Onion Routing

Submitted By,

Harikrishnan S

Ramji Nagariya

Sai Sambhu J

Motivation

- Public Network

  "*Encryption does not hide Routing Information*"

- Traffic Analysis

  - "*Who is Talking to Whom?*" by analyzing the traffic pattern instead of data that is sent.
  - Reveals Identities.

Motivation(contd.)

- Anonymity may be desired.
  - Existence of Inter company collaboration.
  - Email users do not want to disclose whom they are contacting to Rest of World etc..

Motivation(contd.)

- Need For System that is
  - ✓ Complicates traffic analysis.
  - ✓ Separates Identification from Routing.
  - ✓ Also supports many different applications.

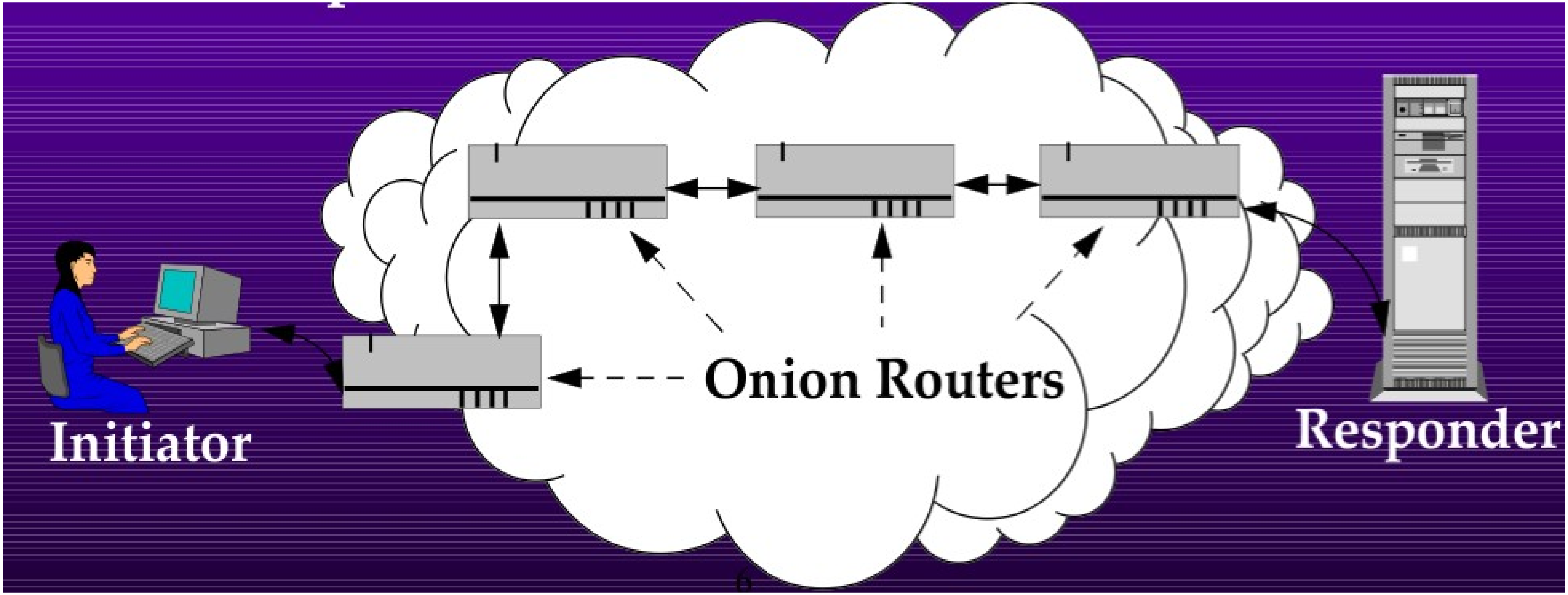
Onion Routing

- Limits Network's vulnerability to Traffic Analysis by separating identification from routing.
- Onion routing provides anonymous connections that are resistant to both eavesdropping and traffic analysis.
- Instead of containing source and destination information, packets moving along an anonymous connection contain only next hop and previous hop information.

Onion Routing(Contd.)

- Consist Of two parts
  - Network Infrastructure.
    - Carries Anonymous Connection.
  - Proxy Interface.
    - Uses this connections to applications.

Onion Routing – Network Infrastructure.



Network Infrastructure

- Onion Routers talk to their neighbors.
- Neighboring Onion Routers are neighbors for onion routing only.
- Between the Onion Routers the link is encrypted.
- Anonymous Connection is established through neighboring routers.
- Each Router Passes Data to one another after applying cryptographic operations.

Onion Routing- Proxy Interface

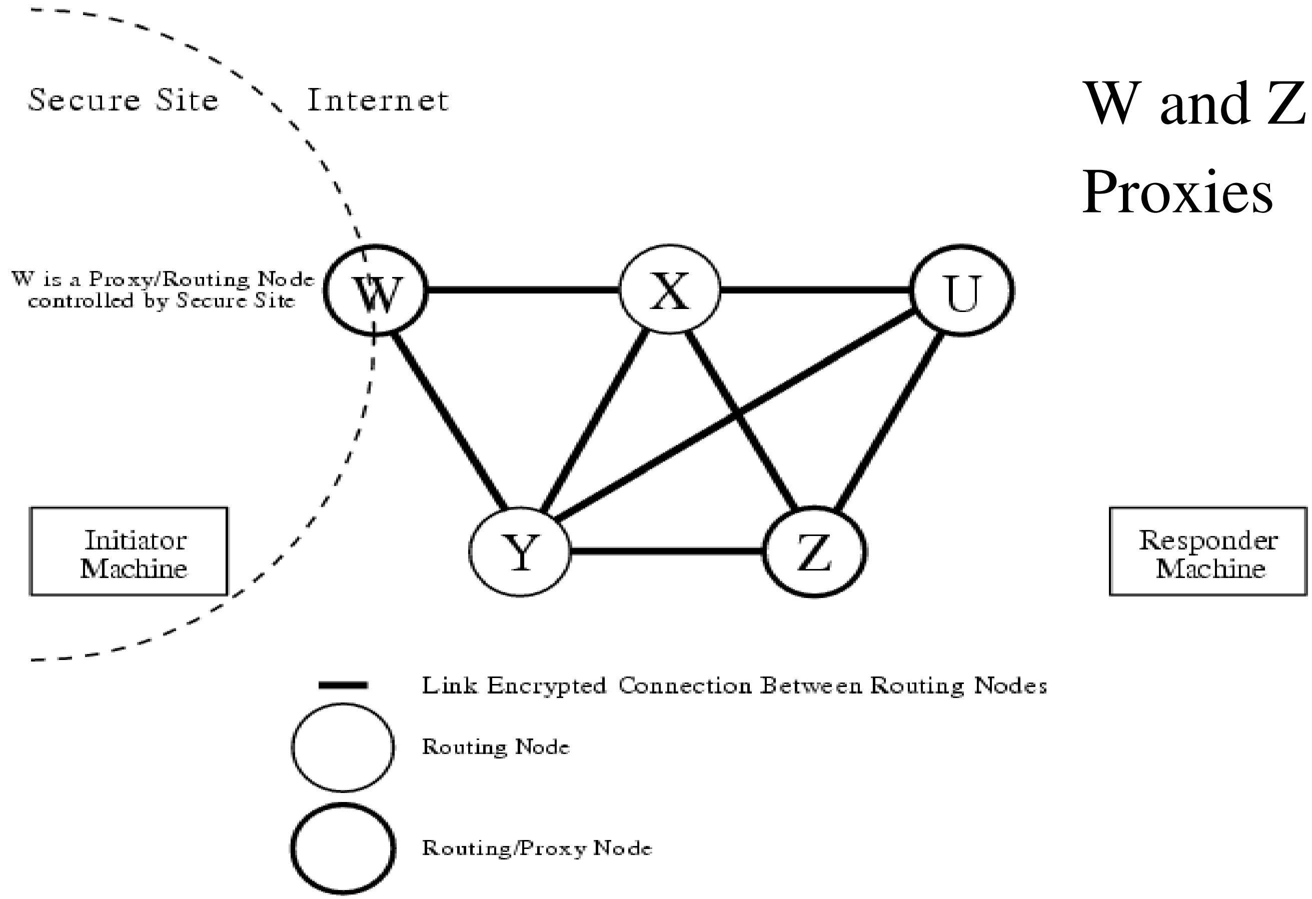

Secure Site
Internet
W is a Proxy/Routing Node controlled by Secure Site
W
X
U
Y
Z
Initiator Machine
Responder Machine
Link Encrypted Connection Between Routing Nodes
Routing Node
Routing/Proxy Node

Fig. 1. Routing Topology.

W and Z are Proxies

Proxy Interface

- Onion Routing Proxy has two functions
  - Links Initiator to anonymous connection.
  - Links anonymous connection to Responder.

- Instead of a single socket connection between an initiator and a responder, onion routing requires a socket connection between the initiator and his proxy, an anonymous connection between the initiator’s proxy and the responders proxy, and a socket connection between the responders proxy and the responder.

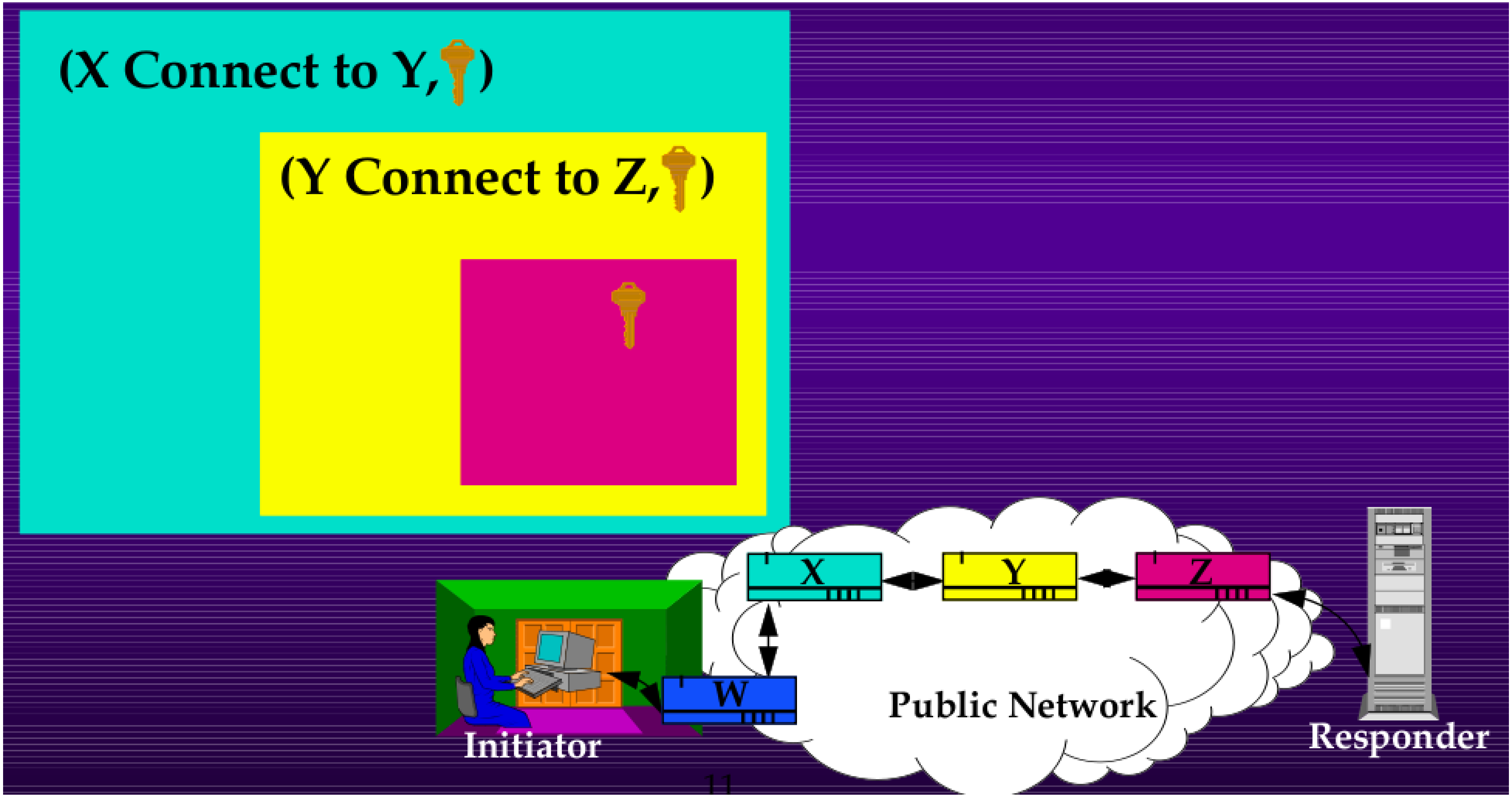
Routing Phases

- Define Route.
- Construct the anonymous connection.
- Move data through the anonymous connection.
- Destroy the anonymous connection.

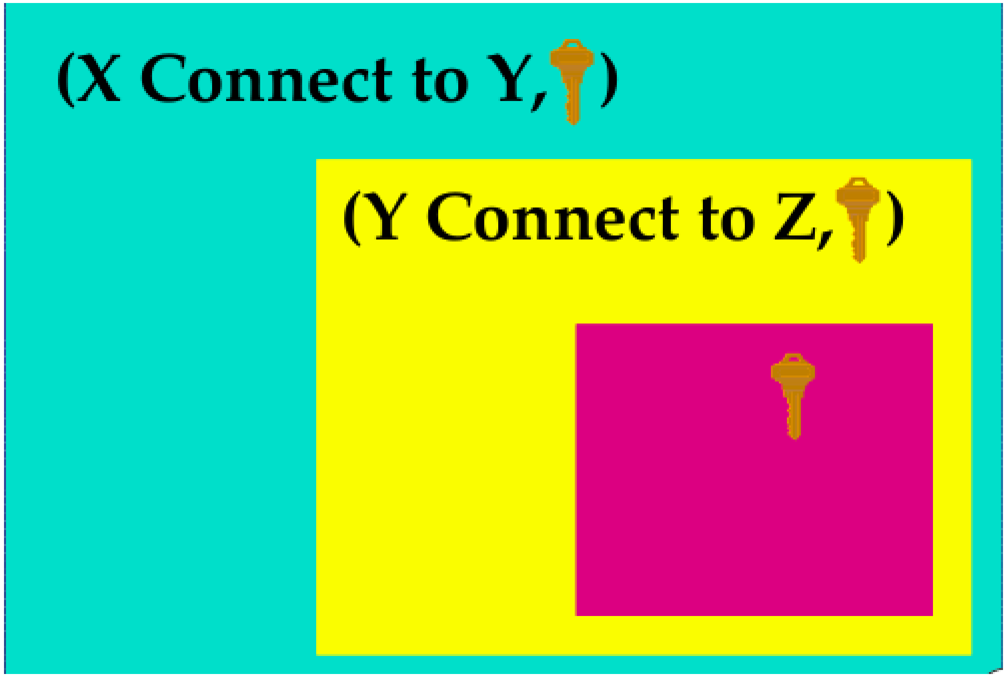
Defining Route

- The Initiator's Proxy chooses to make anonymous connection through the determined route.
- Initiator constructs layered data structure called Onion.

Defining Route(Contd.)



Defining Route(Contd.) - Onion



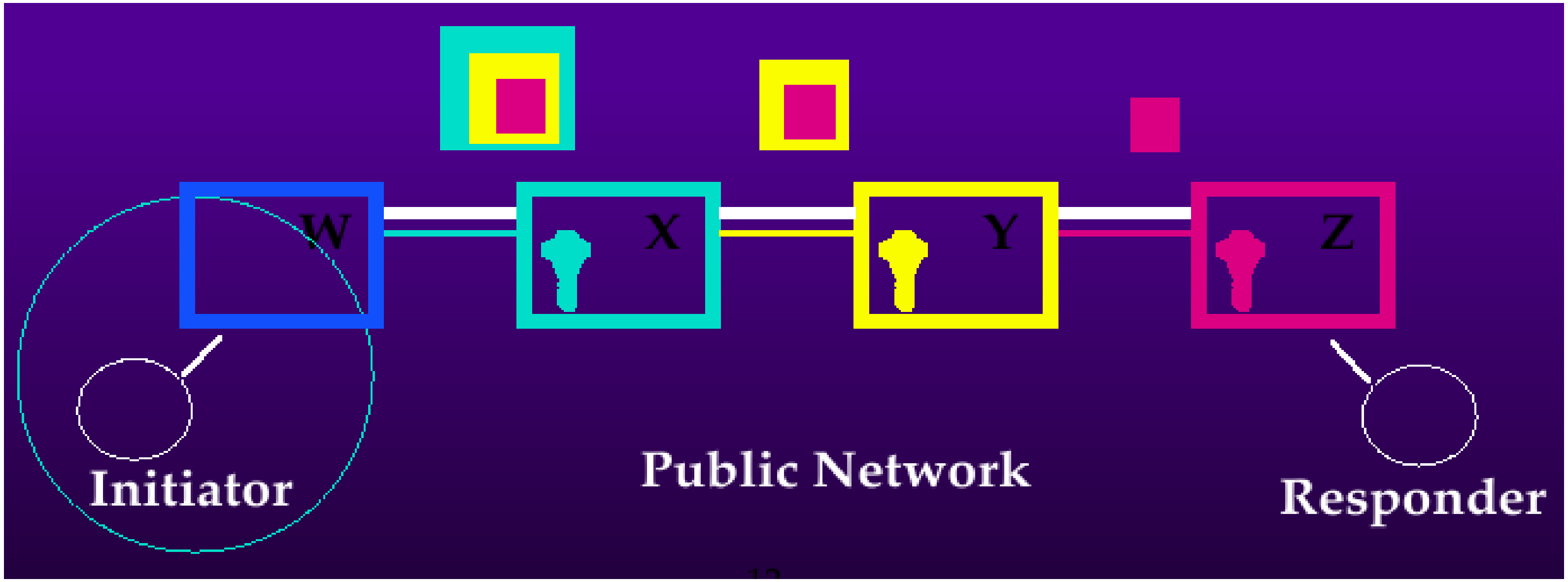
Each Layer of Onion is intended to a particular Onion Router.

Each Layer of Onion is constructed using public key cryptography so only intended onion router can peel it.

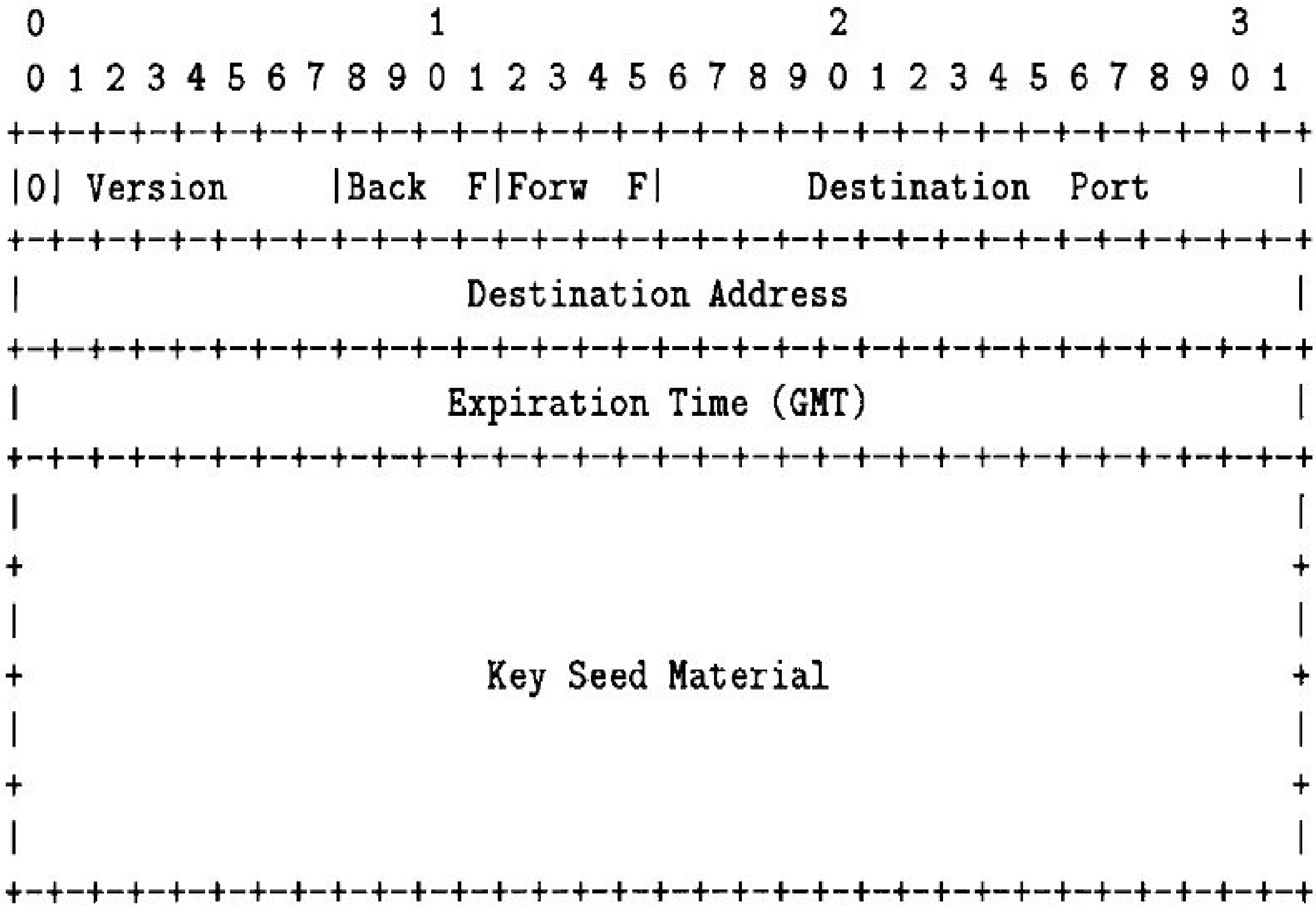
"As data move through the network it appears different to each onion router. Therefore, an anonymous connection is as strong as its strongest link, and even one honest node is enough to maintain the privacy"

Construct anonymous connection

The Initiator Constructs the onion and sends the onion to the Onion Routers through CREATE command.



Single Onion Layer Format



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0| Version     |Back  F|Forw  F|      Destination  Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Destination Address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Expiration Time (GMT)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                       Key Seed Material                       +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

g. 2. A single onion layer.

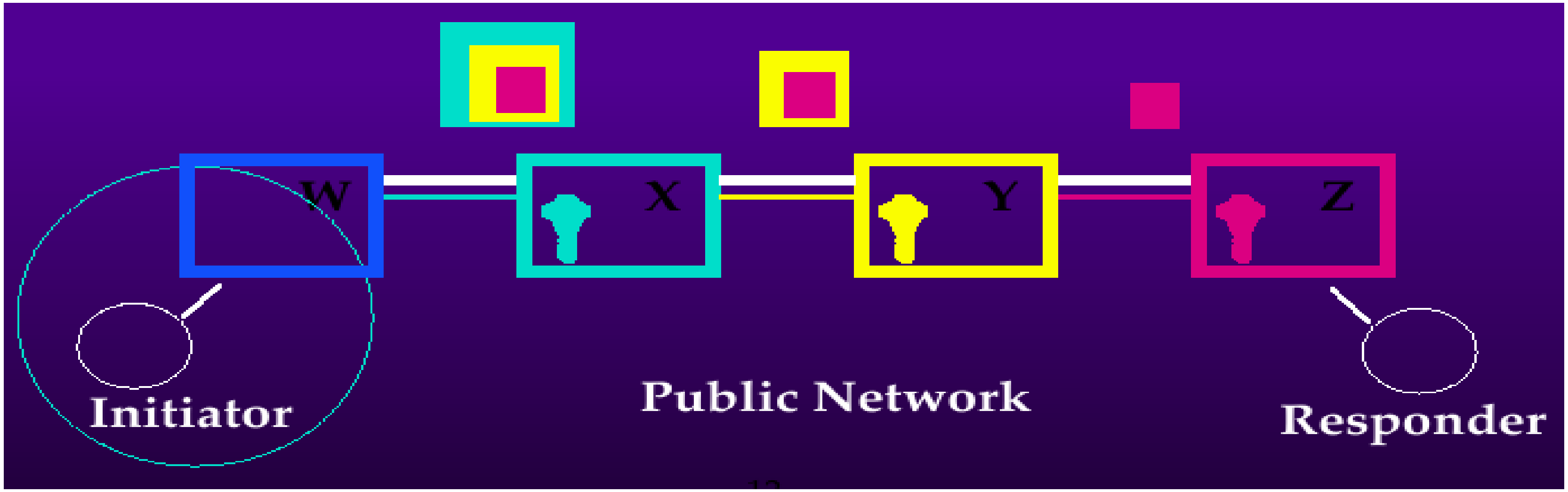
Steps Done by an Onion Router on CREATE message.

- Peels off its layer from the Onion.
- Checks its freshness.
- Generate keys from the seed.
- Get the next hop address.
- Determine the cryptographic operations be done from Back F for backward data transfer and Forw F for forward data transfer.
- Add a mapping between the anonymous connection id and the keys to used on this connection.

Moving Data Forward

Data Sent by Initiator is pre-crypted repeatedly by W , applying the inverse of forward crypt operation specified in the onion(of previous phase), inner most first. And send the data using the DATA message.

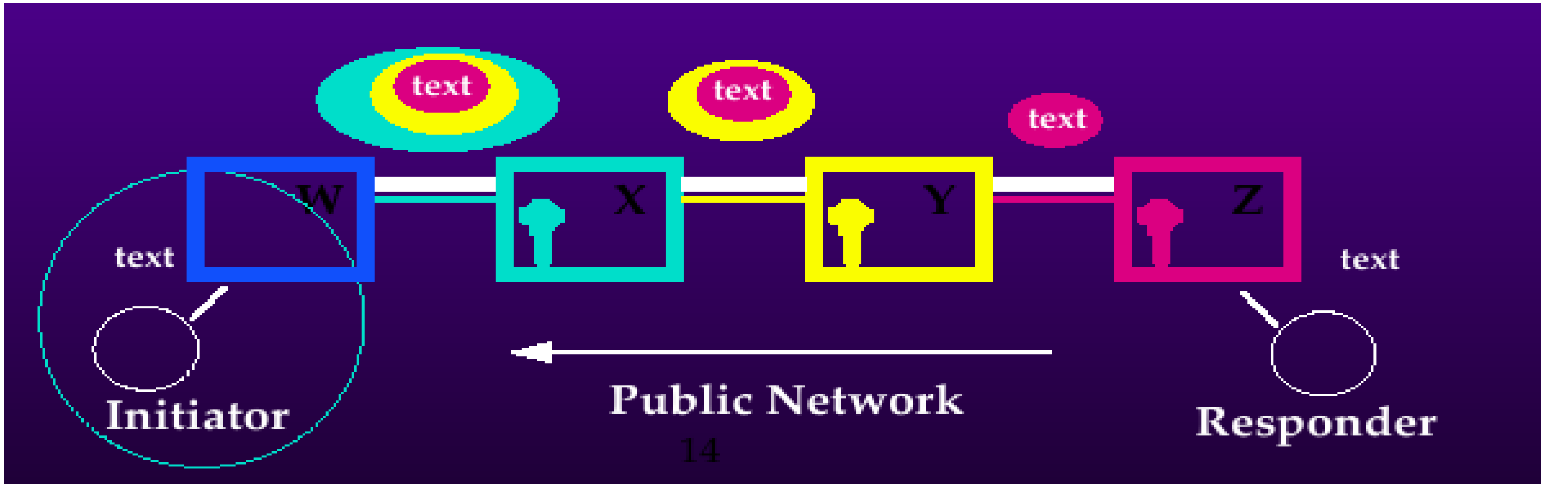
Each of the Onion router removes the crypt information added by initiator by applying the crypt operation using forward key obtained in the first phase.



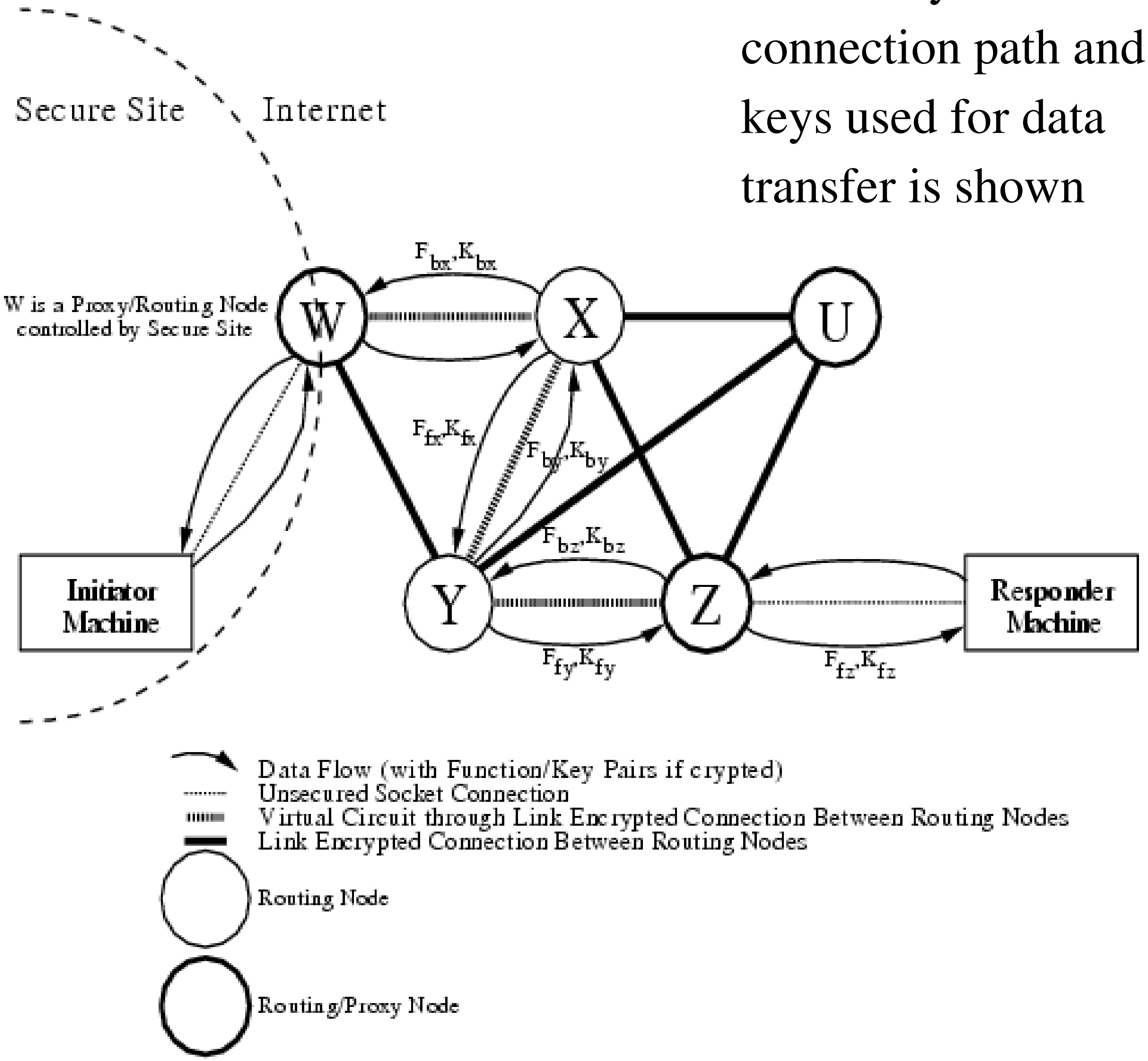
Moving Data Backward

Each of the Onion router crypts the text using backward key obtained in the first phase and send the data using DATA message.

Initiator's proxy applies the inverse of backward crypt operation specified in the onion and sends the plain text to Intiator.



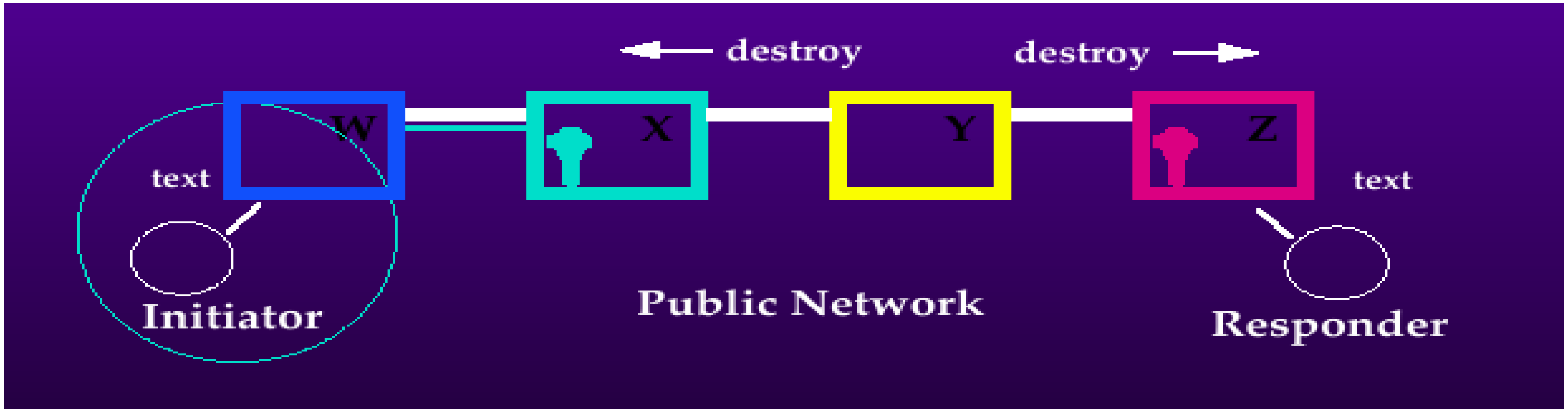
The anonymous connection path and the keys used for data transfer is shown


Secure Site
Internet
W is a Proxy/Routing Node controlled by Secure Site
W
X
U
Y
Z
F_{bx},K_{bx}
F_{fx},K_{fx}
F_{by},K_{by}
F_{bz},K_{bz}
F_{fy},K_{fy}
F_{fz},K_{fz}
Initiator Machine
Responder Machine
Data Flow (with Function/Key Pairs if crypted)
Unsecured Socket Connection
Virtual Circuit through Link Encrypted Connection Between Routing Nodes
Link Encrypted Connection Between Routing Nodes
Routing Node
Routing/Proxy Node

Destroy the anonymous connection

Each of the Onion router maintains the details of the keys , the type of encryption used for each of the anonymous connection.

So each of these resources should be removed while closing the anonymous connection. Achieved by sending DESTROY message.
 Upon receipt of a DESTROY command, it is the responsibility of an onion router to forward the DESTROY appropriately and to acknowledge receipt by sending another DESTROY command back to the previous sender.

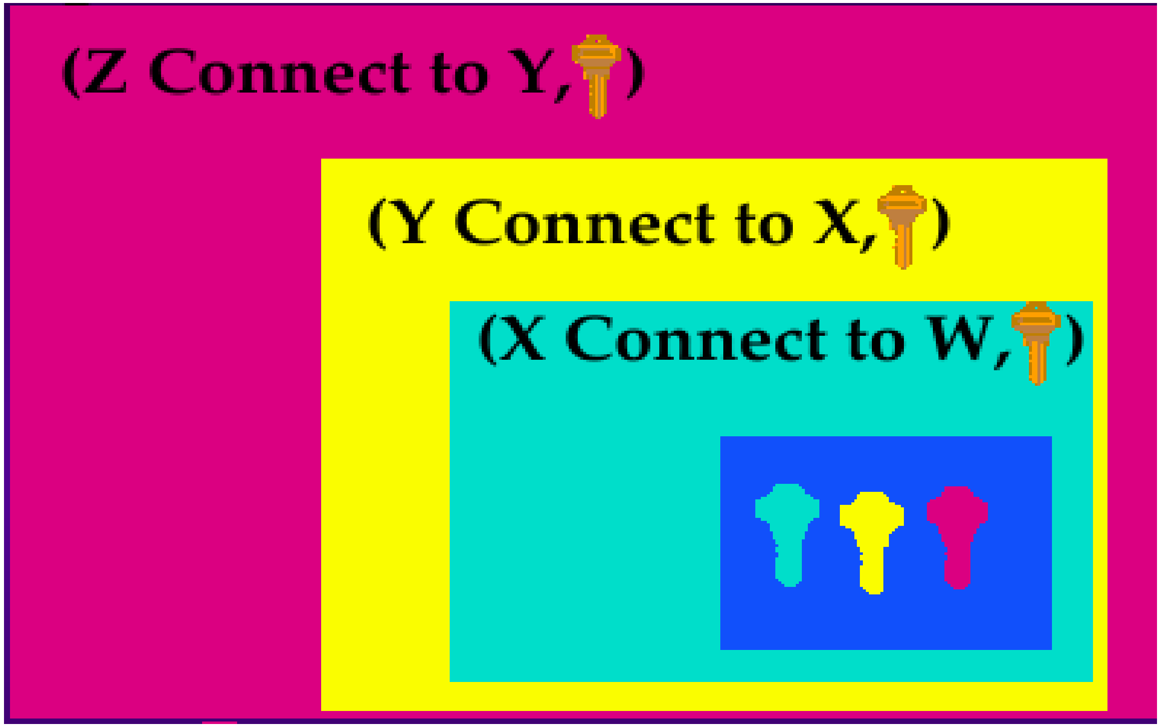


How to send a reply to the initiator after the connection is destroyed?

- ~~Keep anonymous connection open??~~

- Or we can use “ Reply Onions”.

Reply Onion



- An initiator’s onion routing proxy can create a reply onion that defines a route back to it.
- A reply onion can be used by a responder to create an anonymous connection back to the initiator at a later point in time.

Reply Onion Demonstration

(Initiator) -- W <----- X <----- Y <----- Z <---- (Responder)

W, X, Y, Z are onion routers.

- Responder sends reply onion to onion routing proxy Z.
- Z peel off a layer. Gets the key seed intended for itself and an onion to be passed to Y.
- Y peels of the next outermost layer and gets the keyword for itself and an onion.
- This process repeats back until it reaches initiator's proxy.
- This process creates a anonymous connection back to the initiator.

Vulnerabilities

- Timing Attacks
- Intersection Attacks
- Predecessor Attacks

Applications

- Tor
- Decoy Cipher

References

- Anonymous Connections and Onion Routing [Michael G. Reed, Member, IEEE, Paul F. Syverson, and David M. Goldschlag].
- Proxies for Anonymous Routing[Michael G. Reed, Paul F. Syverson, and David M. Goldschlag].
- Hiding Routing Information[Paul F. Syverson, David M. Goldschlag and Michael G. Reed].
- Wikipedia [http://en.wikipedia.org/wiki/Onion_routing]