Next-Generation Internet. Reliable. Secure.

ANAPAYA

WHITE PAPER

Know where your data travels

This whitepaper will examine the issue of data security in more detail as well as show you how you can protect yourself in today's unstable, insecure and fragile digital environment.

Introduction

It’s official: Cybercrime is on the rise and shows no signs of slowing down.

Financial institutions are on the frontline. Over 25% of all malware attacks target the banking and financial services sector—more than any other industry. The number of compromised credit cards increased by 212% in 2019 and credential leaks rose by over 129%.

With stats like these, you don’t need a hypothetical example to demonstrate the possibility of cybercrime, because these attacks are no longer in the realm of the theoretical. They’re happening, and they’re happening today.

Data has become a valuable commodity and increasingly sensitive. The right information in the wrong hands can have adverse effects for businesses, individuals, and even entire countries. However, many of us have little or no control over where our data travels, who sees it, and who can take advantage of it. Servers are being hacked and data is stolen on a daily basis these days. This exposure is especially threatening for financial institutions like banking companies.

Fortunately, there are solutions to this problem. SCION represents a new way to connect that enables the sender of data to assemble the travel route for their data based on their best interests, policies, and preferences, making them immune to cyber threats such as routing attacks. This whitepaper will examine the issue of data security in more detail as well as show you how you can protect yourself in today’s unstable, insecure and fragile digital environment.

Over 25% of all malware attacks target the banking and financial services sector—more than any other industry

The number of compromised credit cards increased by 212% in 2019 and credential leaks rose by over 129%

Threats to the financial industry (why data control is essential)

The financial industry deals with highly valuable and sensitive data. Daily, massive amounts of consumer and business data are exchanged. Given the sensitivity and quantity of data, undesired disclosures result in high costs for handling the situation, and serious legal and reputational risks.

Let's take a look at this in more detail.

Cybercrime

The financial industry is one of the most highly targeted industries when it comes to cybercrime. With so much data being exchanged, it provides numerous opportunities for criminals to intercept and misuse that data.

One such example is the Equifax data breach that is estimated to cost the company over $600 million in damages. Another example of these attacks occurred in 2017, where large chunks of network traffic belonging to MasterCard, Visa, and more than two dozen other financial services companies were briefly routed through a Russian government-controlled telecom company under unexplained circumstances—a good example of how data can be hijacked from remote servers. Details such as PIN codes, banking information and others were left vulnerable to unknown individuals who could easily use that information against those companies and individuals.

Financial organisations such as banks are often targeted with ransomware, malware and routing attacks.

With so much data being exchanged, it provides numerous opportunities for criminals to intercept and misuse that data.

Ransomware

Ransomware occurs when a data breach results in an organisation losing access to their data. That data is then locked and held ransom by criminals demanding payment for its release. Ransomware is often the result of malware infiltrating the organisation undetected, or via a direct routing attack.

Malware

Malware refers to any kind of software that causes damage to a computer in some way. Malware can open up vulnerabilities in your networks and organisation, allowing criminals to access and control data from its rightful owners.

Routing attacks

We discuss routing attacks in more detail below, but briefly, routing attacks occur when criminals intercept your data on its way to its intended destination. The criminal who conducts the routing attack creates a fake node offering a seemingly faster route for your data, at which point the data can be recorded.

These categories present a general overview of the main threats that threaten financial organisations. Anapaya's solutions are able to make your organisation completely immune to routing attacks, one of the major threats that financial organisations have historically had no control over.

The control problem

We all use the internet daily, but do we understand how it works?

For most of us, the answer is no. We conduct business, wire through money and share some of our most sensitive data online, yet we don't actually have control over where that data goes, or even who may see it.

How your data travels on the internet

The internet itself is made up of multiple different networks, controlled by many different kinds of companies around the world. Your data, whether it be a post on Facebook or highly sensitive financial business information, travels through these networks, each making their own decisions about where your data goes independently of the rest.

These networks are all connected, loosely, by a system called the Border Gateway Protocol, that works like a telephone directory helping the networks to locate one another. Through the Border Gateway Protocol, the networks automatically attempt to identify the shortest or most optimal route to your data's final destination according to your ISP.

While this system is widely used, it is not secure or controlled. Owners of the data being sent through the internet usually have no say over what networks handle their data, where those networks are located or even who owns that specific network. You'd be quite surprised to find out that your banking data might travel through countries with dubious privacy laws or areas with a history of cybercrime.

As recently as April 1st 2020, the largest Russian ISP, Rostelecom, leaked prefixes (an aggregation of IP addresses) belonging to prominent internet hosts such as Akamai, Cloudflare, Hetzner, Digital Ocean, Amazon AWS and others. Before the issue was resolved, copious amounts of data were leaked to the world.

Businesses like financial institutions who deal with highly valuable and sensitive data have virtually no control over where their data travels. They effectively are sending banking information from one location to another, and not controlling where it may go along the way.

Businesses like financial institutions who deal with highly valuable and sensitive data have virtually no control over where their data travels. They effectively are sending banking information from one location to another, and not controlling where it may go along the way.

How your data is at risk

Since the network nodes of the internet described above make automatic choices on the route your data travels based on network distance and cost optimisations, it's relatively easy to intercept the data.

All cyber criminals need to do is publish fake routes and networks on the Border Gateway Protocol to get network nodes to send data through them instead. On these counterfeit routes and networks, cybercriminals hijack and harvest your data within seconds, and send it towards its final destination with no-one the wiser. This is known as a routing attack.

The reason for this insecure system is the simple fact that the internet was never built with security in mind. The internet began within a trusted domain and was modified to be used by the public. Thus, it has no built-in protection methods from routing attacks and as a result, financial organisations–and indeed, everyone who uses the internet–is at risk every time they send data.

In addition to cyberattacks, lack of control comes with civil risks such as GDPR and Patriot Act violations. Without the ability to control where your data goes, you cannot guarantee that you will avoid areas where strict data protection laws are active.

When considering the risks, this situation is simply not acceptable for financial institutions and their clients.

The reason for this insecure system is the simple fact that the internet was never built with security in mind..

What solutions are available

The internet is an adequate solution for communication between a bank and its clients. As the only global public network, it is the only viable option, and the amount of data exchanged is minimal, which also minimises the risk.

However, the real danger is when banks transmit data to each other. These business-to-business exchanges are highly critical due to the volume of data shared, its sensitivity, and the impact a leak will have on the business. They are prime, valuable, and vulnerable targets for cyber attacks.

Banking and financial organisations need to find a better way to connect and handle their data. There are a few solutions to consider for organisations that deal with sensitive data on a regular basis.

The most crucial aspect of this is how these solutions make forwarding decisions, i.e., how they decide where to forward data. Generally, routers attempt to transmit data along the shortest or cheapest path. Nowadays, several technologies determine these paths called routing protocols. Routing protocols have advantages and disadvantages and serve different purposes and in various environments such as global internet, private wide area networks (WANs), and local area networks (LANs).

There are two established protocols—namely BGP and MPLS—that have severe issues. These issues are addressed by a new protocol, SCION, which we will discuss as well.

The real danger is when banks transmit data to each other. These business-to-business exchanges are highly critical due to the volume of data shared, its sensitivity, and the impact a leak will have on the business.

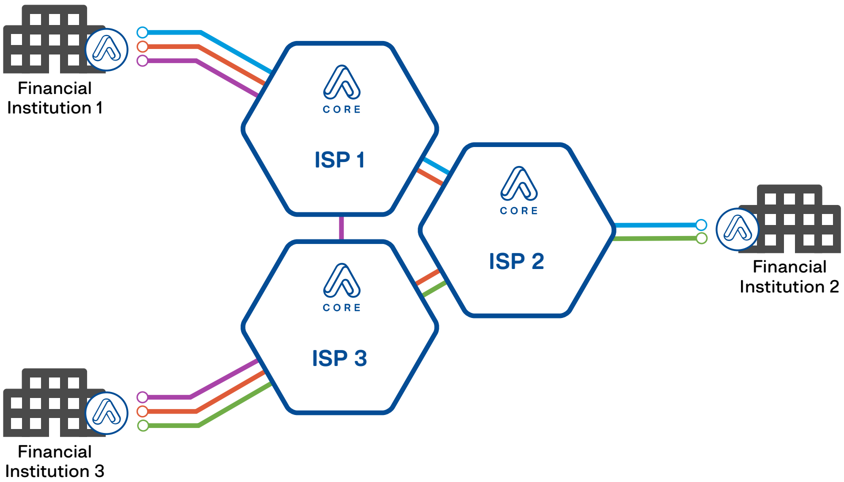


Figure 1
Three service providers were enabled with Anapaya CORE and interconnected together.

Transmit over the internet: Border Gateway Protocol (BGP)

BGP is a mainstream routing protocol for routing on the internet. In BGP, routers perform both packet forwarding and routing, based on their destination IP addresses.

Each router uses its own forwarding table. For every IP address, it indicates an outgoing link interface which is influenced by the cost of the path to the destination. For each arriving data-packet, a router checks a packet's destination IP with its forwarding table and forwards the packet onto the interface defined there.

The internet consists of interconnected networks known as Autonomous Systems (AS), which are a set of IP-networks and routers that belong to a single administrative domain and share a single routing policy. Each AS has internal routers and border routers.

Border routers connect ASs with border routers via the BGP protocol. Every single IP address belongs to a particular AS, and end-to-end data paths usually pass through several ASs. The goal for BGP is to utilise the shortest path, in terms of numbers of AS hops.

As the internet is continually evolving, new interconnections are established, and old ones vanish daily. Today's best path will not remain the best one tomorrow. To stay up to date, routers regularly exchange their routing tables and update them accordingly. If there is a new and cheaper path between routers, this information spreads throughout the entire network, and routers include it into their forwarding tables. Alternatively, if an existing interconnection fails, routers are aware and remove it from their tables.

BGP is useful but is unfortunately vulnerable to active attacks. The protocol relies on the mutual trust of routers, and there is limited protection against deception. Malicious routers can distribute a fake routing table claiming a shorter distance to specific IP addresses. Misguided neighbour routers will then reroute the traffic towards the attacking router. This attack is called BGP hijacking and can have disastrous effects such as loss of data and data ransom.

BGP Advantages

- Effective and cheap
- Optimised for routing performance

BGP Disadvantages

- Unreliable
- Insecure
- Vulnerable to attacks and leaks
- Lack of control

Use for Financial Institutions

As a bank client, using BGP is usually secure and good enough for general banking. The amount of data that is transmitted is limited, and not a primary target for cyber attacks. However, using BGP as a protocol for financial institutions to exchange data with one another is not a good idea on many fronts. These exchanges have a huge volume of data and are a primary target for cyber criminals. Security and control should be at the forefront of routing considerations, and BGP does not deliver on either. BGP's vulnerability to cyberattacks furthermore makes it a risky choice for financial organisations.

Using a private network: Multi-Protocol Label Switching (MPLS)

In MPLS, routers do not bother with routing at all. A few central controllers instead perform routing. Routers are only focused on forwarding packets, thus speeding up the entire process.

Central controllers pre-compute virtual paths between pairs of remote routers. Paths are marked with labels known as label-switched paths (LSP). Once a packet is assigned to a path, it gets an appropriate label which routers rely on for forwarding.

A single router may belong to several paths and act as an intermediate hop. Therefore, each router keeps a Label Information Base: a rulebook on how to forward packets assigned to different LSP. There are neither forwarding table lookups nor forwarding table data exchanges. This makes MPLS time efficient.

MPLS does not scale up for vast networks like the internet, but smaller systems benefit from it. Thus, MPLS is widely used within ASs or private VPNs. As it belongs to a single entity, it allows centralised routing. Data-packets travel through AS's infrastructure via label-switch paths much faster than with the assistance of conventional forwarding tables. With MPLS, routing tables are not installed on every single inner router. The routing protocol (such as BGP) is instead only installed on border routers to connect AS's infrastructure with other ASs and with clients.

✚ MPLS Advantages

- Optimised for speed
- Greater control over data travel
- Better security

− MPLS Disadvantages

- Not public, nor pervasive
- Vulnerable to connection failure
- Reliant on a single Service Provider

Use for Financial Institutions

MPLS may be beneficial for private VPNs, but will not find much use for multiple organisations that require collaboration. The lack of flexibility, ubiquity and the ability to scale with growing needs limits MPLS and makes it a less than suitable choice for inter-financial institutions communications.

Another way: SCION

In SCION, it is the sender who defines the path for a data packet. This means the sender does the routing, and routers only do forwarding. Routers in the network are connected via virtual predefined path segments, while the sender constructs the end-to-end path out of them—similar to how one would build a path out of Lego.

The information about the segments is stored on special path servers. When a sender wants to send a message, he requests information about the available segments, assembles an end-to-end path out of the segments, and includes information about the path into the SCION header of the data packet.

The SCION header contains information on every single hop (router) and its forwarding interface along the path. Routers along the way find forwarding directions in the packets header and do not need to lookup forwarding tables. This increases forwarding speed and reduces errors. Moreover, paths are cryptographically protected and once on the path, data-packets cannot deviate from it. Thus, “BGP-like” hijacking attacks are impossible.

SCION enables the sender of data to assemble the travel route for their data based on their best interests, policies, and preferences. It further allows these path segments to be interchangeable at will, meaning that any failed segments can be substituted with an equivalent one automatically, without the loss of performance.

✚ SCION Advantages

- Secure
- Controllable
- Flexible
- Reliable

− SCION Disadvantages

- Limited footprint
- Only available for B2B communication

Use for Financial Institutions

SCION provides flexibility, security, and control to the sender. Data pathing information contains cryptographically authenticated IDs of the Service Providers’ networks, the jurisdiction to which it belongs, its latency, bandwidth, and other meta-information. SCION EDGE receives the information for all the possible paths and selects the most appropriate based on business policies defined by the sender. These policies could include geographical constraints, speed considerations, security precautions, and more. Thus, the financial institution has true control over where its data goes and how it gets there. In addition, all the information is verifiable and accountable, contributing to compliance.

Furthermore, with its immunity to routing attacks and additional security benefits, it is the most secure protocol available today for a public network. Due to its security, control and reliability, it is the best option for financial organisations to use.

How financial institutions can protect themselves

Today, it's imperative to protect yourself in the best way you can. Courts from around the world have laid the responsibility of data protection on businesses, and cybercriminals have ramped up their efforts to exploit any digital weaknesses a company may have.

The question, therefore, is how organisations like financial institutions can protect themselves and the data of their clients.

Here are a few steps financial institutions can take to protect their key applications:

Phishing prevention and education

Financial institutions should hold frequent employee training and client awareness so that they can recognise and avoid phishing scams. They should also implement an easy way to report phishing attempts, as the majority of successful phishing attacks are completed in the first hour.

Implement two factor authentication

Two factor authentication on customer-facing applications and cloud-based email accounts helps guard their systems from unauthorised access because it demands additional information and credentials.

Monitor system access

To avoid and detect privileged misuse, financial businesses could monitor and log employee access to sensitive financial data. They should also educate employees on the importance and seriousness of system access.

Introduce malware monitoring and protection

Financial services organisations must monitor their systems for any suspicious behavior. By merely monitoring and staying vigilant, these organisations can guard against botnet or DoS attacks, and be alerted to the presence of malware before it causes damage.

Finally, we also recommend that financial institutions regain control of their network traffic, where their data goes and how it gets there. Joining the SCION-Fabric, which is the ecosystem of all the interconnected service providers enabled with the SCION protocol, is the single best step toward real data security for exchanging information with your peers (clearing, trading, etc) or towards gaining real control over the network underlying a SD-WAN solution. By reducing the impact of a DDoS attack, the SCION-Fabric also contributes to your business continuity and security.

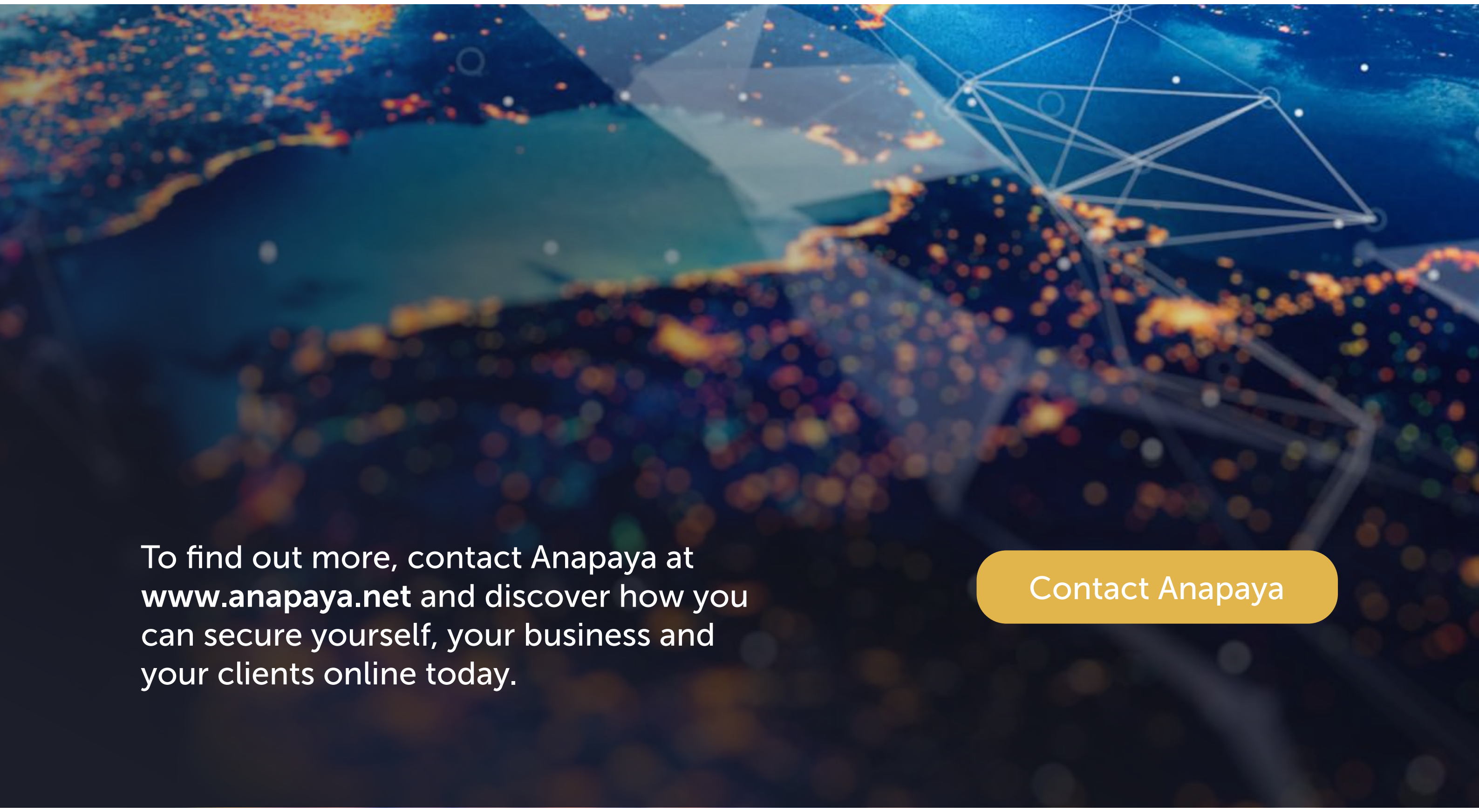
Financial institutions can either join the SCION-Fabric through any local SCION-enabled Service Provider or Anapaya CONNECT, an international SCION-transit service. This will enable you to reach all other participants, and become part of this next-generation internet.

Access SCION with Anapaya

This whitepaper has highlighted the risks involved, both criminal and civil when dealing with sensitive data. Financial institutions can no longer ignore the online threats that come with being a modern business. With immunity to routing attacks, protection against DDoS, full control over where data flows to ensure compliance with legislation, regulation or internal policies, the SCION-Fabric is the best connectivity solution that professional organisations have access to.

If you would like to join the SCION-Fabric, increase your business continuity and regain control over the data entrusted in your care, consider Anapaya.

Anapaya Systems provides users with the opportunity to access the SCION-Fabric through its industrial-grade product suite. Users can thus connect to their peers in a highly secure, reliable and controllable way.



To find out more, contact Anapaya at **www.anapaya.net** and discover how you can secure yourself, your business and your clients online today.

Contact Anapaya