you.are.all.screwed

the

Luna Correspondence Protocol

aRgus

d4yj4y

sMURFBOy

Why Are We Here?

The security of our world as we know it is at stake. The nature of our project may lend itself to abuse by malicious users, cooperate espionage, and even terrorism. More positive applications include freedom of speech and information under oppressive regimes, and personal privacy on a largely public network.

- Secure, un-traceable, anonymous communication.
- This is the Luna protocol.
- This is our goal.

Abstract

- Luna is a revolutionary new protocol used to anonymously transmit and receive data securely across the Internet.
- Luna is based on finite improbabilities of vast random data dispersal and exploits properties of IP to accomplish a portion of it's goals.

Loki?

Achieving Anonymity

the Luna way

Relaying Trickery

- Luna makes use of well known and existing flaws in network protocols and conventional firewall implementations.
- Luna uses tactics for which logging and filtering would be costly and impractical on high traffic relay hosts.
- When properly implemented, Luna harms no host along it's path, or impairs it's bandwidth.

Host-Level Transmission

Receivers Network

Relay 1

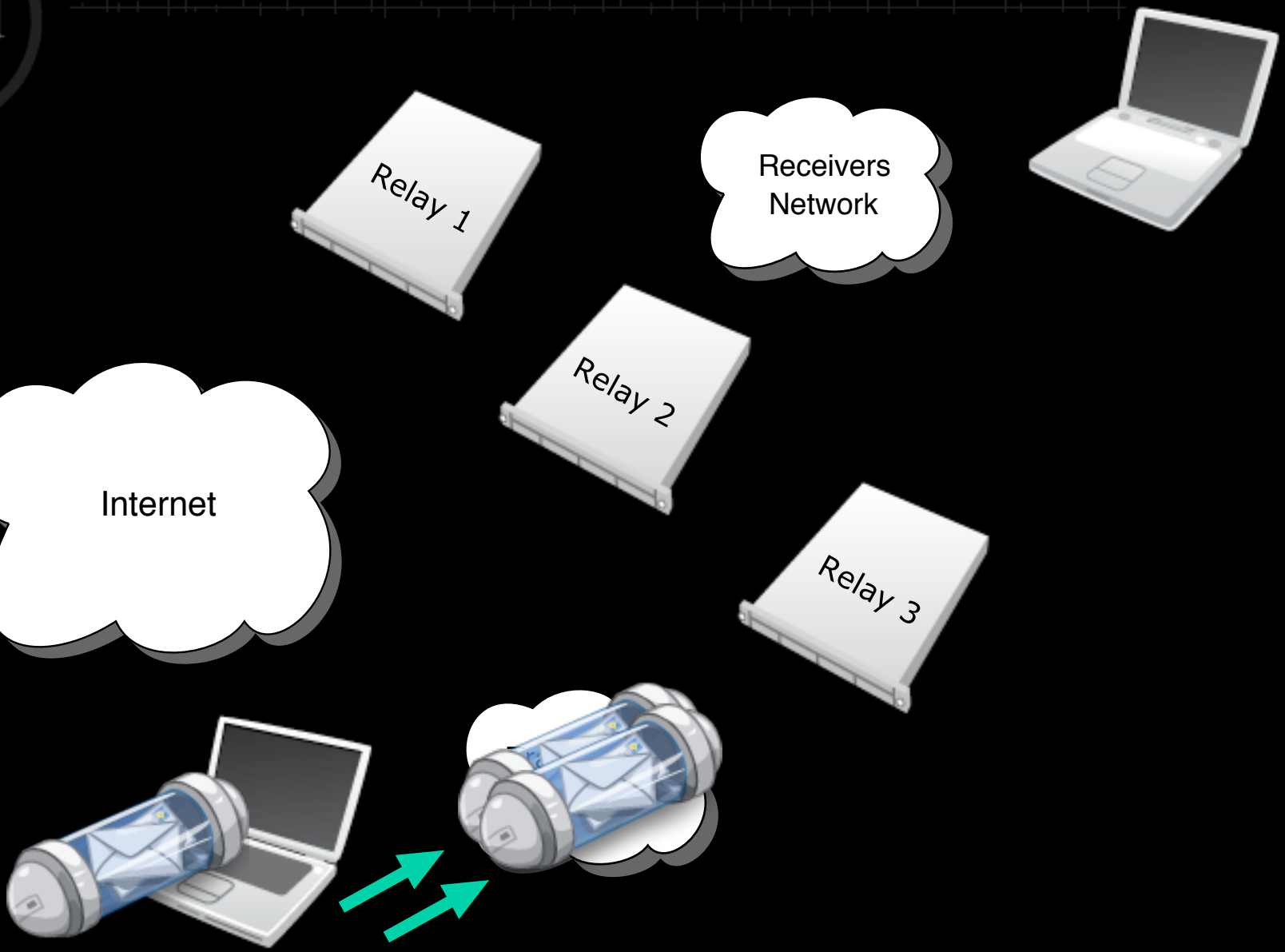
Relay 2

Relay 3

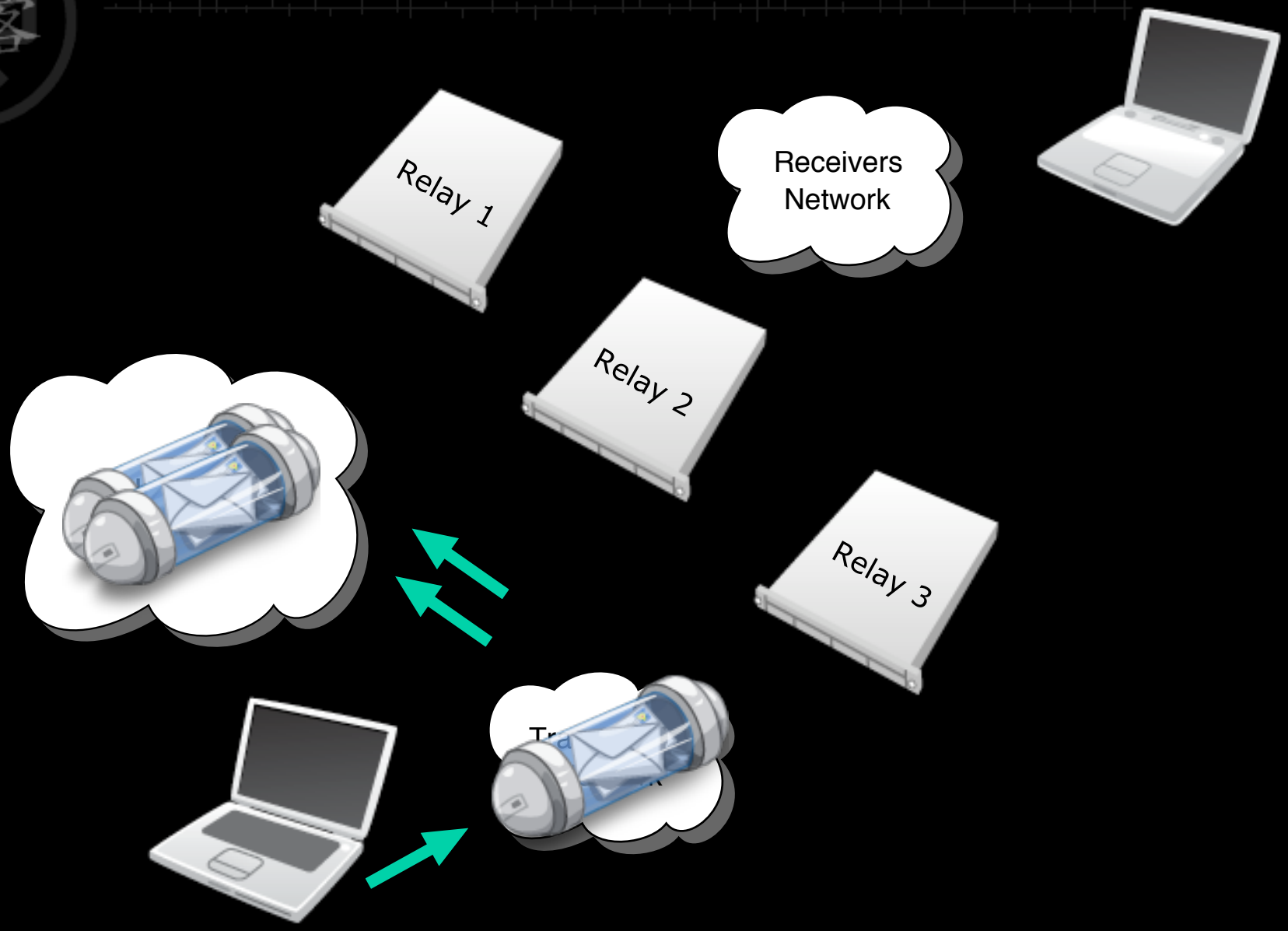
Internet

Transmitters Network

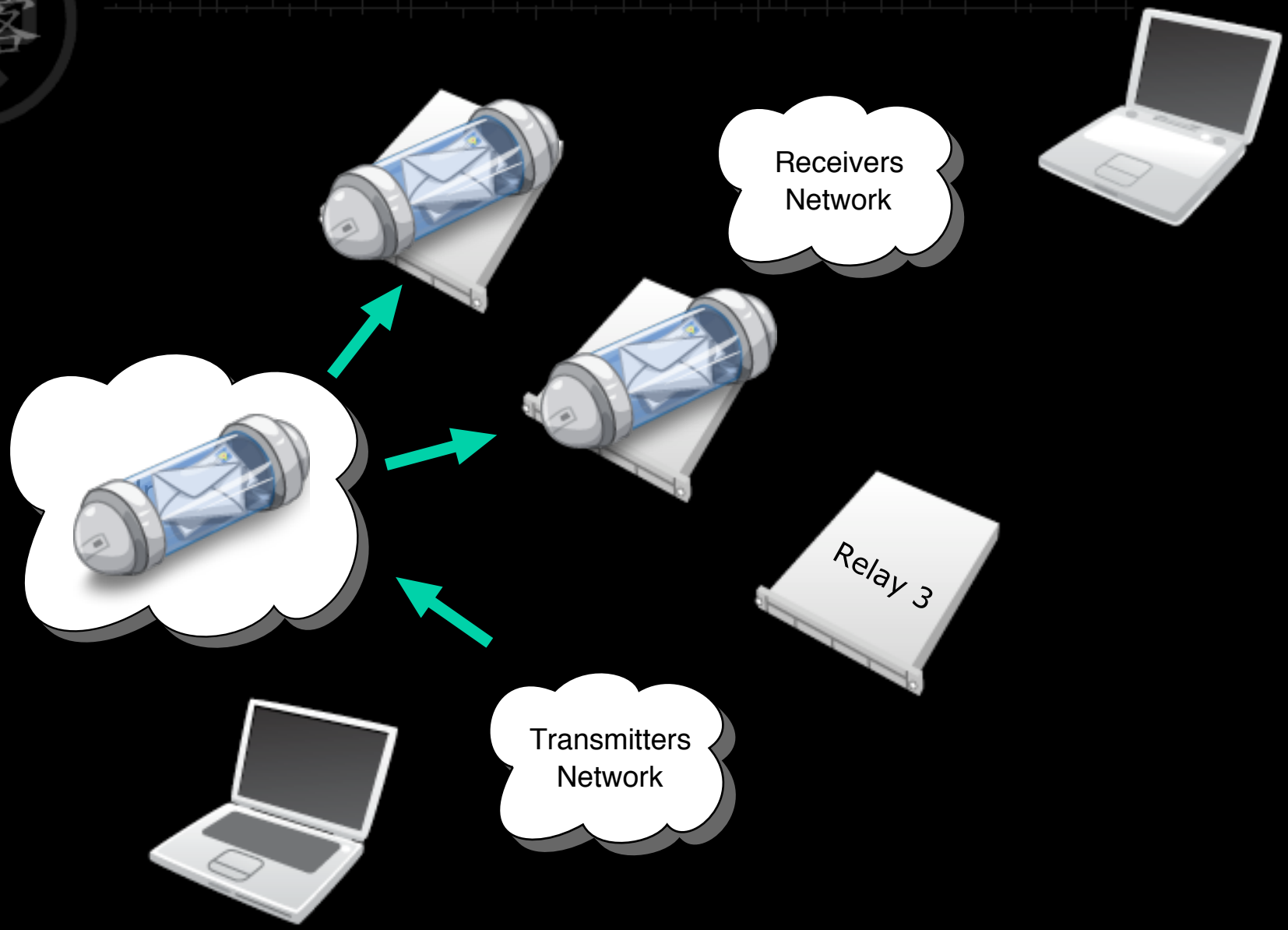
Host-Level Transmission



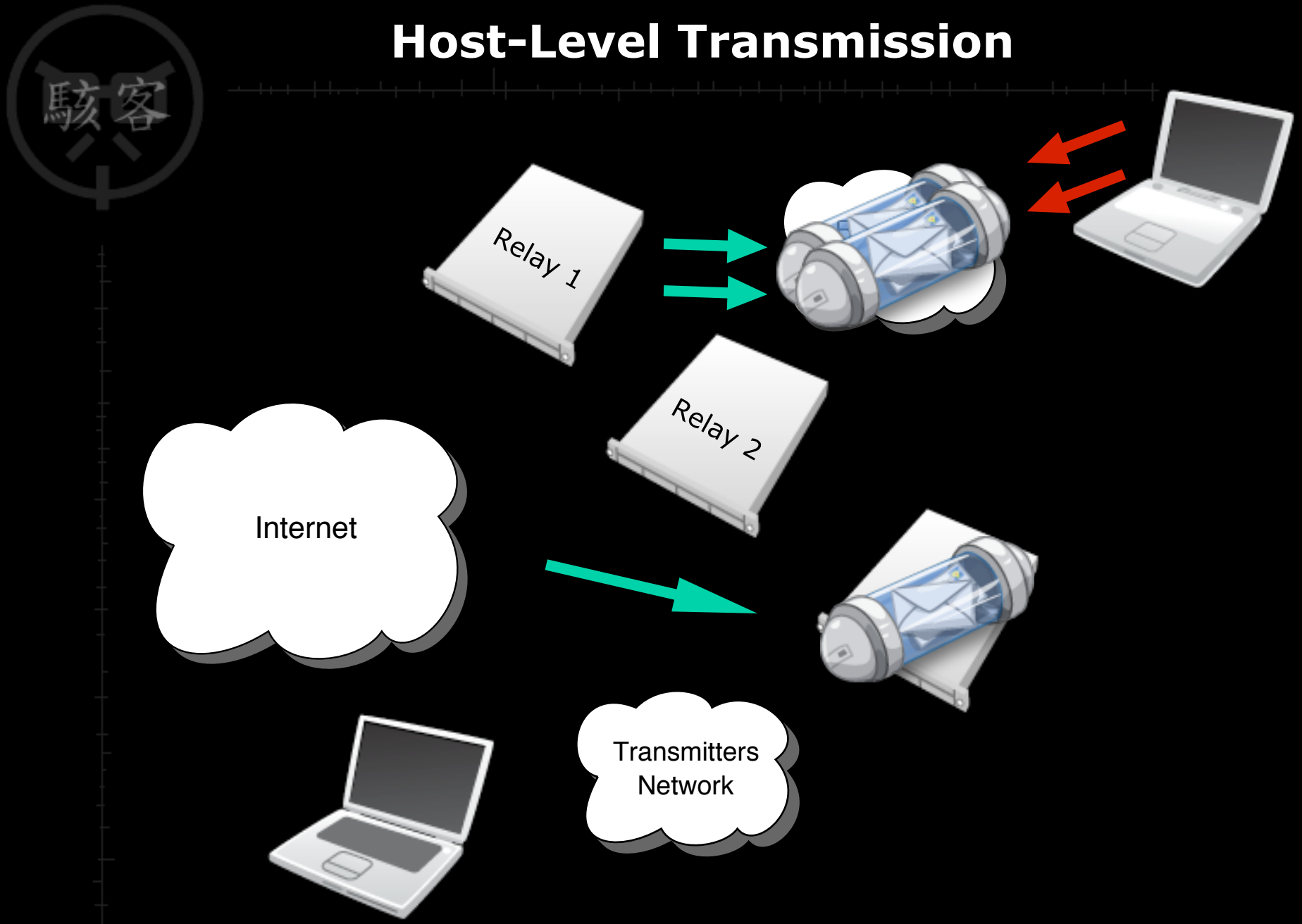
Host-Level Transmission



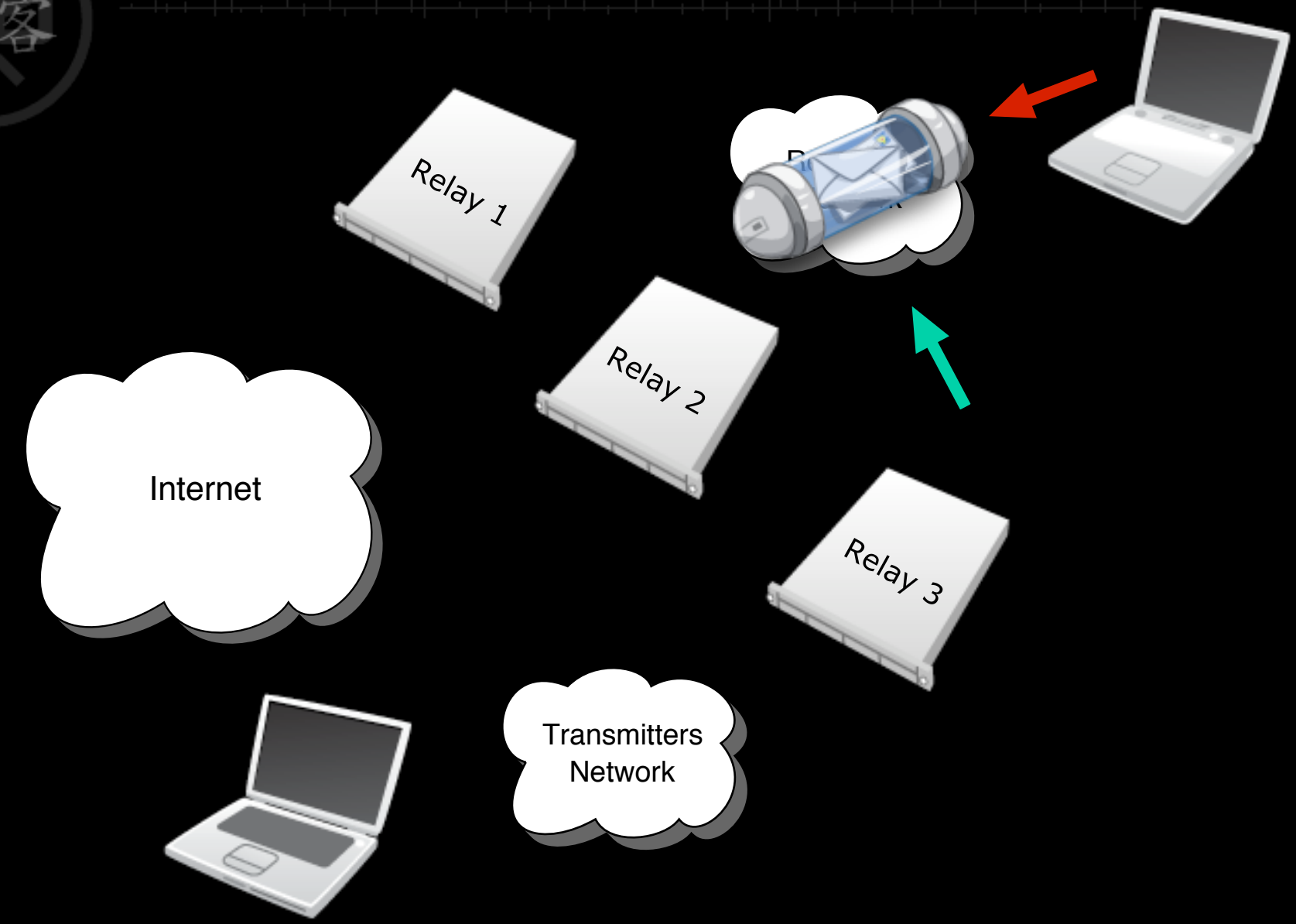
Host-Level Transmission



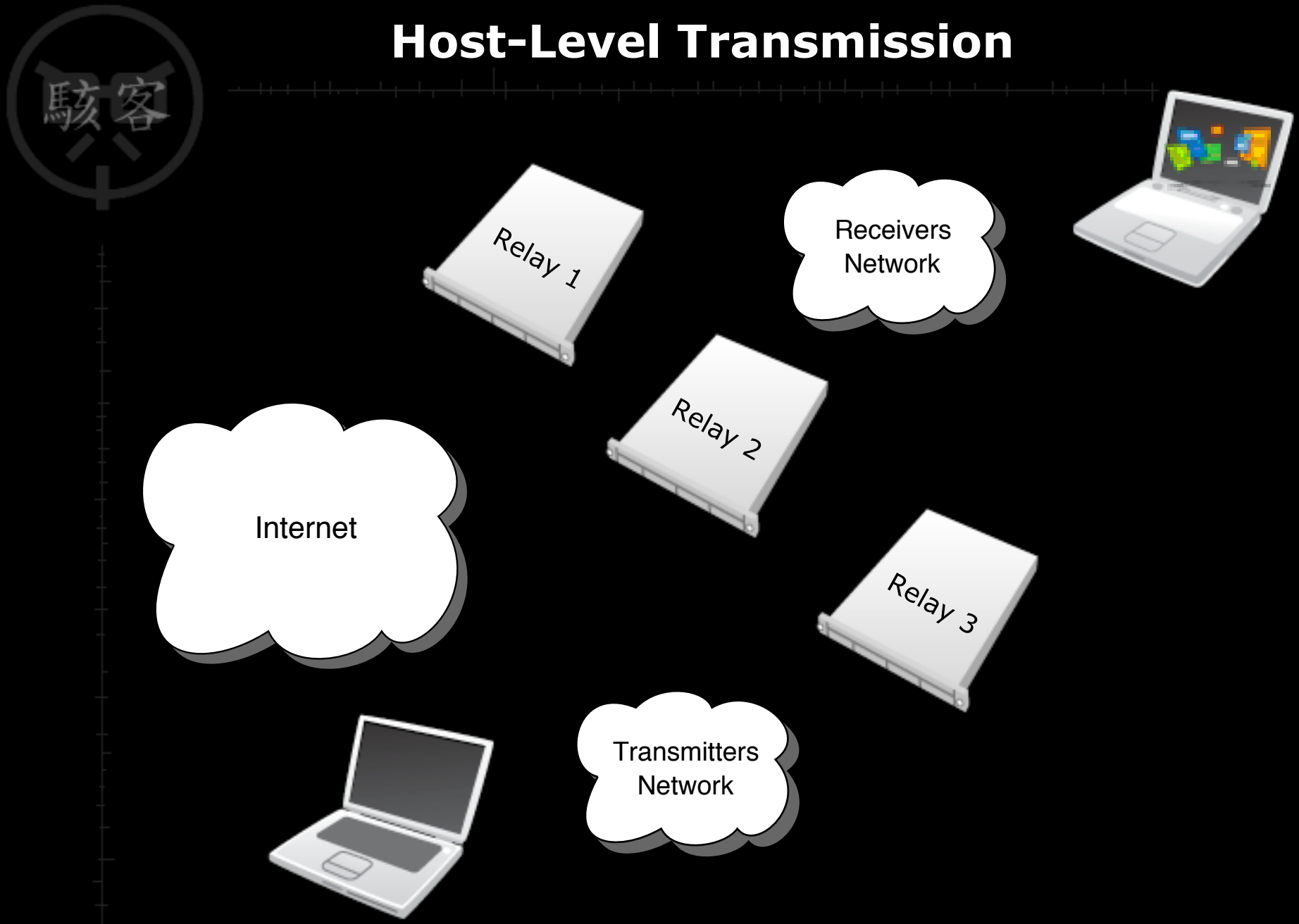
Host-Level Transmission



Host-Level Transmission



Host-Level Transmission



Spoofing

Several means of host deception are employed to facilitate anonymous transfer:

- MAC Address Spoofing (ISO Layer 2)- Luna assumes multiple Media Access Control Addresses.
- IP Address Spoofing (ISO Layer 3)- Luna bounces transmissions off a high traffic 3rd party host using a source address from the target destination.

Achieving Inefficiency

the Luna way

Inefficiency Briefing

- Data must not be sent in a predictable fashion in predictable time
  - Avoid all patterns
- Data must be reordered
  - Avoid all patterns
- Data must be randomized
  - Avoid all patterns
- Data must contain false positives
  - Avoid all patterns

And Then There is Crypto ...

Cryptography is insufficient for primary means of communication, however it is far from trivial.

Achieving Security

the Luna way

Mathematical Permutation Function

$P(n,r) = n! / (n-r)!$

N = total number of packets
R = set of packets composing real data (eliminating bogus packets)

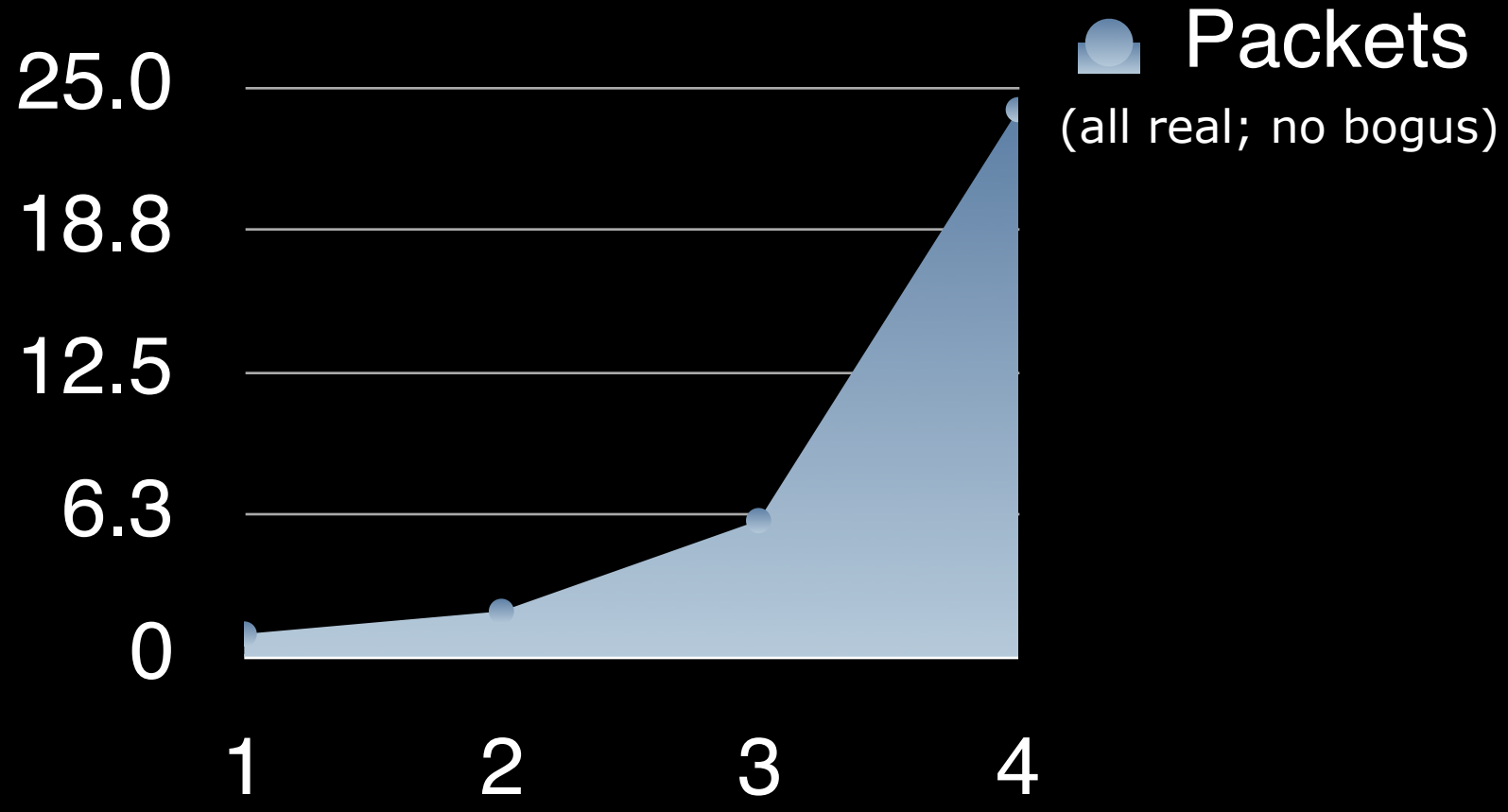
Mathematical Permutation Function

P(60,10) = 60! / (60-10)!
P = 2.735898472+E17

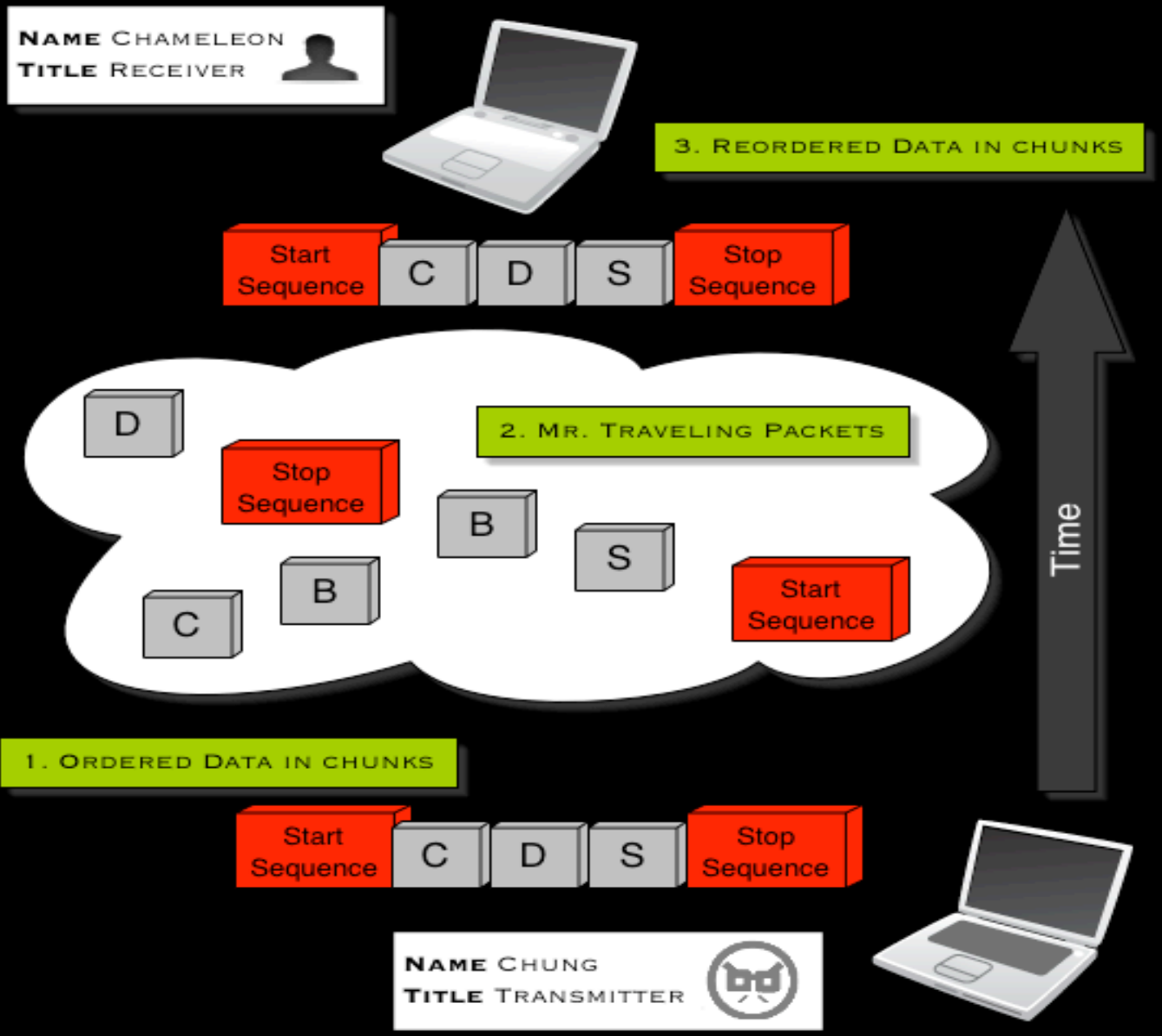
P(100,80) = 100! / (100-10)!
P = Overflow

Arrg. My trusty ti-83 can't comprehend the possibilities of even 100 packets.

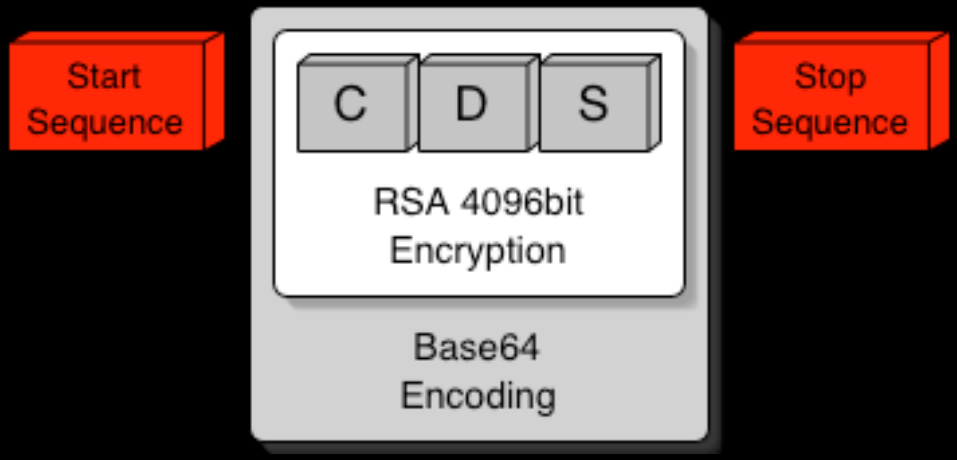
Mathematical Permutation Function



Packet-Level Transmission



Data Filters



- Filters are applied over the entire datum, before it's chunked into packets
- Filter plug-ins can be anything from encryption ciphers such as RSA, PGP, and Blowfish to Base64 and ASCII translation encoding
- Filters are not applied to the start and stop sequences

Multi-Tiered Security

Even if the Luna protocol is cracked or flawed and an encryption data filter is used (Base64 encoding isn't an encryption data filter, it's an encoding data filter), data is still secured by the encryption filters strength. Thus, Luna is at least as strong as the weakest encryption filter used.

Summary

- Achieving inefficiency via The Luna Protocol
  - Packet bleeding
- Achieving anonymity via The Luna Protocol
  - Spoofing
  - Relaying
  - Host-level transmission (OSI Layers 2 and 3)
- Achieving security via The Luna Protocol
  - Mathematical Formula
  - Packet-level transmission (OSI Layer 5)
  - Data filters

Chung's Final Thoughts

"There is no tool that makes up for a lack of knowledge or poor implementation."
- aRgus Chung 2003

"The west side is the best side."
- d4yj4y Chung 2003

"Live and learn; no one is above making mistakes."
- sMURFBOy Chung 2003

To The Moon!

the Luna way

Forward Pointers

- Government IP_TAPPING by Jaya Baloo
  Today @ 5:00-5:50
- Airsnarf by Beetle & Bruce Potter
  Tomorrow @ 2:00-2:50
- Technical Security Countermeasures by Jeffrey Prusan
  Sunday @ 2:00-2:50

Acknowledgments

- The moon bounce team. Saqib @ SystemV
- The infamous Mr. Tang for the genius mathematical guidance
- Douglas Adams and the meaning of life: 42; R.I.P
- YOU for the support--thank you very much

Rosco’s for the chicken and waffles

Live Demo

Q & A