

Cryptographically Resilient Application Servers (RCrypto)

 Enables resilient Internet security

Introduction



Electronic communications over the internet has increased orders of magnitude in the last few years. The ubiquity of internet enabled devices and increasing user familiarity with such devices has seen an explosion of applications being internet enabled. Internet enabled applications span many domains such as e-commerce, enterprise, e-government, healthcare to name a few. This trend is unstoppable and will only gather momentum.

Internet enabled applications range from very simple email applications to complex multi-party negotiation schemes. Moreover, Internet enabled applications have the anywhere, anytime, almost any device advantages and are very attractive to both consumers and service providers.

But as more applications become internet enabled, the important issue of security needs to be addressed. Since internet uses public networks that can span many countries and even continents, the network traffic potentially passing through so many public nodes, it is essential that such communications be fully protected from trouble makers. Even in an intranet setting, it is essential that unauthorized people cannot access internal network traffic.

Public key cryptography through secure socket layer (SSL) protocol has come to the rescue of security needy applications. SSL has become the de facto protocol for protecting internet based communications. All popular internet clients and servers support the SSL protocol and SSL-enabling an internet application is fairly straight forward.

Issues

Even though SSL-enabling an application is simple, there are some important problems with this solution. Since SSL relies on public key cryptography, sensitive information, technically

called the “private key” needs to be highly protected since the security of the entire system relies on the private key. However, in most current systems, the private key is software based mainly because hardware based schemes are expensive and difficult to administer.

An attacker who manages to penetrate the computer on which the private key resides will be able to retrieve the private key (even if the private key is password protected, if the password is not judiciously selected, such protection can be easily broken). The attacker’s computer can then masquerade as the legitimate computer or eavesdrop on what users assume as secure communications.

Moreover, such SSL enabled applications are difficult to scale to multiple machines because it involves duplicating the private key or using multiple private keys increasing the operational cost of the system. Such systems are also not very fault-tolerant.

Technology

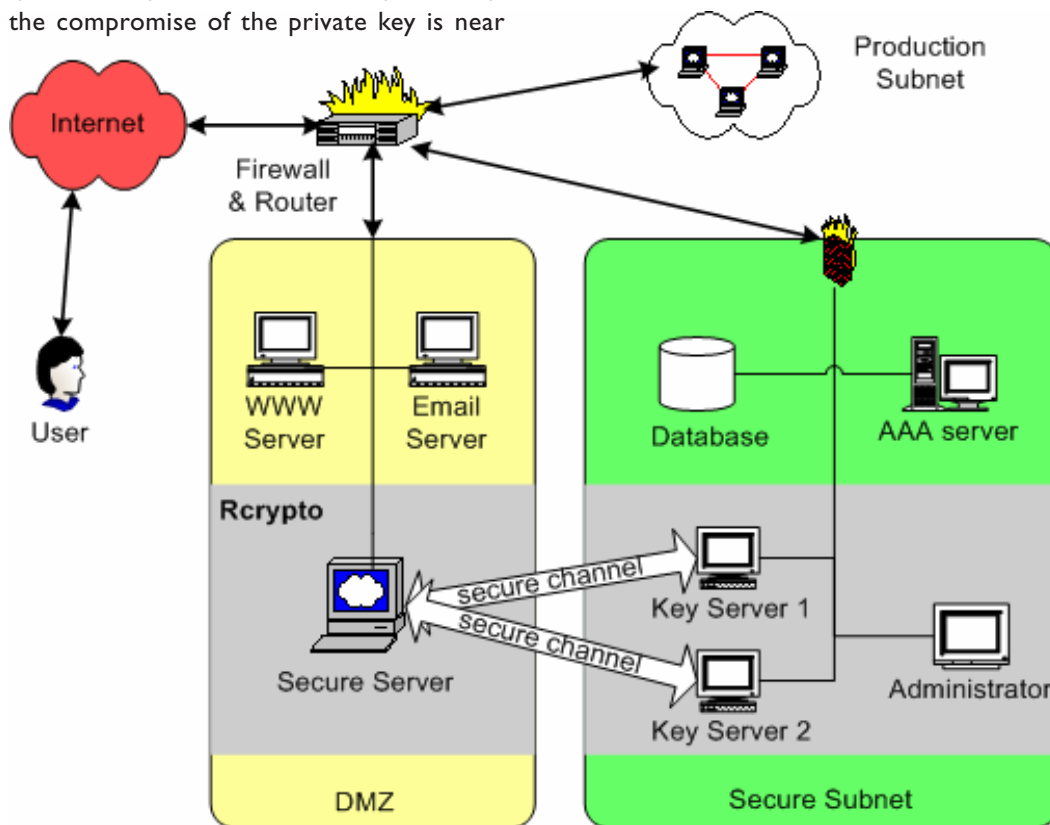
There is an old mother’s saying – Don’t put all your eggs in one basket. This simple truism is literally the basis of the RCrypto solution. The solution consists of two major components, one cryptographic and the other system architecture based. The cryptographic solution involves splitting the private key into multiple parts. Each of these partial keys resides on key servers and is capable of only performing a partial decryption or creating a partial signature. The partial keys are never reconstructed in any single location and are split forever. The entire solution uses a simple and elegant architecture to distribute these partial keys, generate partial signatures/decryptions and combine these partial results into a complete one such that the whole process is seamless and transparent to the reliant application.

For further information, please contact:

Industry Development Department
Institute for Infocomm Research
21 Heng Mui Keng Terrace
Singapore 119613
Tel: (65) 6874 8399
Email: inddev@i2r.a-star.edu.sg

The architecture includes support for load balancing and fault tolerance. Using this scheme, it is easy to manage multiple servers with partial private keys. The system also tolerates faults such as computer, hard disk crashes much more gracefully.

The system also has a novel key refresh feature whereby the partial keys can be updated periodically. Hence an attacker not only needs to penetrate many machines, but also needs to do so within a specific time period to extract the private key, ensuring that the compromise of the private key is near impossible.



Platforms

The entire system has been developed as a pluggable module. Currently the modules are J2SE 5.0 compliant and can be used to enable java based web servers e.g. J2EE based application servers, Tomcat based web applications. A C based apache add-on is also available. The modules are pluggable in the sense no change needs to be made to the relying applications.

Applications

All SSL enabled applications can benefit from our solution. Moreover other PKI enabled services such as time stampers, revocation servers can incorporate RCrypto. RCrypto is ideally suited for security sensitive applications such as banking, enterprise applications, healthcare etc.

Market Potential

Security and the infrastructure to support it will be an absolute necessity for doing business henceforth. Recent market analysis has estimated that revenue from security applications to multiply manifold. As the need for security grows, organizations will need their own security infrastructure and I²R's RCrypto I will be an ideal solution.