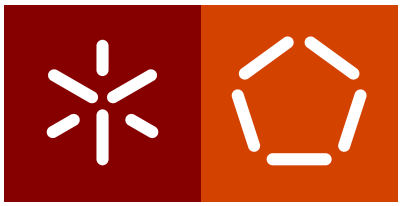
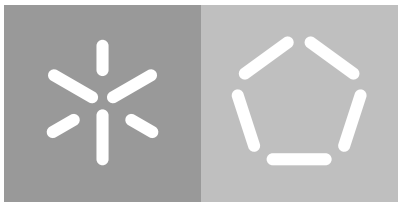


Universidade do Minho
Escola de Engenharia
Departamento de Informática

João Diogo Pereira da Rocha

Análise de Segurança para Soluções de Software para a Cloud

janeiro 2017



Universidade do Minho
Escola de Engenharia
Departamento de Informática

João Diogo Pereira da Rocha

Análise de Segurança para Soluções de Software para a Cloud

Dissertação de Mestrado
Mestrado em Engenharia Informática

Trabalho realizado sob orientação de
Professor José Carlos Bacelar Almeida
Professor Manuel Bernardo Martins Barbosa

janeiro 2017

AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer ao Professor Manuel Bernardo Barbosa e ao Professor José Carlos Bacelar Almeida pela forma como orientaram este trabalho. Toda a sua ajuda, disponibilidade e passagem de conhecimentos foram essenciais para me guiar no melhor sentido e garantir a motivação necessária durante a sua realização.

Agradecer também à Primavera bss e a todos os amigos que lá fiz pela forma como me receberam e sempre se demonstraram disponíveis para ajudar. Um agradecimento especial ao Hugo Ribeiro e ao Rui Monteiro por toda a experiência que transmitiram, pela compreensão demonstrada e pela forma organizada e profissional com que supervisionaram este trabalho.

Um agradecimento especial a toda a minha família, por quem sempre me esforço por deixar orgulhosos. Aos meus pais, o verdadeiro pilar de toda a minha formação académica e pessoal, por serem desde sempre o meu suporte e me presentearem diariamente com exemplos de força, coragem e superação. Seria impossível concluir os meus objetivos sem o seu constante apoio. Aos meus irmãos, ajuda preciosa no meu crescimento, por serem a minha principal fonte de inspiração e o exemplo que procuro seguir em qualquer circunstância. À Clara, por tudo o que significa, pela motivação e apoio transmitidos e por ser sempre o primeiro sinal de reconhecimento do meu trabalho. À sua família, pelos convites e pela forma como tão bem me acolheu durante este percurso.

Agradecer também a todos os amigos que me acompanharam durante estes cinco anos na Universidade, para os quais todas as palavras são poucas. Sem eles não seria certamente o que sou hoje.

Por último, mas não menos importante, à minha pequena sobrinha Beatriz, a quem dedico este trabalho, por ser a força final para esta última etapa.

Agradeço também a todos que direta ou indiretamente contribuíram na minha formação e a todos os meus familiares e amigos pela compreensão dada à minha indisponibilidade durante a realização desta dissertação.

ABSTRACT

Application life cycle management is a continuous process that, in the most successful cases, is extended for periods exceeding two decades and becomes a critical aspect to the activity of companies that develop and sell these products. The natural evolution of a product of this type results in predictable stimulus associated with technological innovation in computing platforms, such as the increasing use of mobile platforms, with the improvement of existing features and introduction of new characteristics. It also incorporates less predictable stimuli, like changes in business models resulting from changes in service provision paradigms, such as migrating to cloud model.

In this context, the implications for information security management of the gradually introduced changes are not always clear, and it's common that development teams are not prepared to deal with the diversity of new risks that come with these changes.

Accordingly, and in view of combating the possible failures mentioned above, the aim of this project is to make a software security analysis for PRIMAVERA BSS 's cloud products, identifying potential risks and security threats and presenting viable solutions to mitigate them.

RESUMO

A gestão do ciclo de vida de produtos informáticos é um processo contínuo que, nos casos de maior sucesso, se prolonga por períodos que ultrapassam duas décadas e se transforma num aspeto crítico à atividade das empresas que desenvolvem e comercializam esses produtos. A evolução natural de um produto deste tipo resulta de estímulos previsíveis associados à inovação tecnológica nas plataformas computacionais, como a cada vez maior utilização de plataformas móveis, à melhoria de funcionalidades existentes e à introdução de características novas. Incorpora também estímulos menos previsíveis, tais como alterações nos modelos de negócio resultantes de mudanças nos paradigmas de prestação de serviços, como a migração para o modelo *Cloud*.

Neste contexto, as implicações para a gestão da segurança da informação das alterações gradualmente introduzidas nem sempre são claras, e é comum as equipas de desenvolvimento não estarem preparadas para lidar com a diversidade de novos riscos que surgem com estas mudanças.

Deste modo, e na perspetiva de combater as possíveis falhas supra referidas, pretende-se com este projeto efetuar uma análise de segurança de produtos de software para a *Cloud* da PRIMAVERA BSS , identificando potenciais riscos e ameaças de segurança e apresentando soluções viáveis para os mitigar.

CONTEÚDO

1 INTRODUÇÃO 2
1.1 Contextualização 2
1.1.1 Cloud Computing - Definição 2
1.1.2 Cloud Computing - História 3
1.1.3 A Cloud no contexto empresarial 4
1.1.4 Segurança na Cloud 5
1.2 Contexto e enquadramento do trabalho 9
1.3 Motivação 9
1.3.1 Desafios de segurança na migração para a Cloud 9
1.3.2 Necessidade da análise de segurança 10
1.4 Objetivos do Trabalho 11
1.4.1 Levantamento dos requisitos funcionais e de segurança 11
1.4.2 Identificação de cenários potencialmente comprometedores 11
1.4.3 Classificação dos riscos 12
1.4.4 Identificação de mecanismos de proteção 12
1.4.5 Avaliação das soluções apresentadas 12
1.5 Organização do documento 13
2 ESTADO DA ARTE E TRABALHO RELACIONADO 14
2.1 Proteção de dados 14
2.2 Cloud Computing 15
2.3 Análise de Segurança 17
2.4 Análise de Segurança no contexto da Cloud 18
2.5 Computação móvel 19
3 DESENVOLVIMENTO DO TRABALHO 20
3.1 Definição e caraterização do sistema 20
3.1.1 Elevation Mobile 20
3.1.2 Elevation Framework 23
3.2 Caraterização e delimitação do problema 24
3.2.1 Infraestrutura envolvente 24
3.2.2 Delimitação do problema 27
3.3 Ambições ao nível da segurança - Utilizador 29
3.4 Modelos de dados e necessidades de proteção 29
3.4.1 Componentes 30

3.5 Fluxos de dados 32
3.6 Perfis de atacantes 38
3.7 Ameaças e proteção necessária 39
3.7.1 Objetivos de segurança 39
3.7.2 Ameaças 40
3.7.3 Classificação de ameaças 42
3.8 Propostas de soluções 46
3.8.1 Auditoria/Logging - Repúdio 46
3.8.2 Autenticação - Ataques por força bruta/dicionário 48
3.8.3 Autenticação - Roubo de credenciais 50
3.8.4 Configuração - Acesso indevido a ficheiros de configuração/Recuperação de segredos em texto limpo 51
3.8.5 Autorização - Elevação de privilégios 52
3.8.6 Comunicação - Protocolos de segurança nas ligações aos *endpoints* 54
3.8.7 Dados sensíveis - Acesso a dados críticos armazenados 57
3.8.8 Gestão de sessões - Incapacidade da terminação completa de sessão 61
4 CONCLUSÕES E TRABALHO FUTURO 63
4.1 Conclusões 63
4.2 Trabalho Futuro 64

A MATERIAL DE SUPORTE - ANEXOS 69
A.1 NIST SP 800-118 Draft – Aplicação no caso de estudo 69
A.2 Análise Endpoints 72
A.3 NIST Guidelines for TLS implementatios – SP 800-52 83

LISTA DE FIGURAS

Figura 1	*Elevation Mobile* - capturas de ecrã	21
Figura 2	*Elevation Framework* - arquitetura e componentes	24
Figura 3	Infraestrutura - arquitetura e componentes	25
Figura 4	*Elevation Mobile - system-of-interest*	28
Figura 5	*Fluxos de dados* - Operação de Login	36
Figura 6	*Fluxos de dados* - Operação de acesso aos Módulos e Notícias	37
Figura 7	Ameaças por categoria e necessidades de proteção	43
Figura 8	Matriz de risco	44
Figura 9	Classificação de ameaças	45
Figura 10	Matriz de risco - classificação das ameaças	46

ACRÓNIMOS

AD	Active Directory. 26
AMD	Advanced Micro Devices. 4
AWS	Amazon Web Services. 4, 16
CC	Common Criteria for Information Technology Security Evaluation. 17
CSA	Cloud Security Alliance. 3, 5, 16, 18
DDoS	Distributed Denial of Service. 7
EC2	Amazon's Elastic Compute Cloud. 7, 18
ENISA	European Network and Information Security Agency. 16, 18
GFS	Google File System. 16
HDFS	Hadoop Distributed File System. 16
IaaS	Infrastructure as a Service. 3
IIS	Internet Information Services. 26
NIST	National Institute of Standards and Technology. 2, 3, 8, 16–18
OMS	Operations Management Suite. 26
PaaS	Platform as a Service. 3
PDF	Portable Document Format. 22
SaaS	Software as a Service. 3
SOAP	Simple Object Access Protocol. 18

TDE Transparent Data Encryption. 57–59

XSS Cross-site scripting. 18

1

INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO

1.1.1 *Cloud Computing - Definição*

Em Outubro de 2009, numa apresentação por Peter Mell e Tim Grance do National Institute of Standards and Technology (NIST), designada *"Effectively and Securely Using the Cloud Computing Paradigm"*, o termo *cloud computing* foi definido como:

> *Cloud computing é um modelo que possibilita acesso, de modo conveniente e sob demanda, a um conjunto de recursos computacionais configuráveis (por exemplo, redes servidores, armazenamento, aplicações e serviços) que podem ser rapidamente adquiridos e oferecidos com o mínimo esforço do consumidor ou interação com o prestador de serviços.*

Mais tarde, esta definição viria a ser incluída no relatório técnico oficial (Mell and Grance, 2011) apresentado pelo NIST relativo à definição deste modelo computacional. Nesse mesmo documento é apresentado o modelo segundo cinco características essenciais, três modelos de serviço e quatro modelos de distribuição.

No que diz respeito às principais características da *cloud computing* destacam-se o auto-serviço a pedido e a rápida elasticidade, por se considerarem, de entre as várias características, como aquelas que se revelam mais apetecíveis na ótica do utilizador. A primeira, desde logo, por pôr do lado deste o mínimo de esforço e interação humana com o provedor de serviços. A segunda, pela facilidade e rapidez que fornece na forma como é feita a alocação de mais ou menos recursos de acordo com as necessidades atuais de cada aplicação/serviço do utilizador. Principalmente esta última característica, a elasticidade, é vista de forma bastante positiva pelas organizações, pois resolve um dos principais problemas das empresas: o estudo e previsão do investimento necessários em maquinaria para fornecer o serviço desejado. Esta característica possibilita, dessa forma, que sejam efetuados uma alocação e investimento progressivos de recursos, tendo em conta aquilo que são as necessidades do serviço com o decorrer do tempo, estratégia que facilita também a forma como podem

ser encarados os picos de carga e períodos críticos de utilização. Do mesmo modo, este modelo computacional possibilita a utilização de um fornecimento vulgarmente designado como *pay-as-you-go* que permite que se utilizem e paguem apenas os recursos que estão a ser efetivamente utilizados.

A Cloud Security Alliance (CSA) considera também importante, e acrescenta a estas características, a *multi-tenacy* (Cloud Security Alliance, 2011). De modo simplificado, *multi-tenacy* implica a utilização (ou aplicação) dos mesmos recursos por múltiplos utilizadores, que podem, ou não, pertencer à mesma organização. No contexto do fornecimento de serviços na *cloud*, esta característica implica que sejam, por exemplo, necessários mecanismos de isolamento, segmentação, políticas de acesso e níveis de serviço. Estes mecanismos são essenciais num contexto de múltiplos clientes de forma a garantir que os dados de cada um deles se encontram isolados dos restantes e, do mesmo modo, problemas e falhas num deles não têm efeito nos restantes.

Em relação ao tipo de serviço oferecido na *cloud* são normalmente definidos três tipos - Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) - naquele que é habitualmente designado como o modelo SPI, de acordo com as iniciais de cada tipo. Estes variam, essencialmente, no que é oferecido ao utilizador final em cada um dos casos. No caso do SaaS, é permitido ao consumidor o uso de aplicações a correr numa infraestrutura *cloud*. Já no PaaS, é oferecido ao utilizador a plataforma em si, para que este consiga pôr a correr as suas próprias aplicações na infraestrutura. No IaaS são oferecidas ao consumidor capacidades de processamento, armazenamento, e outros recursos computacionais, sendo este capaz de correr *software* arbitrário que pode incluir tanto sistemas operativos como aplicações (Mell and Grance, 2011).

Dentro dos modelos de distribuição a definição do NIST aponta, desta vez, quatro tipos, dependentes das características destes: *cloud* privada se a infraestrutura for destinada ao uso exclusivo de uma organização contemplando vários utilizadores; *cloud* de comunidade se for destinada a um conjunto de organizações com preocupações comuns; *cloud* pública se a infraestrutura estiver disponível ao uso público generalizado; e *cloud* híbrida se for a combinação de duas ou mais infraestruturas *cloud* distintas. Uma previsão da Gartner Inc. aponta para que, em finais de 2017, aproximadamente metade das grandes empresas possuam estratégias de *cloud* híbridas (Gartner Inc., 2013).

1.1.2 *Cloud Computing - História*

Analisando o que foi o passado histórico da computação, a *cloud computing* pode ser considerada uma evolução de tecnologias ou ideias já existentes. De acordo com Bruce Schneier, especialista em segurança, e pondo de parte toda a expansão recente à volta da *cloud computing*, este modelo não é mais do que uma versão moderna do já conhecido modelo

de *time-sharing*, introduzido nos anos 60 por estudantes e professores da Universidade de Darthmouth. Este modelo foi na altura, apesar de tudo, posto de parte devido à coincidente evolução dos computadores pessoais (Schneier, Bruce, 2009).

Na verdade, já o antigo modelo *time-sharing* tinha objetivos semelhantes aos da *cloud computing* entre eles o facto da procura de redução de custos através do uso partilhado de recursos, numa era onde tanto a manutenção como os próprios computadores possuíam custos elevados. Como tal, as grandes instituições sentiam necessidade de permitir que os diferentes utilizadores se ligassem através de terminais próprios aos computadores centrais pois estes ofereciam melhores condições de processamento. Desta forma, através do modelo de *time-sharing* era possível a um grupo de utilizadores utilizar o tempo de espera de outros tornando eficiente este processo de partilha de tempo entre eles.

Segundo Margaret Lewis, diretora de marketing da Advanced Micro Devices (AMD), a visão de J.C.R. Licklider, nos anos 60, de uma rede global que permitiria a toda a gente do mundo interligar-se e aceder a programas e informação de qualquer site, a partir de qualquer local, é muito parecida com o que hoje em dia chamamos de *cloud computing* (Mohamed, Arif, 2009).

De modo geral, a proliferação do uso dos computadores pessoais, através do aumento da sua capacidade na presença de preços acessíveis, permitiu a expansão em massa do número de utilizadores dos computadores. Aliando-se esse facto às necessidades que levaram à ligação destes computadores entre si, dando origem a uma rede global que hoje conhecemos como a Internet, assim como à exploração do conceito de *grid computing* (computação em grelha), que permitia a partilha de capacidade de computação e armazenamento em sistemas distribuídos, estavam reunidas as condições que levariam à expansão do conceito de *cloud computing*.

O seu rápido crescimento e mais recente mediatismo, com a ajuda do impulso dado por serviços que se tornaram bastante populares (como é o caso dos Amazon Web Services (AWS) e do *Microsoft Azure*) levaram ao conceito revolucionário da forma como o conhecemos nos dias de hoje e permitiram que este atingisse e ocupasse uma respeitável e repleta de importância posição naquilo que é o mundo informático e da computação.

1.1.3 *A Cloud no contexto empresarial*

Através da já analisada expansão do conceito de *cloud computing* de modo generalizado no mundo informático também as empresas sentiram necessidade de oferecer os seus serviços através deste novo modelo, procurando que a aposta numa opção inovadora lhes trouxesse outro tipo de benefícios e abrisse novas áreas de exploração do seu trabalho. Desta forma surgiu a vontade por parte de algumas empresas de migrar os serviços oferecidos de modo tradicional, *on-premises*, para a *cloud*.

Esta migração traz, desde logo, benefícios claros para as empresas como a agilidade do negócio, a disponibilidade dos dados, colaboração e a redução de custos (Cloud Security Alliance, 2015). Ter os recursos disponíveis assim que necessário resulta numa melhoria significativa em termos de tempo de entrega de um produto ou projeto, potenciando uma entrada competitiva no mercado e reduzindo de forma clara o tempo despendido em produção, o que se reflete na agilidade do negócio. Por outro lado, esta mesma agilidade, através do produção de projetos mais eficientes, permite que os funcionários se dediquem a outras atividades e necessidades relevantes do projeto às quais, caso contrário, não teriam disponibilidade para se dedicar. Também pelos mesmos motivos de utilização deste novo modelo, e tal como referido anteriormente, o uso da virtualização e da alocação progressiva dos recursos necessários revela-se bastante positiva em termos monetários, pois resolve problemas de investimento prévio em *hardware*, manutenção deste e respetivo estudo e previsões de utilização, e também porque permite que apenas sejam cobrados os recursos efetivamente utilizados. Por outro lado, e constituindo outra importante vantagem deste modelo no contexto empresarial, está a disponibilidade dos dados e aplicações hospedados na *cloud*. Esta característica abre novas possibilidades de negócio, pois os serviços possuem a facilidade de poderem ser utilizados *online*. Face ao exposto, torna-se possível a expansão do negócio resultando numa capacidade de consumo da informação através de diferentes dispositivos em simultâneo, como é o caso de muitas empresas que recentemente procuram obter vantagens através da criação e fornecimento de serviços para aplicações móveis.

Porém, nem todas as características da *cloud computing* constituem vantagens no que toca à sua utilização em contexto empresarial, sendo que esta migração se debate com uma série de desafios que devem ser tidos em conta. Estes desafios e problemas concretos da migração do modelo tradicional para o modelo *cloud* serão alvo de uma abordagem mais aprofundada em secções seguintes deste documento por constituírem parte do trabalho e objetivos desta dissertação.

1.1.4 *Segurança na Cloud*

Apesar do rápido crescimento e evolução deste modelo de computação, é necessário ter em conta os aspetos menos favoráveis à sua adoção e que, por isso, devem ser alvo de análise para que se consigam balancear tanto os seus benefícios como as suas contrapartidas. Deste modo, reside no fator segurança um aspeto importante a ter em conta quando é feito o planeamento para a implementação de soluções de software para a *cloud*. Segundo um estudo recente, realizado pela CSA em janeiro de 2015 (Cloud Security Alliance, 2015), numa amostra heterogénea de empresas dos diferentes continentes, 73% dos principais desafios à adoção de projetos na *cloud* dizem respeito a problemas relativos à segurança da

informação. Estes resultados são por si só elucidativos da necessidade e importância da segurança neste contexto.

No entanto, são vários os motivos que dão origem às existentes dificuldades presentes aquando do fornecimento de garantias de segurança neste contexto. Tal como referido na secção inicial, o facto de haver ainda uma relativa indecisão no que diz respeito à definição concreta do que é a *cloud*, assim como uma dificuldade em estabelecer quais os limites desta e atingir uma visão comum e global dos utilizadores que não seja vaga e dispersa, constitui, desde logo, uma dificuldade na garantia de segurança deste modelo. Este revela-se um ponto fulcral, na medida em que, não havendo certeza acerca da definição e limites do modelo, se torna difícil perceber o que são as necessidades efetivas de segurança.

Outro fator relevante é a falta de caracterização e conhecimento intrínseco do funcionamento do modelo e das soluções de software para a *cloud*. Isto reflete-se a vários níveis, entre eles ao nível da segurança aplicacional, levando a casos em que muitas das vezes as próprias empresas não têm bem noção do que está a ser feito para garantir a segurança dos seus dados. Por outro lado o facto do modo de fornecimento dos serviços se basear no uso da *Internet* levanta todo um leque de possíveis ataques, vulnerabilidades e novas necessidades de segurança relativos à própria *Internet*. O mesmo acontece devido à utilização partilhada dos recursos computacionais, que dá origem a problemas de segurança novos, com os quais as soluções tradicionais anteriores não tinham de se preocupar. Toda esta alteração dos modelos e paradigmas de prestação de serviços leva a que as diferentes necessidades de segurança tenham de ser repensadas. Isto acontece principalmente porque nas soluções anteriores podem ter sido estabelecidas suposições e assunções para os problemas "clássicos", que podem já não ser válidas ou fazer sentido no novo modelo.

Outro dos grandes desafios prende-se com o facto da ausência ou ambiguidade na legislação que contemple os problemas e necessidades deste modelo, principalmente no que diz respeito à responsabilização, o que torna também difícil o alcance das garantias de segurança necessárias. Uma vez que para uma abordagem clara da segurança de um sistema é necessário estabelecer e definir responsabilidades para os diferentes intervenientes, este aspeto reveste-se de difícil concretização quando procurado no âmbito de um sistema de software para a *cloud*.

O mais recente estudo do LinkedIn acerca da segurança na *cloud*, realizado sobre uma amostra de mais de 250 000 membros da comunidade de segurança da informação do site, é claro no que diz respeito às necessidades de segurança no modelo *cloud* (LinkedIn, 2015). Para além de colocar também a segurança como a principal barreira à adoção da *cloud*, são ainda definidas as principais ameaças de segurança na *cloud* pública. Entre estas lideram o acesso não autorizado e *hijacking* de contas, com 63% e 61% respetivamente, seguidos dos ataques de utilizadores internos (*insiders*) maliciosos.

Na verdade, a história conta com vários episódios de ataques e procura de vulnerabilidades nos serviços *cloud*, os quais, mesmo que efetuados indiretamente sobre os serviços prestados pelo *cloud provider*, podem pôr em causa a credibilidade deste e gerar um sentimento de desconfiança nos utilizadores do serviço. Um exemplo deste cenário aconteceu em 2014, quando foram descobertas vulnerabilidades no *software* distribuído do motor de busca *Elasticsearch*. Através desta descoberta os atacantes procuraram atingir as instâncias dos serviços *cloud* da Amazon (Amazon's Elastic Compute Cloud (EC2)) que possuíam versões deste software instalado, fazendo com que através dessa vulnerabilidade fosse possível instalar malware de negação de serviço (Distributed Denial of Service (DDoS)) nos servidores (Computer World, 2014).

Da mesma forma os grandes serviços *cloud* estão periodicamente a ser notificados, e em certos casos até alvo de ações policiais, devido a alguns dos seus utilizadores usufruírem do serviço para cometer fraudes e ações maliciosas, muitas das vezes afetando outros utilizadores inocentes que por atos de terceiros podem ser prejudicados pessoalmente ou até mesmo nos seus negócios. Todas estas situações, resultantes da utilização partilhada de recursos que a *cloud* promove, geram uma situação constante de desconfiança, quer nos provedores de serviço quer no próprio modelo em si. No entanto, a esperança reside no facto destes acontecimentos levarem também à procura de novas soluções para os problemas existentes e promoverem a procura ou reestruturação de disposições legais que possam ser aplicáveis neste contexto.

Assim sendo, é importante ter noção das áreas mais relevantes sobre as quais as políticas de segurança de um sistema de software para a *cloud* devem incidir, entre elas (Krutz and Vines, 2010):

- Controlo de acesso - de forma a garantir políticas específicas relativas ao tipo de acesso de cada entidade a partes do sistema ou a dados;
- Proteção de dados - de forma a proteger informação crítica do sistema, garantindo a sua confidencialidade e integridade;
- Identificação e autenticação - de modo a obter garantias de conhecimento das diferentes entidades;
- Segurança da comunicação - para proteger as trocas de dados nas comunicações internas e externas ao sistema, garantindo a integridade da informação;
- Responsabilização - de modo a garantir a responsabilização no manuseamento da informação.

Em junho de 2001 (com posterior revisão em 2004), o NIST publica um documento (Stoneburner et al., 2004) onde apresenta uma lista de 33 princípios de segurança que vão desde a fase de *design* de uma aplicação até à continuidade e fim do sistema.

Alguns desses princípios revelam-se fulcrais e aplicam-se no contexto da segurança na *cloud*, entre eles (Krutz and Vines, 2010):

- Princípio 1: estabelecer uma política de segurança sólida que sirva de base ao projeto;
- Princípio 2: a segurança deve ser tratada como uma parte integrante da globalidade do sistema;
- Princípio 3: delinear de forma clara os limites de segurança físicos e lógicos que se encontram sob controlo das políticas de segurança associadas;
- Princípio 6: assumir que as entidades externas ao sistema não são seguras;
- Princípio 7: identificar potenciais *trade-offs* entre a redução do risco e o aumento de custos e decréscimos noutros aspetos da eficiência operacional;
- Princípio 16: implementar um modelo de segurança por camadas (*layered security*) garantido que não existem pontos únicos de falha/vulnerabilidade;
- Princípio 20: isolar os sistemas de acesso público dos recursos críticos como dados, processos, etc;
- Princípio 21: uso de mecanismos de barreira para separar os recursos computacionais das infraestruturas de rede;
- Princípio 25: minimizar os elementos do sistema nos quais deve ser depositada confiança;
- Princípio 26: implementar o princípio do mínimo privilégio;
- Princípio 32: autenticar os utilizadores e processos de modo a garantir que se tomem decisões corretas em termos de controlo de acesso tanto dentro do sistema como fora deste;
- Princípio 33: usar identidades únicas de modo a garantir a responsabilização.

A aplicação deste género de medidas tem sido procurada por diversos agentes, entre eles os desenvolvedores de soluções de *software* para a *cloud*, pelas necessidades que produtos deste tipo trazem a si associadas. Alguns dos problemas de segurança encontrados em soluções deste tipo serão alvo de abordagem nas secções seguintes.

1.2 CONTEXTO E ENQUADRAMENTO DO TRABALHO

Tendo em conta o ciclo de vida longo de um produto de software, e de acordo com os benefícios e desafios já referidos inerentes a uma inovação tecnológica como a migração para a *cloud*, é comum que essas mudanças obriguem também a mudanças na forma como questões como a segurança são vistas no seio de uma organização.

Este trabalho enquadra-se no ambiente tecnológico da PRIMAVERA BSS , no qual os seus produtos têm passado por esta inovação tecnológica, introduzida pelo recurso a um ambiente *cloud* e uma procura pelo aspeto "mobilidade"das suas aplicações, permitindo a utilização dessas soluções numa gama mais variada de dispositivos, entre eles, os dispositivos móveis.

No universo PRIMAVERA, a alteração para este novo paradigma revelou-se bastante positiva, através de um acréscimo significativo do número de utilizadores dos serviços, de um aumento dos rendimentos provenientes desses serviços e pela criação de novos produtos, alguns deles contemplando as novas plataformas suportadas, como é o caso do ELEVATION MOBILE.

Este trabalho visa, portanto, a análise do ponto de vista da segurança de um conjunto situações provenientes dessas mudanças relativamente às soluções de *software* para a *cloud* da PRIMAVERA BSS .

1.3 MOTIVAÇÃO

1.3.1 *Desafios de segurança na migração para a Cloud*

Tal como referido nas secções anteriores, este trabalho só faz sentido se visar responder a problemas concretos existentes no contexto das soluções de software para a *cloud* existentes. Desde logo, a própria migração para a *cloud* que, como já abordado, se tem verificado nos últimos anos em ambiente empresarial, traz, por si só, alguns desafios. Aliados ao facto desta mudança alterar quase que por completo a forma como as empresas olham para a implementação dos seus sistemas, é de extrema importância que esta migração seja analisada, planeada e realizada de forma bastante ponderada. As problemáticas vistas em termos de segurança, o caso novo dos problemas de *reputation fate-sharing* (onde o mau comportamento de um utilizador pode afetar a reputação dos serviços *cloud* como um todo), o mau planeamento na migração dos serviços/plataforma, traduzem-se, de modo geral, na introdução de novos inconvenientes que advêm desta mudança e que deixam de pé atrás os possíveis novos utilizadores deste mais recente modelo.

Um denominador comum entre vários dos diversos problemas apontados reside no facto da necessária confiança no provedor de serviços *cloud*. Sendo que muitas das medidas

alternativas propostas partem do pressuposto que o provedor de serviço é de confiança, quando se lida com informação crítica e dados sensíveis, aliado na maioria dos casos em situações onde o próprio potencial de negócio reside na proteção dessa informação, esse é um luxo a que muitos dos utilizadores (singulares ou coletivos) não se podem dar.

No caso concreto da Primavera bss a migração do seu *software* para novos modelos também se revelou um desafio. A pouca clareza no que diz respeito, principalmente, à gestão da segurança da informação, deu origem a novas situações que a própria empresa e as equipas de desenvolvimento dos produtos em questão identificaram como pontos críticos a abordar. Posto isto, todos estes desafios deram origem à necessidade de uma análise de segurança que se revelasse eficaz no que é a atualidade dos produtos Primavera bss .

1.3.2 *Necessidade da análise de segurança*

De acordo com os problemas identificados nas secções anteriores, torna-se claro que uma análise de segurança se reveste de uma importância extrema quando elaborada sobre software desenhado para suportar serviços na *cloud*. Através da alteração dos paradigmas de prestação de serviços e dos modelos de implementação das soluções de software é bastante comum que, dada a vida longa de um produto de software, esta alteração das regras do produto se reflita numa mudança de abordagem com as quais a organização terá que lidar. Desta forma, e tal como referido anteriormente, o facto de se proceder à alteração do *software* tradicional para um modelo *cloud* pode resultar em novos desafios e situações que podem não se ter verificado, quer por não existirem no modelo anterior, quer por os pressupostos tidos em conta anteriormente poderem já não ser válidos ou não fazerem sentido no novo modelo.

Como tal, e de acordo com essa mudança na abordagem, torna-se necessário um estudo de levantamento de requisitos e necessidades de segurança que depois possa ser entregue às equipas de desenvolvimento, para que estas possam ter informação sobre quais as implementações necessárias no modelo atual, alterações ao sistema, e uma sensibilidade reforçada para os diversos fatores de segurança no geral. O facto da análise de segurança ser realizada por alguém fora da equipa de desenvolvimento também se revela um ponto benéfico, uma vez que esse facto promove a reflexão sobre novas situações relativamente às quais a equipa pode ainda não ter debatido e permite o foco da análise em aspetos diferentes dos tradicionais abordados pela equipa de desenvolvimento.

1.4 OBJETIVOS DO TRABALHO

De acordo com o estabelecido numa primeira fase através do plano de trabalhos, o objetivo principal desta dissertação passa por efetuar uma análise de segurança de produtos de software para a *cloud* da PRIMAVERA BSS . Como tal, uma análise deste tipo compreende várias fases, cada uma, por si só, contendo também um objetivo em particular.

1.4.1 *Levantamento dos requisitos funcionais e de segurança*

Procurando atingir o objetivo principal de encontrar soluções para possíveis problemas de segurança existentes no contexto destas aplicações, toda esta análise passa por uma primeira fase de levantamento dos requisitos funcionais e de segurança do sistema. Pretende-se com esta fase inicial perceber quais as necessidades de segurança que devem ser garantidas de acordo com o conhecimento adquirido do sistema, de forma a que estas necessidades possam servir de base aos campos de análise e possível intervenção das fases seguintes.

Passa, portanto, por esta fase e pela concretização deste objetivo a definição dos limites do sistema, onde devem ser estabelecidas as fronteiras que o delimitam. É também procurada a caracterização do sistema e das suas principais operações.

Esta é uma componente crucial uma vez que o conhecimento da globalidade do sistema e das suas fronteiras é de extrema importância quando se pretende procurar mecanismos de proteção e analisar os níveis de segurança deste.

1.4.2 *Identificação de cenários potencialmente comprometedores*

Depois de efetuado o levantamento dos requisitos funcionais e de segurança do sistema o próximo objetivo do trabalho passa pela identificação de cenários potencialmente comprometedores e que possam pôr em causa o seu funcionamento e segurança. Desta forma, o trabalho que procura a concretização deste objetivo passa pela identificação de riscos - através da conjugação das vulnerabilidades do sistema com ameaças que os explorem - assim como da sua origem, de modo a perceber em que cenários ocorrem e que condições os originam e impulsionam.

Este objetivo vai de encontro às necessidades das fases seguintes do trabalho, às quais deve servir de suporte, uma vez que indica, de certa forma, onde devem ser aplicadas as principais necessidades do sistema de modo a prevenir ou garantir uma menor ocorrência dos cenários indesejados.

1.4.3 *Classificação dos riscos*

Conhecidos os cenários e condições que motivam eventos ou situações indesejáveis no contexto do sistema, o próximo objetivo passa pela classificação dos riscos, ameaças e vulnerabilidades associadas a estes.

Assim, as necessidades para a concretização deste objetivo passam pela sua classificação de acordo com, essencialmente, dois fatores: o impacto/criticidade e a probabilidade de ocorrência. Definidos os níveis de cada ameaça ou vulnerabilidade para cada um dos fatores estes são cruzados de forma a procurar obter um grau geral de gravidade desses riscos e vulnerabilidades. Este novo grau vai permitir estabelecer níveis de prioridade para cada uma das ameaças, que vão posteriormente ser utilizados na fase de tomada de decisões de acordo com o risco e nas decisões sobre quais as necessidades e áreas de intervenção mais urgentes, sendo que devem ser estas alvo de maior preocupação e sobre as quais os mecanismos de proteção devem inicialmente incidir.

1.4.4 *Identificação de mecanismos de proteção*

Como fase seguinte do trabalho o objetivo passa agora pela identificação dos mecanismos de proteção necessários para mitigar os problemas encontrados nas tarefas anteriores. Esta fase revela-se também bastante importante porque resulta de um estudo que deve ser ponderado entre aquilo que queremos ver protegido e quais são as necessidades do sistema, nomeadamente em termos de performance, facilidade de utilização, entre outros. É então necessário definir o tipo de proteção a utilizar assim como os mecanismos que melhor respondem a essas necessidades.

A concretização deste objetivo é também importante para perceber de que forma deve ser feita a implementação destes mecanismos de modo a fazerem sentido no contexto global do sistema e não irem contra os requisitos previamente estabelecidos deste.

1.4.5 *Avaliação das soluções apresentadas*

Por fim, efetuado o estudo dos mecanismos de proteção necessários como soluções para os problemas apresentados, resta atestar a sua conformidade e avaliar o seu desempenho. Deste modo, este objetivo passa pela justificação da necessidade do uso dos mecanismos apresentados, assim como a obtenção de garantias no que diz respeito à capacidade destes em atingir os níveis de segurança pretendidos. Esta informação torna-se bastante relevante uma vez que permite perceber se os mecanismos de proteção apresentados são suficientes para tornar o sistema seguro, na medida do que foi proposto alcançar-se nas fases anteriores.

É também importante perceber, e devem ser feitos esforços nesse sentido, se com o decorrer do tempo a solução apresentada não afeta o funcionamento do sistema e se os níveis de segurança são mantidos através dos pressupostos definidos ou se será necessário proceder a alterações, pelo que esta avaliação não deve ser colocada em segundo plano.

1.5 ORGANIZAÇÃO DO DOCUMENTO

Este documento está organizado em quatro principais capítulos, cada um contendo subcapítulos, e uma secção de anexos onde se encontra informação adicional de forma a complementar o trabalho desenvolvido.

Desta forma no primeiro capítulo, o capítulo introdutório, são abordados aspetos relativos ao contexto do trabalho e ao seu enquadramento, assim como a motivação subjacente à sua realização e os objetivos associados.

Por sua vez, o capítulo dois, compreende todo o estado da arte e trabalho relacionado. Neste capítulo são abordados os principais temas relacionados com o trabalho em questão assim como o levantamento de trabalho realizado anteriormente nessas mesmas áreas.

O capítulo três, engloba todas as componentes relacionadas com o desenvolvimento do trabalho. É neste capítulo que pode ser encontrada toda a parte de definição e caraterização do sistema em estudo, o levantamento das ambições e necessidades de segurança, a definição de perfis de atacantes, assim como a identificação de ameaças e riscos e as respetivas propostas de soluções.

Por último, o capítulo quatro compreende todas as questões relacionadas com as conclusões do trabalho desenvolvido bem como propostas para trabalho que possa vir a ser realizado futuramente.

Na secção de anexos encontram-se informações abordadas ao longo do trabalho que pela sua extensão, e de forma a não prejudicar a leitura global da dissertação, apesar de citadas nos respetivos capítulos, foram movidas para o final do documento.

2

ESTADO DA ARTE E TRABALHO RELACIONADO

2.1 PROTEÇÃO DE DADOS

A cada vez maior quantidade de informação processada, produzida e recolhida pelos sistemas de *software* atuais, contribui de forma significativa para o aparecimento de novos cenários, assim como técnicas de processamento, armazenamento e comunicação bastante distintas daquelas utilizadas em ambientes anteriores à era que se vive atualmente no mundo informático. Um dos cenários emergentes é a *cloud computing*. O aparecimento destes novos cenários trouxe benefícios claros no que diz respeito à disponibilidade da informação, bem como à facilidade com que promove um acesso universal a esta. Contudo, como já foi analisado em secções anteriores, traz também enormes desafios, da mesma forma que introduz novos riscos. É, de facto, difícil garantir nas infraestruturas utilizadas hoje em dia que os dados sensíveis estão efetivamente protegidos e que é mantido controlo sobre quem pode, ou não, aceder a esses mesmos dados quando estes são armazenados em servidores externos (NIS Platform, Working Group 3, 2014).

Uma das áreas mais relevantes no contexto do aparecimento destes novos cenários é, sem dúvida, a proteção de dados sensíveis, mais ainda quando analisada sobre um sistema de *software* de uma empresa, em que a base do seu negócio e muita da confiança depositada pelos seus clientes, residem nas garantias de proteção deste tipo de informação. Uma vez que muitas das empresas que oferecem serviços *cloud* estão dependentes de infraestruturas de outros fornecedores, e que por esse motivo não possuem acesso físico a estas, a questão da segurança da informação reveste-se de especial importância pois dependem das garantias oferecidas por esses mesmos fornecedores (Zhang et al., 2010).

No que diz respeito ao estado atual desta área, as maiores preocupações prendem-se principalmente com as novas abordagens de armazenamento de dados sensíveis em servidores externos, contrariamente ao que acontecia em cenários e modelos anteriores. É, desta forma, de essencial importância, garantir o chamado *CIA triad*, do inglês *confidentiality*, *integrity* e *availability*, respetivamente, confidencialidade, integridade e disponibilidade. A confidencialidade com o objetivo principal de promover a proteção do conteúdo dos dados,

garantindo que estes apenas se encontram acessíveis a quem possui acesso autorizado, a integridade de modo a garantir que a informação não foi alvo de modificações não autorizadas e a disponibilidade promovendo o acesso aos dados no máximo período de tempo possível.

Tipicamente, os dados seriam cifrados para armazenamento em servidores externos. No entanto, apesar de atualmente as técnicas criptográficas gozarem de um custo limitado e de uma complexidade computacional acessível, a cifragem afeta por outro lado a performance global do sistema aquando do consumo dos dados e revela novos desafios, como a gestão de chaves criptográficas. Outros métodos, como a fragmentação da informação, estão também a ser investigados em alternativa à cifragem, de modo a proteger a confidencialidade dos dados. Por outro lado, tem sido também alvo de estudo, no que diz respeito à proteção de dados, o uso de criptografia homomórfica - sistemas utilizados para a realização de operações sobre informação cifrada sem ser necessário proceder à sua decifragem (Tebaa et al., 2012). Apesar desta ser entendida como uma solução viável, e que vai de encontro às necessidades atuais, ainda não se encontra disponível na prática nos principais sistemas *cloud*. Por esse motivo, e tentando combater o problema da privacidade dos dados em ambientes *cloud*, têm também sido procuradas novas soluções arquiteturais e propostas novas arquiteturas *cloud*, como é o caso da *MyCloud* (Li et al., 2013).

Os desafios de investigação neste campo da proteção de dados passam, portanto, por aspetos como as técnicas utilizadas para garantir a confidencialidade, integridade e disponibilidade da própria informação de modo a proteger dados sensíveis, a definição e implementação de medidas de controlo de acesso a dados e as necessidades de proteção da integridade nas computações efetuadas. Em ambiente industrial a estes desafios somase também a procura da independência, uma vez que neste momento o comportamento dos funcionários e colaboradores nas empresas tem um peso significativo na proteção da informação. A procura de novas soluções criptográficas e arquiteturais para a proteção da informação, de como são exemplo os trabalhos apresentados anteriormente, reflete também a necessidade deste tipo de proteção nos sistemas modernos.

2.2 CLOUD COMPUTING

Como já foi referido ao longo deste documento, a alteração dos modelos computacionais das empresas de uma abordagem *on-premises* para a *cloud* gera toda uma nova visão do produto em si e do seu funcionamento. Assim, os mecanismos e medidas de segurança associadas estão também a passar por esta migração, ficando muitas das vezes a segurança longe das mãos do utilizador. De uma forma geral, o que está no cerne da segurança da *cloud* é o controlo sobre os diferentes *assets* (sistemas, redes, dados e aplicações) (NIS

Platform, Working Group 3, 2014). Deste modo, quando um utilizador malicioso consegue controlar esses *assets* cria ameaças e riscos associados a esses *assets*. Contudo, a *cloud computing* torna ainda difícil ter as garantias e exercer esse controlo, sendo que o que se procura constantemente nesta matéria são ferramentas que facilitem este processo.

Em relação ao estado atual na área, uma parte significativa da investigação visa tornar a *cloud* mais transparente, responsável e que inspire confiança (NIS Platform, Working Group 3, 2014), através de:

- *Logs* e gestão de eventos na *cloud*;
- Monitorização, auditoria, gestão de incidentes;
- Segurança da informação: confidencialidade, integridade e disponibilidade;
- Redução de ameaças internas;
- Ferramentas de análise forense para a *cloud*;
- Tecnologias de controlo de acesso;
- Continuidade do negócio e recuperação de falhas.

Uma questão relevante que tem sido alvo do estudo da *cloud computing* prende-se também com a arquitetura, desenho e manutenção dos *data centers* que servem de apoio a toda a infraestrutura, onde se procura ao mínimo comprometer as aplicações no que diz respeito à escalabilidade e resiliência, ao mesmo tempo que são tidas em conta propriedades benéficas como a facilidade de migração entre VM's, compatibilidade e eficiência energética (Buyya et al., 2010). Da mesma forma, a questão do armazenamento de dados na *cloud* tem sido alvo de investigação em campos como a segurança da informação, onde se propõe, por exemplo, protocolos para provar a correção da cifragem dos ficheiros *at-rest* (Van Dijk et al., 2012), ou o armazenamento eficiente de dados em servidores externos, de onde são exemplo a implementação de sistemas de ficheiros distribuídos como o Google File System (GFS) (Ghemawat et al., 2003) e o Hadoop Distributed File System (HDFS) (Shvachko et al., 2010).

Devido à existência de grandes produtos comerciais *cloud* para utilização pública, como os AWS, a plataforma *Azure* da *Microsoft* ou o *Google App Engine*, muitas das questões de segurança na *cloud* têm sido estudadas através da análise destas soluções.

Os principais desafios residem na tentativa de tornar a *cloud computing* mais segura e de fornecer mais controlo aos utilizadores e proprietários dos dados e aplicações. Dessa forma, o trabalho recente nesta área passa muitas das vezes por projetos que procuram soluções que resolvam ou facilitem o combate a estes desafios.

Organizações como a CSA, o NIST e a European Network and Information Security Agency (ENISA) focam também grande parte do seu trabalho na elaboração de documentos

onde apresentam *frameworks*, linhas orientadoras e melhores práticas no que diz respeito à segurança da *cloud* e dos seus serviços.

2.3 Análise de Segurança

A crescente necessidade de atenção aos fatores de segurança no contexto de um produto de software faz com que a elaboração de análises de segurança se torne, cada vez mais, numa componente importante quando vista sob o leque de operações de uma organização. No entanto, este não é um conceito novo, sendo que nos anos 80 já eram investigados resultados na área (Baskerville, Richard, 1993). Através do uso de *checklists* tornou-se possível verificar se os diferentes elementos de segurança estavam a ser utilizados e, com base nisso, tecer considerações acerca da segurança global dos sistemas. Contudo, a necessidade de análises que permitissem comparações entre sistemas distintos e que pudessem servir de base a novas análises deu origem à criação de metodologias propostas em *standards*, como é o caso do Common Criteria for Information Technology Security Evaluation (CC) (Common Criteria, 2012) ou o do NIST.

No caso do CC essa procura é assumida logo à partida, definindo-se nos próprios documentos como um *standard* que permite a comparabilidade entre avaliações de segurança independentes. Este objetivo é alcançado através do fornecimento de um conjunto de requisitos de segurança para as funcionalidades dos sistemas e medidas de segurança a aplicar nesses mesmos produtos. A flexibilidade que os *standards* procuram também fornecer permite que estes possam ser aplicados a uma grande gama de produtos e que possam servir de guia na elaboração de análises de segurança em diversos contextos. O resultado final expectável de uma análise de segurança com base nestes *standards* consiste num documento completo acerca das necessidades de segurança do produto em análise, assim como um conjunto de medidas a ser alcançadas para a obtenção dos níveis de segurança esperados.

Para além do facto destes documentos facilitarem a ajuda na especificação dos requisitos e medidas de segurança (através do estabelecimento de diferentes fases com objetivos concretos) estes *standards* tornam-se bastante procurados pelas garantias fornecidas de condutas rigorosas e padronizadas nos diversos processos de uma análise de segurança.

Desta forma, para este trabalho, revelou-se importante obter uma metodologia de análise faseada que permitisse seguir um conjunto de processos para a obtenção dos resultados finais. Assim, os objetivos referidos anteriormente constituem também essa mesma divisão em fases que englobam a definição do sistema e levantamento de requisitos de segurança, a identificação de cenários potencialmente comprometedores, a classificação dos riscos e a identificação e avaliação de mecanismos de proteção. Relativamente à identificação de cenários e ameaças, e uma vez que o trabalho se enquadra num contexto de ambiente empresarial, faz sentido que seja efetuada uma recolha em bruto de um conjunto de ameaças

que, após investigação, discussão e elaboração de questões para levantamento entre os diferentes *stakeholders* permita perceber quais se refletem no produto em estudo e de que forma as podemos classificar.

2.4 Análise de Segurança no contexto da Cloud

Com a introdução de novos modelos computacionais, de como é exemplo a *cloud computing*, também o campo das análises de segurança tem sofrido alterações para garantir o acompanhamento das novas soluções.

Desta forma, para visar a realização de análises que possam continuar válidas nestes novos contextos, têm surgido mudanças que visam adaptar as necessidades de segurança aos novos problemas resultantes da introdução destes modelos. No caso concreto da *cloud computing*, problemas como o armazenamento externo da informação ou os desafios introduzidos pela virtualização, resultam em novos cenários que necessitam, igualmente, de incidência por parte de uma análise de segurança.

Assim, muitos dos desafios e trabalho relacionado na área passam pela procura de fornecimento de soluções que sirvam de base para uma análise de segurança suficientemente robusta que permita a utilização desta nos contextos recentemente emergentes. Esta procura traduz-se, numa já abordada, adaptação de trabalho e *standards* anteriores, assim como num possível surgimento de novos *standards* e soluções.

Entidades como a ENISA, a CSA e o NIST produzem constantemente revisões ou documentos adaptados a estas novas necessidades, de forma a garantir que as práticas e soluções apresentadas possam continuar a ser consideradas.

No que diz respeito a trabalho relacionado na área foram já efetuadas análises de segurança semelhantes, principalmente sobre grandes plataformas *cloud* como é o caso da *cloud* pública da Amazon e de *software* para *clouds* privadas, como o *Eucalyptus* (Nurmi et al., 2009).

Em 2009, Gruschka e Lo Iacono (Gruschka and Iacono, 2009) investigaram a segurança de interfaces de controlo baseadas no protocolo Simple Object Access Protocol (SOAP), tais como as de serviços como a EC2. Mais tarde, em 2011, esse trabalho viria a ser estendido, através de uma análise de segurança, levada a cabo por Somorovsky et al. (Somorovsky et al., 2011), a qual permitiu obter resultados alarmantes no que diz respeito à segurança destas interfaces sobre ataques de Cross-site scripting (XSS)).

Também um estudo conduzido por Modi et al. (Modi et al., 2012) permitiu perceber as dificuldades de segurança e propor soluções, para as diferentes camadas da *cloud computing*. Por outro lado Dan Boneh et al., no seu trabalho de análise de alojamento de serviços numa *cloud* não confiável, apresentam algumas caraterísticas desejáveis de um serviço *cloud*

seguro, entre elas a segurança contra uma *cloud* maliciosa, contra clientes maliciosos, contra *cloud* e clientes maliciosos e eficiência (Boneh et al., 2015).

Muitas das análises de segurança focadas especialmente em aspetos da *cloud*, centram-se, portanto, em questões como a a segurança da informação em *clouds* públicas, a segurança das interfaces de gestão e controlo, assim como a exploração de ataques *web*, e de problemas resultantes da virtualização e/ou localização de máquinas virtuais.

2.5 COMPUTAÇÃO MÓVEL

Com o crescimento da *mobile computing*, os serviços *web* estão cada vez mais a chegar aos utilizadores através de aplicações móveis, de forma contrária ao que acontecia anteriormente, através dos *web browsers*. Como tal, e uma vez que comparativamente aos *web browsers* as aplicações móveis não fornecem as mesmas garantias de segurança, uma grande parte do estudo na segurança das novas tecnologias foca-se também na segurança da *mobile computing*.

De forma mais representativa deste cenário, maioritariamente devido ao facto de ser um sistema operativo *open-source*, encontra-se o estudo e análise do *Android*, o sistema operativo móvel da *Google*. Algum do trabalho na área foca-se essencialmente no estudo do nível de segurança do *Android* baseado em permissões (Felt et al., 2012), riscos associados às permissões requeridas por determinadas aplicações (Davi et al., 2010), assim como soluções que procuram fornecer ao utilizador controlo e visibilidade acerca da utilização de dados confidenciais por parte de outras aplicações, de como é exemplo o *TaintDroid* (Enck et al., 2014).

Por outro lado, os protocolos criptográficos ou de comunicação utilizados pelos sistemas operativos móveis e aplicações também são alvo de estudo. Fahl, Harbach et al. procederam à análise de um conjunto vasto de aplicações *Android* procurando potenciais problemas de segurança relativamente ao uso do protocolo SSL/TLS por parte destas aplicações (Fahl et al., 2012). Noutros trabalhos na área são também analisados problemas de serviços concretos, como os serviços de *push-messaging* (Li et al., 2014), e de que forma estão presentes riscos de segurança na sua implementação.

Deste modo, relativamente a esta área, o trabalho encontra-se frequentemente na investigação de problemas conhecidos noutros ambientes computacionais aplicados à *mobile computing*, assim como no estudo de questões específicas dos principais sistemas operativos móveis ou dos níveis de segurança oferecidos por aplicações móveis populares.

3

DESENVOLVIMENTO DO TRABALHO

3.1 DEFINIÇÃO E CARATERIZAÇÃO DO SISTEMA

De modo a revelar-se eficaz, uma análise de segurança compreende uma primeira fase de definição e caraterização do sistema em estudo, de modo a tornar claro o alvo sobre o qual recai essa mesma análise. Dessa forma, este capítulo, tem o intuito de proceder a essa definição, sendo nele apresentado o Elevation Mobile, as suas principais características, objetivo, funcionamento chave e enquadramento no ambiente tecnológico Primavera.

3.1.1 *Elevation Mobile*

Embora os resultados e métodos da análise de segurança efetuada possam ser estendidos a diversos produtos de software para a *cloud*, este trabalho foca-se essencialmente na análise de um produto específico do universo Primavera, o Elevation Mobile.

O Elevation Mobile é uma solução que permite aceder a informação de negócio e a determinadas funcionalidades do ERP Primavera a partir de dispositivos móveis, possibilitando assim a tomada de decisão célere e a execução de tarefas relevantes num contexto de mobilidade.

Esta aplicação, disponível em qualquer dispositivo com sistema operativo *iOS*, *Android* ou *Windows Phone*, providencia igualmente acesso permanente às notícias mais importantes do ecossistema Primavera.

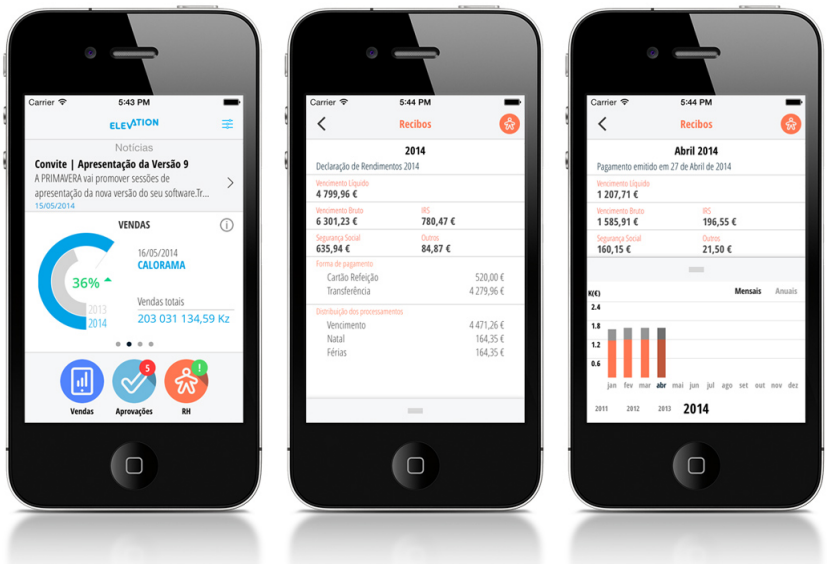


Figura 1.: *Elevation Mobile* - capturas de ecrã

O Elevation Mobile inclui, no momento da presente análise, quatro módulos - Vendas, Aprovações, Recursos Humanos e Clientes - estando previsto que ao longo do tempo sejam acrescentados novos módulos e funcionalidades a esta solução.

O módulo de Vendas, integrando com o ERP Primavera instalado na máquina do Cliente, possibilita a consulta de informação atualizada das suas vendas, apresentando-as em diversos formatos (como gráficos e tabelas) e agrupadas relativamente a diferentes parâmetros como períodos temporais, zona geográfica, por cliente ou vendedor. Dentro dos períodos temporais é permitido ao utilizador definir os intervalos desejados, podendo a informação ser visualizada por semana, mês, trimestre ou em valores acumulados desde o início do ano, sempre em comparação com o período homólogo do ano anterior.

Uma vez que esta solução permite a criação de diversos perfis de utilização, torna-se possível a definição de diferentes níveis de acesso à informação de vendas refletindo dessa forma as permissões necessárias a cada utilizador no acesso a esses dados. É possível também através da aplicação proceder ao envio direto das várias tabelas ou gráficos por email ou em formato PDF, facilitando a partilha de informação com os restantes membros da organização.

O módulo de vendas inclui os seguintes indicadores:

- Vendas totais (por empresa ou por grupo de empresas agregado);
- Vendas semanais, mensais, trimestrais, ou acumuladas desde o início do ano;
- Vendas por zona geográfica (top 5);
- Vendas por cliente (top 5);

- Vendas por vendedor (top 5).

No módulo de aprovações torna-se possível gerir, igualmente a partir do dispositivo móvel, a aprovação dos documentos Internos e de Compras criados no ERP PRIMAVERA, de acordo com os *workflows* e parâmetros pré-definidos. Esta funcionalidade permite ao Cliente aprovar documentos pendentes, visualizando toda a informação relevante do documento, verificar o estado das aprovações criadas, delegar aprovações para outros membros da organização e ainda consultar o histórico das aprovações realizadas.

O módulo de Recursos Humanos por sua vez permite, entre outras funcionalidades, a visualização do estado do processamento do recibo do mês/ano corrente e o respetivo valor, tal como a validação do estado de processamento, formas de pagamento, o valor líquido recebido, etc. A informação é facilmente acedida, organizada em gráficos, podendo proceder-se ao download/envio por email do recibo de vencimento detalhado em formato Portable Document Format (PDF). Este módulo torna assim possível a navegação e formatação da informação relativa a vencimentos num contexto fácil e de mobilidade.

No módulo de Clientes pode ser consultada informação em tempo real sobre qualquer cliente relacionado com a empresa de forma rápida e cómoda, através do *smartphone*. Neste módulo podem ser consultadas as seguintes informações relativas a Clientes:

- Consultar os dados de contacto do Cliente que constam da Ficha de Cliente do ERP Primavera (moradas, telefones, contactos associados via CRM);
- Iniciar navegação até à morada do cliente recorrendo ao software de navegação instalado no dispositivo (por exemplo, Google Maps);
- Aceder a Dados de Vendas (totais, trimestrais, mensais ou semanais);
- Consultar condições de pagamento por cliente e prazo médio de recebimento;
- Aceder a informação de Encomendas Pendentes;
- Consultar valores da Conta Corrente (valores expirados há mais de um mês, no último mês e por expirar);
- Consultar a atividade recente do Cliente (acesso às últimas Faturas, Encomendas, Pagamentos, etc);
- Aceder a relatórios de Análise de Risco (disponível mediante subscrição de serviço associado).

Esta solução revela-se vantajosa devido à presença de diversas caraterísticas que passam pela mobilidade total - permitindo que se possa aceder à informação e processos mais relevantes do ERP Primavera a partir de um dispositivo móvel com acesso à Internet; pelo

facto de ser multiplataforma e multilingue - esta solução está disponível para várias plataformas móveis (*iOS*, *Android* e *Windows Phone*) e em várias línguas (português, inglês e castelhano) abrangendo desta forma uma vasta gama de utilizadores; pela concentração de todos os processos num só lugar - o Elevation Mobile permite reunir numa única aplicação todas as operações do ERP Primavera que são relevantes num contexto de mobilidade; pela maior produtividade e controlo sobre o negócio - a integração desta solução com o ERP Primavera permite aos gestores aceder a dados atualizados, seguindo constantemente a performance da sua organização e facilitando a tomada de decisão em tempo real; e pelo acesso por parte dos colaboradores das diversas áreas da empresa, permitindo também o agilizar dos processos e o aumento dos seus índices de produtividade.

Assim como as restantes soluções para a *cloud*, o Elevation Mobile compreende componentes da *framework* Elevation, cuja definição e caraterização se apresentam de seguida.

3.1.2 *Elevation Framework*

Tal como referido anteriormente, os *CloudServices* são desenhados e implementados sobre e através da combinação de componentes da *Elevation Framework*. Esta *framework* surgiu como consequência da procura da Primavera bss na inovação e consequente migração das soluções tradicionais para a *cloud*. Deste modo, a *Elevation Framework* resulta num conjunto de componentes reutilizáveis nos diferentes produtos oferecidos, facto este que se reflete positivamente em termos de modularidade, facilidade de crescimento, melhoria das soluções atuais e oferta de novos produtos.

De uma forma bastante generalizada e esquemática, encontra-se na Figura 2 o conjunto de componentes integrantes da *Elevation Framework*.

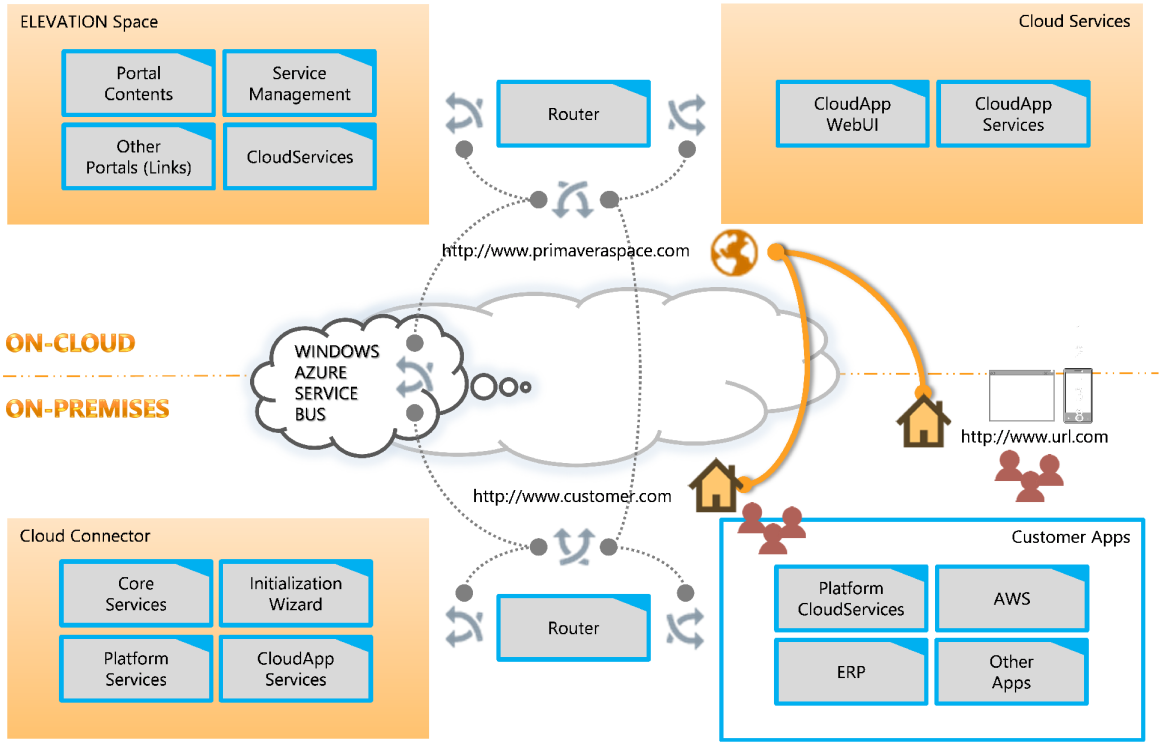


Figura 2.: *Elevation Framework* - arquitetura e componentes

A *framework Elevation* reflete desta forma um conjunto de componentes que foram surgindo ao longo do tempo, baseados nas necessidades das novas soluções oferecidas no universo PRIMAVERA e traduz um ambiente de progressiva evolução procurando facilitar o que é esperado do futuro: a criação de novas soluções de *software* para a *cloud* e a complementação das soluções atuais com novos módulos e funcionalidades.

3.2 CARATERIZAÇÃO E DELIMITAÇÃO DO PROBLEMA

3.2.1 *Infraestrutura envolvente*

Uma vez que são claras as necessidades de escalabilidade e disponibilidade na prestação dos serviços e produtos da PRIMAVERA BSS , a arquitetura e a própria infraestrutura que serve de suporte a esses serviços procura refletir isso mesmo. Toda a gestão e manutenção da infraestrutura de suporte aos *CloudServices* é da responsabilidade da equipa de *Cloud Management*, sendo que apenas os colaboradores pertencentes a esta equipa possuem acesso interno aos diferentes componentes. Um esquema simplificado da sua arquitetura pode ser

encontrado na Figura 3.

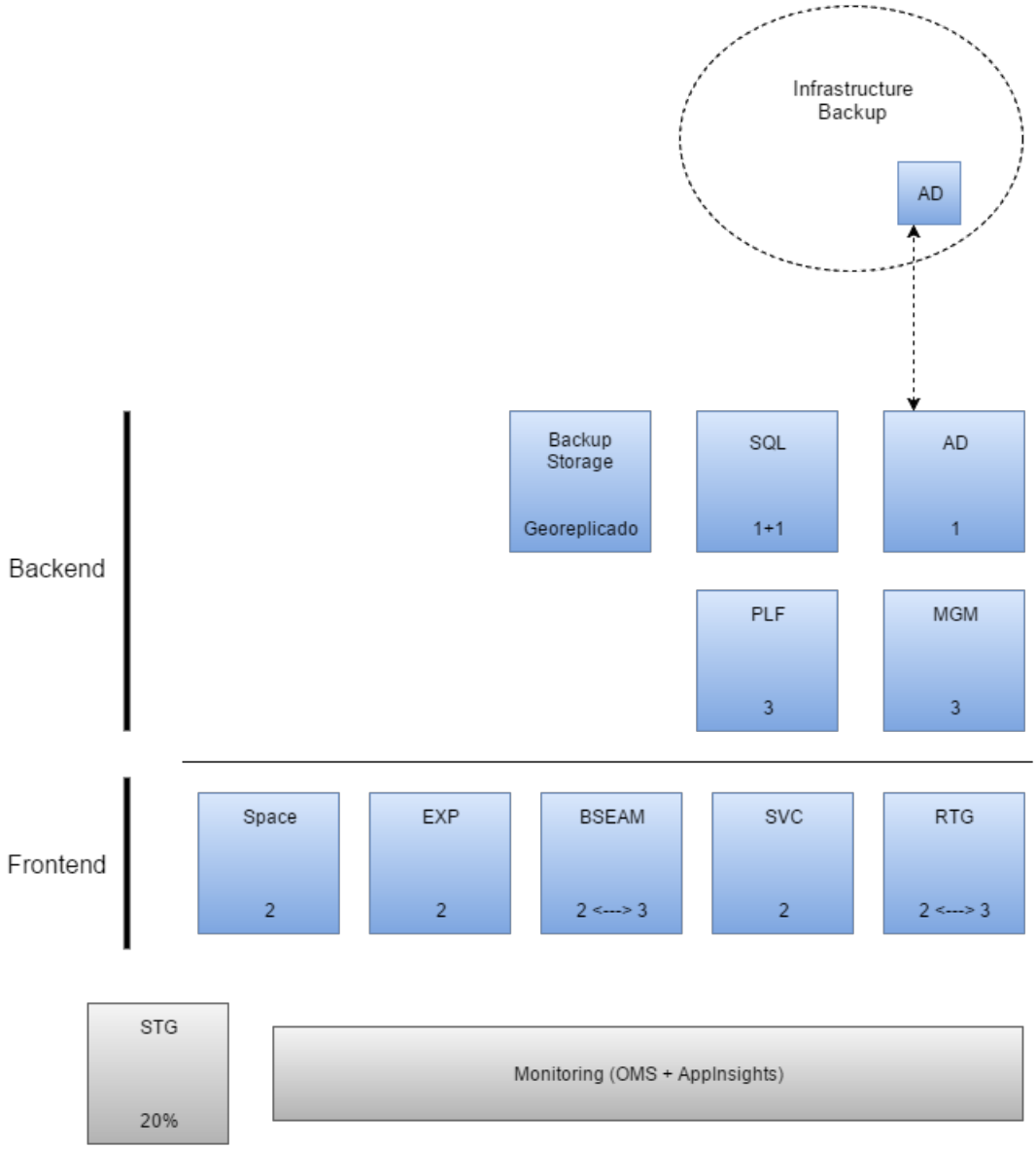


Figura 3.: Infraestrutura - arquitetura e componentes

O centro de toda a infraestrutura passa por um componente designado MGM, onde se encontra o *ServiceManagement*. É esta peça que a generalidade das ligações vai alcançar e onde estão disponíveis os serviços de gestão de serviços, subscrições, aprovisionamento, ligação a componentes *on-premises*, entre outros. É constituída por três servidores que vão ser utilizados mediante políticas de balanceamento de carga disponíveis através do uso de um *load balancer*. Existe também uma peça que funciona como *router*, designada no esquema como RTG. Esta possui funções de comunicação e serve de porta de entrada

para a maioria dos serviços, distribuindo as comunicações para os *endpoints* dos respetivos serviços. Outro *cluster* presente na infraestrutura, designado por PLF, possui os serviços de plataforma, os *workers* (componentes com capacidade de execução automática de tarefas) e serviços de *cache*. É neste componente que são, quando necessários, publicados os *workers*. Já a *cache* está disponível a todas as aplicações de várias formas. Tem o principal objetivo de armazenar as sessões (por exemplo, do Internet Information Services (IIS)), permitindo que quando os pedidos de um utilizador a um serviço sejam redirecionados ou balanceados para outro servidor, o estado e sessão possam ser mantidos, não se perdendo o contexto atual da aplicação. Este é um *cluster* de alta disponibilidade e, através da partilha de memória entre os três servidores de *cache* disponíveis, tanto as falhas como os momentos de manutenção não refletem um impacto negativo no sistema.

Também presente neste ambiente estão as máquinas do SQL, com discos replicados de modo a promover a redundância dos dados e permitir a resolução rápida em cenários de falha, e de serviços de diretoria (Active Directory (AD)), assim como a *storage* para *backups*, que se encontra georeplicada de modo a garantir que a informação relevante não é perdida. Afastado deste contexto encontra-se a a infraestrutura que contém as aplicações para AD, o serviço de *backup*, entre outros. Todo o funcionamento destes componentes é transparente para o Cliente, sendo que os serviços e aplicações por ele utilizados não interagem diretamente com estes componentes.

Os *clusters* que suportam as aplicações encontram-se no diagrama com as designações de SVC para o caso dos *CloudServices*, BSEAM onde estão publicadas as aplicações *Business Suite*, *Elevation Starter Easy* e *EAM*, EXP relativamente ao *Elevation Express* e Space no caso do portal *Primavera Space*. Todos estes *clusters* possuem um número mínimo de dois servidores, no entanto tanto no BSEAM como no RTG estão presentes mecanismos de *auto-scaling*, entre duas a três máquinas, de forma a suportar picos horários de carga.

Paralelamente a estes componentes existe também uma camada de monitorização que recorre a soluções como o Operations Management Suite (OMS) e *AppInsights* para a monitorização da infraestrutura e das aplicações, respetivamente. Para além da monitorização, esta camada também fornece à equipa de *Cloud Management* os mecanismos de alarmística e *auto-healing*. Em concreto, o OMS procura detetar problemas de sobreaquecimento, memória, utilização do SQL, entre outros, respondendo a incidentes através, por exemplo, de medidas de *auto-scaling*. Já o *AppInsights* procede à monitorização ao nível aplicacional, enviando periodicamente relatórios com comparações e medições temporais de pedidos às aplicações.

Existe também uma réplica completa de toda a infraestrutura no ambiente de *staging*, possuindo esta o mínimo indispensável no que respeita ao número de recursos e sendo os custos desta cerca de 20% dos custos da infraestrutura em ambiente produtivo. É também através desta plataforma que a equipa de *CloudManagement* ensaia as migrações de produ-

tos entre os diferentes ambientes. Esta infraestrutura, tal como a produtiva apenas está acessível à equipa de *CloudManagement*, com a diferença de em *staging* os desenvolvedores possuírem permissões de acesso (visualização) ao SQL.

3.2.2 *Delimitação do problema*

Após a fase de definição do sistema e precedendo o levantamento das necessidades de proteção concretas, faz sentido delimitar o problema em causa de modo a tornar claras as fronteiras que limitam o sistema que será alvo de análise. Uma vez que o termo *sistema* abrange todo um conjunto de componentes e interligações entre eles de uma forma global, é comum ser utilizado o termo *system-of-interest* como forma de definir o conjunto que será alvo de atenção especial num determinado contexto. No enquadramento da análise de segurança que se efetua, o *system-of-interest* será portanto definido como o conjunto de componentes, interligações e ambiente, que possuem interesse no caso concreto em estudo e que, associado a um ambiente relevante do ponto de vista da segurança, será alvo da análise.

Desta forma, isolando o sistema do contexto anterior da infraestrutura e *framework*, o conjunto de componentes e interligações entre estes que será motivo de análise, encontra-se representado na Figura 4.

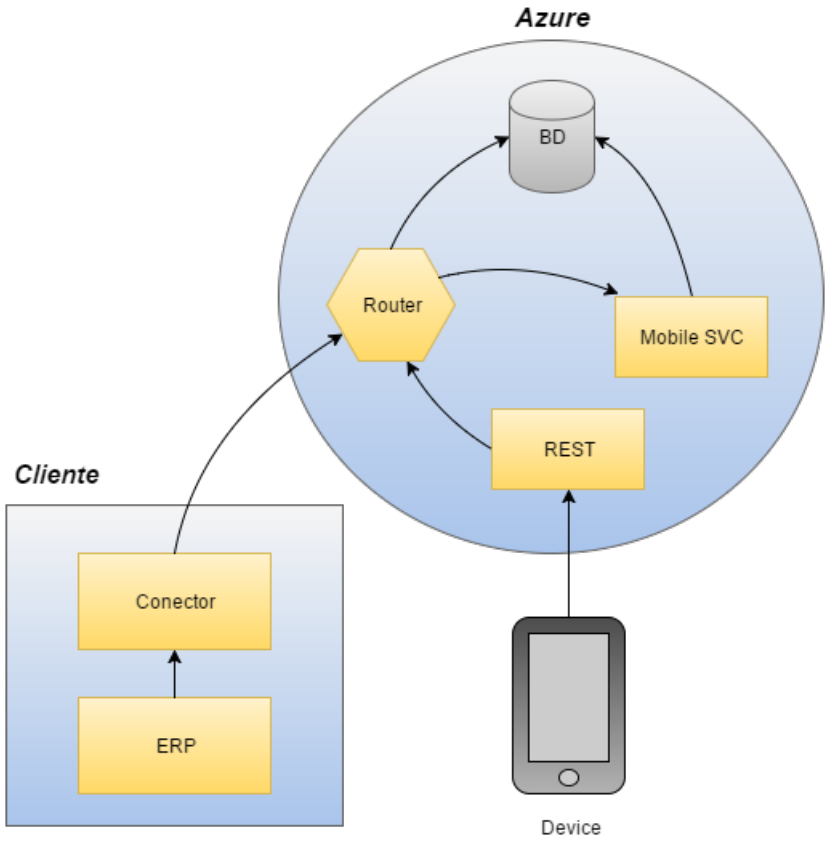


Figura 4.: *Elevation Mobile - system-of-interest*

Uma vez que este sistema se revela bastante completo no que diz respeito à diversidade de componentes, possuindo componentes em diferentes contextos (*cloud* e *on-premises*), com diferentes níveis de importância, níveis de criticidade e necessidades de proteção, a análise de segurança terá de ser cuidada e efetuada de forma a abranger inicialmente cada componente (ou conjunto de componentes) individualmente e, após isso e tendo em conta os resultados obtidos, proceder à sua associação no sistema como um todo.

Também por esse motivo, como pressupostos desta análise encontram-se as garantias de segurança oferecidas pelos serviços *cloud* sub-contratados, de que são exemplo as garantias oferecidas pelo *Microsoft Azure*, relativamente à proteção e confiabilidade das máquinas onde os serviços PRIMAVERA são alojados, às questões legais relativas à localização geográfica da informação nos *data centers* da *Microsoft*, entre outros. Por outro lado, do ponto de vista organizacional, são também assumidos como pressupostos, fatores como a idoneidade da componente humana que integra o sistema, assim como a segurança física das instalações e a correção das implementações do produto.

Deste modo, serão efetuadas nas secções seguintes o levantamento das necessidades de proteção nos diferentes contextos, assim como a definição dos modelos e fluxos de dados para os componentes e ligações estabelecidos.

3.3 Ambições ao nível da segurança - Utilizador

O utilizador típico do Elevation Mobile consiste naquele que procura essencialmente obter informação do seu negócio de forma rápida e num contexto de mobilidade, utilizando o seu dispositivo móvel para essa tarefa, o qual espera não ter sido comprometido. A informação de acesso disponível por parte dos utilizadores passa por dados do ERP, informação de vendas, clientes, dados de recursos humanos, entre outros. Desta forma, e uma vez que o utilizador deposita confiança nesses mesmos dados, ele espera obter garantias de proteção dessa informação, tais como a confidencialidade, a integridade e disponibilidade. O acesso ao serviço é feito através da introdução das credenciais do utilizador, as quais acredita que sejam apenas do seu próprio conhecimento. De modo a garantir proteção no que diz respeito a intrusões no sistema através do uso das suas credenciais, espera conseguir obter informação de acessos com sucesso à sua conta e tentativas falhadas. No que diz respeito à comunicação com a aplicação, o utilizador acredita que está a comunicar com os *endpoints* corretos e que a segurança destes não foi comprometida. Espera que a comunicação entre o seu dispositivo e os componentes do sistema seja segura, promovendo a segurança da informação. O utilizador espera também que caso a segurança física do seu dispositivo seja comprometida, isso afete o mínimo possível a sua segurança, a segurança do sistema e a segurança da informação. Tendo noção da construção da solução num ambiente *cloud* este espera também que a presença de informação de outros utilizadores no mesmo ambiente não afete a confidencialidade dos dados da sua organização.

Como tal, podem assumir-se as seguintes categorias, como categorias que o utilizador valoriza e deposita interesse na sua segurança:

- Segurança da informação;
- Segurança na comunicação;
- Autenticação e identificação;
- Controlo de acesso;
- Segurança física do dispositivo.

3.4 Modelos de dados e necessidades de proteção

Consideradas as necessidades de proteção do ponto de vista do utilizador do sistema (que não possui conhecimento acerca do funcionamento interno deste), e de modo a obter uma análise completa para os diferentes intervenientes, torna-se também necessário analisar os componentes internos no que diz respeito aos modelos de dados e necessidades de

proteção para cada um destes. Desta forma, procura definir-se para cada um dos componentes do *system-of-interest* quais os tipos de dados com que lida e quais os seus níveis de criticidade, uma vez que essa informação se revela útil para perceber quais as necessidades de proteção e sobre que componentes incidem os aspetos mais críticos da análise.

3.4.1 *Componentes*

CloudConnector

O *CloudConnector* é um componente *on-premises* cuja função e objetivo se focam, essencialmente, em permitir o consumo de informação *on-premises* para a *cloud* e vice-versa. Assim, este componente faz com que seja possível, por exemplo, consumir e apresentar informação do ERP nos *CloudServices*.

Uma vez que este componente se encontra instalado do lado do Cliente, é importante ter em atenção aspetos como o acesso por parte de utilizadores maliciosos, pois não se encontra sobre as políticas de controlo de acesso de outros componentes que se situam do lado interno à Primavera.

Por outro lado a informação consumida por este componente é informação que carece de proteção, uma vez que é informação do negócio do Cliente. No entanto, este componente não procede ao armazenamento dessa informação pois constitui apenas o mecanismo de consumo e troca de informação entre os serviços na *cloud* e o ERP *on-premises*.

Dispositivo móvel

Este componente consiste no dispositivo através do qual o utilizador acede ao serviço e dá uso à aplicação. Desta forma, é através deste dispositivo que o utilizador efetua os pedidos à aplicação e obtém as respostas a esses mesmos pedidos, visualizando nele a informação desejada. A troca de pedidos/respostas é efetuada através de uma API REST que será também analisada. A comunicação deste dispositivo com os restantes componentes é estabelecida através do uso de protocolos de comunicação segura (TLS), embora não recorra a autenticação através de certificados do lado do cliente.

Uma vez que muita da proteção deste dispositivo reside em medidas a impor pelo próprio Cliente/utilizador, a análise a este componente não será tão aprofundada nesse aspeto e terá esse fator em conta.

REST

Esta camada é a responsável pela resolução dos pedidos e respostas enviados pelo utilizador aos serviços e vice-versa. É através desta API que os pedidos são mapeados para os respetivos métodos e posteriormente tratados. Deste modo, através deste componente passam todos os pedidos enviados pelo dispositivo móvel ao próprio serviço *mobile*, pelo que deve ser dada atenção a esse aspeto na avaliação das suas necessidades de segurança.

Router

Este componente tem como objetivo o reencaminhamento dos pedidos de *on-premises* para a *cloud* e vice-versa. É esta peça que permite o redirecionamento dos pedidos para os respetivos *endpoints*, como tal, todos os pedidos efetuados pelo utilizador através do dispositivo assim como aqueles efetuados, com recurso ao *CloudConnector*, à própria instalação *on-premises* do ERP, passam por este componente. Devem ser por isso salvaguardadas as questões de acesso a estes *router*, assim como ter em conta as necessidades de proteção dos dados que por ele passam.

Mobile SVC

Este componente reflete o próprio serviço oferecido e é o responsável pela resolução das operações relevantes da aplicação. Uma vez que é este componente que vai trabalhar os dados a fornecer pela aplicação e está encarregue das principais operações do sistema, reveste-se de especial importância pelo que devem também recair nele atenções especiais do ponto de vista de segurança.

Armazenamento de dados

Por fim, as bases de dados SQL são os componentes responsáveis pelo armazenamento dos dados dos diversos clientes. Uma vez que são estes dados que alimentam o sistema e sendo que o sucesso da aplicação reside essencialmente na segurança desta informação, também neste componente devem ser dadas garantias claras no que diz respeito à confidencialidade, integridade e disponibilidade da informação. De acordo com a importância deste componente, e tal como em outros semelhantes, o controlo de acesso a este também deve ser alvo de especial atenção.

3.5 FLUXOS DE DADOS

De forma a complementar a secção anterior, respeitante ao tipo de dados a lidar em cada componente, faz sentido analisar também os fluxos que estes dados atravessam na comunicação entre os diversos componentes do sistema. Como tal, esta secção procura analisar esses fluxos numa primeira fase tendo em conta os componentes envolvidos e posteriormente de acordo com as principais operações disponíveis no uso da aplicação.

Ligação ERP - *CloudConnector - Router*

Ativos:

- Dados do utilizador (comunicados do ERP para a cloud e vice-versa);
- Dados de autenticação (certificados utilizados);
- Canal de comunicação entre componentes;
- Conector (como componente, acesso físico através da máquina do Cliente).

Fluxos de informação:

- Dados comunicados do ERP para a cloud e vice-versa.

Necessidades de proteção:

- Confidencialidade, integridade e disponibilidade dos dados transmitidos;
- Segurança dos mecanismos de autenticação;
- Proteção do canal de comunicação de dados;
- Mecanismos de controlo de acesso ao conector.

Fluxo de informação - Dados do utilizador

Numa fase inicial, e no que diz respeito ao fluxo de dados entre estes componentes, começa por ser enviado um pedido de *Register* ao *ServiceManagement* para registar a instância do ERP *on-premises*, pedido esse enviado através do *router* por um *endpoint* autenticado por certificado. O certificado utilizado é o presente na máquina do Cliente aquando da instalação do *CloudConnector* (certificado distribuído por todos os clientes). O *ServiceManagement* responde ao pedido de *Register* com o ID da *Location* e o ID da Instância do ERP.

Idealmente a resposta seria um certificado gerado que identificasse unicamente o Cliente em questão, passando todos os pedidos (trocas de informação/dados do ERP para a *Cloud* e vice-versa) a ser identificados por esse certificado. Os diferentes canais de comunicação utilizados (*CloudConnector – Router*, *Router – ServiceManagement*) estão protegidos pelo uso do TLS promovendo a confidencialidade e integridade da informação em trânsito. A camada da mensagem nas mensagens transmitidas também se encontra protegida, tornando impossível a um componente intermédio (como o *Router*, que troca a camada do TLS para o reencaminhamento das mensagens para os endpoints do destino) interpretar o conteúdo da mensagem.

Necessidades de proteção

Confidencialidade e integridade dos dados transmitidos – promovida pelo uso do TLS na fase de transporte, não havendo armazenamento de dados críticos quer no *CloudConnector* quer no *Router*.

Segurança dos mecanismos de autenticação – através do uso atual dos certificados perde-se a noção em alguns pedidos do utilizador em causa.

Proteção do canal de comunicação de dados – promovida pelo uso do TLS.

Mecanismos de controlo de acesso ao conector – necessidade de garantias do acesso físico ao conector por parte de utilizadores maliciosos do lado do Cliente.

Ligação *Device* - REST - *Router*

Ativos:

- Dados do utilizador (enviados nos pedidos ou recebidos como resposta);
- Dados de autenticação e autorização (credenciais, tokens, ...);
- Canal de comunicação entre componentes;
- Acesso ao dispositivo.

Fluxos de informação:

- Pedidos à camada REST num dos sentidos, respostas recebidas no sentido inverso.

Necessidades de proteção:

- Confidencialidade e integridade dos dados transmitidos;

- Segurança dos mecanismos de autenticação e autorização;
- Proteção do canal de comunicação de dados.

Fluxo de informação

Uma vez que a comunicação nesta área do sistema depende das credenciais de autenticação, esta é precedida de uma operação de *Login*, onde depois do utilizador inserir as credencias na aplicação é enviado um pedido através da camada REST para se efetuar a sua validação (validação feita através do recurso a outro serviço, uma vez que as credenciais são as do *ELEVATION Space*). Validadas as credenciais é obtida uma resposta contento a chave do *token* de autenticação atribuído ao utilizador em questão. Os restantes pedidos são enviados aos diferentes módulos, contendo nos *headers* a chave do *token* atribuída, para posterior validação, verificação de autorizações, informação dos dados a recolher, entre outros. Nos canais de comunicação em causa é utilizado o TLS promovendo a confidencialidade e integridade da informação em trânsito. No caso dos pedidos ao módulo de Clientes, uma vez que este necessita de dados *on-premises*, é utilizado o *Azure Service Bus*, sendo a comunicação estabelecida com o certificado necessário e disponibilizado o certificado do cliente através do campo *Scoped Certificates*.

Necessidades de proteção

Confidencialidade e integridade dos dados transmitidos – promovido na camada de transporte pelo uso do TLS.

Segurança dos mecanismos de autenticação e autorização – proteção do armazenamento de *tokens* e da informação do *token* (credenciais, *role*, etc).

Proteção do canal de comunicação entre componentes – promovida pelo uso do TLS em todas as comunicações entre componentes.

Ligação *Router - Mobile SVC*

Ativos:

- Comunicação entre serviços;
- Dados transmitidos entre serviços.

Fluxos de informação:

- Dados comunicados entre serviços.

Necessidades de proteção:

- Confidencialidade e integridade dos dados transmitidos;
- Proteção do canal de comunicação entre componentes;
- Mecanismos de controlo de acesso aos diversos *endpoints*.

Ligação *Router/Mobile SVC - BD*

Ativos:

- Informação armazenada e em trânsito;
- Canal de comunicação entre componentes.

Fluxos de informação:

- Dados armazenados a ser comunicados.

Necessidades de proteção:

- Confidencialidade e integridade da informação armazenada;
- Confidencialidade e integridade da informação em trânsito;
- Proteção do canal de comunicação entre componentes.

Analisados os fluxos de dados entre os principais pares de componentes é também interessante que sejam revistos os tipos de dados transmitidos e quais os caminhos percorridos por estes nas principais operações que o Elevation Mobile permite realizar. De um modo geral, estas podem resumir-se a operações de autenticação e operações de acesso aos diferentes módulos. Assim, serão descritas as operações de *login*, *logout* e acesso aos módulos de clientes, recursos humanos, vendas, aprovações e notícias.

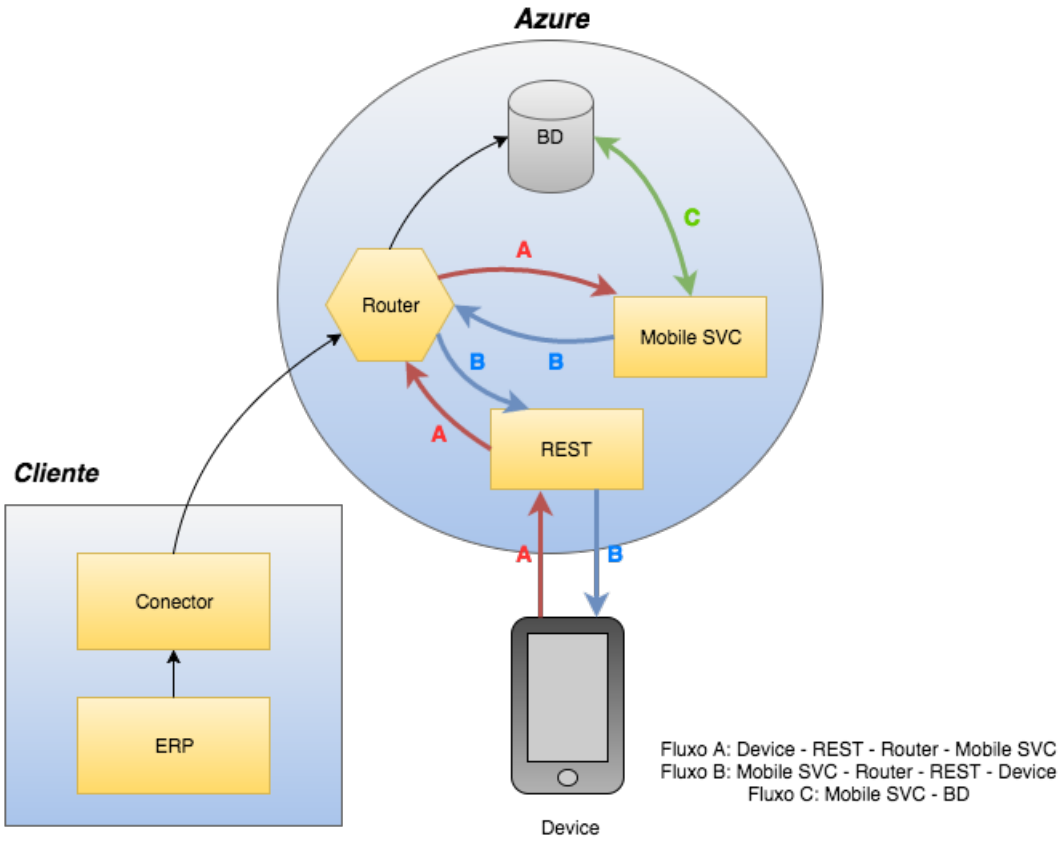


Figura 5.: *Fluxos de dados* - Operação de Login

Operação: Login

1. Efetua pedido de login ao serviço - Fluxo A
2. Apresenta página de login - Fluxo B
3. Utilizador insere e envia as credenciais - Fluxo A
4. Credenciais são validadas - *Primavera.IdentityService*, serviço PRIMAVERA externo ao sistema
5. Atribuído token ao utilizador contendo a sua informação - Mobile SVC
6. Pedido de apresentação do dashboard ao serviço - Fluxo A
7. Validação do token - Comparação com o token em cache (*Primavera.CachingService*)
8. Obtida informação (resumos) de acordo com o role do utilizador que fez o pedido - Fluxo C
9. Apresentado dashboard - Fluxo B

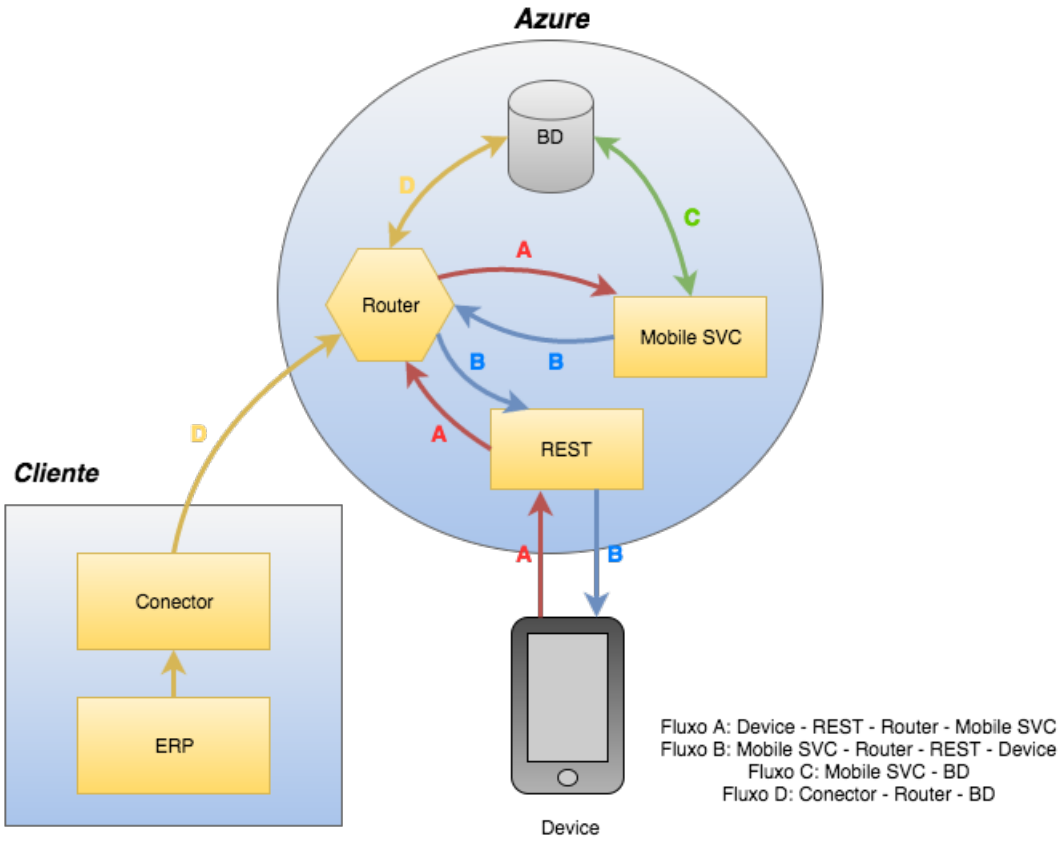


Figura 6.: *Fluxos de dados* - Operação de acesso aos Módulos e Notícias

Operação: Módulo de Vendas/Aprovações/RH

1. Pedido de entrada no módulo - Fluxo A
2. Validação do token - Comparação com o token em cache (*Primavera.CachingService*)
3. Obtenção dos dados armazenados (carregamento periódico de acordo com a utilização do serviço) e posterior tratamento - Fluxo C e D
4. Apresentação da informação - Fluxo B

Operação: Notícias

1. Pedido de entrada nas notícias - Fluxo A
2. Validação do token - Comparação com o token em cache (*Primavera.CachingService*)
3. Obtenção do conjunto de notícias - Serviço PRIMAVERA externo ao sistema, notícias do PRIMAVERA Space

4. Apresentação da informação - Fluxo B

Operação: Logout

1. Indica intenção do pedido de logout
    a) Não existe comunicação com o Mobile SVC neste pedido;
2. Token é invalidado do lado do cliente
3. Apresentado ecrã de login

Através da definição destes fluxos, quer em termos de operações quer entre pares de componentes, torna-se possível perceber quais os caminhos percorridos pela informação nos principais aspetos da execução da aplicação e consegue-se perceber de forma mais clara em que componentes residem as principais necessidades para proteção dos dados transmitidos. Assim, é possível ter uma perceção geral dos componentes em que devem recair as soluções que procuram mitigar os problemas encontrados, de que forma estas devem ser implementadas e quais os possíveis constrangimentos à sua adoção, aspetos que serão serão alvo de atenção nas secções seguintes da análise.

3.6 PERFIS DE ATACANTES

Uma vez que, na exploração de uma ameaça, se podem definir diversos tipos de origem, motivações e capacidades, é comum efetuar-se uma distinção entre os tipos de atacantes que procedem a essa exploração e que dão origem ao ataque, pois estes diferem também bastante entre si.

Desta forma, é usual a utilização do termo *threat agent* para definir pessoas individuais ou coletivas que podem explorar uma ameaça. Assim, este termo envolve todo um conjunto de capacidade, intenções e motivações de modo a estabelecer um perfil de atacante para cada um destes grupos.

No caso em estudo, para a divisão nas diferentes categorias/grupos, correspondente aos diversos tipos de perfis de atacantes, destacam-se os seguintes:

Anonymous Attacker - este perfil engloba os atacantes que não possuem qualquer conhecimento do sistema nem possuem acesso a este. São por isso atacantes externos, que procuram comprometer o sistema através da sua exploração por meios externos e acessíveis a qualquer utilizador malicioso. Este tipo de utilizador é o menos poderoso entre os perfis estabelecidos no que diz respeito ao conhecimento e acesso direto ao sistema, no entanto é o que engloba um maior número de entidades que podem possuir os mais diversos fatores

de motivação.

Trusted Attacker - este perfil engloba os atacantes externos que possuem mais conhecimento do sistema, uma vez que têm acesso a este (por exemplo através do uso de credenciais próprias). Este tipo de utilizador é mais poderoso em relação ao anterior pois possui acesso a partes distintas do sistema e, por isso, mais conhecimento acerca deste.

Malicious Insider - este perfil engloba atacantes internos que possuem acesso interno ao próprio sistema e mecanismos envolventes. É neste perfil que se enquadram, por exemplo, os colaboradores Primavera, que podem desempenhar funções de administradores do sistema, programadores, *testers*, entre outros. Este tipo de utilizador é bastante poderoso pois o acesso aos componentes do sistema e dados críticos é facilitado. As motivações que podem dar origem a ataques por parte de utilizadores deste perfil são também bastante distintas dos anteriores perfis.

A definição destes perfis e a sua aplicação faz sentido e deve ser tida em conta aquando da definição e classificação das ameaças, uma vez que estas diferem entre os diversos perfis, pela variação de fatores como o nível de capacidade de ataque, acesso, intenções, que devem ser conjugados e considerados para cada grupo de atacantes.

3.7 Ameaças e proteção necessária

3.7.1 *Objetivos de segurança*

Após a análise anterior das necessidades de proteção por componente e por fluxo de informação, os objetivos de segurança do sistema a ter em conta para a procura de ameaças relevantes, pode reduzir-se, de um modo geral, às seguintes categorias:

Proteção ao nível da comunicação - Uma vez que a comunicação entre subcomponentes do sistema ou entidades externas envolve informação crítica torna-se necessário garantir a segurança dessa comunicação, de modo a não comprometer a segurança da informação transmitida.

Proteção ao nível da informação persistente - Uma vez que a informação armazenada pode conter dados sensíveis dos clientes torna-se necessário garantir a sua proteção através de mecanismos de confidencialidade e integridade. Esta proteção revela-se bastante necessária uma vez que o cliente deposita confiança na segurança desta informação.

Autenticação e autorização - Dado que o acesso à informação e funcionalidades do sistema variam de acordo com o cliente que efetua o pedido é necessário garantir e fornecer mecanismos de autenticação e autorização para que a identidade do cliente nunca deva ser posta em causa.

Integridade da informação - Tendo em conta que a viabilidade do sistema enquanto produto reside na validade da informação e das funcionalidades presentes torna-se necessário garantir que estas não sofrem qualquer tipo de modificações ou alterações não previstas, garantindo assim a sua integridade.

Controlo de acesso - Devido à possibilidade de diferentes ações e acesso a informação distinta por parte dos diversos utilizadores do sistema, torna-se necessário garantir um controlo eficaz do acesso a funcionalidades, dados, entre outros, não permitindo desta forma o acesso indevido por parte utilizadores não autorizados.

3.7.2 *Ameaças*

De modo a concretizar todo o objetivo de análise de ameaças e possíveis soluções para as mitigar, uma parte do trabalho consistiu na recolha em bruto de conjuntos de ameaças. Antes de uma análise exaustiva de ameaças específicas do sistema, e de modo a ter uma primeira visão global de um conjunto de ameaças comuns a diferentes soluções num contexto *cloud*, promovendo também uma maior abrangência no que diz respeito à diversidade de ameaças, foi tida como base uma lista disponibilizada pela *Microsoft*, a *Cloud Security Frame* [1], uma vez que o próprio sistema em estudo dá uso a soluções e plataformas *cloud* da própria *Microsoft*. Para uma mais fácil compreensão deste conjunto de ameaças, estas encontram-se divididas nas categorias a que dizem respeito, entre elas:

Auditoria e Logging – nesta categoria enquadra-se a forma como os eventos relativos à segurança são armazenados, monitorizados, expostos, particionados, etc. Exemplos incluem: quem fez o quê, quando ou através de onde;

Autenticação – esta categoria é referente aos processos e mecanismos de autenticação, onde também se incluem aspetos relativos às credenciais do utilizador, tipicamente um nome de utilizador e uma palavra passe;

1 https://blogs.msdn.microsoft.com/jmeier/2010/07/08/cloud-security-threats-and-countermeasures-at-a-glance/

Autorização - nesta categoria abordam-se aspetos relativos aos processos de autorização do utilizador, assim como as estratégias utilizadas para mecanismos de controlo de acessos, entre outros;

Comunicação - esta categoria engloba os aspetos que dizem respeito à forma como a informação é transmitida através dos diferentes canais de comunicação, onde se abordam questões como a segurança no transporte, segurança da mensagem, entre outros;

Criptografia - nesta categoria são analisados os mecanismos que promovem a confidencialidade e integridade da informação, assim como a forma como estes são utilizados e as garantias que fornecem;

Validação dos dados/input - esta categoria refere-se à forma como a aplicação filtra ou rejeita o *input* de dados por parte do utilizador e dos mecanismos que estão por trás do tratamento desses mesmos dados;

Tratamento de exceções - esta categoria diz respeito à forma como a aplicação lida em casos de erros e tratamento de exceções;

Dados sensíveis - nesta categoria são abordados os mecanismos subjacentes à proteção dos dados sensíveis, a forma como estão a ser utilizados e de que forma é assegurada essa proteção;

Gestão de sessões - esta categoria é referente à forma como a aplicação lida com a interação com o utilizador, que mecanismos de gestão de sessões estão subjacentes a essa interação e de que forma são utilizados.

Dada esta divisão por categorias, e de acordo com o leque completo de ameaças presentes na lista base, faz sentido analisar e perceber, para cada uma dessas ameaças, quais estão a ser protegidas no contexto atual do sistema e quais constituem efetivamente uma ameaça, não estando para estas disponível no imediato e a ser utilizado um mecanismo de proteção adequado. De modo a concretizar esse objetivo, tal como referido anteriormente no capítulo 2.3, e uma vez que o produto em estudo se encontra inserido num contexto empresarial, para além da investigação relativa a cada ameaça, foram também conduzidas questões aos diferentes *stakeholders* de modo a perceber quais destas ameaças se aplicam realmente e de que forma poderão posteriormente ser classificadas.

Desta forma, e tendo em conta essa análise foi estabelecido um quadro onde para cada ameaça se definem por cores, e para cada grupo distinto de atacantes, as seguintes características:

- Cor verde - na situação atual do sistema em análise existem mecanismos que garantem a proteção contra a ameaça em questão;
- Cor vermelha - na situação atual do sistema em análise não existem mecanismos que protejam a exploração da ameaça em questão;
- Cor cinzenta - a ameaça em questão não faz sentido no contexto do sistema em análise.

Com base nesta definição, encontra-se na Figura 7 a correspondência para cada uma das ameaças, assim como as garantias de proteção necessárias a cada uma delas.

Desta lista destacam-se, obviamente, as ameaças que necessitam, no contexto atual do sistema, de uma análise mais cuidada, pelo facto de apresentarem problemas relativamente àquele que é o nível de segurança desejado para um sistema com as características deste. Entre elas, as ameaças nas categorias: de auditoria e *logging*, onde se encontra o facto de não ser possível relacionar um pedido ao sistema com o utilizador que o efetua; na categoria de autenticação, na qual não se encontra em vigor qualquer tipo de proteção sobre múltiplas tentativas de autenticação nem esforços no que diz respeito ao tamanho e força das credenciais; na categoria de autorização, onde é procurada a melhoria das garantias de proteção dos *tokens* e dos dados que neles se encontram; na categoria de comunicação, na qual são analisadas as garantias oferecidas nos protocolos de comunicação entre componentes e com o exterior; na categoria de configuração, onde se encontram problemas no que diz respeito à proteção dos ficheiros de configuração do sistema e dados neles presentes; na categoria de criptografia, onde se encontram em uso protocolos e algoritmos que não fornecem as garantias de proteção necessárias; na categoria de tratamento de exceções, onde se aborda a necessidade de acesso à informação por parte dos colaboradores na resolução de erros e casos de suporte; na categoria de dados sensíveis, onde se encontra o facto da necessidade de proteção dos dados do Cliente; e na categoria de gestão de sessões onde é abordada a necessidade das alterações aos mecanismos de *logout* e gestão de *tokens*.

3.7.3 *Classificação de ameaças*

Após a identificação das ameaças que fazem sentido no contexto do sistema em estudo, torna-se também necessário proceder à sua classificação. A classificação das ameaças é importante quando se efetua uma análise de segurança sobre um sistema pois é através deste

		Entidade			Garantias necessárias			
		Anonymous Attacker	Trusted Attacker	Malicious Insider	Confidencialidade	Integridade	Disponibilidade	Responsabilização
Auditoria e Logging	Repúdio							X
	Negação de serviço (DoS)						X	
	Revelação de informação confidencial				X			
Autenticação	Interseção na rede				X			
	Ataques por força bruta				X			
	Ataques por dicionário				X			
	Ataques por repetição de cookies							
	Roubo de credenciais				X			
Autorização	Elevação de privilégios				X	X		
	Revelação de dados confidenciais				X			
	Adulteração de dados					X		
	Luring attacks							
	Roubo de tokens				X			
Comunicação	Falha na cifragem de mensagens				X	X		
	Roubo de chaves criptográficas				X			
	Ataques de man-in-the-middle				X	X		
	Repetição de mensagens de sessão							
	Adulteração de dados					X		
Configuração	Acesso indevido a ficheiros de configuração				X	X		
	Recuperação de segredos de configuração em texto limpo				X			
Criptografia	Quebra do algoritmo criptográfico				X	X		
	Obtenção de chaves criptográficas				X	X		
Tratamento de exceções	Revelação de informação				X			
	Negação de serviço						X	
	Elevação de privilégios				X			
Validação dos dados/input	Ataques de normalização							
	Cross-site scripting							
	SQL injection				X	X	X	
	Cross-site Request Forgery							
	XML bomb							
	Manipulação dos headers HTTP				X			
Dados sensíveis	Dumping de memória				X			
	Interseção na rede				X			
	Sniffing de ficheiros de configuração				X			
	Acesso a dados sensíveis armazenados				X			
Gestão de sessões	Roubo de sessão				X	X		
	Repetição de sessão				X			
	Ataques de man-in-the-middle				X	X		
	Incapacidade de terminar sessão				X			
	Cross-site Request Forgery							
	Fixação de sessão							
	Balanceamento de carga e afinidade de sessão							

Figura 7.: Ameaças por categoria e necessidades de proteção

método que se torna possível perceber quais as prioridades na necessidade de intervenção e resolução. Desta forma, as ameaças definidas anteriormente devem ser detalhadas quanto à sua probabilidade de ocorrência e impacto de modo a que seja possível classificá-las. Tal como na secção anterior, também aqui a classificação das ameaças no contexto do sistema foi alcançada através de discussão e questões entre os diferentes *stakeholders*, garantindo dessa forma um maior rigor no que diz respeito à classificação das probabilidades de ocorrência e impactos.

De modo a facilitar a visualização na definição de prioridades as ameaças serão também colocadas sobre a matriz de risco presente na Figura 8.

Likelihood	Impact				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	Moderate	High	High	Extreme	Extreme
Likely	Moderate	Moderate	High	High	Extreme
Possible	Low	Moderate	Moderate	High	Extreme
Unlikely	Low	Moderate	Moderate	Moderate	High
Rare	Low	Low	Moderate	Moderate	High

Figura 8.: Matriz de risco

A classificação encontra-se descrita na Figura 9 para as várias ameaças nas diferentes categorias. Na tabela podem ser encontradas as várias ameaças e respetivas medidas de probabilidade e impacto, que quando combinadas na matriz da Figura 8 dão origem a uma medida de risco global. Também se encontram na tabela os fatores de impacto técnico e no negócio das referidas ameaças.

Tendo em conta a classificação estabelecida para os diferentes níveis de probabilidade de ocorrência e impacto, e de forma a facilitar a visualização dos riscos e promover uma tomada de decisão eficiente aquando da sua mitigação, as ameaças anteriores podem ser enquadradas numa matriz de risco, como se apresenta na Figura 10.

	Ameaça	Probabilidade	Impacto	Risco	Fator Impacto Técnico	Fator Impacto Negócio
Auditoria e Logging	**1.** Repúdio	Improvável	Moderado	Moderado	Perda da capacidade de responsabilização	Dano na reputação da organização
Autenticação	**2.** Ataques por força bruta/dicionário	Possível	Significativo	Elevado	Perda da confidencialidade	Dano na reputação da organização, Violação da privacidade
	3. Roubo de credenciais	Improvável	Significativo	Moderado	Perda da confidencialidade	Dano na reputação da organização, Violação da privacidade
Autorização	**4.** Elevação de privilégios	Improvável	Significativo	Moderado	Perda da confidencialidade	Dano na reputação da organização, Violação da privacidade
	5. Roubo de tokens	Possível	Significativo	Elevado	Perda da confidencialidade e integridade	Dano na reputação da organização, Violação da privacidade
Comunicação	**6.** Roubo de chaves criptográficas	Raro	Severo	Elevado	Perda da confidencialidade e integridade	Dano na reputação da organização, Violação da privacidade
Configuração	**7.** Acesso indevido a ficheiros de configuração	Improvável	Reduzido	Moderado	Perda da integridade	Dano na reputação da organização
	8. Recuperação de segredos em texto limpo	Improvável	Reduzido	Moderado	Perda da confidencialidade	Dano na reputação da organização, Violação da privacidade
Criptografia	**9.** Quebra do algoritmo criptográfico	Raro	Severo	Elevado	Perda da confidencialidade e integridade	Dano na reputação da organização, Violação da privacidade
	10. Obtenção de chaves criptográficas	Improvável	Sever	Elevado	Perda da confidencialidade e integridade	Dano na reputação da organização, Violação da privacidade
Tratamento de exceções	**11.** Revelação de informação	Possível	Reduzido	Moderado	Perda da confidencialidade	Violação da privacidade
Dados sensíveis	**12.** Acesso a dados sensíveis armazenados	Possível	Severo	Extremo	Perda da confidencialidade	Dano na reputação da organização, Violação da privacidade
Gestão de sessões	**13.** Roubo de sessão	Possível	Significativo	Elevado	Perda da confidencialidade	Dano na reputação da organização, Violação da privacidade
	14. Incapacidade de terminar sessão	Quase certo	Significativo	Extremo	Perda da confidencialidade	Dano na reputação da organização, Violação da privacidade

Figura 9.: Classificação de ameaças

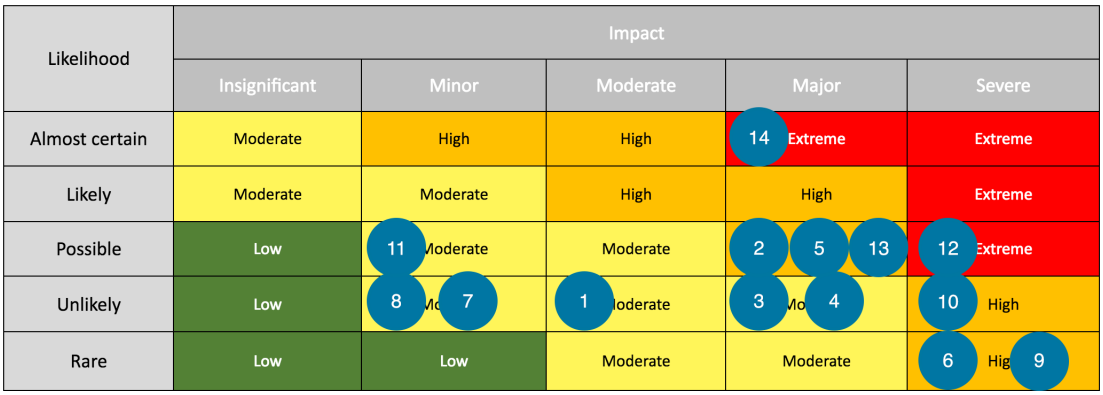


Figura 10.: Matriz de risco - classificação das ameaças

3.8 PROPOSTAS DE SOLUÇÕES

Seguindo a abordagem anterior, no que diz respeito à divisão por categorias, também as propostas de soluções para as ameaças analisadas seguem essa abordagem. Para cada uma dessas propostas será então descrito o problema em causa, quais as propostas sugeridas para alteração ou solução desse mesmo problema e quais as necessidades de implementação e exequibilidade da solução proposta.

3.8.1 *Auditoria/Logging - Repúdio*

Problema atual: Caso não seja feito o registo das ações efetuadas por um utilizador na aplicação, este pode negar tê-las efetuado assim como explorar a aplicação sem que isso seja percebido e sem deixar rasto. Caso as ações sejam registadas num ficheiro com tamanho limitado (possivelmente escrevendo as novas entradas "por cima"das mais antigas) um atacante pode encobrir os seus registos maliciosos, procurando dessa forma apagar indícios da sua atividade. Por outro lado, caso o ficheiro cresça indefinidamente o seu tamanho pode afetar o próprio serviço ou a máquina onde se encontra armazenado. Com os mecanismos existentes apenas são registados os pedidos que passam pelo *router* e acessos às bases de dados, não sendo, no entanto, possível associar esses pedidos a um utilizador concreto.

- *Probabilidade*: Improvável
- *Impacto*: Moderado
- *Risco global*: Moderado
- *Fator de impacto técnico*: A exploração do problema em causa implica a perda da capacidade de responsabilização

- *Fator de impacto no negócio*: A exploração do problema em causa implica danos na reputação da empresa

De acordo com os problemas apresentados, as propostas de solução possíveis passam por:

1. Efetuar *logging* das ações dos utilizadores
2. Efetuar a gestão dos ficheiros de *log*

1. Efetuar logging das ações dos utilizadores

De forma a contrariar o problema em causa, torna-se necessário proceder ao registo das ações efetuadas por um utilizador do Elevation Mobile, guardando em ficheiros de log os pedidos efetuados ao serviço. Desta forma, torna-se possível relacionar as ações efetuadas com o utilizador, garantindo a responsabilização.

Necessidades de implementação

De modo a concretizar a solução em causa terão de ser ativados mecanismos que registem as ações efetuadas, sendo que atualmente apenas são registados os pedidos no Router. Terá também de se proceder ao relacionamento de todos os pedidos ao serviço com o utilizador que os efetua, permitindo dessa forma que se identifique unicamente um utilizador.

Exequibilidade

Apesar da necessidade e mais-valias apresentadas por esta solução, esta torna-se de difícil concretização na prática devido ao volume de dados gerado no registo de todas as ações de todos os utilizadores do sistema. Devido a este motivo, atualmente apenas são efetuados *logs* quando estritamente necessário. Uma solução alternativa, reduzindo substancialmente o volume de dados, passa pelo registo em *logs* apenas de ações consideradas relevantes/críticas. Existem, no entanto, soluções adicionais que podem ser úteis, as quais vão ser descritas no ponto seguinte.

2. Gestão dos ficheiros de log

Tal como referido anteriormente o tamanho dos ficheiros de log deve ser um aspeto a considerar, uma vez que esse ficheiro não deve crescer indefinidamente em tamanho, pois pode afetar o desempenho do sistema ou máquina onde é armazenado, mas também não deve ter um tamanho fixo pois isso pode afetar os registos armazenados. De forma a combater estes problemas podem ser consideradas opções como mecanismos de rotação de *logs*, os quais promovem a divisão destes ficheiros por diversas máquinas e/ou a sua renovação

automática de modo a que as entradas não sejam perdidas. Através deste tipo de mecanismos pode ser feita a gestão dos ficheiros de log, não permitindo que registos mais antigos sejam apagados, nem que o tamanho dos ficheiros afete o sistema em causa.

Necessidades de implementação
A solução apresentada necessita da implementação dos mecanismos de gestão de *logs*.

Exequibilidade
A solução apresentada apenas necessita da adaptação dos mecanismos de gestão de *logs* aos ficheiros em causa gerados pelo sistema.

3.8.2 *Autenticação - Ataques por força bruta/dicionário*

Problema atual: Com os mecanismos existentes não é incentivado o uso de credenciais fortes por parte dos utilizadores do sistema nem são registadas tentativas de login com sucesso e falhadas, permitindo, por isso, que um utilizador malicioso consiga efetuar múltiplas tentativas de autenticação num curto espaço de tempo.

No Anexo A.1 será analisado este problema com base no documento do NIST SP 800-118 Draft (Scarfone and Souppaya, 2009).

- *Probabilidade*: Possível
- *Impacto*: Significativo
- *Risco global*: Elevado
- *Fator de impacto técnico*: A exploração do problema em causa implica a perda da confidencialidade e/ou integridade da informação
- *Fator de impacto no negócio*: A exploração do problema em causa implica danos na reputação da empresa e/ou violação da privacidade do Cliente

De acordo com os problemas apresentados, as propostas de solução possíveis passam por:

1. Criação de políticas de *passwords*
2. Registo de tentativas de acesso

1. Criação de políticas de passwords

De modo a combater os problemas em causa, devem ser postas em prática políticas que promovam o uso correto dos mecanismos de autenticação, neste caso, as passwords. Nessas políticas devem ser claras as opções de geração de passwords aquando do registo de forma a gerar credenciais fortes, estabelecer limites relativos a tamanho e força das credenciais utilizadas, assim como estabelecer o funcionamento de ações como o *reset* à password ou a opção de recuperação de credenciais após esquecimento. No Anexo A.1 podem ser encontradas mais informações relativamente a este problema.

Necessidades de implementação

A solução apresentada implica alterações na forma de geração e validação das credenciais utilizadas.

Exequibilidade

A solução apresentada não implica um impacto negativo significativo no sistema, aumentando substancialmente a qualidade e força das credencias de autenticação, melhorando a segurança dos utilizadores.

2. Registo de tentativas de acesso

De modo a combater os problemas que dizem respeito aos número de pedidos de autenticação consecutivos devem ser registadas todas as tentativas de acesso, isto é, *logins* com sucesso e falhados. Desta forma torna-se possível pôr em prática mecanismos de combate a ataques que explorem a capacidade de ser possível efetuar múltiplas tentativas de *login*. Através do registo destas ações é possível restringir o número máximo de tentativas de acesso consecutivas a um determinado número, ou introduzir um *delay* entre essas tentativas de modo a dificultar possíveis ataques. Através do registo de *logins* com sucesso, e apresentando essa informação ao utilizador dentro da própria aplicação, é possível manter este informado sobre possíveis comprometimentos das suas credenciais ou ataques realizados com sucesso.

Necessidades de implementação

A solução apresentada implica alterações que permitam o registo das tentativas de autenticação no sistema, assim como a criação de mecanismos para restringir o número de tentativas consecutivas e/ou informar o utilizador dessas tentativas.

Exequibilidade

A solução apresentada implica um custo computacional extra, embora reduzido, no momento do processo de autenticação. No entanto melhora substancialmente a segurança do

sistema e do próprio utilizador no que diz respeito aos mecanismos de autenticação.

3.8.3 *Autenticação - Roubo de credenciais*

Problema atual: O atacante pode obter acesso a credenciais através do roubo destas em ataques de *phishing* ou *social engineering*. Neste tipo de ataques um utilizador malicioso, através de diversas técnicas pode tentar manipular quem tem conhecimento das credenciais de acesso ao serviço, obtendo por parte destes as credenciais sem que se apercebam que a estão a divulgar a um atacante.

- *Probabilidade*: Improvável
- *Impacto*: Significativo
- *Risco global*: Moderado
- *Fator de impacto técnico*: A exploração do problema em causa implica a perda da confidencialidade e/ou integridade da informação
- *Fator de impacto no negócio*: A exploração do problema em causa implica danos na reputação da empresa e/ou violação da privacidade do Cliente

De acordo com o problema apresentado a solução possível passa por:

1. Manter o Cliente informado relativamente a este tipo de ataque
Relativamente a este problema a solução passa por manter o Cliente/utilizador informado da existência destes ataques, alertando-o do modo de funcionamento da PRIMAVERA e da necessidade de manter as suas credenciais de acesso ao sistema privadas e seguras.

Necessidades de implementação
Esta solução não necessita de mecanismos complexos de implementação.

Exequibilidade
Esta solução é relativamente simples de ser implementada, não apresentando impactos negativos para a globalidade do sistema.

3.8.4 *Configuração - Acesso indevido a ficheiros de configuração/Recuperação de segredos em texto limpo*

Problema atual: O acesso indevido a ficheiros de configuração facilita a um atacante interno o acesso a informação secreta presente nesses ficheiros em texto limpo. Essa informação pode incluir *strings* de conexão a bases de dados, chaves de autenticação, entre outros. No caso concreto do sistema em análise não é armazenada informação extremamente crítica nesses ficheiros resultando por isso num impacto reduzido. Por outro lado a alteração da informação desses ficheiros não se reflete num ambiente produtivo, uma vez que estes ficheiros passam por análise por parte de uma equipa especializada aquando da sua migração para esse ambiente.

- *Probabilidade*: Improvável
- *Impacto*: Reduzido
- *Risco global*: Moderado
- *Fator de impacto técnico*: A exploração do problema em causa implica a perda da confidencialidade e/ou integridade da informação
- *Fator de impacto no negócio*: A exploração do problema em causa implica a violação da privacidade dos dados em causa

De modo a combater os problemas apresentados, as propostas de solução possíveis passam por:

1. Garantir mecanismos de controlo de acesso aos ficheiros
2. Proteger a informação crítica presente nesses ficheiros

1. Garantir mecanismos de controlo de acesso aos ficheiros

De modo a garantir a responsabilização devem ser estabelecidas políticas de controlo de acesso a estes ficheiros, diminuindo o número de pessoas com acesso à sua visualização e/ou modificação. Da mesma forma, com o mesmo objetivo e como já acontece no sistema atual, todas as alterações nestes ficheiros antes de se refletirem num ambiente produtivo devem passar por uma análise cuidada da equipa responsável pela sua migração, afetando assim um número mínimo de utilizadores/Clientes.

Necessidades de implementação

A solução apresentada está neste momento a ser utilizada, estando previstas também modificações que visem melhorar o controlo de acesso e facilidade de responsabilização.

Exequibilidade

A solução apresentada, apesar de todas as vantagens que possui, tem a desvantagem de visualizações e modificações necessárias precisarem de passar por um membro da equipa com acesso a essa informação.

2. Proteger a informação crítica presente nesses ficheiros

Outra solução paralela passa por proteger a informação crítica de uma revelação não intencional, garantindo que apenas aqueles com acesso a informação secreta (chave privada, por exemplo) a possam visualizar. Esta solução passa então pela cifragem da informação crítica e/ou secções dos ficheiros de configuração antes de os disponibilizar.

Necessidades de implementação

Esta solução pode passar pelo uso de mecanismos presentes nas tecnologias utilizadas, de modo a facilitar a sua implementação. O próprio IIS e serviços WCF oferecem algumas opções válidas para a cifragem de secções de ficheiros de configuração neste contexto.

Referências:

Walkthrough: Creating and Exporting an RSA Key Container - https://msdn.microsoft.com/en-us/library/2w117ede%28v=vs.100%29.aspx

RsaProtectedConfigurationProvider (blog post) - http://austrianalex.com/rsaprotectedconfigurat
html

RsaProtectedConfigurationProvider Class - https://msdn.microsoft.com/en-us/library/system.configuration.rsaprotectedconfigurationprovider%28v=vs.110%29.aspx

Exequibilidade

As dificuldades do uso desta solução passam pela implementação dos mecanismos sugeridos, assim como algum impacto relativo aos processos de cifragem/decifragem da informação.

3.8.5 *Autorização - Elevação de privilégios*

Problema atual: Um atacante pode procurar obter níveis de acesso superiores aos que normalmente possui através de um ataque interno ao serviço ou de um utilizador interno malicioso.

Atualmente os níveis de privilégios e controlo de acesso são definidos por valores presentes no *token*. Através do campo *role*, um dos vários campos do *token*, a aplicação verifica o privilégio de cada utilizador, alterando com isso o grau de acesso de cada utilizador à

informação, o que se reflete na informação que lhe é apresentada pela aplicação. Um atacante com acesso a esse *token* pode, portanto, alterar o *role*, alterando os níveis de privilégio, e, consequentemente, dando mais ou menos acesso a um utilizador.

- *Probabilidade*: Improvável
- *Impacto*: Significativo
- *Risco global*: Moderado
- *Fator de impacto técnico*: A exploração do problema em causa implica a perda da confidencialidade e/ou integridade da informação
- *Fator de impacto no negócio*: A exploração do problema em causa implica danos na reputação da empresa e/ou violação da privacidade do Cliente

De modo a combater os problemas apresentados, a proposta de solução possível passa por:

1. Proteger o acesso ao *token*

Neste caso, e uma vez que este ataque carece de falta de motivação, pois o acesso ao *token* garante por si só acesso às credenciais do utilizador, não sendo necessária a alteração do *role*, a solução passa por restringir o acesso ao *token* de modo a proteger a informação nele contida. Esta solução pode ser alcançada através de mecanismos de controlo de acesso que não permitam a leitura e escrita deste tipo de dados por parte de utilizadores internos, ou através da proteção dos dados do *token*, o que se pode revelar mais difícil devido à necessidade de leitura desses dados por parte da própria aplicação.

Necessidades de implementação

A solução em causa necessita do estabelecimento de políticas de controlo de acesso a estes dados, ou, por outro lado, caso sejam implementadas medidas de proteção da informação presente no *token*, a necessidade de alteração dos mecanismos de leitura desses dados do lado aplicacional.

Exequibilidade

No contexto atual do sistema, a opção de restringir a leitura/acesso ao *token* é mais fácil de ser contemplada quando comparada com a opção de proteção direta dos dados do *token*, uma vez que esta última obrigaria a alterações significativas da própria aplicação para além de introduzir custos computacionais extra nas operações de leitura desses mesmos dados.

3.8.6 *Comunicação - Protocolos de segurança nas ligações aos endpoints*

Problema atual: A configuração atual dos protocolos de comunicação segura implementados nos diferentes *endpoints* possui aspetos suscetíveis a alteração de modo a promover melhores garantias de segurança do que as encontradas atualmente.

Uma análise aos certificados utilizados nos protocolos de comunicação, assim como às respetivas configurações, aponta para alguns aspetos cuja alteração se pode revelar uma mais-valia no contexto da segurança global do sistema.

A análise individual (*reports*) de cada um dos *endpoints* pode ser encontrada no Anexo A.2 – Análise endpoints.

No Anexo A.3 – NIST Guidelines for TLS implementations – SP 800-52 (Polk et al., 2014) podem ser encontradas algumas das considerações do NIST sobre a implementação e configuração aconselhável do protocolo TLS.

- *Probabilidade*: Improvável
- *Impacto*: Severo
- *Risco global*: Elevado
- *Fator de impacto técnico*: A exploração do problema em causa implica a perda da confidencialidade e/ou integridade da informação
- *Fator de impacto no negócio*: A exploração do problema em causa implica danos na reputação da empresa e/ou violação da privacidade do Cliente

De acordo com o conjunto de análises individuais presentes no Anexo A.2 – Análise endpoints, as propostas de solução podem-se reduzir a:

1. Alteração do algoritmo de assinatura do certificado – migração do algoritmo SHA1 para um da família SHA2
2. Alteração das versões do protocolo suportadas – desabilitar o uso do SSLv3
3. Alteração dos algoritmos criptográficos suportados – desabilitar o uso do RC4
4. *Forward Secrecy*

1. Alteração do algoritmo de assinatura do certificado

O certificado utilizado do lado do servidor usa SHA1withRSA como algoritmo de assinatura, o que se revela fraco atualmente devido a ataques (collision attacks, etc) explorados no uso do SHA1. Devido a esse facto também diversas entidades (entre elas a *Microsoft*) estão

a proceder a planos de migração do algoritmo inseguro SHA1 para uma versão que ofereça melhores garantias, como é o caso dos algoritmos da família SHA2. A alteração do algoritmo de assinatura do certificado é aconselhável por questões de segurança e necessária devido às políticas de migração existentes, deixando o SHA1 de ser suportado num futuro próximo [2]. Uma vez que a validade do certificado utilizado expira dentro de pouco tempo, é desejável que esta alteração se proceda aquando da renovação desse mesmo certificado.

Necessidades de implementação

A solução apresentada necessita de um pedido à CA para a emissão de um certificado com o algoritmo de assinatura necessário.

Exequibilidade

A alteração proposta não provoca significativos impactos negativos ao nível da globalidade do sistema. Uma vez que a data de validade do certificado utilizado expira num futuro próximo, a alteração poderá proceder-se aquando da renovação desse mesmo certificado.

2. Alteração das versões do protocolo suportadas

A configuração atual de alguns dos endpoints analisados permite a utilização do protocolo SSL versão 3, que se revela bastante insegura pelo conhecimento de ataques específicos a esta versão do protocolo, de como é exemplo o *POODLE attack* [3] . É recomendado que a possibilidade de utilização do SSL versão 3 seja desabilitada, não sendo permitida a sua utilização.

Mais informação relativamente às versões dos protocolos sugeridas poderá ser encontrada no Anexo A.3 – NIST Guidelines for TLS implementatios – SP 800-52 (Polk et al., 2014).

Necessidades de implementação

A solução apresentada necessita de pequenas alterações ao nível da configuração do protocolo de comunicação nos endpoints afetados. Uma avaliação que permita verificar se existem Clientes afetados por esta alteração pode também revelar-se útil.

Exequibilidade

A alteração proposta não provoca significativos impactos negativos ao nível da globalidade do sistema, diminuindo por outro lado a possibilidade de ataques conhecidos ao

2 https://security.googleblog.com/2014/09/gradually-sunsetting-sha-1.html
https://konklone.com/post/why-google-is-hurrying-the-web-to-kill-sha-1
3 https://en.wikipedia.org/wiki/POODLE

protocolo. Esta solução pode afetar Clientes que apenas consigam utilizar o SSL, uma vez que apenas passa a estar disponível o uso do TLS, no entanto não é de esperar que este problema afete qualquer cliente atualmente, ou então que afete apenas uma quantidade muito residual.

3. Alteração dos algoritmos criptográficos suportados

A configuração atual de alguns dos endpoints permite a utilização de algoritmos inseguros, como é o caso do RC4. Sugere-se a não utilização deste algoritmo.

Mais informação relativamente aos algoritmos sugeridos poderá ser encontrada no Anexo A.3 – NIST Guidelines for TLS implementatios – SP 800-52 (Polk et al., 2014).

Necessidades de implementação

A solução apresentada necessita de pequenas alterações ao nível da configuração do protocolo nos endpoints afetados.

Exequibilidade

A alteração proposta não provoca significativos impactos ao nível da globalidade do sistema, melhorando por outro lado a sua segurança.

4. Forward Secrecy

A configuração atual permite a utilização de mecanismos de acordo de chaves fracos que não permitem obter as propriedades de *forward secrecy*. Sugere-se a alteração destes para algoritmos que permitam obter *forward secrecy* como DHE e ECDHE, sendo desejável também a alteração dos parâmetros destes [4].

Necessidades de implementação

A solução apresentada necessita de pequenas alterações ao nível da configuração do protocolo nos endpoints afetados.

Exequibilidade

A alteração proposta não provoca significativos impactos ao nível da globalidade do sistema, melhorando por outro lado a sua segurança.

4 https://blog.qualys.com/ssllabs/2013/06/25/ssl-labs-deploying-forward-secrecy

3.8.7 *Dados sensíveis - Acesso a dados críticos armazenados*

Problema atual: Um atacante com acesso ao armazenamento de dados (bases de dados) consegue obter informação crítica uma vez que esta não se encontra protegida.

Uma vez que no cenário atual os dados críticos apenas se encontram protegidos durante a sua transmissão (dados em trânsito), um atacante com acesso ao armazenamento de dados (bases de dados) consegue obter acesso à informação, pois esta não se encontra protegida ao nível do armazenamento. Devido aos mecanismos de proteção existentes, este cenário é mais comum com a intervenção de utilizadores maliciosos internos (que podem ser colaboradores PRIMAVERA) pois a alguns destes é concedido acesso livre às bases de dados. Não estando a informação protegida, esta pode ser vista e/ou manipulada por esses utilizadores. A distribuição dessa informação por parte de utilizadores maliciosos internos pode também ser possível.

- *Probabilidade*: Possível
- *Impacto*: Severo
- *Risco global*: Extremo
- *Fator de impacto técnico*: A exploração do problema em causa implica a perda da confidencialidade e/ou integridade da informação
- *Fator de impacto no negócio*: A exploração do problema em causa implica danos na reputação da empresa e/ou violação da privacidade do Cliente

De modo a combater os problemas apresentados, as propostas de solução possíveis passam por:

1. *Transparent Data Encryption*
2. *Column/Cell Level Encryption*
3. Controlo de acesso

1. Transparent Data Encryption

Com o objetivo principal da proteção, as diferentes soluções propostas passam por mecanismos que procuram proteger a informação *at-rest*, proteger os dados nela contidos ou proteger o acesso à própria informação.

A Transparent Data Encryption (TDE) é uma tecnologia disponível nas bases de dados SQL Server para promover a cifragem dos dados nela contidos. A sua implementação é ao

nível do motor de base de dados tornando-a transparente do ponto de vista aplicacional, sendo por isso a sua implementação independente da aplicação, o que se revela bastante benéfico pois dispensa alterações na aplicação após a sua introdução. A TDE protege os dados at-rest (dados que não estão em trânsito) protegendo-os ao nível dos ficheiros, logs e backups. Esta solução revela-se bastante útil contra ataques em que um atacante com acesso à base de dados, ou a algum dos backups, a procura replicar ou obter a base de dados completa, pois a TDE não permite a instalação dessa base de dados noutro sistema. No entanto a TDE não oferece solução a um dos principais problemas atuais - a visualização da informação por quem possui acesso à BD.

Algumas das vantagens e limitações da TDE apresentam-se de seguida:

TDE – vantagens:

- Facilidade de implementação – todo o trabalho de implementação é resolvido pelo motor da BD, sendo apenas necessário criar os certificados e ativar esta opção
- Não há necessidade de alterações no código – completamente transparente ao nível aplicacional
- Eficiência – relativamente mais eficiente quando comparado com a cifragem por coluna
- Fornece automaticamente mecanismos de gestão de chaves

TDE - limitações:

- Chave única para toda a BD – uma única chave permite cifrar/decifrar toda a BD
- Não cifra a informação em trânsito – apenas protege os dados *at-rest* e não na comunicação (necessário o uso do TLS neste caso)
- Não protege a informação de ser vista por quem tem acesso à base de dados (DBA, colaboradores, casos de suporte,...)
- Disponível apenas em algumas edições do SQL Server (geralmente apenas nas edições Enterprise - possuem um custo elevado)

Necessidades de implementação

Para a implementação desta solução as necessidades passam por configurações básicas dos mecanismos de segurança a utilizar (password, certificado, etc) apenas ao nível da base

de dados e respetiva permissão para a utilização da cifragem nas bases de dados em questão.

Exequibilidade

Uma das desvantagens apresentadas para a implementação da TDE foi a sua disponibilidade em relação às edições utilizadas no caso do SQL Server. Uma vez que no caso do SQL Server 2012 esta opção apenas está disponível na edição *Enterprise*, e sendo utilizada a edição *Standard* nos *CloudServices*, uma alteração da edição atual para a *Enterprise* seria necessária para a implementação dos mecanismos de cifragem em causa. Sendo a licença paga por número de cores, e sendo o custo da licença para a edição Enterprise muito mais elevado do que o custo atual (cerca de 4 vezes mais), torna difícil a concretização desta solução no contexto do sistema em análise. Uma alteração deste género tornaria o custo com licenças SQL Server mais elevado do que o custo de manutenção de toda a infraestrutura atual, sendo por isso o fator custo o principal entrave à adoção deste mecanismo no cenário atual.

2. Column/Cell Level Encryption

Outro possível mecanismo para a proteção dos dados críticos armazenados passa pela cifragem ao nível da coluna - *Column Level Encryption*, definido pela Microsoft como *Cell Level Encryption*. Esta opção promove maior controlo da forma de cifragem da informação, de como esta é feita, onde e por quem, uma vez que esse trabalho deixa de ser totalmente controlado pelo motor de base de dados. Devido a esse facto esta opção provoca também alterações ao nível das aplicações que usam/controlam essa informação, assim como de todos os mecanismos de leitura/escrita dos dados em causa. Ao contrário da cifragem ao nível da base de dados, que protegia ao nível dos ficheiros, *logs* e *backups*, esta opção protege os dados ao nível da coluna, sendo por isso possível distinguir entre informação que deve ou não ser protegida e de que forma é efetuada a sua proteção.

Algumas das vantagens e limitações desta opção apresentam-se de seguida:

Column Encryption - vantagens:

- Flexibilidade na escolha dos pedaços de dados a cifrar – esta opção permite cifrar apenas a informação que necessita de ser protegida
- As aplicações podem controlar quando, onde, por quem e como a informação é vista – todo o trabalho de decifragem passa para o lado aplicacional
- Diferentes colunas podem ser decifradas com chaves diferentes – podem ser utilizadas chaves diferentes para colunas diferentes ou tipos de informação diferentes

- Disponível na maioria das versões do SQL Server.

Column Encryption - limitações:

- Impacto na performance – quanto maior o número de colunas cifradas maior o impacto na performance
- Limitações no tipo de *queries* que podem ser feitas – dependendo se a coluna está ou não cifrada a procura por um determinado critério nessa coluna pode não ser possível
- O uso de índices nas colunas cifradas torna-se impossível
- As funções pré definidas para este tipo de cifragem apenas devolvem dados no tipo *varbinary* e o *output* está limitado a 8000 bytes.

Necessidades de implementação

Esta solução necessita de alterações relativamente à forma como a informação é armazenada e lida, sendo por isso necessário proceder a alterações quer ao nível das aplicações/-serviços, quer ao nível da camada persistente (camada de dados).

Exequibilidade

No caso concreto dos *CloudServices* esta opção revela uma dificuldade relativamente elevada de implementação, apresentada por diversos fatores. Desde logo por ser uma solução que apresenta mudanças significativas ao funcionamento atual da implementação, necessitando da reescrita de todos os métodos de consulta e armazenamento da informação crítica. Por outro lado, esta solução, introduz também um ligeiro impacto negativo na performance desses mesmos métodos (uma vez que acresce a estes as necessidades de cifragem/decifragem da informação), refletindo-se isso na performance global dos serviços. Por fim, esta solução torna impossível a realização das *queries* utilizadas atualmente sobre as colunas cifradas, sendo esse um entrave relevante à adoção desta solução.

3. Controlo de acesso

Outra possível solução passa pela implementação de medidas mais restritivas de controlo de acesso à informação. Está de momento a ser planeada uma mudança que permite reduzir o número de pessoas com acesso total à informação crítica. Desta forma, torna-se mais fácil a responsabilização em casos específicos da exploração da ameaça. No caso concreto dos *CloudServices*, a informação passaria apenas por uma equipa que trataria da sua disponibilização (podendo esta ser parcial), montada noutra infraestrutura que não a mesma onde se encontram os dados do cliente, para a resolução de casos específicos de suporte, análise de dados, manutenção, etc. O objetivo desta solução passaria então pela obtenção

de maior controlo sobre quem tem acesso à informação, facilitando dessa forma também a responsabilização em caso de ataque.

Necessidades de implementação

Esta solução necessita de uma alteração na forma como é efetuado o acesso à informação crítica.

Exequibilidade

Apesar desta solução se demonstrar de concretização mais fácil do que as anteriores possui também o problema de tornar o acesso à informação menos imediato, o que para pequenas resoluções de suporte se pode revelar prejudicial, atrasando a resolução desses casos. Por outro lado deposita todo o trabalho de seleção e disponibilização da informação/BD apenas numa equipa, motivo que pode também atrasar essa disponibilização em casos de excesso de pedidos. Embora se revele benéfica, esta solução também não resolve por completo o problema apresentado, uma vez que o utilizador interno malicioso pode pertencer à equipa que possui acesso livre às bases de dados.

3.8.8 *Gestão de sessões - Incapacidade da terminação completa de sessão*

Problema atual: Um atacante pode explorar o facto da terminação da sessão não eliminar por completo todos os objetos relacionados com a sessão ou deixar o canal aberto.

No caso concreto da aplicação em causa, a operação de logout apenas "esquece" a chave do token do lado do cliente, não efetuando qualquer contacto com o servidor. O dispositivo deixa de enviar pedidos com a chave do token nos headers, no entanto, um utilizador malicioso com acesso ao token (não possível pela intersecção de pedidos anteriores mas, por exemplo, por acesso ao local de armazenamento dos tokens) pode reenviar pedidos com aquele token (válido, pois ainda se encontra em cache), recebendo como resposta informação relativa ao utilizador atacado.

- *Probabilidade*: Quase certo
- *Impacto*: Significativo
- *Risco global*: Extremo
- *Fator de impacto técnico*: A exploração do problema em causa implica a perda da confidencialidade e/ou integridade da informação

- *Fator de impacto no negócio*: A exploração do problema em causa implica danos na reputação da empresa e/ou violação da privacidade do Cliente

De forma a combater os problemas apresentados, a solução possível passa por:

1. Invalidar os objetos de sessão (tokens) após a terminação

De forma a combater o problema em causa devem obter-se garantias de que, após a terminação da sessão por parte de um utilizador, todos os objetos relativos a essa sessão são excluídos/invalidados tanto do lado do utilizador como do lado do servidor, de modo a garantir que esses objetos não possam ser reutilizados.

Necessidades de implementação

A solução apresentada requer alterações ao modo de como são utilizados os objetos de sessão (*tokens*) e o processo de *logout*. Devem por isso ser garantidos ou mecanismos de expiração de *tokens*, não permitindo que após o período de expiração os *tokens* sejam reutilizados (expirando automaticamente na operação de *logout*) ou mecanismos que permitam que após o *logout* todos os *tokens* relativos a um utilizador (um por módulo por dispositivo) sejam invalidados ou apagados do local de armazenamento de *tokens*, não permitindo assim a sua reutilização.

Exequibilidade

A solução apresentada, apesar das alterações à forma como são utilizados os objetos de sessão, não apresenta impactos negativos na globalidade do sistema embora introduza mecanismos adicionais às operações de *logout* e de limpeza/gestão de *tokens*.

4

CONCLUSÕES E TRABALHO FUTURO

4.1 CONCLUSÕES

Analisando o trabalho desenvolvido, este foi de encontro ao principal objetivo proposto, apresentando uma análise de segurança que resulta num conjunto de propostas de soluções aos principais desafios encontrados e a necessitar de intervenção iminente.

Tal como referido no decorrer do documento a constante inovação tecnológica e a procura de novos modelos de prestação de serviços, associada a uma mudança de paradigmas e formas de abordagem, reveste de especial importância um trabalho como este que foi desenvolvido. Neste caso concreto, e tendo em conta o produto em que esta análise de segurança se focou, o principal problema advinha da alteração da forma como o serviço era oferecido, resultante da migração de um modelo tradicional para um modelo *cloud*. Dessa forma, a análise foi conduzida sob um produto de *software* já desenvolvido, não se encontrando este no início do seu ciclo de vida. No entanto, a existência deste trabalho acaba por alertar a organização para um conjunto de aspetos relativos a questões de segurança, que podem ser tidos em conta no desenvolvimento de novos produtos, para que essas questões possam ser pensadas e introduzidas desde as fases de desenho e conceção do sistema.

O resultado final deste trabalho apresenta, assim, o concretizar de duas principais necessidades. Desde logo, apresenta uma série de propostas aos principais desafios identificados no sistema em análise. Este resultado pode, desta forma, ser entregue às equipas de desenvolvimento para que estas possam trabalhar sobre estas propostas e planear a sua implementação no sistema, podendo atacar no imediato alguns dos principais pontos críticos abordados. Por outro lado, a procura na produção de um documento que aborde os vários aspetos e fases de uma análise de segurança e apresente uma forma metódica de a realizar, dota a organização de um conjunto de ferramentas que pode ser usado e adaptado para outras soluções de *software*, servindo também este trabalho como *input* para a produção e análise de produtos futuros.

4.2 TRABALHO FUTURO

Relativamente ao trabalho que pode ainda ser efetuado sobre o já desenvolvido, este prende-se essencialmente com a implementação das soluções propostas no combate aos problemas identificados. Essa implementação permitirá obter conclusões acerca da forma como o sistema é afetado após a sua introdução. Deste modo, um estudo posterior a essa implementação poderá revelar-se benéfico no sentido de perceber se as melhorias esperadas no que diz respeito à segurança global do sistema estão a ser alcançadas, e se a introdução da solução proposta não afeta negativamente o sistema, quer ao nível de *performance*, quer ao nível do negócio, componentes bastante valorizadas em ambiente empresarial.

Por outro lado, como trabalho futuro poderão também ser aprofundadas as ameaças e propostas de soluções, de modo a obter mais detalhe e cobrir um leque maior de aspetos e situações consideradas. Também toda a análise pode ser alvo de reformulação de modo a apresentar os resultados segundo os critérios mais rigorosos, entre eles os definidos por *standards*, podendo até permitir a obtenção de certificações de segurança para os produtos alvo.

BIBLIOGRAFIA

Baskerville, Richard. Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Comput. Surv.*, 25(4):375–414, December 1993. ISSN 0360-0300. doi: 10.1145/162124.162127. URL http://doi.acm.org/10.1145/162124.162127.

Dan Boneh, Divya Gupta, Ilya Mironov, and Amit Sahai. Hosting services on an untrusted cloud. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 404–436. Springer, 2015.

Rajkumar Buyya, Anton Beloglazov, and Jemal Abawajy. Energy-efficient management of data center resources for cloud computing: A vision, architectural elements, and open challenges. *arXiv preprint arXiv:1006.0308*, 2010.

Cloud Security Alliance. Security Guidance for critical areas of focus in Cloud Computing V3.0. *CSA (Cloud Security Alliance), USA. Online: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf*, 2011.

Cloud Security Alliance. Cloud Adoption Practices & Priorities Survey Report, Janeiro 2015. URL https://downloads.cloudsecurityalliance.org/initiatives/surveys/capp/Cloud_Adoption_Practices_Priorities_Survey_Final.pdf.

Common Criteria. Common Criteria for Information Technology Security Evaluation, sep 2012. (CCMB-2012-09-001, Ver. 3.1, Rev. 4).

Computer World. Ataque DDoS à cloud da Amazon explora falha no Elasticsearch, 2014. URL http://www.computerworld.com.pt/2014/07/28/ataque-ddos-a-cloud-da-amazon-explora-falha-no-elasticsearch/. Acedido a: 10-12-2015.

Lucas Davi, Alexandra Dmitrienko, Ahmad-Reza Sadeghi, and Marcel Winandy. Privilege escalation attacks on android. In *International Conference on Information Security*, pages 346–360. Springer, 2010.

William Enck, Peter Gilbert, Seungyeop Han, Vasant Tendulkar, Byung-Gon Chun, Landon P Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N Sheth. TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS)*, 32(2):5, 2014.

Sascha Fahl, Marian Harbach, Thomas Muders, Lars Baumgärtner, Bernd Freisleben, and Matthew Smith. Why Eve and Mallory love Android: An analysis of Android SSL (in) security. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 50–61. ACM, 2012.

Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, page 3. ACM, 2012.

Gartner Inc. Gartner Says Nearly Half of Large Enterprises Will Have Hybrid Cloud Deployments by the End of 2017, 2013. URL http://www.gartner.com/newsroom/id/2599315. Acedido a: 30-10-2015.

Sanjay Ghemawat, Howard Gobioff, and Shun-Tak Leung. The Google file system. In *ACM SIGOPS operating systems review*, volume 37, pages 29–43. ACM, 2003.

N. Gruschka and L.L. Iacono. Vulnerable Cloud: SOAP Message Security Validation Revisited. In *Web Services, 2009. ICWS 2009. IEEE International Conference on*, pages 625–631, July 2009. doi: 10.1109/ICWS.2009.70.

Ronald L. Krutz and Russell Dean Vines. *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Wiley Publishing, 2010. ISBN 0470589876, 9780470589878.

Min Li, Wanyu Zang, Kun Bai, Meng Yu, and Peng Liu. MyCloud: supporting user-configured privacy protection in cloud computing. In *Proceedings of the 29th Annual Computer Security Applications Conference*, pages 59–68. ACM, 2013.

Tongxin Li, Xiaoyong Zhou, Luyi Xing, Yeonjoon Lee, Muhammad Naveed, XiaoFeng Wang, and Xinhui Han. Mayhem in the push clouds: Understanding and mitigating security hazards in mobile push-messaging services. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 978–989. ACM, 2014.

LinkedIn. LinkedIn Report: 2015 Cloud Security Survey, 2015. URL https://pages.cloudpassage.com/2015-cloud-security-survey-report-linkedin.html.

Peter M. Mell and Timothy Grance. SP 800-145. The NIST Definition of Cloud Computing. Technical report, Gaithersburg, MD, United States, 2011.

Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, and Muttukrishnan Rajarajan. A survey on security issues and solutions at different layers of cloud computing. *The Journal of Supercomputing*, 63(2):561–592, 2012. ISSN 1573-0484. doi: 10.1007/s11227-012-0831-5. URL http://dx.doi.org/10.1007/s11227-012-0831-5.

Mohamed, Arif. A history of cloud computing, 2009. URL http://www.computerweekly.com/feature/A-history-of-cloud-computing. Acedido a: 01-12-2015.

NIS Platform, Working Group 3. State-of-the-art of Secure ICT Landscape. Technical report, 2014.

Daniel Nurmi, Rich Wolski, Chris Grzegorczyk, Graziano Obertelli, Sunil Soman, Lamia Youseff, and Dmitrii Zagorodnov. The eucalyptus open-source cloud-computing system. In *Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on*, pages 124–131. IEEE, 2009.

Tim Polk, Kerry McKay, and Santosh Chokhani. Guidelines for the selection, configuration, and use of transport layer security (TLS) implementations. *NIST Special Publication*, 800: 52, 2014.

Karen Scarfone and Murugiah Souppaya. Guide to enterprise password management (draft). *NIST Special Publication*, 800:118, 2009.

Schneier, Bruce. Cloud Computing, Junho 4 2009. URL https://www.schneier.com/blog/archives/2009/06/cloud_computing.html. Acedido a: 01-12-2015.

Konstantin Shvachko, Hairong Kuang, Sanjay Radia, and Robert Chansler. The hadoop distributed file system. In *2010 IEEE 26th symposium on mass storage systems and technologies (MSST)*, pages 1–10. IEEE, 2010.

Juraj Somorovsky, Mario Heiderich, Meiko Jensen, Jörg Schwenk, Nils Gruschka, and Luigi Lo Iacono. All Your Clouds Are Belong to Us: Security Analysis of Cloud Management Interfaces. In *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*, CCSW '11, pages 3–14, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-1004-8. doi: 10.1145/2046660.2046664. URL http://doi.acm.org/10.1145/2046660.2046664.

Gary Stoneburner, Clark Hayden, and Alexis Feringa. SP 800-27 Rev. A. Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A. Technical report, Gaithersburg, MD, United States, 2004.

Maha Tebaa, Saïd El Hajji, and Abdellatif El Ghazi. Homomorphic encryption applied to the cloud computing security. In *Proceedings of the World Congress on Engineering*, volume 1, pages 4–6, 2012.

Marten Van Dijk, Ari Juels, Alina Oprea, Ronald L Rivest, Emil Stefanov, and Nikos Triandopoulos. Hourglass schemes: how to prove that cloud files are encrypted. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 265–280. ACM, 2012.

Qi Zhang, Lu Cheng, and Raouf Boutaba. Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1):7–18, 2010. ISSN 1869-0238. doi: 10.1007/s13174-010-0007-6. URL http://dx.doi.org/10.1007/s13174-010-0007-6.

A

MATERIAL DE SUPORTE - ANEXOS

A.1 NIST SP 800-118 DRAFT – APLICAÇÃO NO CASO DE ESTUDO

NIST SP 800-118 – Guide to Enterprise Password Management

http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

Este documento procede a uma divisão em 4 categorias: ameaças que capturam diretamente as password, como a instalação de keyloggers; ameaças que adquirem vantagem do uso de passwords ou funções de hash fracas, como password guessing e cracking; ameaças que alteram a password; e ameaças que envolvem o reúso por parte do atacante de passwords comprometidas.

1. Captura de passwords

Armazenamento

Neste caso não se encontram problemas significativos na solução atual, uma vez que são armazenadas apenas hashes das passwords utilizadas. Uma possível ataque que permita acesso às hashes também não se revela um problema uma vez que são utilizadas funções de hash criptográficas sendo extremamente difícil reverter a hash para a password original em tempo útil.

Transmissão

No que diz respeito à transmissão das passwords também não se apontam problemas significativos, uma vez que todas as comunicações externas e entre componentes utilizam o TLS como protocolo de segurança na comunicação.

Conhecimento e comportamento do utilizador

Não há muito que possa ser feito em relação a este aspeto que vise melhorar a situação atual. Atualmente o utilizador entra na aplicação sendo-lhe pedidas as credenciais de acesso. Este introduz as credenciais na aplicação através do teclado do telemóvel. A segurança do telemóvel relativamente às aplicações instaladas, presença de atacantes nas redondezas com possibilidade de visualizar a inserção da password, entre outros, recaem portanto noutro campo da análise. No que diz respeito a possíveis ataques de social engineering, tanto os utilizadores da aplicação como o pessoal interno devem possuir conhecimento pleno desses ataques e da forma como são efetuados. O Cliente deve ser informado de medidas da PRIMAVERA que o permitam distinguir entre uma resolução de suporte e um cenário de ataque, por exemplo.

2. Password Guessing and Cracking

Guessing

Em relação este aspeto há possibilidades para algumas alterações com vista a reforçar a segurança do sistema e dos mecanismos de autenticação. Na solução atual não é efetuado qualquer registo de tentativas de autenticações sucessivas, permitindo-se dessa forma que um utilizador malicioso efetue inúmeras tentativas, sendo por isso concretizável um ataque por força bruta e/ou dicionário. As formas de mitigação deste problema passam, normalmente, pela combinação de dois métodos. Primeiro, garantir que as passwords são suficientemente fortes e complexas. Por outro lado limitar a frequência dos pedidos de autenticação à aplicação. Neste último caso a solução pode passar pelo bloqueio da conta do utilizador após um número de consecutivas tentativas falhadas (o que pode ter impacto ao nível dos utilizadores legítimos) ou pelo adicionar de um delay crescendo exponencialmente entre tentativas de login falhadas. Este tipo de ataque revela-se mais fácil quanto mais informação o atacante tiver. Essa informação pode ir desde o tamanho máximo de carateres necessários para a password, a informação de que um utilizador existe ou não, o botão de “Login” estar cinzento até o número mínimo de carateres de uma password for cumprido, etc. Embora esta informação seja útil no processo de registo, no que diz respeito ao processo de login este conhecimento revela-se mais benéfico para o atacante do que para os utilizadores legítimos. Outra questão relevante neste aspeto tem que ver com o facto da operação de "reset"da password atribuir uma password default, ou até no processo de criação da conta, passwords essas que podem não oferecer as mesmas garantias de segurança. No caso das credenciais do ELEVATION Space, esta operação procede ao envio de um link para redefinição da password, não sendo por isso relevante este problema. É aconselhável a utilização de um link com um espaço temporal curto (diminuindo a janela temporal de ataque) e que possa ser usado apenas uma vez. Na maioria das vezes esse link é enviado por mail tomando como garantida a proteção oferecida pelo servidor de email e o acesso

ao email como fator de identificação do utilizador que realiza o pedido. O processo de identificação do utilizador através do email pode revelar-se relativamente seguro se este necessitar também de ativar a sua conta ou definir as suas credenciais de acesso depois de aceder a esse mesmo email.

Cracking

O processo de cracking procura encontrar conjuntos de carateres que produzam a mesma hash que a password. No caso concreto desta análise, este não se revela um problema, sendo as garantias de segurança depositadas no algoritmo de hash utilizado no armazenamento das passwords.

Força da password

Em relação à força das passwords no caso atual esta não é avaliada uma vez que não existem restrições relativamente ao tamanho e complexidade das mesmas. O melhoramento deste aspeto tornaria mais difíceis os ataques de password guessing e cracking.

Seleção da password do utilizador

Na primeira utilização do sistema e consequente atribuição de uma password a um utilizador devem ser tidas em conta todas as necessidades e restrições ao tamanho e força das credenciais, garantindo assim a geração de uma password forte.

3. Password Replacing

Recuperação de passwords e resets

Aquando do esquecimento de uma password há 2 procedimentos possíveis: a recuperação da password antiga - password recovery - ou a atribuição de uma nova password - password reset. Em ambos os casos é necessário ter garantias da identidade do utilizador que efetua o pedido de password recovery ou reset, uma vez que caso isso não aconteça um atacante pode facilmente fazer-se passar por outro utilizador, obtendo a sua password.

Acesso a informação armazenada da conta e passwords

Este caso não se revela um problema no contexto atual da aplicação uma vez que o que é armazenado é uma hash da password, não estando por isso disponível a password em plain-text.

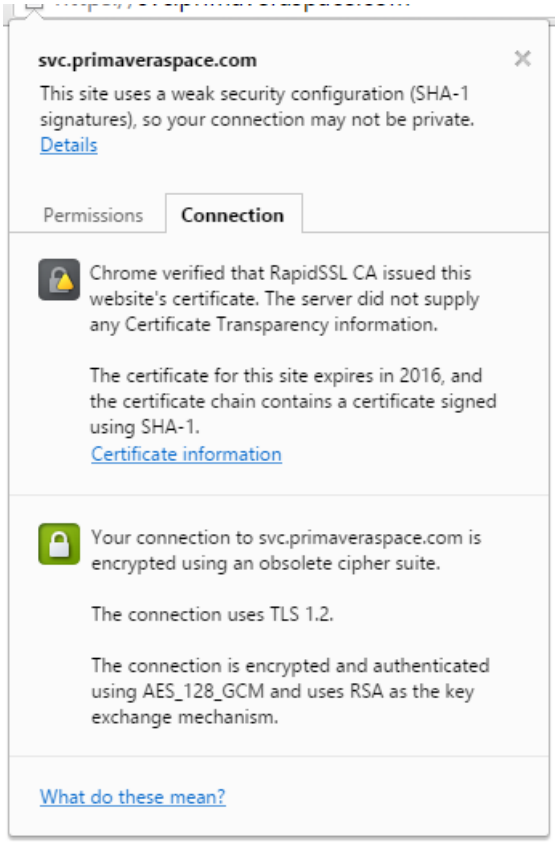
Uso de password comprometidas

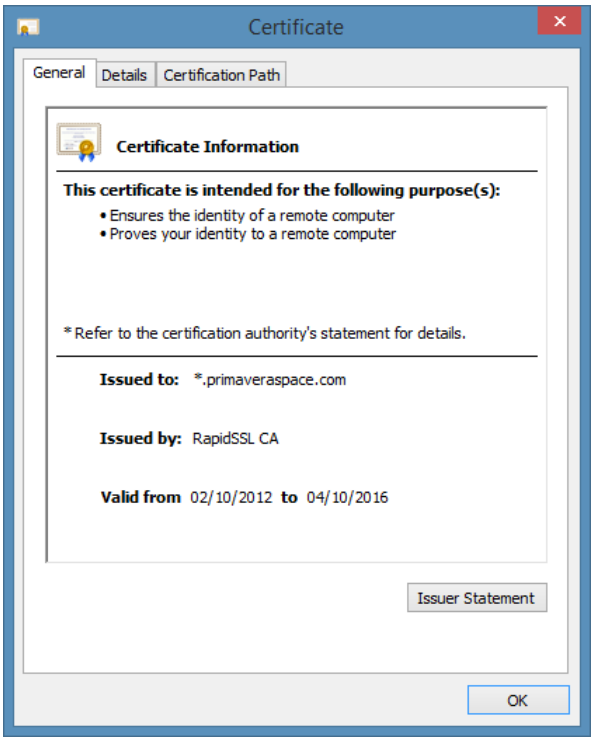
Políticas de expiração de passwords – o uso de políticas de expiração de passwords no contexto do sistema em análise não se revela benéfica, uma vez que os seus benefícios não

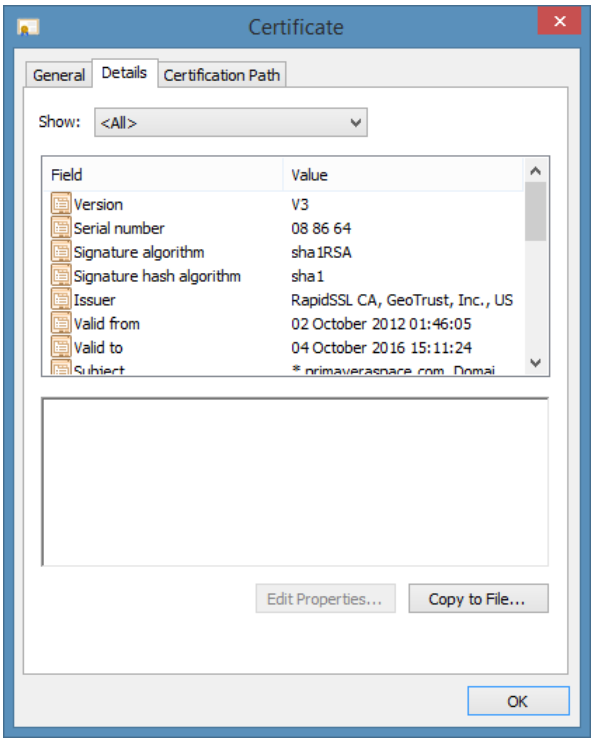
justificam os potenciais fatores adversos.

A.2 ANÁLISE ENDPOINTS

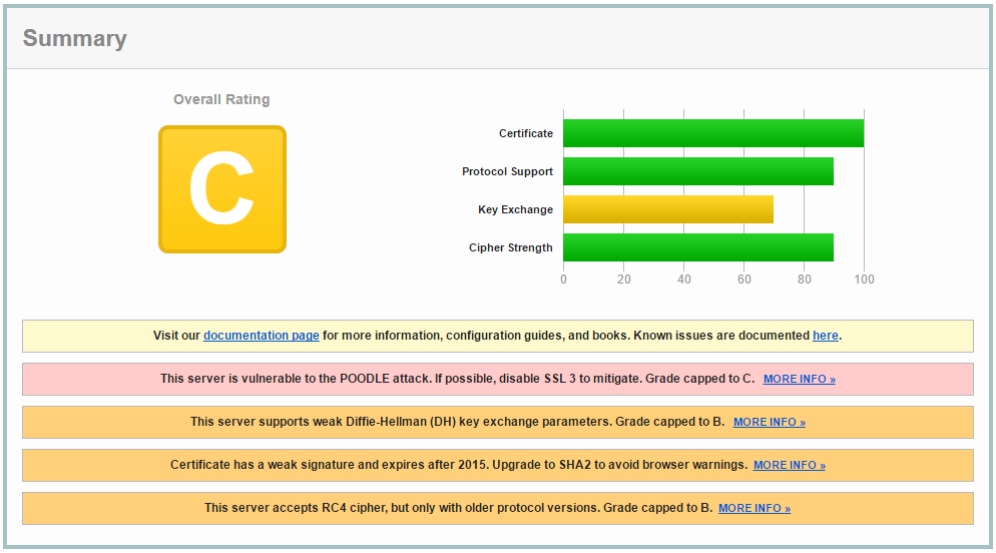
- **https://svc.primaveraspace.com/**

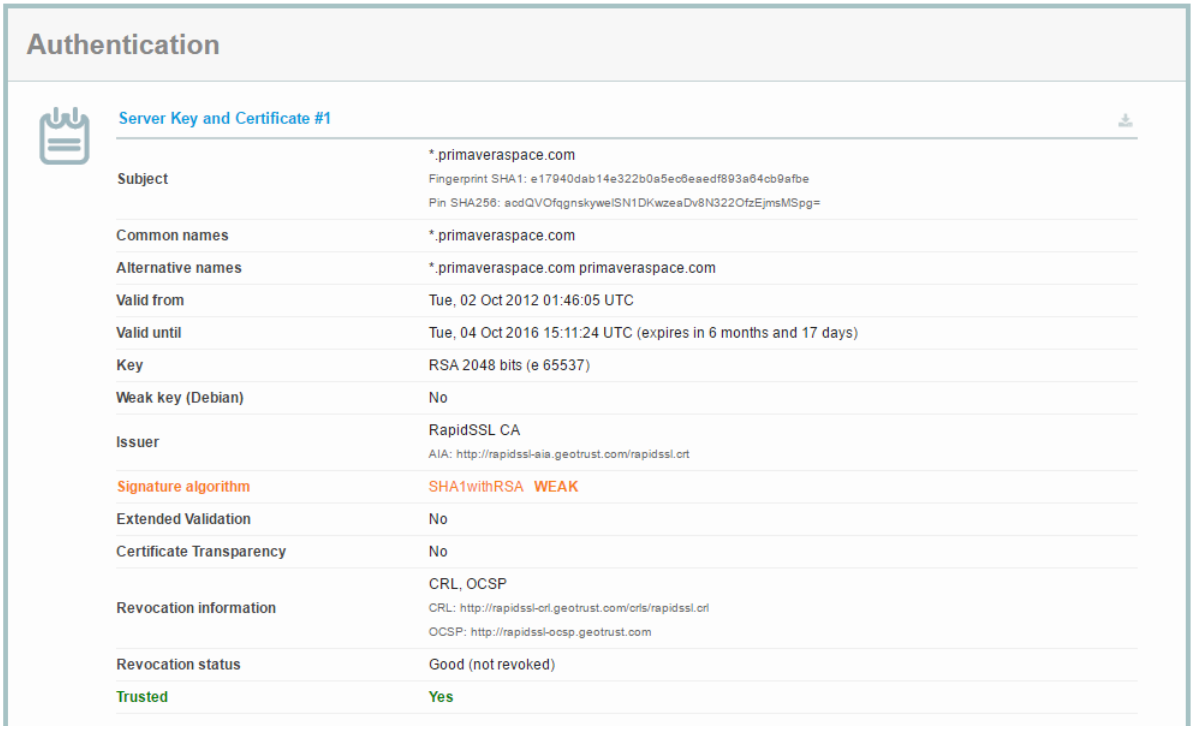



Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.primaveraspace.com
Issued by: RapidSSL CA
Valid from 02/10/2012 to 04/10/2016
Issuer Statement
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
08 86 64
Signature algorithm
sha1RSA
Signature hash algorithm
sha1
Issuer
RapidSSL CA, GeoTrust, Inc., US
Valid from
02 October 2012 01:46:05
Valid to
04 October 2016 15:11:24
Edit Properties...
Copy to File...
OK

SSL Report


Summary
Overall Rating
C
Certificate
Protocol Support
Key Exchange
Cipher Strength
0
20
40
60
80
100
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.
This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »
This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »
Certificate has a weak signature and expires after 2015. Upgrade to SHA2 to avoid browser warnings. MORE INFO »
This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »


Authentication
Server Key and Certificate #1
Subject
*.primaveraspace.com
Fingerprint SHA1: e17940dab14e322b0a5ec6eaedf893a64cb9afbe
Pin SHA256: acdQVOfqgnskyweISN1DKwzeaDv8N322OfzEjmsMSpg=
Common names
*.primaveraspace.com
Alternative names
*.primaveraspace.com primaveraspace.com
Valid from
Tue, 02 Oct 2012 01:46:05 UTC
Valid until
Tue, 04 Oct 2016 15:11:24 UTC (expires in 6 months and 17 days)
Key
RSA 2048 bits (e 65537)
Weak key (Debian)
No
Issuer
RapidSSL CA
AIA: http://rapidssl-aia.geotrust.com/rapidssl.crt
Signature algorithm
SHA1withRSA WEAK
Extended Validation
No
Certificate Transparency
No
Revocation information
CRL, OCSP
CRL: http://rapidssl-crl.geotrust.com/crls/rapidssl.crl
OCSP: http://rapidssl-ocsp.geotrust.com
Revocation status
Good (not revoked)
Trusted
Yes

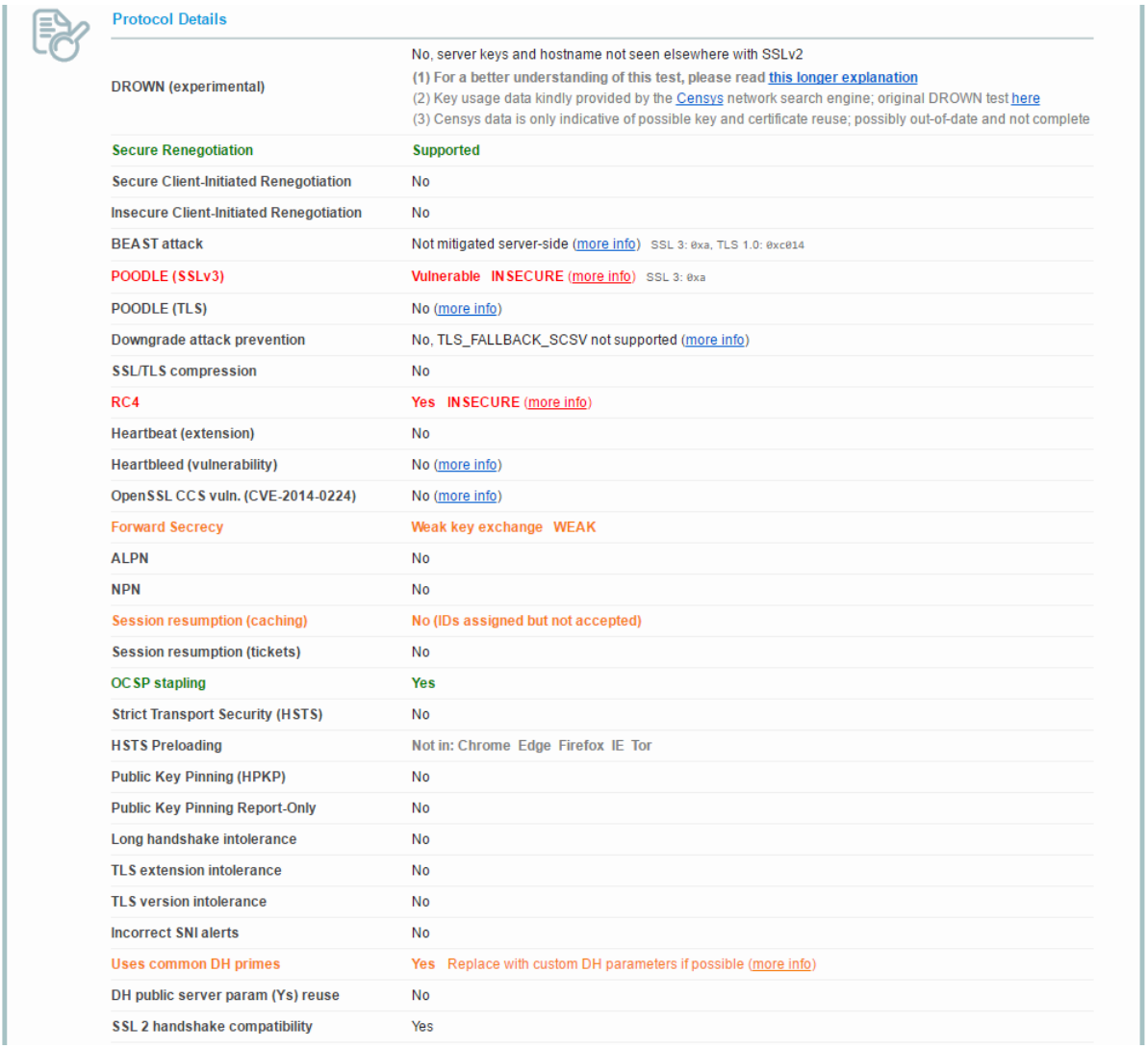
Configuration

Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3 **INSECURE**	Yes
SSL 2	No

Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)

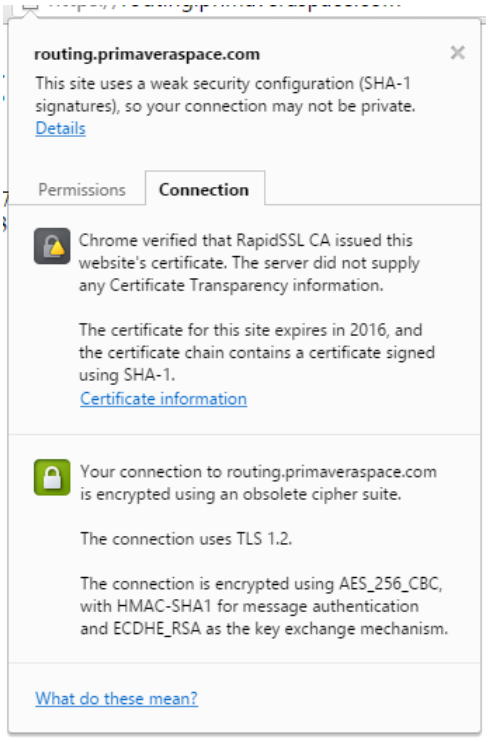
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 1024 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 1024 bits FS **WEAK**	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_RSA_WITH_RC4_128_SHA (0x5) **INSECURE**	128
TLS_RSA_WITH_RC4_128_MD5 (0x4) **INSECURE**	128



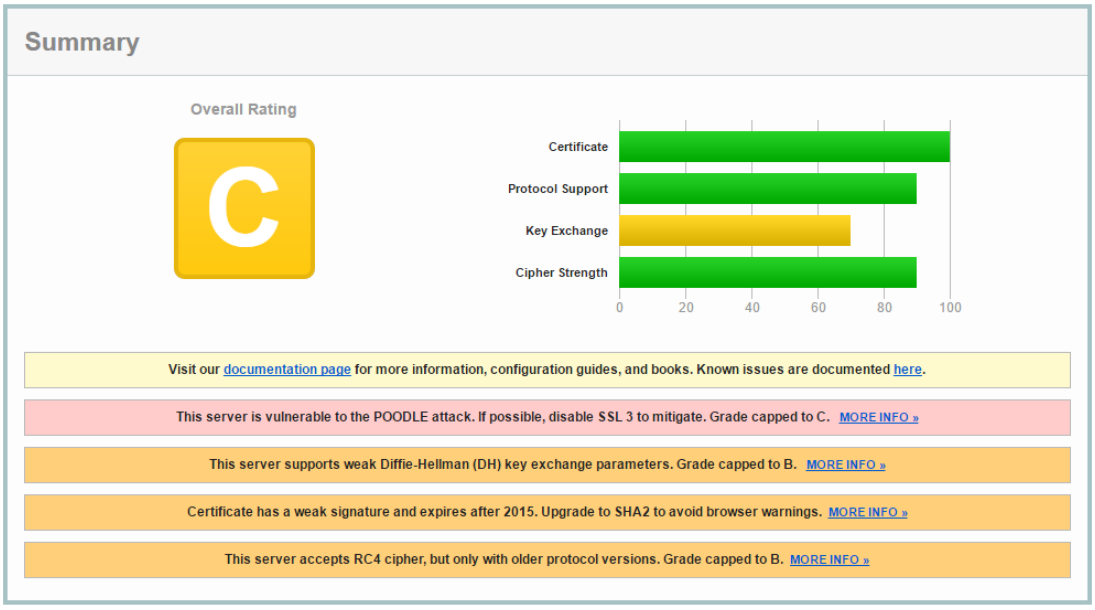
Protocol Details

DROWN (experimental)	No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN test here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: 0xa, TLS 1.0: 0xc014
POODLE (SSLv3)	Vulnerable INSECURE (more info) SSL 3: 0xa
POODLE (TLS)	No (more info)
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)
SSL/TLS compression	No
RC4	Yes INSECURE (more info)
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	Weak key exchange WEAK
ALPN	No
NPN	No
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	No
OCSP stapling	Yes
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE Tor
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	Yes Replace with custom DH parameters if possible (more info)
DH public server param (Ys) reuse	No
SSL 2 handshake compatibility	Yes

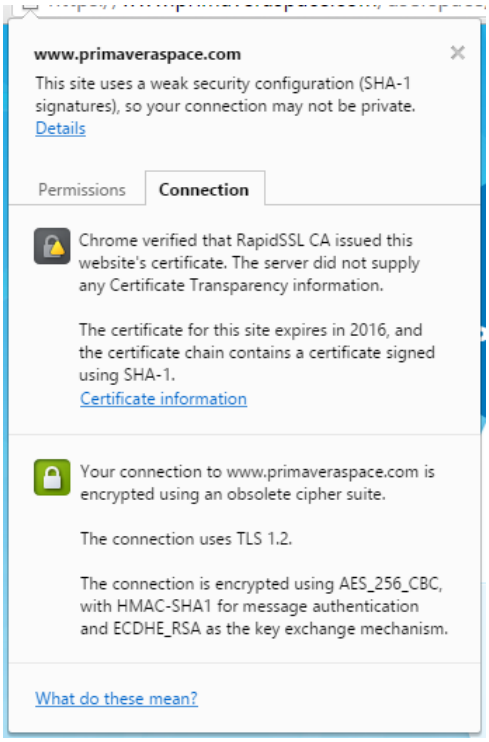
- **https://routing.primaveraspace.com/**



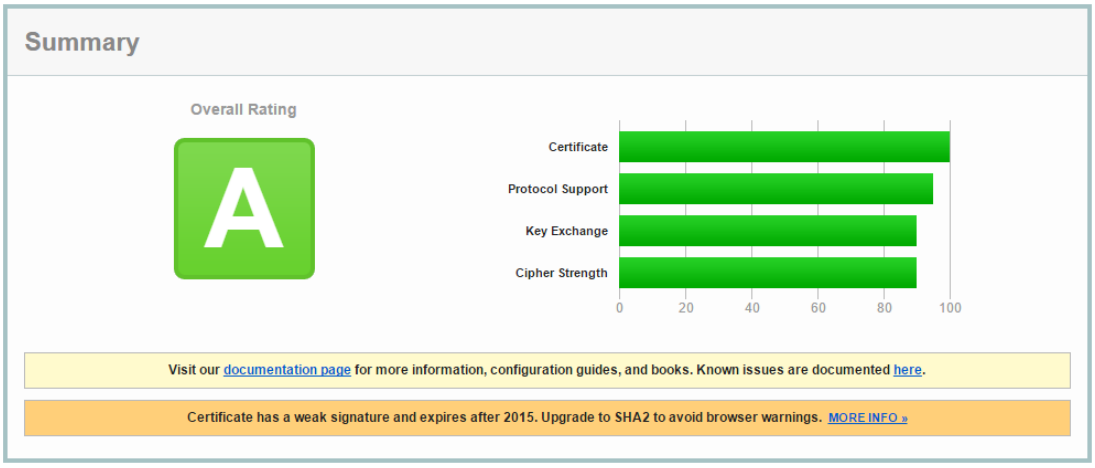
SSL Report



- **https://www.primaveraspace.com/**


www.primaveraspace.com
This site uses a weak security configuration (SHA-1 signatures), so your connection may not be private.
Details
Permissions
Connection
Chrome verified that RapidSSL CA issued this website's certificate. The server did not supply any Certificate Transparency information.
The certificate for this site expires in 2016, and the certificate chain contains a certificate signed using SHA-1.
Certificate information
Your connection to www.primaveraspace.com is encrypted using an obsolete cipher suite.
The connection uses TLS 1.2.
The connection is encrypted using AES_256_CBC, with HMAC-SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism.
What do these mean?

SSL Report


Summary
Overall Rating
A
Certificate
Protocol Support
Key Exchange
Cipher Strength
0
20
40
60
80
100
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.
Certificate has a weak signature and expires after 2015. Upgrade to SHA2 to avoid browser warnings. MORE INFO »

Configuration

Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

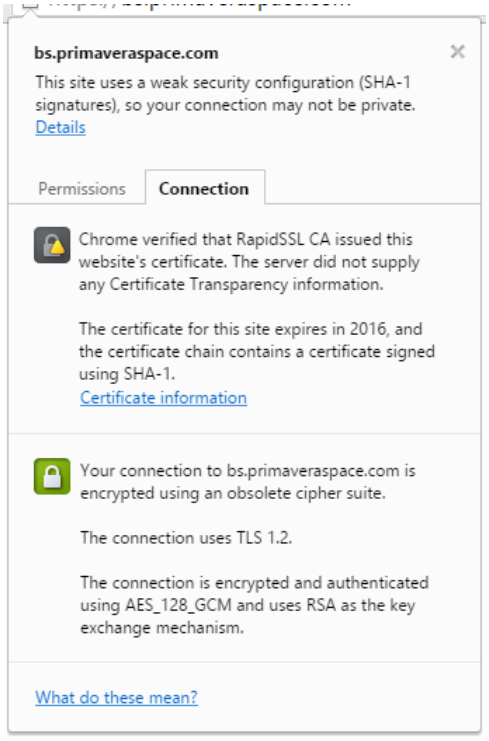
Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112

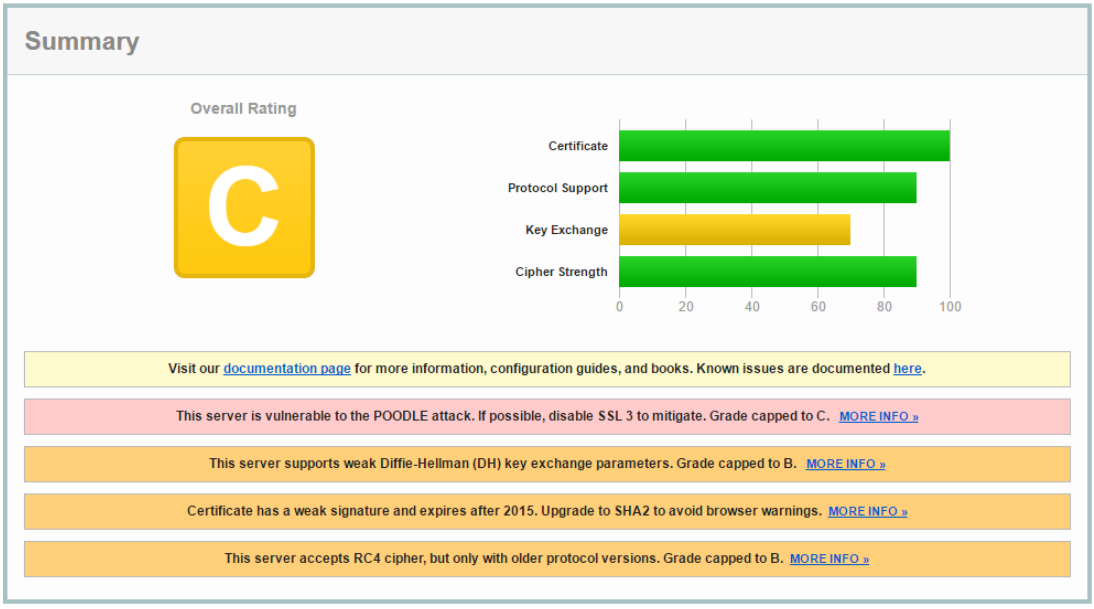
Protocol Details

DROWN (experimental)	No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN test here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	With modern browsers (more info)
ALPN	No
NPN	No
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	No
OCSP stapling	Yes
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE Tor
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
SSL 2 handshake compatibility	Yes

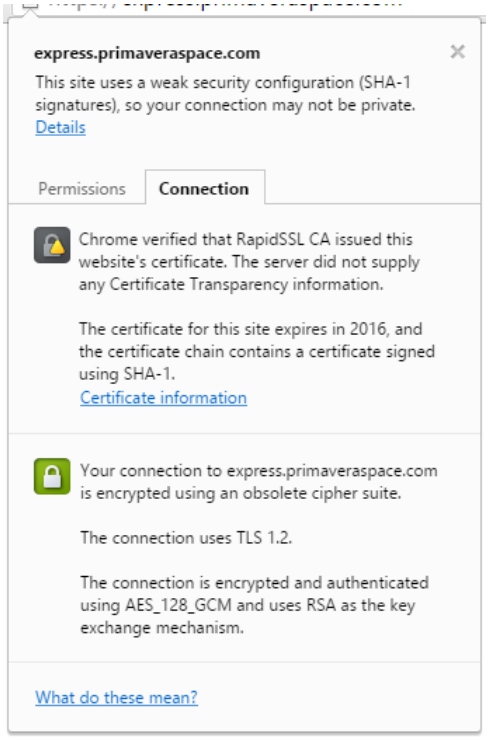
- **https://bs.primaveraspace.com/**



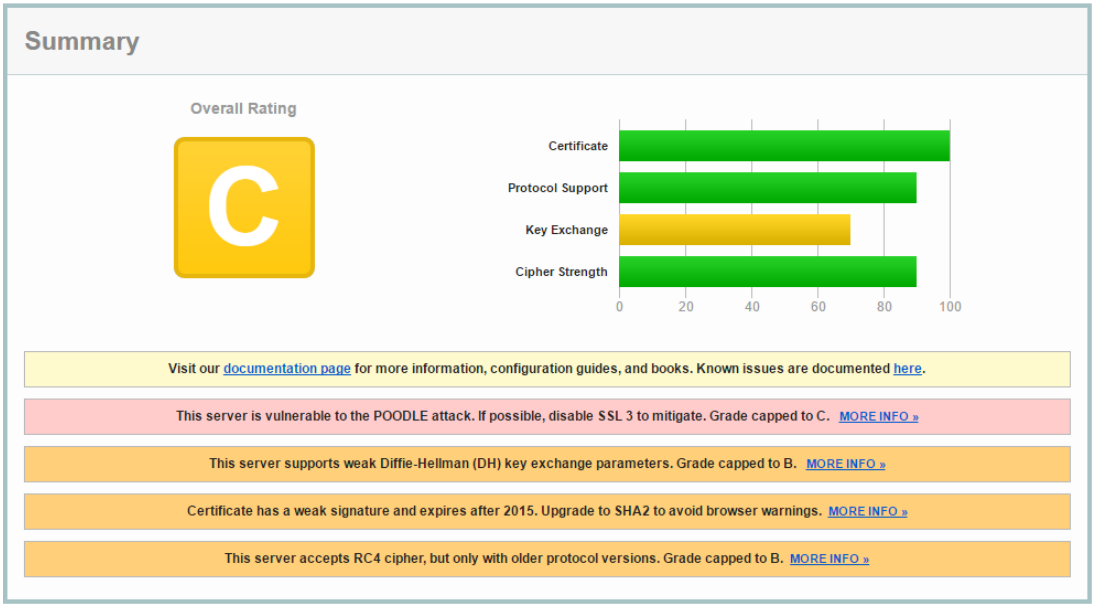
SSL Report



- **https://express.primaveraspace.com/**


express.primaveraspace.com
This site uses a weak security configuration (SHA-1 signatures), so your connection may not be private.
Details
Permissions
Connection
Chrome verified that RapidSSL CA issued this website's certificate. The server did not supply any Certificate Transparency information.
The certificate for this site expires in 2016, and the certificate chain contains a certificate signed using SHA-1.
Certificate information
Your connection to express.primaveraspace.com is encrypted using an obsolete cipher suite.
The connection uses TLS 1.2.
The connection is encrypted and authenticated using AES_128_GCM and uses RSA as the key exchange mechanism.
What do these mean?

SSL Report


Summary
Overall Rating
C
Certificate
Protocol Support
Key Exchange
Cipher Strength
0
20
40
60
80
100
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.
This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »
This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »
Certificate has a weak signature and expires after 2015. Upgrade to SHA2 to avoid browser warnings. MORE INFO »
This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »

A.3 NIST GUIDELINES FOR TLS IMPLEMENTATIOS – SP 800-52

Throughout this document, key words are used to identify requirements. The key words **"shall"**, **"shall not"**, **"should"**, and **"should not"** are used. These words are a subset of the IETF Request For Comments (RFC) 2119 key words, and have been chosen based on convention in other normative documents [RFC2119]. In addition to the key words, the words "need", "can", and "may" are used in this document, but are not intended to be normative.

(...)
3. Minimum Requirements for TLS Servers

3.1 Protocol Version Support

TLS version 1.1 is required, at a minimum, in order to mitigate various attacks on version 1.0 of the TLS protocol. Support for TLS version 1.2 is strongly recommended.

(...)

Servers that support citizen or business-facing applications **shall** be configured to support version 1.1 and **should** be configured to support version 1.2. These servers may also be configured to support TLS version 1.0 in order to enable interaction with citizens and businesses. These servers **shall not** support SSL version 3.0 or earlier. If TLS 1.0 is supported, the use of TLS 1.1 and 1.2 **shall** be preferred over TLS 1.0.

Some server implementations are known to implement version negotiation incorrectly. For example, there are TLS 1.0 servers that terminate the connection when the client offers a version newer than TLS 1.0. Servers that incorrectly implement TLS version negotiation **shall not** be used.

3.2 Server Keys and Certificates

The TLS server **shall** be configured with one or more public key certificates and the associated private keys. TLS server implementations **should** support multiple server certificates with their associated private keys to support algorithm and key size agility.

There are six options for TLS server certificates that can satisfy the requirement for Approved cryptography: an RSA key encipherment certificate; an RSA signature certificate; an Elliptic Curve Digital Signature Algorithm (ECDSA) signature certificate; a Digital Sig-

nature Algorithm (DSA)8 signature certificate; a Diffie-Hellman certificate; and an ECDH certificate.

At a minimum, TLS servers conforming to this specification **shall** be configured with an RSA key encipherment certificate, and also should be configured with an ECDSA signature certificate or RSA signature certificate. If the server is not configured with an RSA signature certificate, an ECDSA signature certificate using a Suite B named curve for the signature and public key in the ECDSA certificate **should** be used.

TLS servers **shall** be configured with certificates issued by a CA, rather than self-signed certificates. Furthermore, TLS server certificates **shall** be issued by a CA that publishes revocation information in either a Certificate Revocation List (CRL) [RFC5280] or in Online Certificate Status Protocol (OCSP) [RFC6960] responses. The source for the revocation information **shall** be included in the CA-issued certificate in the appropriate extension to promote interoperability.

(. . .)

3.2.1 Server Certificate Profile

For these guidelines, the TLS server certificate **shall** be an X.509 version 3 certificate; both the public key contained in the certificate and the signature **shall** have at least 112 bits of security. The certificate shall be signed with an algorithm consistent with the public key:

- Certificates containing RSA (key encipherment or signature), ECDSA, or DSA public keys **shall** be signed with those same signature algorithms, respectively;
- Certificates containing Diffie-Hellman public keys **shall** be signed with DSA; and
- Certificates containing ECDH public keys **shall** be signed with ECDSA.

3.3 Cryptographic Support

Cryptographic support in TLS is provided through the use of various cipher suites. A cipher suite specifies a collection of algorithms for key exchange and for providing confidentiality and integrity services to application data. The cipher suite negotiation occurs during the TLS handshake protocol. The client presents cipher suites that it supports to the server, and the server selects one of them to secure the session data.

Cipher suites have the form:

TLS_KeyExchangeAlg_WITH_EncryptionAlg_MessageAuthenticationAlg

For example, the cipher suite TLS_RSA_WITH_AES_128_CBC_SHA uses RSA for the key exchange, AES-128 in cipher block chaining mode for encryption, and message authentication is performed using HMAC_SHA12.

3.3.1 Cipher Suites

The server **shall** be configured to only use cipher suites that are composed entirely of Approved algorithms. A complete list of acceptable cipher suites for general use is provided in this section, grouped by certificate type and TLS protocol version.

In order to maximize interoperability, TLS server implementations shall support the following cipher suites:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

In addition, TLS server implementations **should** support the following cipher suites:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

In addition to supporting the cipher suites listed above, TLS 1.2 servers **shall** be configured to support the following cipher suite:

- TLS_RSA_WITH_AES_128_GCM_SHA256

TLS 1.2 servers **should** be configured to support the following cipher suites:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

O documento oficial providencia tabelas, resumos e informação sumária relativamente à seleção, manutenção e configuração do protocolo TLS.

Referência: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295