What is the Problem?

How big a risk is all data on the internet or over the wires?

1/3 of data stored in the cloud are encrypted. 90% of all data is “in flight” and 87% of that is currently encrypted. Only 50% of internet data are encrypted. But LokDon has identified a systemic weakness that makes these data vulnerable.

Does the lock icon in browsers mean that they are secure?

Unfortunately, no. The internet's security infrastructure is 30 years old and was not built to protect data at-rest or in-flight. It still relies on keys and certificates, which are often lost, stolen, and misappropriated. A compromised key can expose your data without your browser being able to detect it. So, no, the lock icon is not a reliable indicator.

Why is a lost key or certificate a problem?

Encryption works like a lock. With the right key, the lock opens easily. It is the same way with encryption where compromising the key that protects data in flight means the data is compromised as well.

Does this mean that if I carefully protect my site’s key, it could be safe?

No. While losing that key would expose the data in flight, that key is not the only problem. Any key that is trusted by the connecting party would also expose the data in flight. This means that every sender, receiver, and the entire Certificate Authority (CA) system must all be perfectly secure for today’s system to be secure. To use industry terminology, every key in the CA system (and there are hundreds) is a Single Point of Failure. This just means that each key, if compromised, also compromises the protection for all data in flight. This is the reason keeping them secret is so important. As Ben Franklin once said, “Three can keep a secret, if two of them are dead.” Expecting that the dozens of companies and hundreds of employees that comprise the CA system will keep their secrets seems foolhardy in this light.

We understand you are not technical. What would the technical staff say about this?

This conversation is been had by the likes of Ponemon Institute, Gardner, IBM and many other cyber security luminaries. We are not saying that you need to build out a brand-new infrastructure. Rather, we are saying , it is possible to secure the entire internet starting with your organization first by using simple instructions embedded wherever your data live regardless of your current software or platform. The fact is that LokDon is an entity with the most practical solution at hand.

This problem seems larger than life itself.

Yes! It is a big concern because no one knows when security incident will occur or when they will be compromised. Everyone knows that the easiest way to get into the kingdom behind the castle is to find the key/s to the castle. Hackers know all these and that is why they are winning.

What are we doing?

Just like the old saying goes: “LokDon is here to send the fox out of the hen house.” Yes! We decided to redefine data completely.

Data -> Redefine data -> Data Nucleus Aggregator (DNA) -> Intermediate Representation -> Digital Data Nucleic Authority (DDNA)

Anywhere a customer uses LokDon they will not need certificates. LokDon’s security exceeds the currency, replaces the legacy and braces up the post quantum security. These are not provided by certificates authorities of PKI.

Does this really mean no stored keys anywhere in the system?

Yes. Stored, or persistent, keys are NOT a part of securing data at-rest and in-flight.

How are we doing it?

Security of information by encrypted verification-validation and evaluation (SIEVVE)

How is the LokDon solution different from TLS 1.3?

In many ways LokDon and TLS solve the same problem – We don’t store or manage keys for data communication. A few points on this:

1. LokDon does not rely on a stored private key or CA system.
2. LokDon provides security modules as a service, so that companies like you can build encrypted connections to allow for autonomous encryption, IAM, control of access list and administration of sensitive systems and sites.
3. Because LokDon and TLS solves the same problem in a different age and light, we will integrate the two. It is possible to use LokDon by compiling with a LokDon enabled version of TLS.

What if an Endpoint is imaged or reproduced by a Bad Actor?

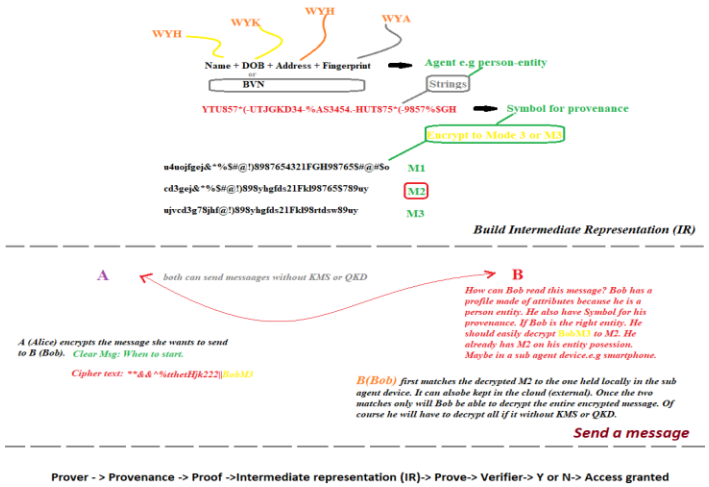
There are many defenses to prevent this from happening. However, even if all these defenses are overcome and the endpoint is completely and successfully reproduced, the Bad Actor will still be defeated. While some of the details of this are proprietary, if a Bad Actor successfully duplicates an Endpoint one of two things will happen:

1. In most cases the impersonating device is usually flagged as invalid and kept off the network.
2. In some cases, for example when the real device is shut down until the impersonating device is started, the real device is flagged as being an impersonator. In this case the user will quickly realize that there is an issue and the impersonating device can be tracked down using the IP address. Either way, whether the impostor' device fails to connect and sets off an alarm, or connects and causes the actual device to fail, the intrusion is detected almost immediately.

Why is Endpoint Provenance important?

The most sensitive data that any company deals with should only be shared with known and trusted employees or partners. Encryption is not enough to secure data. Knowing that only the intended recipient can decrypt the data is crucial to information security. In other words:
Identity + Encryption = Information Security.

The recipient of the message must satisfy the provenance process to be able to read the message.
Prover ->provenance-> proof -> Intermediate representation (IR)->Prove->Verifier-> Y or N-> Access granted



This guarantees that the encryption is correct and sound as well. -The message is tamper-proof.

What does Audit-able Security for Data in Flight mean?

Logging every transaction between provisioned parties allows us to report exactly who accessed the information. Additionally, any attempted breaches are immediately logged. It is already a best practice to regularly audit anything of value including physical and endpoint security. The ability to automatically audit the security of data in flight is something no legacy system can provide.

Is LokDon solution scale-able enough to solve this problem?

Yes. We scale by simply adding more systems. You can use any technology you like to run our system.

Isn't LokDon's service a Single Point of Failure?

LokDon is not a single system. LokDon's systems are distributed for availability as well as scale. In addition to autonomous functionality for reliability, LokDon also encrypts information in such a discrete way so that no single user or attack can expose customer data. LokDon doesn't touch customer data, the data pathway would have to be separately compromised. In short, with LokDon there are a plethora of mechanism and minimum of three separate modes that must all be successfully compromised to attack your data. Compare that to current best practice where compromising a single key provides the ability to unlock all data in flight.

Who is affected by the problem?

Who are LokDons target customers?

While most organizations that have data-in-flight and at rest can benefit from the enhanced security, auditing capabilities, and cost reduction, our concentration is in industries that have private data, intellectual property, or national secrets as part of their data at rest and in-flight. These include but are not limited to:

Government and Military
HealthCare/HealthTech
Banking/Fintech
Communication Platform Providers (Video Conferencing Services, Collaboration Tools, etc.)
Supply Chain
Internet of Things (IoT)
Security Offerings and Platforms (VPNs, etc.)

How to deploy?

What platforms does LokDon support?

LokDon can run almost anywhere. We currently have packages to support servers running Windows, OSX or Linux. We also deploy to mobile devices and will be able to run in any modern browser with no additional software installs soon.

How much work is it to deploy a solution?

This really depends on the solution. Generally speaking, we can classify integrations into three buckets:

- **Small Effort** -- In some cases it may be as easy as configuring our secure environment then recompiling with a LokDon enabled library or buy the already made production tools.
- **Medium Effort** -- In other cases, the communication portion of an application may need to be extended with our APIs to enable our audit-able security. Depending on the scope of the integration the effort here can vary by the industry.
- **Large Effort** -- In many cases, LokDon will be integrated such that a company need only select and deploy a solution they already use with "LokDon SDK inside." – Retrofit with LokDon SDK.

How does a new user or system get added to LokDon's Cryptographic Network?

Different organizations require different levels of security. Even within an organization, some users may require more vetting than others. So, there is no "one size fits all" *process*. For example, a mobile banking user requires less security care to check a balance than for making large financial transactions. National security applications would require even more care. LokDon's solution is completely configurable and able to handle any of these. It can be automated to add a new user by simply adding username and email but it also supports work flows where valid Identification must be manually verified, in person (KYC) or automatically through the authorities, or in a secure environment.