The Role of Practical Validation for Homeland Security

Contact us at:
CoreStreet Ltd.
One Alewife Center
Suite 200
Cambridge, MA
02140

info@corestreet.com
Tel: 617-661-3554

Introduction

As government and industry struggle to implement effective security policies, many previously downplayed challenges have reemerged as significant obstacles to nationwide safety. One crucial area is transactional authentication and validation. Put simply, there are many everyday actions (such as getting on an airplane, going into an office building, withdrawing cash at an ATM or booting up a secure laptop) that should not be performed without making sure that the person attempting the action is authorized to do so. What's more, with available information changing so frequently, we should make sure that the person is authorized to do so *right now*. These kinds of checks are currently performed only for high-risk transactions and, even then, often at random intervals.

In order to provide an adequate degree of safety, validation must become ubiquitous. Every important transaction should be protected by a meaningful validation test. In order for validation to become ubiquitous, it must be performed quickly - without burdening the vast numbers of legitimate participants - and it must be performed at far-flung and diverse locations. Until now, validation technology was too expensive and cumbersome to rise to this ambitious task. CoreStreet has developed a new way to perform validation that finally makes it practical for the millions of common tasks performed every day across the country. We think that this can have a significant positive impact on effective homeland security.

About the Company

Founded in 2001 and staffed entirely by security and software industry veterans, CoreStreet, Ltd. is a new company focused on commercializing a groundbreaking but practical security technology developed by world-leading cryptographer and MIT professor Silvio Micali. The technology is embodied in our principal product – the Real Time Credential Server™. While we believe that there are many commercial applications for our product, the current national climate compels us to focus primarily on government and homeland security applications.

What is Validation and Why is it so Important?

There are two vital questions that must be answered in every secure transaction. The first is, "Are you who you say you are?" This question, known as ***authentication,*** can be answered in a variety of ways. Technologies such as biometrics, PIN numbers, passwords, digital certificates and smart ID cards are all commonly used to establish a person's identity thereby answering the first question. However, authentication is only half of the problem.

The second question is, "Are you really supposed to be doing what you're trying to do, right now?" This question, called ***validation*** or ***authorization*** is often more important and much harder to answer. There are no preexisting technologies for answering it in a practical way in a wide variety of situations. The reason for the difficulty is that while authentication is a two-party problem (answerable through an inspection of credentials between the attempted user and controlling agent), all current validation solutions require a secure, costly and real time connection to a trusted third party.

For illustrative purposes consider the example of a traffic stop. By examining the physical integrity of the offender's driver's license and comparing the photograph to the actual driver, the police officer can reasonably establish the driver's identity (thereby performing authentication). However, a physically valid driver's license doesn't mean that the motorist still has the right to drive – and it certainly doesn't prove that the motorist isn't on a list of wanted fugitives. The officer cannot get these proofs from the driver's license itself (because, unlike eye color, the status of these privileges can change more frequently than the driver's license is updated), cannot ask the motorist (because the motorist is not trustworthy on this point) and cannot ask another officer or consult a local list (because the information may be missing or out of date). The only reliable way to check that the motorist is actually supposed to be doing what he's trying to do right now (drive), is for the officer to connect to the police computer back at the station and check several centralized databases. This validation check can take several minutes.

In the case of a routine traffic stop (a low-volume transaction that is not particularly time sensitive and only occurs when an infraction has already been committed), calling a central computer and waiting for a few minutes may be acceptable. However, consider the case of checking every single passenger going through an airport checkpoint. Authentication can still be performed quickly (for example by scanning the ticket and ID), but validation is almost impossible because (1) connecting every airport counter to a central computer is impractical, (2) inserting a delay of even several seconds per passenger can cause unacceptable traffic levels and (3) the central computer would quickly become swamped trying to respond to so many requests. But without validation, the whole system becomes largely

The Role of Practical Validation for Homeland Security

meaningless. When an airline employee is facing someone who has just been added to a terrorist watch list, the important thing is not to determine the person's identity, but to determine that *they're currently on the terrorist list*.

What's needed is a way to eliminate the need to talk to a trusted third party at every transaction and make validation a two-party problem like authentication - then authentication and validation can be performed in one step for any important transaction. That's exactly what the CoreStreet Real Time Credentials™ (RTC™) does.

How Does it Work?

The RTCS™ is based on an elegant yet powerful set of algorithms invented by Dr. Micali and implemented by CoreStreet's engineering team.

Our product provides three primary advantages over all other validation technologies:

- It seamlessly scales to billions of users
- It can work in connected, partially connected or entirely disconnected environments
- It can manage multiple, independent dynamic privileges for each credential

At the heart of the technology is our ability to generate short messages (sometimes called tokens), which serve as mathematical proofs of the current validity of some *privilege* (such as the ability to read confidential documents) associated with an individual *credential* (such as a smart ID card). These proofs are very small, easy and quick to compute and completely secure. There is never a need to protect the proofs from interception or theft because they contain no secret information and are unforgeable and unspoofable. These characteristics make it possible to embed the proofs into credentials and pass them around public, unsecured networks. To positively validate the current status of any privilege, an agent only has to cryptographically compare the proof to a value stored on the credential. This action is secure, can be done in a fraction of a second, scales to literally billions of users and eliminates the need for a trusted third party to participate in the transaction. Twelve issued patents protect the technology. Further details on the algorithms and software are beyond the scope of this paper, but are available from the company (at www.corestreet.com or see the "Contact Us" section below).

Vital Attributes of the RTC™

For validation to become ubiquitous enough to be useful for homeland defense, a proposed technology must possess the defining characteristics outlined below. While other technologies meet some of these criteria, we believe that the RTC™ is unique in meeting them all.

Disconnected Access

Most locations in the real world – airports, subway turnstiles, border crossings, etc. – don't have the benefit of an always-on network connection. Even in places that are easy to wire, network connections are often slow, expensive and unreliable. The RTC™ is the only known system for performing sophisticated validation in both connected and disconnected environments.

Operational Transparency

Any technology that aims to make validation possible at every secure transaction has to be unobtrusive and nearly transparent in everyday usage. A cumbersome security procedure may be well intentioned, but will often become compromised and ineffective, as frustrated users are motivated to find shortcuts and workarounds. The speed, simplicity and wide operational flexibility of the RTC™ allows for true operation transparency. In most cases, users will not be aware of any extra steps or delays in their familiar routines as their privileges are validated.

Cryptographic Certainty

The mathematical bases for CoreStreet's patented technology are public one-way hashing algorithms (such as the NSA's SHA-1). These algorithms are among the best understood, most vigorously tested and most trusted algorithms in the world. RTC™ proofs cannot be effectively forged or spoofed by any method currently known to the cryptographic and security communities. Furthermore, the nature of our patented algorithm makes it virtually impossible for an attacker to produce either false positive or false negative results.

Non-Repudiation

All transactions performed by the RTC™ are logged in such a way as to provide positive proof that the transaction took place. More than simply an entry in a log file, RTC™ logs can provide hard and unalterable evidence of the time, place, involved parties and result for every important privilege check.

Practical Update Times

A far-flung and heterogeneous security system is only effective if important data can be disseminated

CORESTREET
REAL TIME CREDENTIALS

The Role of Practical Validation for Homeland Security

in a timely fashion. Since an individual RTC™ proof of privilege is very small in size and change can be transmitted over any unsecured medium, it's easy to ensure that important changes get communicated quickly.

Guaranteed Freshness

RTC™ data includes an unforgeable date stamp to make sure that stale information can never be confused for current information.

Worst-Case Survivability

A unique feature of the RTC™ is its robust and predictable behavior even in the face of total system failure. Traditional security technologies allow for a very limited set of options in dealing with a systemic shutdown. For example, typical smart locks can be set to either lock or unlock in the case of a facility-wide power or communications failure. Neither is a wholly satisfactory solution – one may hinder access for emergency personnel while the other may admit dangerous individuals. In contrast, with RTC™ the same smart locks and keys become completely autonomous and, in the case of a system failure, are able to continue enforcing the last valid security policies. Locks will continue to open and close for the duration of their configured time interval. Since time intervals can be varied by credential, an RTC™-enabled lock system may allow certain highly trusted individuals (FBI agents, for example) to continue to access all doors after everybody else's access has been suspended. We believe that RTC™ offers great flexibility to security system designers in dealing with worst-case scenarios.

System Interoperability

No single monolithic technology will ever practically secure an area as large and diverse as the United States. The RTC™ is based on open standards and designed for easy integration with other systems. In many cases, validation can be added to an existing authentication framework by installing the RTC™ and leaving the other pieces intact.

Practical Examples

The RTC™ is a horizontal platform enabling developers of security systems to add validation and privilege management to a wide variety of applications. We've built sample prototypes in three specific areas to demonstrate the value of real time credentials. Each of these applications represents a dramatic and high value problem space with a high level of current investment by both government and industry. Please contact us for more information about any of these areas.

Physical Access

Smart door locks to protect sensitive areas at airports, government buildings, campuses and shipping locations are in high demand but very cumbersome and expensive. Current centrally managed solutions require a secure network connection between every door lock or access panel and a trusted validation server. This costs thousands of dollars per door (mostly for the networking) and can only be installed in locations that are easy to wire. Disconnected doors such as those found on trucks, airplanes, cargo containers or simply remote installations cannot be secured by current smart lock technology. By using the RTC™, we've developed a working prototype lock that can be installed at any location and requires absolutely no connections or communications (either wired or wireless) at all. This can save up to 75% off the cost of a wired lock, and makes it possible to fully secure remote or disconnected areas which were previously impossible to protect - thus substantially improving the overall security of a complex installation. Our goal is to work with leading physical access manufacturers to bring the prototype to market.

Computer Security

Our technology can remotely disable access to any mobile computer, PDA or smart phone. Thus we can prevent unauthorized access and data theft even in a completely disconnected environment and even from users who have only recently lost their authorization (terminated employees, for example). CoreStreet has developed a working prototype of this application that runs on most Microsoft-based laptops and Palm-based organizers.

Certificate Validation

Existing technologies for validating and revoking digital certificates, such as CRLs and OCSP, do not scale past approximately 100,000 users and cannot be used in a disconnected environment. Furthermore, current technologies cannot easily handle multiple independently managed privileges on a single certificate – forcing costly certificate re-issuance every time a privilege changes. The RTC™ can handle multiple privileges for literally billions of users and can be deployed in places that OCSP cannot support. The federal government has programs in place that are committed to issuing tens of millions of digital certificates on smart cards. The RTC™ offers a practical way to manage, validate and revoke all of those certificates.