Segurança e Privacidade

Assignment 1

Data Sharing with Encrypton

Relatório

André Abreu Couto | 2019215056 Edgar Rafael Cristo Antunes | 2016251340

Introdução

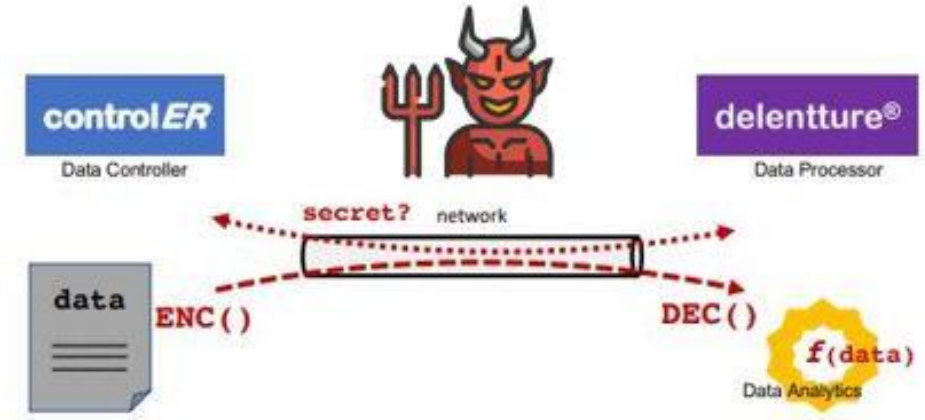
No âmbito da cadeira de Segurança e Privacidade foi realizado o *Assignment 1- Data Sharing with Encrypton* que tinha como principais objetivos:

- Estudar ameaças que afetam situações de partilha de dados;
- Compreender como podemos usar a criptografia para garantir a segurança dos dados;
- Aplicar estas técnicas na resolução de problemas reais.

A empresa *ControlER* presta serviços de crédito ao consumo e está preocupada com o a estratégia atual para avaliar o risco de um empréstimo devido a um aumento das infrações nos contratos de empréstimo. Por esta razão contratou a *Delentture*, uma empresa especializada em tratamento de dados, para que estes possam tentar resolver a situação. Surge então o problema de partilhar os dados com a *Delentture* garantindo a segurança destas informações confidenciais.

O que nós fizemos foi então garantir a segurança da partilha dessas informações através dos conhecimentos adquiridos na cadeira até então. Uma empresa encripta os dados, envia-os, a outra empresa recebe os dados, desencripta-os e analisa a integridade e autenticidade dos mesmos, e de seguida faz a análise pretendida.

O Problema



Na figura acima está descrito o cenário que nos foi apresentado e para podermos partilhar os dados com a *Delentture* de forma segura temos que nos proteger do pequeno diabo acima representado, o *attacker*. Ora se não o fizermos este pode destruir a integridade e autenticidade dos dados uma vez que estes ao passarem para a *Delentture* estão vulneráveis podendo ser facilmente manipulados. Se isso acontecer a contratação da *Delentture* passa a ser ineficiente uma vez que com dados alterados a análise a esses dados não tem propósito.

A Solução

Para resolver este problema, e com base nas aprendizagens da cadeira de Segurança e Privacidade decidimos que a melhor forma de encarar esta situação seria:

- Utilizar *sockets* para fazer a comunicação entre as duas empresas;
- Utilizar o *AES* para encriptar o ficheiro;
- Utilizar o *RSA* para encriptar a chave do *AES;*
- Utilizar *sockets* para a troca de chaves e depois o ficheiro encriptado é guardado num ficheiro binário e depois desencriptado pela outra empresa.

O *AES-Advanced Encryption Standard* é um algoritmo bastante utilizado em criptografia e tem como objetivo encriptar os dados de forma que não seja possível interpretá-los. É um mecanismo de criptografia simétrica e, portanto, utiliza a mesma chave para encriptar e desencriptar os dados. É bastante rápido, mas tem o problema de daqui a bastantes anos a chave ser recuperada e com ela poderem desencriptar o ficheiro.

Por esta razão decidimos utilizar o *RSA* para encriptar a chave do *AES*. Ora o *AES* já é um mecanismo de criptografia assimétrica e, portanto, necessita de uma chave pública e uma privada sendo que o nosso pequeno diabo apenas tem acesso à chave pública, não a podendo utilizar para desencriptar. A chave privada apensas poderia ser recuperada passados bastantes anos com uma falha na empresa ou algo do género.

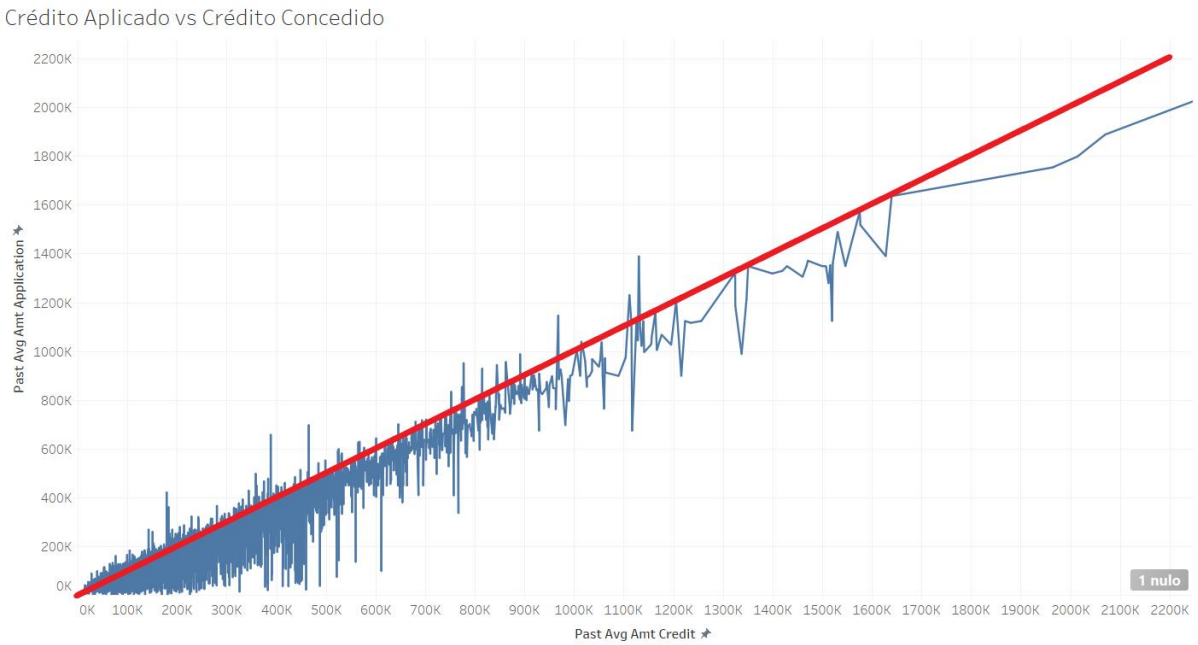
Posto isto, quando utilizamos o *AES* para encriptar o ficheiro com uma chave que por sua vez foi encriptada com *RSA* torna-se praticamente impossível para o *attacker* ter acesso aos dados. Este apenas pode ver a chave pública do *RSA* e a chave do *EAS*, mas encriptada, não conseguindo fazer nada com isso.

Como pedido, garantimos também a autenticidade dos dados ao permitir que a *Delentture* quando recebe e desencripta os dados verificar se estes não sofreram alterações.

Análise 1

Para fazer a análise dos dados, já desencriptados, decidimos colocar num ficheiro *csv* os dados dos clientes que infringiram de alguma forma o contrato de empréstimo juntamente com a informação de contratos anteriores.

Com a ajuda da ferramenta *Tableau* obtivemos os seguintes resultados:

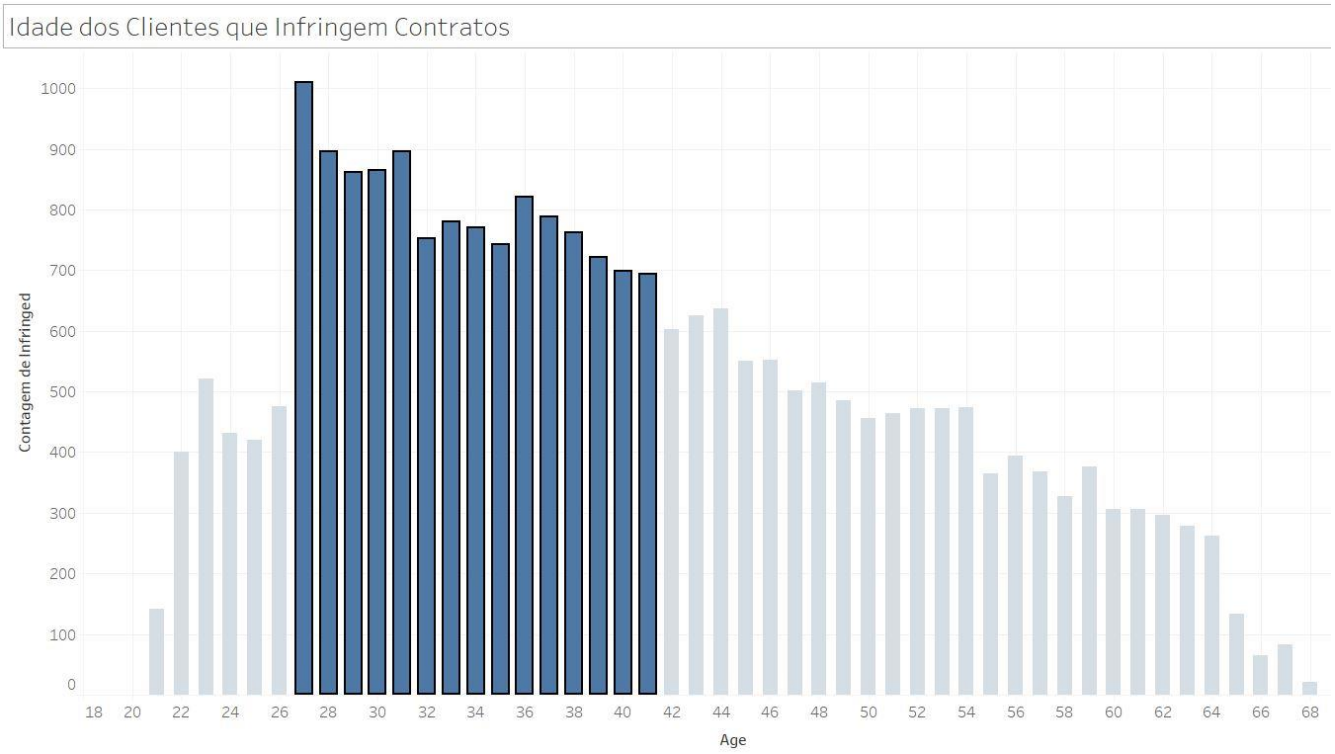


Este gráfico reflete a relação que existe entre a média de crédito concedido a cada cliente e a média de crédito aplicado pelo cliente, nos clientes que infringiram os contratos de empréstimo. A linha vermelha representa aquele que deveria ser o registo ideal, ou seja, os valores de crédito concedido coincidiam com os valores de crédito aplicado. Não acontece, pelo contrário, na maior parte dos clientes os valores estão bastante abaixo do pretendido. É importante referir que cerca de 4% (24825 em 615023) dos clientes infringiram de alguma forma os contratos.

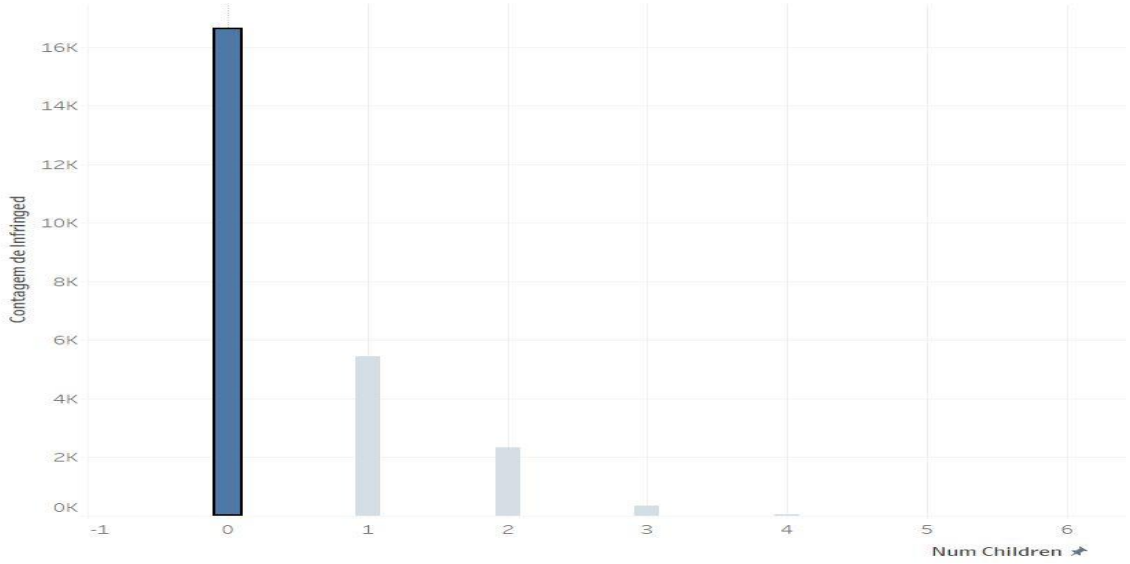
Análise 2

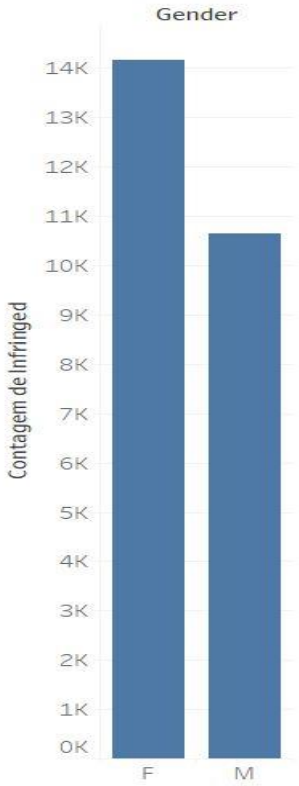
Quanto à segunda análise resolvemos colocar num ficheiro *csv* os dados dos clientes que infringiram de alguma forma o contrato de empréstimo juntamente com a informação relativa à sua idade, género e número de filhos.

Com a ajuda da ferramenta *Tableau* obtivemos os seguintes resultados:



O gráfico acima relaciona a quantidade de contratos infringidos com a idade do cliente e é então possível observar que a maior parte dos clientes que infringiram de alguma forma o contrato têm idades compreendidas entra os 27 e os 41 anos.





Os dois gráficos acima relacionam a quantidade de contratos infringidos com o número de filhos e com o género do cliente, respetivamente. Podemos observar que a maior parte dos clientes que infringiram de alguma forma os contratos de empréstimos não têm filhos (cerca de 67%, 16609 em 24825). Podemos também ver que os casos se encontram divididos quase da mesma forma por homens e mulheres, registando as mulheres mais 4 mil casos que os homens.

Conclusão

Em forma de conclusão resta apenas referir que o projeto relativo a este relatório permitiu-nos perceber a importância da segurança no tratamento de dados. Tivemos a oportunidade de desenvolver competências em criptografia e perceber quais os melhores algoritmos a ser utilizados. Conseguimos trabalhar com dados com a garantia de que estes estavam intactos e prontos a ser analisados. Consideramos, portanto, que todos os objetivos foram cumpridos com sucesso.

Bibliografia

- Documentação oficial da biblioteca de encriptação;
- Apontamentos teóricos da cadeira de Segurança e Privacidade.