MaTaDoR: MOVING TARGET DEFENSE ROUTER

Berkan Ufuk, Mehmet Tahir SANDIKKAYA

OUTLINE

1. Introduction

    1. 1 Background

2. Related Works

    2.1 Advantages & Disadvantages

3. Use Case

    3.1 Demo

4. Performance Evaluation

5. Conclusion

1. INTRODUCTION

Motivation

Hypothesis

Contributions

- -Chaffing unwanted traffic
- -Early message authentication & cross-layer decision making
- -Going Unnoticed
- -Lightweight, fast and scalable protection

1.1. BACKGROUND

-Moving Target Defense (MTD)

-Denial of Service (DoS)

-TCP–Authentication Option (TCP-AO)

-Proxy

-Hash-based Message Authentication Codes (HMAC)

-IPTables

1.1. BACKGROUND – Moving Target Defense (MTD)

Collection of technologies that seek to improve security and increase resilience and availability of an application through increasing diversity of software and network paths.

Diversity, Shuffling, Redundancy

1.1. BACKGROUND – Denial of Service (DoS)

Targets «AVAILABILITY»

Different variants of DoS:

- Volume based
- UDP attacks
- ICMP attacks
- HTTP flood
- Slowloris

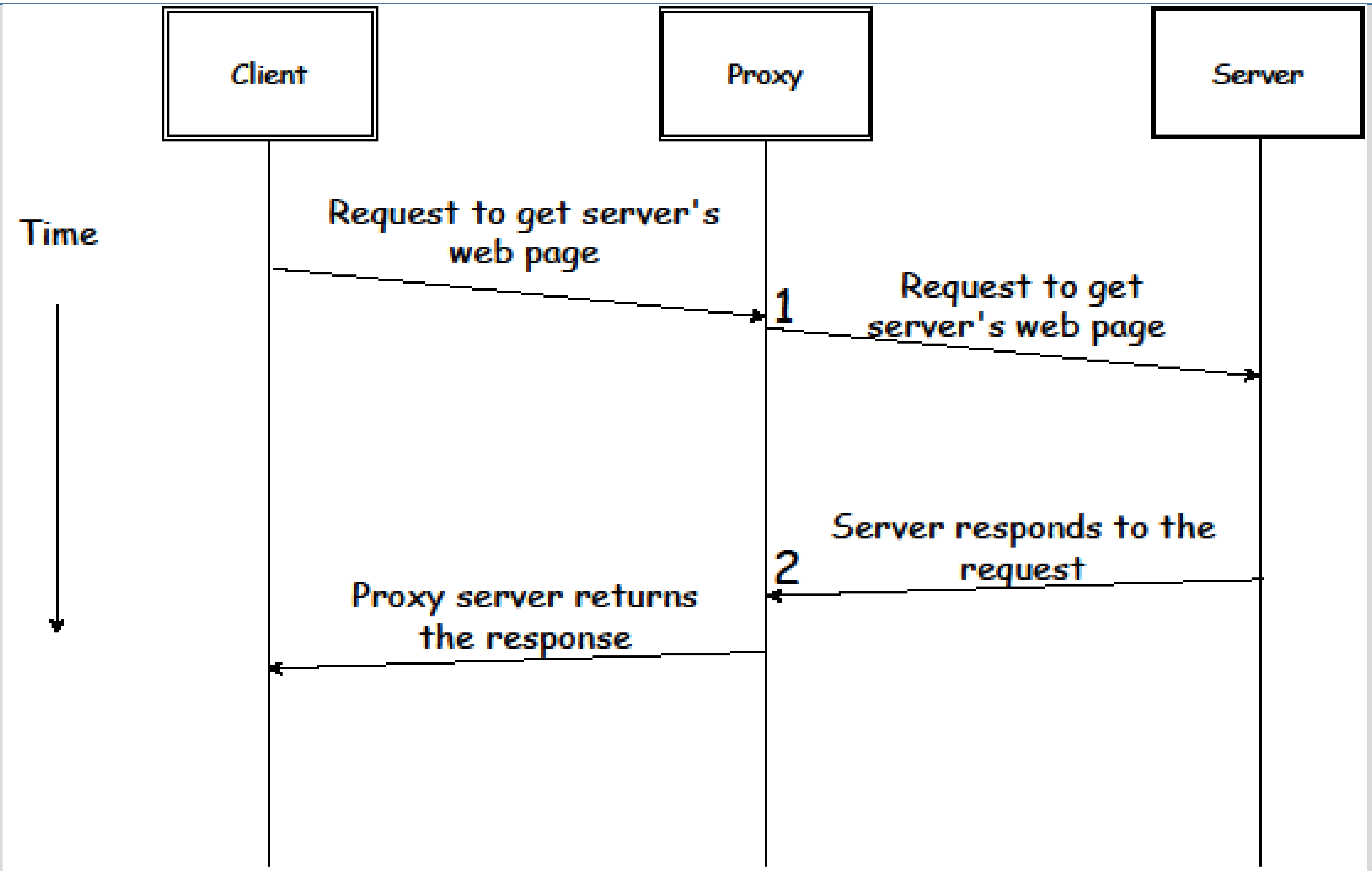
1.1. BACKGROUND – TCP-AO

Message authentication method

BGP & LDP Sessions

Enhance the Security and Authenticity of TCP segments

1.1. BACKGROUND - Proxy


Client
Proxy
Server
Time
Request to get server's web page
1
Request to get server's web page
Server responds to the request
2
Proxy server returns the response

1 - Proxy server changes the client's address in the request to its own

2- Proxy server changes the server's address in the response to its own

1.1. BACKGROUND – Hash-based Message Authentication Codes (HMAC)

Hash function

Secret Key

Verify data is correct and authentic with shared secrets

1.1. BACKGROUND - IPTables

Configures IP packet filter rules

- **PREROUTING:** Immediately after being received by an interface.
- **POSTROUTING:** Right before *leaving* an interface.
- **INPUT:** Right before being handed to a local process.
- **OUTPUT:** Right after being *created* by a local process.
- **FORWARD:** For any packets coming in one interface and leaving out another.

2. RELATED WORK

MTD is first mentioned by Zhou et al.

Several uses: MTD approach in CANbus by Bogosyan et al. MTD algorithm for space systems by Jenkins et al.

GhostMTD designs a key distribution mechanism (Park et al.)

Kampanakis et al. & Jafarian et al. & Macfarland et al. designed MTD approach for SDN

Network-based MTD, NAT implementation that constantly changes server properties RPAH by Luo et al.

Survey and classification by Hong et al.

2.1. ADVANTAGES & DISADVANTAGES

Advantages

Early message authentication & cross-layer decision making

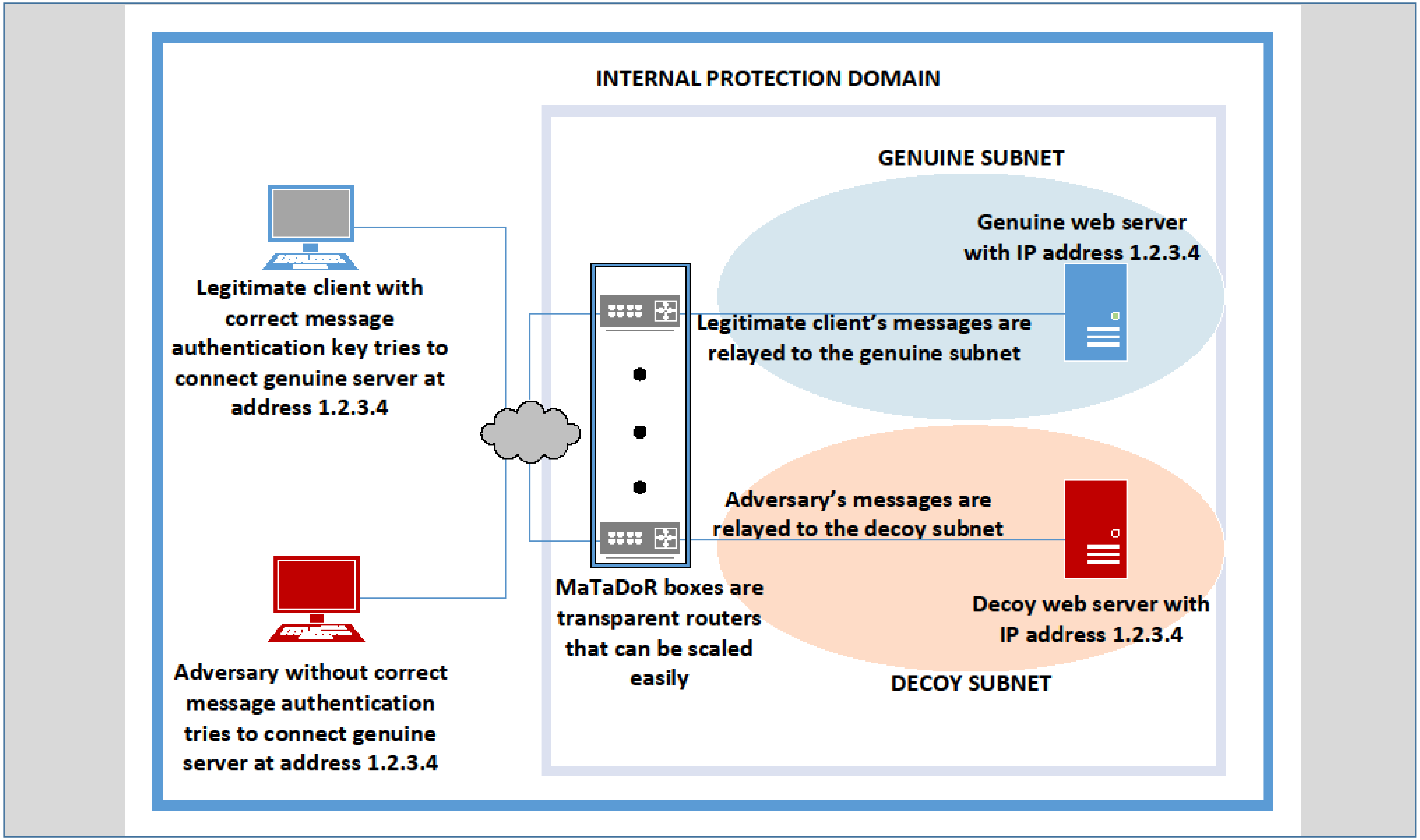
Hidden from the users of the network

Lightweight, fast and scalable

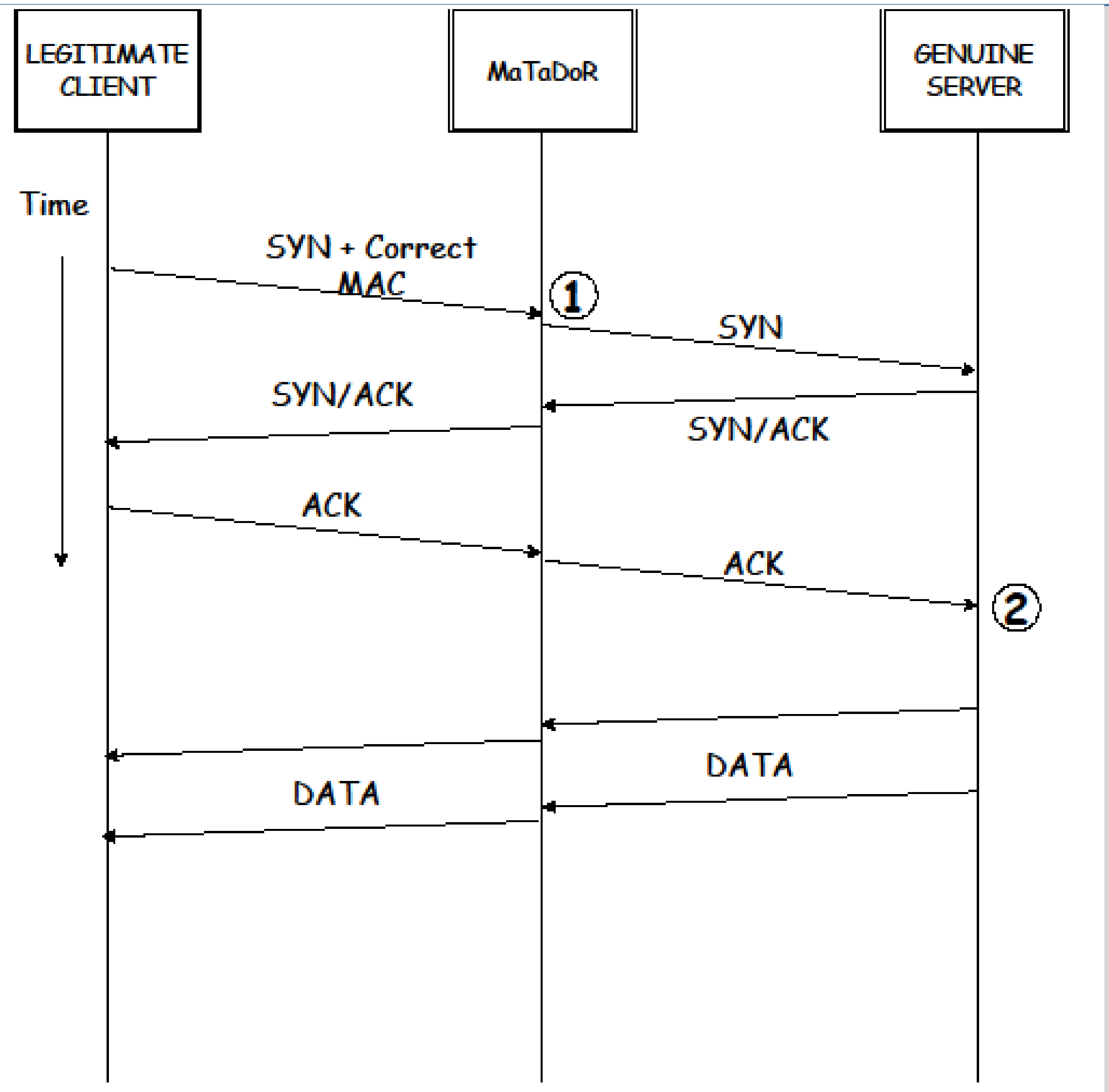
Disadvantages

Use cases are specific

3. USE CASE


INTERNAL PROTECTION DOMAIN
GENUINE SUBNET
Genuine web server with IP address 1.2.3.4
Legitimate client with correct message authentication key tries to connect genuine server at address 1.2.3.4
Legitimate client's messages are relayed to the genuine subnet
Adversary's messages are relayed to the decoy subnet
Decoy web server with IP address 1.2.3.4
MaTaDoR boxes are transparent routers that can be scaled easily
DECOY SUBNET
Adversary without correct message authentication tries to connect genuine server at address 1.2.3.4

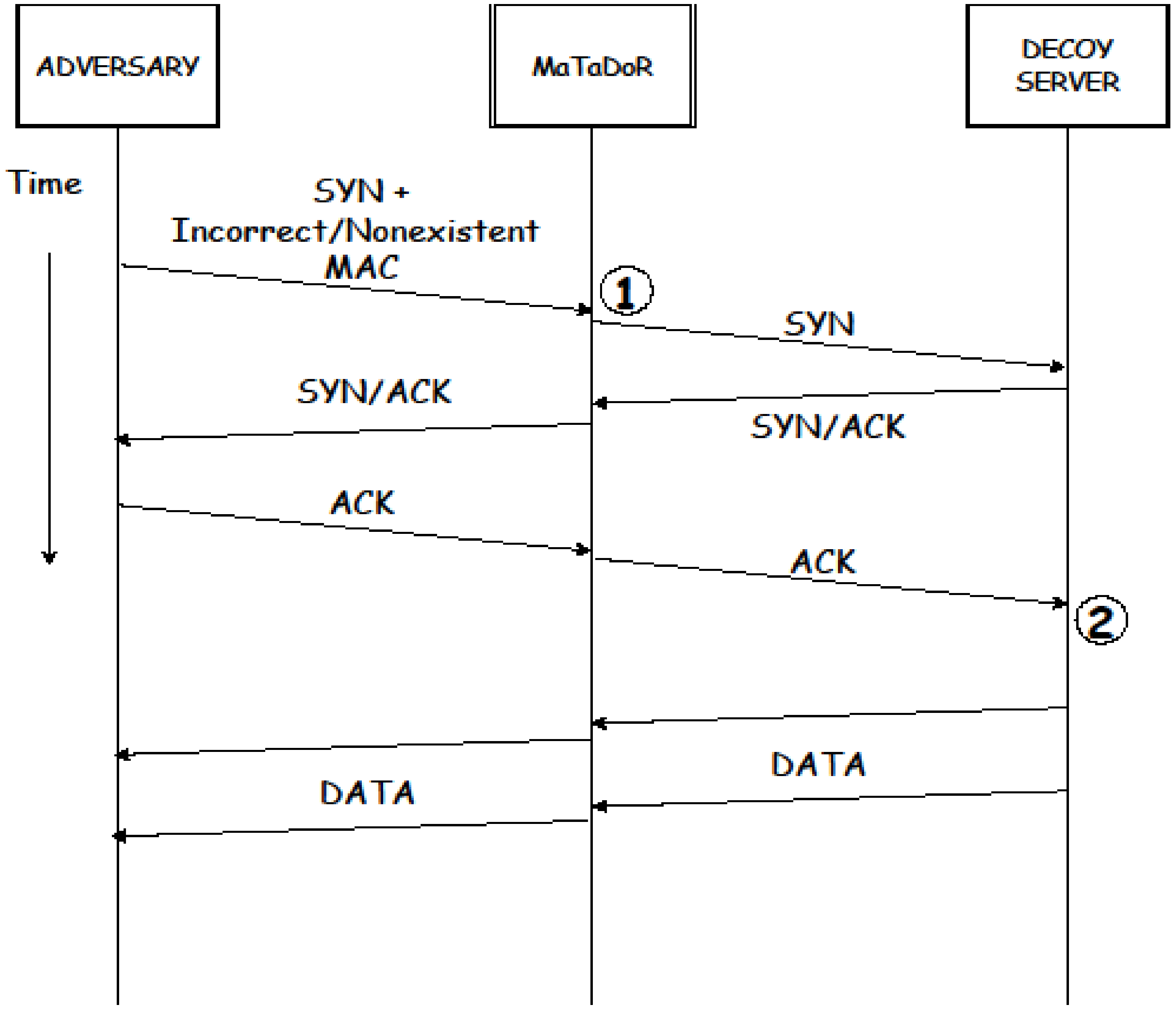
3. USE CASE



1 - MaTaDoR verified the segment and forwarded the client to the genuine server

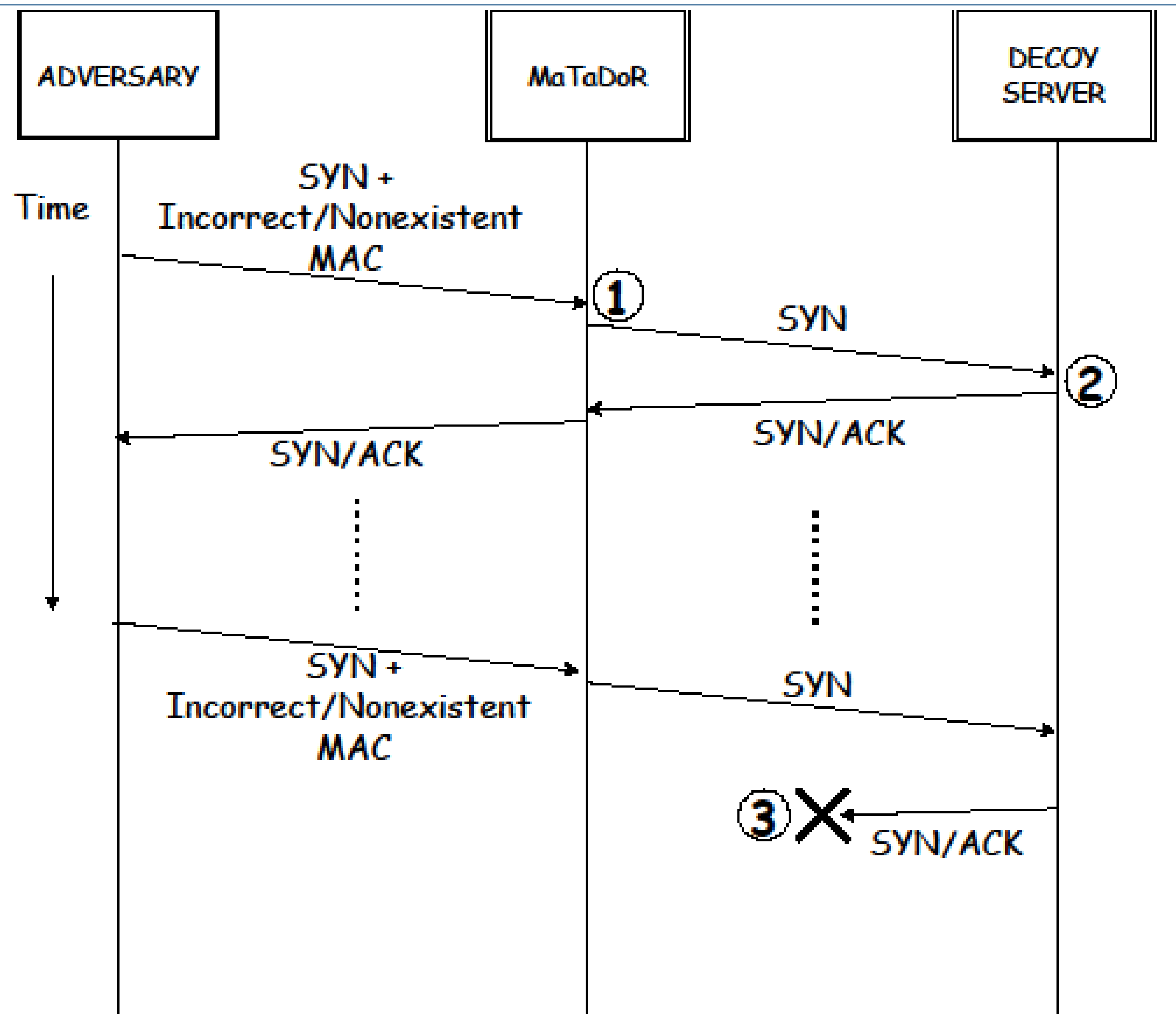
2- Handshake with the genuine server is completed

3. USE CASE



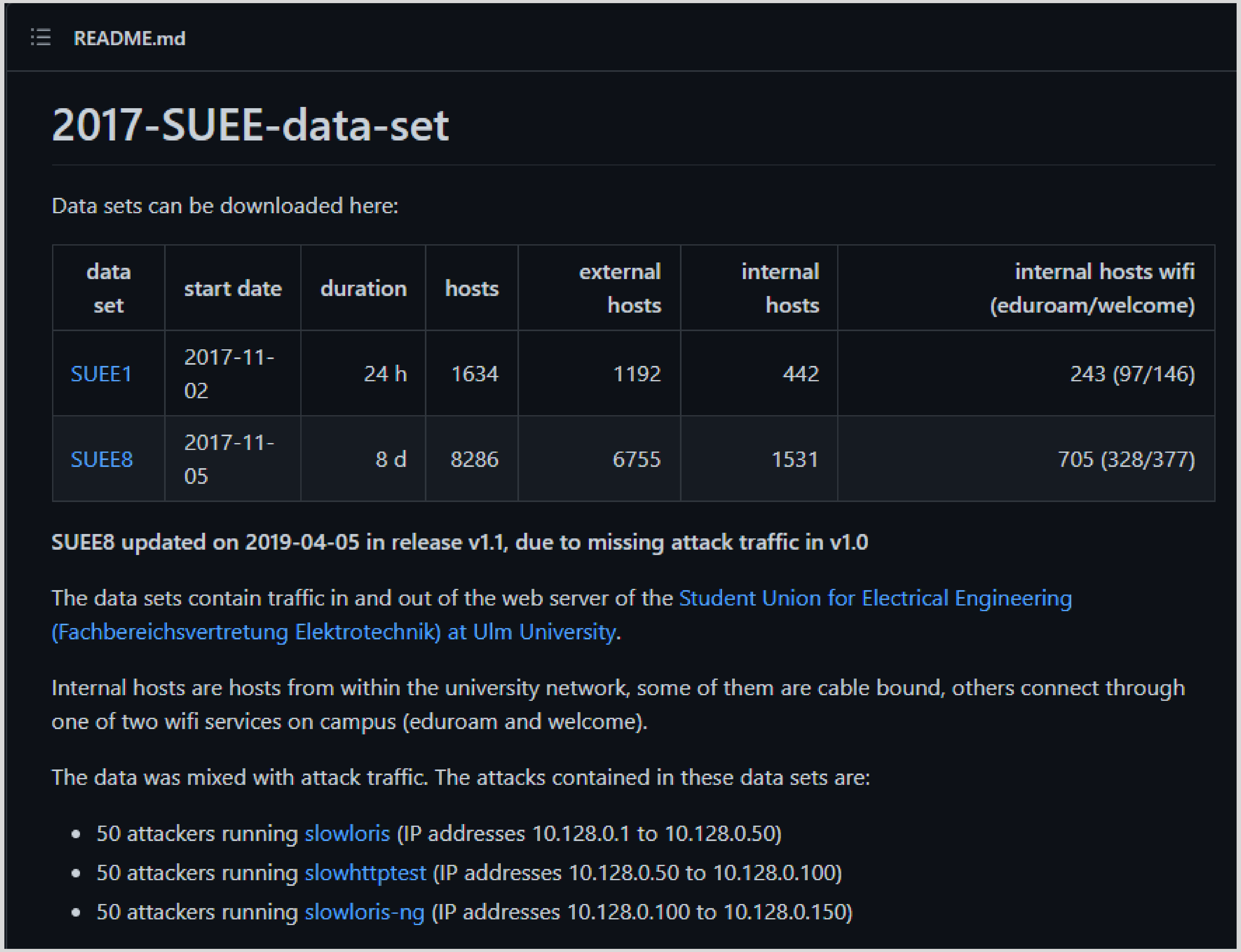
1 -MaTaDoR did not authenticate the message and forwarded the client to the decoy server
2- Handshake with the decoy server is completed

3. USE CASE


ADVERSARY
MaTaDoR
DECOY SERVER
Time
SYN + Incorrect/Nonexistent MAC
1
SYN
2
SYN/ACK
SYN/ACK
SYN + Incorrect/Nonexistent MAC
SYN
3
SYN/ACK

1 -MaTaDoR cannot authenticate the segment and forwarded the adversary to the decoy server
2- Decoy Server responds to SYN packets
3- Decoy Server becomes unavailable so that the adversary believes the attack has succeded. In the meantime, MaTaDoR is still available as it is stateless. Legitimate users are able to use the genuine server.

3. USE CASE



README.md

2017-SUEE-data-set

Data sets can be downloaded here:

data set	start date	duration	hosts	external hosts	internal hosts	internal hosts wifi (eduroam/welcome)
SUEE1	2017-11-02	24 h	1634	1192	442	243 (97/146)
SUEE8	2017-11-05	8 d	8286	6755	1531	705 (328/377)

SUEE8 updated on 2019-04-05 in release v1.1, due to missing attack traffic in v1.0

The data sets contain traffic in and out of the web server of the Student Union for Electrical Engineering (Fachbereichsvertretung Elektrotechnik) at Ulm University.

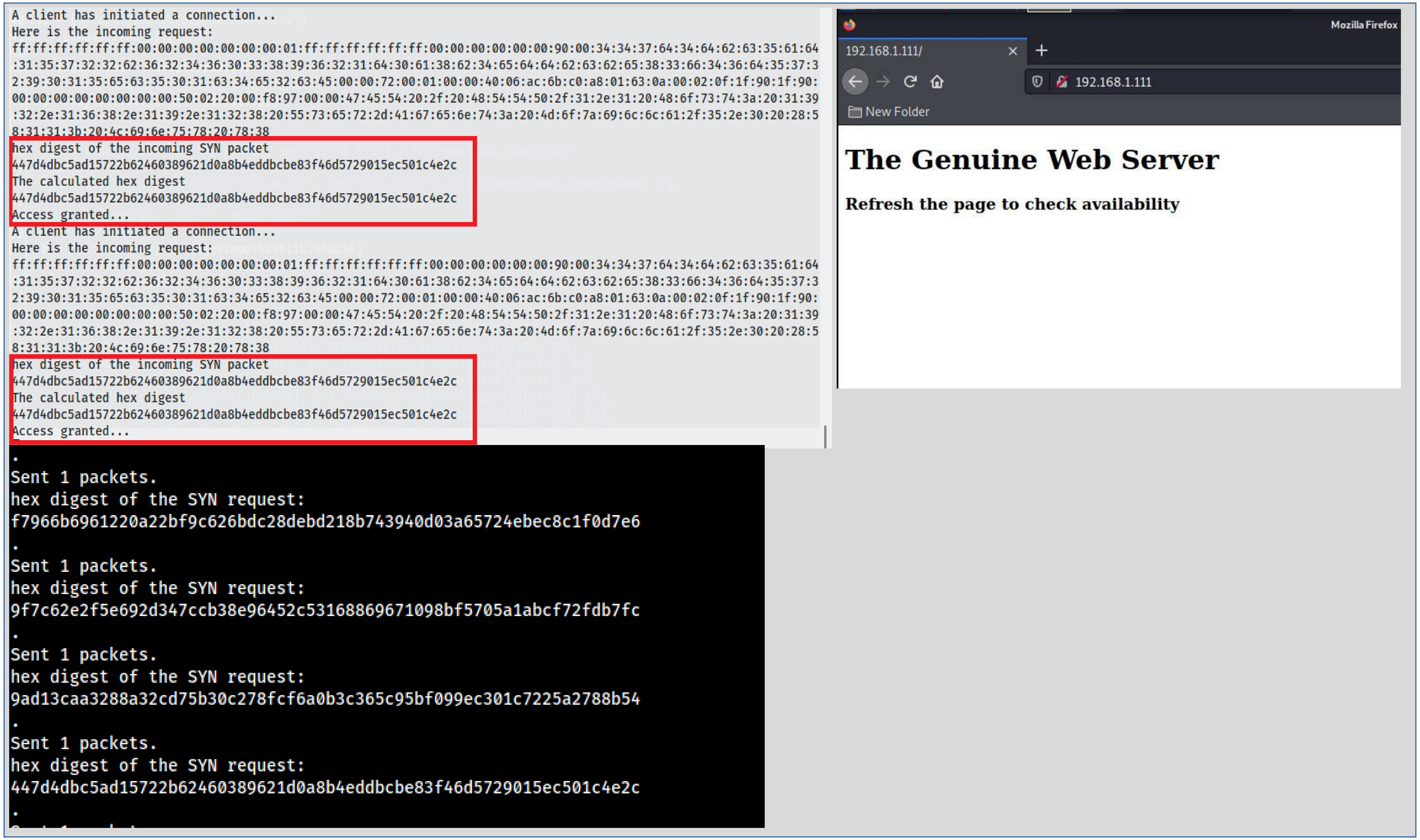
Internal hosts are hosts from within the university network, some of them are cable bound, others connect through one of two wifi services on campus (eduroam and welcome).

The data was mixed with attack traffic. The attacks contained in these data sets are:

- 50 attackers running slowloris (IP addresses 10.128.0.1 to 10.128.0.50)
- 50 attackers running slowhttptest (IP addresses 10.128.0.50 to 10.128.0.100)
- 50 attackers running slowloris-ng (IP addresses 10.128.0.100 to 10.128.0.150)

https://github.com/vs-uulm/2017-SUEE-data-set

3.1 DEMO



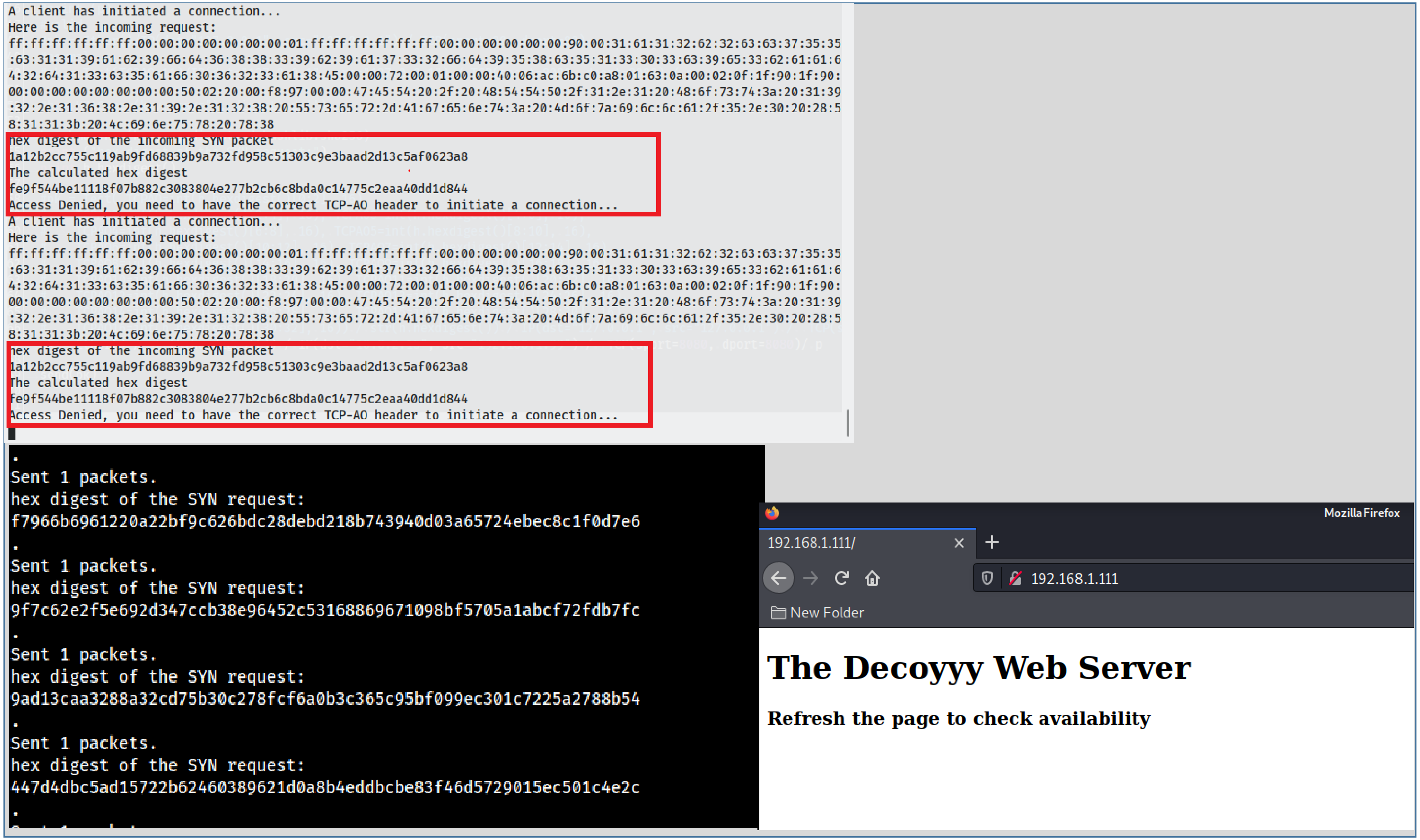
```
A client has initiated a connection...
Here is the incoming request:
ff:ff:ff:ff:ff:ff:00:00:00:00:00:00:01:ff:ff:ff:ff:ff:ff:00:00:00:00:00:00:90:00:34:34:37:64:34:64:62:63:35:61:64
:31:35:37:32:32:62:36:32:34:36:30:33:38:39:36:32:31:64:30:61:38:62:34:65:64:64:62:63:62:65:38:33:66:34:36:64:35:37:3
2:39:30:31:35:65:63:35:30:31:63:34:65:32:63:45:00:00:72:00:01:00:00:40:06:ac:6b:c0:a8:01:63:0a:00:02:0f:1f:90:1f:90:
00:00:00:00:00:00:00:00:50:02:20:00:f8:97:00:00:47:45:54:20:2f:20:48:54:54:50:2f:31:2e:31:20:48:6f:73:74:3a:20:31:39
:32:2e:31:36:38:2e:31:39:2e:31:32:38:20:55:73:65:72:2d:41:67:65:6e:74:3a:20:4d:6f:7a:69:6c:6c:61:2f:35:2e:30:20:28:5
8:31:31:3b:20:4c:69:6e:75:78:20:78:38
hex digest of the incoming SYN packet
447d4dbc5ad15722b62460389621d0a8b4eddbcbe83f46d5729015ec501c4e2c
The calculated hex digest
447d4dbc5ad15722b62460389621d0a8b4eddbcbe83f46d5729015ec501c4e2c
Access granted...
A client has initiated a connection...
Here is the incoming request:
ff:ff:ff:ff:ff:ff:00:00:00:00:00:00:01:ff:ff:ff:ff:ff:ff:00:00:00:00:00:00:90:00:34:34:37:64:34:64:62:63:35:61:64
:31:35:37:32:32:62:36:32:34:36:30:33:38:39:36:32:31:64:30:61:38:62:34:65:64:64:62:63:62:65:38:33:66:34:36:64:35:37:3
2:39:30:31:35:65:63:35:30:31:63:34:65:32:63:45:00:00:72:00:01:00:00:40:06:ac:6b:c0:a8:01:63:0a:00:02:0f:1f:90:1f:90:
00:00:00:00:00:00:00:00:50:02:20:00:f8:97:00:00:47:45:54:20:2f:20:48:54:54:50:2f:31:2e:31:20:48:6f:73:74:3a:20:31:39
:32:2e:31:36:38:2e:31:39:2e:31:32:38:20:55:73:65:72:2d:41:67:65:6e:74:3a:20:4d:6f:7a:69:6c:6c:61:2f:35:2e:30:20:28:5
8:31:31:3b:20:4c:69:6e:75:78:20:78:38
hex digest of the incoming SYN packet
447d4dbc5ad15722b62460389621d0a8b4eddbcbe83f46d5729015ec501c4e2c
The calculated hex digest
447d4dbc5ad15722b62460389621d0a8b4eddbcbe83f46d5729015ec501c4e2c
Access granted...
```

```
.
Sent 1 packets.
hex digest of the SYN request:
f7966b6961220a22bf9c626bdc28debd218b743940d03a65724ebec8c1f0d7e6
.
Sent 1 packets.
hex digest of the SYN request:
9f7c62e2f5e692d347ccb38e96452c53168869671098bf5705a1abcf72fdb7fc
.
Sent 1 packets.
hex digest of the SYN request:
9ad13caa3288a32cd75b30c278fcf6a0b3c365c95bf099ec301c7225a2788b54
.
Sent 1 packets.
hex digest of the SYN request:
447d4dbc5ad15722b62460389621d0a8b4eddbcbe83f46d5729015ec501c4e2c
.
```

The Genuine Web Server

Refresh the page to check availability

3.1 DEMO



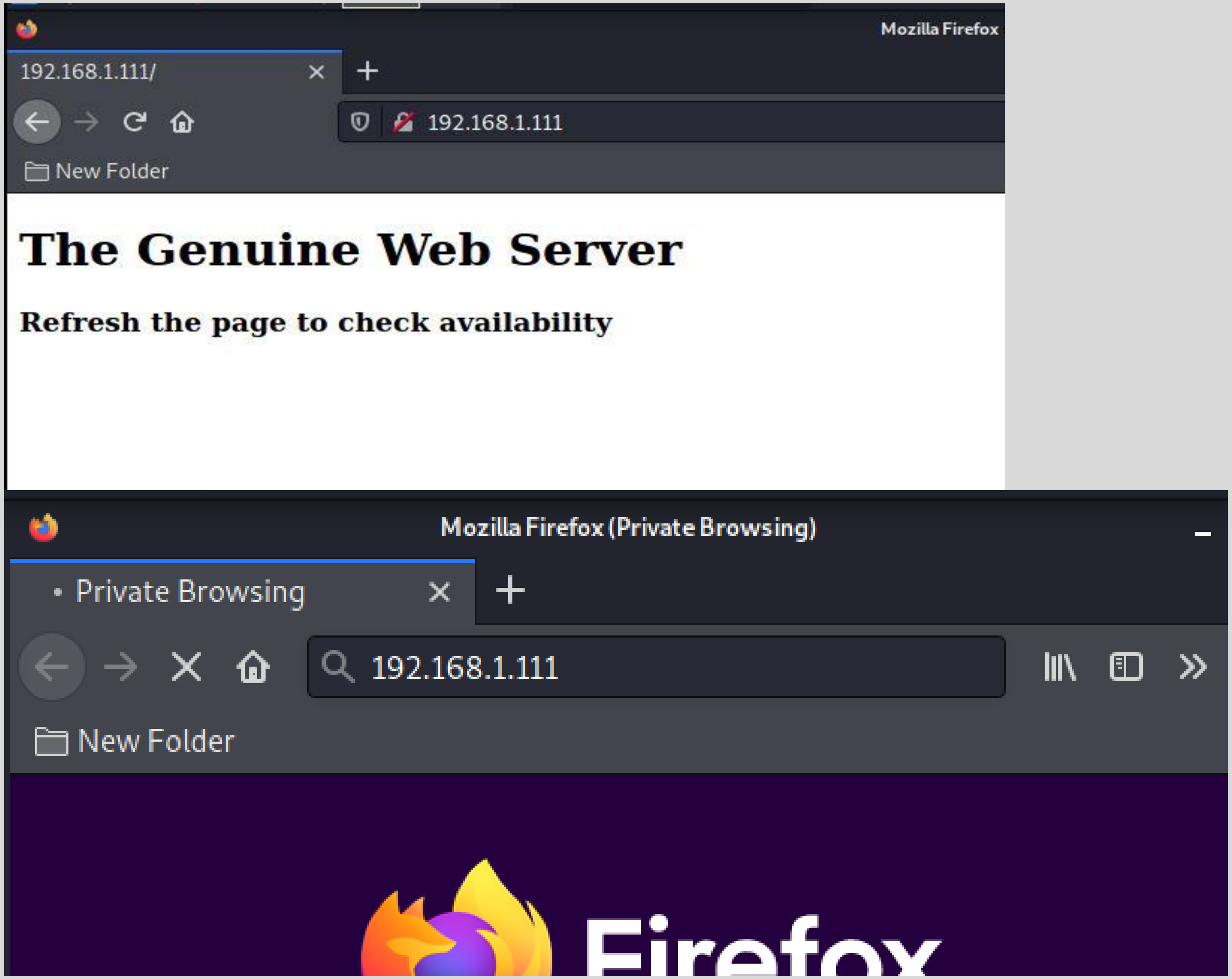
```
A client has initiated a connection...
Here is the incoming request:
ff:ff:ff:ff:ff:ff:00:00:00:00:00:00:00:01:ff:ff:ff:ff:ff:ff:00:00:00:00:00:00:90:00:31:61:31:32:62:32:63:63:37:35:35
:63:31:31:39:61:62:39:66:64:36:38:38:33:39:62:39:61:37:33:32:66:64:39:35:38:63:35:31:33:30:33:63:39:65:33:62:61:61:6
4:32:64:31:33:63:35:61:66:30:36:32:33:61:38:45:00:00:72:00:01:00:00:40:06:ac:6b:c0:a8:01:63:0a:00:02:0f:1f:90:1f:90:
00:00:00:00:00:00:00:00:50:02:20:00:f8:97:00:00:47:45:54:20:2f:20:48:54:54:50:2f:31:2e:31:20:48:6f:73:74:3a:20:31:39
:32:2e:31:36:38:2e:31:39:2e:31:32:38:20:55:73:65:72:2d:41:67:65:6e:74:3a:20:4d:6f:7a:69:6c:6c:61:2f:35:2e:30:20:28:5
8:31:31:3b:20:4c:69:6e:75:78:20:78:38
hex digest of the incoming SYN packet
1a12b2cc755c119ab9fd68839b9a732fd958c51303c9e3baad2d13c5af0623a8
The calculated hex digest
fe9f544be11118f07b882c3083804e277b2cb6c8bda0c14775c2eaa40dd1d844
Access Denied, you need to have the correct TCP-AO header to initiate a connection...
A client has initiated a connection...
Here is the incoming request:
ff:ff:ff:ff:ff:ff:00:00:00:00:00:00:00:01:ff:ff:ff:ff:ff:ff:00:00:00:00:00:00:90:00:31:61:31:32:62:32:63:63:37:35:35
:63:31:31:39:61:62:39:66:64:36:38:38:33:39:62:39:61:37:33:32:66:64:39:35:38:63:35:31:33:30:33:63:39:65:33:62:61:61:6
4:32:64:31:33:63:35:61:66:30:36:32:33:61:38:45:00:00:72:00:01:00:00:40:06:ac:6b:c0:a8:01:63:0a:00:02:0f:1f:90:1f:90:
00:00:00:00:00:00:00:00:50:02:20:00:f8:97:00:00:47:45:54:20:2f:20:48:54:54:50:2f:31:2e:31:20:48:6f:73:74:3a:20:31:39
:32:2e:31:36:38:2e:31:39:2e:31:32:38:20:55:73:65:72:2d:41:67:65:6e:74:3a:20:4d:6f:7a:69:6c:6c:61:2f:35:2e:30:20:28:5
8:31:31:3b:20:4c:69:6e:75:78:20:78:38
hex digest of the incoming SYN packet
1a12b2cc755c119ab9fd68839b9a732fd958c51303c9e3baad2d13c5af0623a8
The calculated hex digest
fe9f544be11118f07b882c3083804e277b2cb6c8bda0c14775c2eaa40dd1d844
Access Denied, you need to have the correct TCP-AO header to initiate a connection...
```

```
.
Sent 1 packets.
hex digest of the SYN request:
f7966b6961220a22bf9c626bdc28debd218b743940d03a65724ebec8c1f0d7e6
.
Sent 1 packets.
hex digest of the SYN request:
9f7c62e2f5e692d347ccb38e96452c53168869671098bf5705a1abcf72fdb7fc
.
Sent 1 packets.
hex digest of the SYN request:
9ad13caa3288a32cd75b30c278fcf6a0b3c365c95bf099ec301c7225a2788b54
.
Sent 1 packets.
hex digest of the SYN request:
447d4dbc5ad15722b62460389621d0a8b4eddbcbe83f46d5729015ec501c4e2c
.
```

The Decoyyy Web Server

Refresh the page to check availability

3.1 DEMO



The Genuine Web Server

Refresh the page to check availability

4. PERFORMANCE EVALUATION

Traffic	Real [s]	User [s]	Kernel [s]	CPU [%]	Delay [µs]
Benign w/o MaTaDoR	49159	827	4803	13	512
Benign w/ MaTaDoR	52647	1534	5132	14	598
Malicious w/o MaTaDoR	1332	12	186	16	462
Malicious w/ MaTaDoR	1467	32	365	17	631

4. PERFORMANCE EVALUATION

Traffic	CPU [%]	Additional CPU [%]
with MaTaDoR	0.7	4.2
without MaTaDoR	0.7	None

4. PERFORMANCE EVALUATION

Throughput Comparison	Ghost MTD*	MaTaDoR
Loss [%]	3.84	2.86

* Park, J.-G., Lee, Y., Kang, K.-W., Lee, S.-H., and Park, K.-W. (2020). Ghost-MTD: Moving target defense via protocol mutation for mission-critical cloud systems. Energies, 13(8).

5. CONCLUSION

A mechanism acting as a transparent router with authentication based filtering capabilities

Stateless and easily scalable

Lure adversaries away from the protected resources

TCP-AO like authentication mechanism is adapted to general purpose computers

REFERENCES

Bogosyan, S., Akgul, T., and Gokasan, M, “Mtd based novel scheme for bms security against can bus attacks during bev charging”, In 2020 9th Mediterranean Conference on Embedded Computing (MECO), pages 1–7. IEEE

Jenkins, C., Vugrin, E., Manickam, I., Troutman, N., Hazelbaker, J., Krakowiak, S., Maxwell, J., and Brown, R, “Moving target defense for space systems”. In 2021 IEEE Space Computing Conference (SCC), pages 60–71. IEEE.

Fang, Shih-Wei, Anthony Portante, and Mohammad Iftekhar Husain., “Moving target defense mechanisms in cyber-physical systems." *Securing Cyber-Physical Systems* (2015): 63.

Jafarian, J. H., Al-Shaer, E., and Duan, Q, “Openflow random host mutation: Transparent moving target defense using software defined networking”. In Proceedings of the First Workshop on Hot Topics in Software Defined Networks, HotSDN ’12, pages 127–132, New York, NY, USA. Association for Computing Machinery

Kampanakis, P., Perros, H., and Beyene, T, “Sdnbased solutions for moving target defense network protection”, In Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, pages 1–6.

Krawczyk, H., Bellare, M., and Canetti, R, “HMAC: Keyed-Hashing for Message Authentication”, Request for Comments 2104, Fremont, CA, USA: Internet Engineering Task Force.

Lukaseder, T., Maile, L., Erb, B., and Kargl, F, “Sdn-assisted network-based mitigation of slow ddos attacks”, In International Conference on Security and Privacy in Communication Systems, pages 102–121. Springer.

Luo, Y.-B., Wang, B.-S., Wang, X.-F., Zhang, B.-F., and Hu, W, “Rpah: A moving target network defense mechanism naturally resists reconnaissances and attacks”, IEICE Transactions on Information and Systems, E100.D(3):496–510.

MacFarland, D. C. and Shue, C. A, “The sdn shuffle: Creating a moving-target defense using host-based software-defined networking”, In Proceedings of the Second ACM Workshop on Moving Target Defense, MTD ’15, pages 37–41, New York, NY, USA. Association for Computing Machinery.

Park, J.-G., Lee, Y., Kang, K.-W., Lee, S.-H., and Park, K.-W, “Ghost-mtd: Moving target defense via protocol mutation for mission-critical cloud systems” Energies, 13(8).

Rivest, R. L. et al., “Chaffing and winnowing: Confidentiality without encryption.”, CryptoBytes (RSA laboratories), 4(1):12–17.

Rohith, R., Moharir, M., Shobha, G., et al., “Scapy a powerful interactive packet manipulation program”, In 2018 international conference on networking, embedded and wireless systems (ICNEWS), pages 1–5. IEEE.

Touch, J., Mankin, A., and Bonica, R. P., “The tcp authentication option. Request for Comments 5925”, Fremont, CA, USA: Internet Engineering Task Force.

Zhuang, Rui, Scott A. DeLoach, and Xinming Ou., “Towards a theory of moving
target defense.” Proceedings of the first ACM workshop on moving target defense. 2014

Hong, J. B. and Kim, D. S., “Assessing the effectiveness of moving target defenses using security models”, IEEE Transactions on Dependable and Secure Computing, 13(2):163–177.

THE END…

THANKS