Uma Implantação de Criptosistemas Gratuitos em Projeto de Pesquisa e Desenvolvimento

Regina Paiva Melo[1], Eduardo Sakaue[1], Adilson Marques da Cunha[1]

[1] Divisão de Ciência da Computação – Instituto Tecnológico de Aeronáutica (ITA)
Pça Mal Eduardo Gomes, 50 - Vila das Acácias, - 12.228-900 São José dos Campos -SP - Brasil

{rpmdias,cunha}@ita.br,{e.sakaue}@uol.com.br

***Resumo* —** A segurança das informações digitais em sistemas computadorizados passou a ser de fundamental importância para o sucesso dos institutos de pesquisa científica e tecnológica, A partir desse contexto, adotou-se uma visão estratégica para a implantação de políticas de segurança de comunicações e operações das informações, utilizando controles criptográficos simétricos e assimétricos. Este trabalho propõe uma metodologia para implantação de políticas de controle criptográfico, utilizando softwares gratuitos, a fim de desmistificar e mostrar que soluções, de custo reduzido, são boas alternativas para prover maior confiabilidade e confidencialidade nos Projetos de P&D**.**

***Palavras-chaves* — Segurança das Informações, Criptografia, Software Gratuitos.**

I. INTRODUÇÃO

À medida que as redes de computadores se disseminaram e a internet se popularizou, a necessidade de assegurar que os dados estejam seguros cresceu significativamente. A segurança das informações digitais em sistemas computadorizados passou a ser de fundamental importância para o sucesso dos institutos de pesquisa científica e tecnológica.

No Instituto Tecnológico de Aeronáutica (ITA), existem diversos Projetos de Pesquisa e Desenvolvimento (P&D) caracterizados pela necessidade de sigilo e confidencialidade sem que os custos financeiros ultrapassem os orçamentos estipulados. Para atender a estes requisitos, fez-se necessário à implantação de um planejamento contendo políticas de segurança de informações, abordando aspectos tecnológicos, processos e pessoas.

A partir desse contexto, políticas de comunicações e operações em segurança da informação que utilizam controles criptográficos vêm sendo adotadas nos Projetos de P&D. Controles criptográficos simétricos e assimétricos foram pesquisados e testados, buscando assegurar a Confidencialidade, Integridade e Disponibilidade (CID) no armazenamento, transporte e transmissão das informações confidenciais em estações e servidores [1].

Este artigo propõe uma metodologia para a implantação de políticas de controle criptográfico, utilizando softwares gratuitos, a fim de desmistificar soluções de custo reduzido como boas alternativas para prover maior confiabilidade e confidencialidade nos Projetos de P&D do ITA. Esta metodologia deve ser estendida aos parceiros do Projeto em outros locais envolvendo, por exemplo, a Universidade Estadual de Campinas (UNICAMP); discutindo o sistema de gestão de segurança das informações, as ferramentas utilizadas, os principais resultados obtidos e seus impactos nos usuários.

Este artigo esta organizado em cinco seções. Na seção dois apresentam-se os principais conceitos de criptografia computacional; na seção três apresenta-se a metodologia de implantação de criptosistemas gratuitos; na seção quatro apresenta-se a estratégia de implantação de criptosistemas gratuitos e na seção cinco apresentam-se as principais conclusões.

II.CRIPTOGRAFIA COMPUTACIONAL

A criptografia é definida como a ciência de escrever em cifras. Em outras palavras, é um conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que apenas o destinatário a decifre e compreenda. A criptografia moderna visa uma grande quantidade de problemas. Mas o problema básico continua o clássico: garantir a comunicação segura em um meio inseguro [6].

Em geral, o algoritmo criptográfico é uma função matemática aplicada a informação, para realizar a cifragem e a decifragem dos dados. O processo de cifrar consiste em transformar dados legíveis em ilegíveis e o processo de decifrar é o contrário.

Estes processos estão baseados na utilização de chaves de acesso que interagem com os algoritmos criptográficos. As chaves de acesso possuem diferentes tamanhos e seu grau de segurança esta associada com sua extensão em bits.

Segundo [1], a criptografia é utilizada para alcançar diversos objetivos de segurança, principalmente:

- Confidencialidade - A garantia de que uma mensagem seja lida apenas pelo receptor desejado;
- Integridade- A garantia de que uma mensagem não tenha sido alterada;
- Autenticidade- A garantia de que a mensagem recebida realmente originou-se do seu emissor; e
- Irretratabilidade- A garantia do emissor não poder negar a autoria da mensagem.

A. Criptografia de Chave Simétrica

Um sistema de criptografia simétrica ou chave secreta é aquele onde o emissor e os receptores das mensagens utilizam a mesma chave para os processos de cifrar e/ou decifrar. A segurança desses algoritmos é baseada inteiramente na chave utilizada, e não em detalhes técnicos dos algoritmos [6]-[8].

No processo de criptografia simétrica, uma mensagem é cifrada no emissor por meio da aplicação de um algoritmo de criptografia, tendo a chave privada como parâmetro. Alguns algoritmos importantes são: *Data Encryption Standard* –DES; TripleDES; e *Advanced Encryption Standard* – AES [2]-[7]-[8].

O resultado desse processo consiste num conjunto de dados, que se conhece como texto cifrado. O processo de decifrar, por sua vez, ocorre por intermédio da aplicação do mesmo algoritmo de criptografia pelo receptor, tendo como parâmetro a mesma chave utilizada pelo emissor na cifra, conforme é ilustrado, a seguir na Figura 1.

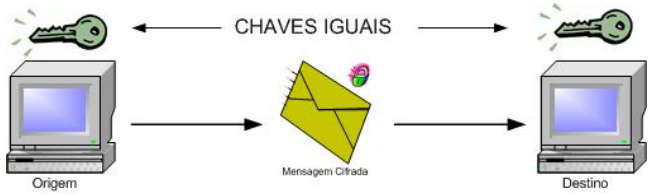

Fig. 1. Criptografia Simétrica.

B. Criptografia de Chave Assimétrica

A criptografia por chaves assimétrica é uma técnica criptográfica que utiliza um par de chaves para cada interlocutor: uma chave chamada de pública e a outra chave chamada de privada. A chave pública é distribuída livremente para todos os correspondentes com os quais se quer manter comunicação. A chave privada, por sua vez, deve ser mantida confidencial e conhecida apenas pelo seu dono.

Conforme mostrado a seguir na Figura 2, em um sistema de criptografia de chaves assimétricas, uma mensagem cifrada com uma da chave pública denominada A_y ou B_y pode somente ser decifrada pela chave privada denominada A_x ou B_x correspondente. Do mesmo modo, uma mensagem cifrada com a chave privada pode somente ser decifrada pela sua chave pública correspondente.

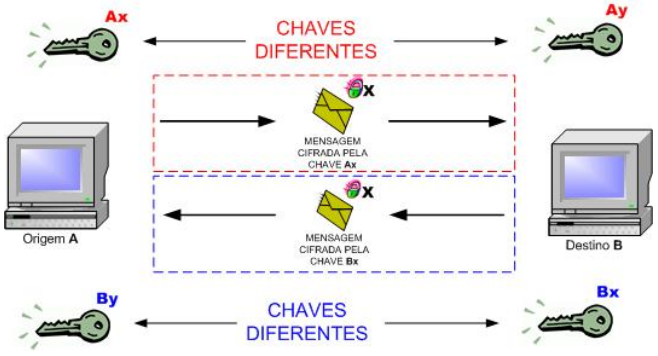

Fig. 2. Criptografia Assimétrica.

As principais características da Criptografia Assimétrica são:

- A chave pública é gerada a partir da chave privada;
- É computacionalmente impossível gerar a chave privada, a partir da chave pública;
- O gerenciamento de chaves é potencialmente mais simples do que nos sistemas baseados em chaves simétricas;
- Os algoritmos mais clássicos empregados em criptográfica de chaves assimétricas são *Rivest, Shamir e Adleman* - RSA, ElGamal, *Data Encryption Standard* - DES. O tamanho de chaves criptográficas consideradas seguras contra ataques é de no mínimo 1024 bits; e
- A grande vantagem de se adotar este método de criptografia assimétrica é que não precisa haver uma chave compartilhada para cada pessoa em um grupo, reduzindo drasticamente o número global de chaves necessárias na comunicação de grupos com mais de 3 indivíduos. Porém, cada usuário precisa compartilhar uma chave pública e esconder a sua privada.

C. Assinatura Digital e *Fingerprint*

Assinatura Digital é criada a partir de uma função *Hash* sobre a mensagem de texto. Em um sistema de assinaturas digitais construídos adequadamente, é impossível, estatisticamente, que duas mensagens diferentes apresentem assinaturas idênticas [6].

Os principais sistemas para assinatura digital utilizam combinações de algoritmos conhecidos, dentre eles o *RSA*, *DSA*, *Secure Hash Algorithm -SHA-1* e ElGamal [8].

A assinatura digital garante a autenticidade da mensagem, propiciando que a alteração de um texto seja facilmente identificada. Outra característica importante da assinatura digital é chamada de não-repúdio, pois se alguém assina digitalmente um documento, depois não poderá dizer que não o fez, isto é, não poderá repudiar a autoria, pois qualquer um poderá comprová-la a partir da chave pública do emitente.

Uma chave pública também pode ter uma assinatura denominada *fingerprint*. O *fingerprint* é apresentado como um número escrito como 32 ou 40 dígitos hexadecimais, sendo este um identificador único para cada chave.

Quando é informada um chave a alguém, esse alguém deve comparar o *fingerprint* fornecido pela chave com o informado pelo dono da chave pública, de forma a garantir a identidade do interlocutor. Este processo somente precisa ser realizado uma única vez para uma dada chave.

III. METODOLOGIA DE IMPLANTAÇÃO DE CRIPTOSISTEMAS GRATUITOS

A implantação de um sistema de gestão, primeiramente, requer a formação de uma equipe qualificada para tratar especificamente desta área cercada de desafios inovadores. Após a consolidação da equipe de segurança em um projeto elegeu-se a norma ISO/IEC 27001 como modelo de gestão de segurança a ser seguido, sem descartar outras normas importantes da área.

Na fase de análise de risco, a equipe de segurança identificou que o ativo de maior valoração é a informação digital do Projeto armazenada nos servidores e em unidades de transferência de arquivos. Posteriormente, a avaliação de risco realizada classificou esta informação com o grau de sigilo confidencial [3]. Para proteger a informação de forma adequada e apropriada, fez-se necessária à utilização de controles criptográficos eficientes.

Investigações e testes foram realizados, visando escolher uma ferramenta de software gratuita e de credibilidade, sem aumentar os riscos nem os custos financeiros. A partir desse

contexto, adotou-se uma visão estratégica para a implantação de políticas de segurança de comunicações e operações das informações, utilizando-se controles criptográficos simétricos e assimétricos.

Os principais resultados inicialmente planejados foram alcançados com a utilização de duas ferramentas de criptografia: a ferramenta de criptografia de chave simétrica *TrueCryp* [5], capaz de ocultar as informações dos arquivos do sistema; e a ferramenta de criptografia de chaves assimétrica *Gnu Privacy Guard – GnuPG* [4], baseada no padrão chamado *Open Pretty Good Privacy - Open PGP*, capaz de assegurar confidencialidade nas transmissões das informações via Internet.

Considerando as ferramentas adotadas, foram desenvolvidos manuais e realizados *workshops* objetivando a rápida compreensão dos processos criptográficos e a conscientização dos problemas em caso de exposição de informações confidenciais. Esta apresentação também melhorou a receptividade por parte dos membros do Projeto.

IV. ESTRATÉGIA DE IMPLANTAÇÃO DE CRIPTOSISTEMAS GRATUITOS

A estratégia de implantação consistiu da utilização das ferramentas adotadas, a fim de alcançar os objetivos propostos. Para tanto, testes exaustivos foram realizados pela equipe de segurança por dois meses, objetivando relatar uma metodologia rápida de utilização pelos usuários menos familiarizados e confirmar a confiabilidade das ferramentas.

A. Criptografia Simétrica

Sob o ponto de vista dos requisitos de segurança que se deseja alcançar em relação à proteção das informações contidas nos arquivos armazenados de estações e servidores dos Projetos, ou mesmo de mídias em trânsito, utilizam-se o software de criptografia simétrica *TrueCrypt* [5].

Esta ferramenta criptografou partições inteiras em qualquer dispositivo de armazenameto de arquivos. A sua utilização baseou-se na criação e utilização de arquivos como volumes virtuais (unidades, *drives* ou discos). Quanto ao tamanho da chave, ela é variável de acordo com o conjunto de algoritmos selecionados.

No software *TrueCrypt*, primeiro cria-se um arquivo. Para utilizar este arquivo é necessário montá-lo como um volume virtual que em seguida é exibido como uma unidade no gerenciador de arquivos. Ao finalizar os trabalhos, é necessário desmontar a unidade virtual.

Esta unidade virtual é sempre montada de acordo com as configurações selecionadas, como por exemplo, o tipo de algoritmo de criptografia e função *hash* escolhida e o tamanho fixo que a unidade deverá ter.

A unidade virtual pode ser criptografada através de algumas opções de algoritmos simétricos e de *hash*. A ferramenta tem capacidade de encadear algoritmos, totalizando uma chave de até 768 bits derivada de uma senha fornecida pelo usuário.

A ferramenta disponibiliza um gerador randômico de chaves que pode ser combinada com uma senha fornecida pelo usuário de no mínimo 8 (oito) dígitos.

B. Criptografia Assimétrica

Sob o ponto de vista dos requisitos de segurança que se deseja alcançar em relação às mensagens eletrônicas é a proteção contra acesso não autorizado, modificação ou negação de serviço e assinaturas eletrônicas.

Buscando atender os requisitos de segurança das mensagens eletrônicas, apresenta-se a implementação GnuPG que representa uma alternativa de software de código aberto que pode ser instalada em diversos Sistemas Operacionais (Unix, Linux, Mac OS, RISC OS e Windows). O GnuPG pode ser usado em associação a diferentes aplicativos, como por exemplo, *chats* e leitores de *e-mail* [4].

Tipicamente, o uso do sistema OpenPGP envolve dois principais componente. O primeiro é o motor criptográfico propriamente dito, do qual o GnuPG é uma implementação. O segundo componente é o de interface gráfica com o usuário – o *front-end*. Para se utilizar esse sistema de criptografia, de uma maneira mais fácil, basta escolher algum *front-end* compatível com o GPG.

O processo de gerenciamento das chaves é essencial para o uso eficaz das técnicas de criptografia. Este processo consiste na geração, distribuição e armazenamento das chaves criptográficas, onde qualquer exposição ou perda das chaves criptográficas pode levar ao comprometimento da segurança.

A equipe de segurança descentralizou a geração do par de chaves pública. Cada usuário do Projeto gerou seu par de chaves ou solicitou a um gerador a criação do par de chaves. A chave pública foi publicada na Internet para livre acesso aos membros do grupo. Depois que as chaves foram trocadas, a comunicação passou a ser criptografada e assinada entre os membros do projeto.

Foram salvas e armazenadas duas réplica do par de chaves, uma unidade virtual cifrada dentro de um DVD e da mesma forma, em um servidor, ambos protegidos fisicamente por mecanismos de segurança de acesso restrito.

V . CONCLUSÃO

Este artigo apresentou, de forma sucinta, uma metodologia de implantação de controles criptográficos para atingir as metas da política de segurança da informação nos Projetos de P&D do ITA, visando difundir o uso das tecnologias utilizadas e, conseqüentemente, aumentar a confiabilidade dos dispositivos de armazenamento e transferência de arquivos.

De maneira geral, foram explicadas as aplicações dos conceitos de controles criptográficos, tais como criptografia simétrica, funções *hash*, assinatura digital, chaves de acesso, entre outros.

O cenário da implantação dos controles criptográficos mostrou-se complexo. A princípio, ocorreram dificuldades de difusão e aceitação por quase toda a equipe do Projeto. Princípios metodológicos foram definidos e implantados para facilitar a rápida assimilação das técnicas utilizadas, conseguindo-se bons resultados e atingindo-se níveis de segurança satisfatórios com um baixo custo.

Outro ponto importante foi a necessidade da formação de uma equipe de segurança para interagir, monitorar e auditar as atividades, no âmbito da segurança das informações seguindo, um modelo de gestão definido, criando procedimentos e métodos.

REFERÊNCIAS

[1] ABNT NBR ISO/IEC 27001:2006, Tecnologia da informação - Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.
[2] *Data Encryption Standard*, FIPS Publication 46, NBS, U.S. Departament of Commerce, 1977.
[3] Salvaguarda de Assuntos Sigilosos: Proteção ao Conhecimento - Legislação Vigente - Série Coletânea de Legislação nº4 – ABIN/DF.
[4] http://www.gnupg.org/.
[5] http://www.truecrypt.org/
[6] BELLARE, M.; ROGAWAEY P. **Introduction to Modern Cryptography.** San Diego: University of California, 2008. Notas de Aula da Disciplina CSE 207. Disponível em: <http://www-cse.ucsd.edu/users/mihir/cse20 7/classnotes.html>
[7] COOPER, J. A. **Computer & Communications Security Strategies For the 1990s**, McGraw-Hill, 1989.
[8] LINDELL, Y. **Introduction to Cryptography.** Israel: Bar Ilan Univerity, 2008. Notas de Aula. Disponível em:<http://www.cs.biu.ac.il/~lindell/89-656/Intro-to-crypto-89-656.pdf>