Nota de aplicação

Usando o Atmel ATSHA204 para operações de senha segura

Características

- Armazene senhas com segurança
- Verifique a senha sem revelar o valor esperado
- Mapear senha para chave de alta entropia

1. Introdução

As senhas são usadas em muitos sistemas digitais que contêm uma interface de usuário. Eles fornecem um mecanismo conveniente e bem compreendido para limitar o acesso, habilitar recursos e muitos outros propósitos. Em um sistema digital típico sem qualquer tipo de dispositivo de hardware seguro, no entanto, pode haver muitos pontos fracos no processo geral de senha.

Existem várias classes de preocupações de segurança, mas geralmente elas se enquadram em duas

categorias: 1. A senha correta está armazenada onde um invasor pode acessá-la em qualquer caminho? A senha aparece em claro em qualquer barramento ou conexão interna ou externa que um invasor possa observar? Essas informações podem ser recuperadas remotamente ou o invasor precisa ter acesso físico ao sistema?

2. Se não for possível acessar a própria senha, o invasor pode montar um ataque offline para analisar as informações disponíveis e encontrar a senha? Um tipo de análise é um ataque de dicionário exaustivo.

Dispositivos de hardware seguros podem fornecer mecanismos para ocultar o valor claro da senha, evitar ataques exaustivos off-line e aumentar consideravelmente a dificuldade de ataques físicos locais. O Atmel® ATSHA204 oferece esse recurso em um pacote muito pequeno e com baixo custo. É fácil de integrar em qualquer sistema digital.

Aqui estão cinco modelos de uso típico para senhas, possíveis problemas de segurança e maneiras pelas quais o ATSHA204 aborda essas questões.

- **Validade da senha**

  A senha digitada estava correta? Nesse caso, o sistema pode ativar vários recursos ou ações. Em alguns sistemas, a senha esperada pode ser armazenada em uma EEPROM serial ou memória flash que um invasor pode ler facilmente.

  O Atmel ATSHA204 armazena a senha correta na memória interna não volátil de alta segurança e faz a comparação internamente. Ele retorna uma resposta sim/não simples ao sistema, de modo que o invasor nunca tenha acesso à senha correta. • **Transmissão de senha segura**

  Em muitos sistemas, a senha inserida pelo usuário pode ter que passar por uma conexão com ou sem fio para chegar ao sistema. Um invasor pode observar essa comunicação e ler o valor que um usuário inseriu, permitindo que o invasor o envie novamente posteriormente.

  O Atmel ATSHA204 permite que o dispositivo de entrada misture (usando SHA-256) o valor inserido com um número aleatório antes de transmiti-lo. O Atmel ATSHA204 executa a mesma função de mistura para determinar a validade. Dessa forma, o bisbilhoteiro não pode dizer qual é a senha real ou reenviar a mesma mensagem mais tarde e obter uma resposta bem-sucedida.

- **Senha como chave de criptografia**

  Se o sistema local contiver armazenamento em massa, como memória flash, ou precisar processar pacotes de comunicação criptografados, talvez não seja suficiente saber que um usuário válido está presente. Se a senha for usada para a chave de criptografia/descriptografia, o sistema local precisará do valor da senha real. Esse valor seria então suscetível a malware ou depuradores, qualquer um dos quais pode estar observando os barramentos internos.

  O Atmel ATSHA204 permite que o projetista do sistema combine com segurança a senha com um número visível.
  O resultado é usado como uma chave de sessão efêmera para comunicações ou como uma chave de descriptografia específica de arquivo para dados.

- **Senha mapeada para proteger a chave de criptografia**

  Como a entropia (complexidade ou aleatoriedade) das senhas da maioria das pessoas é limitada, nos casos acima geralmente é possível para um invasor observando o barramento “tentar todas as combinações possíveis” e determinar qual era a senha.

  Para combater isso, o Atmel ATSHA204 fornece uma maneira de mapear uma senha específica em uma chave de alta entropia que é usada para fins de criptografia/descriptografia. Ataques exaustivos a esta chave são essencialmente impossíveis.

- **Recuperação de senha**

  Um problema bem conhecido com senhas é que as pessoas costumam esquecê-las. Algum tipo de mecanismo de recuperação geralmente é desejável para permitir o uso contínuo do sistema ou dos dados. Se esse mecanismo fornecer acesso ao valor da senha antiga ou nova, um ataque terá uma vantagem distinta.

  O Atmel ATSHA204 fornece vários métodos de atualização ou recuperação de uma senha usando dados completamente criptografados para manter o mesmo nível de segurança do uso geral.

É importante observar que nenhum sistema de segurança é perfeito e aqueles que incluem uma senha de usuário estão sempre suscetíveis a engenharia social e outros possíveis vetores de ataque que não são abordados aqui.

2. Problemas de segurança de senha

Há uma série de limitações bem conhecidas para a entropia de senha, incluindo:

- Às vezes, a senha é realmente apenas um PIN de quatro dígitos. Se houver alguma maneira de testar valores eletronicamente, o ataque será fácil porque há poucas possibilidades.
- Na ausência de uma política imposta em contrário, muitas pessoas usarão um único nome ou uma palavra em um dicionário como seu senha

Além disso, existem vários problemas de protocolo e/ou política, incluindo o seguinte: • É comum

usar a mesma senha para muitos sistemas e, portanto, a segurança da senha é tão forte quanto como a segurança do sistema mais fraco

- Se a senha inserida for transmitida por um barramento acessível, um invasor poderá desviar o valor sem que o usuário saiba que a violação ocorreu

Os problemas mais sérios com senhas ocorrem quando um invasor pode determinar remotamente a senha sem que o usuário saiba que a senha está em risco, mesmo sem acesso físico ao sistema protegido. Ataques offline como esses podem empregar uma rede de computadores de alta velocidade para a análise e, às vezes, são conhecidos como *ataques de dicionário* porque o computador pode tentar todas as palavras de um dicionário. No exemplo em que uma senha é usada diretamente como uma chave AES para criptografar um arquivo, o invasor pode copiar o arquivo criptografado para vários computadores e fazer com que cada computador pesquise uma parte do universo de possibilidades de senha para a descriptografia adequada em uma taxa muito rápida.

Mesmo as políticas de senha “fortes” não fornecem muita defesa contra um ataque exaustivo off-line. Suponha uma política que declare que uma senha deve ter mais de oito caracteres e incluir um número e pelo menos um caractere não alfanumérico. Um invasor offline pode pensar sobre isso da seguinte maneira:

- O invasor pode adivinhar que uma senha contém uma ou duas palavras ou nomes. Segundo a Wikipedia, cerca de 6.000 palavras compreendem 90% do texto escrito em inglês e, de acordo com o Censo dos EUA de 1990, 4.250 nomes femininos e 1.208 nomes masculinos cobrem 90% da população. Isso produz 11.458 × 11.458, ou 131.000.000 de possibilidades para verificar. (Essas estatísticas variam de acordo com o país e o idioma, mas não o suficiente para alterar o resultado dessa estimativa.)

- Normalmente, a porção numérica seria pequena para ser fácil de lembrar e provavelmente não ocorre no meio de uma palavra. O invasor pode assumir que tem um valor máximo de 31, pois os dias do mês são comumente lembrados. Para uma senha de duas palavras, isso adiciona um fator de 32 × 3 ou 96. (Muitas vezes, vogais ou letras semelhantes são substituídas por números; o=0, e=3, i=1, p=9, @=a, etc. Isso também é bem conhecido pelos invasores de dicionário)

- Existem apenas 30 caracteres não alfanuméricos em um teclado ocidental típico, e eles podem ocorrer apenas em o início ou o fim da senha. Isso adiciona outro fator de 30 × 2 ou 60.

  O número total de possibilidades a verificar seria então cerca de 8 × 1012. Se o invasor tiver 20 computadores, cada um com um processador quad-core, 80 possibilidades por vez podem ser tentadas. Em 2011, os processadores de 3 GHz são comuns. Se forem necessárias 30.000 instruções para tentar uma possibilidade, cada processador poderá tentar 100.000 senhas possíveis por segundo. Nessa situação hipotética, o invasor pode verificar todas as combinações de senha em até 27 horas.

Por outro lado, usando a sequência mais segura descrita abaixo na Seção 3, com um único ATSHA204 (talvez um que tenha sido roubado) para verificar cada senha (ou seja, um ataque online exaustivo); levaria cerca de 25.000 anos para chegar ao final da lista.

As melhores senhas são grandes números completamente aleatórios. Dependendo da situação e do especialista a quem você perguntar, números completamente aleatórios na faixa de aproximadamente 80 a 128 bits simplesmente não podem ser exaustivamente atacados. As senhas (ou chaves) armazenadas no ATSHA256 têm 256 bits, em comparação.

A maioria das pessoas não consegue se lembrar de longas sequências de caracteres aleatórios e, portanto, a realidade é que as senhas nunca chegarão nem perto da força de um bom número aleatório. Por causa disso, a capacidade de traduzir uma senha fraca em um número aleatório forte é uma vantagem significativa, especialmente para pen drives, equipamentos médicos e outros sistemas que armazenam dados.

3. Detalhes da Implementação

Os exemplos de implementação abaixo são todos expressos em termos de um usuário inserindo uma *“senha”* por meio de alguma interface de usuário. Freqüentemente, a *senha* seria, na verdade, um resumo SHA-256 de uma frase secreta para que o sistema obtenha uma senha de comprimento uniforme, independentemente do tamanho do item que o usuário digita. Nos casos em que o ATSHA204 está em um local fisicamente seguro, a *senha* pode ser simplesmente um PIN de quatro dígitos.

Consulte a folha de dados completa do Atmel ATSHA204 em www.atmel.com para obter informações sobre os detalhes do comando. Além disso, o site da Atmel inclui várias outras notas de aplicativos e bibliotecas de código-fonte para facilitar o desenvolvimento do sistema.

As sequências de exemplo a seguir mostram como habilitar alguns requisitos comuns. Existem, é claro, muitas combinações das seguintes sequências que podem fornecer o melhor nível de segurança possível.

3.1. Habilitando o acesso a um sistema independente

Muitos sistemas digitais precisam de uma maneira para que um técnico de manutenção de fábrica habilite determinados recursos ou exiba determinados dados. Para um dispositivo de monitoramento médico pessoal, o médico ou o paciente podem querer que o acesso a determinados recursos ou informações se tornem disponíveis somente após a entrada da senha correta.

Nessas e em outras situações, é útil poder armazenar a senha esperada em um dispositivo seguro e permitir que esse dispositivo faça a comparação de senha internamente. O ATSHA204 implementa esta capacidade facilmente. A implementação básica é a seguinte:

1. O sistema envia o comando nonce para o Atmel ATSHA204 para gerar um nonce aleatório. o aleatório
   A parte numérica deste nonce é retornada ao sistema.
2. A interface do usuário aceita a senha do usuário e o sistema faz o hash da senha com o nonce
   do passo 1.
3. O Atmel ATSHA204 calcula o mesmo resumo usando a senha armazenada internamente, compara-o com o cálculo do sistema da etapa 2
   usando o comando CheckMac e retorna True/False ao sistema.

3.2. Entrada de senha para acesso à sala do servidor

Um uso direto para uma senha é permitir o acesso a uma sala de servidores (ou qualquer outra área segura) por meio de um teclado próximo à porta. No entanto, não é tão simples quanto parece construir um dispositivo de teclado remoto:

1. Se a senha for transmitida ao controlador central de forma clara, um bisbilhoteiro pode aprender facilmente a senha
   valor tocando no barramento ou monitorando o sinal sem fio.
2. Se a senha tiver um hash com uma chave de mascaramento fixa associada ao teclado, o sistema estará sujeito a um
   ataque de repetição.
3. Se o controlador central enviar um desafio aleatório, que é então misturado com a senha no teclado,
   o sistema está sujeito a um ataque offline.

Uma excelente estratégia é combinar a segunda e a terceira opções acima, usando o ATSHA204 para armazenar a chave fixa e calcular as operações de hash dentro do chip. Um benefício adicional dessa configuração é que o ATSHA204 pode gerar um número aleatório de alta qualidade no teclado, fornecendo proteção adicional contra um controlador central falsificado. O mesmo segredo de mascaramento pode ser usado em cada teclado se o número de série exclusivo do ATSHA204 for incluído nos cálculos.

A implementação básica é a seguinte:

1. O controlador central gera um desafio aleatório e o envia para o teclado 2. O Atmel ATSHA204
   gera um número aleatório e o envia para o sistema 3. O ATSHA204 combina o número aleatório da
   etapa 2 com o desafio de entrada do controlador 4. O ATSHA204 combina a saída do passo 3 com a chave de máscara
   armazenada na EEPROM 5 do ATSHA204. A interface de usuário do teclado aceita a senha do usuário. O usuário pode,
   opcionalmente, enviar um ID de usuário no
   claro
6. O ATSHA204 combina a senha com a saída do passo 4 e envia o resultado para o controlador 7. O controlador combina o
   resultado do passo 6 com o valor esperado

3.3. Acesso à sala do servidor com um número limitado de funcionários

Se o sistema de controle central exigir apenas um número limitado de senhas (talvez menos de 10-12), o ATSHA204 também é ideal como controlador central. Do lado do controlador, o ATSHA204 pode:

- Armazene com segurança a chave de
  máscara • Armazene com segurança todas as senhas (até o número de slots livres no ATSHA204), evitando que um funcionário aprenda as senhas de outro funcionário
- Valide com segurança o código de resposta do teclado

3.4. Senha como chave de criptografia no Flash Drive

Em uma unidade flash, uma senha pode ser usada como chave de criptografia de arquivo. Como a mesma senha protege todos os arquivos da unidade, o valor da senha deve ser cuidadosamente protegido. O problema é que, em uma implementação simples, a senha precisa ser passada de forma transparente para o pendrive, que então a utiliza como chave de descriptografia do arquivo. Isso o deixa suscetível a perdas devido a malware no PC.

O ATSHA204 fornece um excelente mecanismo para implementar a transferência segura da senha e, se a senha corresponder, uma combinação de hash da senha com um blob de chave de arquivo criptografado para permitir a descriptografia externa do arquivo. O valor da senha nunca é revelado em nenhum barramento dentro do pendrive, nem mesmo dentro da memória do processador no pendrive.

A implementação básica é a seguinte:

1. O computador envia o comando Nonce para o ATSHA204 na unidade flash para gerar um nonce aleatório 2. A parte do número aleatório desse nonce é retornada ao computador. A senha é inserida pelo usuário e combinada com o número aleatório no software usando o ATSHA256. O resumo é então passado de volta para a unidade flash pelo barramento USB.
3. O comando ATSHA204 CheckMac aceita o resumo da etapa 2, calcula internamente o valor esperado e retorna um booleano em caso de sucesso
4. Além disso, o comando CheckMac na etapa 3 deve ser executado no modo de cópia, caso em que a senha será copiado para TempKey
5. O blob de chave de criptografia de arquivo individual é recuperado da memória flash e combinado com a senha usando o comando Mac. O resumo resultante é usado como a chave de descriptografia AES para o arquivo.

3.5. Senha mapeada para chave de criptografia segura no Flash Drive

Este é o mecanismo mais seguro para criptografar ou descriptografar arquivos em uma unidade flash, dados em um dispositivo de monitoramento médico pessoal e aplicativos relacionados. Ele combina as vantagens descritas na seção anterior com dois recursos adicionais:

1. Ofuscação secundária da senha quando transmitida pelo barramento para evitar um ataque off-line no barramento tráfego que pode revelar a senha.
2. Uma 'tradução' de hardware da senha em uma chave de 256 bits completamente aleatória. Um invasor com acesso ao arquivos criptografados não podem mais montar um ataque offline nas chaves de criptografia de arquivo.

A implementação básica é a seguinte:

1. O ATSHA204 gera um número aleatório e o envia para o sistema 2. O sistema faz o hash desse número aleatório com um “segredo de mascaramento” compilado no software 3. O sistema aceita a senha da interface do usuário, faz o hash com o resumo da etapa 2 e envia para o unidade flash contendo o NOVO 204
4. O ATSHA204, usando o “segredo de mascaramento” e a senha armazenada em dois slots separados, verifica a exatidão da senha.
5. Se os resumos coincidirem, o ATSHA204 copia o “segredo de criptografia” para TempKey 6. O ATSHA204 combina o valor em TempKey com o blob de chave armazenado com o arquivo criptografado, gerando um Chave AES específica para esse arquivo.
7. O processador na unidade flash ou sistema principal descriptografa (criptografa) o arquivo

3.6. Mapeamento de senha para sites

Geralmente, as senhas inseridas em um site são transmitidas ao servidor usando algum tipo de protocolo seguro (geralmente SSL/TLS). Esses protocolos são muito eficazes para garantir que o acesso aos pacotes à medida que eles passam pela Internet não forneça o valor da senha a um invasor.

No entanto, existem alguns casos em que ter o ATSHA204 em um dongle USB conectado a um PC pode oferecer maior segurança, conveniência e/ou flexibilidade.

- Para implementar um esquema de autenticação de fator duplo (o que você sabe – senha e o que você tem – o dongle), o dongle USB pode agir independentemente do mecanismo de senha
- Especialmente onde as operações locais estão habilitadas, mapeando uma senha de usuário de baixa entropia para uma alta entropia chave criptográfica pode reduzir a exposição a ataques exaustivos off-line aos dados. Essa chave também pode ser enviada para o site no lugar da senha para melhorar a segurança geral.
- Em algumas arquiteturas de sites, pode ser benéfico fazer o oposto, mapear todas as senhas de usuários individuais para um única chave secreta que permite o acesso a alguma capacidade.

  Nota: Neste caso, não há necessidade de armazenar várias senhas no servidor. Se o servidor tiver um chip ATSHA204 complementar anexado de alguma forma, não há necessidade de armazenar *nenhum* segredo no servidor.

3.7. Recuperação de senha

O método usual de recuperar uma senha é que um administrador tenha permissões para escrever uma nova senha se a antiga for esquecida. O ATSHA204 suporta isso por meio da capacidade de gravação criptografada, armazenando o segredo do administrador em um slot separado da senha.

Observação: Isso pode assumir uma forma hierárquica, com algum superadministrador recuperando o segredo do administrador e assim por diante

Um método alternativo de recuperação é permitir que o administrador leia o valor atual do segredo, novamente armazenando o segredo do administrador em um slot separado da senha.

Muitas vezes, é útil poder atualizar a senha se o conhecimento da senha atual puder ser comprovado (expiração da senha). O ATSHA204 também permite isso por meio do recurso de gravação criptografada, onde a chave de criptografia e autenticação para a gravação é o valor existente da senha.

O ATSHA204 não permite que duas entidades controlem gravações em um slot e, portanto, não é possível para um usuário escrever uma nova senha com conhecimento da senha atual ou *com* conhecimento de um segredo de administrador.
No entanto, a parte pode ser configurada para permitir gravações de senha com conhecimento da senha atual ao mesmo tempo em que permite leituras de senha com conhecimento do segredo do administrador.

O método básico para implementar esta última configuração é o seguinte:

- Configurar o slot de senha para aceitar leituras e gravações criptografadas
- Definir ReadKey para apontar para o slot que contém a chave do administrador
- Definir WriteKey para apontar para o próprio slot de senha

4. Histórico de Revisão

Doc. rev.	Data	Comentários
8752A	04/2011	Liberação inicial do documento

Atmel Corporation
2325 Orchard Parkway
São José, CA 95131
cervo
Tel: (+1)(408) 441-0311
Fax: (+1)(408) 487-2600
www.atmel.com

Atmel Asia Limited
Unidade 01-5 e 16, 19F
Torre BEA, Millennium City 5
Estrada Kwun Tong 418
Kwun Tong, Kowloon
HONG KONG
Tel: (+852) 2245-6100
Fax: (+852) 2722-1369

Atmel Munich GmbH
Business Campus
Parkring 4
D-85748 Garching b. Munique,
Alemanha
Tel: (+49) 89-31970-0
Fax: (+49) 89-3194621

Atmel Japão
9F, Tonetsu Shinkawa Bldg.
1-24-8 Corte
Chuo-ku, Tóquio 104-0033
JAPÃO
Tel: (+81)(3) 3523-3551
Fax: (+81)(3) 3523-7581