Estudo das vulnerabilidades em sistemas onde a segurança se baseia no princípio da "Segurança através da Obscuridade"

Thiago C. Sandoval - Número USP 3286381

Claudio Penasio Junior - Número USP 5223770

Resumo

Neste artigo serão abordados os conceitos de "Segurança através da Obscuridade", a fragilidade de sistemas onde a segurança é baseada neste princípio, as alternativas a esse conceito e a discussão de casos notórios que ilustram o tema. Onde sua principal motivação é fornecer subsídios para uma base de argumentação na produção de objetos jurídicos para casos onde este tipo de "Segurança através da Obscuridade" é um dos elementos da perícia.

Abstract

In this paper the concepts of "Security through the Obscurity" will be boarded, the fragility of systems where the security is based on this principle, the alternatives to this concept and the quarrel of well-known cases that illustrate the subject. Where its main motivation is to supply subsidies a base of argument in the legal object production for cases where this type of "Security through the Obscurity" is one of the elements of the skill.

Palavras chaves: segurança, obscuridade, vulnerabilidade, criptografia.
Keywords: security, obscurity, vulnerability, cryptography.

Introdução

Diversos sistemas atuais baseiam sua segurança no princípio da "Segurança através da Obscuridade", e é importante compreender o que é esse princípio e suas implicações para que seja possível analisar em que situações este tipo de segurança é desejável e quando não o é.

Neste artigo pretendemos defender a tese de que "a segurança por obscuridade depende apenas de um segredo", essa tese pode visualizada com maior facilidade quando imaginamos um sistema qualquer onde sua segurança é baseada na ignorância por parte de seus usuários a respeito de seu modo de funcionamento, com base nisso afirmamos que se um de seus usuários passa a conhecer esse "segredo", todo o sistema está vulnerável pelo simples fato de que todos os outros usuários acreditam que estar seguros.

A Segurança através da Obscuridade

Para entender o conceito de segurança através da obscuridade, precisamos antes definir o que é segurança e em que condições a segurança é importante. Veremos também como a obscuridade pode ser aplicada para fornecer segurança a um sistema ou situação.

Segurança pode ser entendido como a garantia da preservação de um estado, condição ou situação. Por exemplo, a preservação da integridade física de um presidente durante um discurso, ou a garantia de que determinadas informações sejam acessíveis apenas a determinadas pessoas.

Sendo a segurança a garantia da preservação de um estado, ela é importante na medida em que essa preservação é importante. Nos casos em que tal preservação é essencial, como o acesso a uma conta bancária restrito ao correntista, a segurança passa a ser essencial.

A obscuridade, relacionada à segurança, pode ser entendida como a falta de informação sobre o contexto em que o estado a ser preservado se encontra, ou até mesmo sobre o próprio estado em questão.

Metodologia de teste

Para um sistema com segurança baseada em obscuridade qualquer, estabelecer uma metodologia de teste sistemática e reproduzível é difícil, senão impossível, pois a falta de informação sobre o sistema dificulta o estabelecimento de um critério para a definição de um conjunto de testes qualquer.

Portanto, dado um conjunto de testes em que o sistema falhe, corrigir a falha de segurança encontrada não garante que outras falhas anteriores não detectadas ainda existam, ou que novas falhas de segurança não tenham sido criadas com a alteração feita no sistema para corrigir a falha exposta.

Em face desse problema, o critério mais razoável a ser adotado para testar um sistema onde a segurança é baseada na obscuridade é realizar o maior número de testes possíveis. Isso deixa muito a desejar, pois não é uma abordagem nem científica e nem quantificável.

Outra característica indesejável dessa abordagem é a garantia pela falta de contra-exemplo. Qualquer afirmação sobre a qualidade de determinada segurança pode ser feita e assumida como verdade até que se prove o contrário, o que é extremamente difícil devido à falta de metodologia para analise.

A fragilidade de sistemas onde a segurança é baseada na obscuridade

Levando em conta a impossibilidade de quantificação de o quanto um sistema onde a segurança é baseada na obscuridade é seguro, devido à impossibilidade de se criar uma metodologia de testes confiável, podemos crer que um sistema baseado neste princípio tenha toda a garantia de sua segurança baseada em uma crença de que o segredo que garante sua integridade será sempre bem guardado. Em função disso podemos afirmar que um sistema onde a segurança de seus dados é baseada em uma crença, que com um pouco de reflexão pode ser traduzida em uma esperança de que os detentores do segredo nunca o revelem, a nossos olhos é um sistema extremamente frágil.

Há um grande número de pessoas que admitem que a segurança através da obscuridade ainda é melhor do que nada, é esse o caso de quem, por exemplo, guarde a chave de casa embaixo do tapete da porta. Outro grupo defende que este tipo de atitude resulta em uma segurança semelhante a deixar a porta destrancada, pois quem quiser entrar, após tentar abrir a porta,

fatalmente irá dar uma olhada embaixo do tapete. Neste caso o dono da casa, que é o interessado na segurança do sistema, sabe que a segurança de sua casa está baseada em um segredo. O que não acontece com a maioria dos usuários de sistemas computacionais que utilizam sistemas baseados nesse tipo de segurança, e o que acontece fatalmente é que quando esse segredo é revelado a um membro desse grupo, toda a segurança fica comprometida, porém todos continuam acreditando na confiabilidade do sistema por desconhecer que o segredo já foi revelado.

Alternativas a obscuridade

A única alternativa realmente eficaz para a obscuridade é justamente sua antítese, ou seja, você só saberá se seu sistema é realmente seguro se todos souberem como ele realmente é construído nos mais profundos detalhes, e ainda assim ele permanecer seguro. Essa é a base da robustez de todo software de código fonte aberto. No software de código fonte aberto todos que tiverem interesse podem saber o que há em seu interior, isso faz com que um número muito maior de usuários testem esse software, e os bugs de segurança sejam de conhecimento de todos, para que possam ser corrigidos por um número muito maior de programadores. Esse processo caótico é muito bem explorado por Eric S. Raymons em [3], e é a principal garantia de que o software foi exaustivamente testado, que não há segredos em seu código, e ainda assim ele é seguro. Em [5], onde é explicada a lei de Kerckhoff, que diz basicamente que um sistema deve ser seguro ainda que todo seu conteúdo seja conhecido com exceção de sua chave de encriptação. Existem vários exemplos de sistemas que possuem concorrentes similares tanto em código aberto como em código proprietário, e são recorrentes os casos em que o de código aberto possui uma segurança muito mais robusta, estes e outros casos são explorados na seção “Casos Notórios”.

Casos Notórios

Talvez um dos casos mais conhecidos sobre esse assunto seja o relatado em [2], que revela que uma funcionalidade de criptografia de um popular programa de planilha eletrônica foi quebrada anos atrás, quando um programador percebeu que o programa armazenava a mesma seqüência de caracteres em posições fixas dentro de um arquivo criptografado. Pelo fato deste programador saber exatamente onde aqueles caracteres estavam, quando quisesse decodificá-los, e em função da planilha usar um método muito rudimentar de codificação, ele podia apenas olhar o código e decodificá-la sem utilizar a chave para isso. Este programador escreveu uma aplicação que automaticamente decodificava toda a planilha sem a necessidade da chave. Neste momento o programador avisou o fabricante da planilha que sua função de criptografia possuía um bug de segurança. Ele esperava com isso que o fabricante informasse seus consumidores sobre o bug, e lançasse uma correção a esse problema.

O fabricante das planilhas eletrônicas tentou resolver o problema através da *segurança pela obscuridade.* Ele ameaçou o programador com um processo ou ação criminal se ele revelasse o método de quebrar o código. Porque outro programador descobriu o método apenas com uma dica de que aquele código era facilmente quebrável, o fabricante também ameaçou este programador com um processo ou ação criminal caso ele contasse a alguém que a função de criptografia era facilmente quebrável. Este caso ilustra como a *segurança pela obscuridade* é um péssimo negócio.

Outro exemplo citado no documento [2], é o fato do governo americano proibir a exportação de softwares com criptografia “forte”, achando que as pessoas de outras nações não são espertas o suficiente para produzir softwares similares.

Outro caso é descrito por Eric Raymond em [4], onde ele comenta o incidente de roubo e publicação do código fonte do (IOS router firmware) Sistema Operacional que acompanhava o firmware nos roteadores da marca Cisco, e que isso poderia significar uma onda de “exploits” contra a infra-estrutura de grande parte da Internet. Neste caso o autor comenta o fato da Cisco ter ignorado a Lei de Kerckhoff [5], e em função disso agora quem pagaria o preço seriam os usuários. O autor neste caso também comenta que se o IOS fosse constituído de código fonte aberto, poderíamos acreditar pelo menos que ele já teria passado pelo teste dessa lei.

Observações finais

A segurança baseada na obscuridade pode dificultar a exploração de uma falha, mas não é uma medida de segurança confiável e científica. Conforme discorrido nas seções anteriores, ficou claro que a impossibilidade de se quantificar a segurança fornecida pela obscuridade torna a mesma imprópria para alicerçar a segurança de qualquer sistema.

De forma antagônica a este princípio, a exposição de um sistema por si só não garante sua segurança. Porém, quanto mais exposto um sistema é, mais fácil fica modelar e analisar sua segurança de forma metódica e científica. Um exemplo são os algoritmos criptográficos atuais, que já são conhecidos pelo público há muito tempo e vêm tendo sua segurança testada de forma metódica e direcionada para seus pontos fracos potenciais. Algumas vezes falhas são encontradas, levando a criação de sistemas ainda mais seguros. Outras vezes a segurança do sistema passa pelos testes, comprovando sua validade e utilidade.

Referências Bibliográficas

1. Wikipedia http://en.wikipedia.org/wiki/Security_through_obscurity
2. Perens, B. 1998 Parens, Bruce. Artigo site Slashdot de 20 de julho de 1998, “Why Security Through Obscurity Won't Work” (http://slashdot.org/features/980720/0819202.shtml) acessado em 04/04/2005.
3. Raymond, E, S. 2000 Raymond, Eric Stevens, The Cathedral and the Bazaar, (http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/), acessado em 01/04/2005.
4. Raymond, E, S. 2004 Raymond, Eric Stevens, If Cisco ignored Kerckhoffs's Law, users will pay the price, 2004,(http://lwn.net/Articles/85958/), acessado em 06/04/2005.
5. Kerckhoffs, A. 1883 Auguste Kerckhoffs, Kerckhoffs' second law, http://en.wikipedia.org/wiki/Kerckhoffs%27_law acessado em 10/04/2005.