Autenticação Utilizando Senhas Descartáveis Baseadas em Caos

Fabiano Goellner dos Santos[1] **, Júlio da Silva Dias**[2*]**,**
Ricardo Felipe Custódio[1] **,**
Carlos Roberto De Rolt[2]

[1]Laboratório de Segurança em Computação – Universidade Federal de Santa Catarina
Caixa Postal 476 – 88040-900 Florianópolis, SC

[2]Universidade do Estado de Santa Catarina
Av. Madre Benvenuta, 2037 – 88035-001 Florianópolis, SC

{goellner,jdias,custodio}@inf.ufsc.br

rolt@bry.com.br

Abstract. *Client authentication process through public networks reveals several problems that compromises many applications. We propose and implement an authentication method based on a challenge-response protocol with an one-time password calculated through the use of quadratic functions. It is also discussed the use of virtual keyboards. This authentication method is used by financial institutions in order to achieve secure authentication. We present a new virtual keyboard layout and functional procedure to fulfill authentication security requirements.*

Resumo. *O processo de autenticação de usuários perante um sistema utilizando redes de comunicação de dados públicas apresenta diversos problemas que comprometem o uso de várias aplicações. Apresentamos uma proposta desenvolvida para a autenticação em sistemas de informação distribuídos. Este mecanismo utiliza um protocolo desafio-resposta com senhas de uso único geradas a partir de uma função quadrática. Neste trabalho apresenta-se também um estudo sobre os mecanismos utilizados pelas instituições financeiras na tentativa de tornar segura a autenticação de usuários, os teclados virtuais. São analisadas as implementações atuais, assim como evoluções propostas para este modelo para que os requisitos de segurança necessários sejam atendidos.*

1 Introdução

Sistemas de informação distribuídos estão presentes em várias áreas da sociedade. Estes sistemas tem agilizado o processamento de informações, gerando economia de recursos financeiros e facilitando o acesso e seu uso por parte dos usuários. Entretanto, para que estas aplicações distribuídas possam ser utilizadas de forma segura elas necessitam que o atendimento de alguns requisitos tais como autenticidade, confidencialidade, não-repúdio e tempestividade.

*Apoiado pela Universidade do Estado de Santa Catarina e CAPES.

A confidencialidade, ou sigilo das informações tanto no armazenamento quanto na transmissão é obtida através do uso de técnicas criptográficas [Kent and Atkinson, 1998a, Kent and Atkinson, 1998b, Dierks and Allen, 1999]. O não-repúdio tem sido alcançado através do soluções utilizando *software* e *hardware* [Austrália et al., 1998]. A tempestividade é garantida através de autoridades de datação que fornecem a referência temporal necessária [Pasqual et al., 2002]. O uso de funções resumo criptográficas e assinaturas digitais garantem o atendimento do requisito integridade e em alguns casos a autenticidade [Stinson, 2002].

O presente trabalho trata especificamente da autenticação de usuários perante sistemas de informação distribuídos, que utilizam redes de computadores como canal de comunicação, tais como aqueles disponibilizado pelas instituições financeiras ou bancos, que propiciam aos seus clientes a facilidade de efetuarem transações utilizando a Internet. Este serviço conhecido como *Home Banking*, tem como requisito de segurança a autenticação, uma vez que é a partir desta que os usuários tem acesso a serviços e informações. A autenticação pode ser realizada através de diversos fatores tais como algo que se sabe, algo que se tem, algo que o usuário apresenta de forma única, localização temporal, localização espacial ou existência de testemunhas. A autenticação utilizando algo que se sabe faz uso de informações compartilhadas entre o usuário e a autoridade de autenticação. Neste caso as partes envolvidas na autenticação compartilham um segredo, a senha. A identificação utilizando algo que se tem, é feita através de algo que somente o usuário possui, um cartão magnético, smart-card ou outro dispositivo físico que reconhecidamente está de posse do usuário. A autenticação utilizando alguma característica própria do usuário é realizada normalmente utilizando técnicas biométricas tais como reconhecimento facial, da íris ou impressões digitais. A autenticação utilizando localização temporal é baseada na data e na hora em que o usuário se apresenta perante o sistema. Este procedimento utiliza uma Protocoladora Digital de Documentos Eletrônicos (PDDE) para atribuir a data e hora. A autenticação por localização espacial baseia-se na posição geográfica da entidade que pode ser obtida através de dispositivos GPS. A autenticação testemunhal é obtida através da presença física perante uma ou mais testemunhas que atestam a identidade do usuário. Para dificultar fraudes no momento da autenticação perante o sistema, e por conseqüência aumentar a segurança, dois ou mais destes fatores de autenticação podem ser utilizados em conjunto [Smith, 2002].

A autenticação utilizando algo que se sabe, mais especificamente senha reutilizável, é a forma mais comum de autenticação. A identidade do usuário é confirmada uma vez que o usuário demonstre perante o sistema o conhecimento desta informação. A senha é normalmente fornecida utilizando-se somente um teclado, sem a necessidade do uso de dispositivos adicionais. Esta senha tem seu valor determinado pelo usuário ou fornecido pelo sistema e se mantém fixa por longos períodos de tempo. Este tipo de abordagem, apesar da simplicidade, é vulnerável a diversos tipos de ataques. As senhas podem ser facilmente obtidas por terceiras partes maliciosas através da observação do usuário digitando os caracteres no teclado, da utilização de programas, os *sniffers*, que observam a comunicação de dados e registram as senhas utilizadas nos processos de autenticação ou então de ataques físicos como a inserção de dispositivos entre o teclado e o computador coletando as teclas pressionadas pelo usuário, incluindo nomes de usuários e senhas. Os meios utilizados para realizar a autenticação apresentam uma série de vulnerabilidades, mas também deve-se considerar o fator humano que é vítima de ataques utilizando

engenharia social nas quais o usuário, acreditando na entidade maliciosa, fornece dados sigilosos como senhas e números de cartões de crédito, que são posteriormente utilizadas em fraudes. Como exemplo de ataques utilizando engenharia social temos telefonemas de suposto gerente de banco ou técnicas de *scam*, onde mensagens de correio eletrônico conduzem o usuário a um sítio clonado de uma instituição bancária onde os dados sigilosos são solicitados. Além da fragilidade do processo, estas senhas ainda possuem outro grande problema, podem ser esquecidas pelo usuário, que muitas vezes tem que memorizar várias senhas. Isto faz com que muitas vezes as senhas sejam escritas para que possam ser utilizadas posteriormente, o que faz com que a informação possa ser roubada sem grande esforço [Anderson, 2001].

Uma forma de evitar o envio de senhas através da rede é a autenticação utilizando protocolos desafio-resposta. Neste caso o servidor de autenticação envia um desafio ao usuário que deve processar a informação recebida utilizando para tal a senha compartilhada com o servidor. A resposta é enviada ao servidor que pode então confirmar a identidade do usuário [Devegili and Parente, 2003] e permitir o uso dos recursos do sistema. Esta abordagem, apesar de aumentar o grau de segurança, ainda é vulnerável a ataques de captura de teclas.

As instituições financeiras, devido à fragilidade na utilização das senhas para a realização da autenticação perante os sistemas de informação distribuídos, desenvolveram uma forma de autenticação visual chamada teclado virtual. O teclado virtual é um sistema de autenticação no qual o cliente utiliza como interface o terminal de vídeo e um *mouse*, sem a necessidade de utilização do teclado [Brasil, 2003]. Isto faz com que ao invés de receber códigos relativos as letras ou números do teclado, o servidor receba códigos dos botões impressos na tela. Este sistema foi desenvolvido para que o usuário, com o uso do apontador do *mouse*, consiga informar a senha necessária para sua autenticação. O teclado virtual busca sanar o problema de ataques contra a entrada de dados via teclado do computador, tornando o processo mais seguro [Bradesco, 2003]. Este mecanismo busca atingir um grau de segurança aceitável a um custo acessível, mas constata-se que este não é imune a ataques como cavalos de tróia ou captura de telas.

Há ainda técnicas que utilizam senhas descartáveis *(one-time password)*, desenvolvidas como forma de impedir ataques físicos como captura de teclas ou de monitoração da rede por *sniffers*. Uma proposta inicial para um mecanismo deste tipo foi apresentada por Lamport [Lamport, 1981]. A RFC2289 [Haller et al., 1998] especifica uma forma de implementação deste mecanismo através de um protocolo desafio-resposta. Neste caso o servidor envia uma informação como desafio. Este desafio é recebido pelo cliente, que o concatena com a senha secreta. Sobre este valor é aplicada uma função resumo criptográfico, gerando a senha descartável a ser utilizada pelo cliente somente nesta seção. O servidor realiza um cálculo semelhante e verifica se o valor recebido do cliente corresponde ao calculado localmente. Se o valor recebido for válido, o cliente é autorizado a utilizar o sistema. Neste caso o usuário não fica imune à ataques físicos de captura de teclas uma vez que a senha secreta deve ser fornecida ao sistema local pelo usuário. Um processo é semelhante é utilizado pelo produto da RSA, o SecureID [RSA, 2004]. O RSA SecureID utiliza uma forma de autenticação com dois fatores, um segredo compartilhado entre as partes e o *token*, que é um dispositivo físico que somente o usuário tem. O *token* gera senhas descartáveis baseadas em informação compartilhada com um servidor

de autenticação e o instante de tempo no qual a autenticação será realizada [RSA, 2004]. Neste caso a senha descartável é gerada pelo cálculo de uma função resumo criptográcia sobre a concatenação do segredo mantido secreto pelo *token* com uma informação temporal também fornecida pelo *token*. O cliente informa ao servidor de autenticação o valor obtido visualmente do *token*. O servidor realiza um cálculo semelhante, autenticando o usuário com base na resposta correta que depende do *token*, que deve estar de posse do cliente. As senhas capturadas por entidades maliciosas não podem ser utilizadas posteriormente, pois a cada nova conexão, ou identificação, uma nova senha é calculada [Manber, 1994].

Neste trabalho apresentam-se falhas dos mecanismos de autenticação utilizando teclados virtuais. São apresentadas também novas configurações de teclados virtuais que solucionam parcialmente os problemas apresentados. A implementação destas propostas mostrou que o atendimento integral do requisito de segurança autenticação não é possível. Propõe-se também uma solução utilizando protocolo desafio-resposta, com senhas descartáveis calculadas a partir de uma função quadrática ao invés de uma função resumo criptográfica.

O estudo dos sistemas utilizados atualmente levou à determinação dos requisitos de segurança que são apresentados na seção 2. A partir dos requisitos de segurança foram propostas, na seção 3, novas abordagens a serem utilizadas na implementação de teclados virtuais. Um mecanismo baseado em protocolo desafio-resposta e senhas descartáveis é proposto e apresentado na seção 4. Os protótipos desenvolvidos para a validação dos modelos propostos são apresentados na seção 5.

2 Requisitos de Segurança

A autenticação de usuários é um processo de alto risco e de difícil execução. Várias abordagens estão presentes na literatura. Este trabalho trata exclusivamente da autenticação de usuários perante sistemas que utilizam como canal de comunicação entre as partes, redes de comunicação de dados públicas como a Internet. Mais especificamente, o trabalho busca apresentar uma alternativa ou mecanismo complementar aos teclados virtuais utilizados atualmente pelas instituições financeiras.

O estudo deste tipo de aplicação, que necessita de autenticação de usuários e está inserido em um ambiente hostil, permite listar os seguintes requisitos:

Req-1. deve ser possível identificar o usuário perante o servidor, e o servidor perante o usuário do sistema de forma única;
Req-2. o usuário deve demonstrar sua identidade ao sistema sem que a sua senha seja revelada a possíveis entidades maliciosas;
Req-3. os elementos que possíveis atacantes obtenham através de programas ou equipamentos eletrônicos não devem garantir acesso ao sistema;
Req-4. não devem ser necessários equipamentos de alto custo ou alta complexidade.

A proposta é composta de dois elementos, o primeiro se refere à uma nova configuração para teclados virtuais e o segundo a um protocolo desafio-resposta que produz senhas descartáveis. Os sistemas propostos buscam atender aos requisitos apresentados.

3 Proposta de Configuração de Teclado Virtual

As novas configurações para teclados virtuais foram desenvolvidas com o objetivo de aumentar o grau de segurança no processo de autenticação de usuários.

As configurações utilizadas pelos teclados virtuais atuais apresentam um baixo grau de aleatoriedade, sendo portanto vulneráveis a qualquer ataque que capture telas, movimentos e ações do dispositivo apontador, *mouse*.

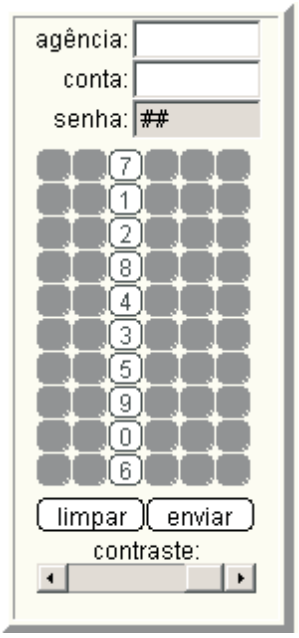

Figura 1: Visualização do funcionamento das caixas, onde apenas a caixa correspondente ao dígito está aberta.

A primeira configuração testada foi o Teclado Virtual com Caixa, que utiliza várias caixas, cada uma com 10 botões. Estes botões contém os números de 0 a 9, de forma aleatória e não repetida conforme ilustra a Figura 1. Cada coluna corresponde a um dígito da senha do usuário, ou seja, se a senha do usuário possui 6 dígitos o teclado virtual possuirá 6 colunas. No momento inicial do teclado, apenas a caixa correspondente ao primeiro dígito esta habilitada, depois de selecionado o número na caixa inicial, esta se fecha e a próxima caixa é aberta para a escolha do próximo dígito da senha do usuário e assim por diante. Este teclado proposto mantém as características de escolha de contraste, vista nos teclados virtuais implantados pelos bancos. E acrescenta um evento de *mouse*, fazendo com que as informações desapareçam assim que ele se situar sobre a caixa de botões, o que dificulta ainda mais a fraude. Esta funcionalidade foi implementada recentemente em alguns teclados virtuais. O objetivo deste teclado é fazer uso das várias caixas de modo que a realização do ataque só será possível com a captura, pelo atacante, de uma tela para cada caixa aberta a digitação. Isto dificulta a obtenção da informação escolhida, mas não inviabiliza um ataque de captura de telas.

O Teclado Virtual com uma Roda é apresentado na Figura 2, e utiliza movimentos circulares dos botões para impedir que uma entidade maliciosa, com a captura da tela, consiga chegar a construção da informação inserida. Fazendo movimento constante dos botões do teclado, ele tenta apresentar um novo fator aleatório ao processo, ou seja, fica em movimento constante como uma roda, em uma velocidade mais baixa que permita ao usuário selecionar o botão sem maiores problemas.

Um possível atacante deverá capturar um número maior de telas e rastrear todos os movimentos do dispositivo apontador desde o carregamento do teclado virtual até o momento de digitação da

senha. Com o movimento constante e aleatoriedade na criação dos números no círculo, o trabalho do atacante é dificultado. Este teclado mantém as mesmas características do teclado com caixas com a técnica de contraste e do evento do *mouse* sobre o botão do teclado. Este teclado possui ainda algumas limitações, pois como a ordem dos botões do teclado não é alterada desde sua criação, é possível ataque de captura de telas e rastreamento de movimentos do apontador.

Figura 2: Visualização do funcionamento do teclado virtual em movimento com a roda de números aleatórios.

A configuração de teclado virtual que apresentou melhor resultado foi o **Teclado Virtual com duas Rodas** que é apresentado na Figura 3. Um grau maior de aleatoriedade foi inserida através uma segunda roda. Os números das duas rodas podem ser transferidos de uma roda para outra no ponto de contato entre ambas. Este fato expõe aleatoriedade aos botões, que além de apresentar movimento constante não apresentam uma configuração estática. A falta de previsibilidade apresentada por esta configuração faz com que um possível atacante tenha que coletar um grande volume de dados para conseguir rastrear a posição dos números visando obter os caracteres pressionados. Deve-se considerar a dificuldade do usuário utilizar o mecanismo pelo fato de ter que perseguir a tecla a ser pressionada com o *mouse*, dificultando a entrada de informações por pessoas com dificuldades motoras ou até mesmo com problemas visuais. Considera-se que este mecanismo atende parcialmente aos requisitos, já que um atacante que possa capturar grande quantidade de telas do terminal de vídeo e registrar os movimentos e ações do *mouse* pode facilmente capturar os números digitados.

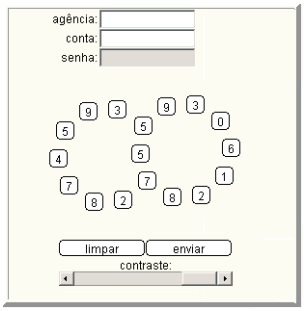

Figura 3: Visualização do funcionamento do teclado virtual com dois círculos permitindo uma maior aleatoriedade.

A implementação destas configurações leva à constatação de que novos elementos aleatórios devem ser inseridos e de que os teclados virtuais sozinhos não são uma boa forma de autenticação para sistemas interligados por redes.

4 Proposta de Autenticação Baseada em Caos

Buscando resolver os problemas decorrentes do uso dos teclados virtuais, desenvolvemos uma proposta para autenticação que consideramos eficiente para atender ao requisito de segurança na autenticação e também no uso facilitado da aplicação pelo usuário. Chamaremos esta proposta de Autenticação Baseada em Caos, que consiste no uso de

equações quadráticas para a geração de senhas descartáveis.

A **autenticação baseada em caos** tem como característica principal a dificuldade de um possível atacante encontrar a relação entre a senha do cliente e o número digitado no teclado virtual para a autenticação. O sistema perante o qual se pretende autenticar utiliza um protocolo do tipo desafio-resposta, enviando um número randomicamente selecionado ao cliente, que conhecendo sua senha e uma função quadrática, gera uma resposta, que é então enviada ao servidor. A função quadrática deve se comportar como um gerador de números pseudo-aleatórios. A forma de alcançar este objetivo foi utilizando uma função quadrática que apresenta comportamento caótico quando os seus coeficientes são selecionados apropriadamente e esta é executada iterativamente.

O presente trabalho utiliza a função logística $X_{n+1} = \lambda.X_n(1 - X_n)$, onde λ é uma constante positiva e o ponto inicial X_0 fica no intervalo $[0, 1]$.

A solução numérica da função para determinados valores de λ, dado um X_0 inicial, gera uma seqüência $\{x\}$. Para estes valores de λ, esta seqüência converge para um valor X_n.

Há uma situação específica desta equação, na qual tomamos um valor de λ entre $3,57$ e $4,00$. Com valores de λ neste intervalo, a equação apresenta um comportamento aleatório, não havendo convergência para um valor único. Os valores da seqüência gerada, $\{x\}$, apresentam comportamento caótico. Pode-se considerar este sistema como um gerador de números aleatórios. É esta a propriedade que nos interessa para a construção do protocolo de autenticação. Visando manter a aleatoriedade dos números gerados pela equação, deve-se evitar valores iniciais de λ iguais a 3,63 , 3,74 ou 3,83 onde o comportamento aleatório não é verificado [de Campos, 2003, Cerqueira et al., 2003a].

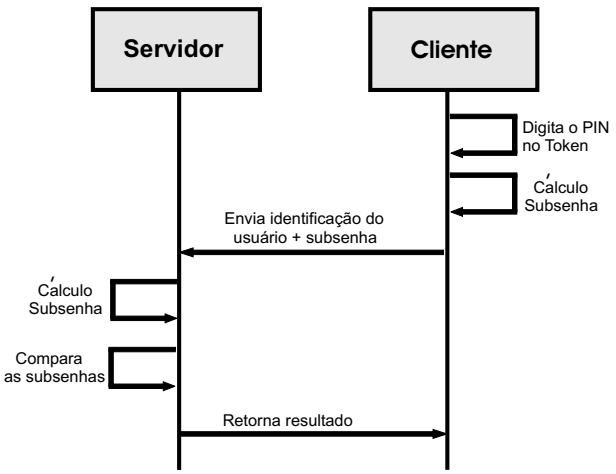

Figura 4: Visualização do processo de autenticação do RSA SecureID.

O funcionamento desta autenticação é baseada na combinação de dois fatores: o PIN (Personal Identification Number), e o número gerado aleatoriamente pelo servidor. Esta proposta de autenticação caótica se parece com a solução RSA SecurID, que pode ser vista na figura 4. Só que, ao invés de utilizar um protocolo de sincronização de tempo, utiliza desafio-resposta e também utiliza-se uma função logística no lugar de técnicas criptográficas, como função resumo, para a elaboração da senha de autenticação. A técnica proposta apresenta baixo custo financeiro e computacional, não sendo necessária a utilização de *hardware* específico e de alto custo como na solução SecurID da RSA.

Para a autenticação baseada em caos, uma combinação de números é colocada a disposição do cliente através de um gerador de palavras aleatórias. Com

posse desta palavra, ou melhor dizendo deste número, uma operação matemática é realizada, retornando um valor para ser utilizado como senha. Sendo que a cada novo processo de autenticação uma nova geração numérica é efetuada e conseqüentemente o valor retornado pela equação será diferente, o que caracteriza a senha como desafio-resposta e descartável, estes passos podem ser vistos na figura 5.

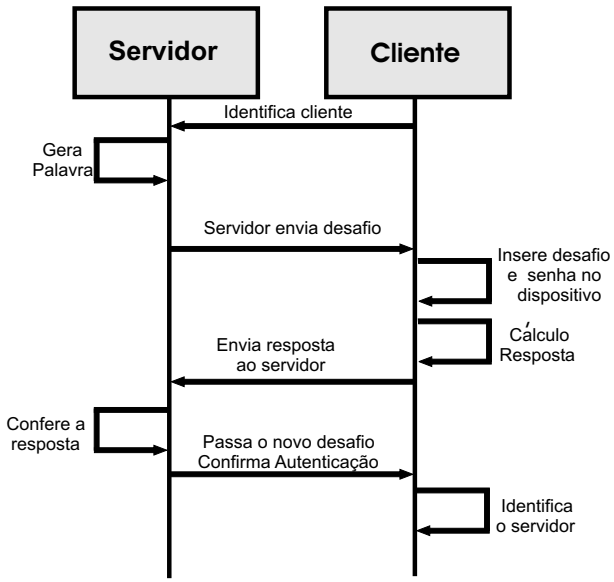

Figura 5: Passos do protocolo proposto.

Esta proposta segue os seguinte passos:

1. Cliente se identifica perante o sistema, como por exemplo o número da sua conta corrente e agência;
2. O sistema, utilizando um gerador de números aleatórios, disponibiliza um valor. Este valor é recebido pelo cliente e é utilizado como complemento do valor de λ. Se o valor é 123456 e o valor inicial de $\lambda = 3,9$ o valor λ a ser utilizado pelo gerador de senhas é 3,912345. O último valor, 6, é utilizado juntamente com o último número da senha do usuário para determinar o número de iterações;
3. Com a visualização deste número aleatório, o usuário faz uso de um dispositivo programável externo de baixo custo, para a realização das operações necessárias a geração da senha descartável. Neste dispositivo o usuário insere sua senha pessoal e o número aleatório tendo a senha descartável como resposta, se o valor da senha for 456789 o valor de X_0 será 0,456789, visto que o X_0 deve ficar no intervalo $[0, 1]$;
4. O dispositivo retorna ao usuário um valor de 10 dígitos, sendo que o usuário utilizará os 6 primeiros dígitos como subsenha;
5. Esta subsenha é utilizada como senha para a autenticação perante o sistema;
6. O sistema, de posse da resposta, pode realizar cálculos similares aos realizados pelo usuário. Desta forma, a verificação da identidade do usuário pode ser realizada. Se o valor retornado for válido, o cliente é identificado e os 4 dígitos restantes são enviados como resposta ao usuário, obtendo assim uma autenticação mútua. Caso o valor retornado não seja válido, a autenticação é negada;
7. O usuário recebe os 4 dígitos restantes. Caso estes dígitos sejam iguais aos calculados anteriormente o usuário tem a identidade do sistema garantida.

5 Implementação da Autenticação Baseada em Caos

Para a validação da proposta foi, implementado um sistema que permite a geração de senhas, bem como a verificação destas. O protótipo foi desenvolvido utilizando a linguagem de programação JAVA.

Para comprovar a aleatoriedade do processo foram realizados testes com vários valores diferentes de λ. Como exemplo apresenta-se o caso de valor inicial de $\lambda = 3.9$. Para desafios variando entre $[0, 1]$ gerando diferentes λ ficou comprovado o comportamento caótico da função. Conforme ilustra a Figura 6 a equação apresenta um comportamento distinto para diferentes valores de λ, não havendo convergência para um valor único. A seqüência de números gerados, $\{x\}$, apresenta comportamento caótico, propriedade desejável no presente caso [de Campos, 2003] [Cerqueira et al., 2003b].

Esta função foi utilizada pelo fato da implementação necessitar de um grande fator aleatório e segundo a literatura [Ceretta, 2002], a Teoria do Caos não está bem compreendida, e seu entendimento está ligado diretamente a três termos básicos: sistema, complexidade e não-linearidade. O sistema representado pela relação de interdependência e inter-relacionamento entre partes, a complexidade está relacionada diretamente com o predizer das ações do sistema real, e a não-linearidade, que é o termo responsável pela segurança da senha reutilizável do cliente. Isto é possível devido à característica de ausência de proporcionalidade constante deste termo, onde o que afeta uma variável não produz efeitos proporcionais em outra [Ceretta, 2002]. A cada nova autenticação valor do λ é alterado, o que garante a segurança da senha contra ataques de análise comparativa, onde mesmo com a obtenção de vários λ, números gerados aleatoriamente, e x, subsenha digitada, a comparação de seus comportamentos não revelará a senha do cliente.

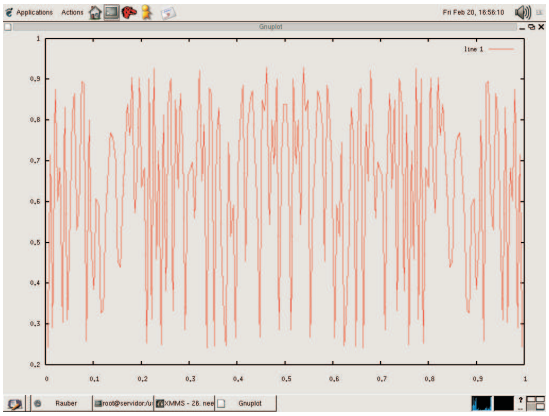

Figura 6: Geração de subsenhas a partir de um determinado λ.

O dispositivo utilizado para a realização desta autenticação, é uma calculadora programável de baixo custo. Este fato se deve a utilização de cálculos de baixa complexidade para a formação da subsenha, não sendo necessário utilizar funções criptográficas, como as utilizadas em outras aplicações.

6 Considerações Finais

Os processos de autenticação para sistemas distribuídos utilizados atualmente apresentam deficiências, o que permite questionar sua segurança. A solução normalmente proposta pelas instituições financeiras consiste na adoção de teclados virtuais, que não resolvem o problema como um todo, apresentando várias vulnerabilidades que podem ser exploradas por entidades maliciosas.

Foi proposto neste trabalho um sistema confiável para a autenticação de usuários perante sistemas de informação distribuídos sem a necessidade de uma plataforma computacional segura. O sistema faz uso de funções quadráticas para a geração de valores aleatórios que são utilizados como senhas. Este mecanismo garante que a entidade auten-

ticada pelo sistema seja realmente quem ela diz ser.

É proposta a utilização desta autenticação em larga escala através do uso de calculadoras programáveis de baixo custo que permitem a operacionalização do procedimento de autenticação sem maiores dificuldades aos usuários.

O protocolo desafio-resposta permite a autenticação mútua das partes, requisito que não é atendido pelos métodos tradicionais de autenticação.

Referências Bibliográficas

Anderson, R. (2001). *Security Engineering*. Wiley Computing Publisher, New York, 1a. edição edition.

Austrália, A. M., Caelli, W., and Little, P. (1998). Electronic signatures - understand the past to develop the future. Disponível em <http://www.austlii.edu.au>. Acesso em 03 Fevereiro 2004.

Bradesco (2003). Como usar com segurança teclado virtual. Disponível em <http://www.bradesco.com.br>. Acesso em 16 de Março de 2003.

Brasil, B. D. (2003). Por que o teclado virtual é mais seguro? Disponível em <http://www.bb.com.br/appbb/portal/bb/ds/TecladoVirtualSeguro.jsp>. Acesso em 18 de Março de 2003.

Ceretta, P. S. (2002). Investigando a presença do caos no IBOVESPA. Disponível em <http://read.adm.ufrgs.br/read29/artigos>. Acesso em 25 de Janeiro de 2004.

Cerqueira, A. G., Costa, A. R. C., Peixoto, A. B. M., Silva, L. F. D., Fontes, L. M. A., de Paula, M. C., and Sabini, P. R. (2003a). Caos decifrado: Família quadrática. *24 Colóquio (IMPA)*.

Cerqueira, A. G., Costa, A. R. C., Silva, L. F. D., de Paula, M. C., Peixoto, A. B. M., and Sabini, P. R. (2003b). Família quadrática : Caos decifrado. Disponível em <http://magnum.ime.uerj.br/ progerio/iniciacao/2003/begin.html>. Acesso em 01 de Fevereiro de 2004.

de Campos, A. M. (2003). A transição para o CAOS e a constante de feigenbaum. Disponível em <http://to-campos.planetaclix.pt/fractal/caos.html>. Acesso em 20 de Fevereiro de 2004.

Devegili, A. J. and Parente, R. V. (2003). Autenticação em HTTP baseada em desafio-resposta. *WSEG*.

Dierks, T. and Allen, C. (1999). The TLS protocol. Technical report, Network Working Group.

Haller, N., Metz, C., Nesser, P., and Straw, M. (1998). A one-time password system. Request for comments: 2289, Network Working Group.

Kent, S. and Atkinson, R. (1998a). Ip authentication header. Technical report, Network Working Group.

Kent, S. and Atkinson, R. (1998b). Ip encapsulating security payload. Technical report, Network Working Group.

Lamport, L. (1981). Password authentication with insecure communication. In ACM, editor, *Communications of the ACM*, pages 770–772. ACM.

Manber, U. (1994). A simple scheme to make passwords based on one-way functions much harder to crack. Disponível em <http://webglimpse.net/pubs/TR94-34.pdf>. Acesso em 08 de abril de 2003.

Pasqual, E. S., Dias, J. D. S., and Custódio, R. F. (2002). A new method for digital time-stamping of electronic document. In FIRST, editor, *Proceedings of the FIRST 14th Annual Computer Security*, 212 West Washington, Suite 1804 Chicago, IL 60606. Phoebe J. Boelter Conference and Publication Services, Ltd.

RSA, S. I. (2004). RSA SecurID. Disponível em <http://www.rsasecurity.com/products/securid/demos/SecurIDTour/RSASecurIDTour.html>. Acesso em 15 de Fevereiro de 2004.

Smith, R. E. (2002). *Authentication from Password to Public Keys*. Addison-Wesley, New York, 1a. edição edition.

Stinson, D. R. (2002). *Cryptography - Theory and Practice*. Chapnan & Hall, 2 edition.