

Forum:[Hack Forums](#)

Thread: [Port-knocking - Fwknop - Single Packet Authorization : Process of encoding the data](#)

Laktick - January 29, 2021, 7:32 am

Hello,

I am working on the Port-knocking concept and i have implemented fwknop that uses Single Packet Authorization. The problem is that i don't understand how the data is encoded and how the authenticity and integrity are guaranteed. I don't understand the role of HMAC, key, digest, SHA256, Rijndael, etc.

That is the output of a test command that shows the data in the SPA packet (don't worry it is a model in personal VMs for tests) :

SPA Field Values:

Random Value: 3055038011819845

Username: ubuntu

Timestamp: 1611964357

FKO Version: 2.0.1

Message Type: 1 (Access msg)

Message String: 192.168.1.2,tcp/22

Nat Access:

Server Auth:

Client Timeout: 0

Digest Type: 3 (SHA256)

HMAC Type: 3 (SHA256)

Encryption Type: 1 (Rijndael)

Encryption Mode: 2 (CBC)

Encoded Data: 3055038011819845:dWJ1bnR1:1611964357:2.0.1:1:MTkyLjE2OC4xLjlsdGNwLzly

SPA Data Digest: Xu/qpfdp8H3Pgx2wzrbtQG7FK/CtR+yTu5LKZI/QH9o

HMAC: Fw6Jk+3OiDS3A/Ac9t93OSYfBgLWOmIP8CrtmgZYoXg

Final SPA Data:

/b3WwdTEqEPUYZnJ+z0mrdSNtY1MiYkjrfCKVmnfcl+2U6PHD0g6wwYBvaW4duys14iuG+Lk+9NN
SFHEiCI8XJA5BkZHcru1tCg8s8Rd+sjn/w+TmKsqZMf0QIUuTis+XqECyhlrvwOQ/nDIJCirBj8rFK2m
s2DcDBt4GuOgh0KwZR2EYXJuY