Aplicação da Técnica Fuzzing em Testes da Implementação de Referência do SPDM

Thiago D. Ferreira[1], Renan C. A. Alves[3], Bruno C. Albertini[2], Marcos A. Simplicio Jr.[2], Daniel M. Batista[1]

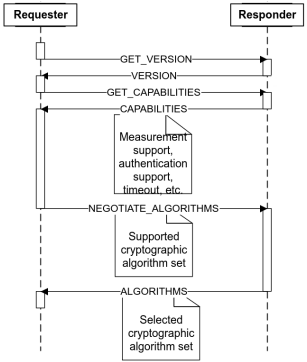
[1]Departamento de Ciência da Computação - USP

[2]Departamento de Engenharia de Computação e Sistemas Digitais - USP

[3]Escola de Artes, Ciências e Humanidades - USP

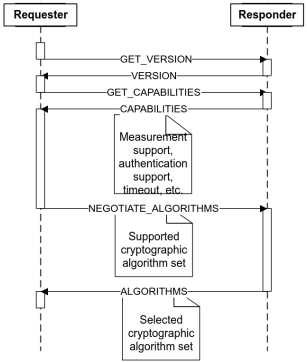
O que é SPDM?

- É a sigla para **Security Protocol and Data Model**, protocolo de 2019.



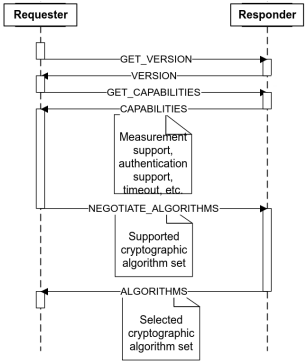
O que é SPDM?

- É a sigla para **Security Protocol and Data Model**, protocolo de 2019.
- Fornece autenticação e comunicação segura de *hardware*.



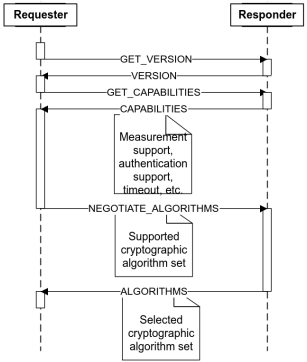
O que é SPDM?

- É a sigla para **Security Protocol and Data Model**, protocolo de 2019.
- Fornece autenticação e comunicação segura de *hardware*.
- Por ser recente, testes manuais vêm sendo feitos para atestar a confiabilidade de sua implementação em diversos cenários.



O que é SPDM?

- É a sigla para **Security Protocol and Data Model**, protocolo de 2019.
- Fornece autenticação e comunicação segura de *hardware*.
- Por ser recente, testes manuais vêm sendo feitos para atestar a confiabilidade de sua implementação em diversos cenários.
- Surge a ideia de criar um fuzzer e comparar sua eficiência ao lado de testes manuais.



O que é *Fuzzing*?

- É uma técnica para testes automatizada.

O que é *Fuzzing*?

- É uma técnica para testes automatizada.
- Envio de grande quantidade de dados para o sistema sobre teste com *fuzzers*.

O que é *Fuzzing*?

- É uma técnica para testes automatizada.
- Envio de grande quantidade de dados para o sistema sobre teste com *fuzzers*.

- **Campanha de fuzzing**: como os dados serão criados e enviados.

O que é *Fuzzing*?

- É uma técnica para testes automatizada.
- Envio de grande quantidade de dados para o sistema sobre teste com *fuzzers*.

- **Campanha de fuzzing**: como os dados serão criados e enviados.
- Existem duas maneiras principais de gerar esses dados:
  - Mutação

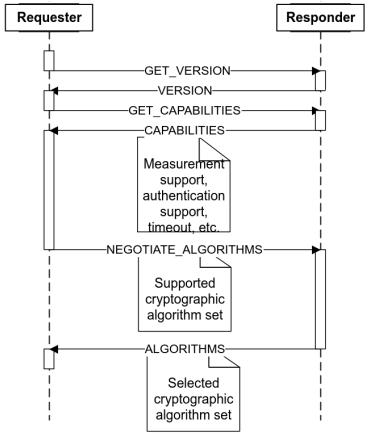
O que é *Fuzzing*?

- É uma técnica para testes automatizada.
- Envio de grande quantidade de dados para o sistema sobre teste com *fuzzers*.

- **Campanha de fuzzing**: como os dados serão criados e enviados.
- Existem duas maneiras principais de gerar esses dados:
  - Mutação
  - **Gramática**

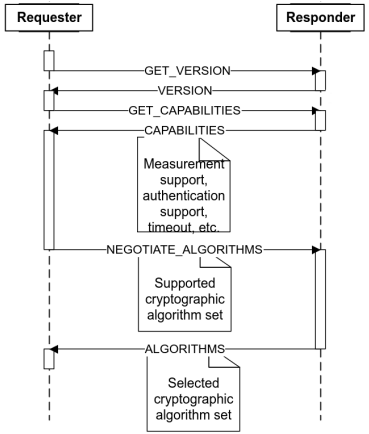
Campanha de *fuzzing*

- **Protocolo engessado**: a ordem das mensagens importa, por isso foi mantida.



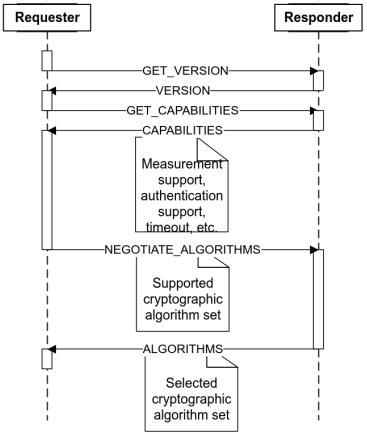
Campanha de *fuzzing*

- **Protocolo engessado**: a ordem das mensagens importa, por isso foi mantida.
- **Request-Response**: o `spdmfuzzer` agirá como *Responder* para emular dispositivo estranho.



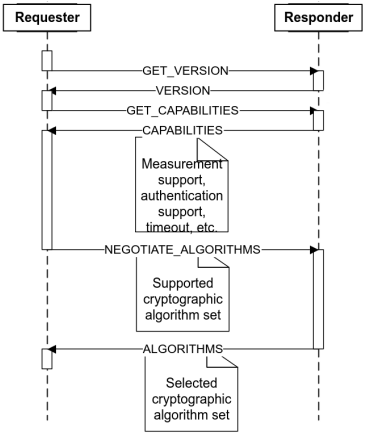
Campanha de *fuzzing*

- **Protocolo engessado**: a ordem das mensagens importa, por isso foi mantida.
- **Request-Response**: o `spdmfuzzer` agirá como *Responder* para emular dispositivo estranho.
- **Uso de gramática**: mensagem gerada possui valores aleatórios, porém, limitados de acordo com valores possíveis dos campos disponíveis.



Campanha de *fuzzing*

- **Protocolo engessado**: a ordem das mensagens importa, por isso foi mantida.
- **Request-Response**: o `spdmfuzzer` agirá como *Responder* para emular dispositivo estranho.
- **Uso de gramática**: mensagem gerada possui valores aleatórios, porém, limitados de acordo com valores possíveis dos campos disponíveis.
- **Modular**: campanha pode ser facilmente modificada.

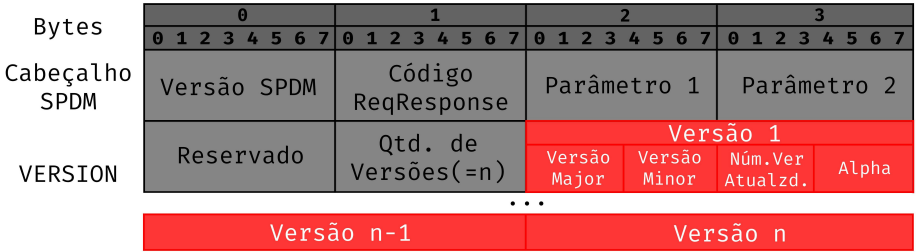


Resultados

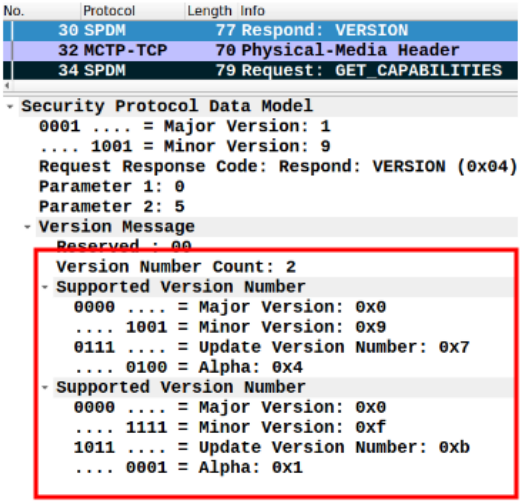
- **Respostas inesperadas**: mensagens inconsistentes com a documentação.

Resultados

- **Respostas inesperadas**: mensagens inconsistentes com a documentação.
- **Qtd. de Versões == 2**: mensagem é aceita independentemente do conteúdo.



Resultados



```
No.     Protocol    Length  Info
    30  SPDM           77   Respond: VERSION
    32  MCTP-TCP       70   Physical-Media Header
    34  SPDM           79   Request: GET_CAPABILITIES

Security Protocol Data Model
  0001 .... = Major Version: 1
  .... 1001 = Minor Version: 9
  Request Response Code: Respond: VERSION (0x04)
  Parameter 1: 0
  Parameter 2: 5
  Version Message
    Reserved : 00
    Version Number Count: 2
    Supported Version Number
      0000 .... = Major Version: 0x0
      .... 1001 = Minor Version: 0x9
      0111 .... = Update Version Number: 0x7
      .... 0100 = Alpha: 0x4
    Supported Version Number
      0000 .... = Major Version: 0x0
      .... 1111 = Minor Version: 0xf
      1011 .... = Update Version Number: 0xb
      .... 0001 = Alpha: 0x1
```

```
Version Number Count: 2
Supported Version Number
  0000 .... = Major Version: 0x0
  .... 1001 = Minor Version: 0x9
  0111 .... = Update Version Number: 0x7
  .... 0100 = Alpha: 0x4
Supported Version Number
  0000 .... = Major Version: 0x0
  .... 1111 = Minor Version: 0xf
  1011 .... = Update Version Number: 0xb
  .... 0001 = Alpha: 0x1
```

Avanços desde a submissão do artigo (1/2)

Máquina utilizada:
CPU AMD RYZEN 7 5800H
16GB de RAM
Debian 12 (Bookworm), com `psutil`
O uso de memória foi fixo de 3MB ao longo de toda a execução do programa.

Table: Uso de CPU ao rodar 30 vezes por 600 segundos cada.

Modo	CPU (%)	Variância$_{CPU}$
SPDM	0,48	0,12
SPDM + Fuzzing	1,23	0,17
Fuzzing	0,75	

Avanços desde a submissão do artigo (2/2)

- O *spdmfuzzer* suporta mais mensagens, todas com respostas inesperadas.

Avanços desde a submissão do artigo (2/2)

- O *spdmfuzzer* suporta mais mensagens, todas com respostas inesperadas.
- O objetivo é coletar métricas de estudo para avaliar a eficiência dessas mensagens antes de avançarmos mais para o suporte a novas mensagens.

Avanços desde a submissão do artigo (2/2)

- O *spdmfuzzer* suporta mais mensagens, todas com respostas inesperadas.
- O objetivo é coletar métricas de estudo para avaliar a eficiência dessas mensagens antes de avançarmos mais para o suporte a novas mensagens.

Mensagem	Status de Desenvolvimento	Resposta Inesperada?
VERSION	Finalizado	Sim (WTICG 24)
CAPABILITIES	Finalizado	Sim
ALGORITHMS	Em exploração	Sim
DIGESTS	Iniciado	Não aplicável
CERTIFICATE	Não iniciado	Não aplicável
CHALLENGE_AUTH	Não iniciado	Não aplicável

Obrigado!

https://github.com/th-duvanel/spdmfuzzer

{thiago.duvanel, renanalves, balbertini, msimplicio}@usp.br
batista@ime.usp.br