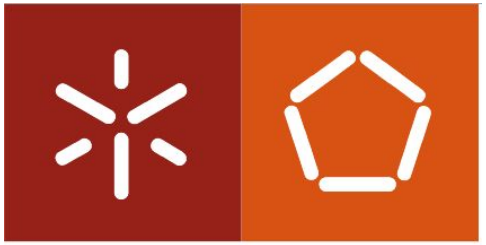


Universidade do Minho
Mestrado Integrado em Engenharia Informática
Julho de 2020

CMD SOAP - SCALA

Engenharia de Segurança

Diogo Duarte PG41843

Mateus Ferreira PG37159

Ricardo Dias PG39295

Introdução

- Este trabalho tem como objectivo testar o SCMD em Scala
- Serviço SCMD, tem 3 operações principais em funcionamento que são:
  - CMDGetCertificate
  - CMDccMovelSign
  - CMDValidateOtp

Implementação

- A nossa implementação foi baseada no serviço CMD-SOAP em Java.
- Foi implementada com auxílio do IDE Intellij, com plugin's activos de indentação, Camel Case, type inference.
- À medida que projecto foi sendo desenvolvido foram efetuados testes de segurança, foram seguidas as guidelines da linguagem, e implementadas outras medidas de segurança.

Técnicas e ferramentas de segurança aplicadas

- *Code Standard*
  - *Guidelines* da Linguagem
  - Indentação
  - *Camel Case*
  - *Type inference*

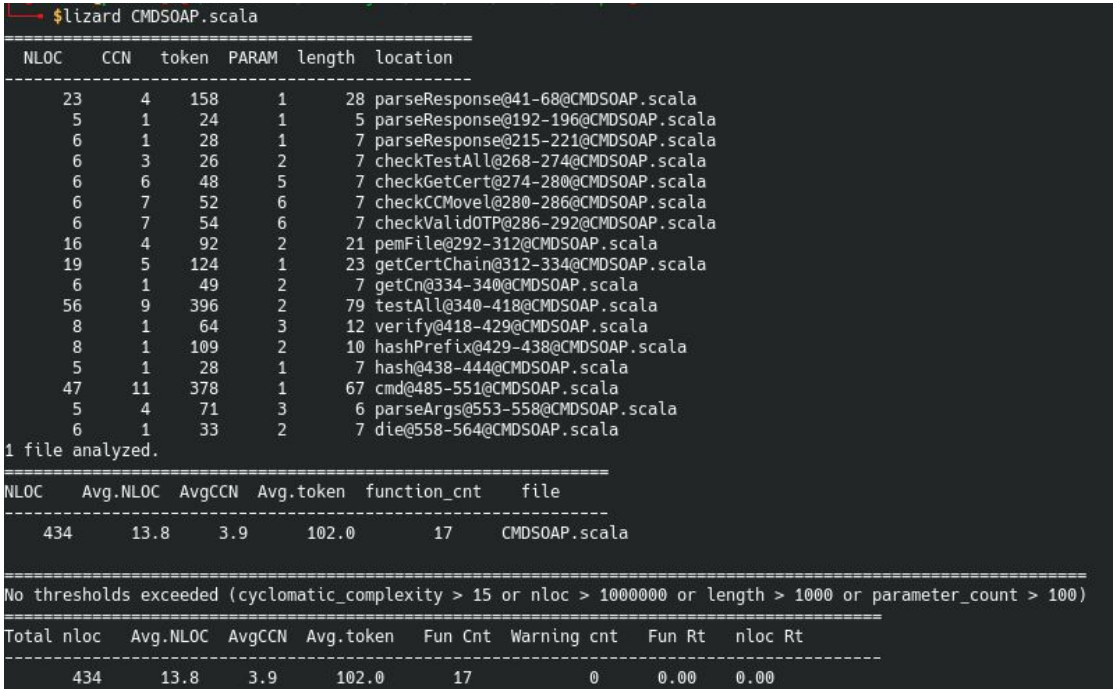
Técnicas e ferramentas de segurança aplicadas

- Validação de *inputs*
  - Recebe *String*
  - Valida tamanho

```
411     println("\nIntroduza o pin:")
412     val pin = scala.io.StdIn.readLine()
413     if (!(pin forall Character.isDigit) && pin.length > 8)
414       die( msg = "Pin not valid",  args = "Pin not valid")
```

Técnicas e ferramentas de segurança aplicadas

- Complexidade Ciclomática
  - Lizard



```
$lizard CMDSOAP.scala
================================================
  NLOC    CCN   token  PARAM  length  location
------------------------------------------------
      23      4    158      1      28 parseResponse@41-68@CMDSOAP.scala
       5      1     24      1       5 parseResponse@192-196@CMDSOAP.scala
       6      1     28      1       7 parseResponse@215-221@CMDSOAP.scala
       6      3     26      2       7 checkTestAll@268-274@CMDSOAP.scala
       6      6     48      5       7 checkGetCert@274-280@CMDSOAP.scala
       6      7     52      6       7 checkCCMovel@280-286@CMDSOAP.scala
       6      7     54      6       7 checkValidOTP@286-292@CMDSOAP.scala
      16      4     92      2      21 pemFile@292-312@CMDSOAP.scala
      19      5    124      1      23 getCertChain@312-334@CMDSOAP.scala
       6      1     49      2       7 getCn@334-340@CMDSOAP.scala
      56      9    396      2      79 testAll@340-418@CMDSOAP.scala
       8      1     64      3      12 verify@418-429@CMDSOAP.scala
       8      1    109      2      10 hashPrefix@429-438@CMDSOAP.scala
       5      1     28      1       7 hash@438-444@CMDSOAP.scala
      47     11    378      1      67 cmd@485-551@CMDSOAP.scala
       5      4     71      3       6 parseArgs@553-558@CMDSOAP.scala
       6      1     33      2       7 die@558-564@CMDSOAP.scala
1 file analyzed.
==============================================================
NLOC    Avg.NLOC  AvgCCN  Avg.token  function_cnt    file
--------------------------------------------------------------
    434      13.8     3.9      102.0        17     CMDSOAP.scala

=================================================================================================================
No thresholds exceeded (cyclomatic_complexity > 15 or nloc > 1000000 or length > 1000 or parameter_count > 100)
=================================================================================================
Total nloc   Avg.NLOC  AvgCCN  Avg.token   Fun Cnt  Warning cnt   Fun Rt   nloc Rt
-------------------------------------------------------------------------------------------------
       434      13.8     3.9      102.0        17            0      0.00    0.00
```

Técnicas e ferramentas de segurança aplicadas

- Sistema de *logs*

```
Jul 03, 2020 11:49:13 P.M. Main$ cmd
INFO: Get Certificate: userID: +351917806614, applicationID: b826359c-06f8-425e-8ec3-50a97a418916
Jul 03, 2020 11:49:14 P.M. Main$CMDgetcertificate sendSOAPrequest
SEVERE: Error java.io.IOException: Server returned HTTP response code: 500 for URL: https://cmd.autenticacao.gov.pt/Ama.Authentication.Frontend/CCMovelDigitalSignature.svc
Jul 03, 2020 11:51:19 P.M. Main$ cmd
INFO: Get Certificate: userID: +351917806614, applicationID: b826359c-06f8-425e-8ec3-50a97a418916
Jul 03, 2020 11:51:19 P.M. Main$CMDgetcertificate sendSOAPrequest
SEVERE: Error java.io.IOException: Server returned HTTP response code: 500 for URL: https://cmd.autenticacao.gov.pt/Ama.Authentication.Frontend/CCMovelDigitalSignature.svc
Jul 03, 2020 11:52:11 P.M. Main$ cmd
INFO: Get Certificate: userID: +351917806614, applicationID: b826359c-06f8-425e-8ec3-50a97a418916
Jul 03, 2020 11:52:12 P.M. Main$CMDgetcertificate sendSOAPrequest
SEVERE: Error java.io.IOException: Server returned HTTP response code: 500 for URL: https://cmd.autenticacao.gov.pt/Ama.Authentication.Frontend/CCMovelDigitalSignature.svc
Jul 03, 2020 11:52:12 P.M. Main$ die
```

Testes

```
└──╼ $scala CMDSOAP.scala TestAll -u +351917806614 -d assinar.txt

+++ Test All inicializado +++

0% ... Leitura de argumentos da linha de comando ficheiro: 'assinar.txt', user: +351917806614
10% ... A contactar servidor SOAP CMD para operação GetCertificate
20% ... Certificado emitido para 'Mateus da Silva Ferreira' pela Entidade de Certificação 'EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de
 Cidadão 00003' na hierarquia do 'Cartão de Cidadão 006'
30% ... Leitura do ficheiro 'assinar.txt'
40% ... Geração de hash do ficheiro 'assinar.txt'
50% ... Hash gerada: MDEwDQYJYIZIAWUDBAIBBQAEIOOwxEKY/BwUmvv0yJlvuSQnrkHkZJuTTKSVmRt4UrhV
Introduza o pin:
2704
60% ... A contactar servidor SOAP CMD para operação CCMovelSign
70% ... ProcessID devolvido pela operação CCMovelSign: 30f38383-e44f-452d-9eec-ea8e8a57661e
80% ... A iniciar operação ValidateOtp

Introduza o OTP recebido no seu dispositivo:
136398
90% ... A contactar servidor SOAP CMD para operação ValidateOtp
100% ... Assinatura devolvida pela operação ValidateOtp: VQ/KO52x+T8xkXSrZjxLR3gU5U0Ku9E9EZvWwqgMXv/D1V6PrLj9dZHrFJB+JXZfeVTd6As3PjF4CJV3X50EgkygOw5OpCVVEFoRGVV56K
9EJVLZanp58CawQR9OslnGHm+srrESN5pJi9O+2sIlAU7eQV5NMUy+q2on6ERNAy2Eks/bILuejwwwsnEhSRtSQOAlIJwdCVD0YPC1ZVSGSLqumgx2glraaQO5C46KmlpQ6V0AbkCntx5AL/bu3iJZ2n1CJxUhO6kv/
Aav/BMrgHq0YlUIu+8y6uZr/+R5hzqrNAqYDz/PzKEClkmg9SlgLlSX2o5Gvdp6z/UxLipeMJ+v9AqgYdDPvoHDgv9qFXQgrOVlcOGkV/mreuLWjSSkbVk3aXMocku87xITmTkBLgz/gASRxyHXceADWeQpRsXFyVy8
a+PRcbFggEk56we0swG3Tj43c5nYUkTeDc+34xQTvqkWALyIE0uBLpEoD4ur81M+QztN2KPPGydblWZU
110% ... A validar assinatura ...
Assinatura verificada? false
```

Dificuldades encontradas

- Falta de experiência com SCALA
- Verificação da assinatura devolvida pelo serviço utilizando RSA

Conclusão

- Foi com desagrado que o grupo que não conseguiu verificar a validação de OTP.
- Podemos aprender a trabalhar com uma nova linguagem de programação.
- Podemos aplicar em tempo real, diferentes medidas de segurança de modo a tornar o nosso código seguro.