# Badge of Shame

Breaking into Secure Facilities with OSDP



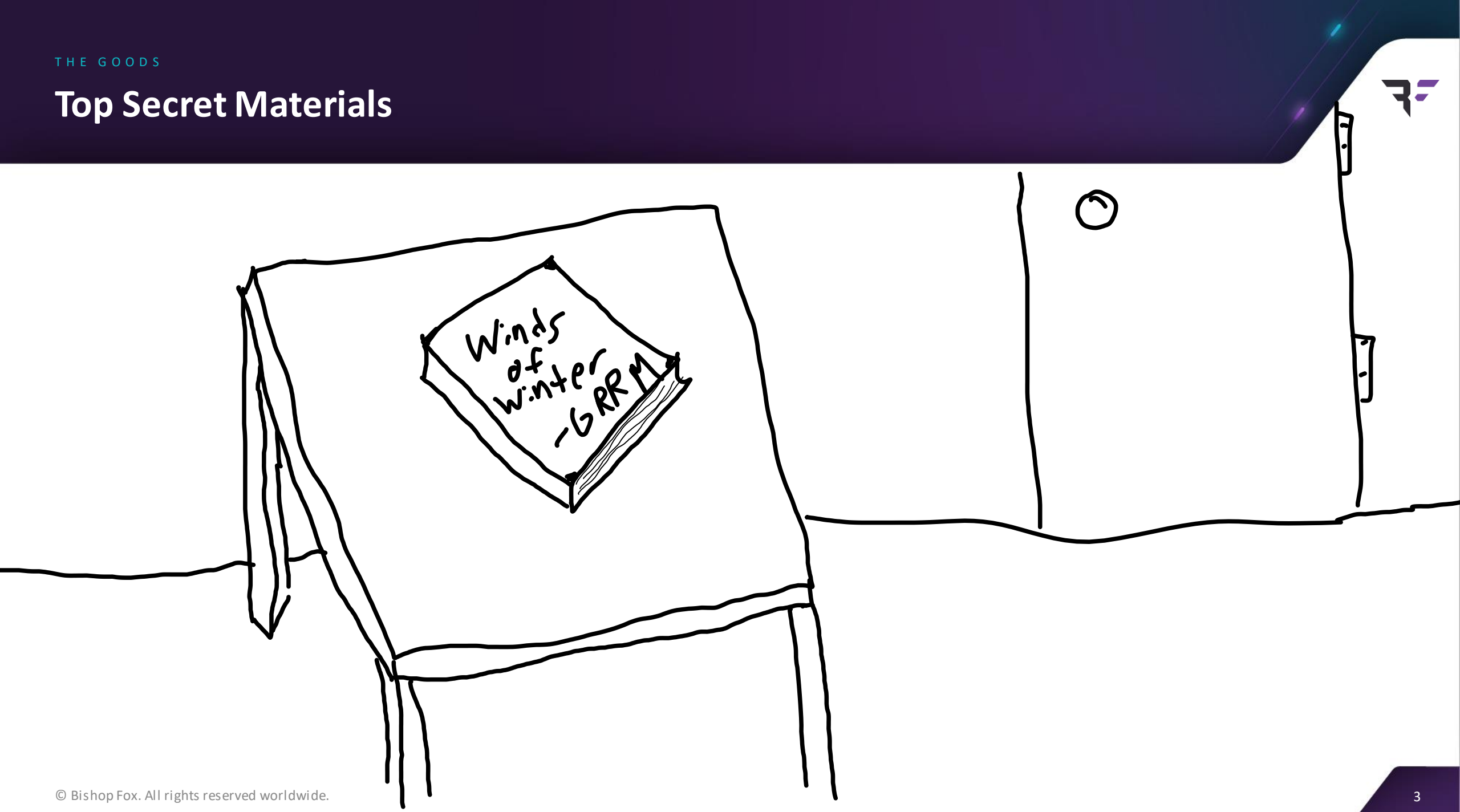
BISHOPFOX

# Secure Facility




© Bishop Fox. All rights reserved worldwide.

# Top Secret Materials



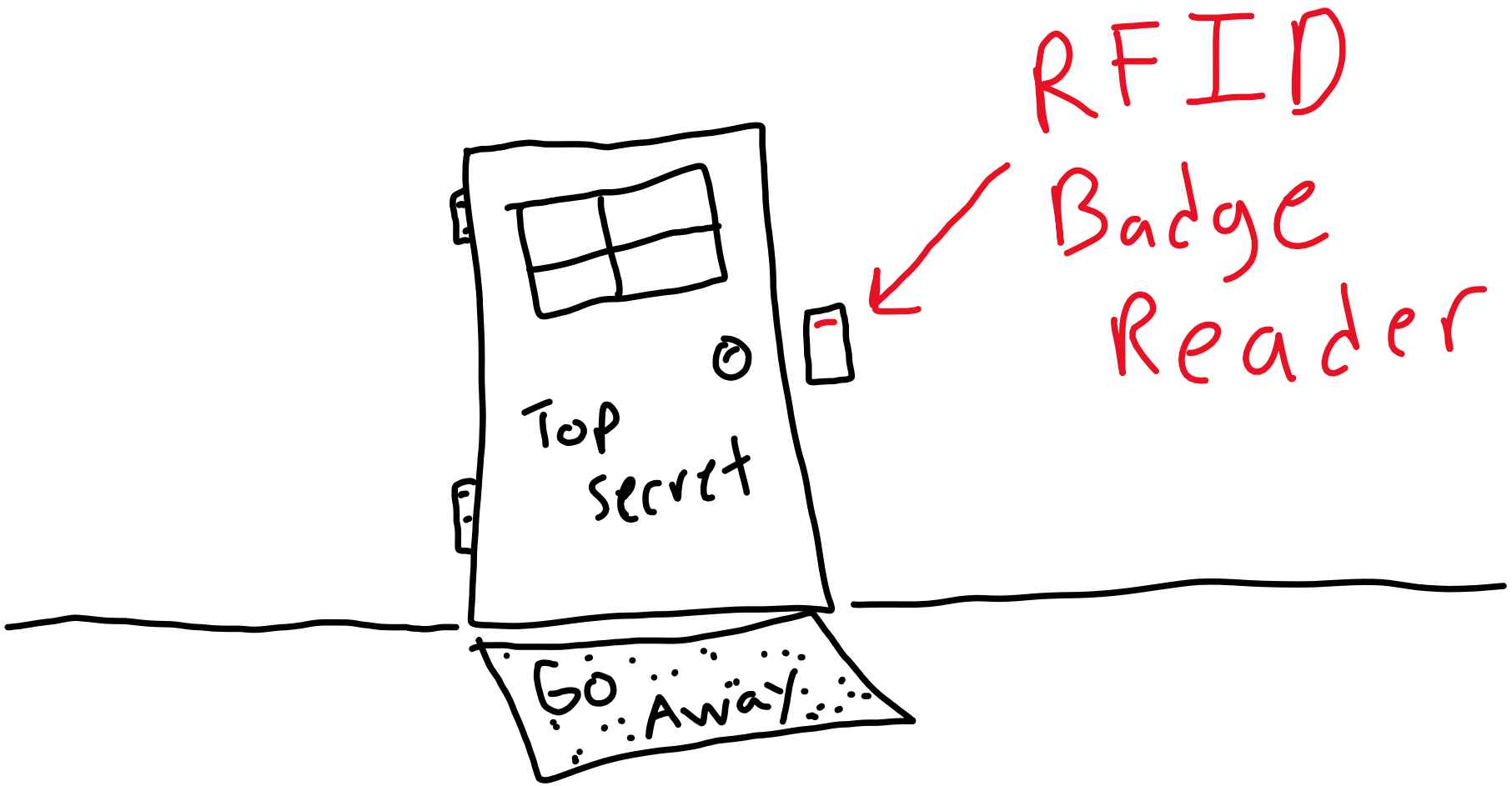

© Bishop Fox. All rights reserved worldwide.

# OSDP




© Bishop Fox. All rights reserved worldwide.

# OSDP




© Bishop Fox. All rights reserved worldwide.

# Other Ways to Hack RFID



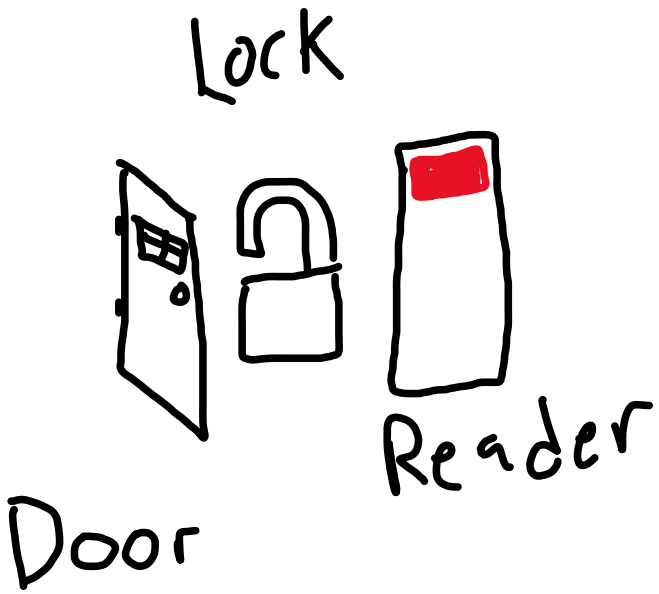

Tastic RFID Thief




I made this!

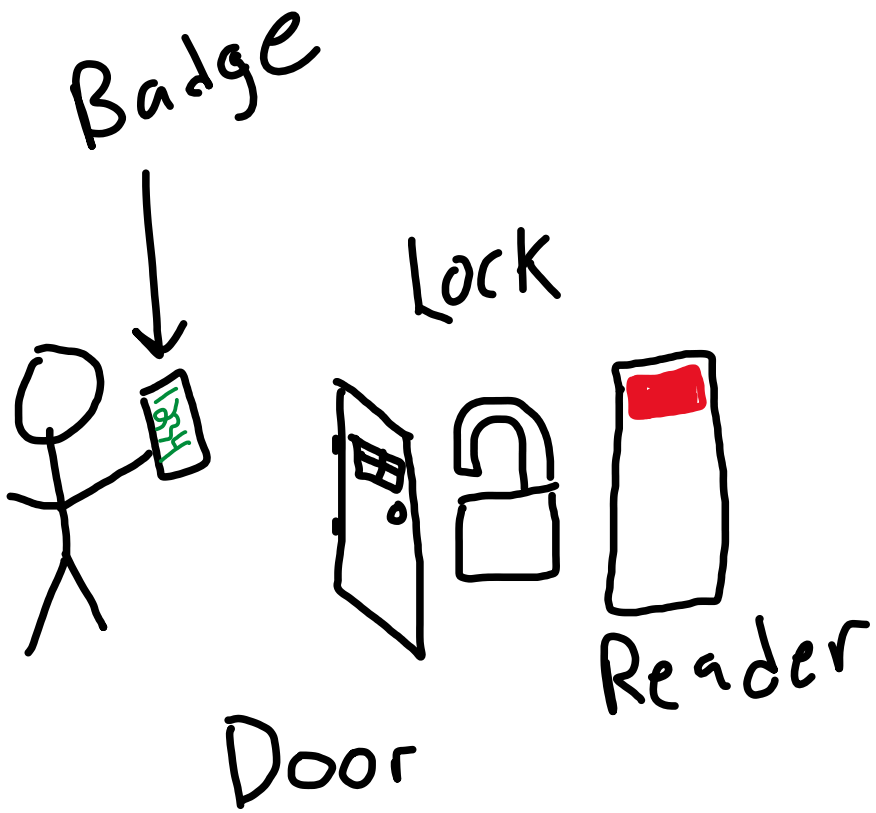
© Bishop Fox. All rights reserved worldwide.

# RFID Badge Setup



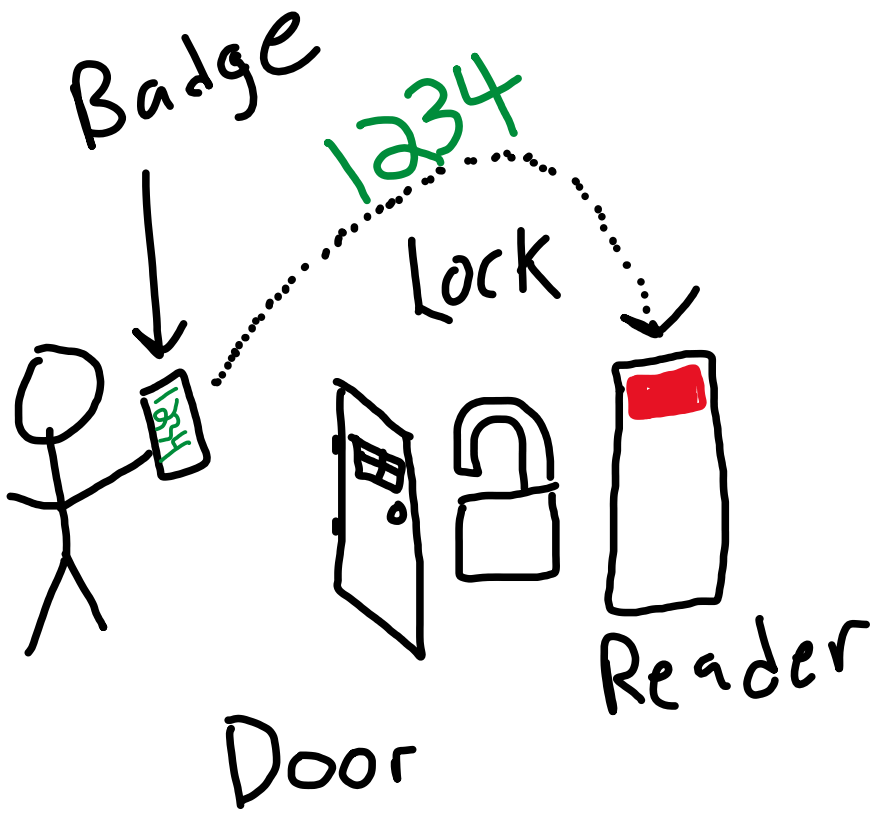

© Bishop Fox. All rights reserved worldwide.

# RFID Badge Setup



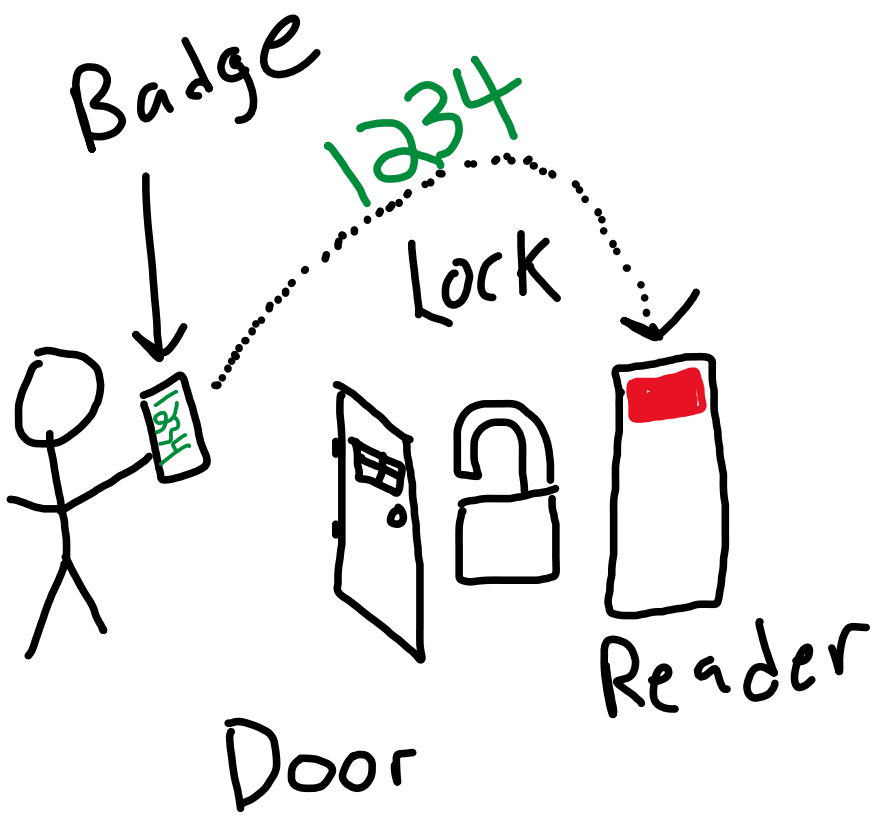

© Bishop Fox. All rights reserved worldwide.

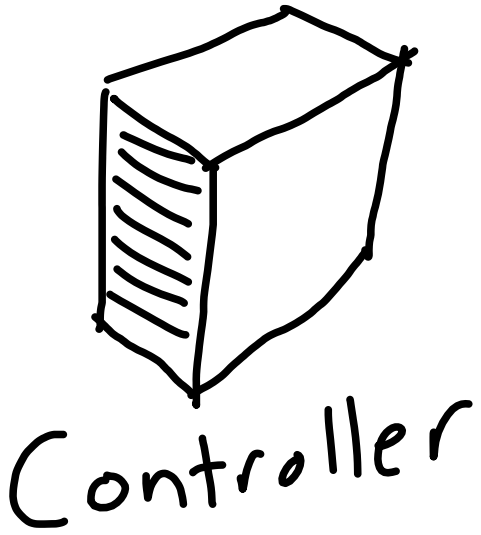
# RFID Badge Setup




© Bishop Fox. All rights reserved worldwide.

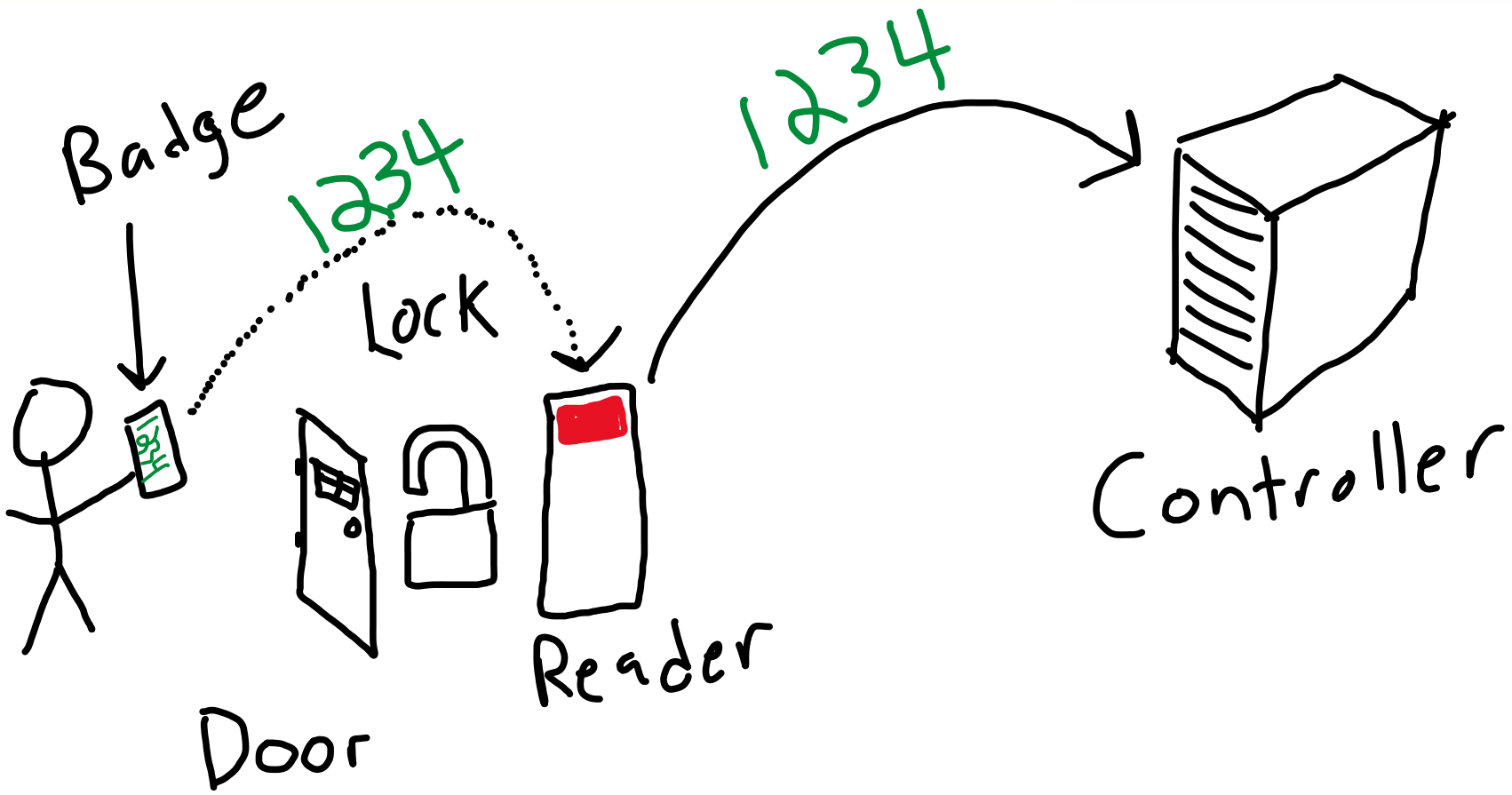
# RFID Badge Setup



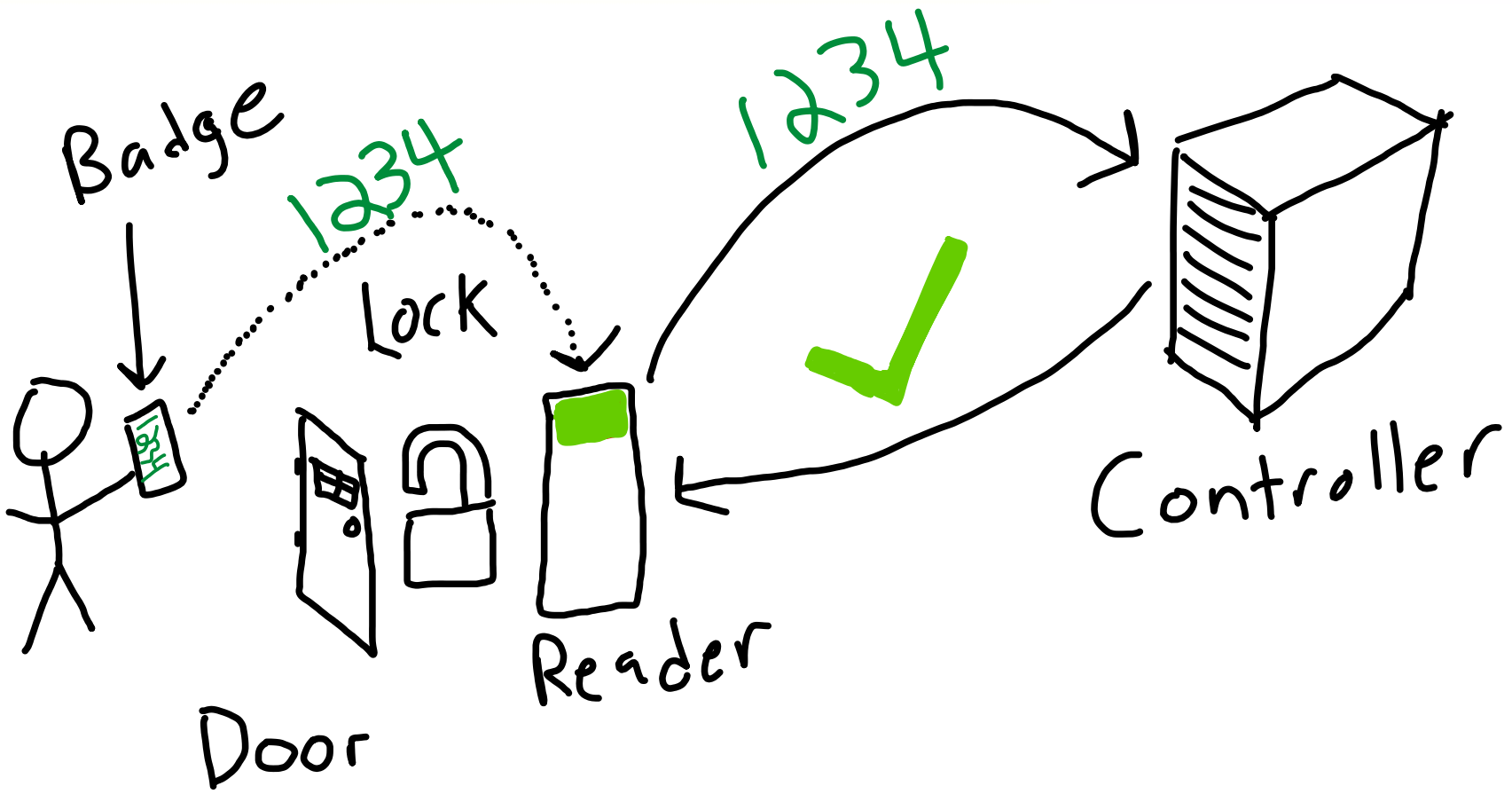

© Bishop Fox. All rights reserved worldwide.

# RFID Badge Setup



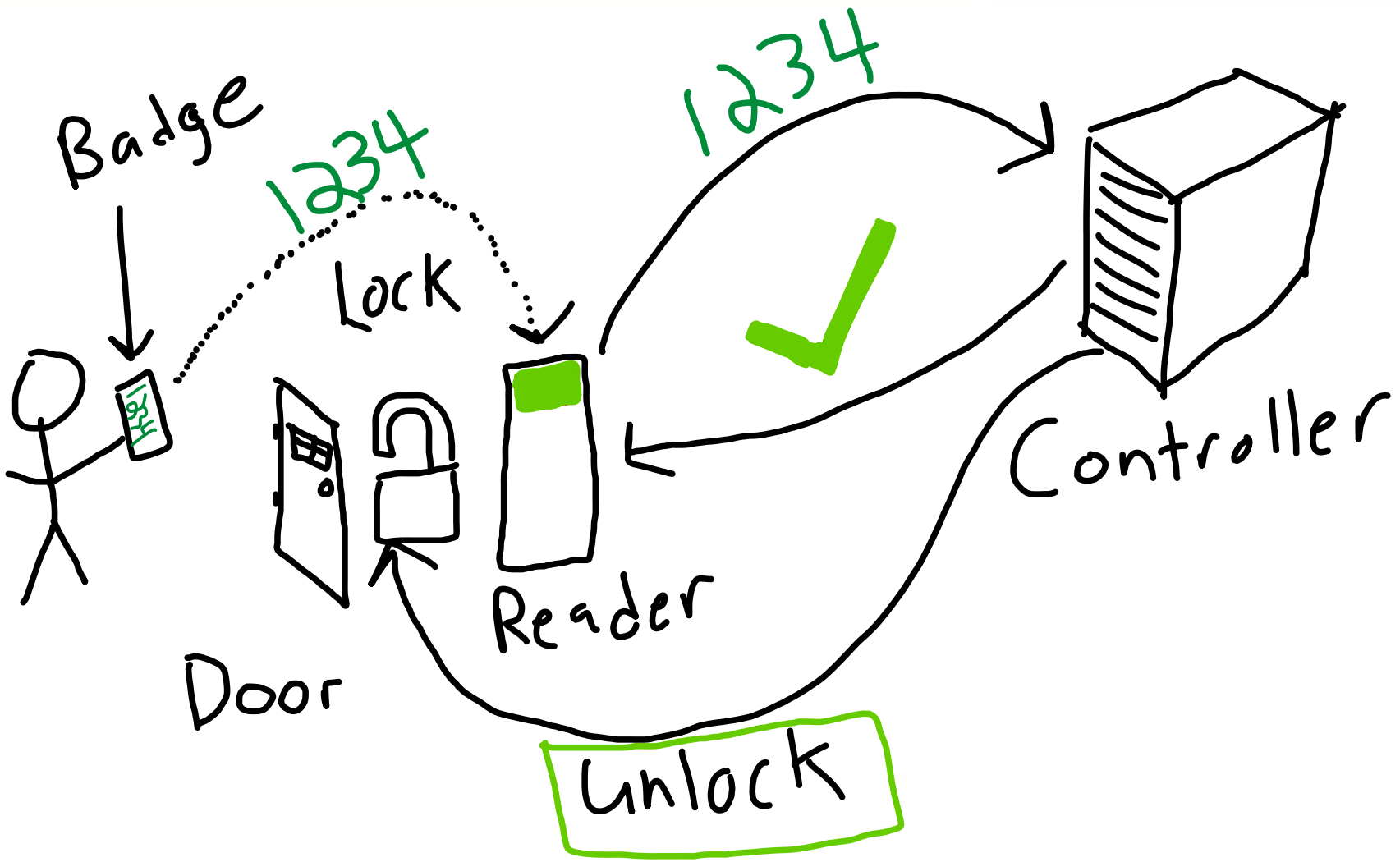

© Bishop Fox. All rights reserved worldwide.

# RFID Badge Setup



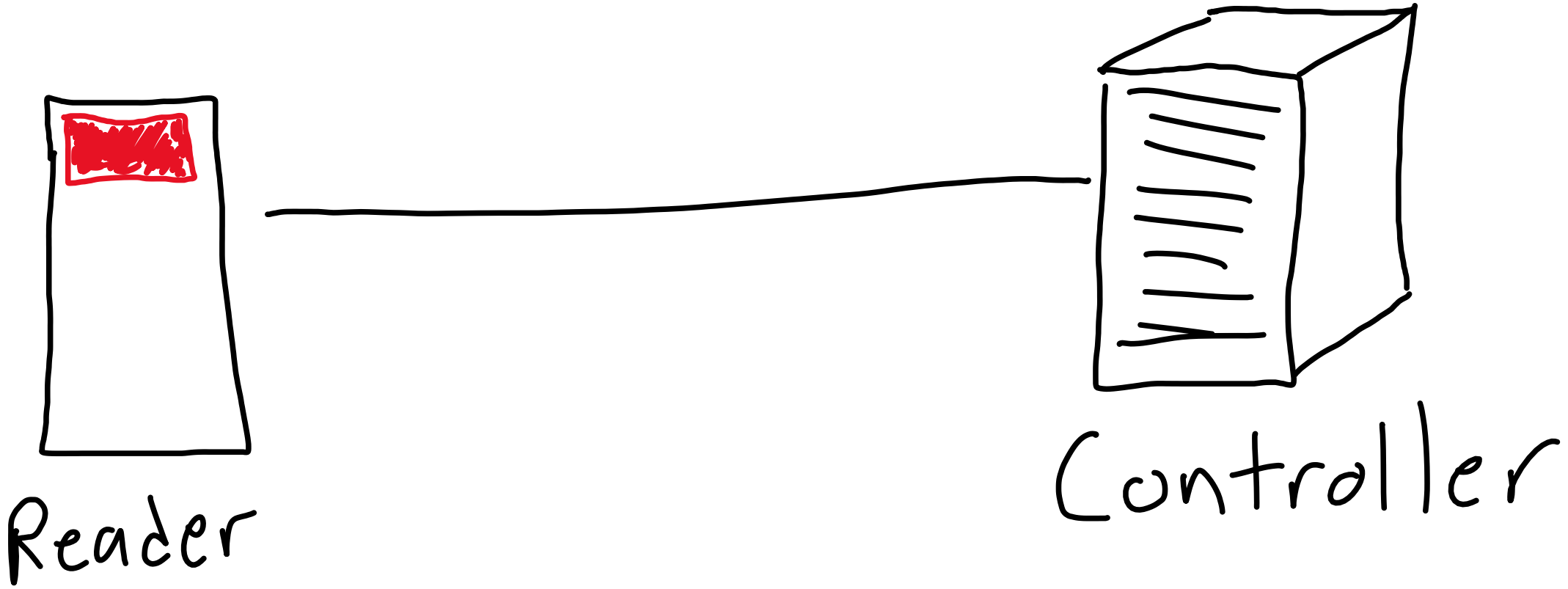

© Bishop Fox. All rights reserved worldwide.

# RFID Badge Setup



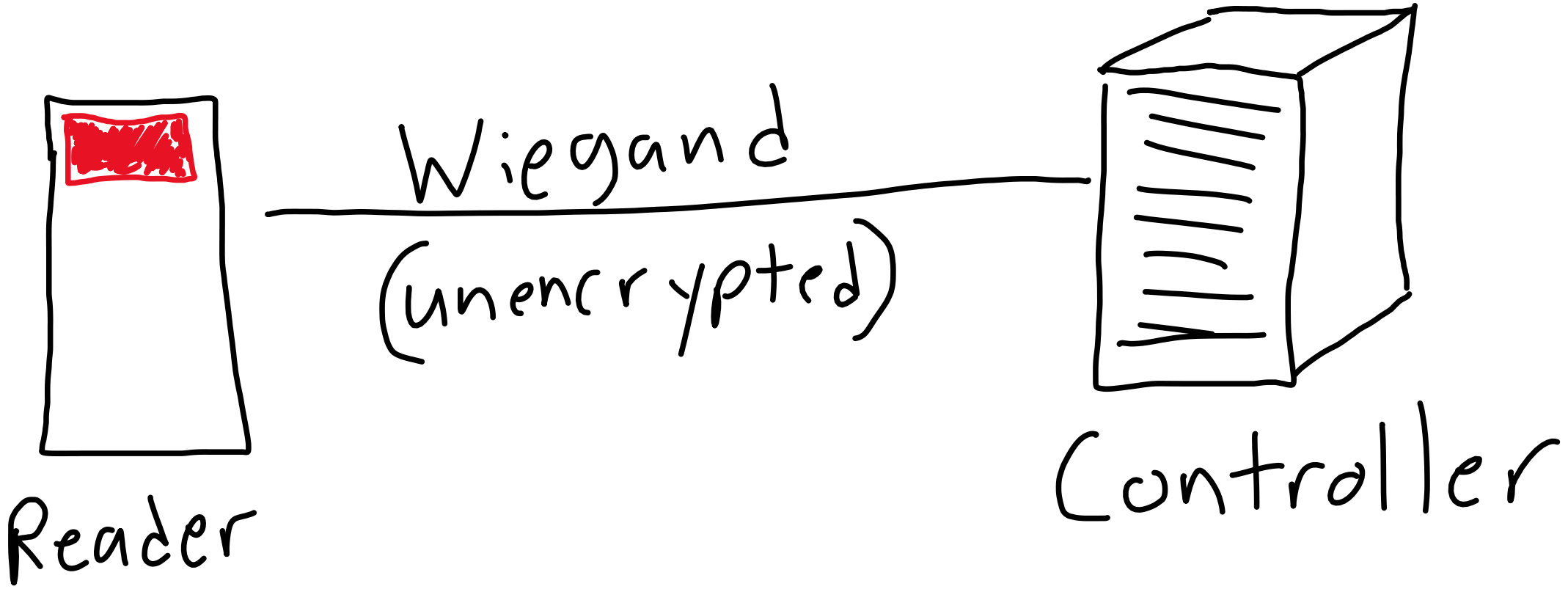

© Bishop Fox. All rights reserved worldwide.

# RFID Badge Setup



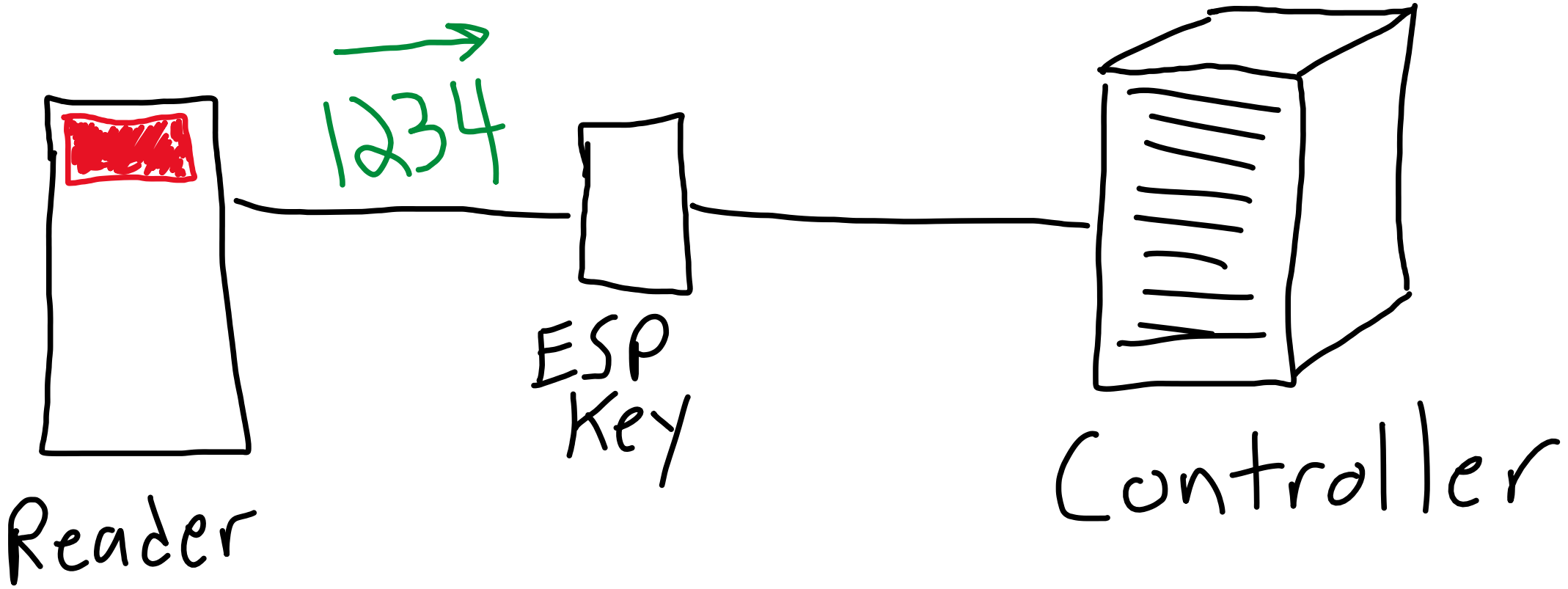

© Bishop Fox. All rights reserved worldwide.

# RFID Badge Setup



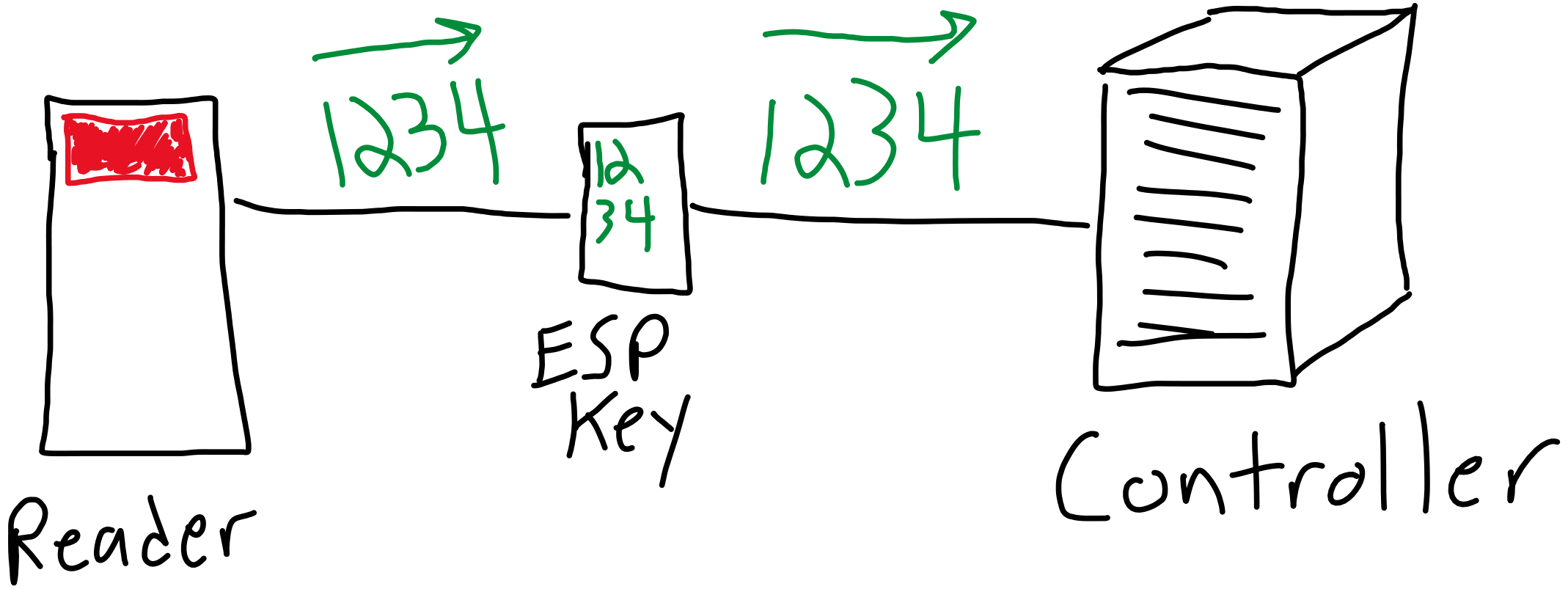

© Bishop Fox. All rights reserved worldwide.

# RFID Badge Setup



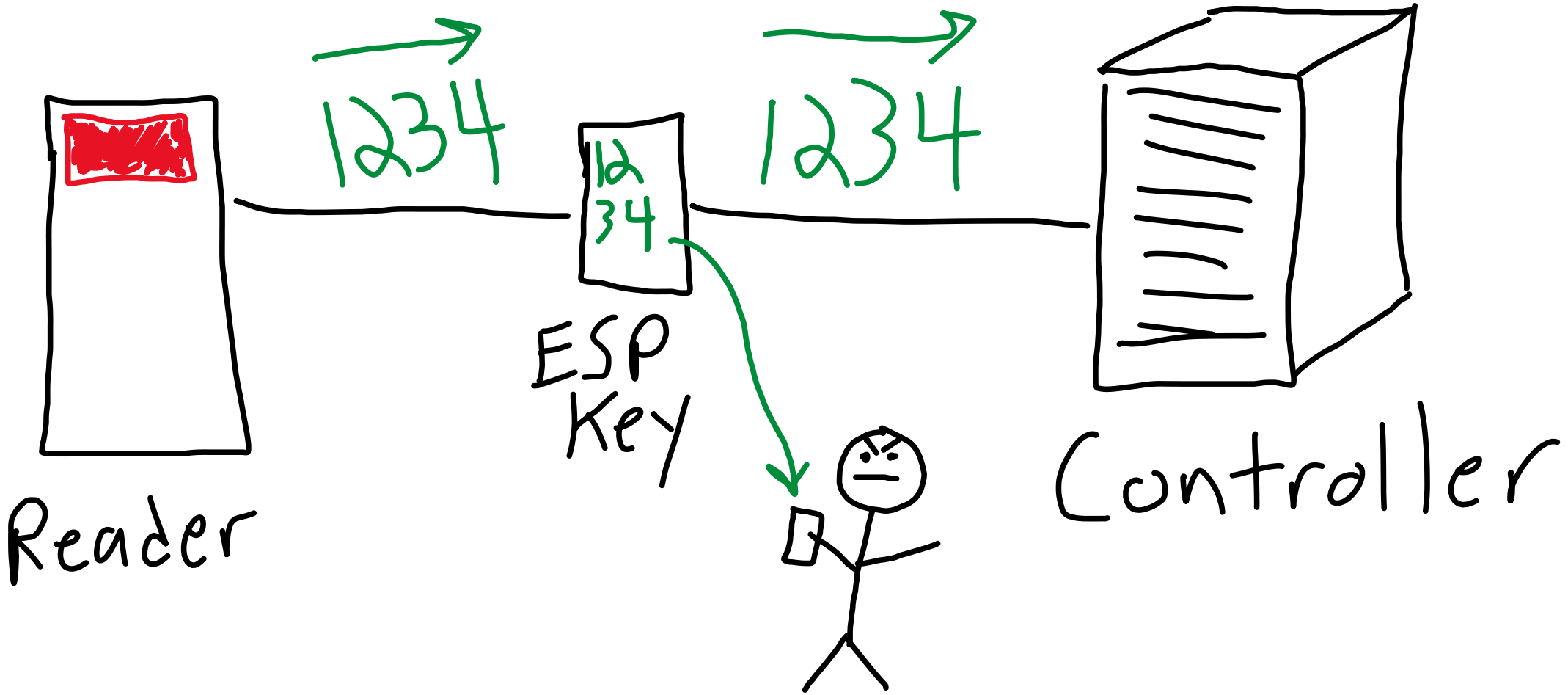

© Bishop Fox. All rights reserved worldwide.

# RFID Badge Setup



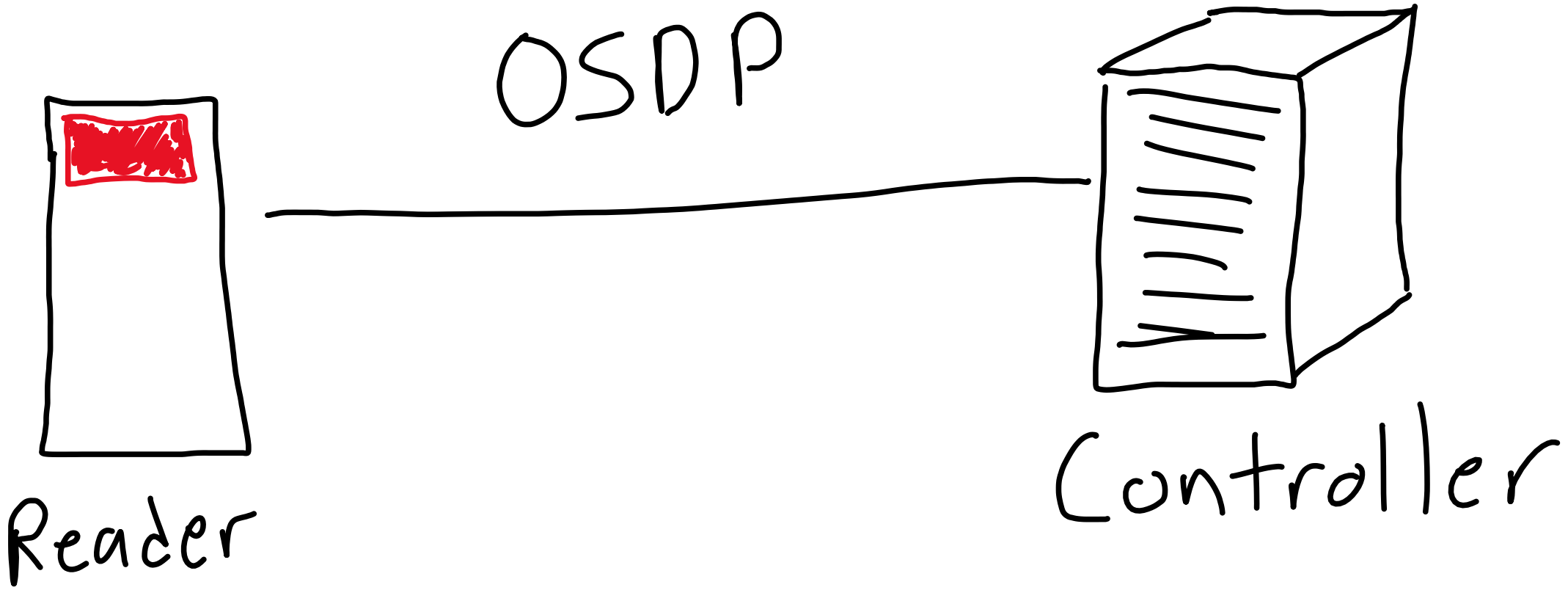

© Bishop Fox. All rights reserved worldwide.

# RFID Badge Setup



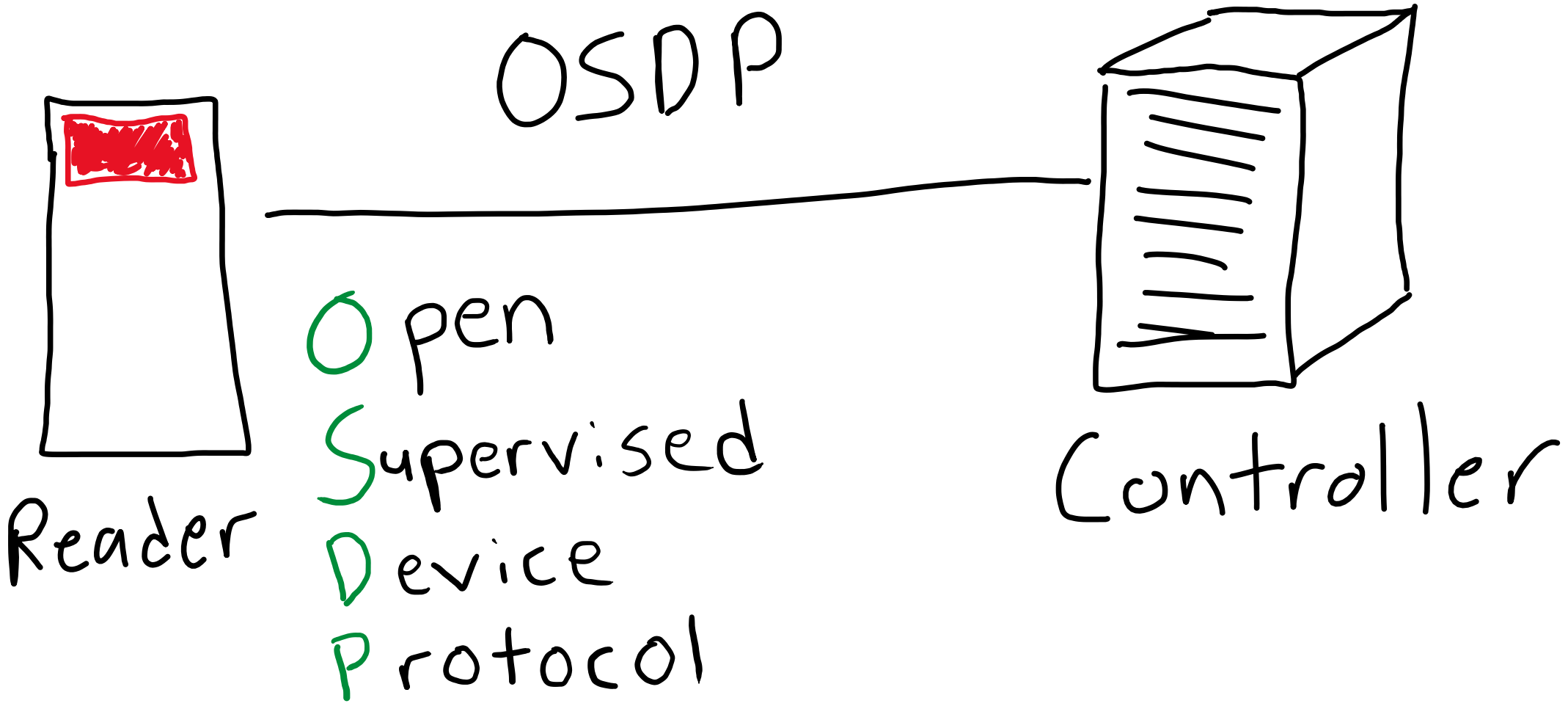

© Bishop Fox. All rights reserved worldwide.

# RFID Badge Setup



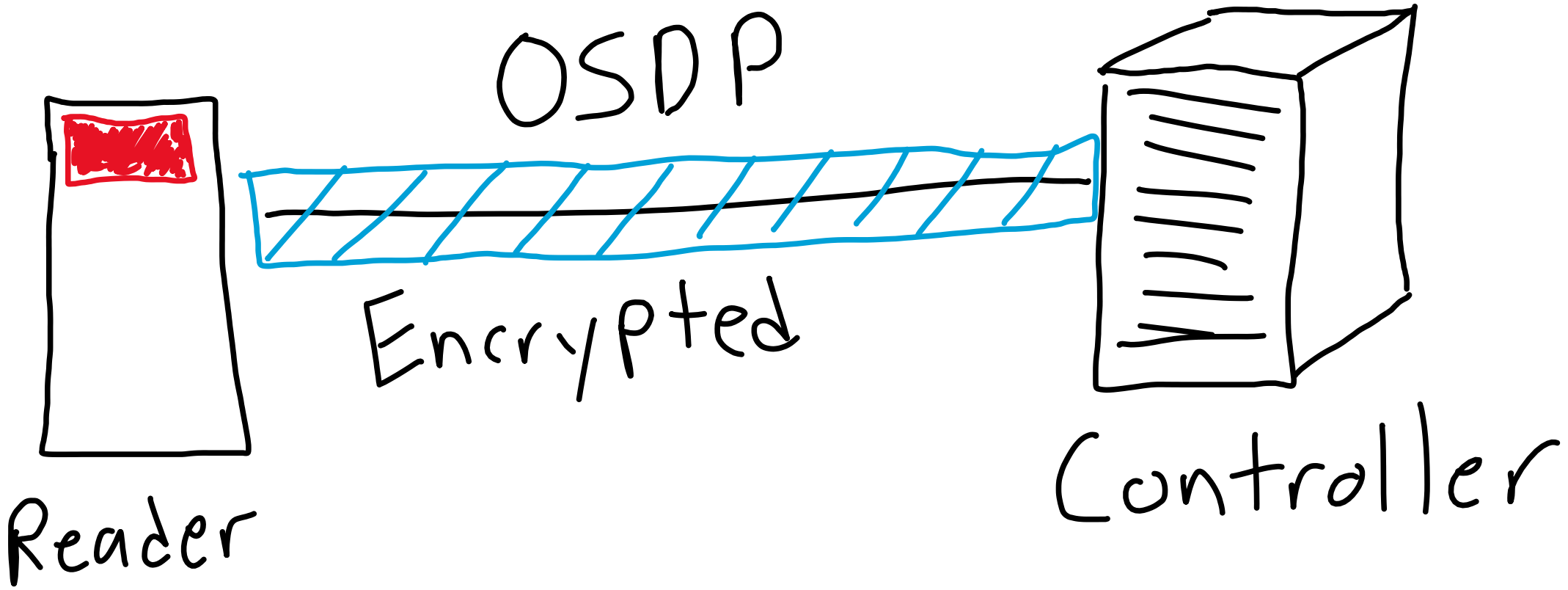

© Bishop Fox. All rights reserved worldwide.

# RFID Badge Setup



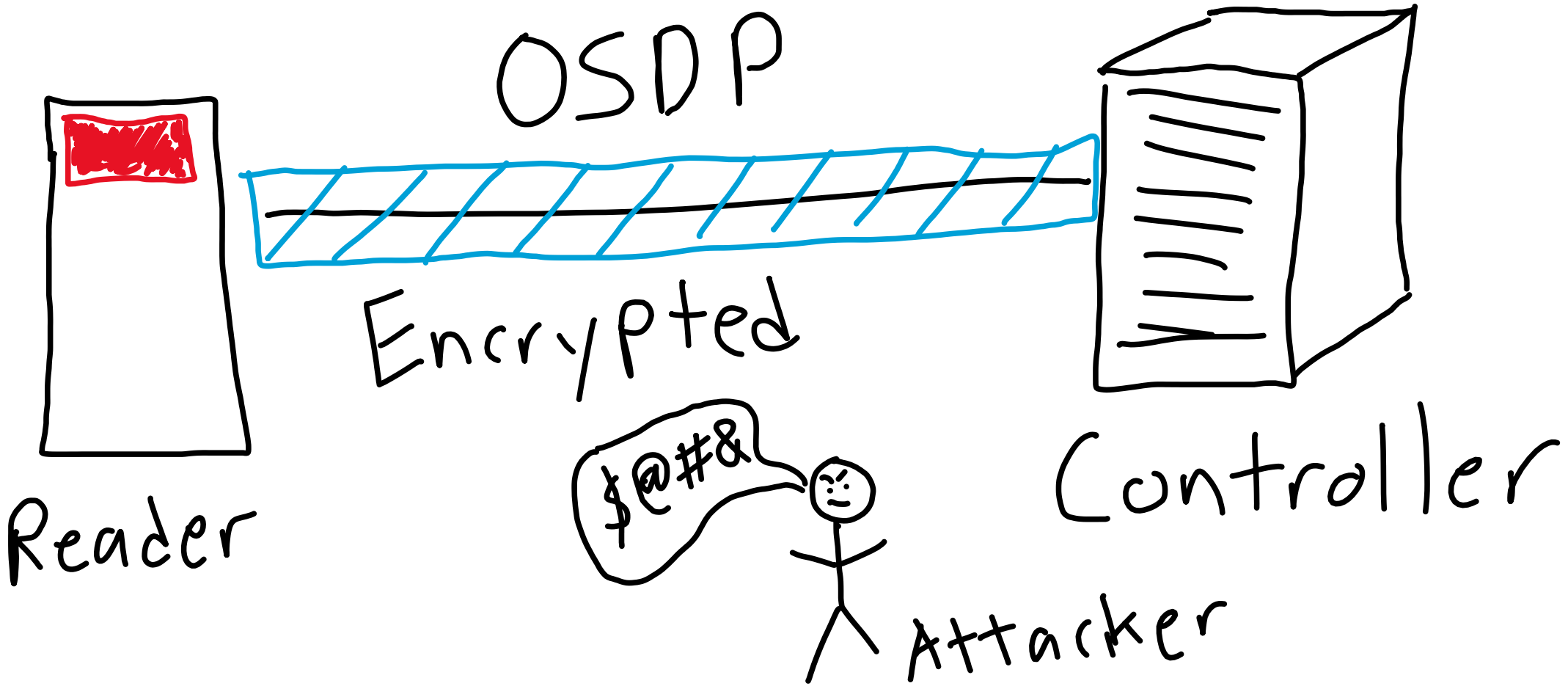

© Bishop Fox. All rights reserved worldwide.

# RFID Badge Setup



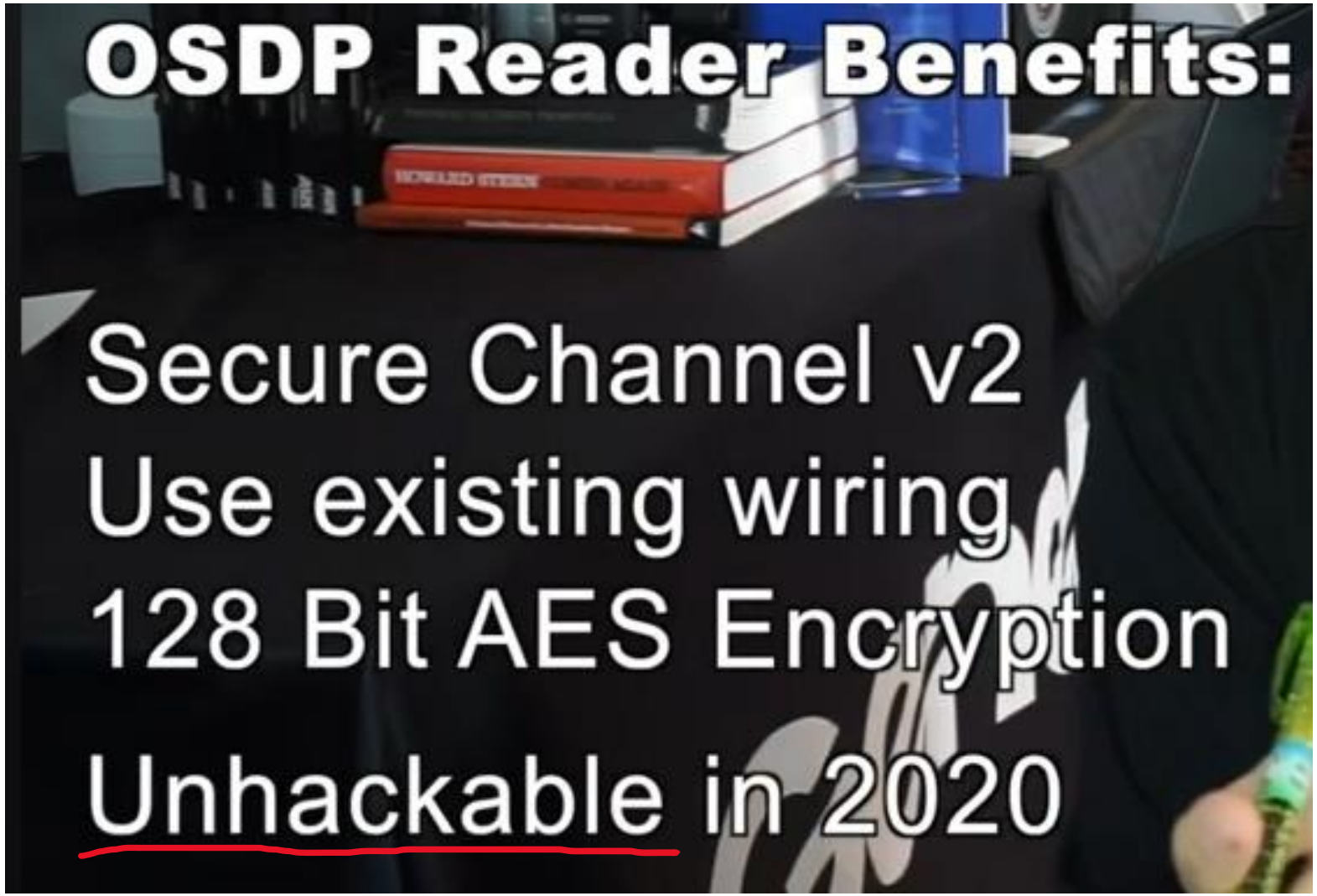

© Bishop Fox. All rights reserved worldwide.

# RFID Badge Setup




© Bishop Fox. All rights reserved worldwide.

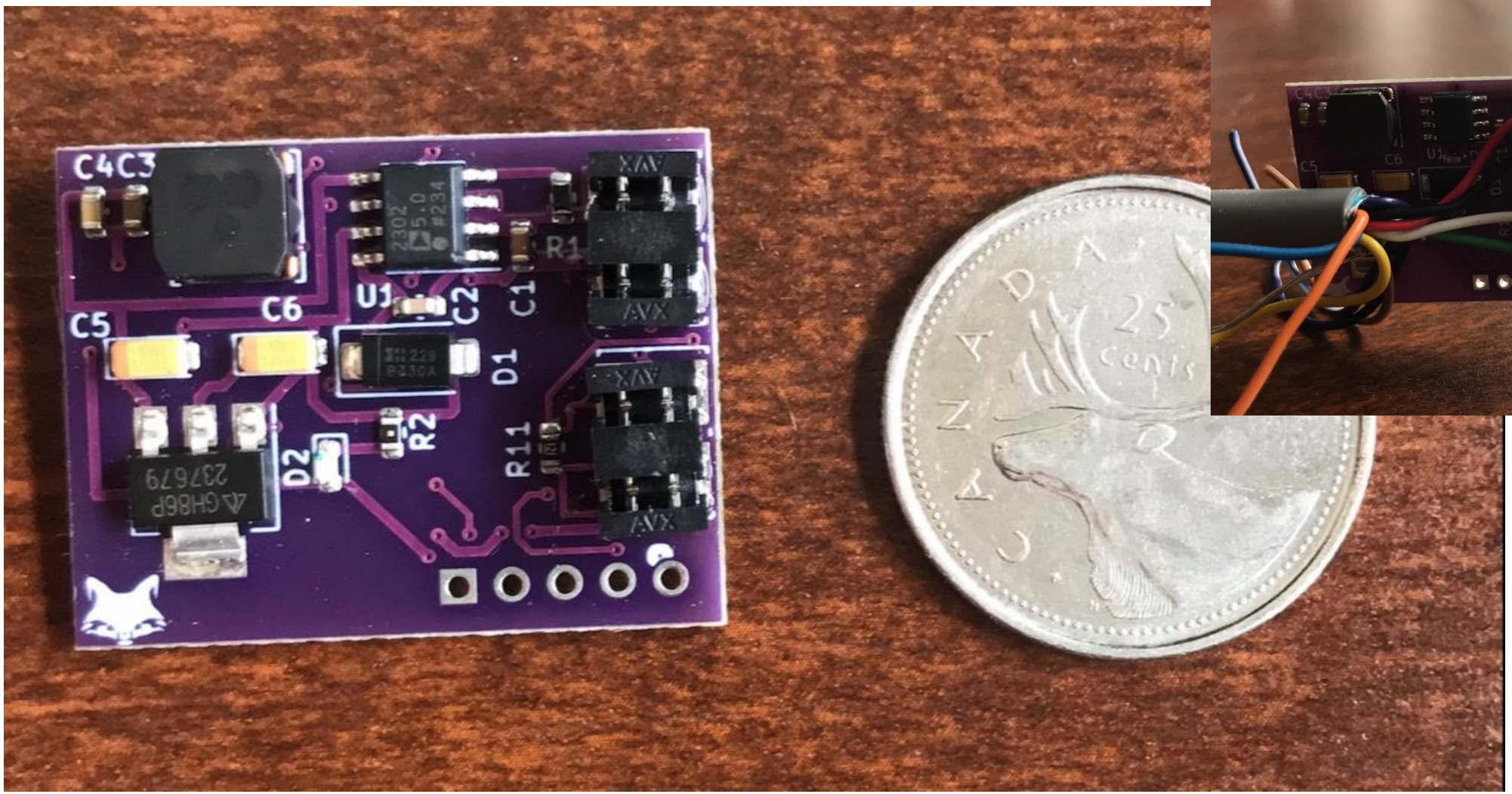
# Bold Claims

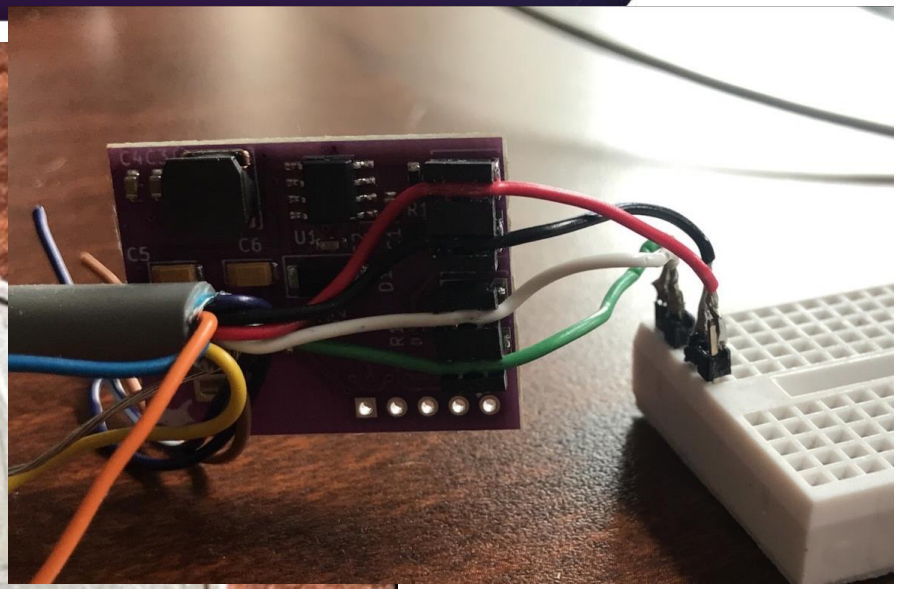



© Bishop Fox. All rights reserved worldwide.

THE ELVISH WORD FOR FRIEND

# Mellon



© Bishop Fox. All rights reserved worldwide.

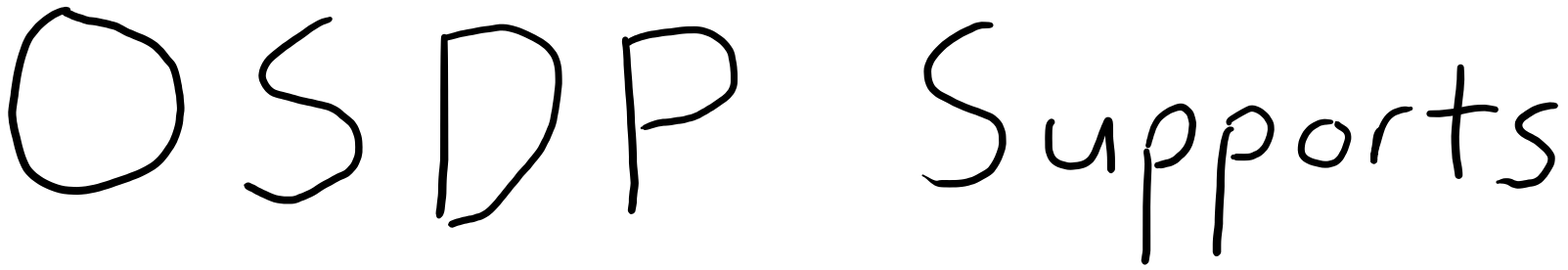
LET'S JUST TAKE A LOOK

# Demo #1




© Bishop Fox. All rights reserved worldwide.

# The Protocol




© Bishop Fox. All rights reserved worldwide.

# The Protocol

OSDP Supports but doesn't require

© Bishop Fox. All rights reserved worldwide.

# The Protocol

OSDP Supports but doesn't require encryption

© Bishop Fox. All rights reserved worldwide.

# The Protocol

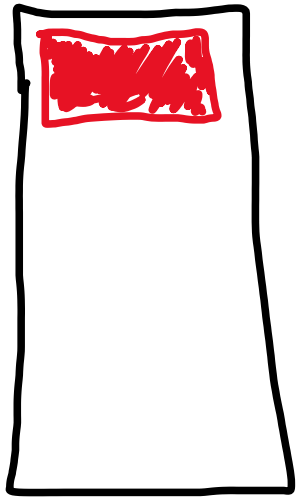
OSDP-SC ("secure" channel)

is an OSDP extension

© Bishop Fox. All rights reserved worldwide.

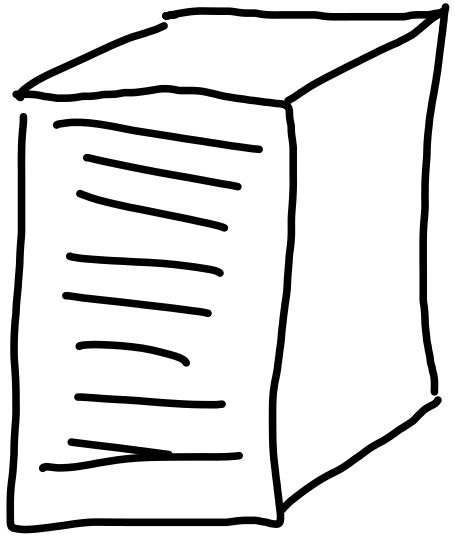
# The Protocol

...to encrypt...



Reader

Controller



...or not to encrypt

© Bishop Fox. All rights reserved worldwide.

# Protocol Basics

© Bishop Fox. All rights reserved worldwide.

# The Protocol

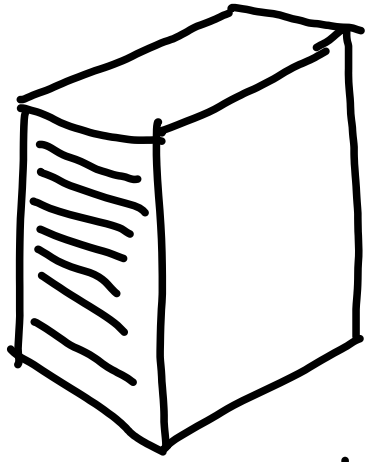
RS-485 (the other serial)

- multi-drop

© Bishop Fox. All rights reserved worldwide.

# The Protocol

RS-485 (the other serial)

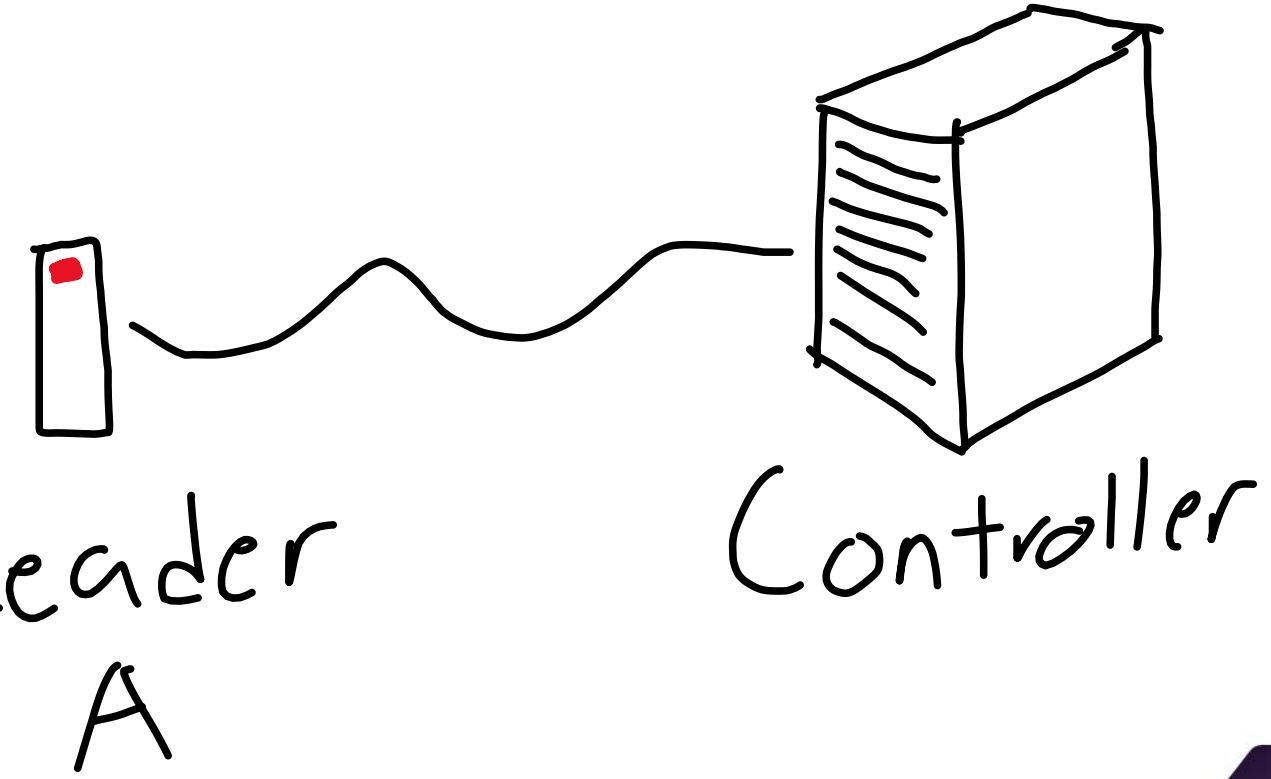


Controller

© Bishop Fox. All rights reserved worldwide.

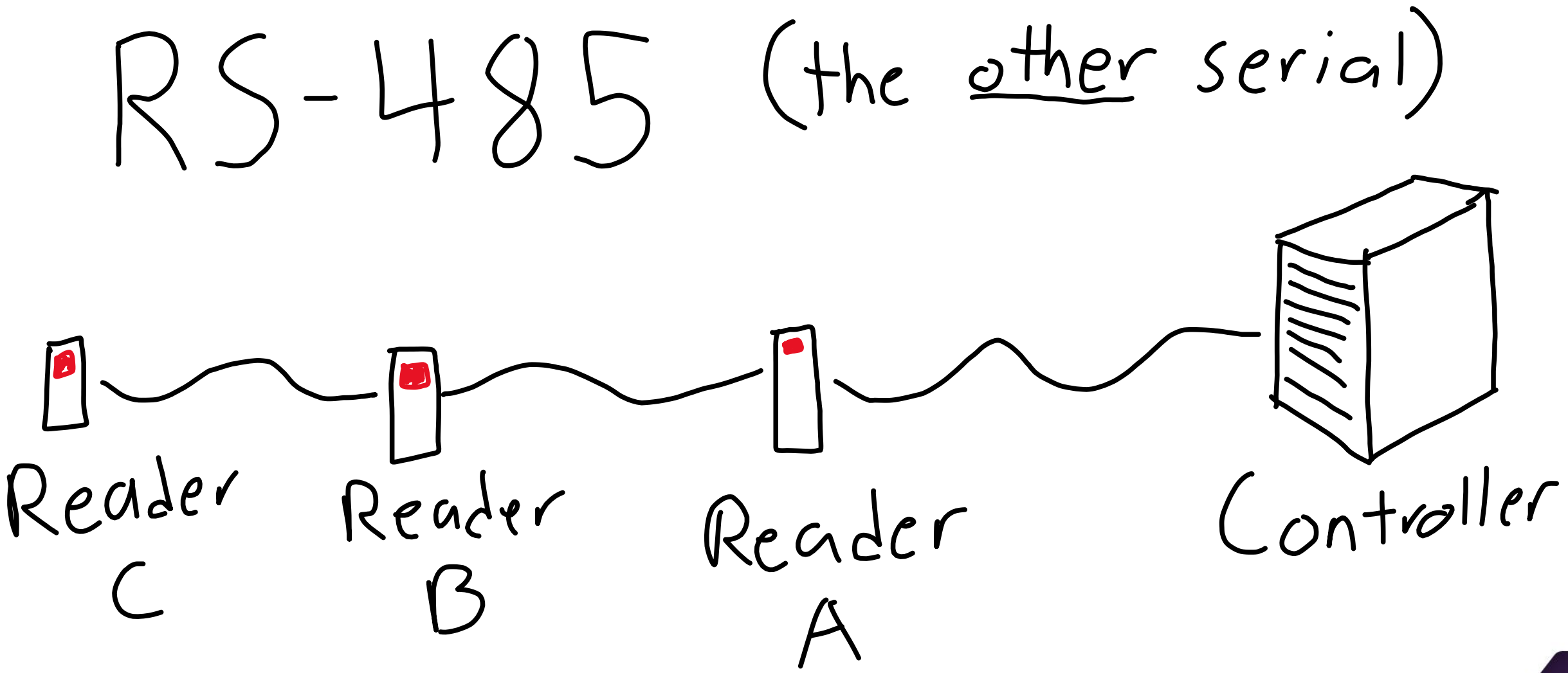
# The Protocol

RS-485 (the other serial)




© Bishop Fox. All rights reserved worldwide.

# The Protocol




© Bishop Fox. All rights reserved worldwide.

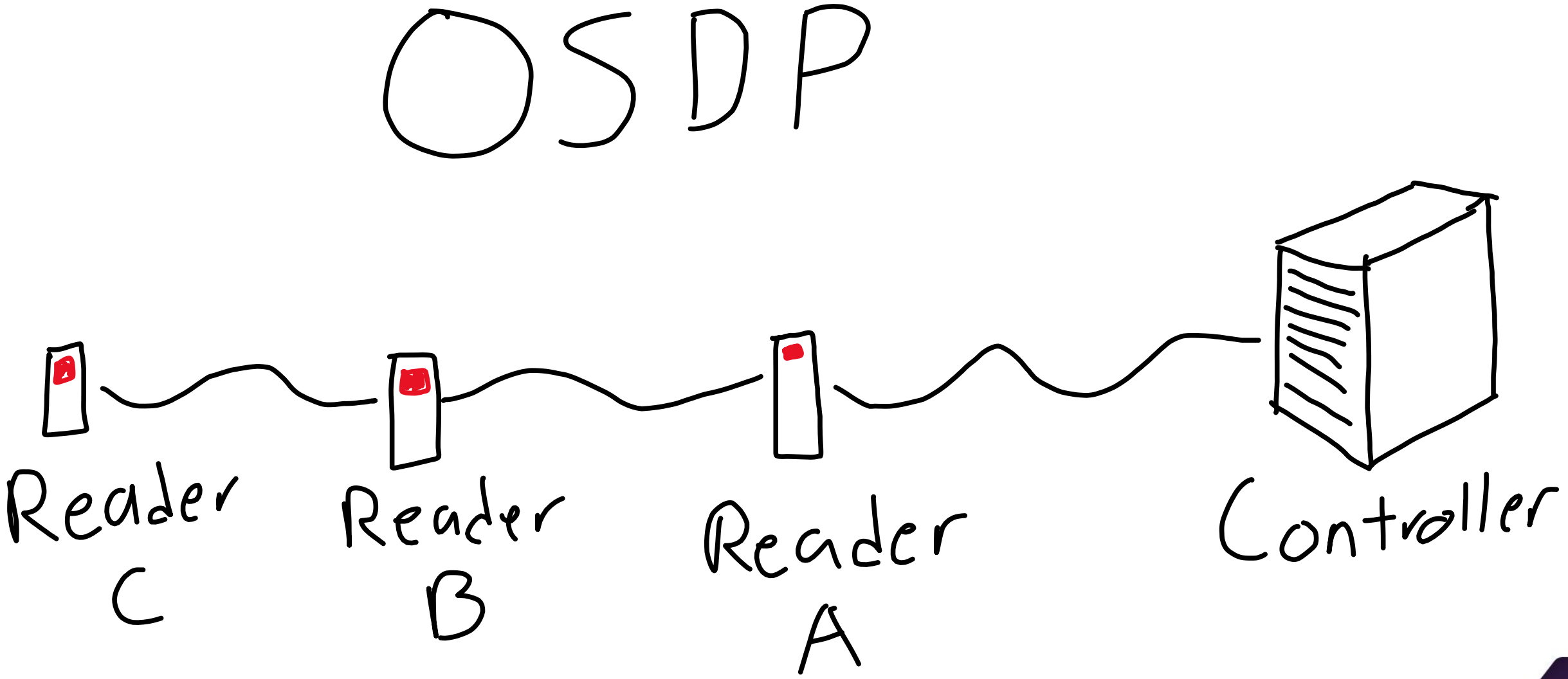
# The Protocol

OSDP:

All messages are broadcast

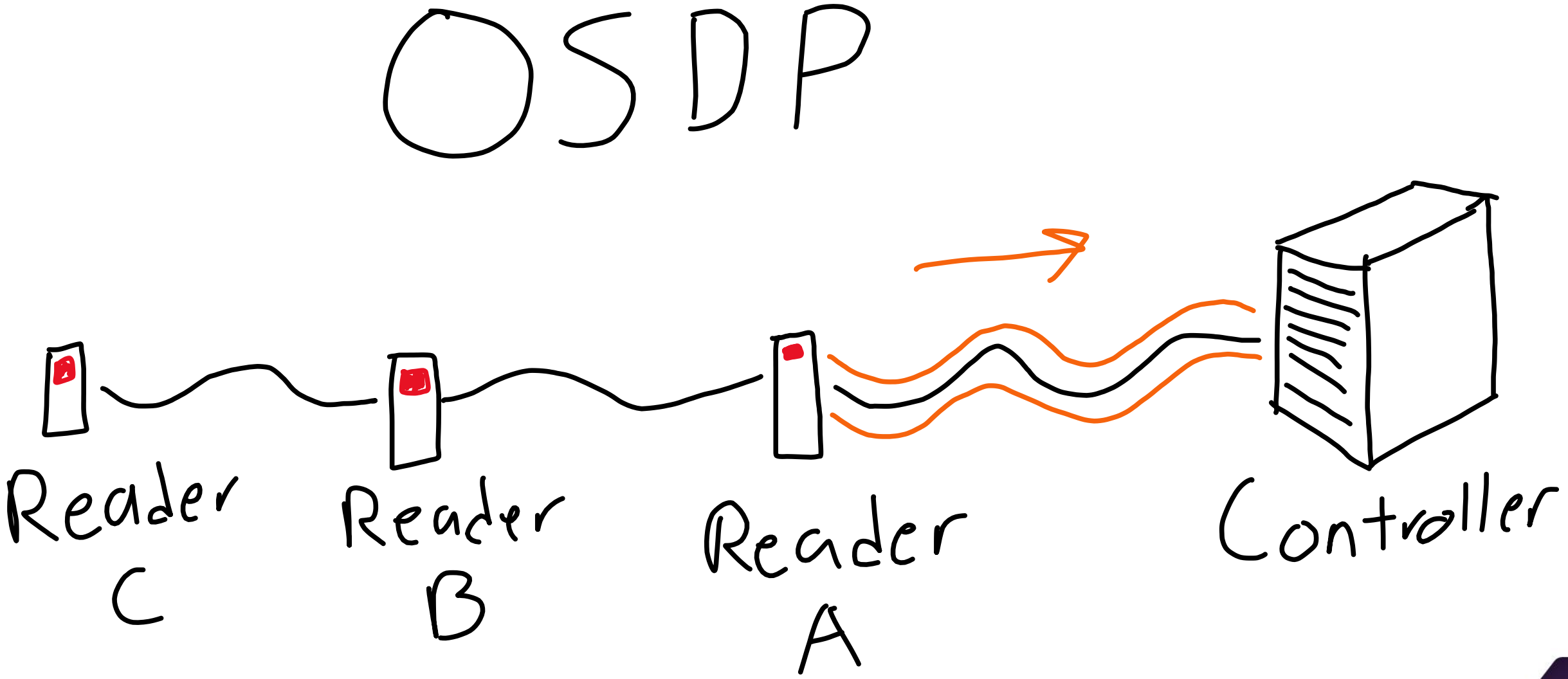
© Bishop Fox. All rights reserved worldwide.

# The Protocol



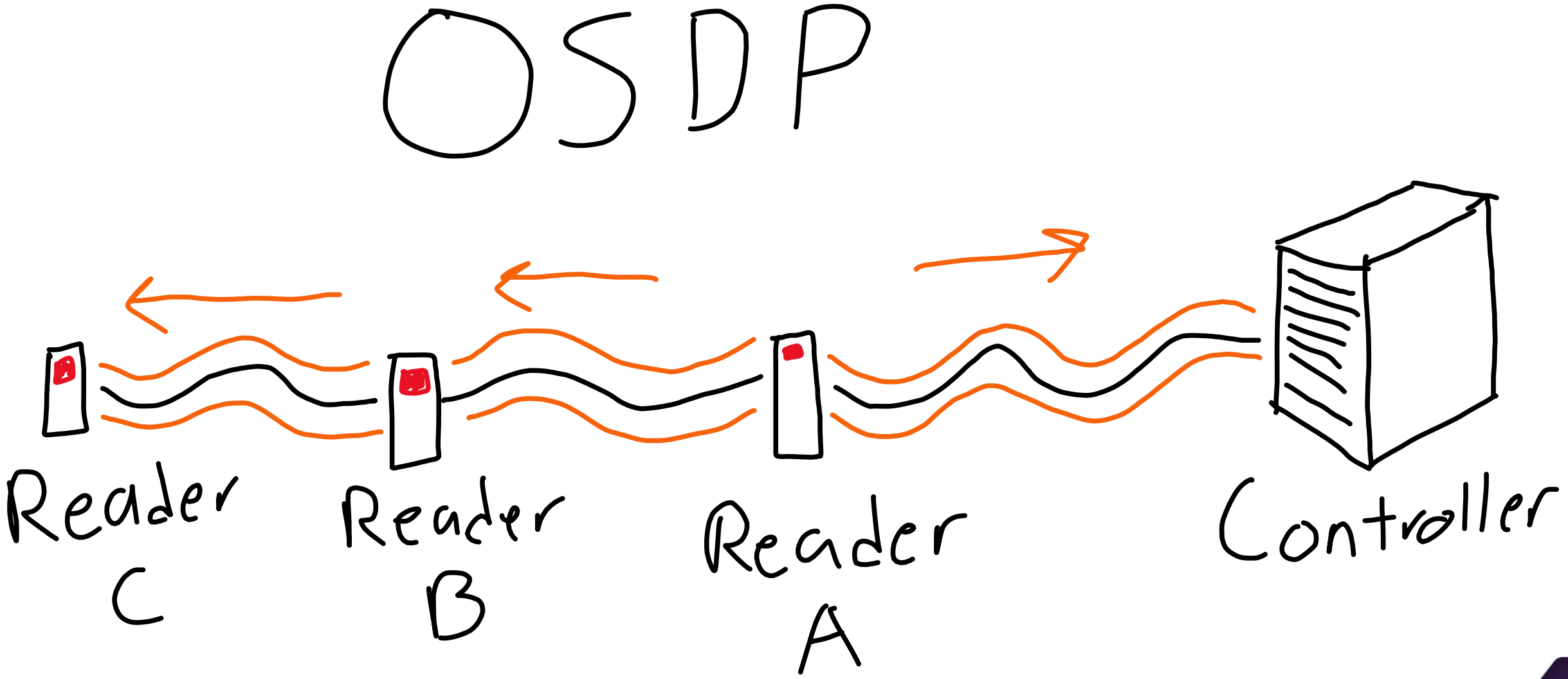

© Bishop Fox. All rights reserved worldwide.

# The Protocol



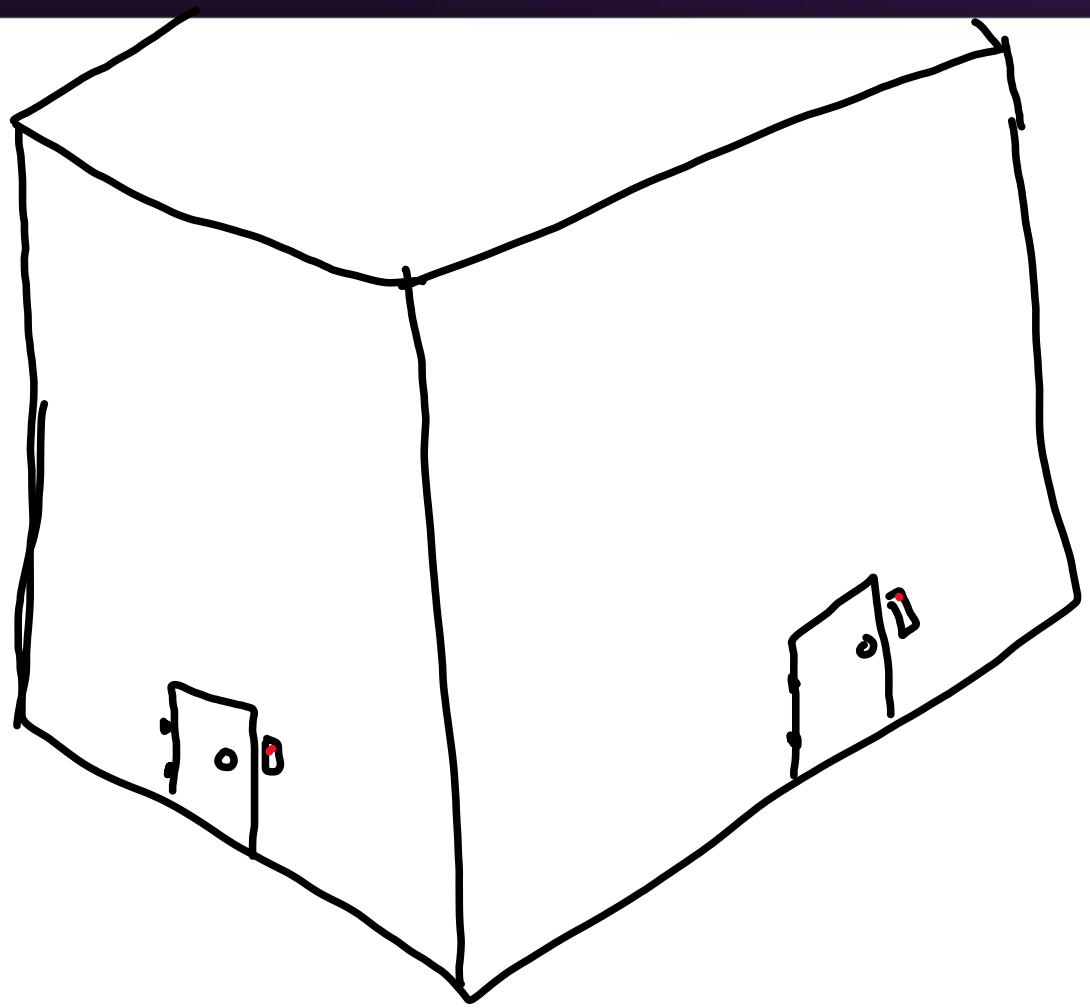

© Bishop Fox. All rights reserved worldwide.

# The Protocol



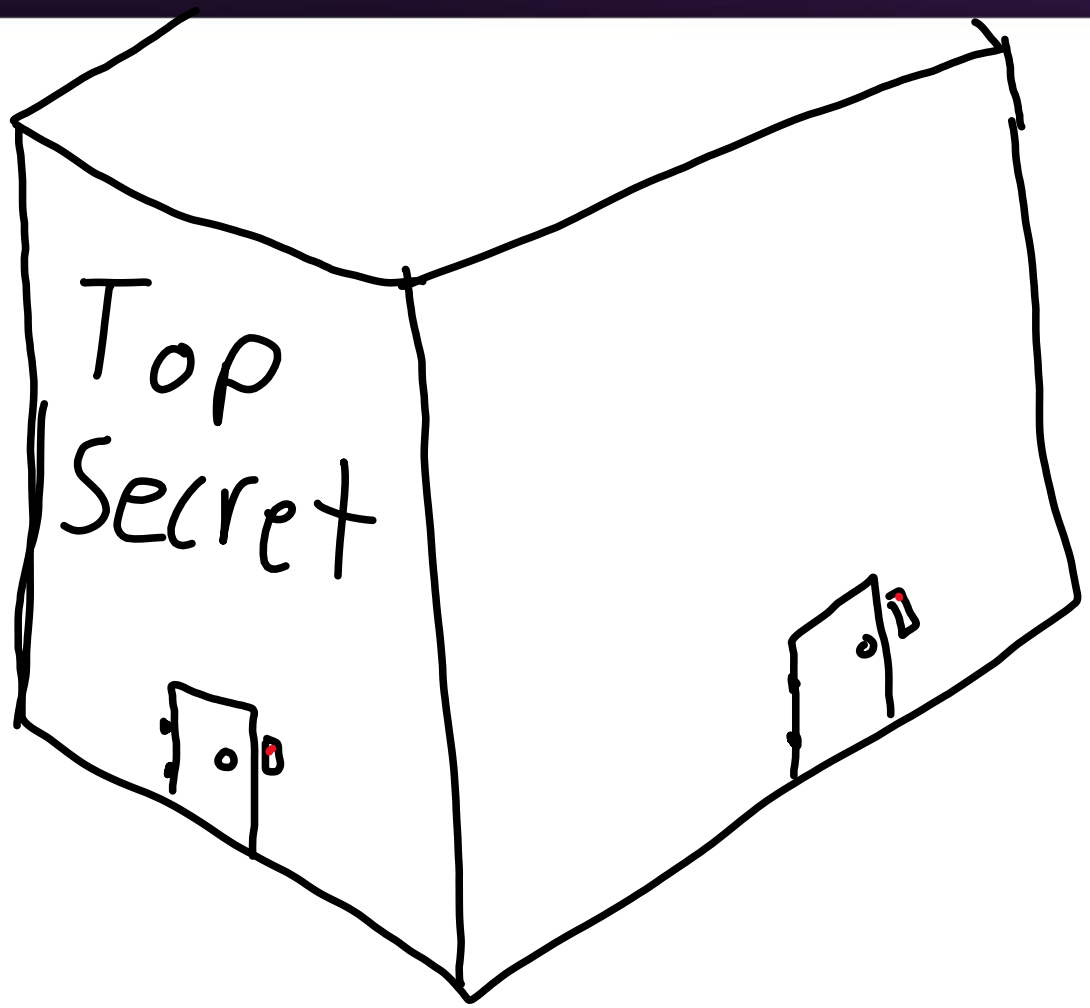

© Bishop Fox. All rights reserved worldwide.

# Undisclosed Location in Santa Fe, NM



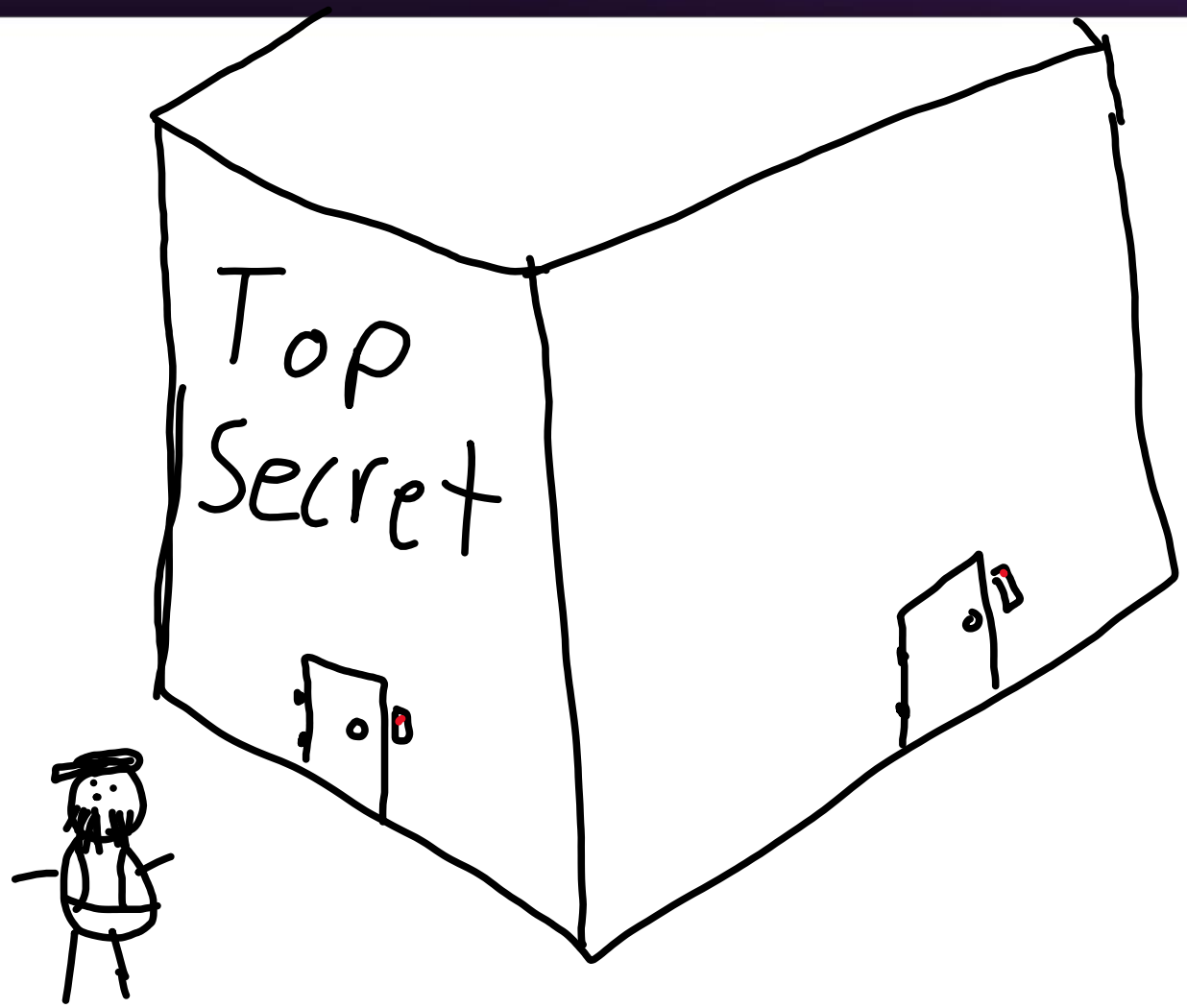
© Bishop Fox. All rights reserved worldwide.

# Undisclosed Location in Santa Fe, NM




© Bishop Fox. All rights reserved worldwide.

# Undisclosed Location in Santa Fe, NM



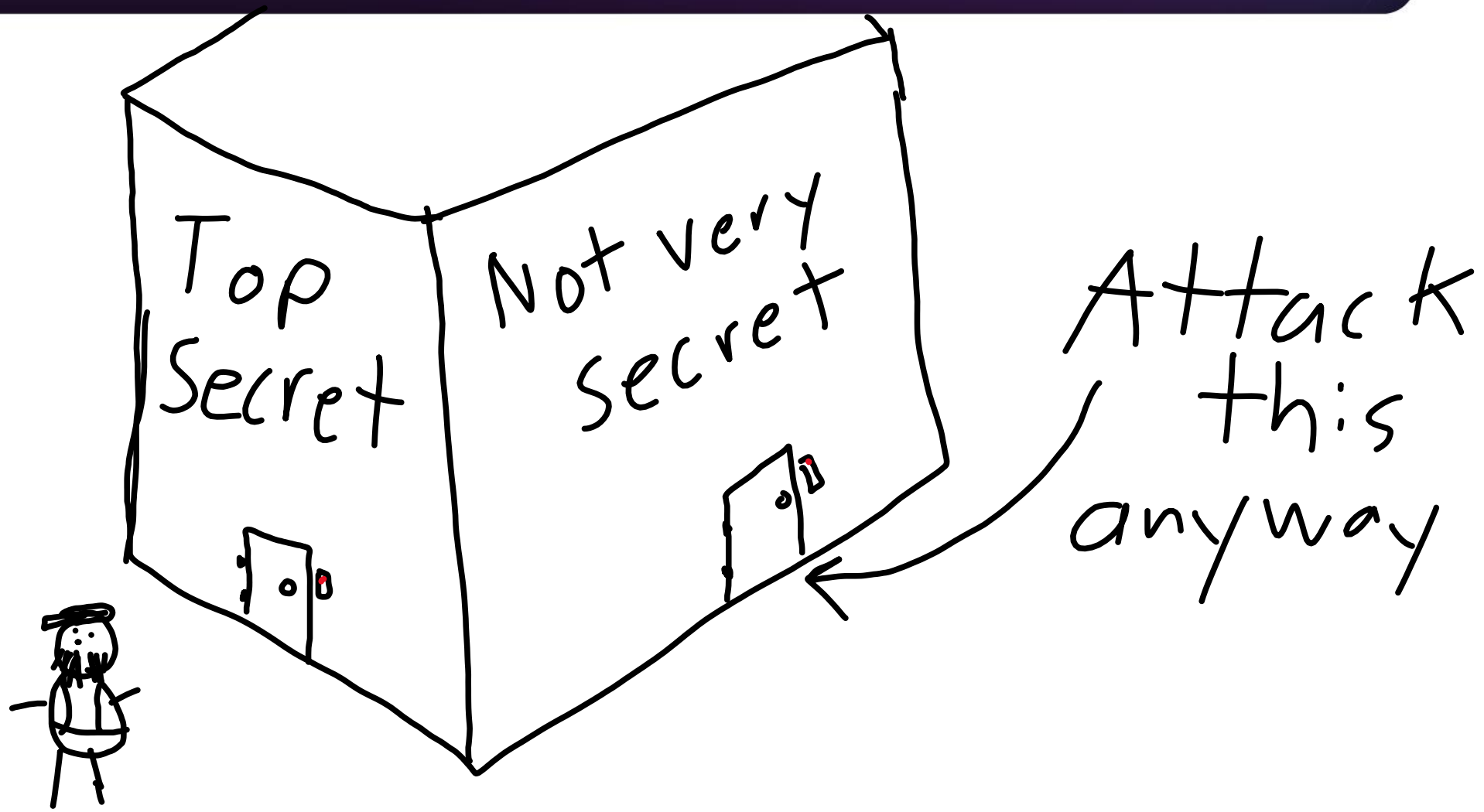

© Bishop Fox. All rights reserved worldwide.

# Undisclosed Location in Santa Fe, NM



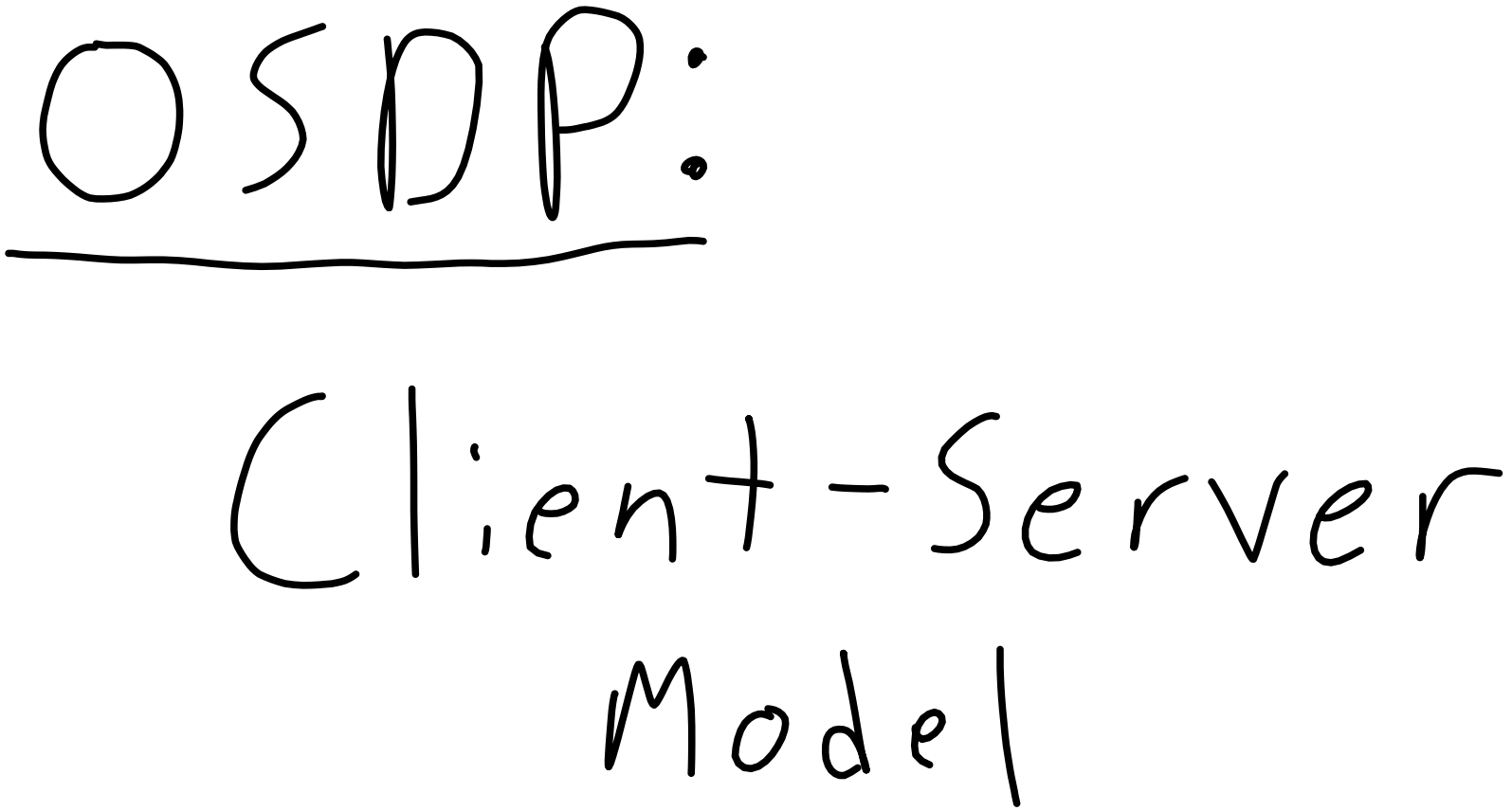

© Bishop Fox. All rights reserved worldwide.

# Undisclosed Location in Santa Fe, NM



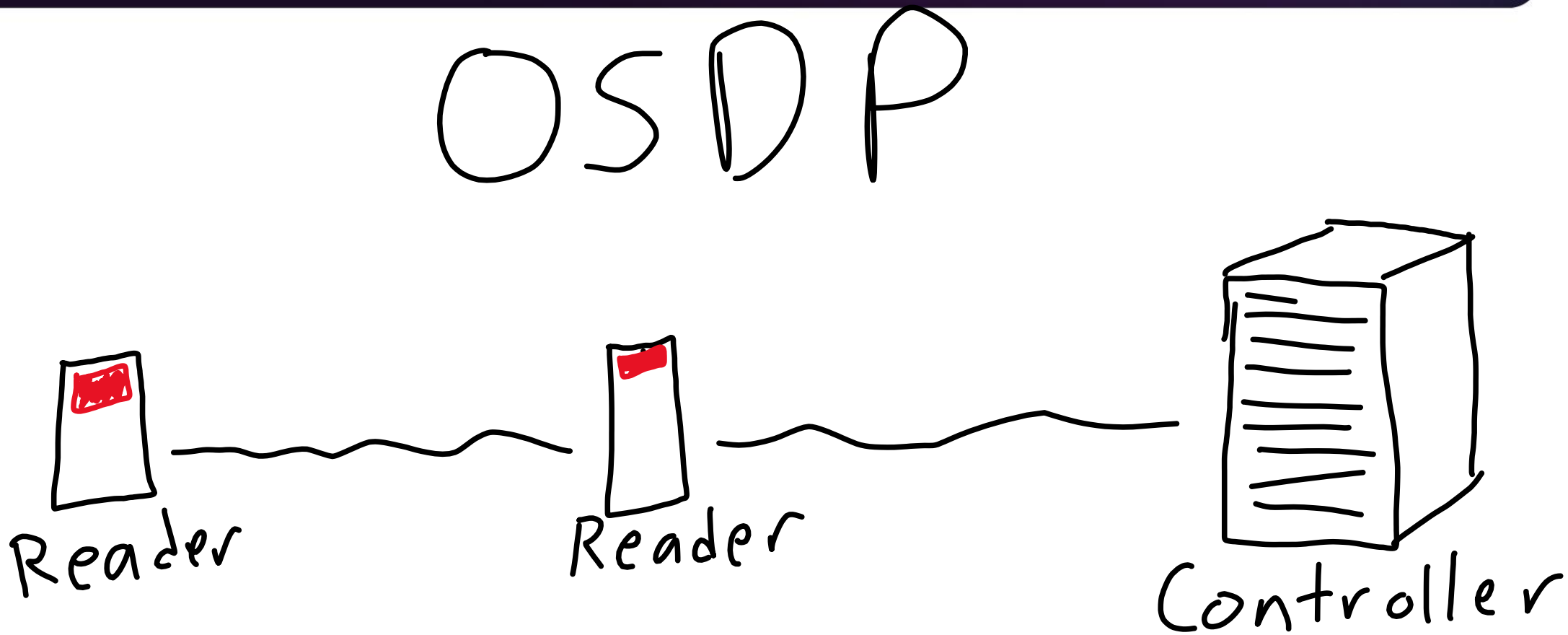

© Bishop Fox. All rights reserved worldwide.

# The Protocol



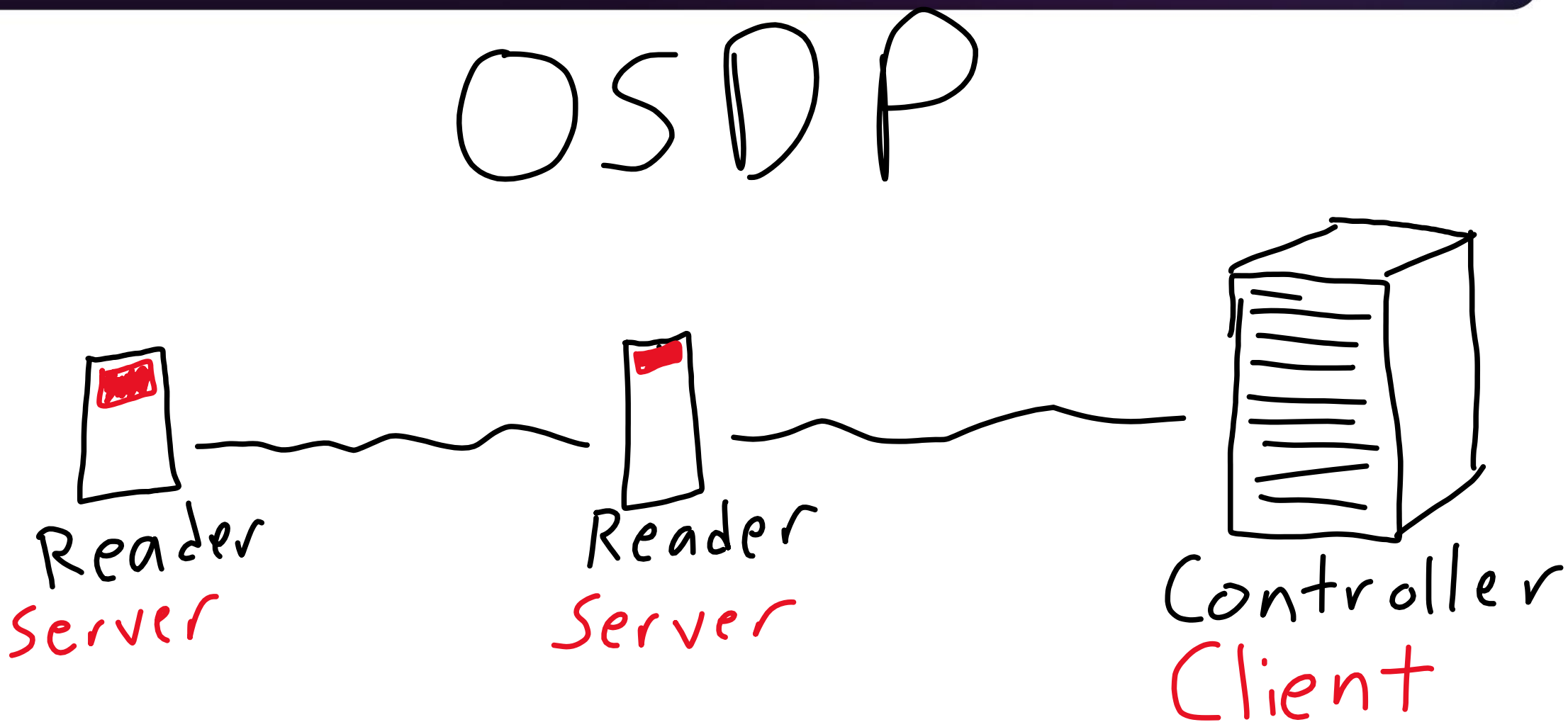

© Bishop Fox. All rights reserved worldwide.

# The Protocol



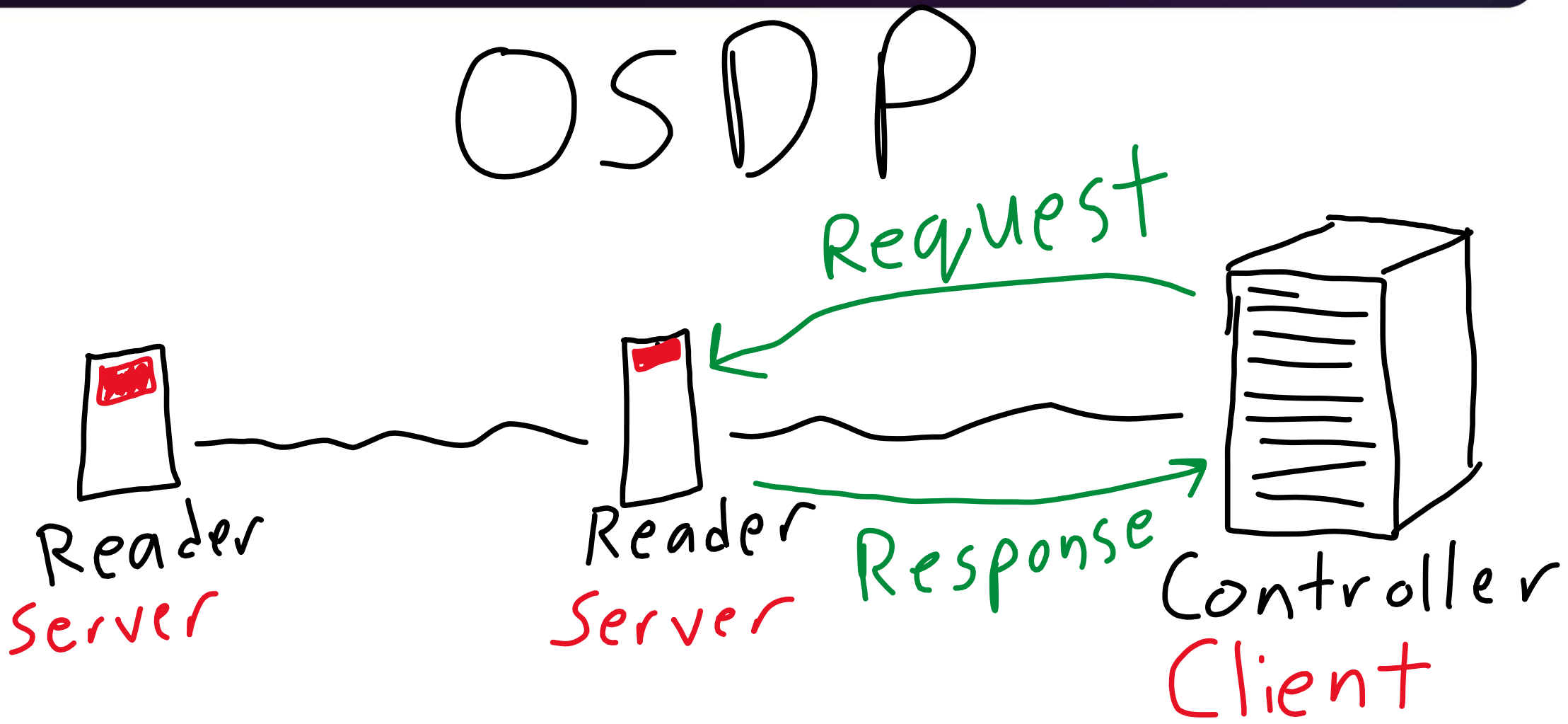

© Bishop Fox. All rights reserved worldwide.

# The Protocol




© Bishop Fox. All rights reserved worldwide.

# The Protocol




© Bishop Fox. All rights reserved worldwide.

# Protocol WTF #1

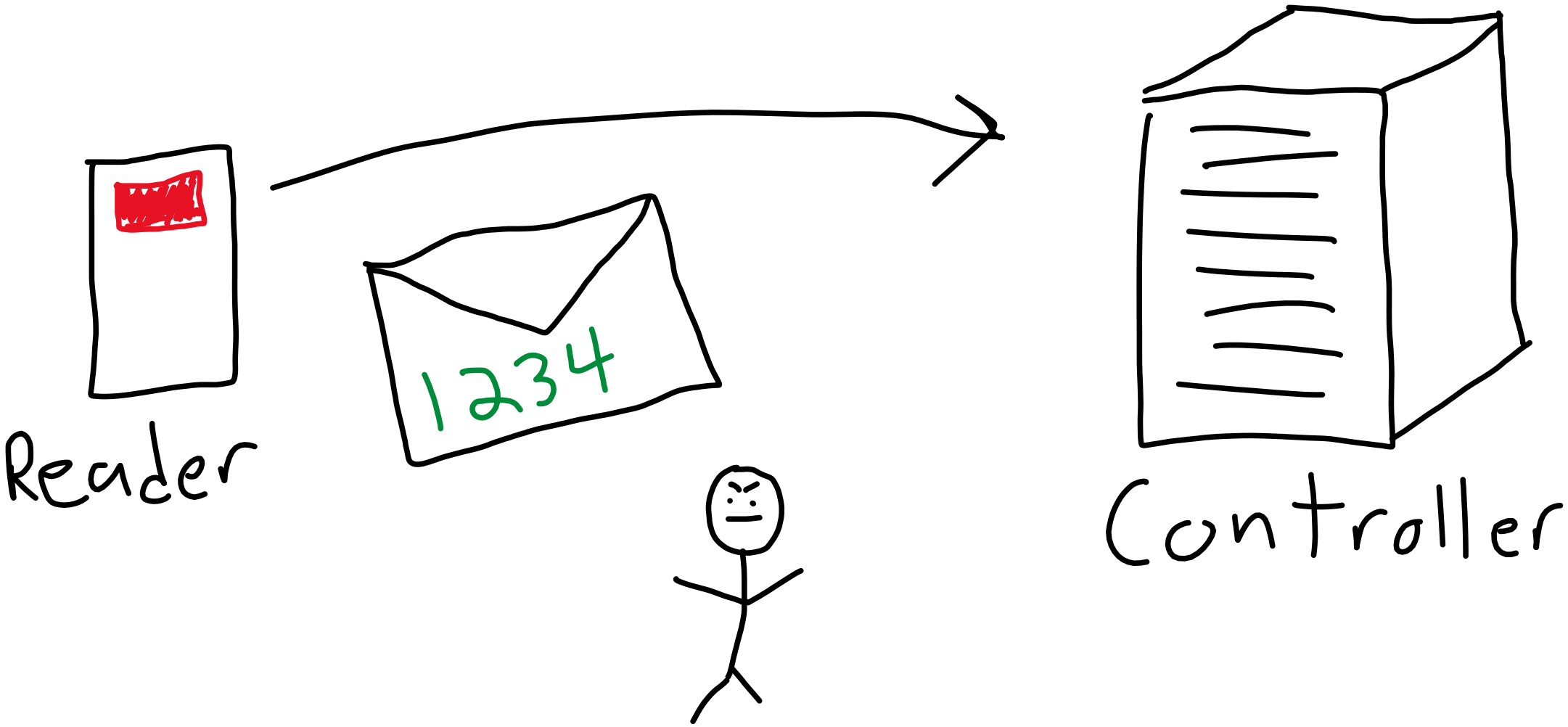
© Bishop Fox. All rights reserved worldwide.

# Protocol WTF #1

What, are we paying by the bit now?

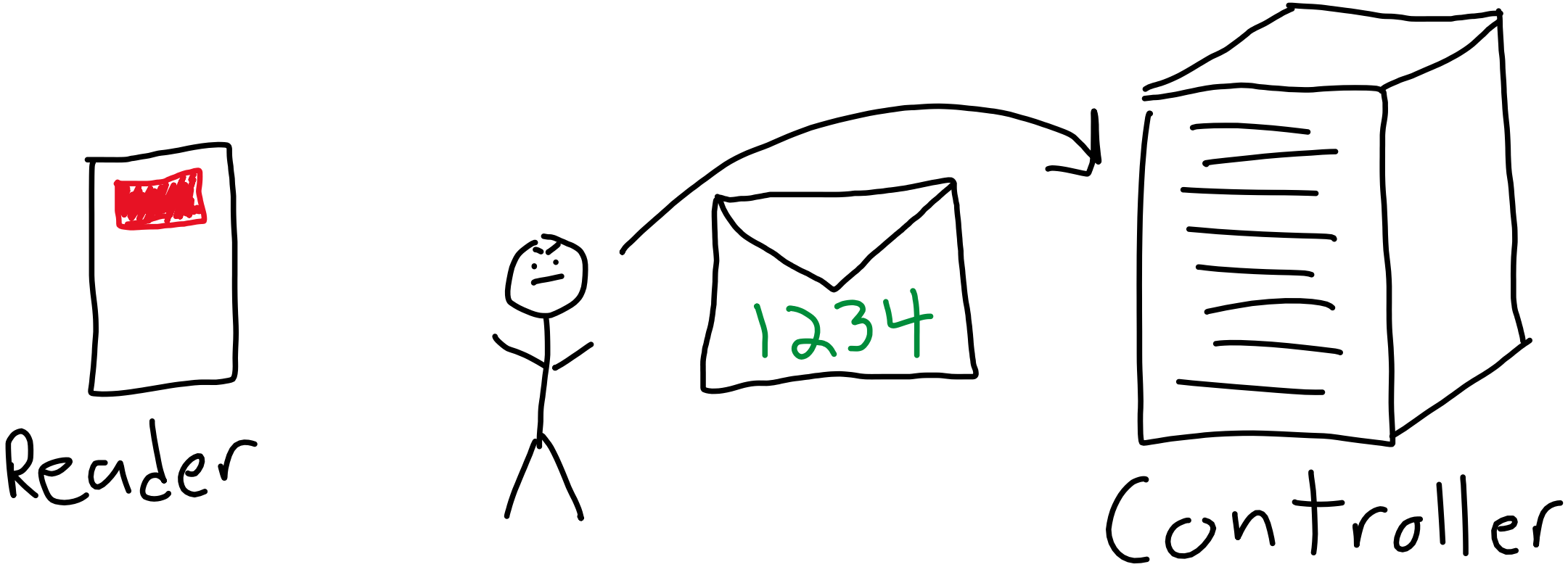
© Bishop Fox. All rights reserved worldwide.

# Replay Attacks



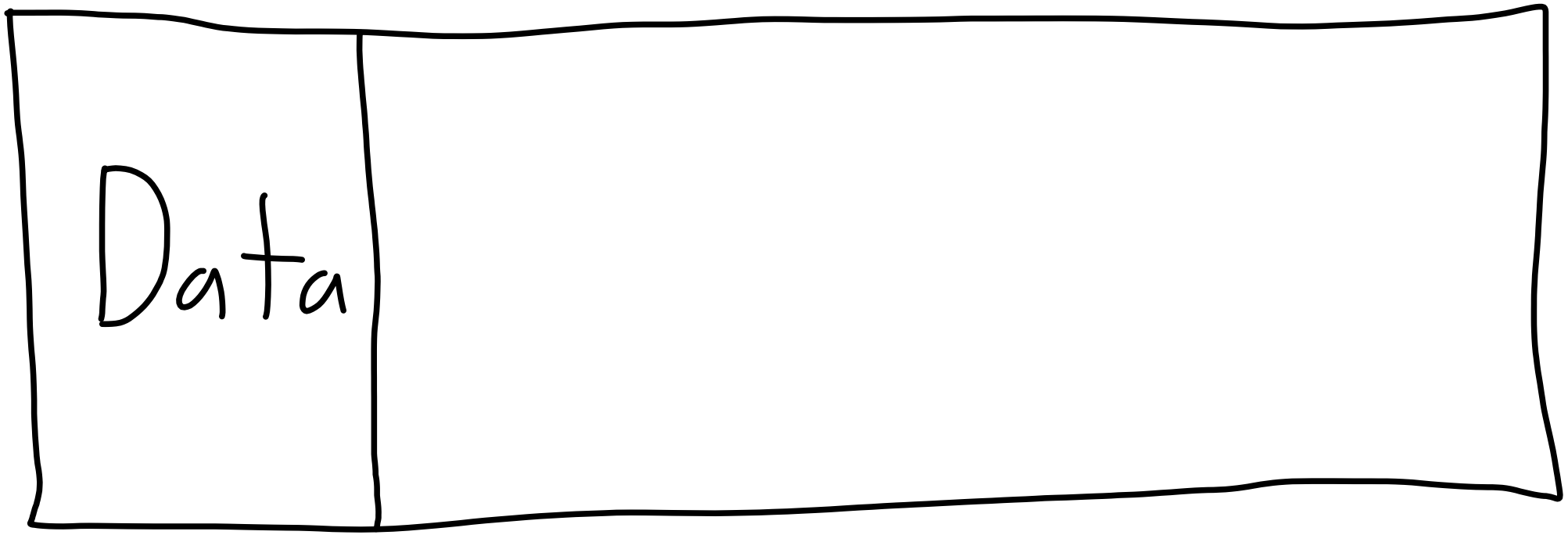

© Bishop Fox. All rights reserved worldwide.

# Replay Attacks



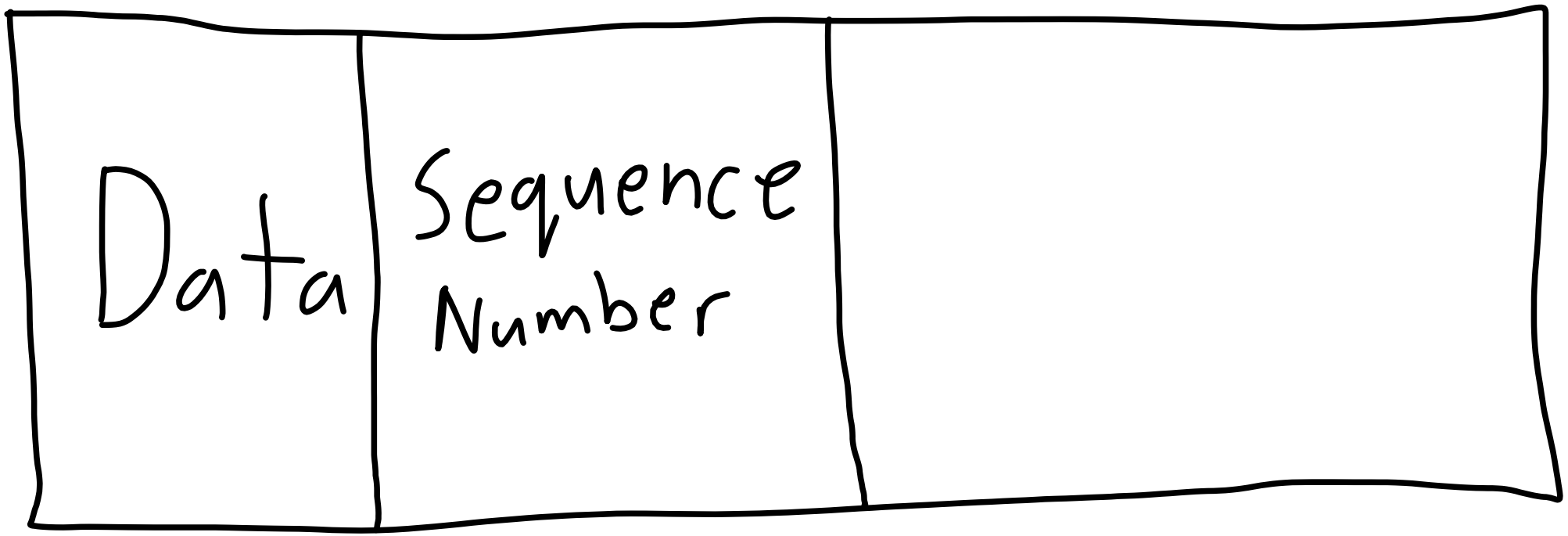

© Bishop Fox. All rights reserved worldwide.

# Sequence Number + HMAC



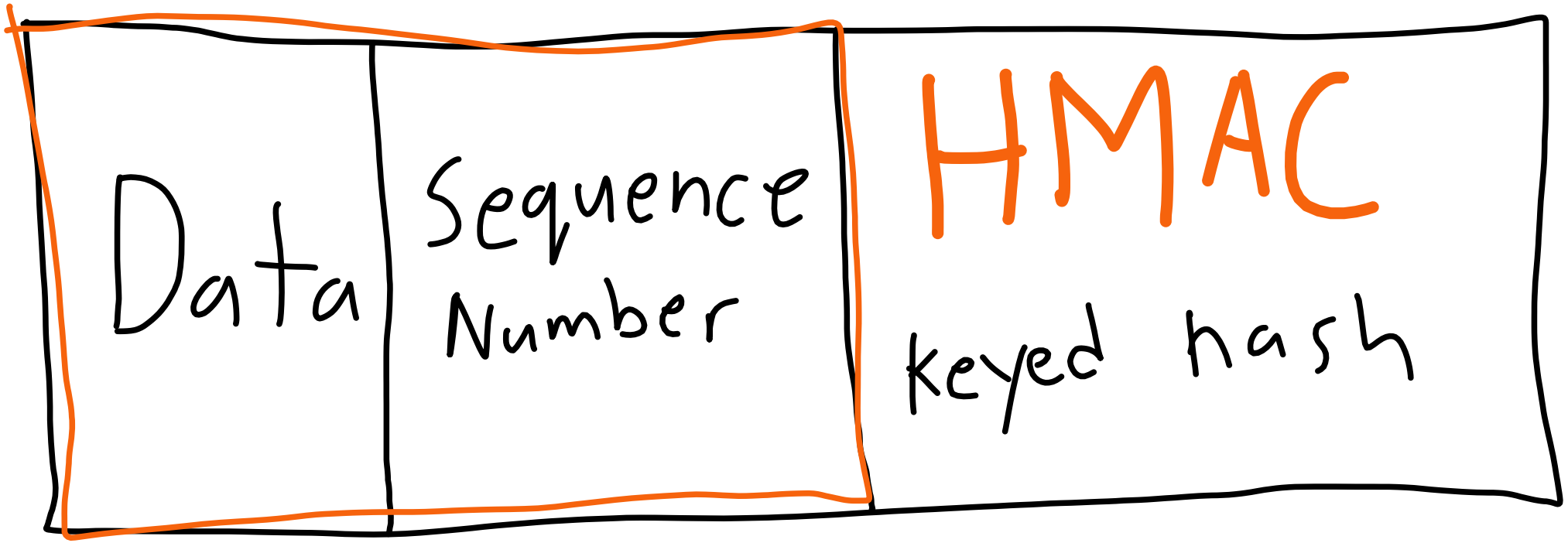

© Bishop Fox. All rights reserved worldwide.

# Sequence Number + HMAC




© Bishop Fox. All rights reserved worldwide.

# Sequence Number + HMAC




© Bishop Fox. All rights reserved worldwide.

# How Many Bits is Enough?

128-bits? - Cryptographic Strength

© Bishop Fox. All rights reserved worldwide.

# How Many Bits is Enough?

128-bits? - Cryptographic Strength

64-bits? - Edge of Enumeration

© Bishop Fox. All rights reserved worldwide.

# How Many Bits is Enough?

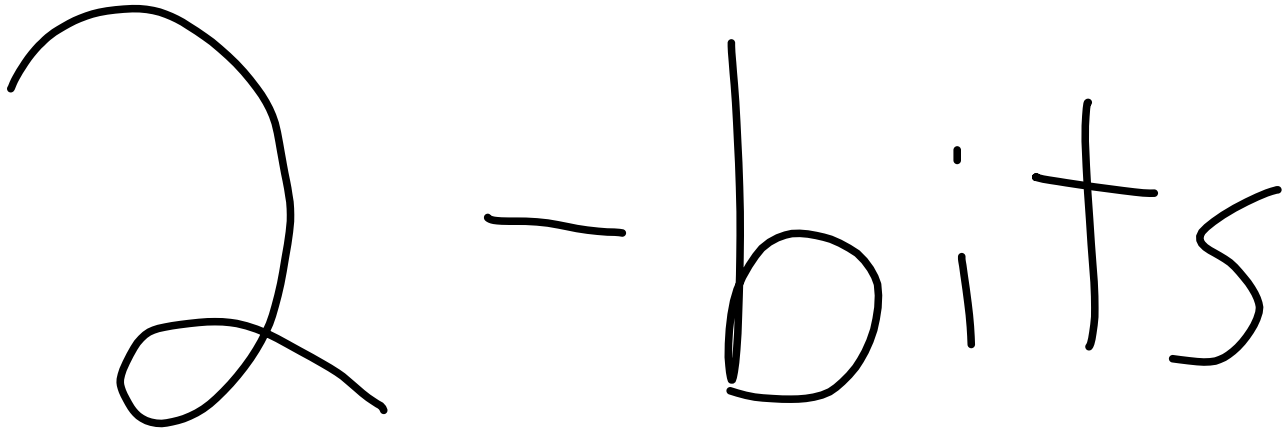
128-bits? — Cryptographic Strength

64-bits? — Edge of Enumeration

32-bits? — Fine, maybe?

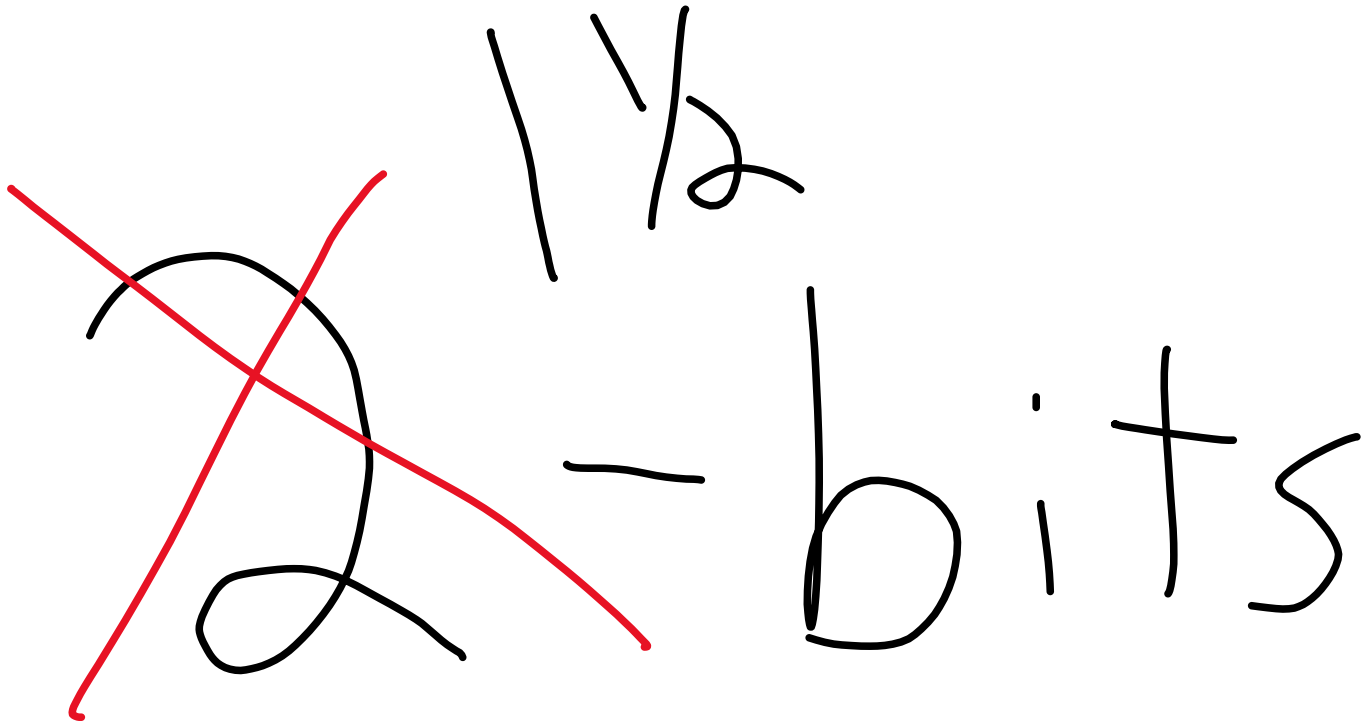
© Bishop Fox. All rights reserved worldwide.

# How Many Bits is Enough?




© Bishop Fox. All rights reserved worldwide.

# How Many Bits is Enough?




© Bishop Fox. All rights reserved worldwide.

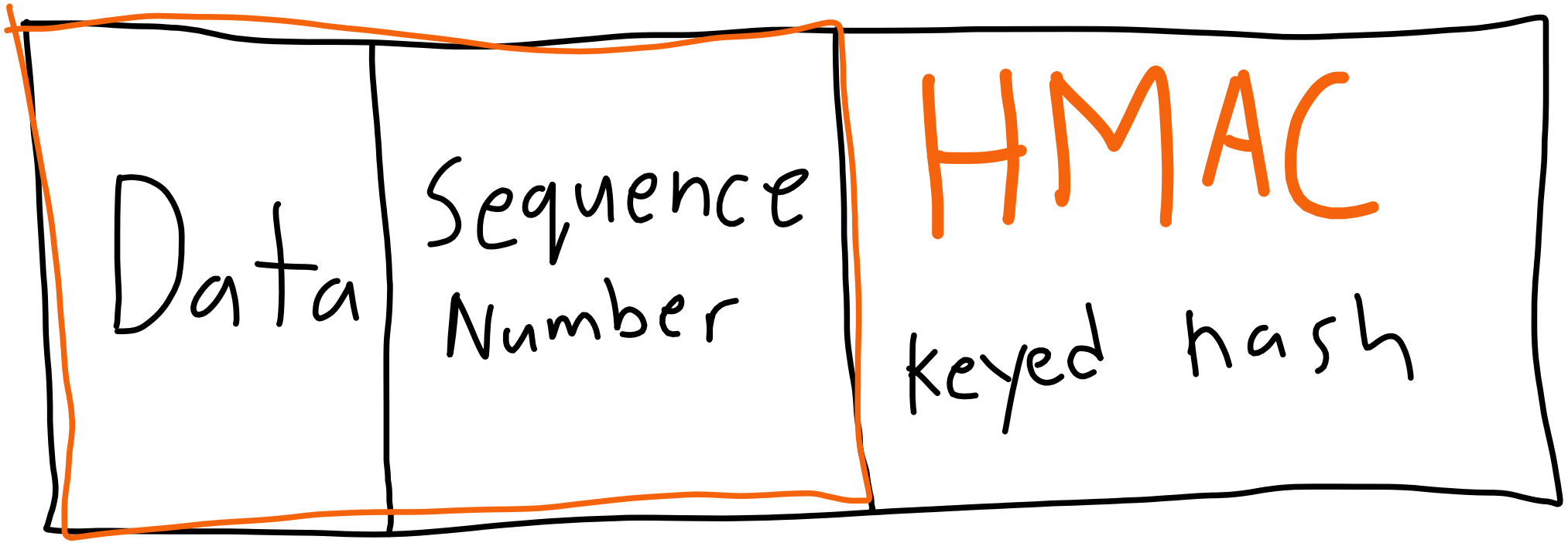
# The Protocol

## SQN Values

The sequence number is incremented by the CP from one command to the next, skipping zero: 0->1->2->3->1->... Non-zero sequence numbers support error recovery: the Control Panel (CP) acknowledges the last reply by sending the next command with the incremented sequence number,

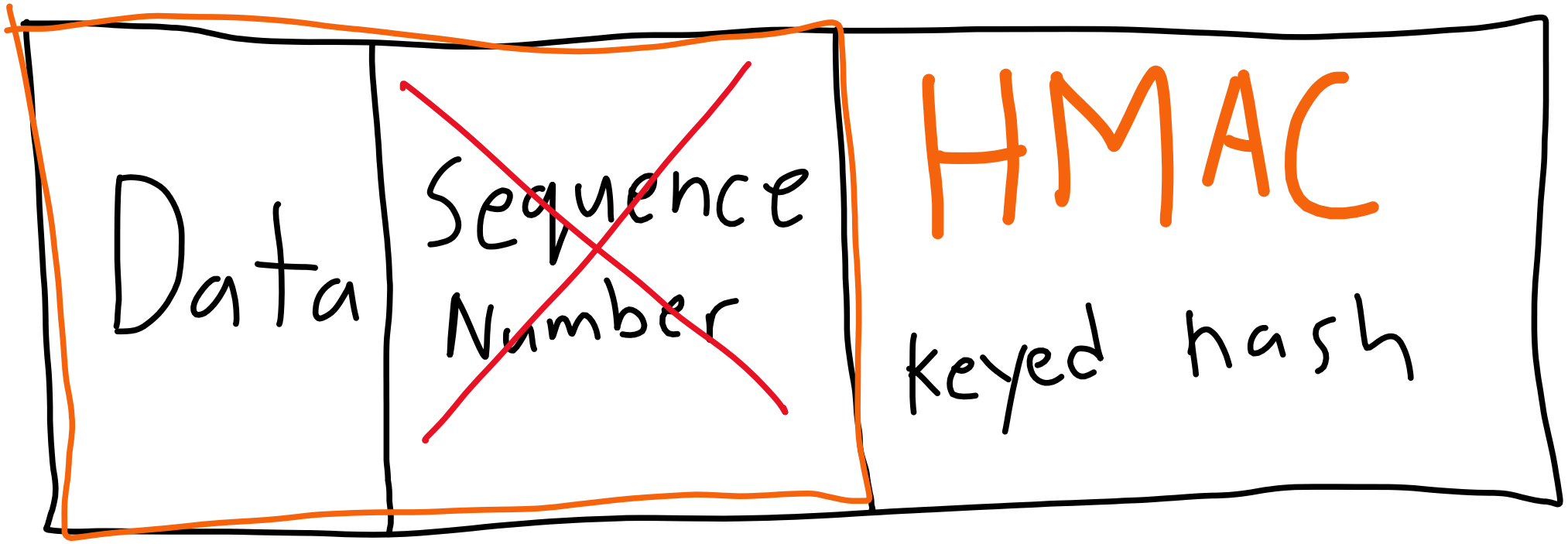
© Bishop Fox. All rights reserved worldwide.

# Sequence Number + HMAC



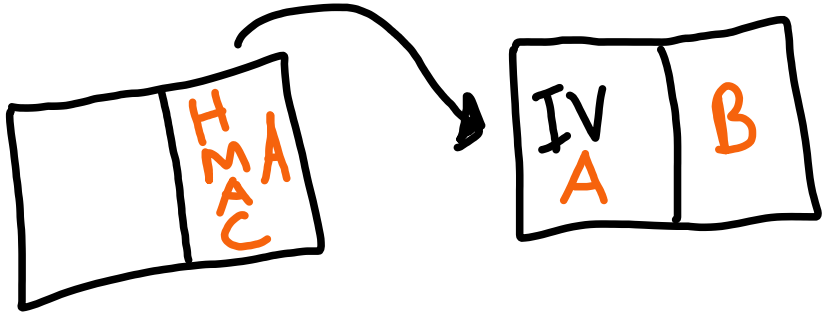

© Bishop Fox. All rights reserved worldwide.

# Sequence Number + HMAC



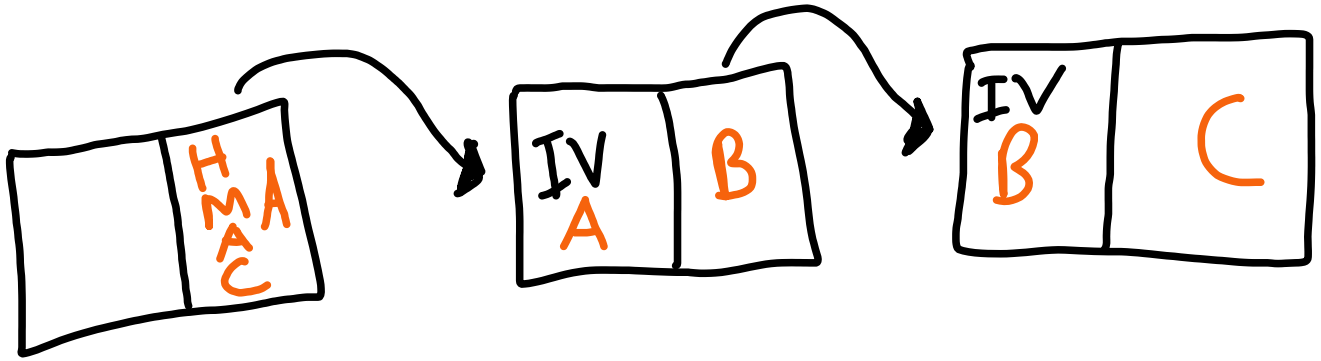

© Bishop Fox. All rights reserved worldwide.

# IV Chaining



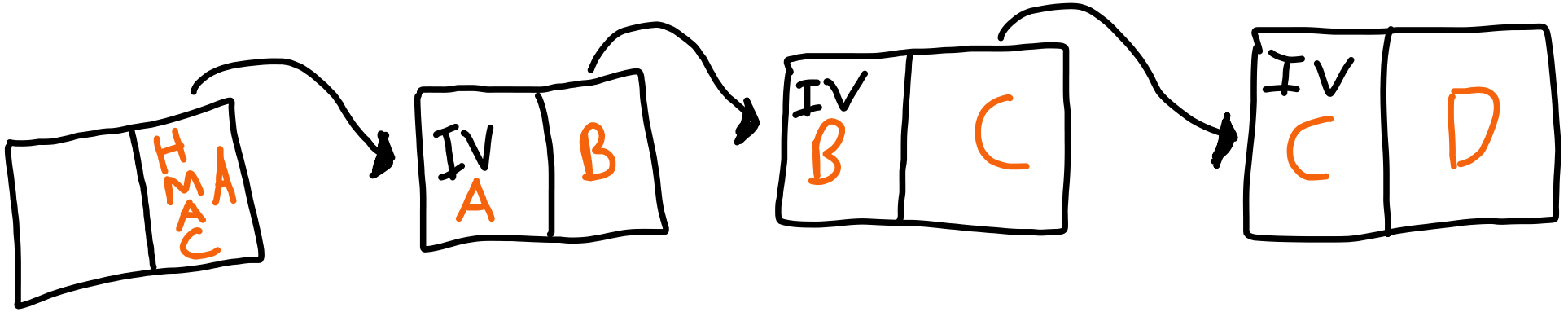

© Bishop Fox. All rights reserved worldwide.

# IV Chaining



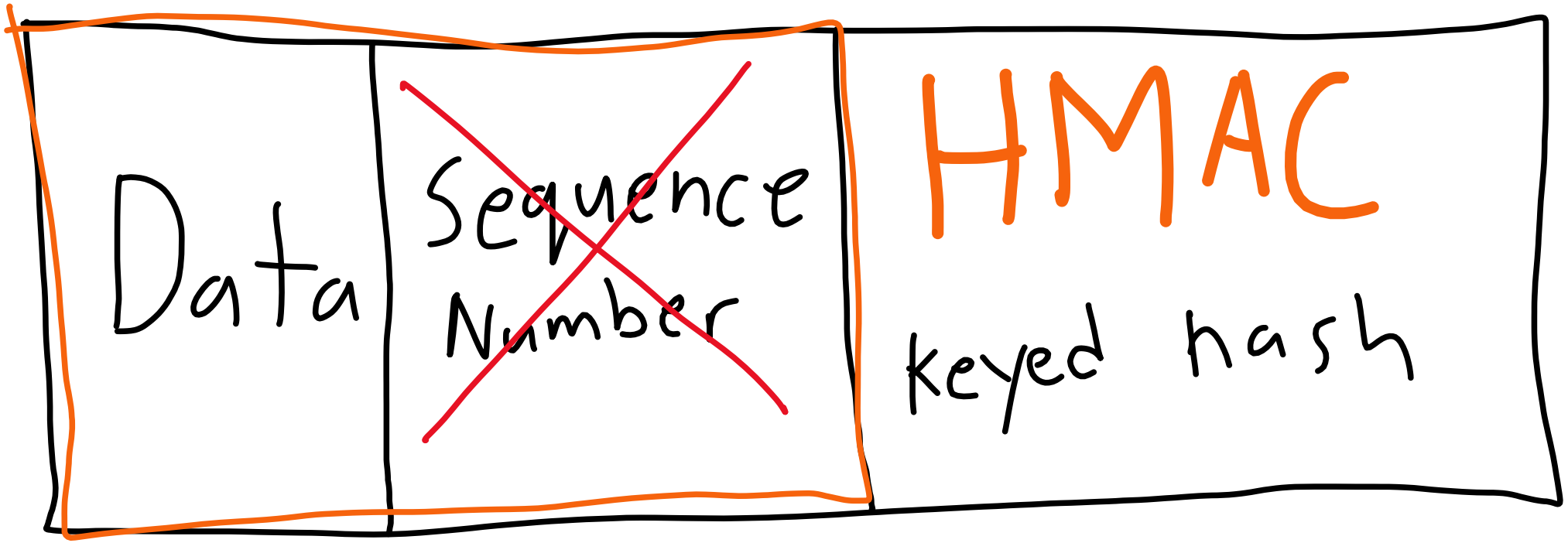

© Bishop Fox. All rights reserved worldwide.

# IV Chaining



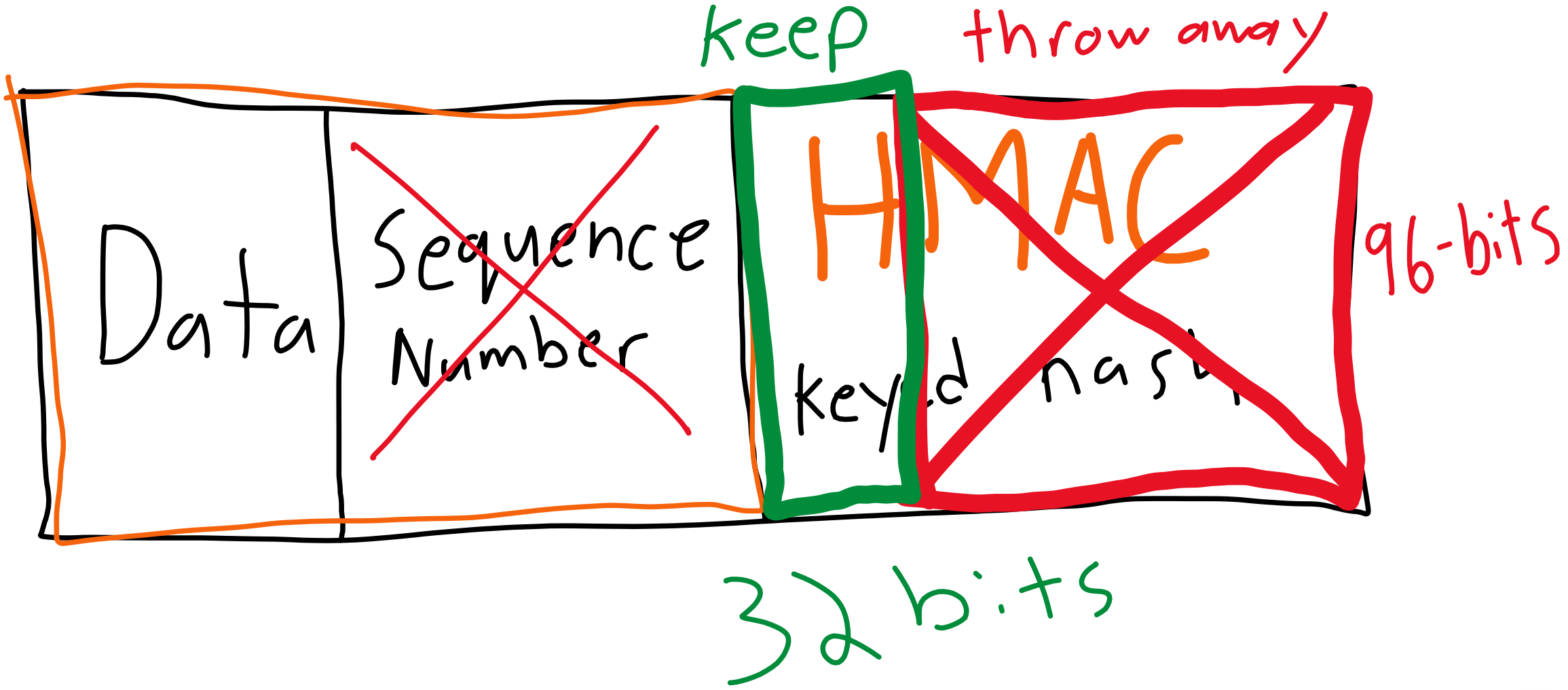

© Bishop Fox. All rights reserved worldwide.

# Sequence Number + HMAC




© Bishop Fox. All rights reserved worldwide.

# Sequence Number + HMAC




© Bishop Fox. All rights reserved worldwide.

# Overhead

## D.4.6 Message Authentication Code (MAC) Generation

General: MAC is computed for and appended only to messages whose SEC_BLK_TYPE is SCS_15, SCS_16, SCS_17, and SCS_18.,The AES algorithm is applied in CBC mode using S-MAC1 as the key for all blocks, except the last one, and using S-MAC2 as the key for the last block. If the message contains only one block, then only S-MAC2 is used.

ICV values: The ICV is initialized during the Secure Connection Sequence by the PD and is passed to the CP during SCS_14 in reply osdp_RMAC_I.

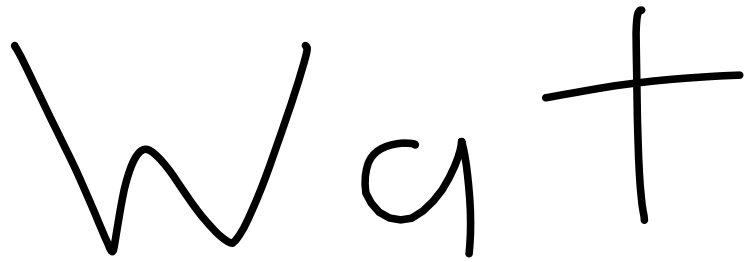
R-MAC – the ICV value for generating the R-MAC is the previously received C-MAC.

C-MAC – the ICV value for generating the C-MAC is the previously received R-MAC.

After the initial OSDP-SC setup, in order to reduce the message size and transmission time overhead, the messages will contain only a partial MAC. For messages whose SEC_BLK_TYPE is SCS_15, SCS_16, SCS_17, and SCS_18 only the first four bytes of the computed MAC are sent. The MAC verification will locally generate the full MAC[16] and compare the actual bytes that were received.

© Bishop Fox. All rights reserved worldwide.

# Overhead




only the first four bytes of the computed MAC are sent.

only the first four bytes

© Bishop Fox. All rights reserved worldwide.



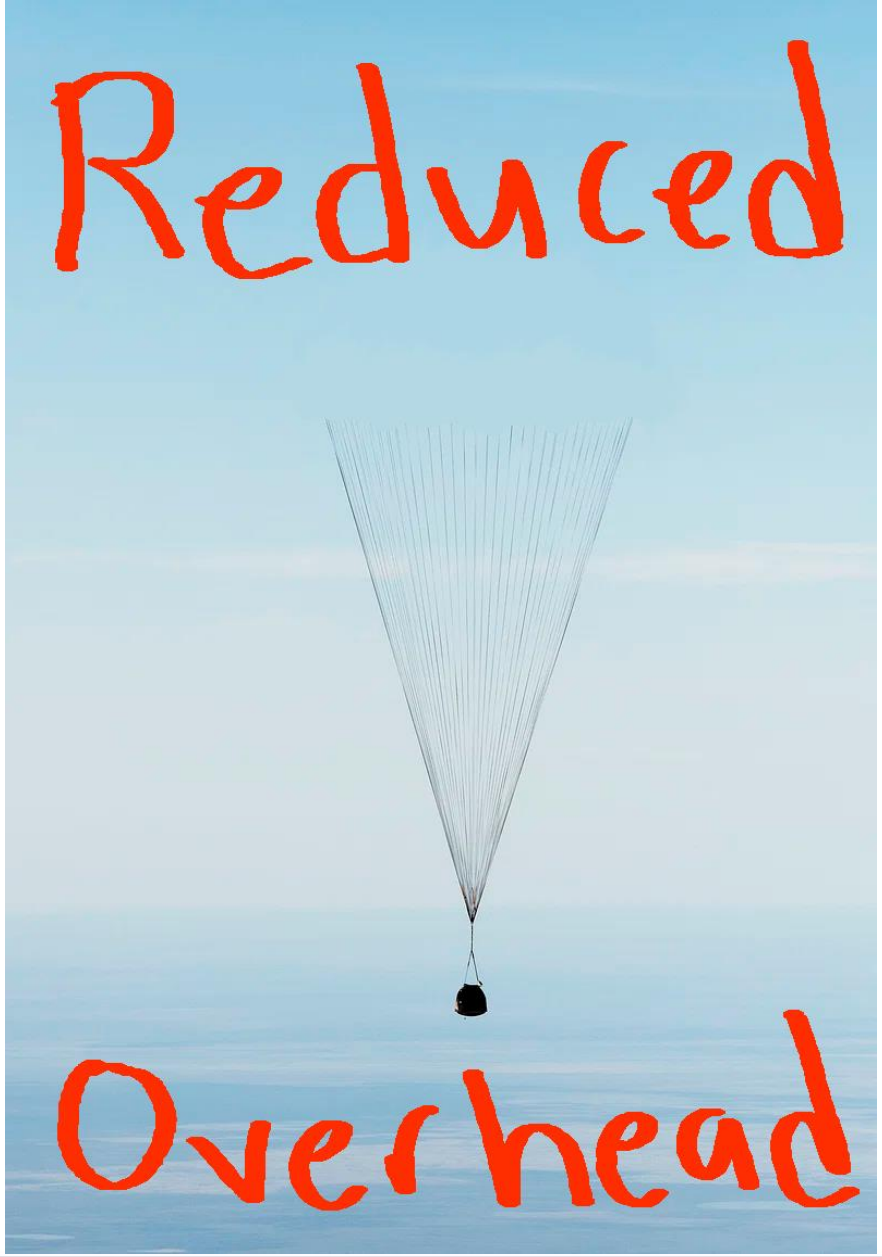

© Bishop Fox. All rights reserved worldwide.




© Bishop Fox. All rights reserved worldwide.



© Bishop Fox. All rights reserved worldwide.




© Bishop Fox. All rights reserved worldwide.

# Math

$2^{31}$ attempts (on average)

© Bishop Fox. All rights reserved worldwide.

# Math

$2^{31}$ attempts (on average)

115,200 baud (RS-485)

© Bishop Fox. All rights reserved worldwide.

# Math

$2^{31}$ attempts (on average)

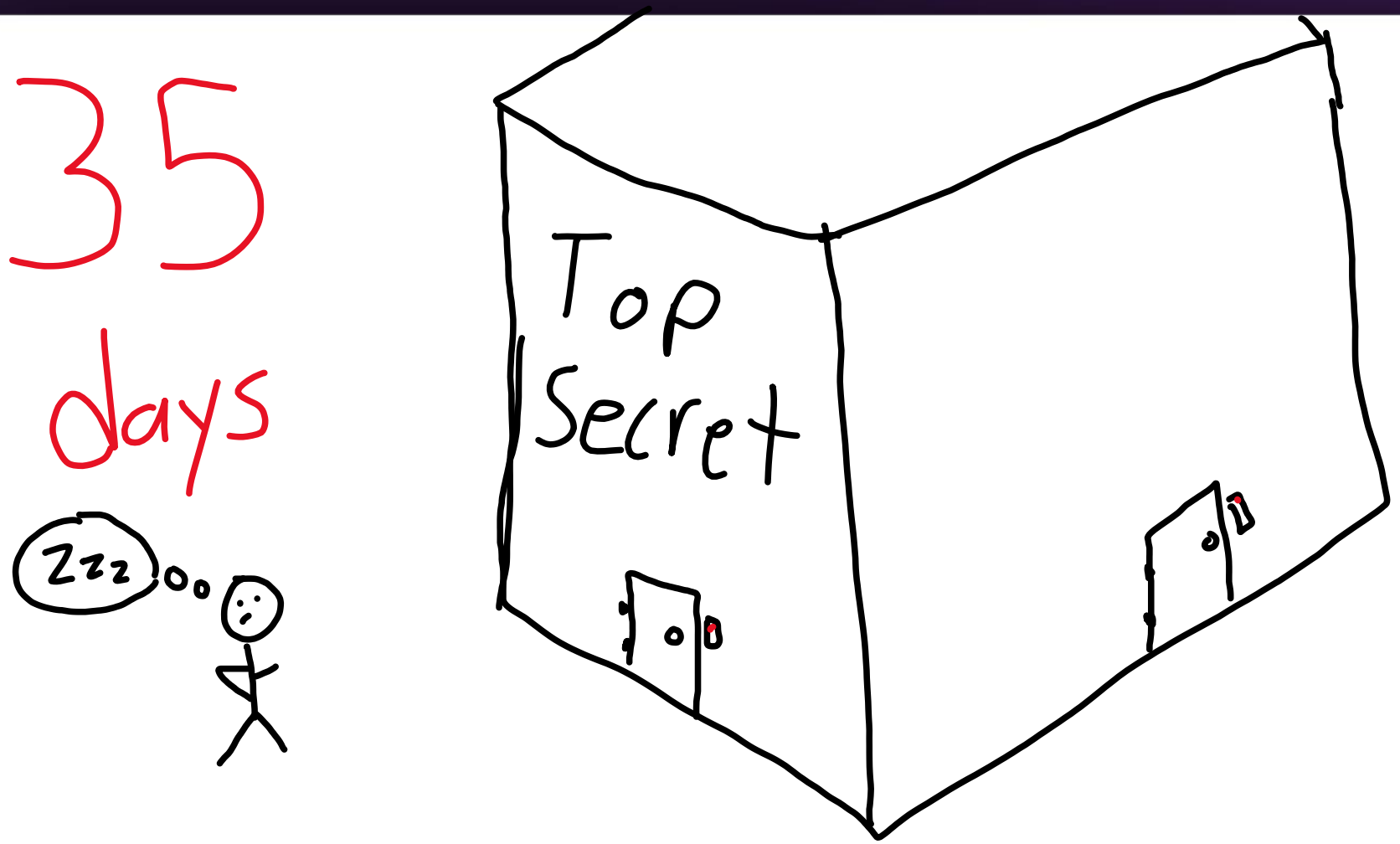
115,200 baud (RS-485)

~ success after

35 days

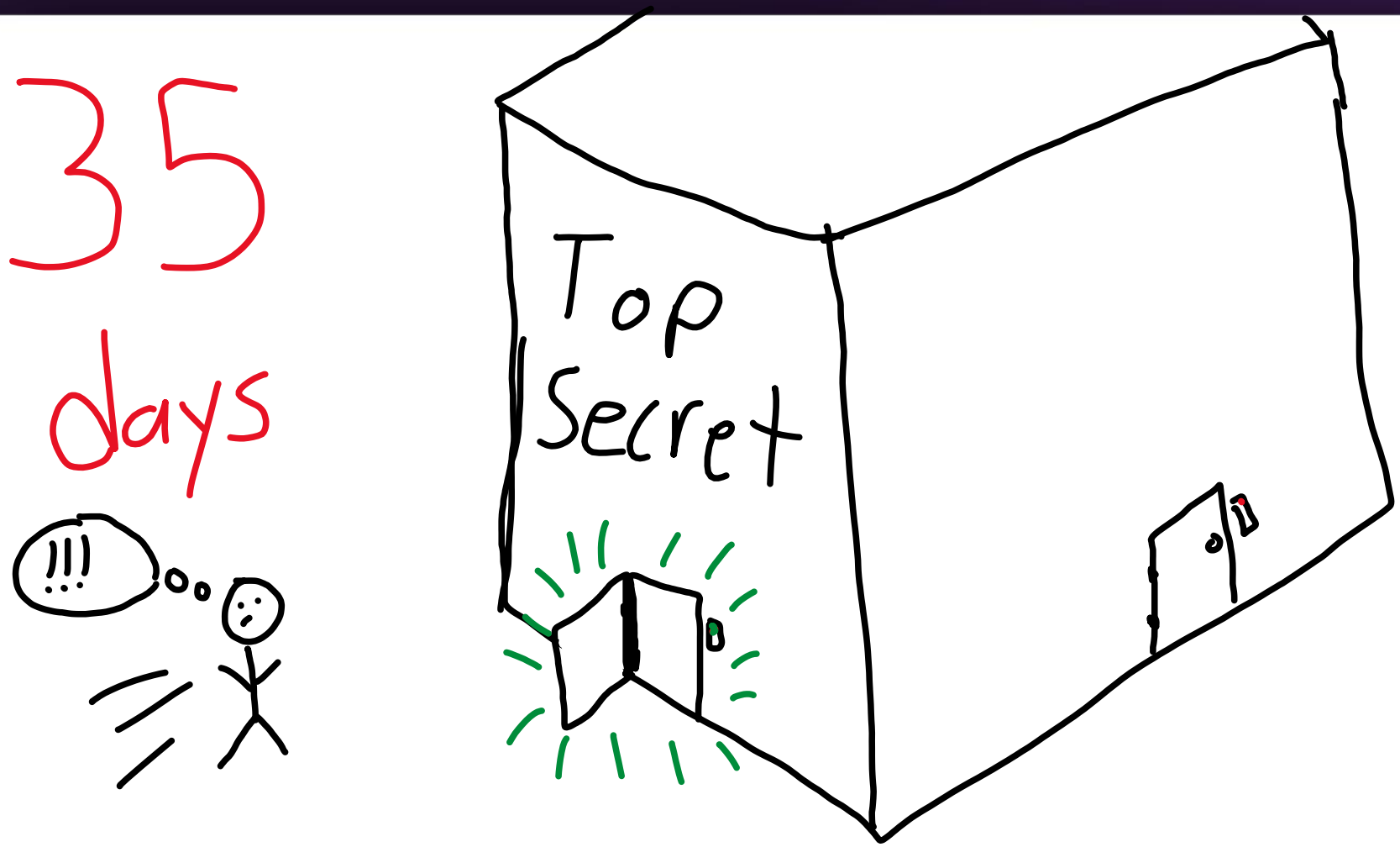
© Bishop Fox. All rights reserved worldwide.

# Math



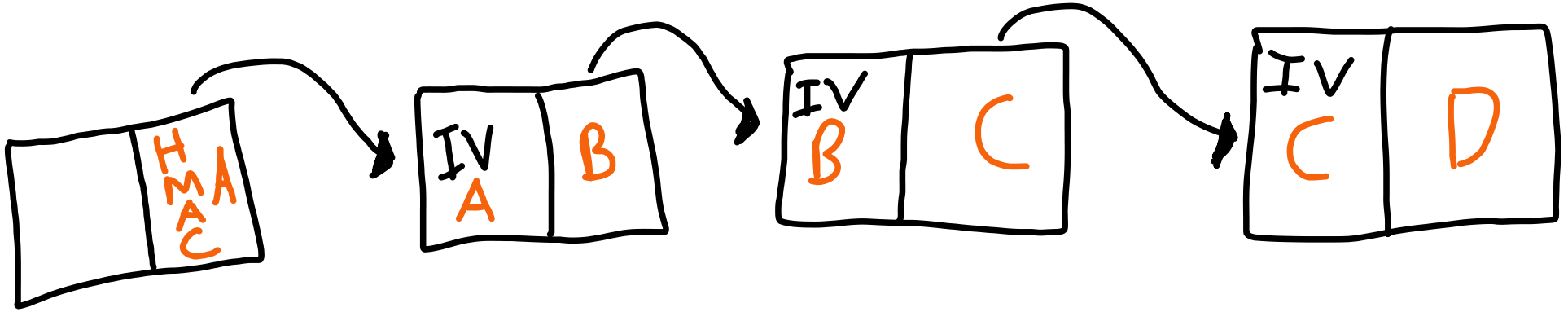

© Bishop Fox. All rights reserved worldwide.

# Math



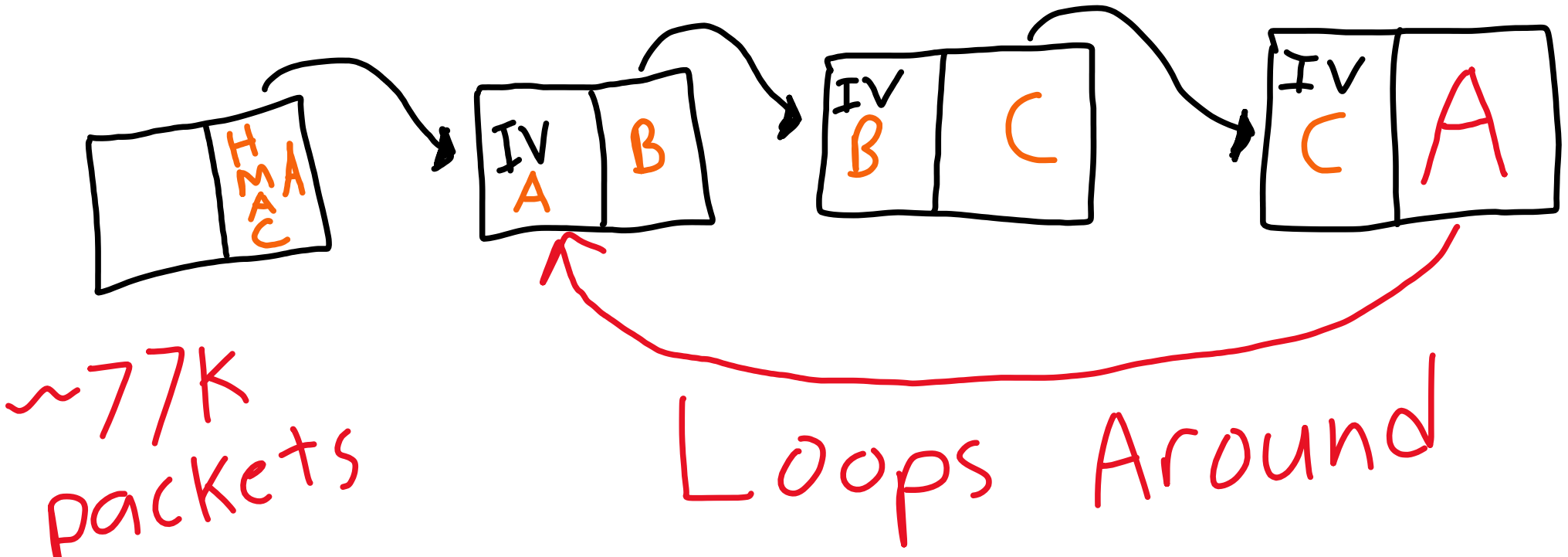

© Bishop Fox. All rights reserved worldwide.

# Happy Birthday



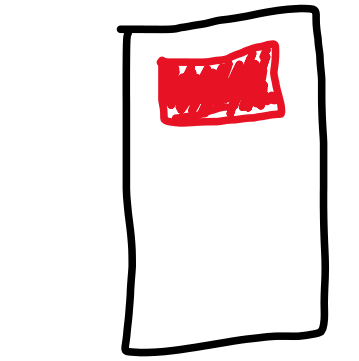

© Bishop Fox. All rights reserved worldwide.

# Happy Birthday

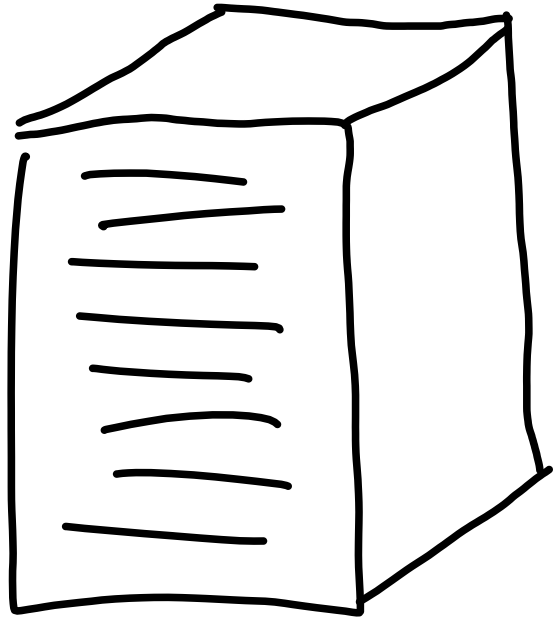



© Bishop Fox. All rights reserved worldwide.

# Session Keys



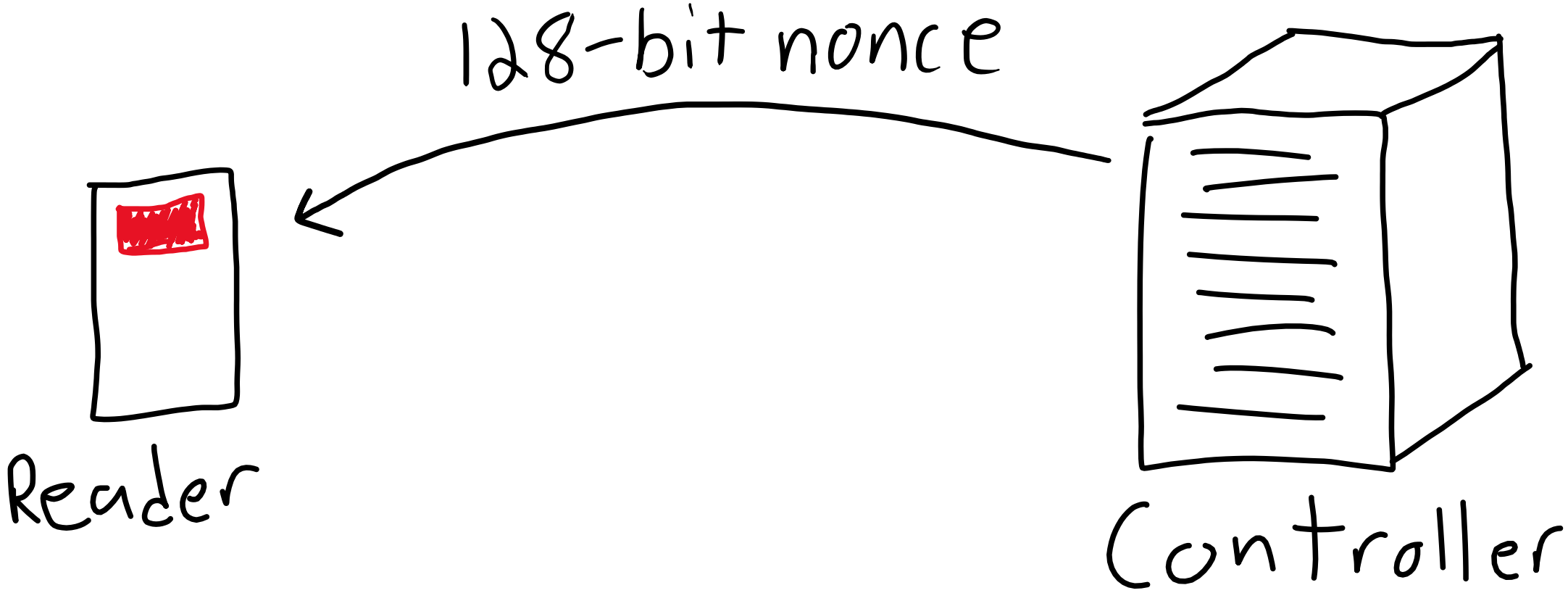
Reader



Controller

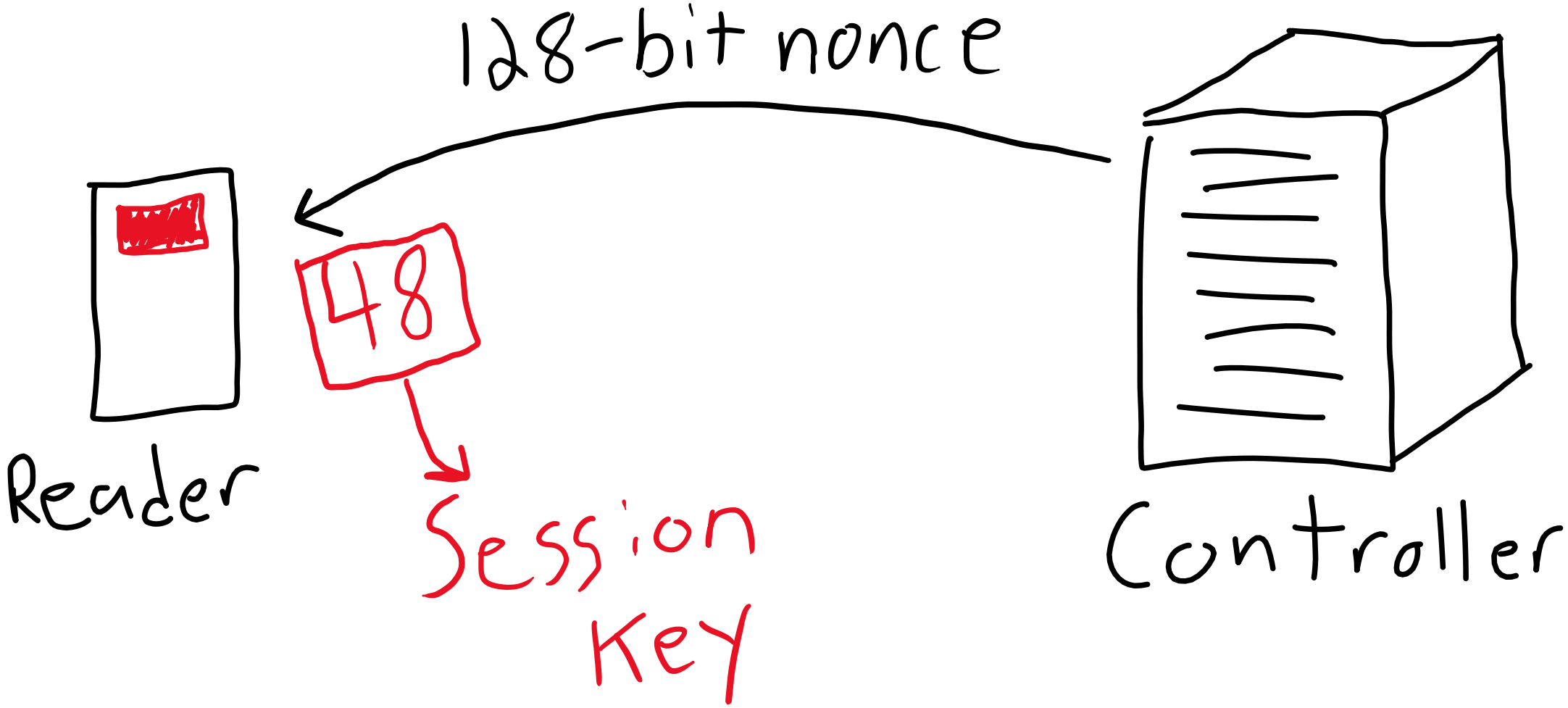
© Bishop Fox. All rights reserved worldwide.

# Session Keys




© Bishop Fox. All rights reserved worldwide.

# Session Keys




© Bishop Fox. All rights reserved worldwide.

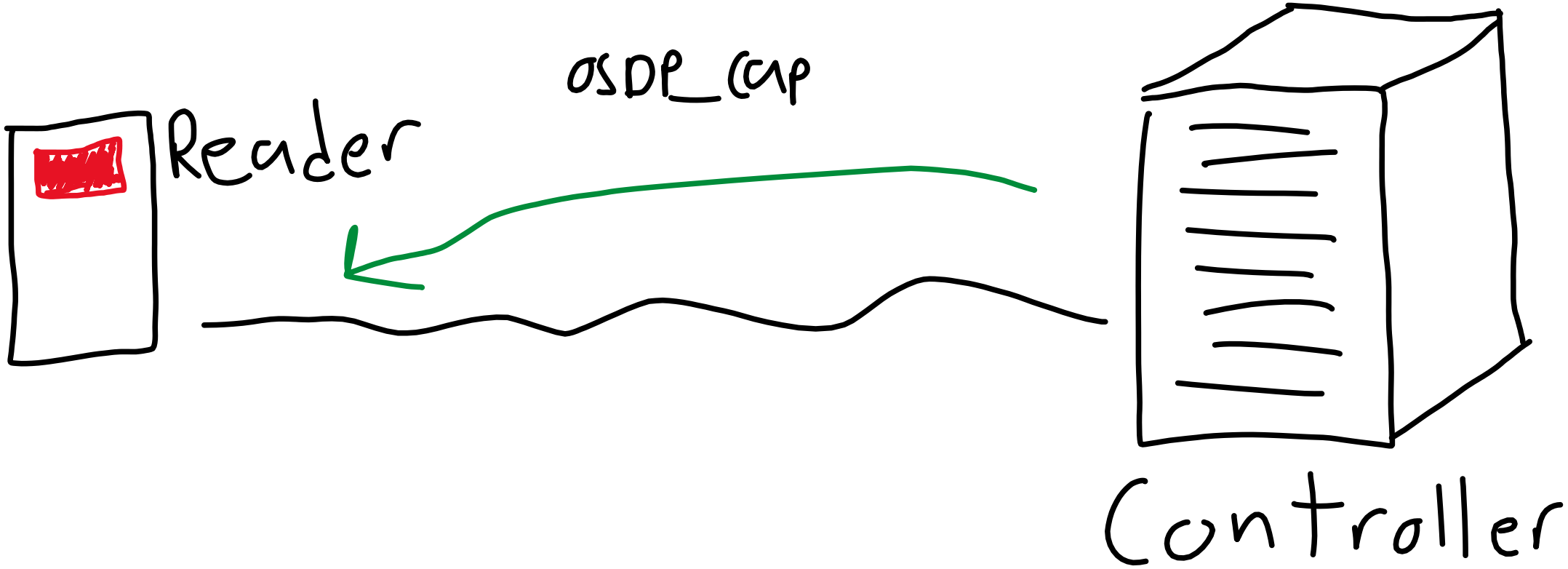
# Demo #2

Downgrade

Attack

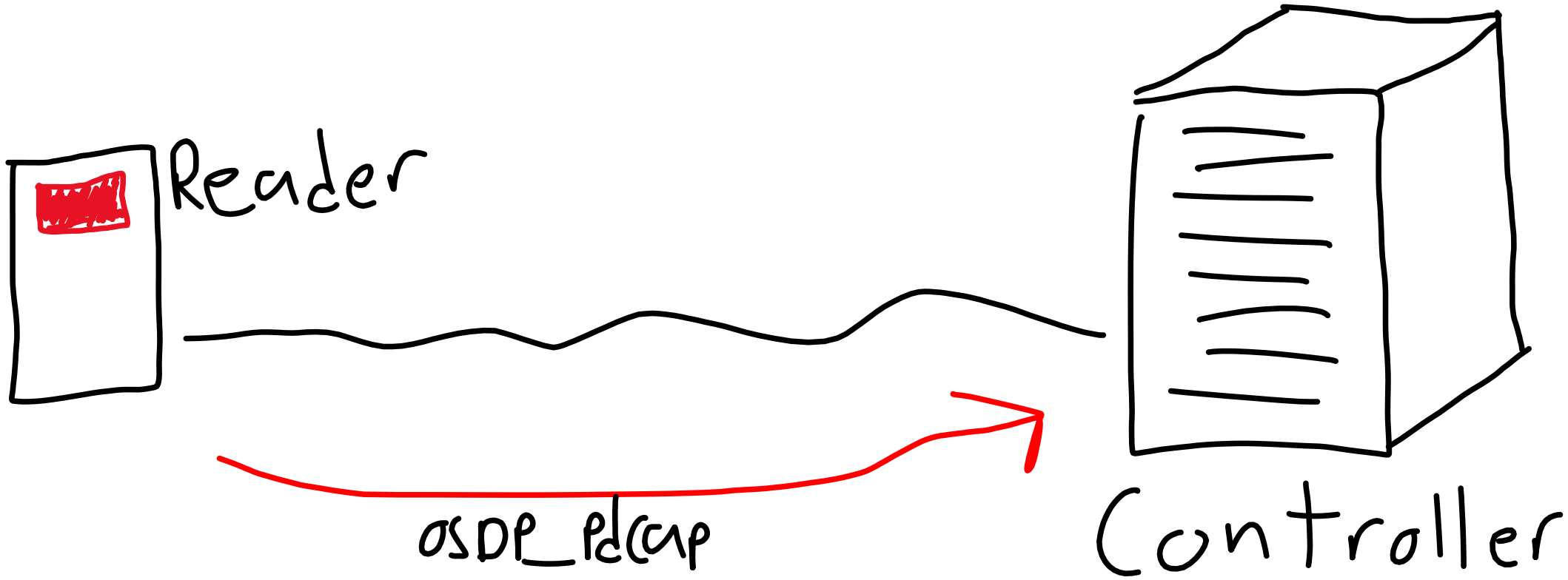
© Bishop Fox. All rights reserved worldwide.

# Me no speak AES




© Bishop Fox. All rights reserved worldwide.

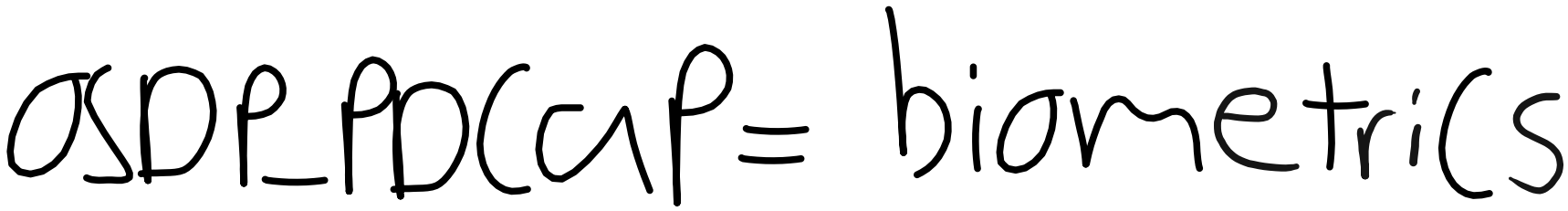
# Me no speak AES




© Bishop Fox. All rights reserved worldwide.

THERE'S ALWAYS ONE...

# Me no speak AES



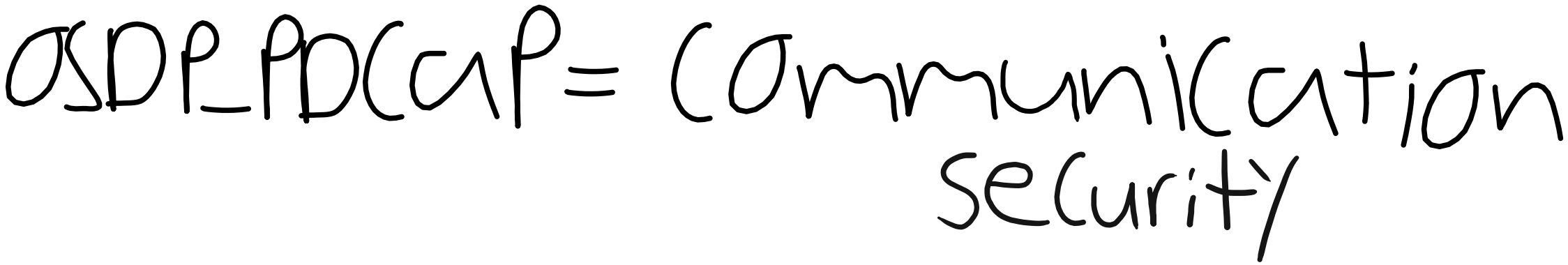

© Bishop Fox. All rights reserved worldwide.

# Me no speak AES



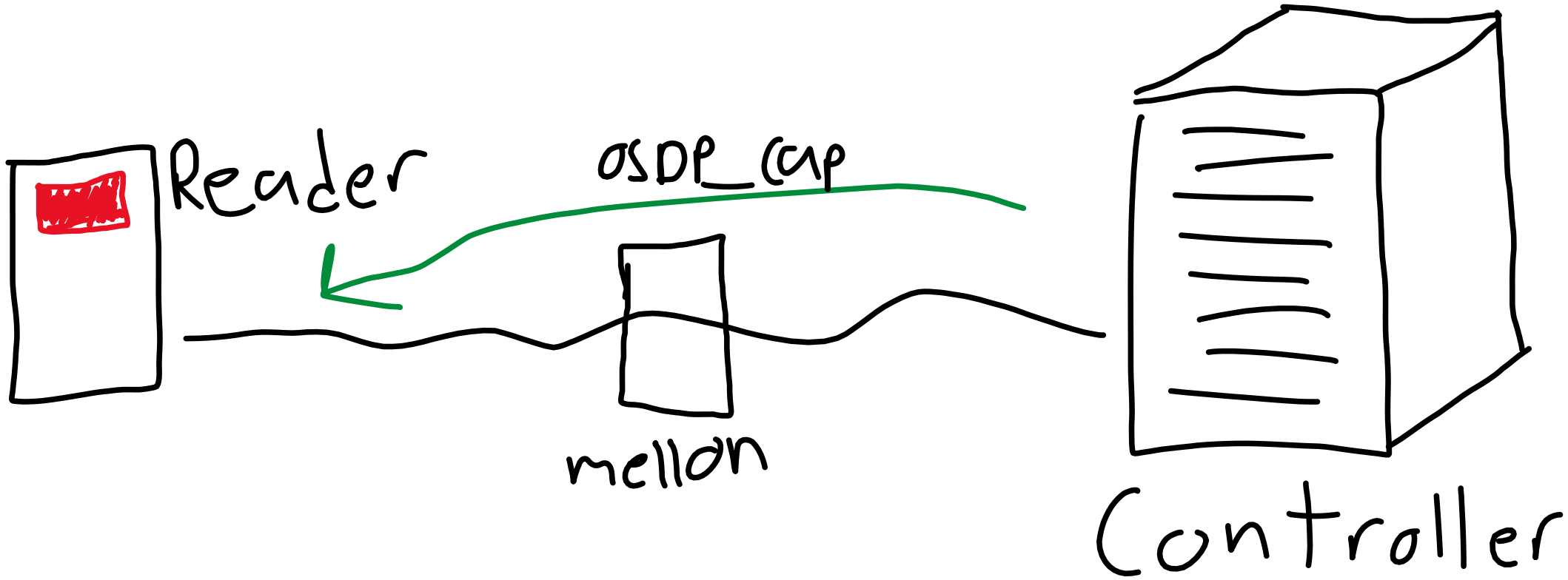

© Bishop Fox. All rights reserved worldwide.

# Me no speak AES



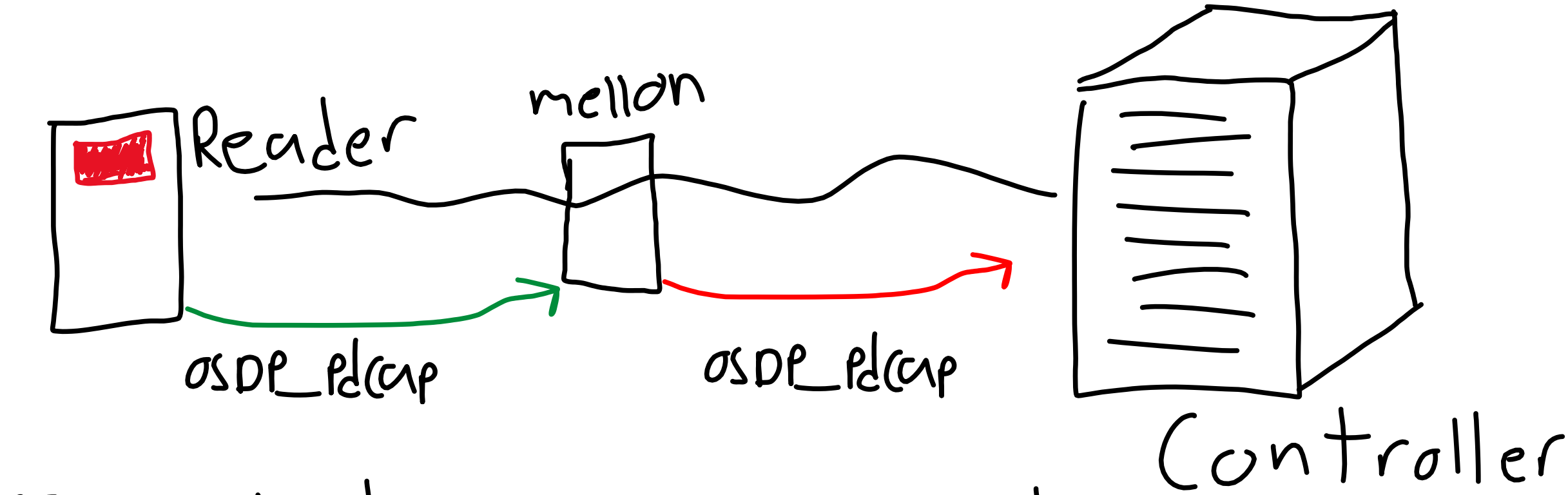

© Bishop Fox. All rights reserved worldwide.

# Me no speak AES



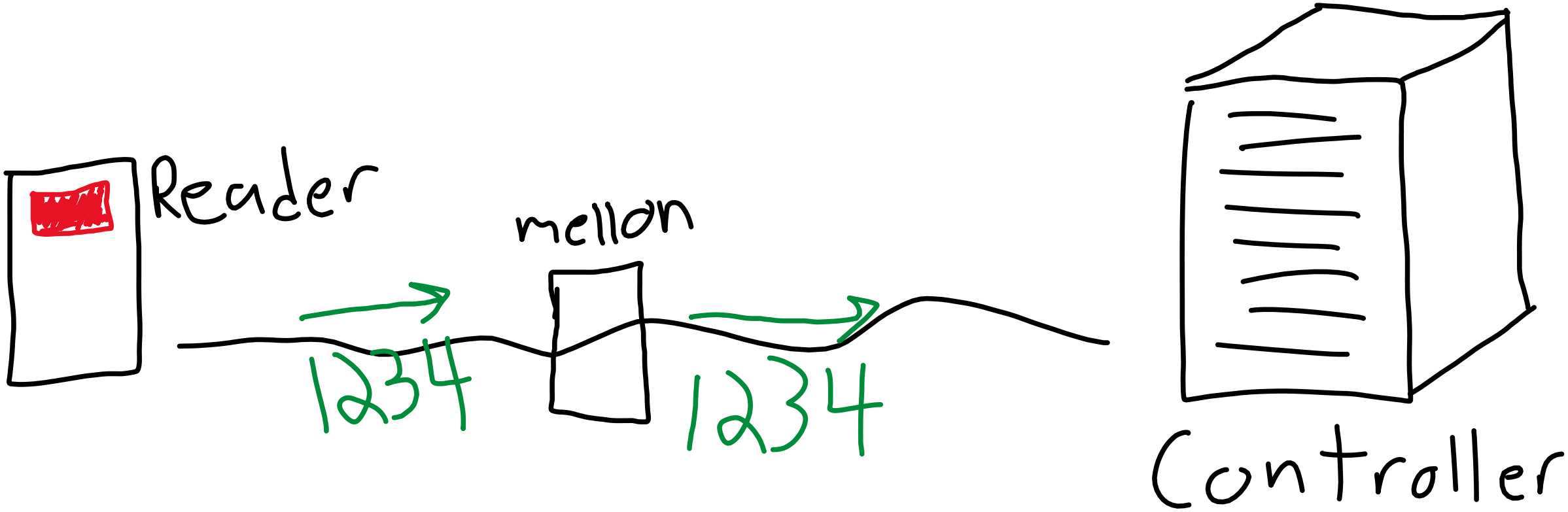

© Bishop Fox. All rights reserved worldwide.

# Me no speak AES




© Bishop Fox. All rights reserved worldwide.

# Me no speak AES




© Bishop Fox. All rights reserved worldwide.

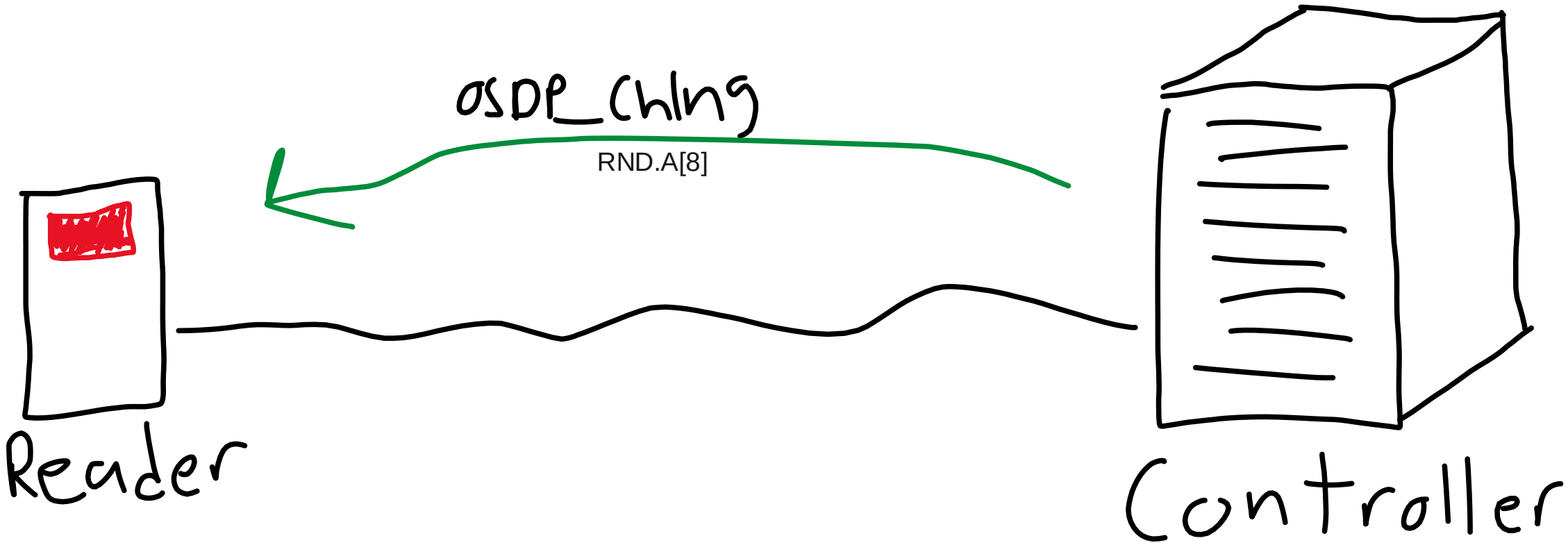
# Protocol WTF #2

Stop Making

Null Ciphers

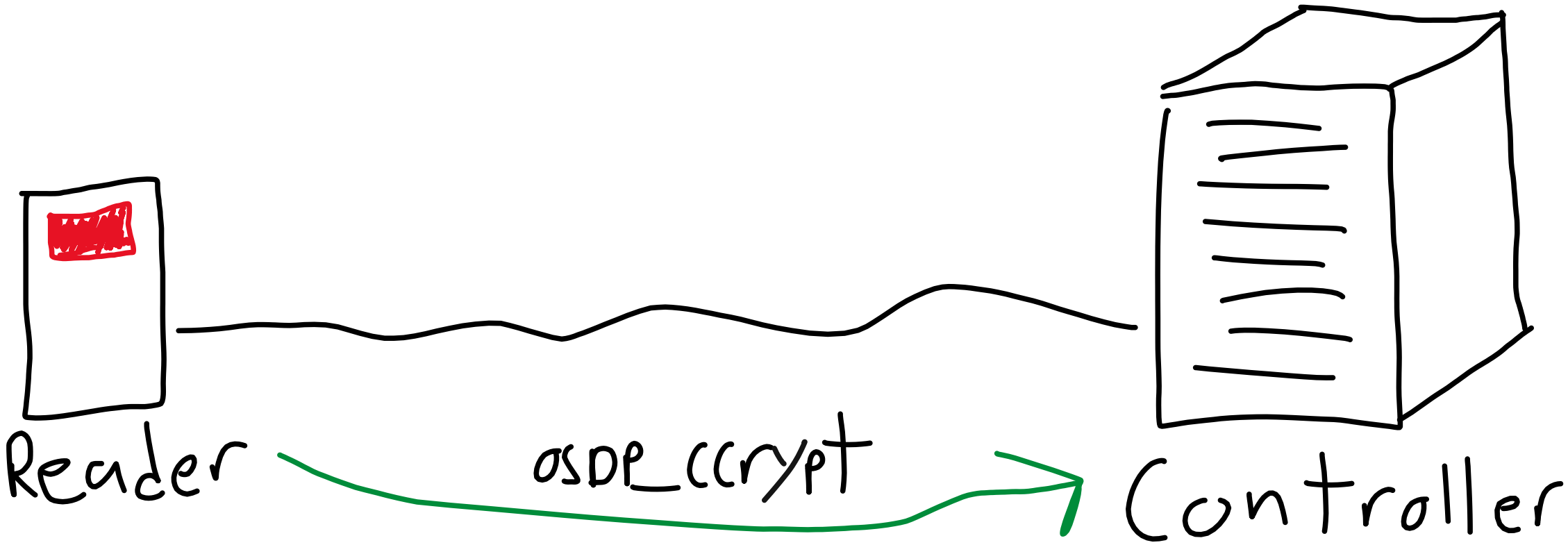
© Bishop Fox. All rights reserved worldwide.

# "Secure" Channel - Connection Sequence: SCS_11




© Bishop Fox. All rights reserved worldwide.

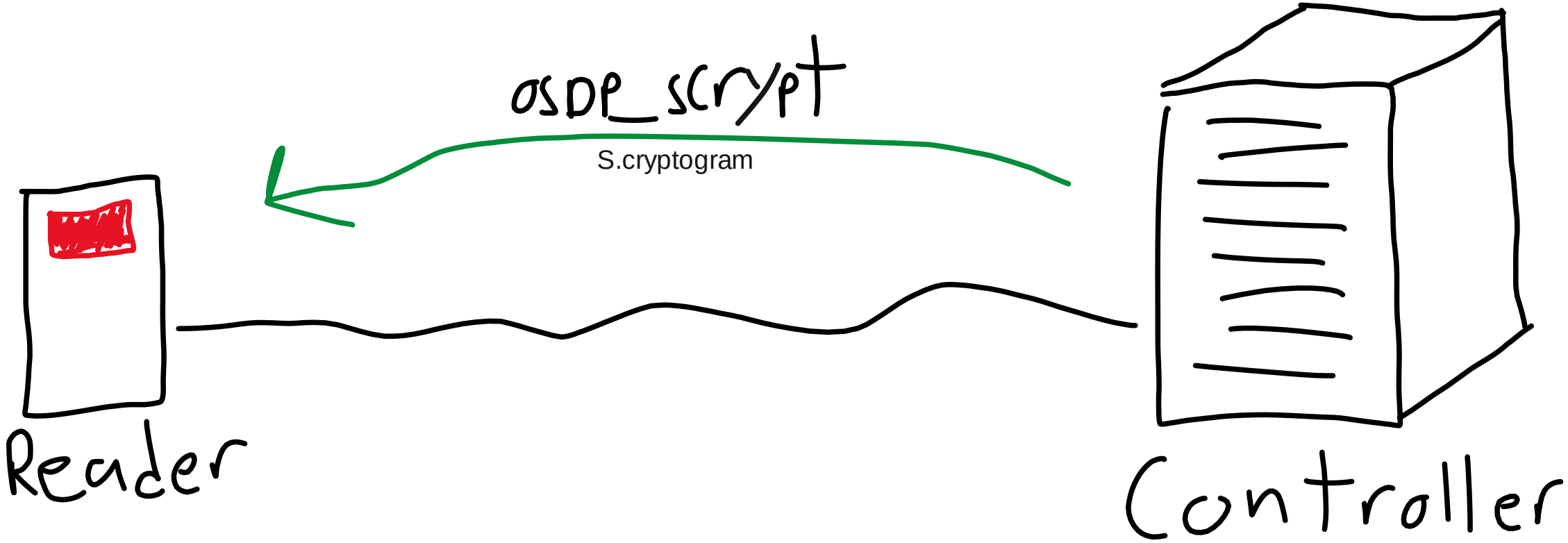
# "Secure" Channel - Connection Sequence: SCS_12




RND.B[8]
C.Cryptogram
PD's cUID

© Bishop Fox. All rights reserved worldwide.

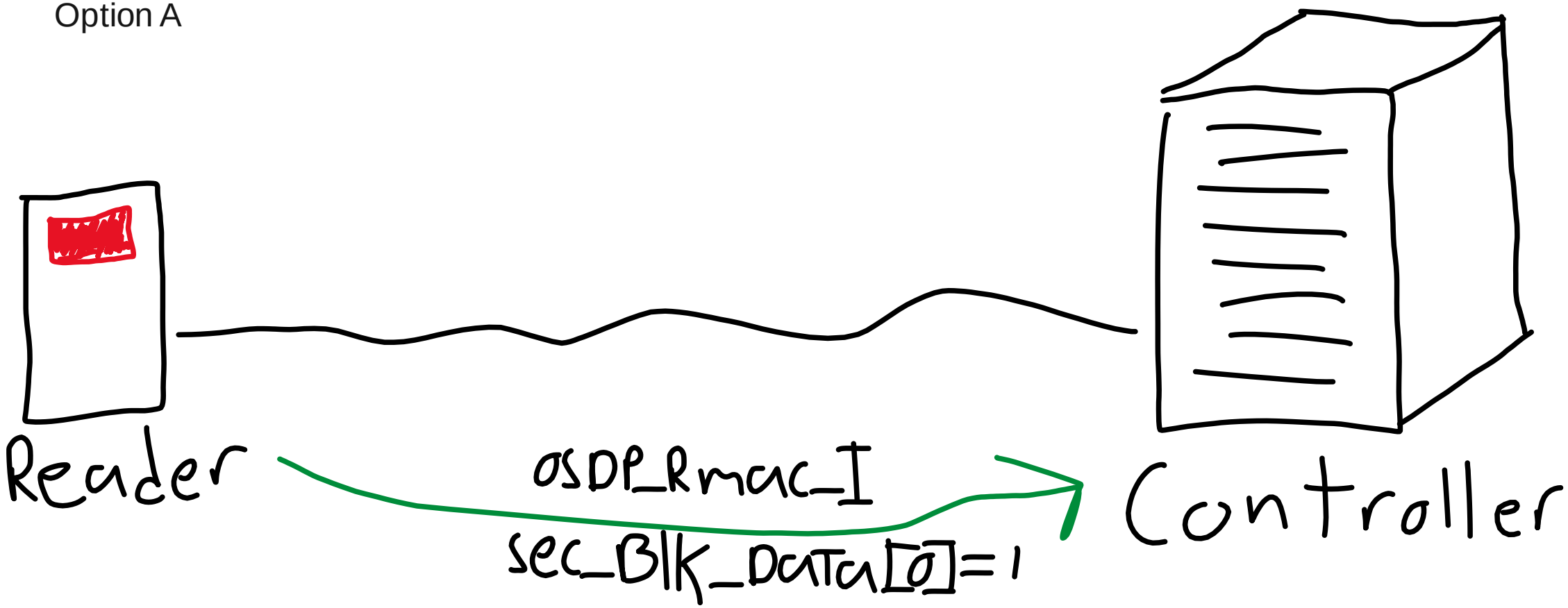
# "Secure" Channel - Connection Sequence: SCS_13




© Bishop Fox. All rights reserved worldwide.

# "Secure" Channel - Connection Sequence: SCS_14

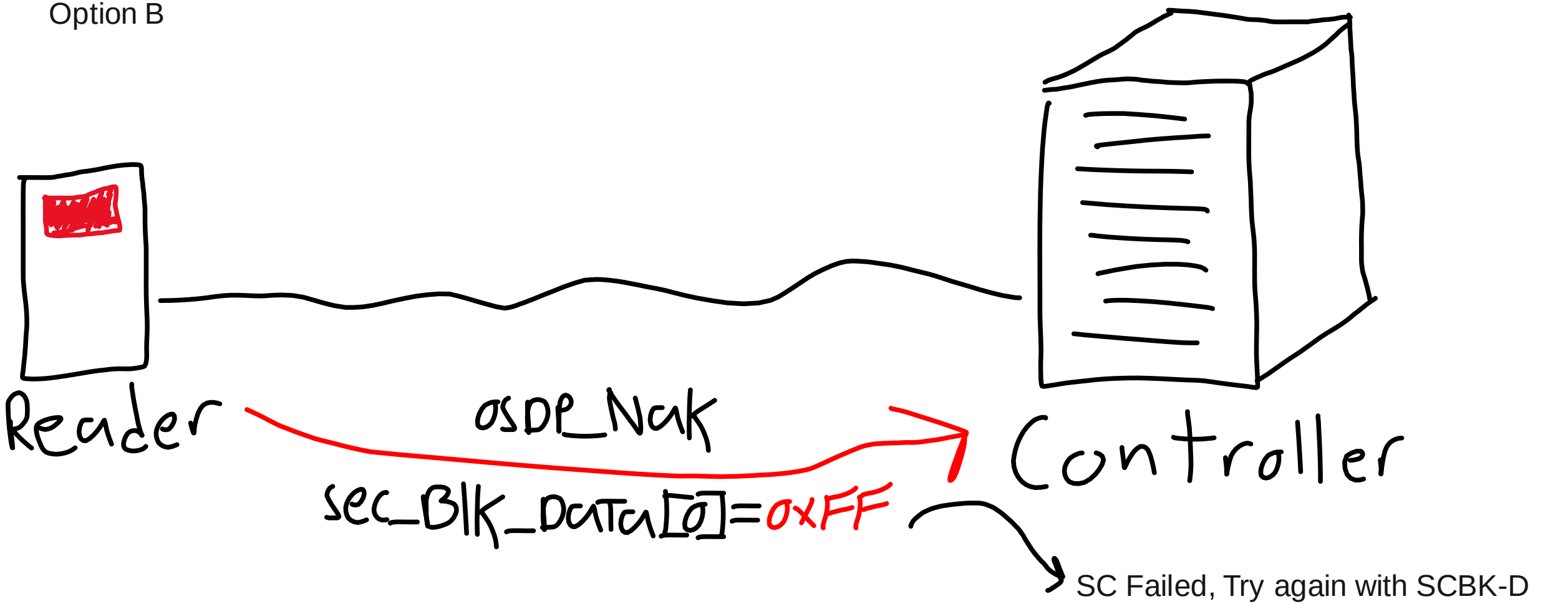
Option A




© Bishop Fox. All rights reserved worldwide.

# "Secure" Channel - Connection Sequence: SCS_14

Option B



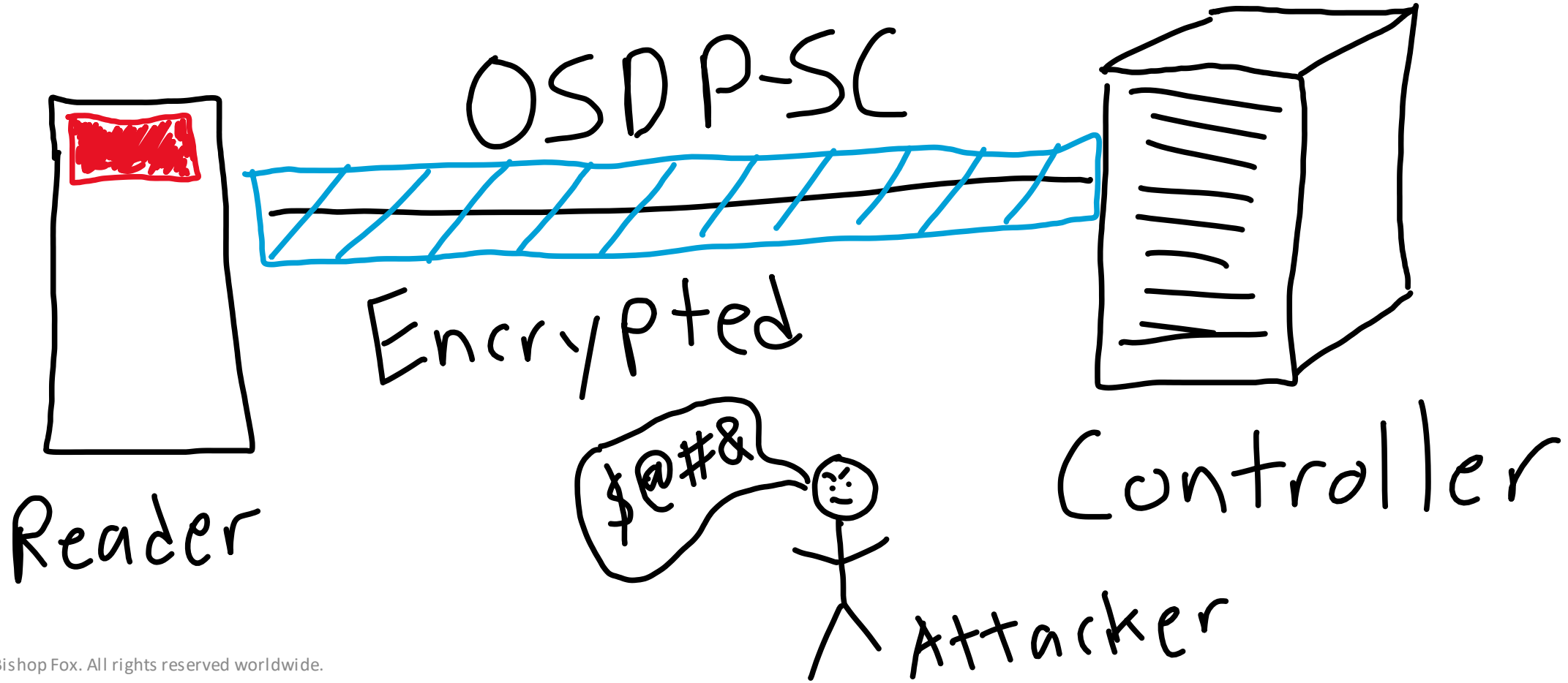



© Bishop Fox. All rights reserved worldwide.

# "Secure" Channel - Established

### D.3.2 Communication during a Secure Channel Session

The successful completion of the synchronization sequence SCS_11 through SCS_14 confirms that the CP and PD established a valid Secure Channel Session. In order to maintain the SCS, the CP must send each message with SEC_BLK_TYPE set to SCS_15 or SCS_17, and the PD must send each if its replies with SEC_BLK_TYPE set to SCS_16 or SCS_18.




© Bishop Fox. All rights reserved worldwide.

# "Secure" Channel - Connection Sequence: SCS_15 & SCS_16

### D.3.2.1 SCS_15 CP->PD

The DATA field is sent in plain text (unencrypted)

Note: this form provides Message Authentication, but does not contain encrypted DATA.

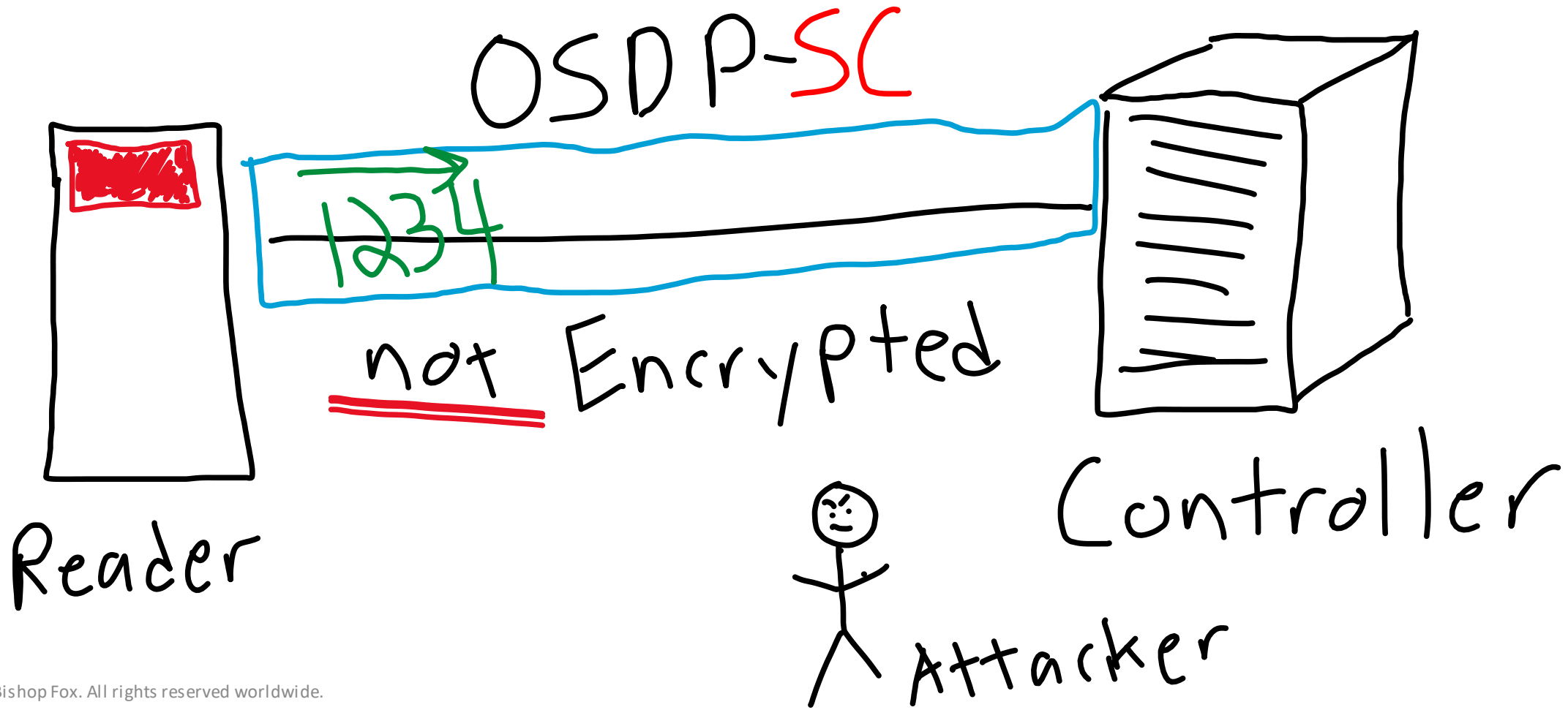
### D.3.2.2 SCS_16 PD->CP

The data field is sent in plain text (unencrypted)

Note: this form provides Message Authentication, but does not contain encrypted DATA.

© Bishop Fox. All rights reserved worldwide.

# "Secure" Channel - Established




© Bishop Fox. All rights reserved worldwide.

# "Secure" Channel - SCS_15 & SCS_16



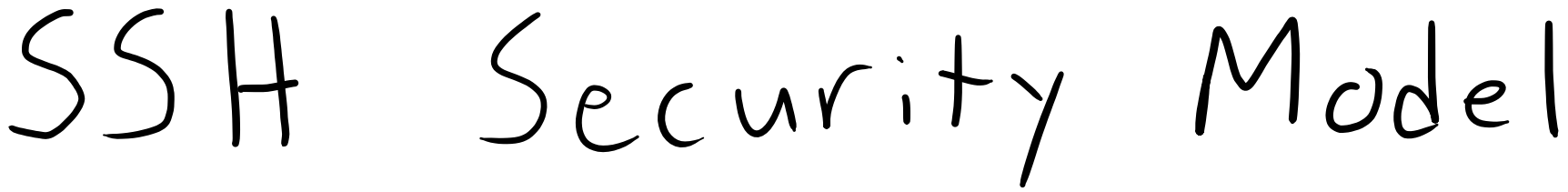

© Bishop Fox. All rights reserved worldwide.

# Demo #3

Install-mode

Attack

© Bishop Fox. All rights reserved worldwide.




© Bishop Fox. All rights reserved worldwide.

# Install-Mode

SSH Security Model

One-time Insecure Setup

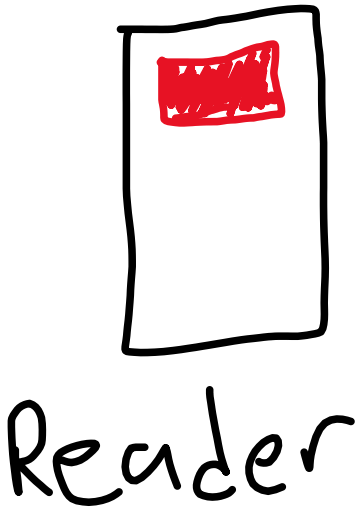
© Bishop Fox. All rights reserved worldwide.

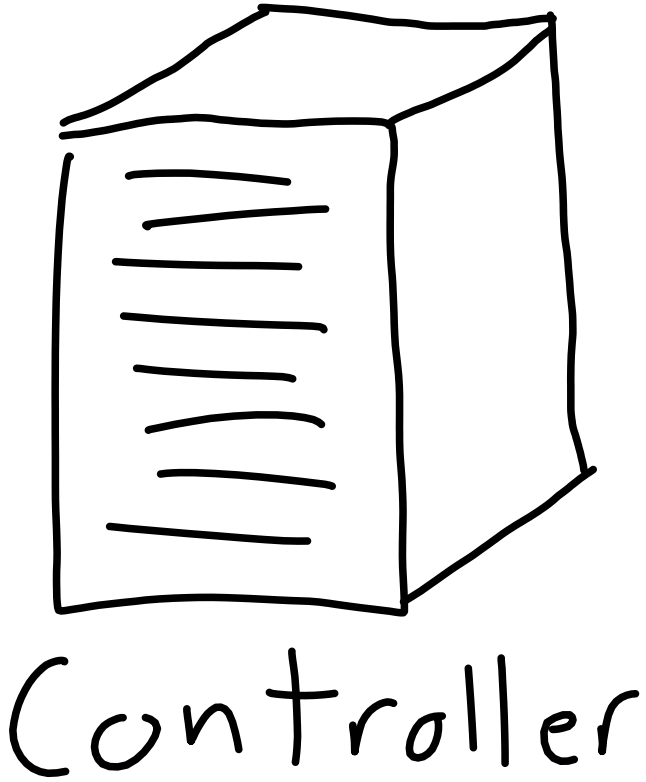
SSH Security Model

One-time Insecure Setup

© Bishop Fox. All rights reserved worldwide.

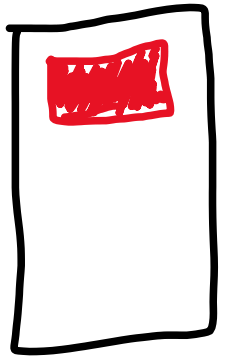
# Install-Mode



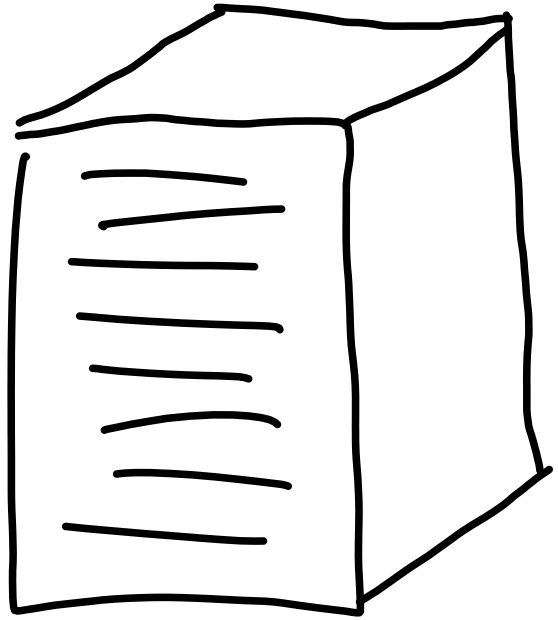

© Bishop Fox. All rights reserved worldwide.

# Install-Mode



Reader

Install-Mode

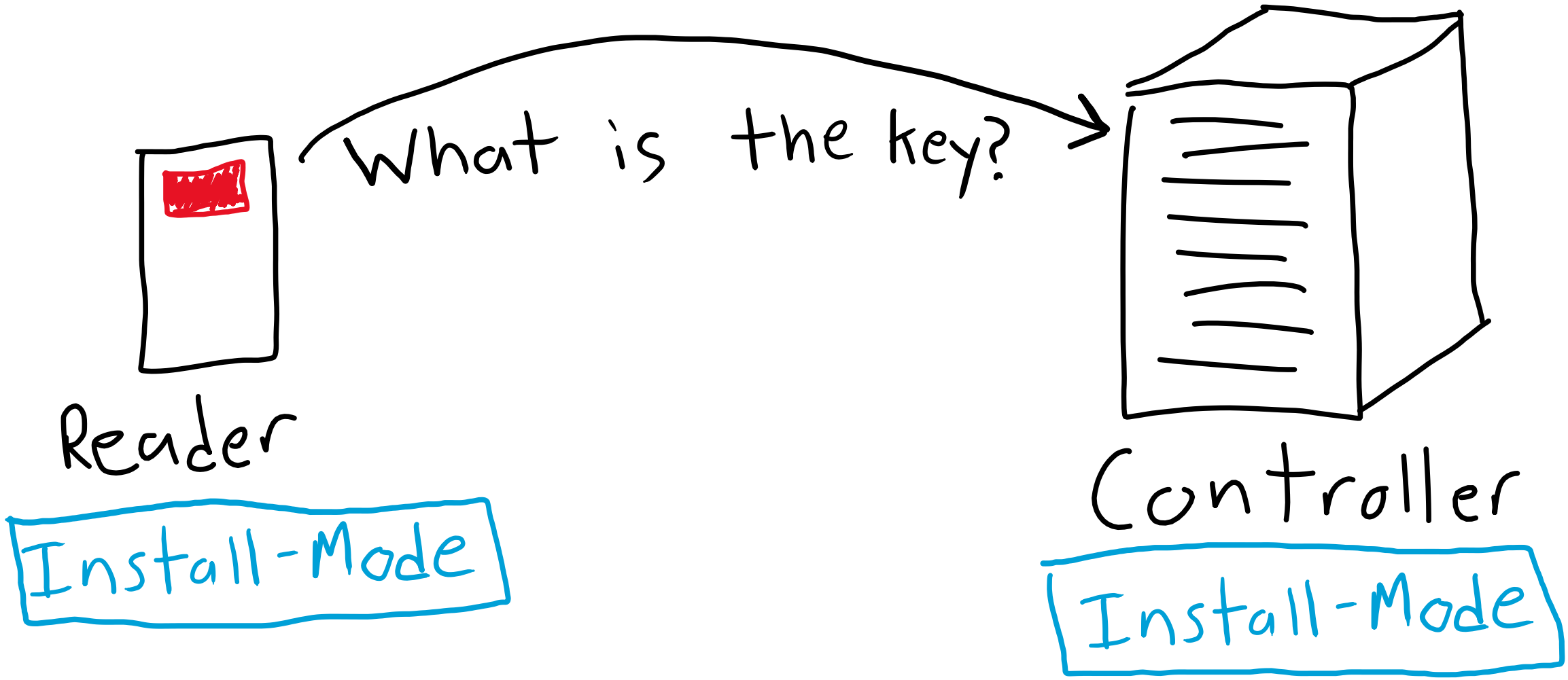


Controller

Install-Mode

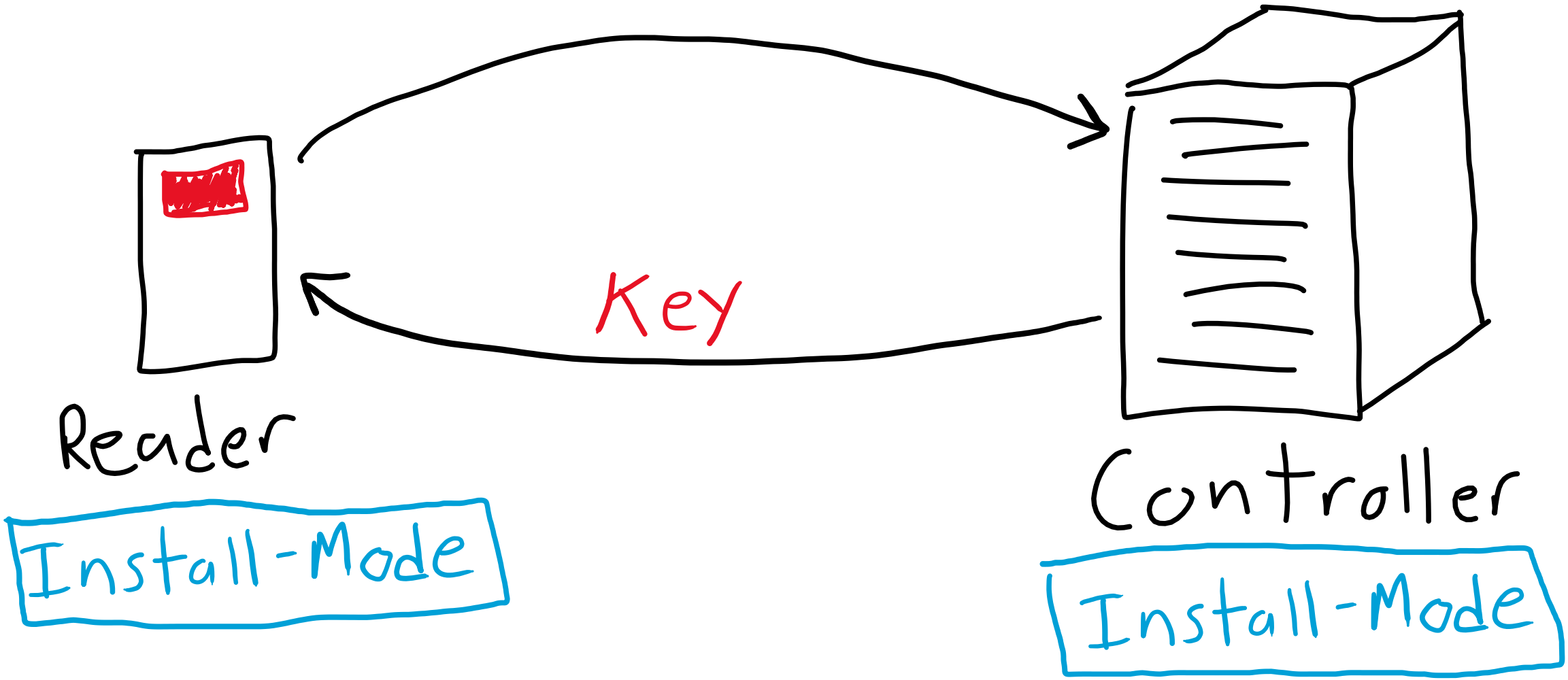
© Bishop Fox. All rights reserved worldwide.

# Install-Mode



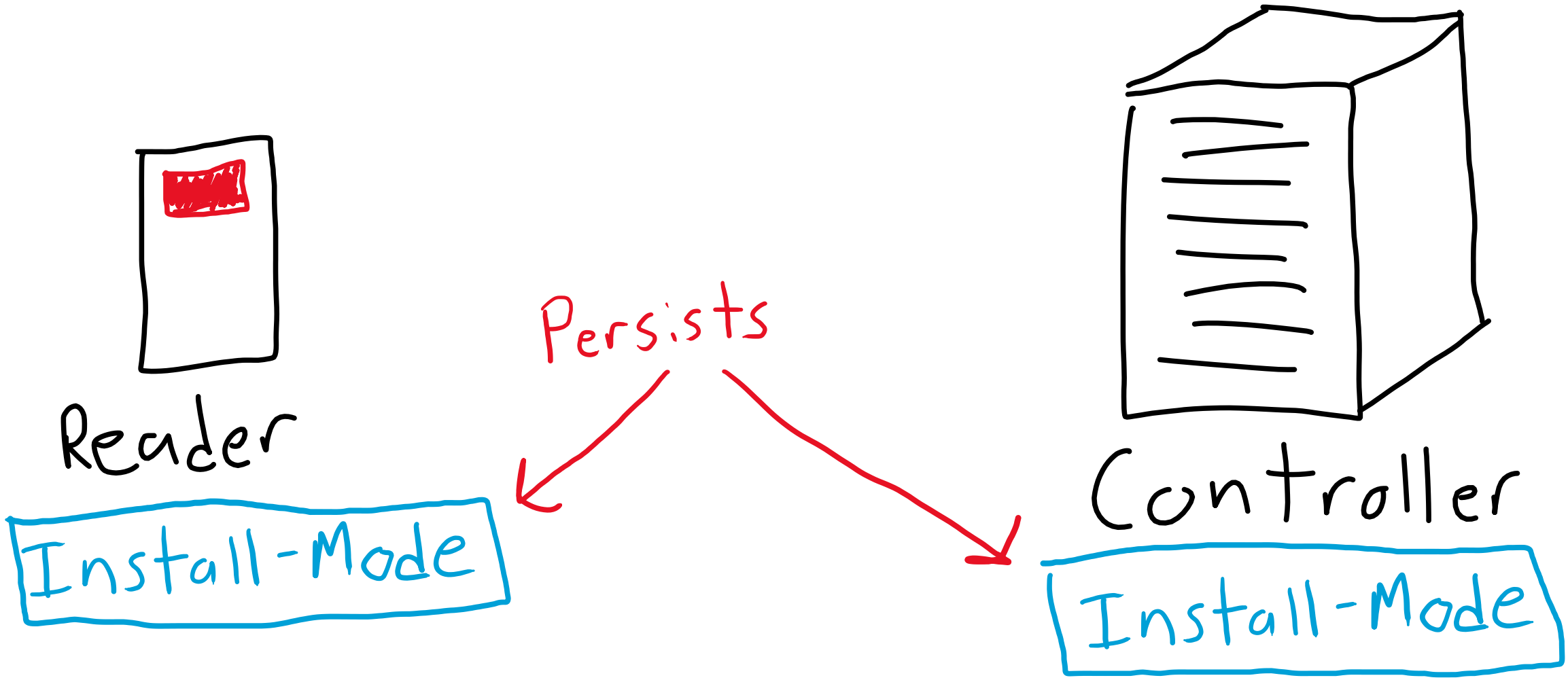

© Bishop Fox. All rights reserved worldwide.

# Install-Mode



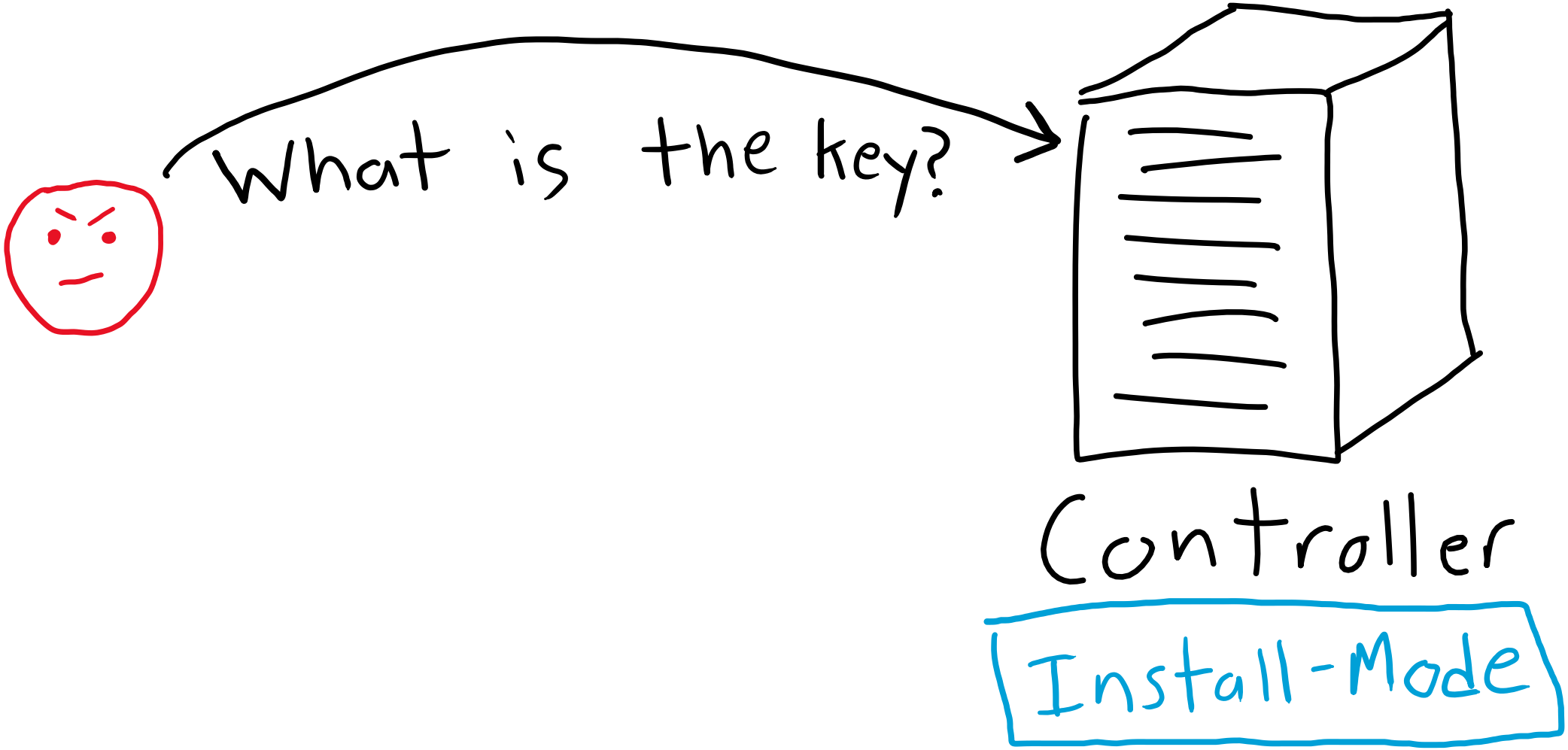

© Bishop Fox. All rights reserved worldwide.

# Install-Mode



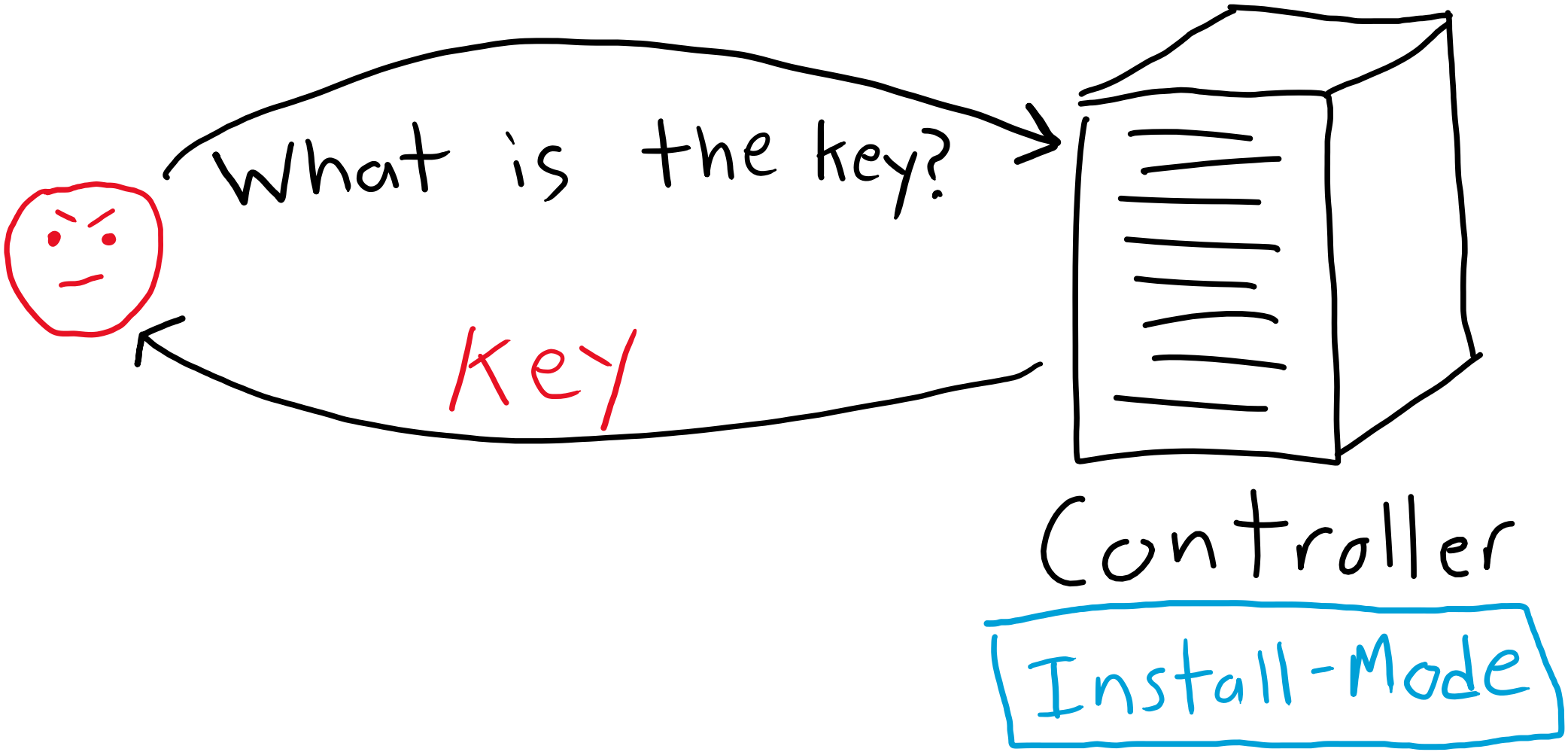

© Bishop Fox. All rights reserved worldwide.

# Install-Mode



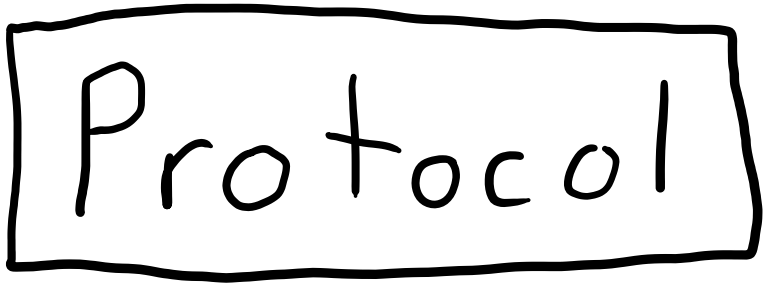

© Bishop Fox. All rights reserved worldwide.

# Install-Mode



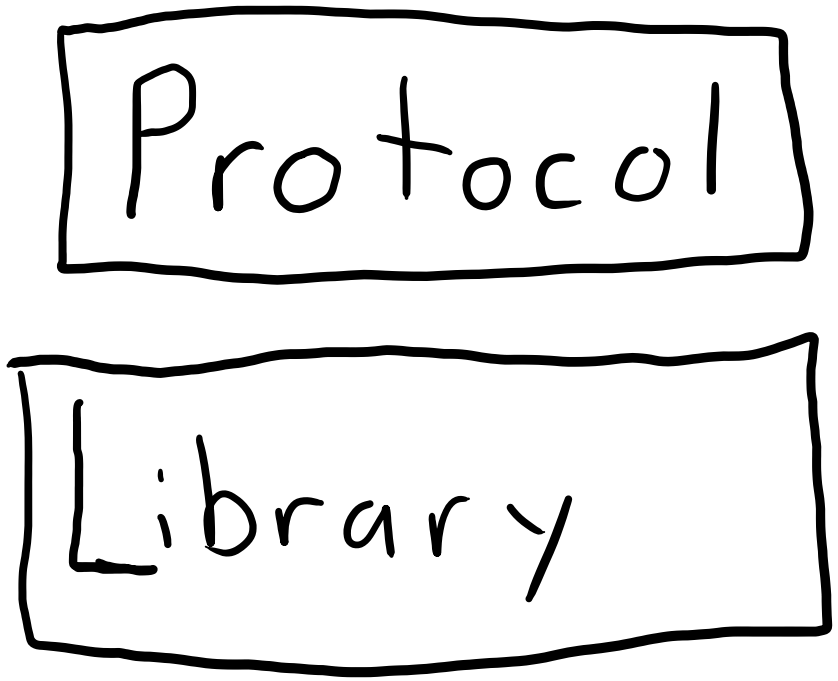

© Bishop Fox. All rights reserved worldwide.

# Where does the vuln lie?



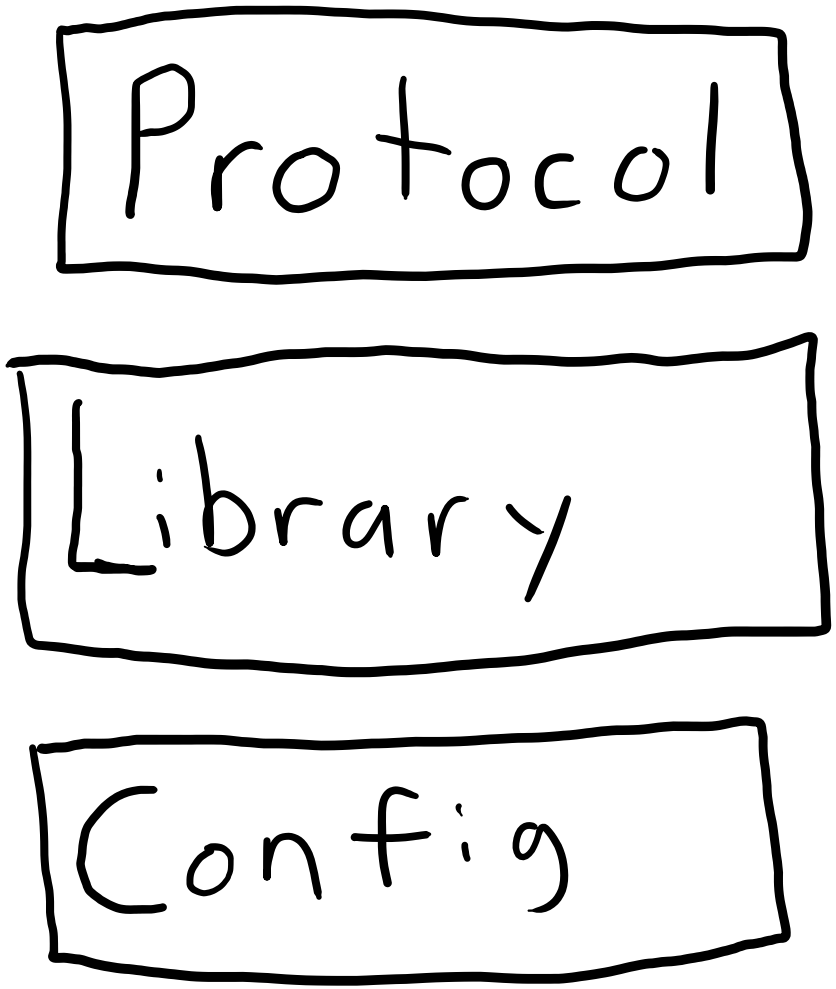

© Bishop Fox. All rights reserved worldwide.

# Where does the vuln lie?



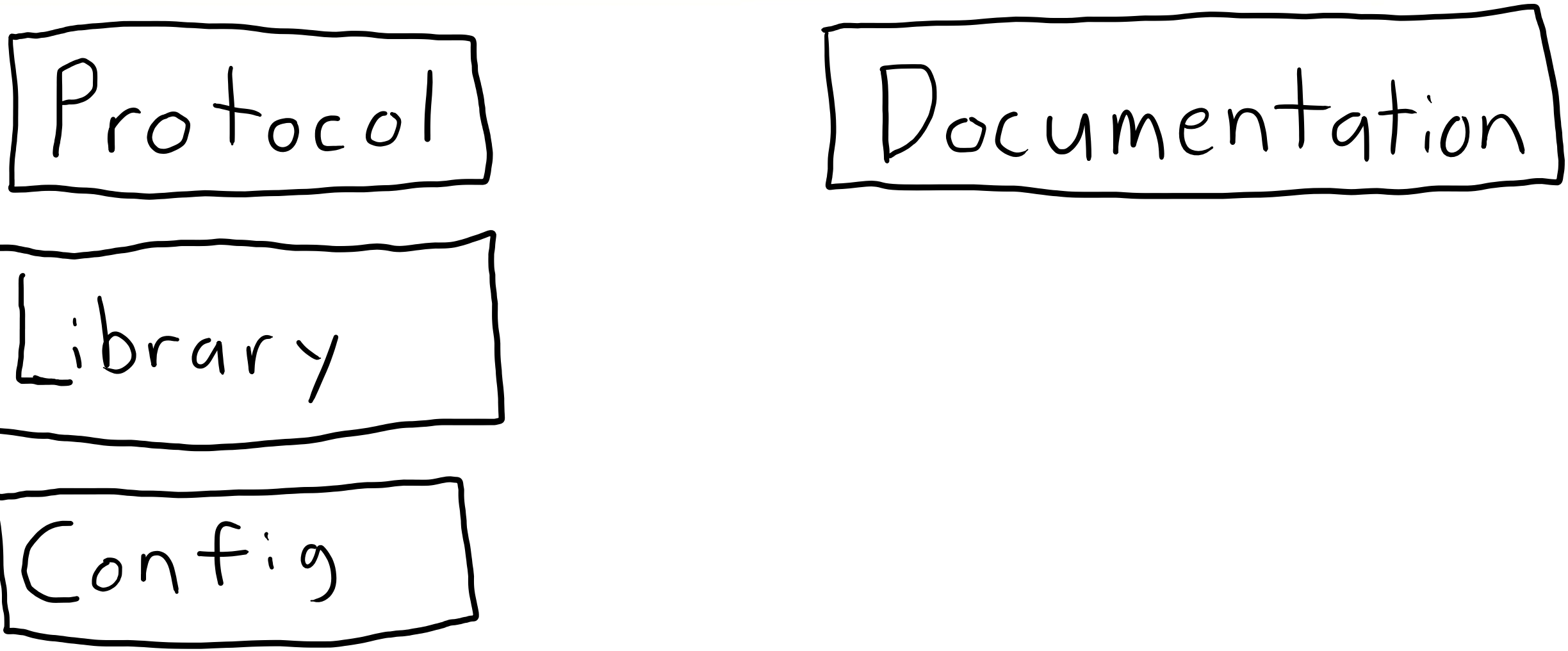

© Bishop Fox. All rights reserved worldwide.

# Where does the vuln lie?



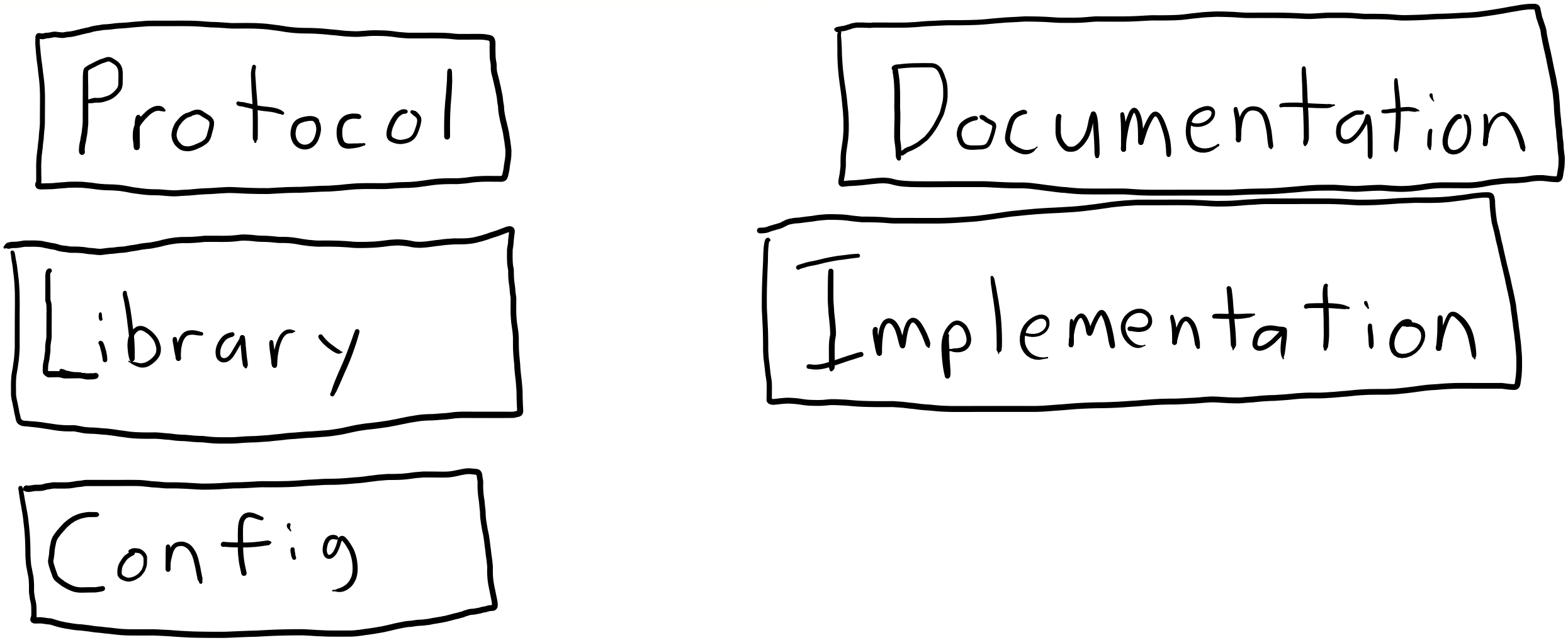

© Bishop Fox. All rights reserved worldwide.

# Where does the vuln lie?



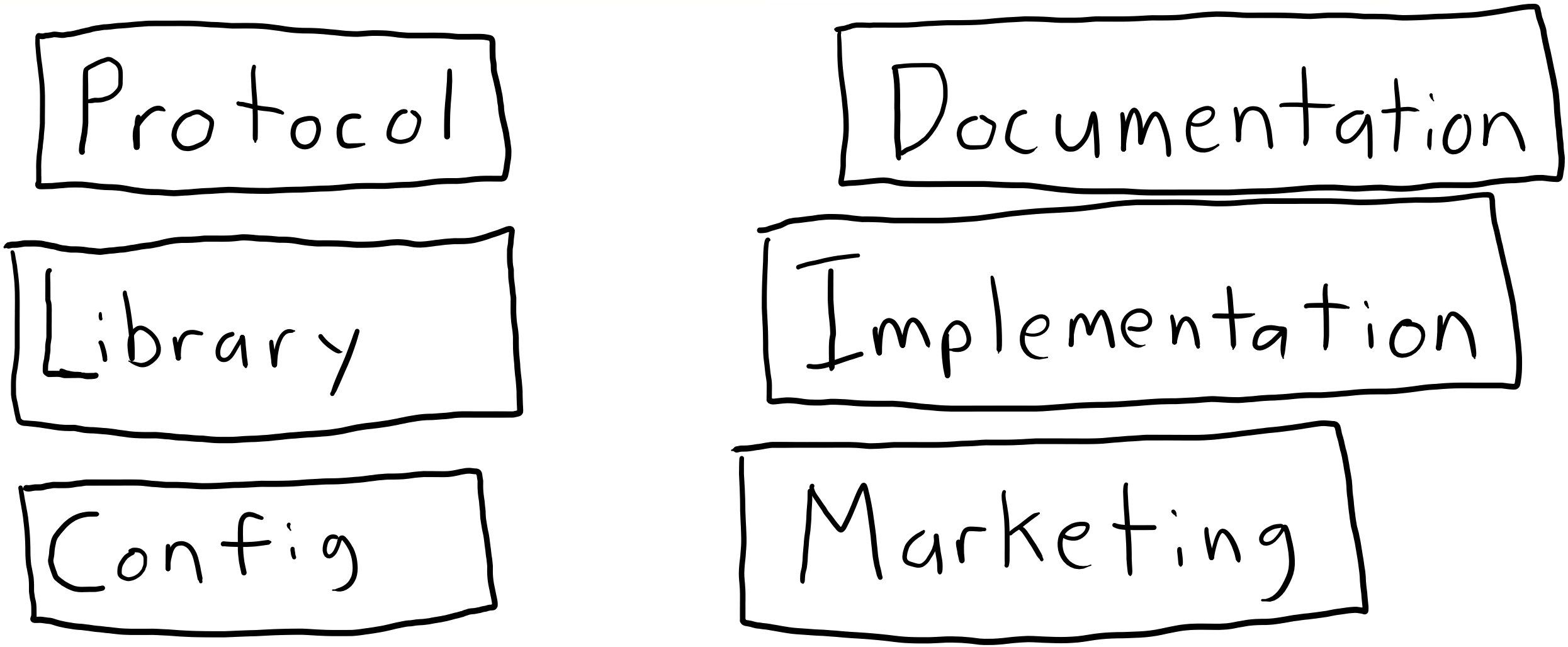

© Bishop Fox. All rights reserved worldwide.

# Where does the vuln lie?




© Bishop Fox. All rights reserved worldwide.

# Where does the vuln lie?



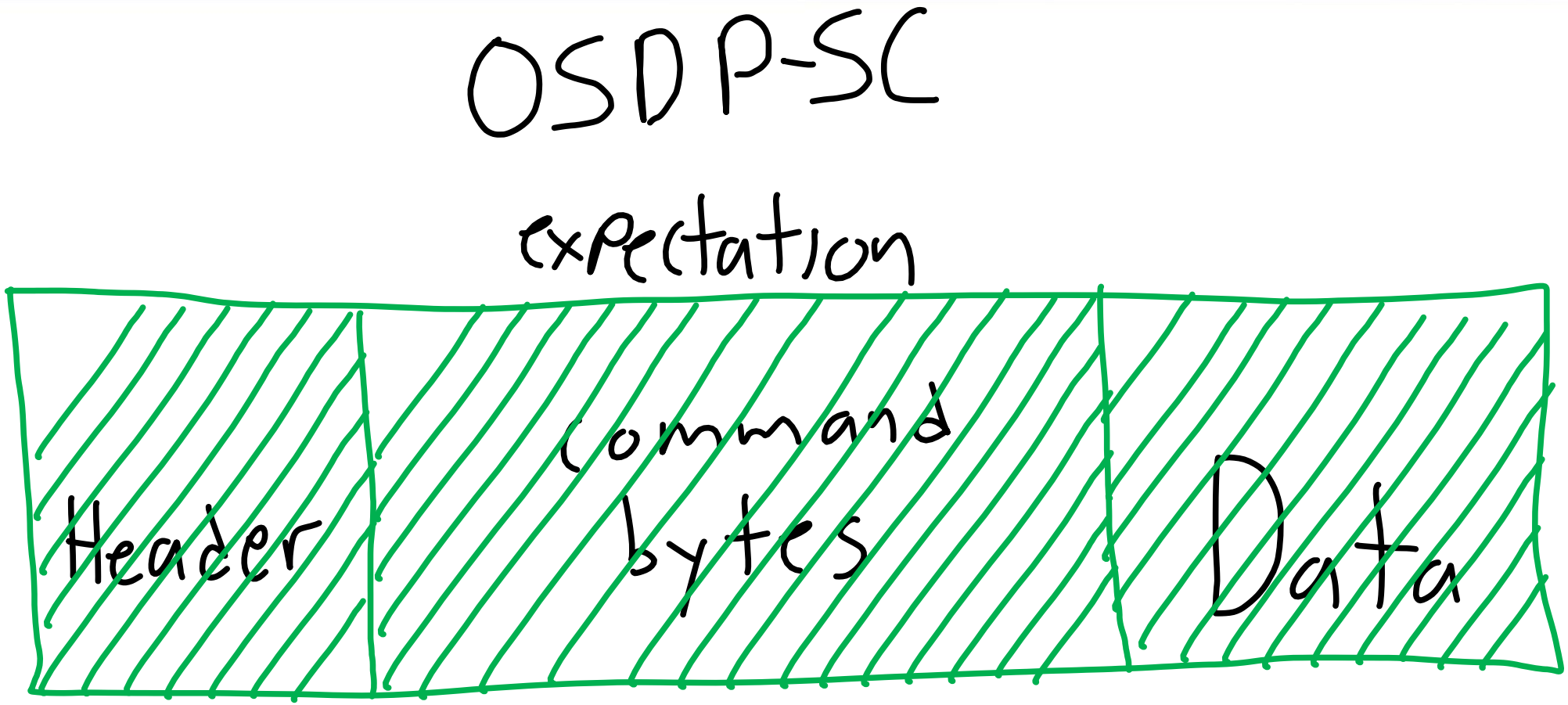

© Bishop Fox. All rights reserved worldwide.

# Protocol WTF #3

We never said we'd encrypt ALL of the data...

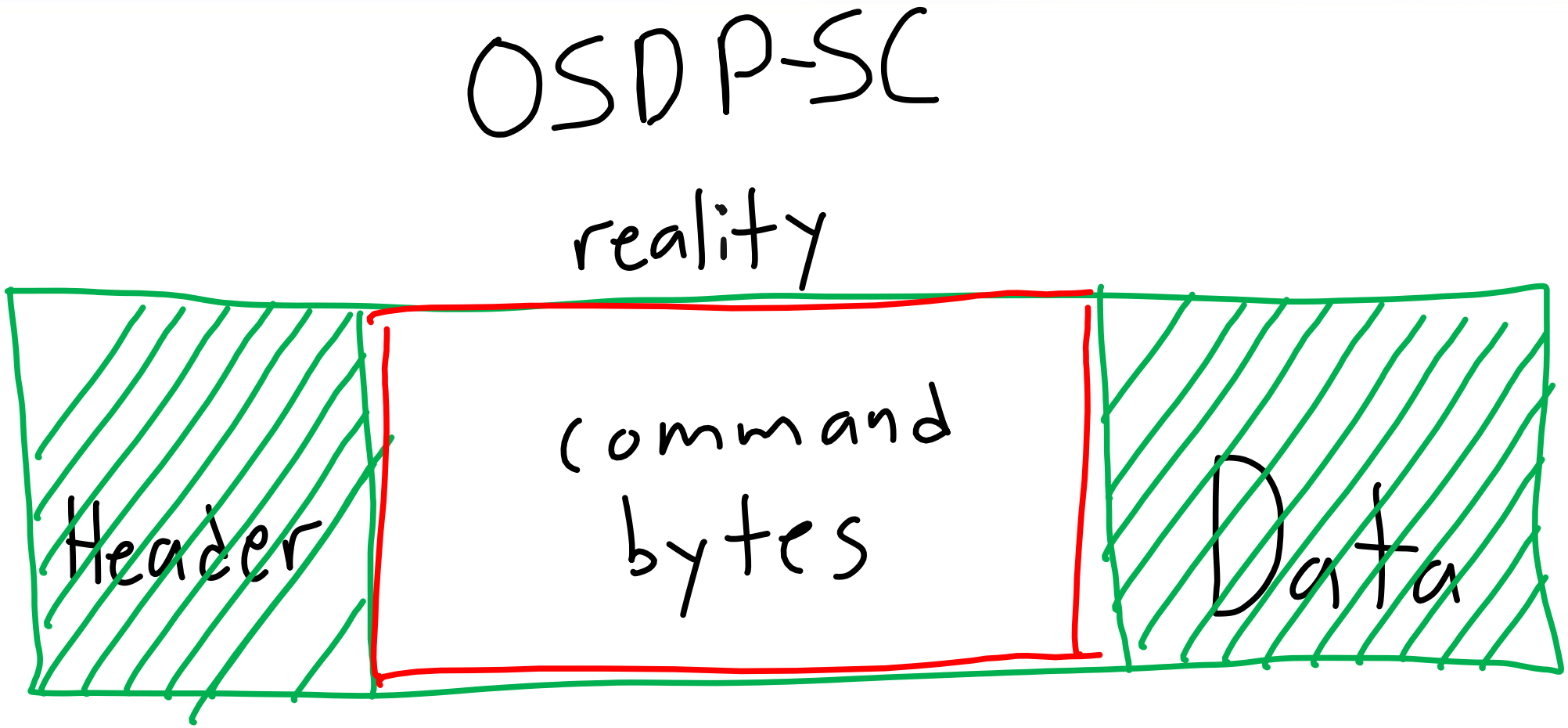
© Bishop Fox. All rights reserved worldwide.

# SCS_17& SCS_18: The whole packet is encrypted…right?




© Bishop Fox. All rights reserved worldwide.

# SCS_17& SCS_18: The whole packet is encrypted…right?




© Bishop Fox. All rights reserved worldwide.

# SCS_17& SCS_18: The whole packet is encrypted…right?

command bytes = PDU/CP data transmitted

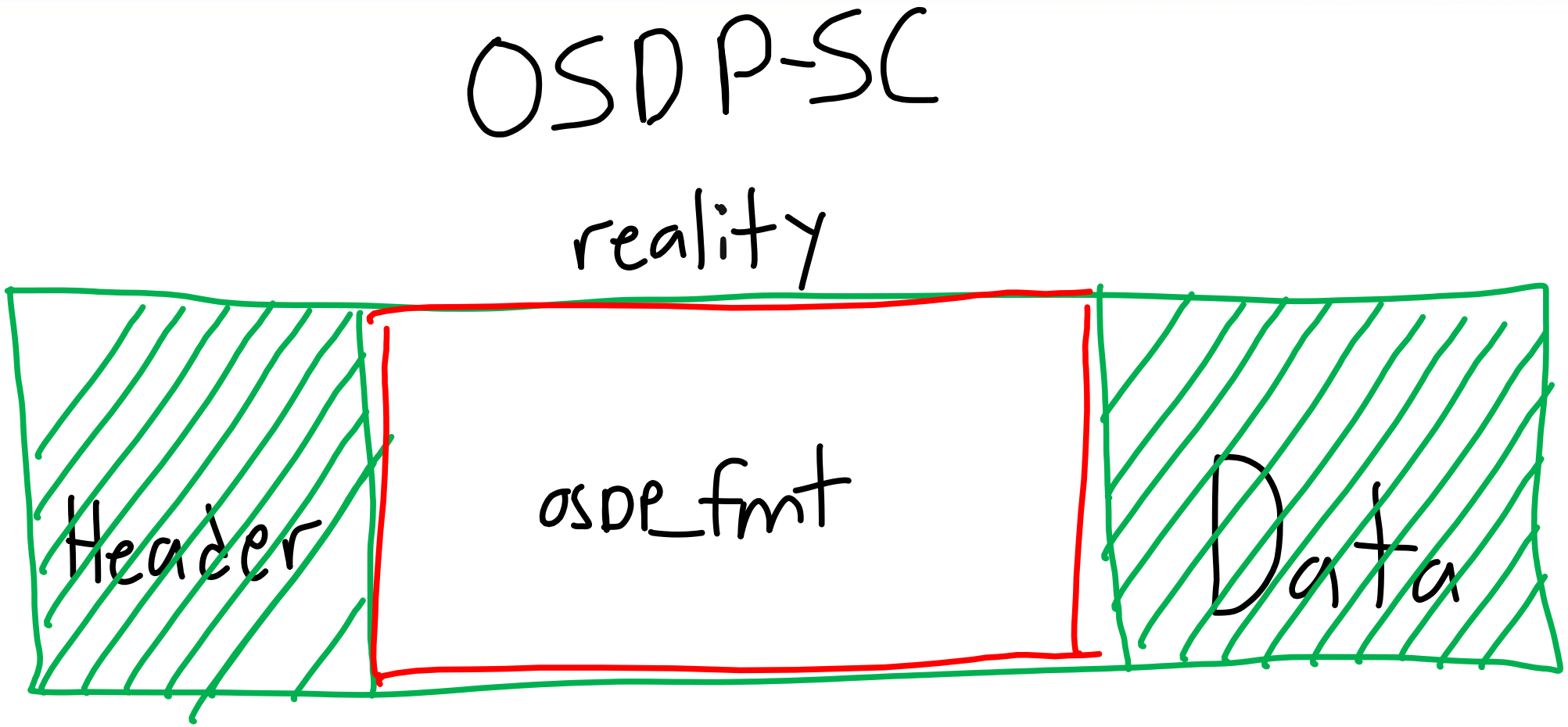
© Bishop Fox. All rights reserved worldwide.

# osdp_RAW




© Bishop Fox. All rights reserved worldwide.

# osdp_FMT



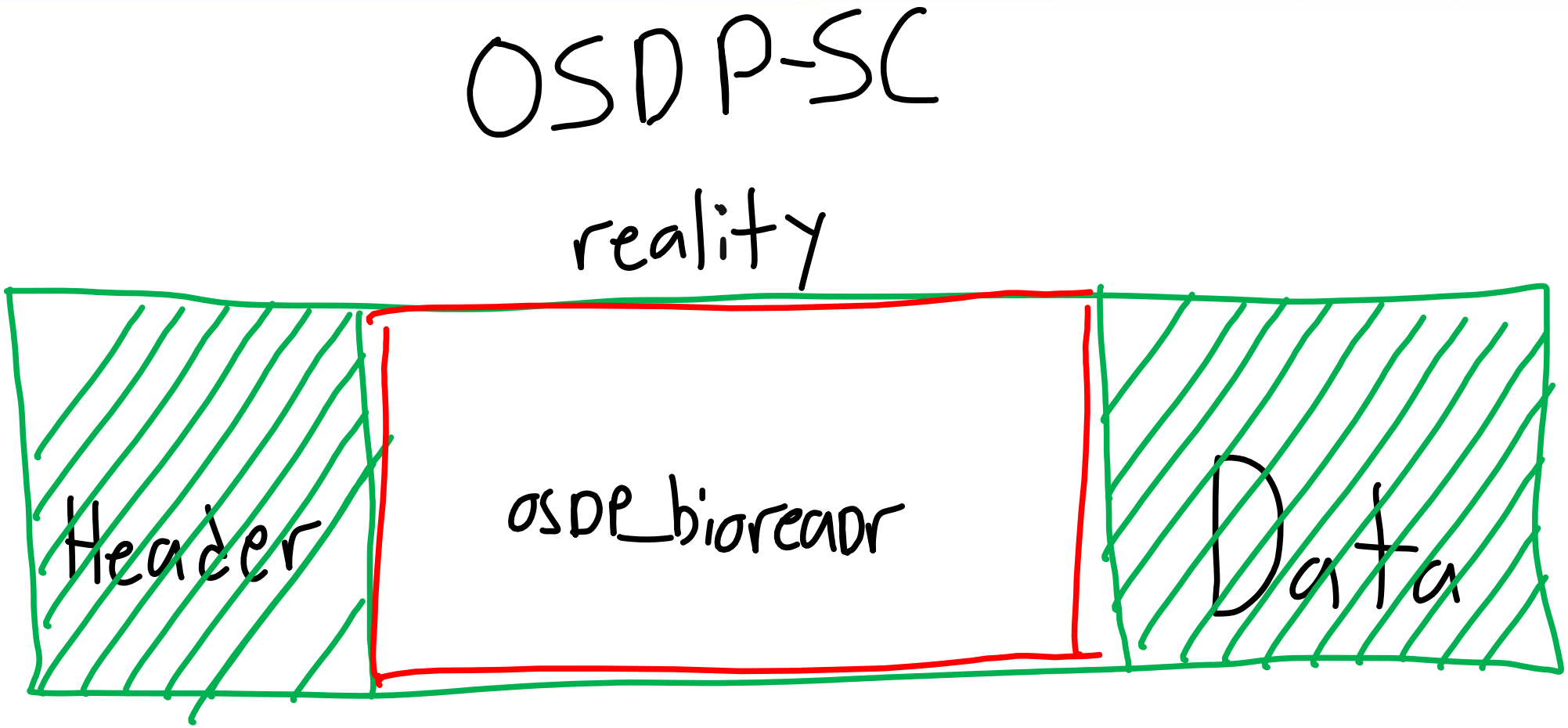

© Bishop Fox. All rights reserved worldwide.

# osdp_KEYPAD



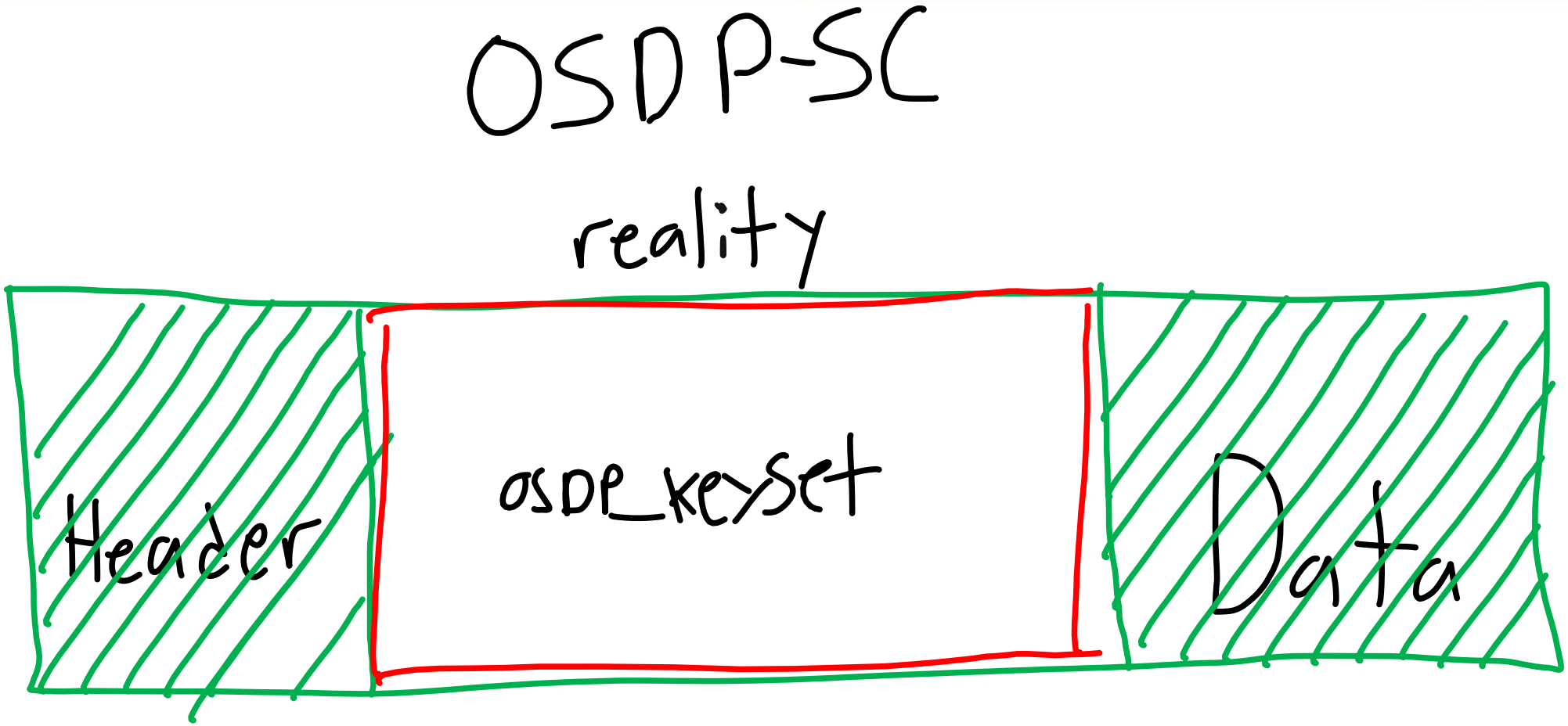

© Bishop Fox. All rights reserved worldwide.

# osdp_BIOREADR




© Bishop Fox. All rights reserved worldwide.

# osdp_KEYSET




© Bishop Fox. All rights reserved worldwide.

# Demo #4

Weak Keys Attack

© Bishop Fox. All rights reserved worldwide.

# Weak Keys

not Protocol Specific

© Bishop Fox. All rights reserved worldwide.

# SCBK




© Bishop Fox. All rights reserved worldwide.

# S-ENC Derivation



### *D.4.2 Session Key Derivation*

A set of three keys are derived and used for each secure communication session. The derivation operation uses the SCBK and encrypts a data block generated for each key. The data block for each key is as follows:

S-ENC: 0x01,0x82,rnd[0],rnd[1],rnd[2],rnd[3],rnd[4],rnd[5],0,0,...

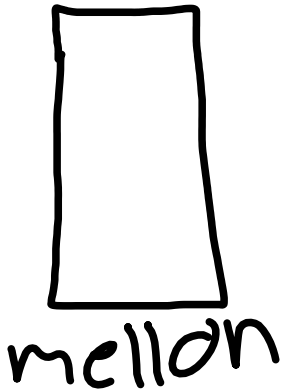
© Bishop Fox. All rights reserved worldwide.

# Introducing: Weak keys

```
 9
10      name = PD0
11      channel_type = uart
12      channel_device = /dev/ttyUSB0
13      channel_speed = 9600
14      scbk = 000102030405060708090a0b0c0d0e0f
15
16      address = 1
```

© Bishop Fox. All rights reserved worldwide.

# Using weak keys cant possibly backfire…




Key 1 = 0x00, 0x00, 0x00…
Key 2 = 0x01, 0x02, 0x03…
Key 3 = 0x30, 0x31, 0x32…
Key 4 = …



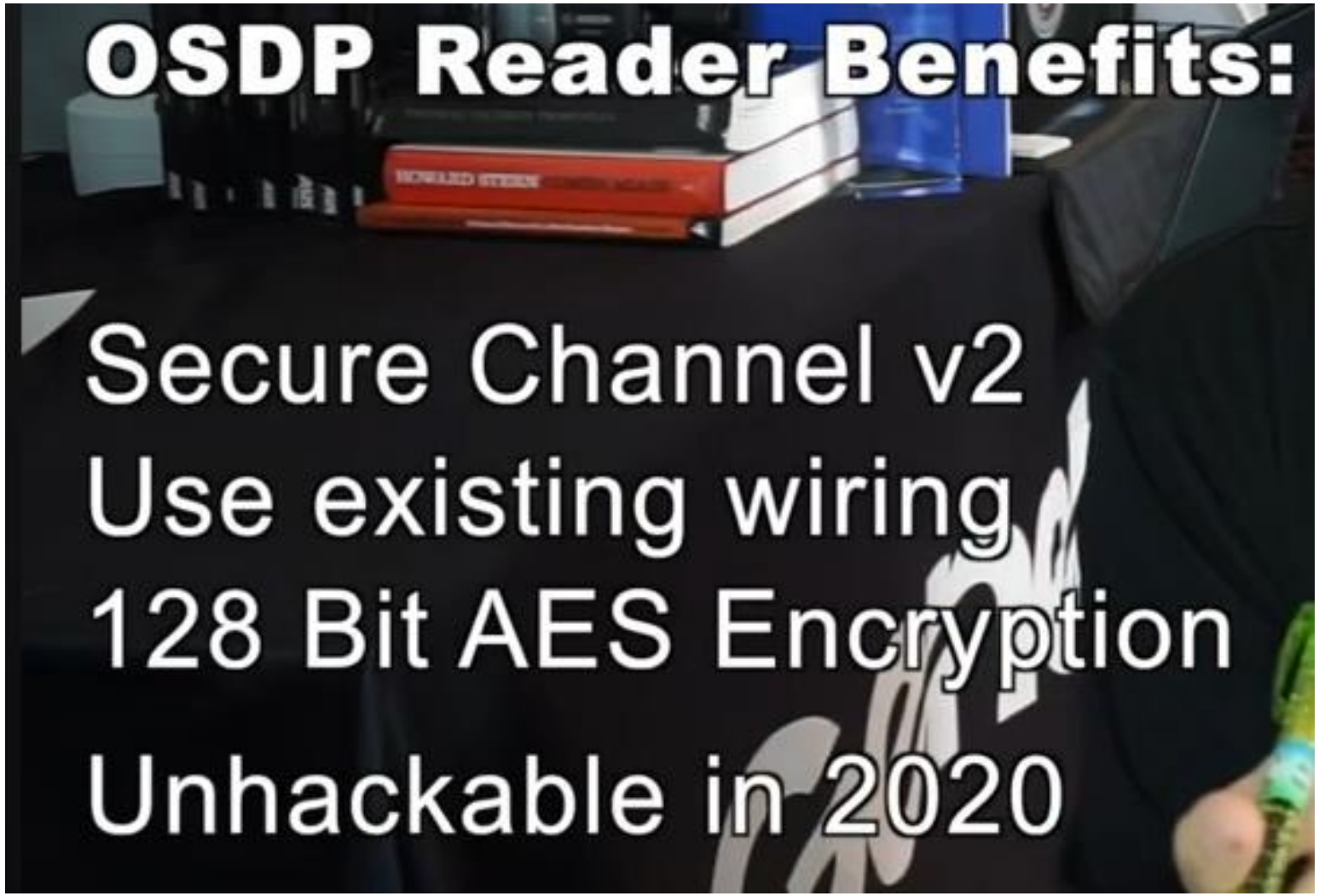

© Bishop Fox. All rights reserved worldwide.

## Protocol WTF #4

Encryption is not magic fairy dust

© Bishop Fox. All rights reserved worldwide.

# Bold Claims




© Bishop Fox. All rights reserved worldwide.

# Bold Claims




© Bishop Fox. All rights reserved worldwide.

# AES



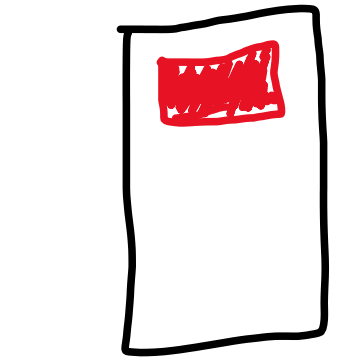

© Bishop Fox. All rights reserved worldwide.

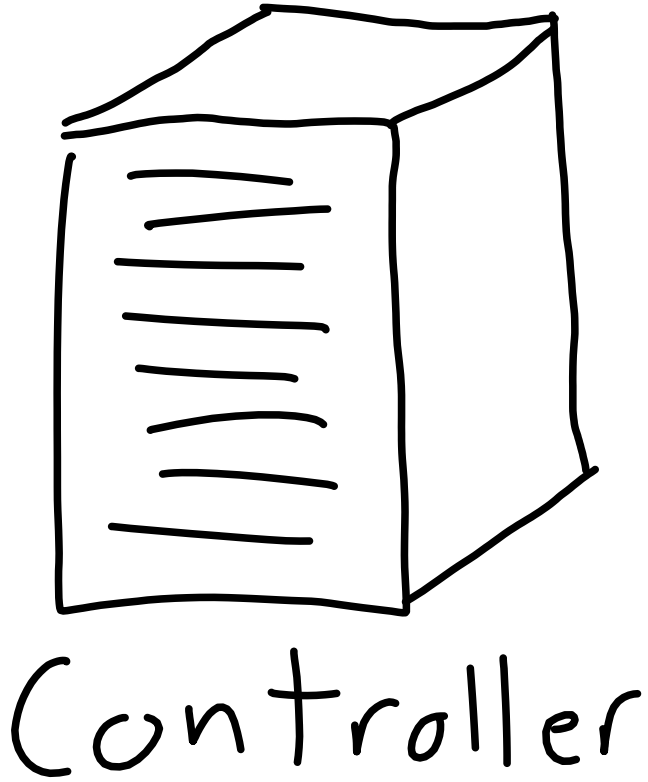
# AES




© Bishop Fox. All rights reserved worldwide.

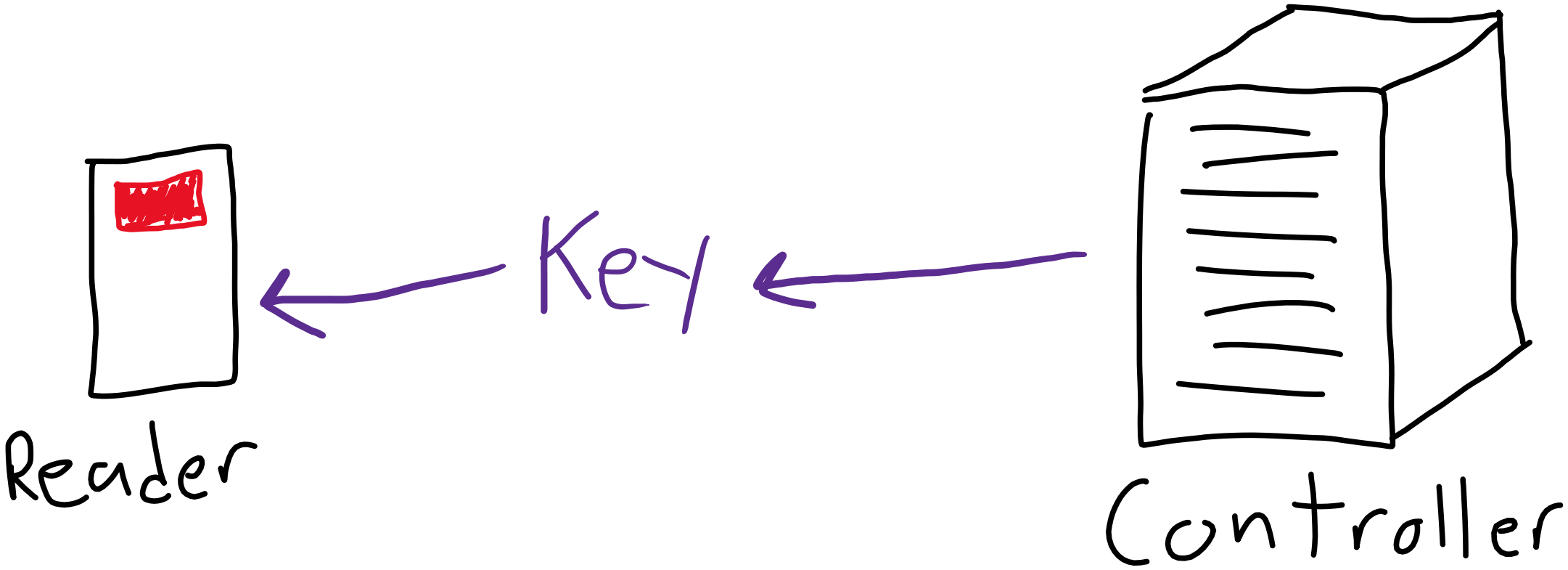
# Key Exchange



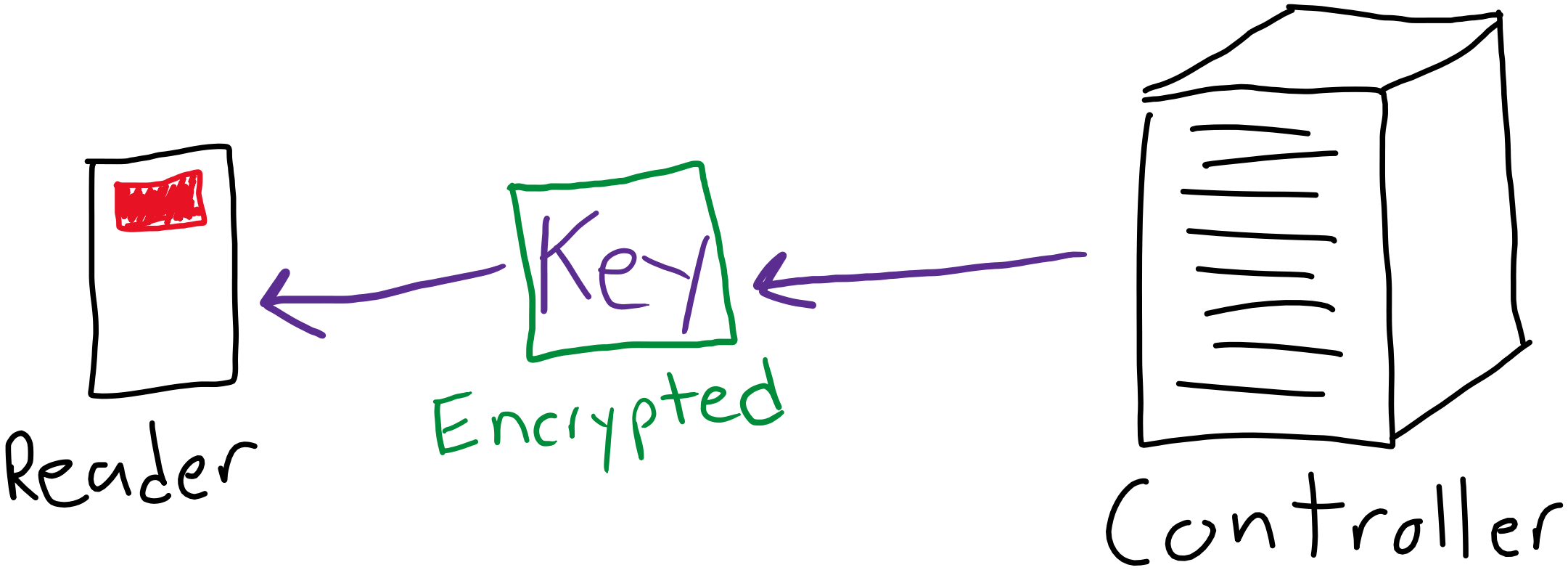

© Bishop Fox. All rights reserved worldwide.

# Key Exchange



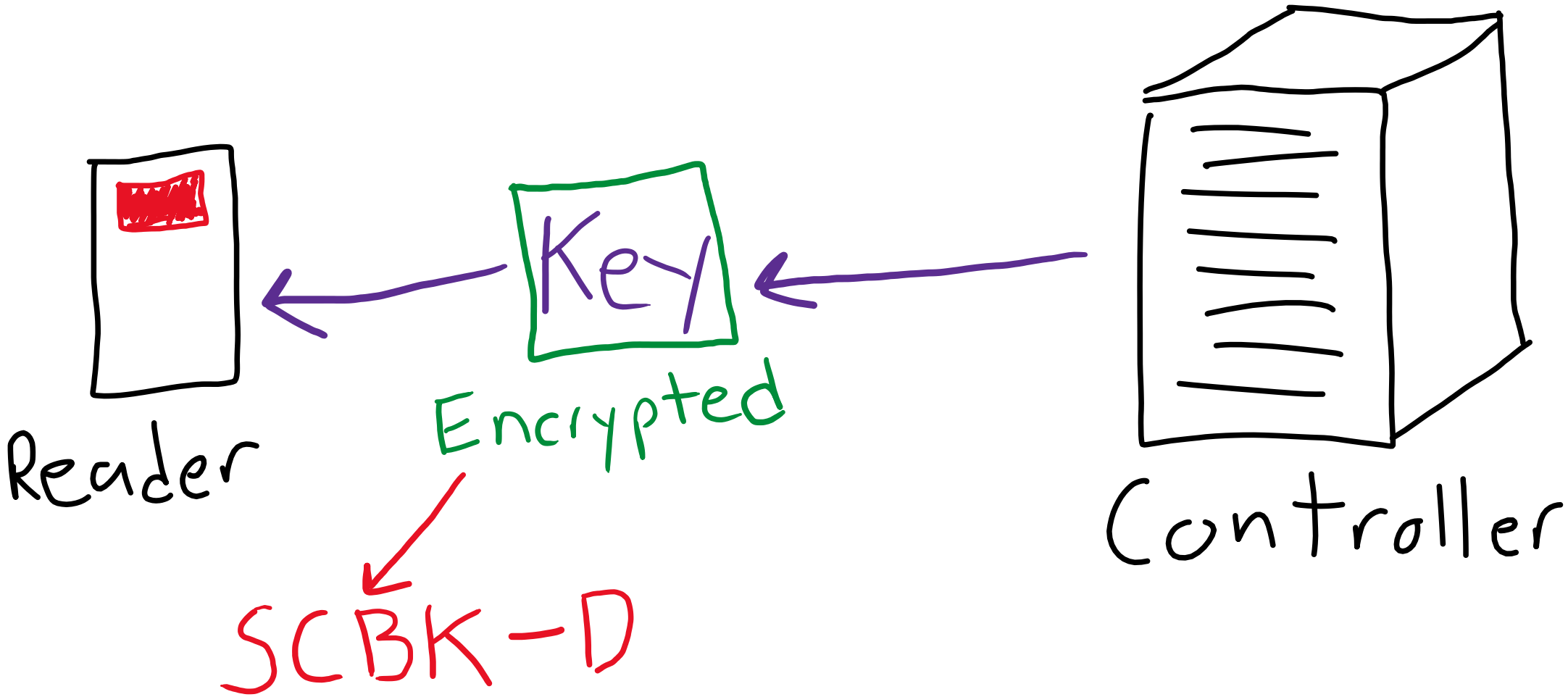

© Bishop Fox. All rights reserved worldwide.

# Key Exchange




© Bishop Fox. All rights reserved worldwide.

# Key Exchange




© Bishop Fox. All rights reserved worldwide.

# Key Exchange



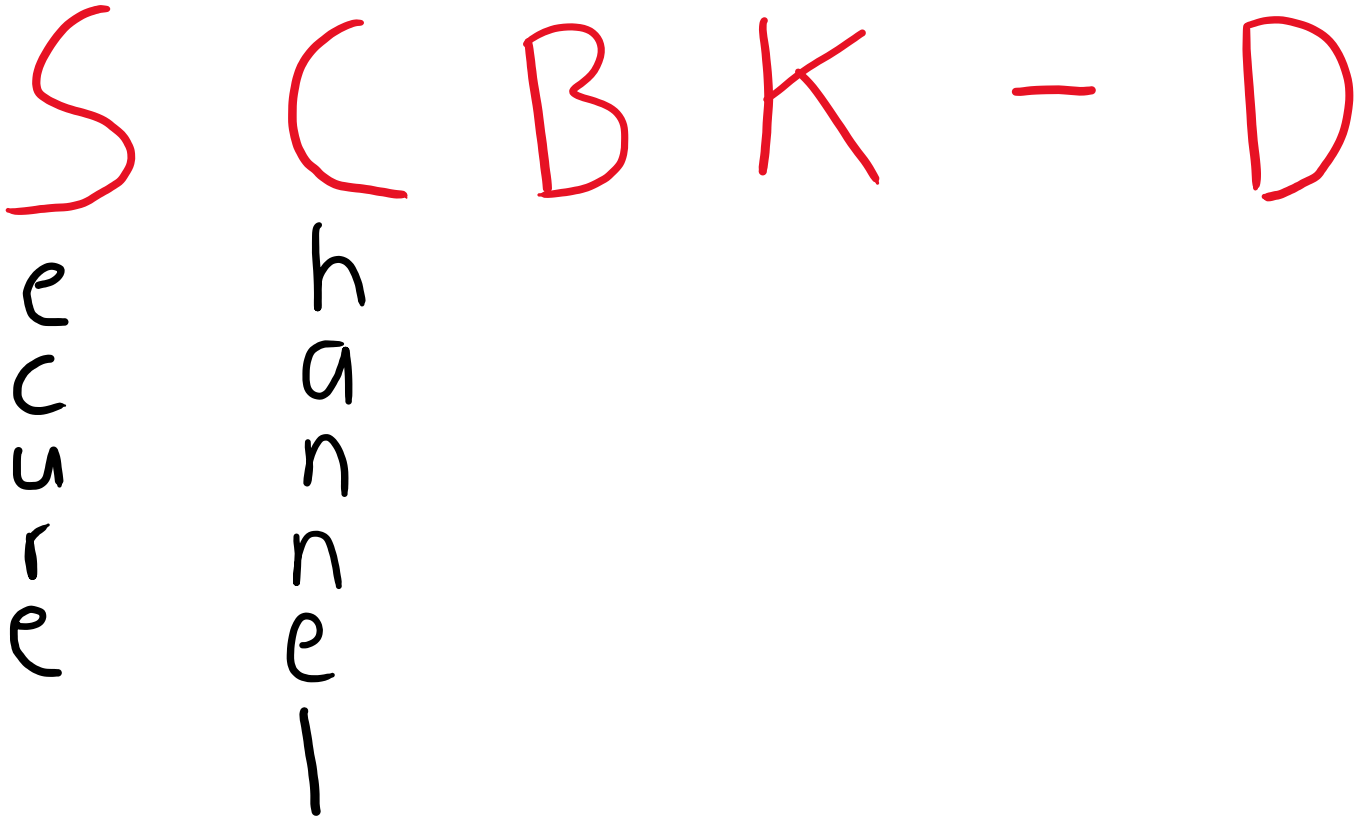

© Bishop Fox. All rights reserved worldwide.

# Key Exchange



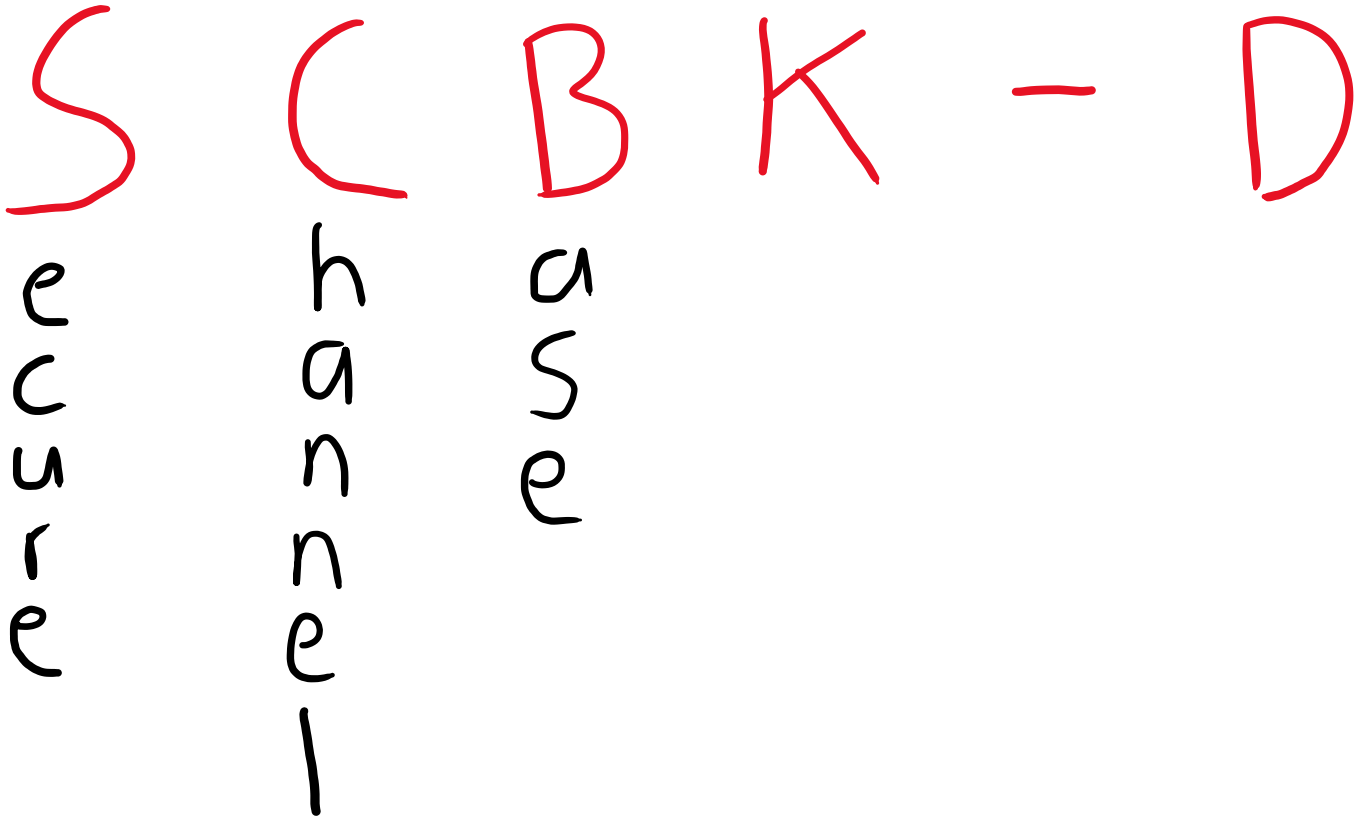

© Bishop Fox. All rights reserved worldwide.

# Key Exchange



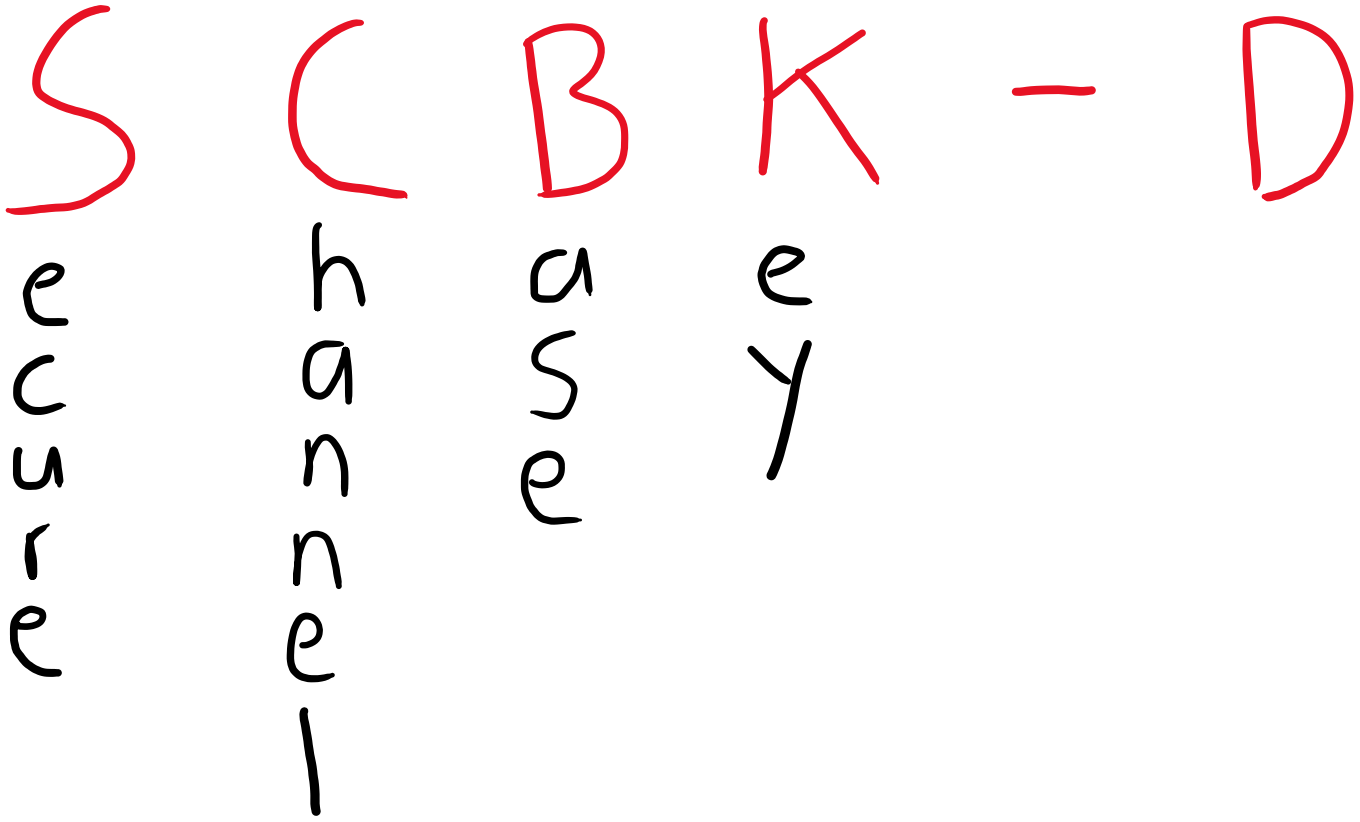

© Bishop Fox. All rights reserved worldwide.

# Key Exchange



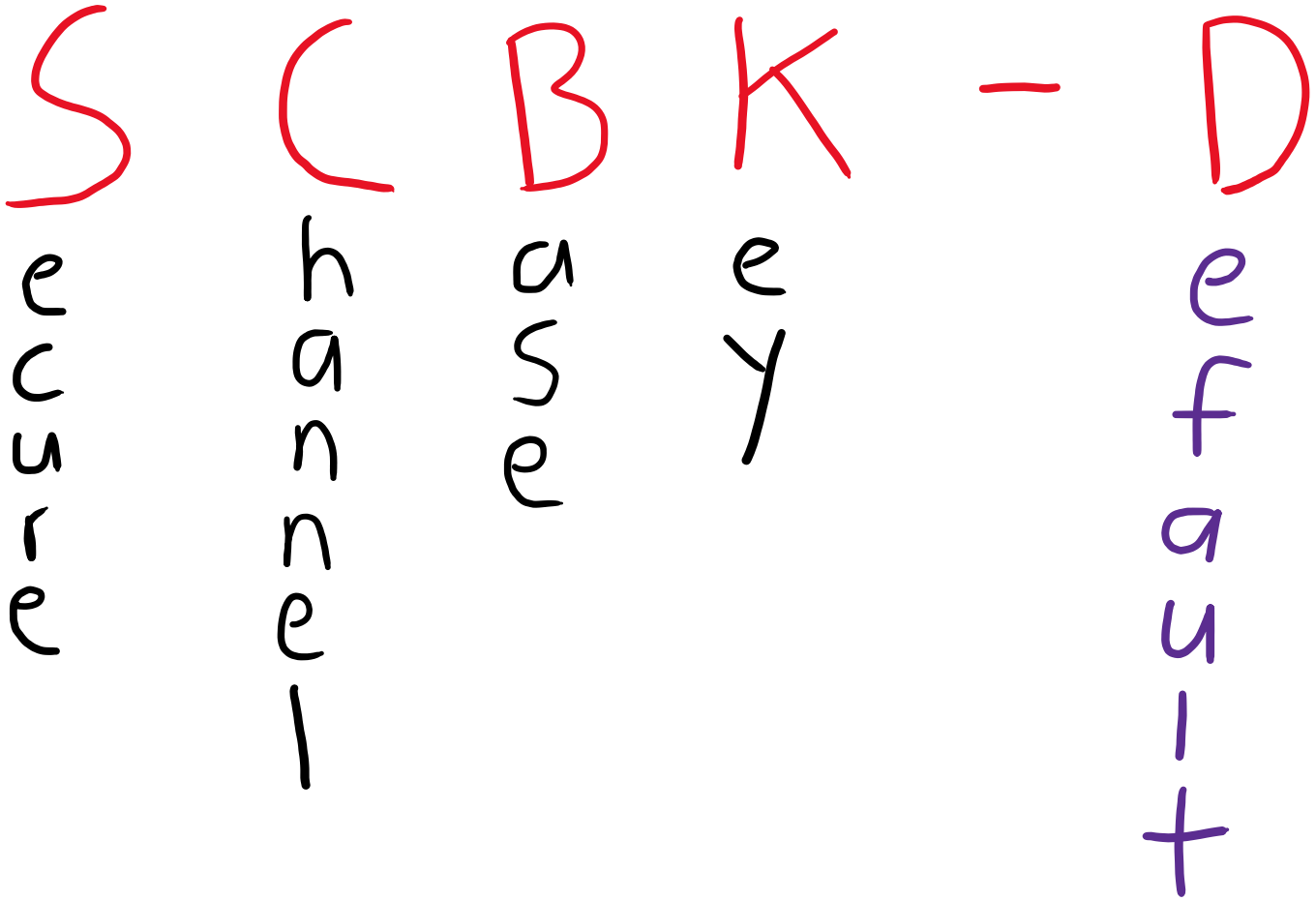

© Bishop Fox. All rights reserved worldwide.

# Key Exchange



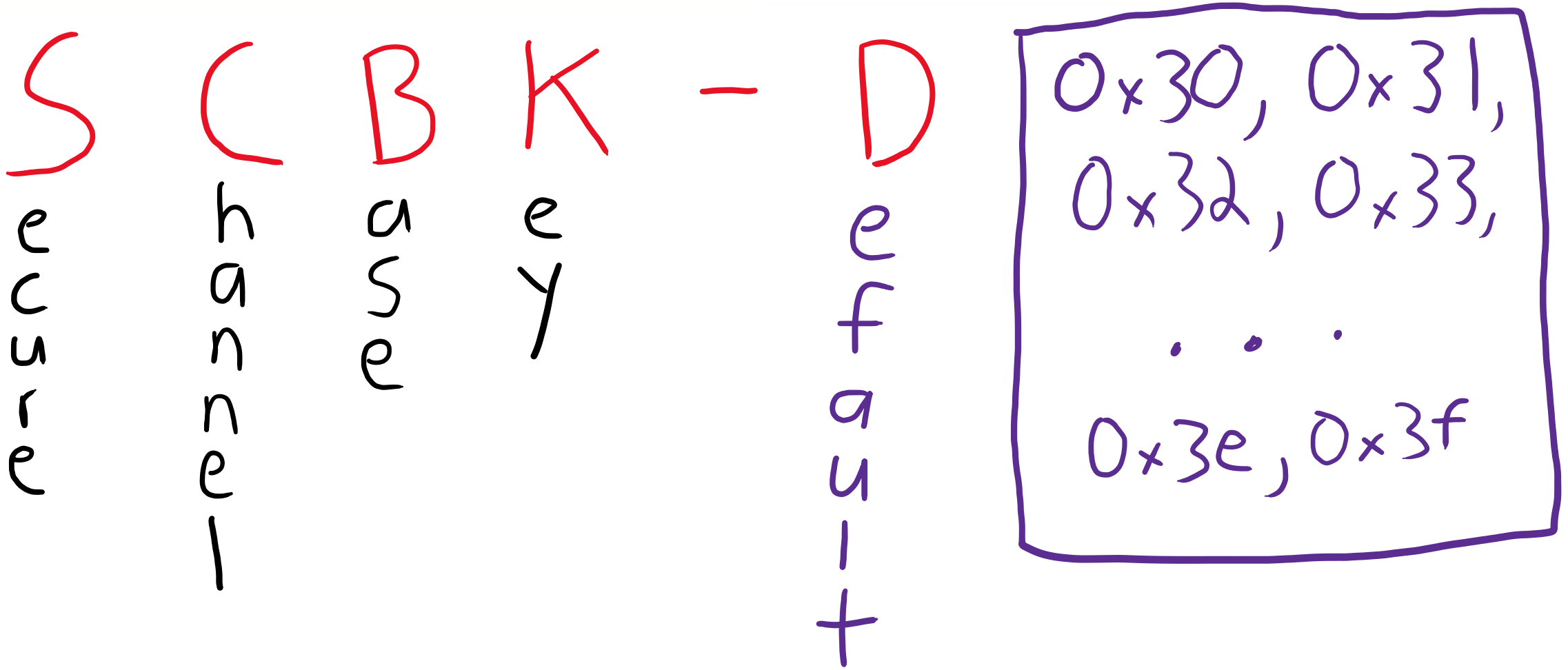

© Bishop Fox. All rights reserved worldwide.

# Key Exchange




© Bishop Fox. All rights reserved worldwide.

# Key Exchange




© Bishop Fox. All rights reserved worldwide.

# Demo #5



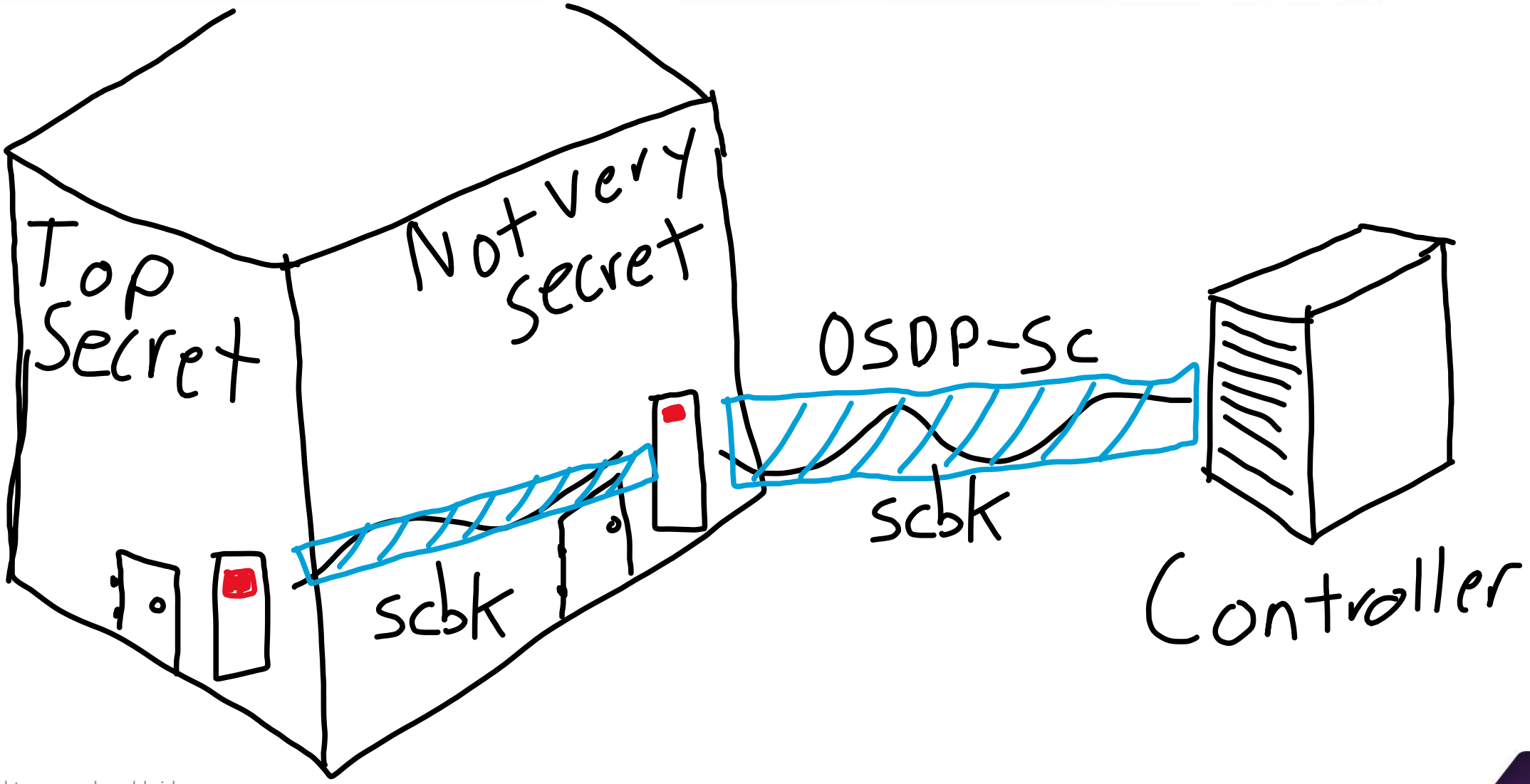

© Bishop Fox. All rights reserved worldwide.

# I've set everything up securely, I'm not affected by any of this

- "But, a lot of this can be avoided by configuring the device properly"
- If best practices were normally followed and devices were set up securely, many of us would be out of a job.
- Remember the broadcast nature of the protocol?

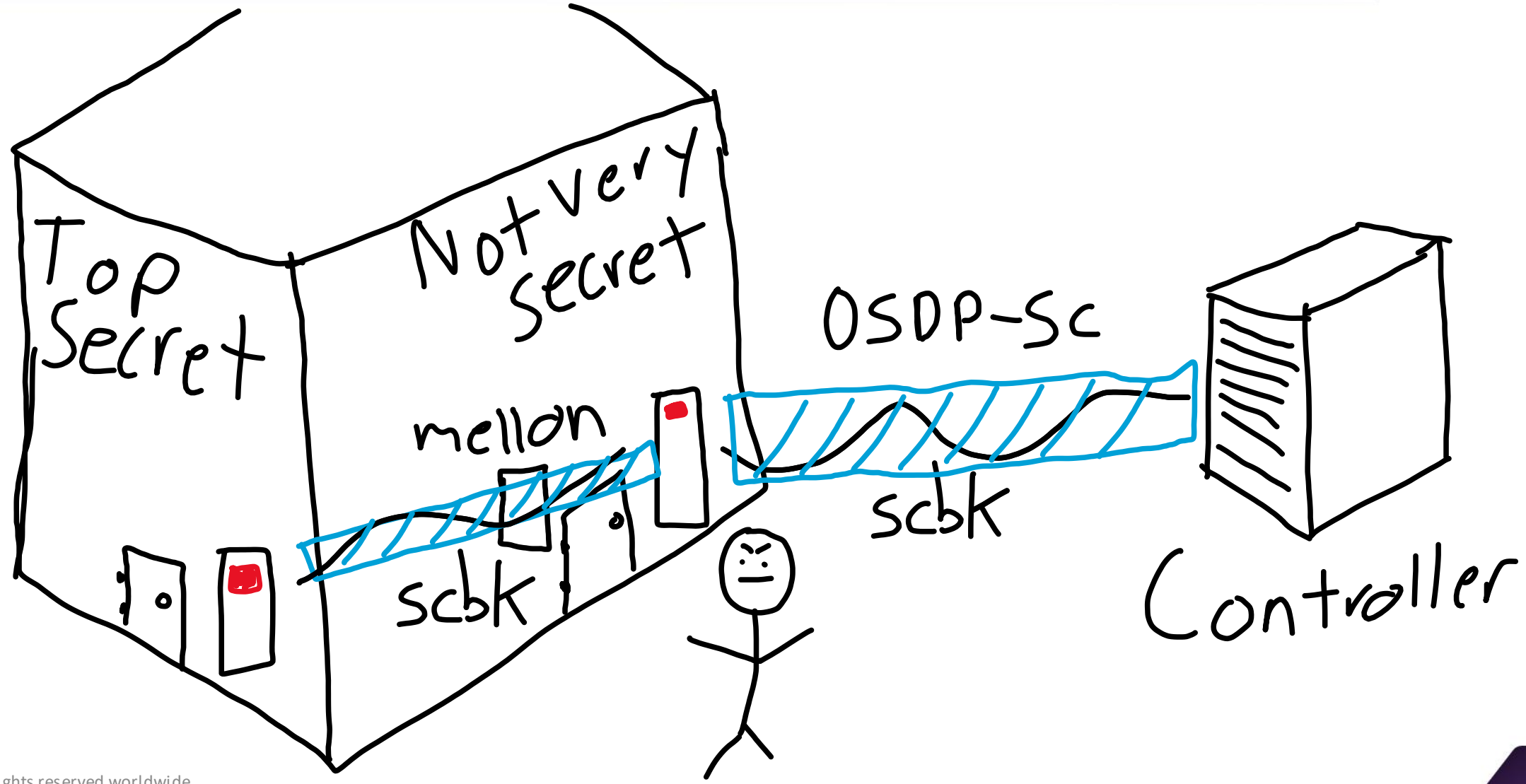
© Bishop Fox. All rights reserved worldwide.

# RS-485



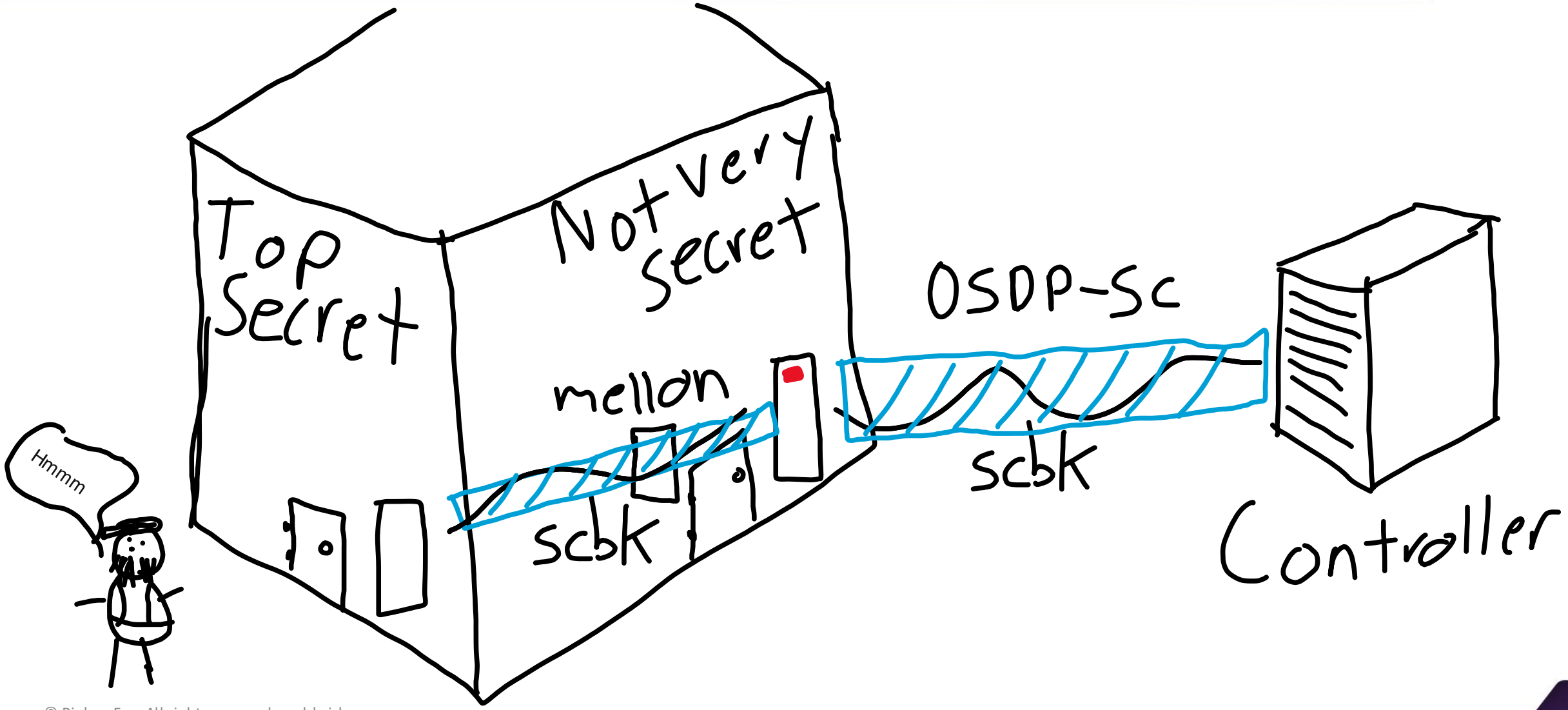

© Bishop Fox. All rights reserved worldwide.

# RS-485



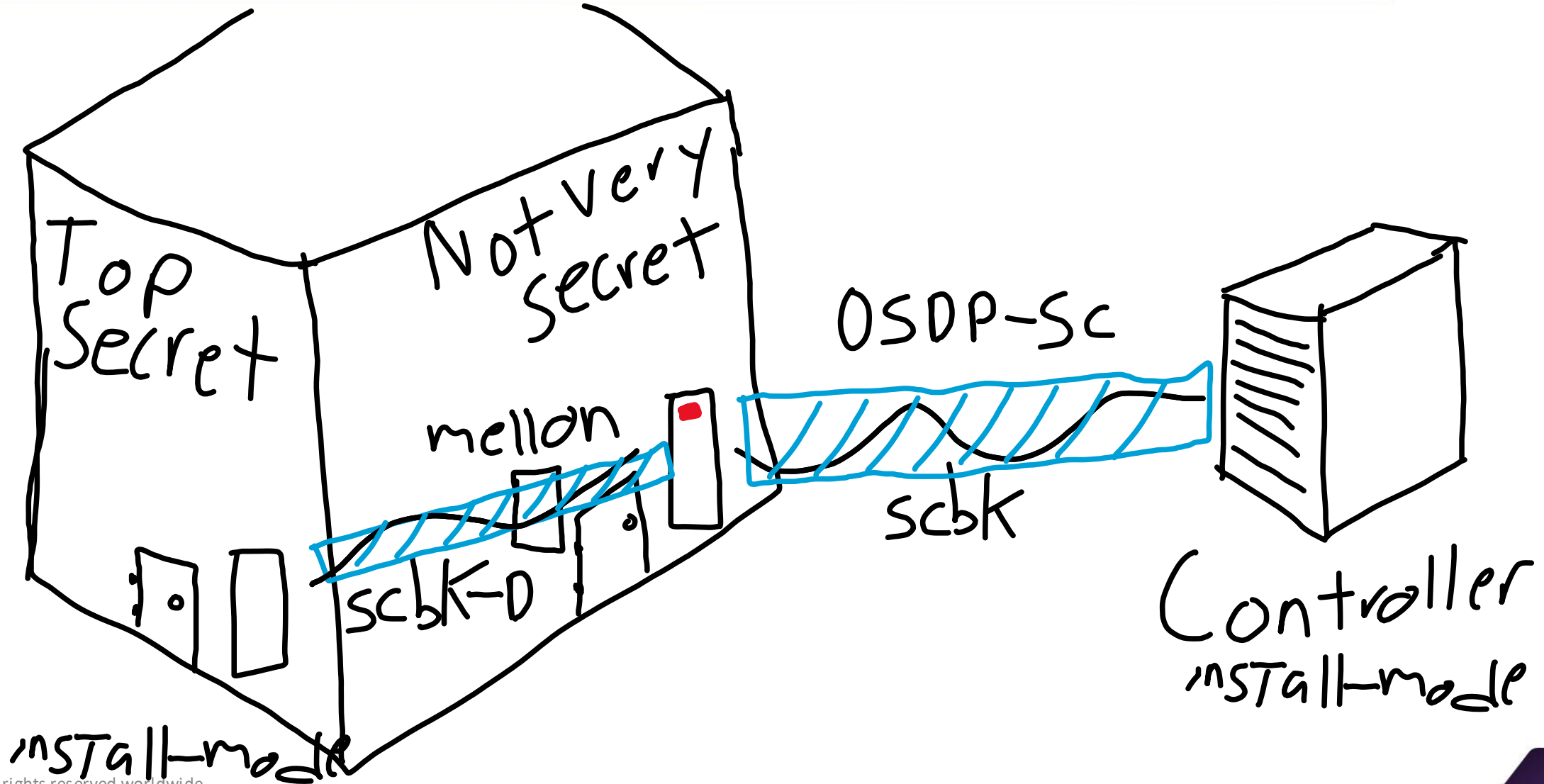

© Bishop Fox. All rights reserved worldwide.

# RS-485



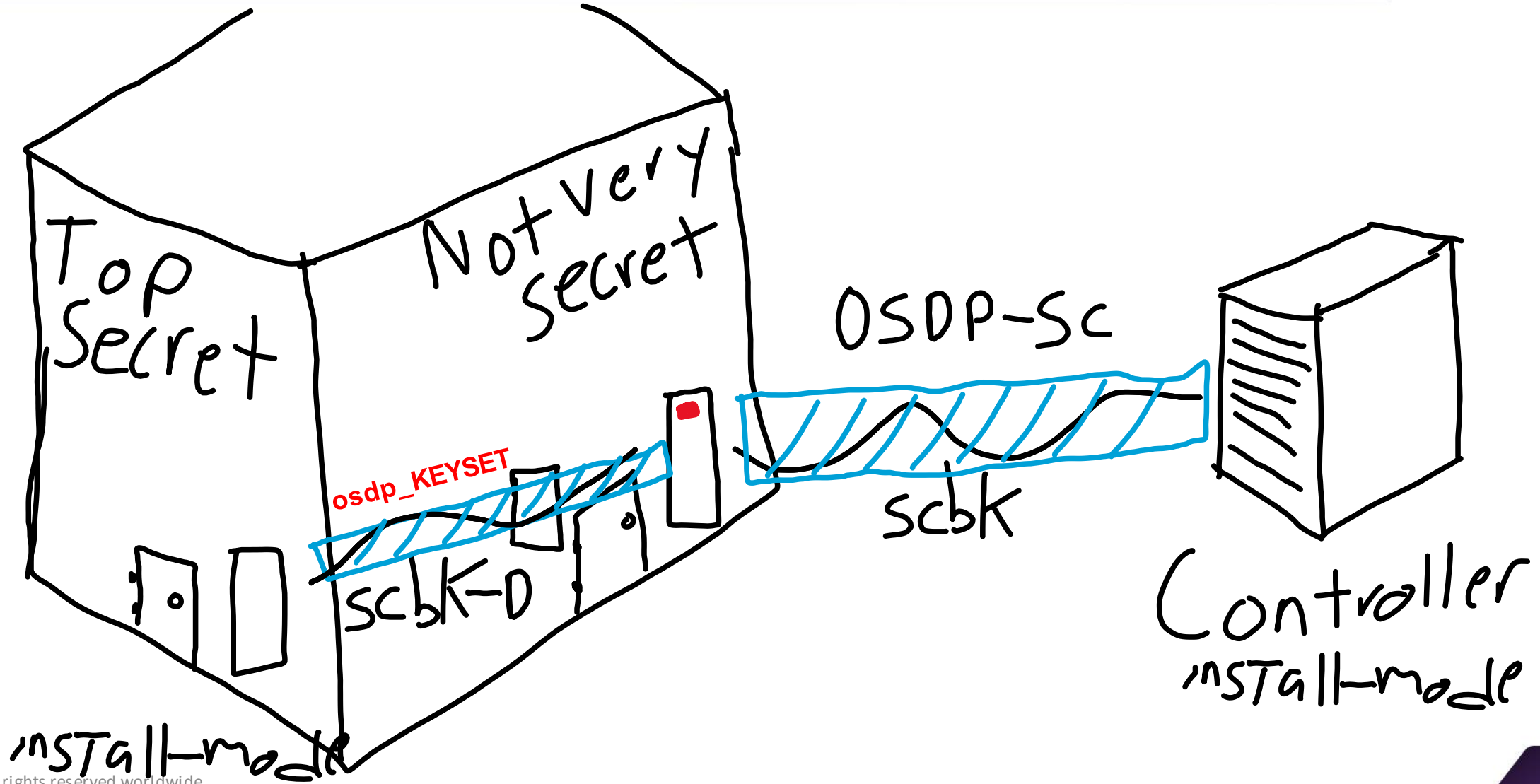

© Bishop Fox. All rights reserved worldwide.

# RS-485



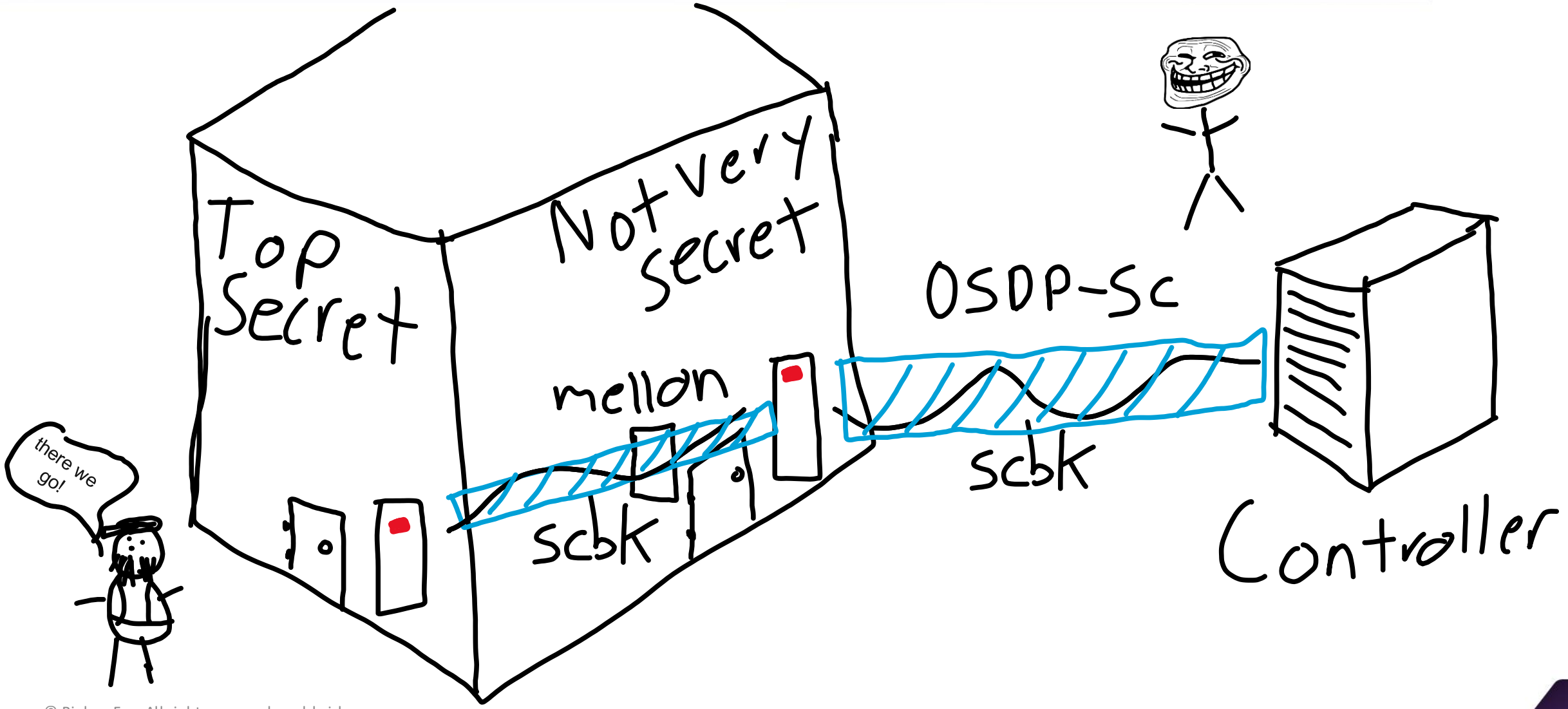

© Bishop Fox. All rights reserved worldwide.

# RS-485



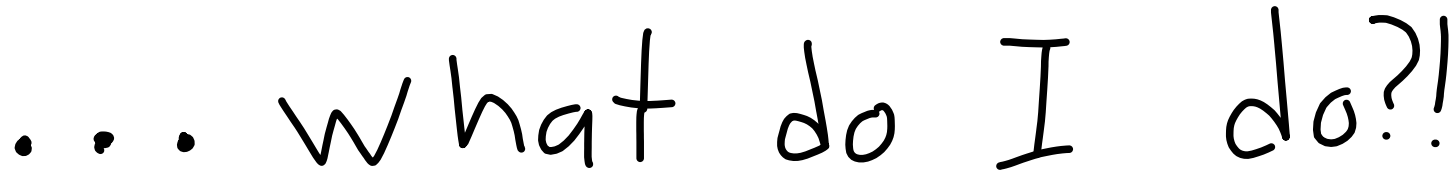

© Bishop Fox. All rights reserved worldwide.

# RS-485




© Bishop Fox. All rights reserved worldwide.

# Conclusion



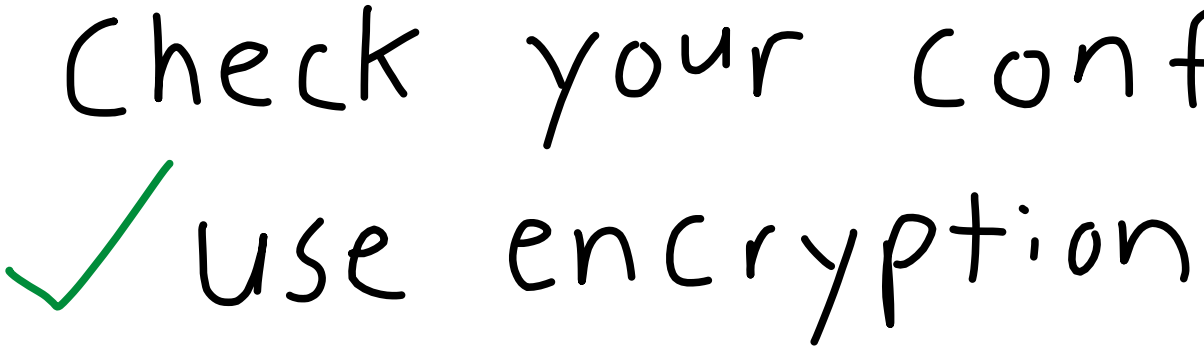

© Bishop Fox. All rights reserved worldwide.

# Conclusion

Check your configs

© Bishop Fox. All rights reserved worldwide.

# Conclusion




© Bishop Fox. All rights reserved worldwide.

# Conclusion

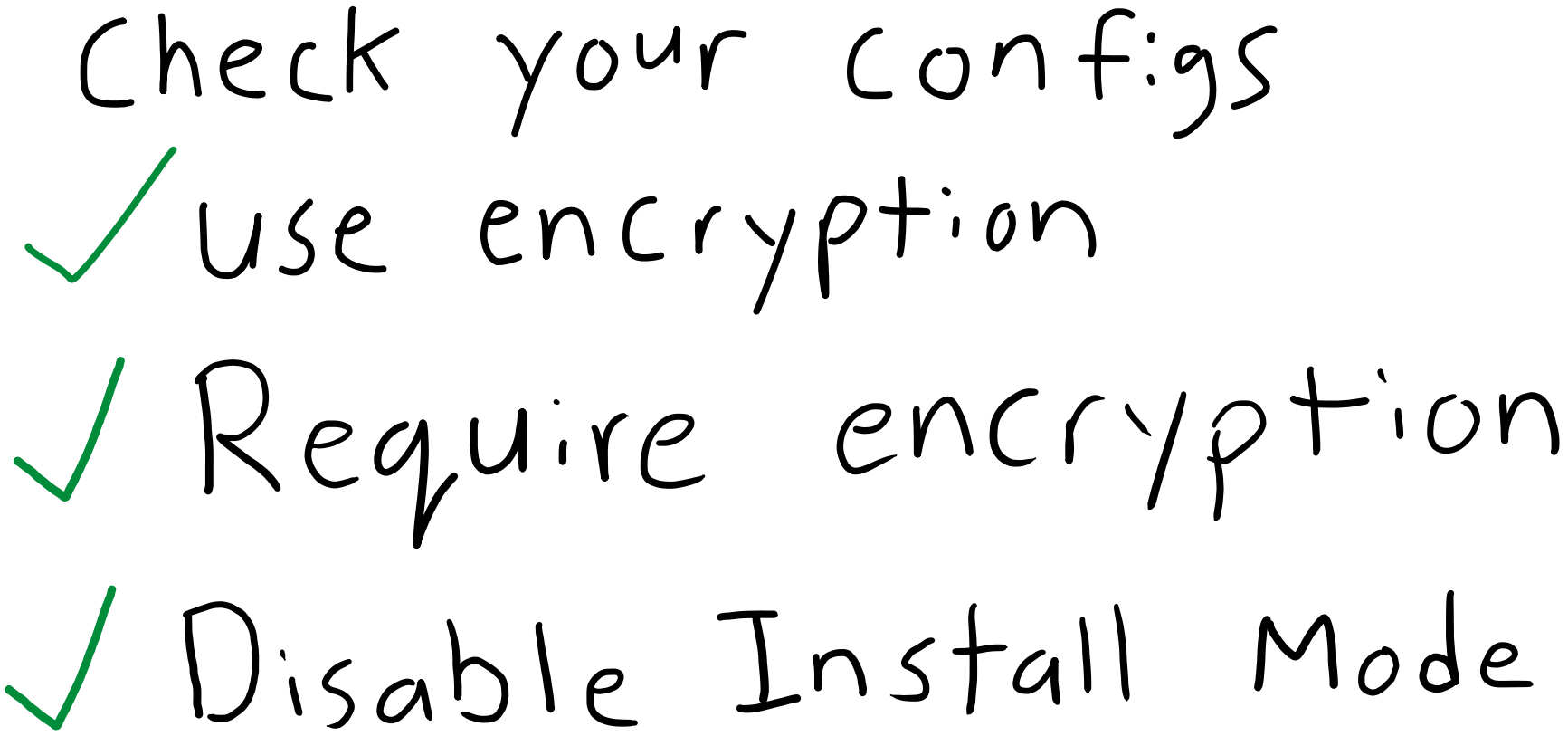
Check your configs

✓ use encryption

✓ Require encryption

© Bishop Fox. All rights reserved worldwide.

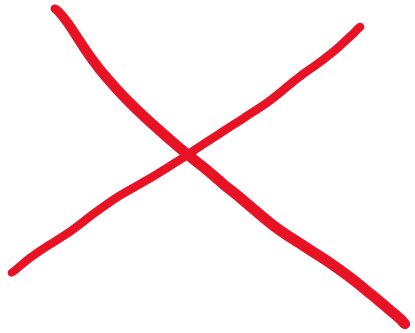
# Conclusion




© Bishop Fox. All rights reserved worldwide.

# Conclusion

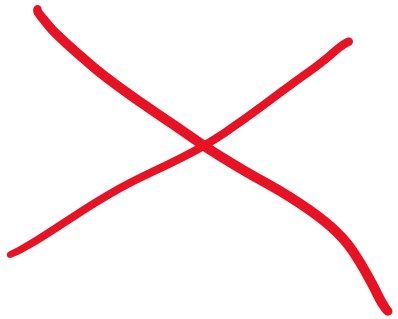
Never configure a reader in production.



© Bishop Fox. All rights reserved worldwide.

# Conclusion

Don't ignore tamper alerts



© Bishop Fox. All rights reserved worldwide.

# Conclusion

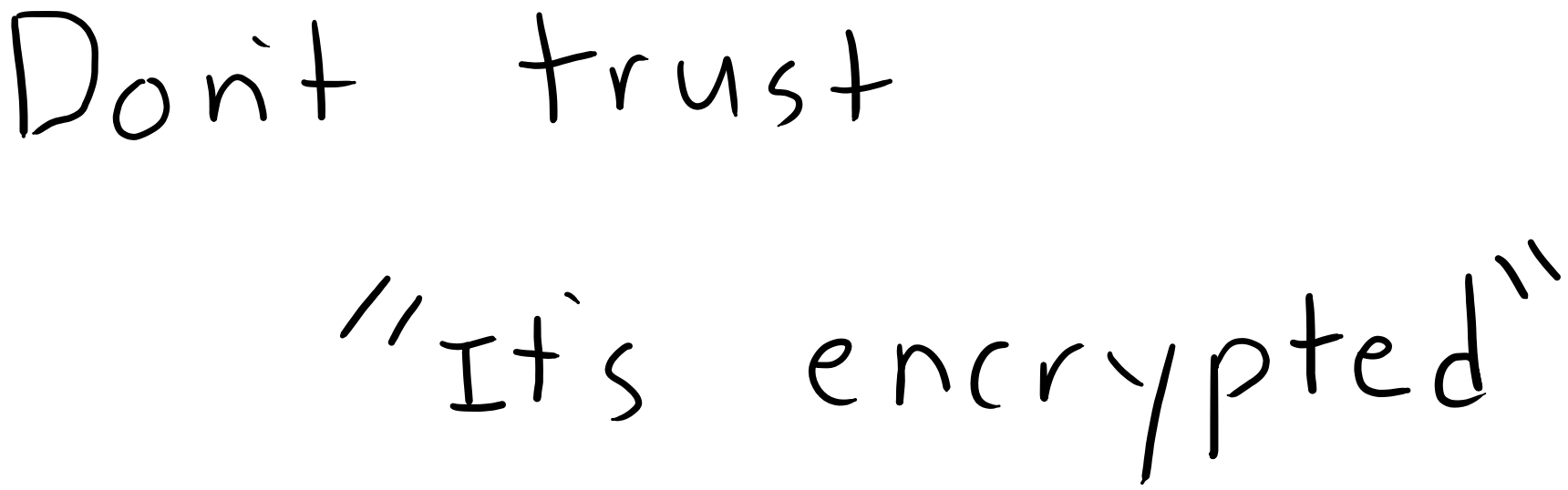
Buy OSDP Verified Devices

✓

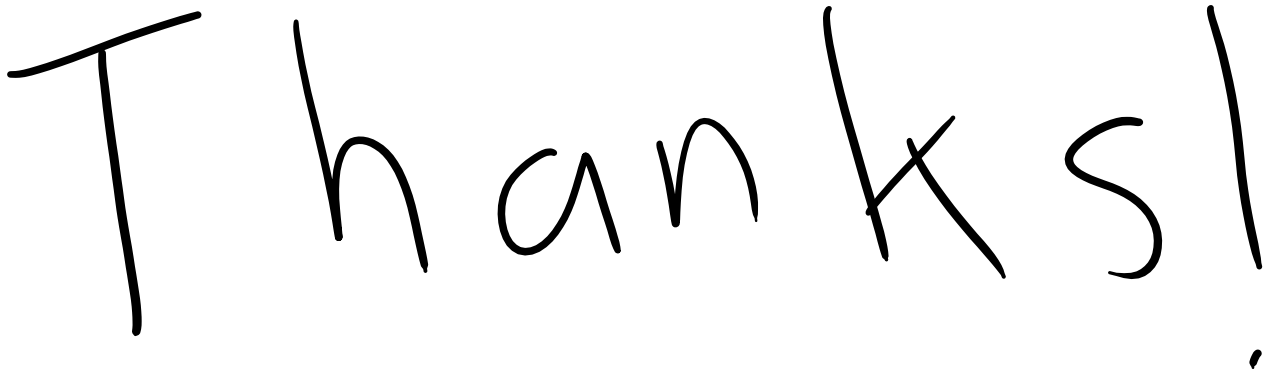



© Bishop Fox. All rights reserved worldwide.

# Conclusion




© Bishop Fox. All rights reserved worldwide.




© Bishop Fox. All rights reserved worldwide.