the same driver upgrade technique; this might be the quickest and simplest and easily most effective solution to immediately address the problem. Endpoints can simply and rapidly harden their defenses with dynamic one-time-pad authentication.

The pilot first proposed an IPSec/IPv6 driver upgrade as a method of virtually and virally distributing the single, unique, private, secret required key to any endpoint or device through a web based driver upgrade install.

Just like the IPSec/IPv6 driver, Microsoft's LDAP (Lightweight Directory Access Protocol) and Central Authentication Service CAS are designed to easily accept new crypto upgrades and standards.

Using the IPSec/IPv6/WN driver upgrade technique, the immediate problem of plugging the hole possibly exploited yesterday is rapidly addressed.

And as a consequence, any Microsoft product that uses LDAP/CAS and has upgraded to our solution version, is by definition protected moving forward if they choose to use our services.

Both the IPSec/IPv6 and LDAP/CAS upgrade can be done simultaneously in the pilot.

The follow up step would be implementation of Whitenoise encrypted databases (we have proof of concept) which satisfies requirements for bi-directional, configurable, replicable databases with perfect provenance of data since communications and the database itself is encrypted with >250,000 bit Whitenoise.

Scalability/interoperability /speed / overhead

This discussion considers a large network making 600,000,000 connections a day.

One major problem that big telecom companies have is scalability. This means that whatever you design and implement for a small network remains valid as the networks grows and become more and more complex. This used to be a very difficult problem particularly when security needs to be implemented with current technologies.

Key based security for all primary network security functions is preferred because it is objective for identity. When the key is unique, unbreakable, and securely distributed we can be assured of the identity of any endpoint, node, cell, component etc. on a network which is requisite for any effective security framework or layer.

WN technologies are specifically designed for interoperability and easy scalability – even viral scalability as the pilot envisions with simple IPv6 and LDAP/CAS online upgrades. Distributed keys in turn can securely distribute more distributed keys making the inclusion of new endpoints, sensors, nodes, components, cells, microcells, etc. natural and fluid. There is no disruption to any of the existing network security controls or frameworks that we are fixing.

As we design new generation networks we must look farther ahead to expected outcomes. We didn't predict the impact of Y2K or IPv4 running out of unique addresses. We must anticipate that vast networks will have trillions of endpoints with the explosion of the number of Internet of Things components, mobiles, and possibly most importantly the exponential explosion in the number of low cost sensors with communication.

The exponentially increasing number of components on the telecom edge each creates points of egress and security vulnerability that not only threatens the clients but is a growing threat to the telecom network framework itself.

The large telecom network averages about 600,000,000 connections per day and each of those connections needs to be secure. The volume of communications and the functions that need to be conducted create a huge amount of overhead and attendant costs. The telecom currently envisions adding 20,000 more cells and microcells so this volume will increase proportionally.

What does this mean in terms of scalability and overhead?

Let's assume that a one-time, secure network, single-sign-on authentication call with existing asymmetric public key frame works take one second for session key exchange and arithmetic processing.

If that is correct, **600 million connections per day** with one second authentication calls **generates 2.89 centuries of processing** between the telecom core and its edge each and every day.

Alternately, using just Whitenoise for that function would reduce the 2.89 centuries of processing overhead per day to 8.3 hours of processing per day. If Whitenoise is added to these systems to fix their fatal flaws (this is the recommended implementation path) than that is the amount of overhead you are adding which is negligible. See addendum below for calculations.

Those 600,000,000 connections are spread out and occur in parallel to some degree. For example, **if each node of the network can process**, and if there are 6,900 nodes (this is a medium-size network), those 2.89 centuries will reduce. But there is a cost. Security integrity of systems and network costs are currently adversely affected by adding more and more nodes to the backbone. Simplicity after all is strength.

RSA style, asymmetric processing is now seriously vulnerable and it is a stifling limiter to new generation networks where the majorities of edge endpoints have severely limited processing requirements and cannot perform the mathematics required to process public keys. See COMPARISON of PKI and DDKI handshakes.

Nodes like modems and encryption processing accelerators etc. limit easy scalability because telecoms need to add more big items to the network architecture as more endpoints are added.

Whitenoise technologies which operate with virtually no processing overhead and operate as fast in software as hardware means that key vaults and gatekeepers can be added to existing components as firmware and upgrades. Even sensors that communicate and are $1 in cost have enough juice to act as nodes with just firmware to provide a secure layer to support trust in software-only or chip paradigms.

This ensures that scalability will always be easy and linear.

A Historical progression affecting scalability

To know where we are headed to we need to understand where we came from.

As we are now well past the point of sensibility in relying solely on asymmetric security frameworks it is interesting to understand how the historical stoppers of large-scale, secure distributed networks now are the same limiters to large scale asymmetric security network frameworks.

Until computers and telecommunications everything important was directly distributed. You are given your passport, driver's license etc. Electronic communications created the problem of how to identify with full confidence and trust the person or endpoint that we are communicating with.

Back then, when trying to maintain security in a distributed system this approach was stopped in its tracks because:

- One needed to be able to get a key securely to the endpoint.

- One needed to manage too many keys because there was not a 1:1 correlation between the number of keys and the number of endpoints on a system. Back then a network needed to manage keys that equaled the square of the number of endpoints. A secure distributed network of 100 endpoints needed to manage 10,000 keys.

- Strong and long keys are preferred for security and trust in identity but increased key storage space, key transfer effort, and computation effort to use them was an impediment.

To address some of those problems asymmetric public key networks came into being. While computers were slow this was sufficiently secure but we knew the problem would catch up eventually. Public keys were always available. Factoring keys although difficult was possible at the outset. At that time the available computing speeds did not create a threat.

Now the world has changed and the problems that hindered development of large-scale distributed symmetric systems where there is only partial sharing of credentials plague public key systems. And there are even more vulnerabilities that are unsolvable in asymmetric security frameworks.

Whitenoise technologies have solved the historical stoppers of distributed key systems.

- There is a 1:1 correlation between WN keys and the number of endpoints.

- Exponentially long and strong WN keys can be stored in a fractional key space.

- Bit independent WN keys means communications are fault tolerant, the strength of keys can always be easily scaled by adding subkeys, and the speed of transmission can always be increased by parsing signals, running them in parallel and reassembling them.

- Whitenoise DIVA is a true one-time-pad which is the only mathematically proven unbreakable key technology. It is dynamic and always changing so hackers always have to start over.
- Distributed keys can in turn distribute more keys making these virtual secure frameworks virally scalable.

Conversely, because computers are now so fast standard key technologies can be broken just with brute force and no key access. This was accomplished on the Snowden files.

As RSA style public key systems try to increase key strength they are stuck in an inverse relationship where key space, overhead, and computational effort explode as these systems try to use stronger keys to improve security. This is what completely rules out those technologies as competitors in IoT and sensor markets.

Those systems cannot scale in real time. Because of identity proofing issues with public key systems, implementing just a VeriSign certificate can take up to a week and you still need your own staff to install it. Whitenoise can do this online in real-time in any context.

Future values adds and considerations

Value add – on/off functionality for smart grids and utilities

WN in conjunction with GloMo technology can turn utility endpoints on and off remotely depending on security assessment. WN provides inherent intrusion detection and can "turn off" endpoints in event of attack or a malfunction without human intervention.

Value add – dealing with throttling

WN in conjunction KTech compression (developed at NASA) can compress secure streams by up to 80% without loss of integrity or clarity.

That has a linear impact in terms of reducing download and upload times of applications, media etc.

Reducing network overhead by that amount will have dramatic implications on network overhead and throttling concerns.

Addendum: Assumption and calculation for the 2.89 centuries of overhead example

The telecom does 600,000,000 connections per day. (This estimate is taken from notes from our teleconference.)

Assumption: This example is an estimate of the current overhead absorbed for a 1 second PKI authentication call.

If all connections are authenticated, and each authentication routine took just one second then the overhead for a single-sign-on network access authentication call on the network would take:

600,000,000 connections times a 1 second authentication routine = 600,000,000 seconds. Divide that by 60 seconds per minute, 60 minutes per hour and 24 hours per day = **6,944** hours of processing **PER DAY!**

6,944 hours processing overhead per day times 365 days per year **= 2,534,722** hours of processing per year

2,534,722 hours of processing per year **= 2.89 centuries of processing per year**

At the Telecom Council of Silicon Valley Showcase a demonstration was done on a 2012 MacBook Pro with a 2.6 GHz Intel Core i7 processor and 16GB 1600 MHz DDR3 of memory. We showed you the encryption and decryption of a 27 K file 2000 times at approximately **.00005 seconds** for each function.

Although we are considering speed of authentication which is just the comparison of tokens and not the transformation of data we will use this value as a defendable speed when using Whitenoise for authentication.

What are the speed implications of using Whitenoise for authentication of 600 million connections?

600,000,000 X .00005 seconds = 30,000 seconds/60 seconds per minute/60 minutes per hour =

8.3 hours of processing **PER DAY**.

8.3 hours per day times 365 days per year = 3,042 hours of processing per year

3,042 hours of processing per year = .35 years

This is preferable to 2.89 centuries of processing.

Note:

These calculations are a baseline and don't add multiple authentication calls during a session just the first secure network access call. Neither does it consider that existing crypto exasperates processing time and overhead for every single key based security control because it is slow, computationally intensive and it bloats data when used for encryption.

SIM cards

Addendum – Deployment of Whitenoise technologies in SIM cards for mobile payments

Recently a request for deployment of Whitenoise and DIVA into SIM cards for mobile payments was received. This approach is being promoted by Canadian telecoms like TELUS, Bell and Shaw for Canadian banks.

There has been unexpectedly slow adoption of mobile payments in Canada.

Banks hate the mobile payment paradigm because they lose their first in line status with their customers to Google and Apple. Regardless of whether they are getting revenue they are losing control.

However, banks can both fix the technological problem and remain in the business position they want to maintain. Please see the following patent provisional on keeping banks first.

http://www.wnlabs.com/pdf/Whitenoise_crypto_currency_mobile_payments_Tata_Innovation_2015.pdf

Technology security concerns

- Security of initial connection is important

- Is the device resident key that is used for signature/authentication vulnerable to Man-in-the-Middle attacks when used on asymmetric frameworks when establishing a secure connection

- Near Field Communications (NFC) data transfer with radio waves cannot be considered secure. Firstly, NFC pegs part of its security on the hope that if the card or phone is really close to the terminal it is communicating with that it is more difficult for hacker technology to intercede. It may be the box that's vulnerable.

  https://en.wikipedia.org/wiki/Near_field_communication

- reasons for poor adoption is considered here.

Consequences of SIM vulnerabilities

https://en.wikipedia.org/wiki/Subscriber_identity_module

In February, 2015 it was reported by The Intercept that the NSA and GCHQ had stolen the encryption keys (Ki's) used by Gemalto (the manufacturer of 2 billion SIM cards annually), enabling these intelligence agencies to monitor voice and data communications without the knowledge or approval of cellular network providers or judicial oversight.

A reality of Whitenoise is that if keys could be stolen (an uproven but necessary theoretical assumption) that they could not be used in an unauthorized manner without rapid if not instant intrusion detection and revocation.

This pilot is proposing several options for the delivery of Whitenoise IdM keys: IPSec/IPv4, LDAP/CAS and Microsoft Certificate Authorities, and now SIM (Subscriber Identity Module)

Integrating Whitenoise technologies and DIVA into extensible drivers like IPSec/IPv6 and CAS means that the driver will manage processing the IPSec or CAS headers, detect it's the WN implementation, retrieve link keys if needed, and use those keys for DIVA or crypto or both depending on what the user or clients wants.

SIM cards are a different paradigm. Using WN with IPSec for ipv6 opens access to the verticals of the Internet of Things, sensors and high bandwidth network systems.

SIM cards are a pathway for phone operating systems to store small amounts of data that isn't easily accessed by applications (so it's a great place to put keys).

Currently SIM cards are not generally used for dynamic connections. This might be overcome by using the lower performance first connection for secure network authentication and access and then invoking a call to an external (to the SIM) third party service that will continue to manage dynamic one-time-pad authentication for "longer sessions." This will be a rare event in a payment processing context.

Consider that most payment transactions are pretty quick, one-shot kind of connections. Exponentially stronger Whitenoise keys can do all security functions including encryption without additional key exchange. It is a preferred choice and adequate on its own for the vast majority of payment processing contexts. It is also designed as a single key system where only the bank has the key!

Where dynamic connections are considered important in payment processing contexts those processes can be redirected.

--

Java script used by SIMs is known not to be very robust. Compiled drivers are a more secure approach on the face of things. However, Whitenoise/DIVA has very low requirements because the algorithm itself is secure. Java has not been problematic for us in the past.

From a hardware point of view we only have two requirements:

- **Can the SIM card be updated with firmware?**

  (Answer: Yes. This also negates requiring telecoms or other commercial players to be involved for deployment. If they lock down their own SIMs to prevent updating than they are limiting their own markets, interoperability with other networks, etc. and they create a host of other problems for themselves.)

- **Can the SIM card run or call dynamic processes?**

  Answer: Yes. See RunGMS algorithm call that might be used as the hook.)

The only requirements that DIVA has is that the device has

- Connectivity
- A little bit of storage space for the key
- Write back capacity to track current dynamic offsets

Testable research

The Ki, Kc or RAND (nonce) in SIMS instead could become our Current Dynamic Offsets. The unique private distributed key and routine can reside outside the SIM in a compiled and encrypted program and can be called by the “RunGSM” function on the SIM.

One WN key can create an infinite number of one-time-pads. One way to look at that is that because WN creates exponentially long keys and is dependent on current valid dynamic offsets

into that resulting key stream that each different offset will result in a different, unique key of arbitrary length.

SIMs are set up to accept a Ki or Kc that are a maximum of 128 bits which is a 16 character value. So that 128 bit is the ceiling on key strength for current crypto.

If that 128 bit Ki becomes the DIVA current dynamic offset to be used instead by an outside routine controlled and called by Run GSM Algorithm then we are looking at a current dynamic offset that can be up to 1 quadrillion bytes long (16 character offset).

That means if we were to view a WN key as sharing an incrementing characteristic like "key rings" that the device now has access to up to a quadrillion keys to be used if a fixed key lengths are used.

Again, it becomes infinite if the routine is using variable length keys.

This creates a completely infeasible brute force attack. Since DIVA is dynamic and that offset keeps changing, the hacker would have to start over and over and over.

The actual distributed keys are securely stored elsewhere on a device.

The final benefit is that keys cannot be stolen and used without DIVA detecting it which is the failsafe. Synchronicity is required between the server and a legitimate key.

Environment for national security level cryptography

National security level crypto requires involvement by reputable universities. RSA is associated with the Massachusetts Institute of Technology (MIT). Elliptical curves (an incremental improvement on RSA with a little smaller footprint) incubate at Waterloo University in Ontario, Canada. Identity Based Encryption was hatched at Stanford University in California.

Whitenoise technologies does research and development, testing and implementations with the assistance of the University of Victoria, British Columbia Canada.

We have reached into programs at other universities like MIT from this vantage point with the assistance of International Trade Canada and Industry Canada. We have been invited into some of the most advanced and prestigious innovation labs in the world from this vantage point as well. These include Tata Innovation Labs, Sprint Advanced Technology Labs, and the General Dynamics GDNexus Innovation portal.

In all cases these schools all have massive resources and, cutting edge IT security expertise and personnel. The university serves as a nexus for different stakeholders involved in critical sciences like security. Government, law enforcement, academia and commercial stakeholders all find a seat at the table at these reputable institutions that work the leading edge of critical sciences.

Affordable opportunities for SM enterprises and developers

S&M companies pay a disproportionate cost to cyber calamities. They have less money to protect themselves and develop secure solutions in the first place for their technologies, services

and businesses. They generally can't afford to pay the costs associated with cyber breaches because they are too small to take such a hit.

"Everything Should Be Made as Simple as Possible, But Not Simpler." Albert Einstein

This is one of the strengths of Whitenoise. The back end is almost always identical because it satisfies the three needs of cryptographic processes: key creation, key distribution and key management in the same manner. See http://sfi.wnlabs.com/help and administrative functions.

Front end modules/drivers/apps for your specific context can rapidly be done on a project basis that can be worked on in parallel and then absorbed into pilot.

On a case-by-case basis with a client we can determine what the best resources are to bring to bear. UVIC [Aspire Labs, Inspire Labs, and ECE], BCNET, Canary, and Planet Labs are examples of readily accessible resources.

6 month blocks for development costs and what the S&M receives

$55 - $100k

- PhD – A context specific expert is dedicated to your specific security project
- Masters – A context specific expert is dedicated to your specific security project

- 6 month – implementation, testing, pilot roll out
    - Implementation of WN technologies into your specific product or context
    - National and global scale pilot (testing scalability and interoperability)
    - Penetration testing for security
        - UVIC ECE Labs, Aspire Labs, Inspire Labs
    - Commercial penetration testing (Deloitte) to certify effectiveness
    - Roll out and technology transfer or management (third party services)

Shared patent opportunities for protectable competitive advantage

There may be opportunities to create patents for a protectable competitive advantage. Patents would not touch the core of Whitenoise technologies but rather be patents on the unique, proper implementations of WN, DIVA and DDKI into specific technology contexts like RF, SIMs, specific drivers, different OS, for unique security outcomes, etc. Patents would be shared by WN, UVIC, and client. Patent filings etc. would be conducted by UVIC. This builds on our R&D license with UVIC and provides a continually expanding IT intellectual property asset base.

Viral marketing and solution implementation

We have seen over the years how companies like PayPal, Face Book etc. built enormous values based on user bases and not revenue.

The same approach is an option you can take of providing free driver upgrades etc. to build and quickly capture enormous user bases. Subsequent monetization is simplified after you are already providing your potential customers with security reports and how you have already protected them. You have proven your worth to the customer.