

## Table of Contents

Introduction.....	2
Accounts.....	3
Adaptive Echo.....	4
Block Cipher Modes of Operation.....	5
Communication Methods.....	6
Constant-Time Comparison Function.....	7
Echo Protocol.....	8
Encrypted and Authenticated Containers.....	9
Key Derivation.....	10
Hybrid System.....	11
Poptastic.....	12
Public Key Infrastructure.....	13
Two-Way Calling.....	14

## **Introduction**

Spot-On is an exploratory research project investigating a variety of communication and cryptographic algorithms. The software is composed of two separate applications, a kernel and a user interface. The two components are written in C++ and require the Qt framework as well as an assortment of libraries. Qt versions 4.8.x and Qt 5.x are supported. The application is available on FreeBSD, Linux, OS X, OS/2, and Windows.

## Accounts

Spot-On implements an original two-pass mutual authentication protocol. The implementation is well-defined with or without SSL/TLS. The protocol is weakened if SSL/TLS is neglected, however. Please see the paragraph at the end of this section for additional details regarding the weakness. The Accounts procedure is as follows:

1. Binding endpoints are responsible for defining account information. During the account-creation process, an account may be designated for one-time use. Account names and account passwords each require at least 32 bytes of data.
2. After a network connection is established, a binding endpoint notifies the peer with an authentication request.
3. After receiving the authentication request, the peer responds to the binding endpoint. The peer submits the following information:  $H_{\text{Hash Key}}(\text{Salt} \parallel \text{Time}) \parallel \text{Salt}$ , where the Hash Key is a concatenation of the account name and the account password. The SHA-512 hash algorithm is presently used to generate the hash output. The Time variable has a resolution of minutes. The peer retains the salt value.
4. The binding endpoint receives the peer's information. Subsequently, it computes  $H_{\text{Hash Key}}(\text{Salt} \parallel \text{Time})$  for all of the accounts that it possesses. If it does not discover an account, it increments Time by one minute and performs an additional search. If an account is discovered, the binding endpoint creates a message similar to the message created by the peer in the previous step and submits the information to the peer. The authenticated information is recorded. After a period of approximately 120 seconds, the information is destroyed.
5. The peer receives the binding endpoint's information and performs a similar validation process, including the analysis of the binding endpoint's salt. The two salt values must be distinct.

Please note that the Accounts system can be promoted by including an encryption key. The additional key will allow for finer time resolutions.

If SSL/TLS is not employed, the protocol may be exploited. A relay station may record the values in the 3<sup>rd</sup> step and subsequently provide the information to the binding endpoint. The binding endpoint will therefore trust the foreign connection. The recording device may then seize the binding endpoint's response, the values in the 4<sup>th</sup> step, and provide the information to the peer. If the information is accurate, the peer will accept the binding endpoint's response.

## Adaptive Echo

The Adaptive Echo is a complement to the Echo Protocol and substantiates the opinion that the Echo Protocol is a tensile method. Endpoints that bind multiple parties may optionally define Adaptive Echo tokens. Adaptive Echo tokens are comprised of authentication and encryption keys as well as details about the choice algorithms. If configured, binding endpoints are able to permit or restrict information flow based on the content of the data. As an example, peers that are cognizant of a specific Adaptive Echo token will receive data from other cognizant peers whereas traditional peers will not. Binding endpoints therefore selectively-echo data.

The Adaptive Echo behaves as follows:

1. A binding endpoint defines an Adaptive Echo token. The information must be distributed securely.
2. A networked peer having the given Adaptive Echo token generates  $H_{\text{Hash Key}}(E_{\text{Encryption Key}}(\text{Message} \parallel \text{Time})) \parallel E_{\text{Encryption Key}}(\text{Message} \parallel \text{Time})$  where the Encryption Key and Hash Key are derived from the Adaptive Echo token. The generated information is then submitted to the binding endpoint as Message  $\parallel$  Adaptive Echo Information.
3. The binding endpoint processes the received message to determine if the message is tagged with a known Adaptive Echo token. If the message is indeed tagged correctly, the Time value is inspected. If the Time value is within five seconds of the binding endpoint's local time, the message is considered correct and the peer's presence is recorded.
4. As the binding endpoint receives messages from other peers, it inspects the messages to determine if the messages have been tagged with Adaptive Echo tokens. This process creates a network of associated peers. Because peers themselves may be binding endpoints, the Adaptive Echo may be used to generate an artificial trust network.

Adaptive Echo is susceptible to eavesdropping. As an example, if a message tagged with an Adaptive Echo token should travel through one or more peers to reach a destination, the peers may record the message and consequently replay the message to a binding peer. The replay must occur within the acceptance window of the message. Additionally, the binding endpoint's congestion control container must not already contain the message. If both conditions are met, the binding endpoint will consider the peer as trustworthy.

## **Block Cipher Modes of Operation**

Spot-On uses CBC with CTS to provide confidentiality. The file encryption mechanism supports the GCM algorithm, without authenticity. To provide authenticity, the application uses the encrypted-then-MAC (EtM) approach. The Encrypted and Authenticated Containers section provides more details.

## **Communication Methods**

Spot-On supports SCTP, TCP, and UDP communication methods. For TCP-based communications, OpenSSL is supported. Spot-On distributes data securely with or without SSL/TLS. Please note that magnet distribution violates this principle and therefore requires SSL/TLS. Communications between the Spot-On Kernel and the Spot-On User Interface also require SSL/TLS via TCP. In essence, the application is generally method-neutral.

## **Constant-Time Comparison Function**

Spot-On attempts to utilize constant-time byte comparison functions so as to avert timing analysis.

## **Echo Protocol**

Spot-On introduced the Echo Protocol. The Echo is a malleable protocol. That is, the protocol does not require rigid implementation details. Each model may adhere to their own peculiar obligations. The Echo functions on the elementary persuasion that information is dispersed over multiple or singular passages and channel endpoints evaluate the suitability of the received data. Because data may become intolerable, Spot-On implements its own congestion control algorithm. Received messages that meet some basic criteria are labeled and duplicates are discarded. Advanced models may define more sophisticated congestion-avoidance algorithms based upon their interpretations of the Echo.

Spot-On provides two modes of operation for the general Echo Protocol, Full Echo and Half Echo. The Full Echo permits absolute data flow. The Half Echo defines an agreement between two endpoints. Within this agreement, information from other endpoints is prohibited from traveling along the private channel.



## Encrypted and Authenticated Containers

Some of the data that Spot-On retains locally is stored in encrypted and authenticated containers. CBC and CTS encryption modes are used with a variety of block ciphers. Encryption and authentication occur as follows:

1. Append the size of the provided data to the original container.
2. Encrypt the augmented data via the selected cipher and specified mode.
3. Compute a keyed-hash of the encrypted container.
4. Concatenate the hash output with the encrypted data,  $H_{\text{Hash Key}}(E_{\text{Encryption Key}}(\text{Data} \parallel \text{Size}(\text{Data}))) \parallel E_{\text{Encryption Key}}(\text{Data} \parallel \text{Size}(\text{Data}))$ .

Spot-On also includes a mechanism for re-encoding data if new authentication and encryption keys are desired.

## Key Derivation

Spot-On uses separate authentication and encryption keys for local data. The key-derivation process is as follows:

1. Generate a cryptographic salt. The size of the salt is configurable.
2. Derive a temporary key via the PBKDF2 function. The hash algorithm, iteration count, passphrase (question/answer), and salt are input parameters to the function. All of the aforementioned parameters are configurable.
3. Using the temporary key from the previous step, derive a new key via the PBKDF2 function. The previous parameters are also used, however, the temporary key replaces the passphrase (question/answer).
4. Separate the derived key into two distinct keys. The encryption key is N bytes long, where N is the recommended key size of the selected cipher. The remaining bytes compose the authentication key. The generated authentication key contains at least 512 bytes.

## Hybrid System

Spot-On implements a hybrid system for authenticity and confidentiality. One portion of the system generates per-message authentication and encryption keys. These two keys are used for authenticating and encapsulating data. The two keys are then encapsulated via the public-key portion of the system. The application also provides a mechanism for distributing session-like keys for data encapsulation. Again, the keys are encapsulated via the public-key system. An additional mechanism allows the distribution of session-like keys via previously-established symmetric keys. Digital signatures are optionally applied to the data. As an example, please consider the following message:  $E_{\text{Public Key}}(\text{Encryption Key} \parallel \text{Hash Key}) \parallel E_{\text{Encryption Key}}(\text{Data}) \parallel H_{\text{Hash Key}}(E_{\text{Encryption Key}}(\text{Data}))$ .

## **Poptastic**

Version 0.17 of Spot-On introduced the Poptastic protocol. The new protocol allows participants to communicate via the IMAP, POP3, and SMTP protocols. The protocol provides a medium for near real-time conversations as well as traditional e-mail. Please note that the protocol does not support the two-way calling mechanism.

## **Public Key Infrastructure**

Spot-On utilizes the libgcrypt and libntru libraries for permanent private and public key pairs. Presently, the application generates ten key pairs during the initialization process. Key generation is optional. Consequently, Spot-On does not require a public key infrastructure.

ElGamal, NTRU, and RSA encryption algorithms are supported. DSA, ECDSA, EdDSA, ElGamal, and RSA signature algorithms are supported. The OAEP and PSS schemes are used with RSA encryption and RSA signing, respectively.

Communications between nodes having diverse key types are well-defined if the nodes share common libgcrypt and libntru libraries.

Non-NTRU private keys are evaluated for correctness via the `gcry_pk_testkey()` function. Public keys must also meet some basic criteria such as including the public-key identifier.

## **Two-Way Calling**

Spot-On implements a plain two-pass key-distribution system. The protocol is defined as follows:

1. A peer generates 128-bit AES and 256-bit SHA-512 keys via the system's cryptographic random number generator.
2. Using the destination's public key, the peer encapsulates the two keys via the hybrid cryptographic system.
3. The destination peer receives the data, records it, and generates separate keys as in step 1.
4. The destination peer transmits the encapsulated keys to the originating peer as in step 2.

Once the protocol is executed, the two peers shall possess identical authentication and encryption keys. Please note that duplicate half-keys are allowed.