Estudo e avaliação dos mecanismos de segurança empregados na tecnologia Bluetooth

Érico Santos Rocha
Ciência da Computação, Centro Universitário Lasalle
Canoas, Rio Grande Do Sul 91.501-970, Brasil
ericomsr@gmail.com

e

Gaspare Giuliano Bruno
Ciência da Computação, Centro Universitário Lasalle
Canoas, Rio Grande Do Sul 91.501-970, Brasil
gaspare.bruno@gmail.com

Abstract

Considering all wireless technologies applied to adhoc environments, Bluetooh is presented as the solution with the most expressive development and application in the last years. However, the aspects of security around this technology had not followed this growth in the same way, resulting in a sort of vulnerabilities founded. Considering all these aspects, this paper presents two proposals with major purpose of improve the Bluetooth security architecture. These proposals, respectively, consider the authentication procedure and paring.

Keywords: Bluetooth. Security. Authentication. Paring. PIN.

Resumen

Dentre as tecnologias de redes sem fio voltadas para ambientes adhoc, Bluetooth apresenta-se como a solução com maior desenvolvimento e expansão nos últimos anos. Entretanto, os aspectos de segurança em volta deste padrão não acompanharam este crescimento de maneira adequada, resultando na descoberta e exploração de diversas vulnerabilidades. Partindo deste cenário, este trabalho apresenta duas propostas visando o melhoramento da arquitetura de segurança Bluetooth. Estas propostas abordam respectivamente os procedimentos de autenticação e paring.

Palavras chaves: Bluetooth. Segurança. Autenticação. *Paring*. PIN.

1 INTRODUÇÃO

Atualmente, a necessidade dos usuários está voltada para a mobilidade. Cada vez mais estes buscam rapidez e agilidade em suas comunicações. Visando suprir estas necessidades, surgiram inúmeras tecnologias com este propósito. Entre estas se destacam a IrDA (*Infrared Data Comunications*) [1], a UWB (*Ultra Wide Band*) [2], a Home RF [3] e finalmente o Bluetooth.

Bluetooth é uma tecnologia para redes sem fio, utilizada na comunicação entre diversos tipos de equipamentos, proporcionando a formação de redes do tipo *piconet* e *scatternet* [4]. A comunicação nestas redes é realizada por meio de ondas de rádio, o que torna a tecnologia Bluetooth mais suscetível a ataques em comparação às tradicionais soluções de rede [5].

Partindo deste cenário e suas respectivas vulnerabilidades, este trabalho visa contribuir com as questões de segurança desta tecnologia através de propostas que alteram os processos de autenticação e *paring*. O artigo esta organizado como segue. A seção 2 aborda a arquitetura de segurança Bluetooth, a seção 3 apresenta as propostas de melhorias, enquanto a seção 4 realiza a respectiva avaliação das mesmas. Por fim, a seção 5 traz os trabalhos futuros e as considerações deste estudo.

2 ARQUITETURA DE SEGURANÇA

Dentre os serviços de segurança, Bluetooth abrange a confidencialidade, a integridade e a disponibilidade. Estes serviços são garantidos por meio da utilização de procedimentos de criptografia, autenticação e autorização [6]. O esquema de gerenciamento de chaves nesta arquitetura é utilizado para criar, armazenar e realizar a distribuição de chaves, sendo que existem diversos tipos, todas derivadas da chave de link. Conforme o tipo de aplicação**,** a chave de link pode atuar como chave de combinação, chave de unidade, chave do mestre ou chave de inicialização [7].

A autenticação é realizada por meio de um sistema de desafio-resposta, onde o dispositivo A tenta confirmar se está se comunicando com o verdadeiro dispositivo B. Para isso, A atua como verificador e desafia a unidade B no papel de reivindicador, solicitando a confirmação da chave de link estabelecida entre eles [8]. Outro processo vital da arquitetura blutooth é o processo de *paring*, pois possibilita que dois dispositivos compartilhem uma chave secreta, denominada K_init (*Inicialization Key*), e serve como base para os demais procedimentos de segurança [5]. Após o *paring***,** as partes envolvidas terão a certeza de que poderão estabelecer uma conexão segura entre as mesmas [8].

No que se refere às vulnerabilidades, apesar da tecnologia Bluetooth apresentar determinado grau de segurança, possui um número considerável de falhas, que podem ser verificadas em pesquisas como [9], [10] e [11]. Estas vulnerabilidades ocorrem geralmente por falhas no padrão, como o caso da força do gerador de números randômicos e o uso de um pequeno valor para o PIN. Outras causas seriam as falhas de implementação e a flexibilidade do padrão, que oferece autonomia aos fabricantes para definição de diversos procedimentos, como autenticação e armazenamento das chaves [5].

3 SOLUÇÕES PROPOSTAS

Baseado na arquitetura atual de segurança e nas respectivas vulnerabilidades, esta pesquisa apresenta duas propostas com o objetivo de aperfeiçoar a arquitetura. Estas propostas atuam nos processos de *paring* e autenticação, como é ilustrado na figura 1a e 1b.

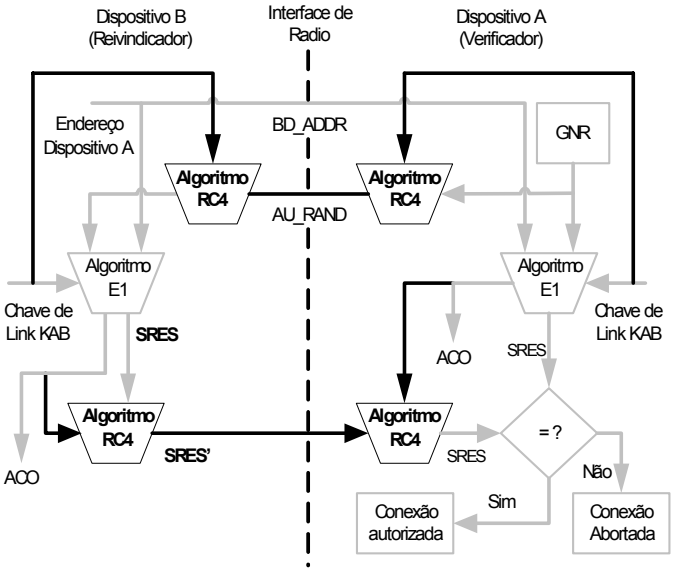

Figura 1a: Modificação no sistema de Autenticação

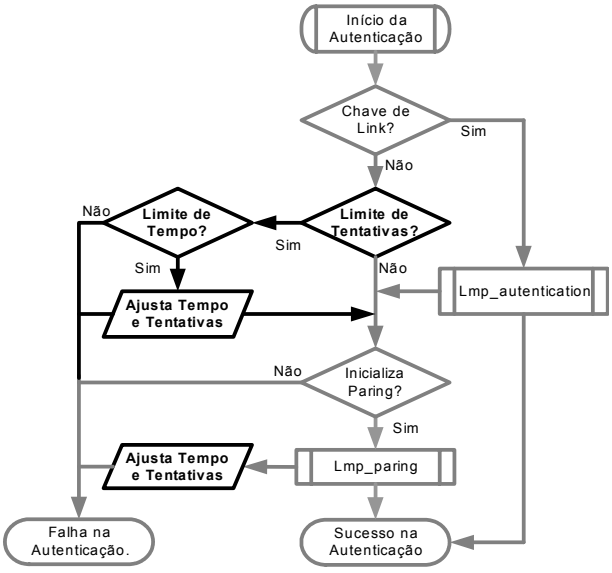

Figura 1b: Modificação no sistema de *paring*

Fonte: Autoria própria,2006

Partindo deste ponto, a seção 3.1 apresenta uma nova proposta para o processo de autenticação, enquanto a seção 3.2 descreve a proposta relacionada ao processo de *paring*.

3.1 Proposta de modificação do processo de autenticação

A nova proposta estabelece que o processo de autenticação deve ser implementado de forma mútua. Além disso, trata de maneira diferenciada os componentes principais deste sistema, denominados AU_RAND e SRES.

Devido ao padrão atual transmitir os componentes de maneira clara pelo meio, esta proposta estabelece a criptografia destes componentes por meio do algoritmo RC4.

O uso do RC4 tem como principal objetivo proteger os dados AU_RAND e SRES, além de não permitir a divulgação das chaves utilizadas durante este processo. Para atender estas definições, o modelo utiliza a chave de *link* para a cifrarem do componente AU_RAND, ao passo que na cifragem do componente SRES a porção ACO derivada do algoritmo E1 é utilizada como chave criptográfica dentro do algoritmo RC4.

O novo esquema de autenticação funciona da seguinte maneira:

- O dispositivo verificador gera um número randômico de 128 bits;
- Este número é criptografado através do algoritmo RC4, tendo como chave criptográfica a chave de *link* estabelecida entre os partes no processo de *paring*;
- O verificador envia o número randômico criptografado para o dispositivo reivindicador. Este processo é realizado através de um pacote LMP_au_rand;
- Enquanto espera a resposta SRES do *host* reivindicador, o dispositivo verificador calcula por meio do algoritmo E1 as porções SRES e ACO;

- O dispositivo reivindicador recebe o pacote LMP_au_rand e utiliza sua respectiva chave de *link* com o algoritmo RC4 para decifrar o AU_RAND recebido do verificador;
- Com posse do AU_RAND, o dispositivo reivindicador calcula os componentes SRES e ACO, através do algoritmo E21;
- Após realizar o cálculo destes componentes, o reivindicador criptografa a porção SRES utilizando o algoritmo RC4, utilizando como chave a porção ACO;
- O passo acima gera o SRES', sendo este enviado para o dispositivo verificador na forma de uma pacote do tipo LMP_sres;
- O dispositivo verificador recebe o pacote LMP_sres e utiliza a porção ACO com o algoritmo RC4, obtendo assim o SRES enviado pelo reivindicador;
- Após obter o valor SRES, o dispositivo compara este com o SRES calculado por ele mesmo. Se os valores forem iguais, o processo de autenticação é validado e a porção ACO é armazenada para utilização no processo de criptografia dos pacotes de dados;
- Por fim, o processo é repedido com as funções de verificador e reivindicador invertidas, para que a autenticação mútua seja garantida.

Para os casos em que o teste de SRES falhar, o dispositivo verificador entenderá esta ocorrência como um erro no processo de autenticação, abortando a conexão com o dispositivo reivindicador.

3.2 Modificação do processo de *paring*

Com relação ao processo de *paring*, nossa proposta traz a implementação de procedimentos adicionais à camada LMP, que evita de forma mais eficiente os ataques por meio de força bruta.

Ataques deste tipo obtêm êxito desde que a cada iteração o dispositivo que origina o mesmo modifique seu endereço Bluetooth. Outro aspecto relevante é o fato de que esta abordagem não possui solução definida pelo padrão atual.

A nova proposta visa garantir as conexões dos dispositivos já conhecidos, por meio de controles existentes na camada LMP, ao mesmo tempo em que avalia a ocorrência de ataques através do método de força bruta.

Basicamente, o controle tem como função responder se ocorreu um número limite de tentativas de conexão para novos dispositivos, e com base nesta informação, o mecanismo pode liberar a inicialização do procedimento de *paring* ou dar início a outras verificações. A seguir é explicado o funcionamento do modelo proposto.

- O dispositivo A recebe um pedido de estabelecimento do *paring* por meio do pacote lmp_in_rand;
- O dispositivo A verifica se existe uma chave de *link* relacionada ao endereço Bluetooth que enviou o pacote lmp_in_rand. Caso esta chave exista, o *paring* com o dispositivo em questão foi realizado com sucesso e este dispositivo é considerado confiável. Caso contrário, o dispositivo é dado como desconhecido e segue a execução do processo;
- Neste ponto localiza-se o primeiro processo da proposta. Este processo analisa a quantidade de tentativas enviadas para o *host* A e com base nesta informação, conclui se o dispositivo está sofrendo algum ataque ou não;
- Caso o limite de tentativas tenha sido alcançado, o processo não permite o inicio do *paring* e passa a responsabilidade da verificação ao controle de tempo;

- O controle de tempo verifica se passou o tempo necessário desde que o dispositivo iniciou o modo de bloqueio a equipamentos desconhecidos. Enquanto este tempo não for alcançado, as novas conexões são abortadas. Caso contrário, o controle de tempo e tentativas é reinicializado pelo módulo de ajuste;
- Para os casos em que a quantidade de tentativas não ultrapassou o limite estipulado, o processo de *paring* continua sua execução normal. Este ponto pode ser alcançado através da falha no processo dado por lmp_authentication, ou após a execução do módulo de ajuste;
- Com base no que ocorreu nos passos anteriores, é iniciado o *paring* com o envio do pacote lmp_accept do *host* A em resposta ao pacote lmp_in_rand;
- O processo de *paring* é executado e são geradas as chaves kinit e kab. Por fim é realizada a respectiva autenticação;

Se as etapas anteriores tiverem sido executadas com êxito, significa que o processo de *paring* foi completado com sucesso. Caso contrário, é registrado o insucesso do processo. Quando o número de tentativas sem sucesso chegar ao limite, o controle de tempo é ativado.

Neste momento, o dispositivo entra no modo de bloqueio e somente aceitará novas conexões de dispositivos confiáveis, ou seja, de dispositivos para o qual ele já obteve sucesso no processo de *paring* anteriormente.

4 AVALIAÇÃO DAS PROPOSTAS

Para avaliar os procedimentos propostos foram utilizados dois métodos distintos. O primeiro por meio do formalismo desenvolvido por BUROWS [12], foi aplicado apenas à proposta de autenticação visto que este formalismo destina-se a exclusivamente a validação de processos de autenticação em desenvolvimento ou respectivo aprimoramento. O segundo método foi a análise de fluxo por meio de um protótipo para a simulação dos processos de *paring* e autenticação no modelo atual e no modelo proposto, ou seja, através do protótipo desenvolvido comparou-se o funcionamento dos processos no modelo atual e proposto para se determinar a respectiva validade destas propostas. A seção 4.1 apresenta a avaliação formal dó processo de autenticação enquanto a seção 4.2 apresenta a avaliação por analise de fluxo aplicada aos processos de autenticação e paring.

4.1 Avaliação formal do modelo de autenticação

O processo de avaliação formal tem como base o formalismo descrito por BUROWS [12], que resultou na criação de um método genérico para avaliação de sistemas de autenticação, sendo aplicável a qualquer processo devido a sua generalização. O uso deste formalismo proporciona ao final de sua respectiva aplicação a possibilidade de responder as seguintes questões:

- O protocolo funciona?
- Qual a exata finalidade do protocolo?
- No caso de modificação de protocolo a nova proposta necessita de procedimentos adicionais em relação ao anterior?
- É realizado algo desnecessário pelo sistema em análise?

Partindo das premissas oferecidas pelo formalismo mencionado anteriormente, este estudo se vale do mesmo para avaliar o novo processo de autenticação executado entre dois *hosts* Bluetooth visto que este formalismo proporciona viabilizar a se determinado mecanismo de autenticação é passível de implementação. Isto é um dos pontos chaves para a continuidade dos estudos relacionados ao melhoramento dos aspectos de segurança deste mecanismo de autenticação.

A primeira fase apresentada a seguir é denominada como a idealização do protocolo e consiste na abordagem do fluxo de mensagens que compõe o sistema proposto. Segundo BUROWS [12], esta abordagem deve estar em completa conformidade com a notação estipulada por este formalismo.

Protocolo Idealizado:

Mensagem 1: A → B : {Na} $_{Kab}$
Mensagem 2: B → A : {X1} $_{K1}$
Mensagem 3: B → A : {Nb} $_{Kab}$
Mensagem 4: A → B : {X2} $_{K2}$

As partes envolvidas nesta autenticação são denominadas A e B, e representam respectivamente o dispositivo mestre e escravo de uma *piconet* qualquer. Dentro deste sistema a chave kAB corresponde à chave de link KAB sendo esta criada de acordo com o atual padrão. Alem da chave kAB o sistema proposto emprega as chaves k1 e k2 que são calculadas durante o processo de autenticação através do algoritmo E1. Na e Nb representam o número gerado por GNR nos dispositivo A e B respectivamente. Por fim, X1 e X2 denotam a porção SRES que foi gerado como resultado do algoritmo E1.

Com a definição dos pacotes envolvidos no procedimento em análise, é permitida a continuidade do processo de avaliação proporcionado por este formalismo onde o passo subseqüente estabelece pré-definições necessárias ao seguimento da avaliação. A notação do método é empregada na definição de dados e procedimentos pré-existentes ao início do processo de autenticação, nos quais são apresentados a seguir.

Definições Assumidas:

1. *A* ***believes*** *A* $\overset{Kab}{\longleftrightarrow}$ *B,*	*B* ***believes*** *A* $\overset{Kab}{\longleftrightarrow}$ *B,*
2. *A* ***believes*** *A* $\overset{Kn}{\longleftrightarrow}$ *B,*	*B* ***believe*** *A* $\overset{Kn}{\longleftrightarrow}$ *B,*
3. *A* ***believes*** *B* ***control*** *(Nb),*	*B* ***believes*** *A* ***control*** *(Na),*
4. *A* ***believes fresh*** *(Nb),*	*B* ***believes fresh*** *(Na),*
5. *A* ***believes*** *B* ***control*** *(X2),*	*B* ***believes*** *A* ***control*** *(X1),*
6. *A* ***believes fresh*** *(X2),*	*B* ***believes fresh*** *(X1),*

A primeira linha informa que a chave de link KAB possui credibilidade para os dispositivos A e B. A segunda linha denota que os dispositivos acreditam nas chaves criadas no decorrer do processo de autenticação, sendo que a chave em questão é a porção ACO derivada como resultado da execução do algoritmo E1. Na terceira linha é assumido que A acredita que B tem a jurisdição sobre a geração do número randômico Nb e, por sua vez B apresenta a mesma confiança em relação ao número Na gerado por A. Em decorrência dos valores Na e Nb mudarem a cada processo de autenticação, a linha quatro estabelece que A acredita na atualização do número Nb e da mesma forma B acredita nas atualizações realizadas no número Na. De maneira similar às linhas três e quatro, as linhas cinco e seis abordam a relação de controle e de atualização dos componentes do processo em relação aos valores X1 e X2 que representam respectivamente a porção SRES obtida em conjunto com a porção ACO.

Com a finalização do processo de montagem das mensagens e o estabelecimento das definições preliminares, é dado início a fase de análise de cada fluxo pertencente ao processo em análise.

- **Análise do fluxo: B recebe mensagem 1 enviada por A**

Mensagem 1: A → B : {Na} $_{Kab}$
Aplicando as regras do método formal,
B sees *{Na}* $_{Kab}$
Segundo hipótese,
B ***believes*** *A* $\overset{Kab}{\longleftrightarrow}$ *B*
Então,

*B **believes** A **said** (Na)*

Os passos mostrados anteriormente são utilizados para legitimar o significado da mensagem, ou seja, visam analisar a mensagem de entrada e através das premissas estabelecer se ela tem algum sentido para o dispositivo que a recebeu. Neste caso, B recebe (Na) cifrado pela chave Kab. De acordo com o que foi pré-estabelecido, a entidade B acredita na chave criptográfica compartilhada com a unidade A por isso B acredita que a mensagem que ele recebeu fora enviada pelo dispositivo A.

Segundo hipótese,
*B **believes** fresh (Na) e B **believes** A **said** (Na)*
Então,
*B **believes** A **believes** (Na)*

Esta hipótese verifica se a mensagem é recente bem como se o emissor continuasse acreditando na mesma. Partindo da hipótese de que B acredita que o valor de (Na) pode ser atualizado a cada pedido de autenticação, e de que B acredita que A emitiu o Na em análise, resulta no fato de B acreditar que A também acredita no (Na) em análise.

Segundo hipótese,
*B **believes** A **control** (Na) e B **believes** A **believes** (Na)*
Então,
*B **believes** (Na).*

` A hipótese anterior avalia a jurisdição do dispositivo A, em ralação ao dado (Na). Seguindo a hipótese B, acredita que A possuía jurisdição sobre o dado (Na). Alem disso o passo anterior demonstrou que B confia em A, por sua vez acredita no dado (Na) em análise. Desta forma por conseqüência que B acredita na veracidade da informação representada por (Na).

Desta forma é comprovado pelo formalismo que a unidade cria um número randômico, criptografa este com o algoritmo RC4 por meio da chave de *link* KAB e a envia de maneira segura para o dispositivo B que por sua vez obtém o dado cifrado pelo fato deste ter compartilhar a chave KAB com o diapositivo A. Assim é encerrada a respectiva avaliação da mensagem 1 viabilizando a análise da mensagem 2.

Antes da análise da mensagem 2 é necessário informar os processos executados pelo *host* B antes deste enviar o pacote para o *host* A. Apenas relembrando o que fora mencionado no funcionamento da proposta na seção 3. O dispositivo B recebe o número randômico de A, e em conjunto com seu endereço Bluetooth gera as porções ACO e SRES por meio do algoritmo E1. ACO é por sua vez utiliza como chave criptográfica para gerar o a cifrarem da porção SRES. Tendo concluído estes procedimentos, o *host* B envia a mensagem 2 dando continuidade ao processo de autenticação.

- **Análise do fluxo: A recebe mensagem 2 enviada por B**

Mensagem 2: B → A : $\{X1\}_{K1}$
Aplicando as regras do método formal,
***A sees** $\{X1\}_{K2}$*
Segundo hipótese,
*A **believes** A $\overset{Kn}{\longleftrightarrow}$ B*
Então,
*A **believes** B **said** (X1)*

De forma análoga à mensagem um, a primeira parte da mensagem dois refere-se ao significado desta perante o dispositivo A. Logo, temos que A recebe o pacote X1 cifrado com a chave k1. Partindo da hipótese de que A confia na chave estabelecida com o dispositivo B, possibilita afirmar que A acredita que B enviou X1 e por sua vez comprova o significado da mensagem.

Segundo hipótese,

*A **believes** fresh (X1), A **believes** B **said** (X1)*
Então,
*A **believes** B **believes** (X1)*

Tendo como base a comprovação do significado da mensagem, mais o fato de A acreditar que o número X1 fora gerado exclusivamente para a seção em execução, resulta que A acredita em B que por sua vez da credibilidade a exclusividade do número X1 perante o processo em corrente. Em outras palavras para cada novo procedimento de autenticação um novo X1 será criado por intermédio do algoritmo E1.

Segundo hipótese,
*A **believes B control** (X1), A **believes** B **believes** (X1)*
Então,
*A **believes** (X1).*

Considerando que A acredita na jurisdição de B sobre o dado X1, e que o dado X1 é de exclusividade da referida seção, resulta que A acredita na legitimidade do dado X1.

Resumidamente, A obtém X1 por meio do cálculo que ele mesmo executa internamente através do algoritmo E1. Como as informações de entrada em ambos os lados são idênticas, proporciona que o algoritmo gere a mesma saída para as partes envolvidas neste sistema. Quanto ao endereço Bluetooth, este é de conhecimento de ambas as partes conforme mencionado na seção 2.4.

Antes de ocorrer à mensagem três, o processo de autenticação pode ser interrompido caso a verificação final realizada internamente pelo *h*ost A não atenda as expectativas, ou seja, se SRES' for diferente de SRES o processo será abortado.

- **Análise do fluxo: A recebe mensagem 3 enviada por B:**

Mensagem 3: B → A : $\{Nb\}_{Kab}$
Aplicando as regras do método formal,
***A sees** $\{Nb\}_{Kab}$*
Segundo hipótese,
*A **believes** A $\overset{Kab}{\longleftrightarrow}$ B*
Então,
*A **believes** B **said** (Nb)*
Segundo hipótese,
*A **believes** fresh (Nb), A **believes** B **said** (Nb)*
Então,
*A **believes** B **believes** (Nb)*
Segundo hipótese,
*A **believes B control** (Nb), A **believes** B **believes** (Nb)*
Então,
*B **believes** (Nb).*

Todo o fluxo da mensagem e seu respectivo funcionamento são idênticos ao da primeira mensagem, exceto pelo fato dos papéis de verificador e reivindicador serem invertidos. Logo, o endereço Bluetooth empregado pertence ao dispositivo A e o número gerado por GNR pertence ao dispositivo B.

Seguindo o formalismo, a mensagem três atende as regras e premissas estabelecidas da mesma forma que a mensagem um e por conseqüência permite o início da análise referente ao fluxo quatro.

- **Análise do fluxo: B recebe mensagem 4 enviada por A:**

Mensagem 4: A → B : $\{X2\}_{K2}$
Aplicando as regras do método formal,

B sees *{X2}* $_{K2}$
Segundo hipótese,
B ***believes*** *A* $\overset{Kn}{\blacktriangleleft\!\!\blacktriangleright}$ *B*
Então,
B ***believes*** *A* ***said*** *(X2)*
Segundo hipótese,
B ***believes*** *fresh (X2), B* ***believes*** *A* ***said*** *(X2)*
Então,
B ***believes A believes*** *(X2)*
Segundo hipótese,
B ***believes A control*** *(X2), B* ***believes A believes*** *(X2)*
Então,
B ***believes*** *(X2).*

De forma análoga a segunda mensagem, esta mensagem executa os mesmos passos que a citada anteriormente exceto o fato de que o sentido desta é o inverso da primeira. Alem disso, neste fluxo a informação X2 é gerada pelo *host* A. Tanto o dispositivo a quanto o dispositivo B calculam internamente a chave k2 por meio do algoritmo E1. Assim o *host* B consegue efetivar seu lado pro processo de autenticação fazendo desta uma autenticação mútua desde que o a verificação por parte de B se SRES' é igual a SRES tenha êxito.

4.2 Avaliação das propostas via análise de fluxo

Para o processo de autenticação, o protótipo executou os processos de autenticação com e sem o uso do algoritmo RC4 para enfatizar a criptografia das porções AU_RAND e SRES. Esta análise foi realizada com a simulação do ambiente atual e do ambiente proposto, sendo que o trafego entre os dispositivos foi capturado através da ferramenta *Ethereal*.

A figura 2 apresenta o pacote no atual processo de autenticação, enquanto a figura 2b apresenta o mesmo pacote criptografado por meio do algoritmo RC4.

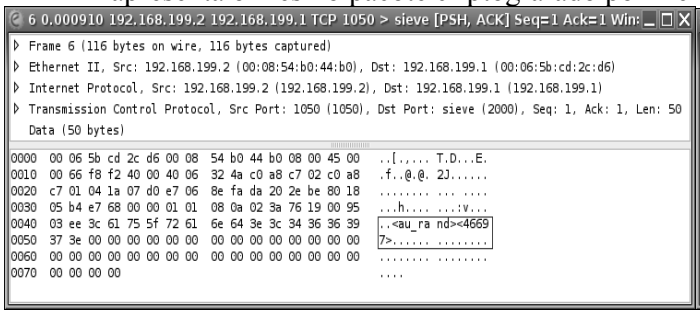

Figura 2a: AU_RAND – Modelo atual

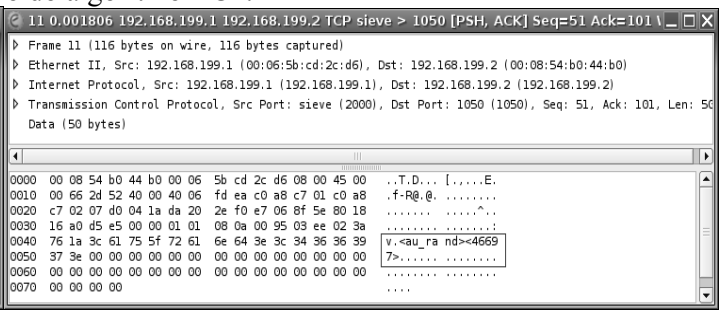

Figura 2b: AU_RAND – Proposta RC4

Fonte: Autoria própria,2006

A diferença primordial entre o modelo proposto e o modelo atual esta relacionada ao fato de que a captura de pacotes pode ser executada no modelo proposto, no entanto a facilidade em obter os dados que antes eram transmitidos de maneira clara deixa de existir. Conseqüentemente para que um ataque utilize os dados referidos será necessário a quebra do algoritmo RC4. Isto pode ser executado através da descoberta da chave que fora utilizada com o referido algoritmo, entretanto o modelo proposto não utiliza métodos para a distribuição das chaves mas sim faz uso dos algoritmos e variáveis existentes no padrão como sua respectiva chave criptográfica o que dificulta ainda mais o processo de descoberta dos dados que estão sendo protegidos por intermédio da nova proposta.

No que diz respeito ao processo de *paring*, foram realizadas simulações de ataques com a utilização de vários tamanhos de PIN, além da troca do endereço Bluetooth em cada tentativa de

descoberta do mesmo. Os testes demonstraram que a nossa proposta obtém êxito ao evitar a quebra do PIN de forma on-line.

Este processo de avaliação foi constituído por duas etapas, a primeira formada pela simulação do modelo atual com e sem ataques, sendo explicado como segue:

- Na execução sem implementação de ataques, o processo escravo aceitou a conexão quando o PIN no lado do nó mestre foi informado de forma correta, e negou quando este fora informado incorretamente. A tentativa de execução em seqüência de tentativas para o procedimento, com o objetivo de descobrir o PIN por meio de força bruta, foi ignorada na quinta tentativa (parâmetro definido na concepção do protótipo), sendo que para cada erro o tempo de espera definido por meio da quantidade de tentativas, foi duplicado a cada falha provinda do mesmo endereço;
- Com o mestre executando o ataque, o PIN foi obtido visto que o modelo atual, apenas incrementa e bloqueia os pedidos de autenticação originados pelo mesmo endereço, para isso o código do mestre possibilitava a troca, de endereço e do PIN a ser utilizado a cada tentativa de execução do *paring*.

A seguir serão analisadas as hipóteses relacionadas à primeira fase da análise.

1ª hipótese – Quebra do PIN sem a troca do endereço Bluetooth: O padrão trata este aspecto corretamente, aumentando o tempo entre os pedidos de *paring* providos do mesmo dispositivo e finalmente bloqueando o dispositivo;

2ª hipótese – Quebra do PIN com a troca do endereço Bluetooth: O protótipo comprovou que isso é viável, desde que ocorra troca do endereço Bluetooth a cada execução deste ataque. Contudo, o tempo de descoberta está relacionado diretamente ao tamanho do PIN utilizado no dispositivo.

A segunda etapa do processo de avaliação, fora idealizada por meio da execução do protótipo, com as características do modelo proposto ao nó escravo, e o nó mestre continuou realizando o papel de entidade confiável, ao inserir o valor correto do PIN e respectivamente de entidade não confiável ao tentar quebrar o PIN.

Estas simulações são relatadas a seguir.

- Na execução sem implementação de ataques, o processo proposto apresentou o mesmo funcionamento do procedimento de *paring* atual, ou seja, tanto para tentativas erradas como para os casos de informação correta do PIN, o processo apresentou o mesmo comportamento;
- Na execução do ataque, o nó escravo passou a bloquear as tentativas do nó mestre após 5 tentativas erradas, independente do endereço utilizado pelo nó mestre.

Com isso a segunda etapa de execução do protótipo fora concluída possibilitando a seguinte analogia das hipóteses que foram estabelecidas.

1ª hipótese – Quebra do PIN sem a troca do endereço Bluetooth*:* Nenhuma diferença no funcionamento, sendo este benéfico ou não, fora constatado que o padrão e proposta possuem o mesmo funcionamento dentro deste cenário.

2ª hipótese – Quebra do PIN com a troca do endereço Bluetooth: O protótipo consegue tratar e identificar os ataques por quebra on-line de PIN, bloqueando-se para novos pedidos de conexão, e assim aumentando a segurança do processo de *paring* em relação ao modelo atual.

5 CONSIDERAÇÕES FINAIS

Inicialmente, a tecnologia Bluetooth foi concebida apenas para a substituição de cabos entre periféricos. Atualmente, a tecnologia está sendo empregada num âmbito maior, em virtude de sua flexibilidade e do baixo custo de implementação.

Entretanto, as questões de segurança não acompanharam de maneira efetiva o crescimento de sua utilização, gerando uma lacuna entre a mobilidade oferecida e a segurança das conexões.

Sendo assim, os aspectos de segurança desta tecnologia são cada vez mais necessários, devido ao aumento da aplicabilidade desta solução e a defasagem existente no aspecto da segurança.

Esta relação viabilizou diversos estudos e propostas que conseqüentemente apresentam novos problemas e possíveis soluções. Com base nisto, o objetivo principal deste trabalho foi realizar uma análise sobre as vulnerabilidades presentes na tecnologia Bluetooth, e por sua vez, proporcionar alternativas possíveis para esta tecnologia.

Para atingir esta meta, foi necessário obter o conhecimento pleno da tecnologia Bluetooth, bem como dos aspectos de segurança e potenciais vulnerabilidades relacionadas.

O conhecimento e experiência adquiridos proporcionaram a visão sistemática de todo o processo de segurança e suas respectivas falhas, acarretando assim a contribuição realizada por meio das propostas destinadas ao aperfeiçoamento do processo de *paring* e autenticação.

As limitações encontradas durante esta pesquisa estão diretamente relacionadas ao funcionamento da arquitetura de segurança da tecnologia Bluetooth, que é interna ao *hardware* de rádio na camada LMP. Quanto às propostas apresentadas, sua limitação esta na abstração de determinados procedimentos, como a criação de chaves e o uso de números fixos para os protótipos implementados.

As principais sugestões de trabalhos futuros estão relacionadas a análise e a melhorias nos aspectos de segurança, que não foram abordados por este estudo devido a sua abrangência.

Dentre estas sugestões, está a mescla das duas propostas apresentas e a avaliação de possíveis soluções para a criação da chave *Kinit*, pois a mesma serve como base para a criação das demais chaves, mas não possui uma boa sistemática para o próprio estabelecimento.

Por fim, uma ultima sugestão é o desenvolvimento de um simulador, que pode ser realizado com alterações no módulo atual da *BlueHoc* ou através da criação de um novo módulo para a ferramenta de simulação NS-2, o que facilitaria trabalhos futuros em cima desta tecnologia.

REFERÊNCIAS

[1] SEEK, D. (2005) IrDA – Infrared communication: http://www.definitionseek.com – visitado em março de 2006. 2006.

[2] UWBG. About UWB – Ultrawideband: http://www.uwbgroup.ru - visitado em março de 2006. 2006.

[3] SYSTEM, A. (2000) Bluetooth Whitepaper: http://www.palowireless.com – visitado em abril de 2006. 2006.

[4] ROUSSEAU, L., Arnoux C., e Cardonnel C. (2001) "A Trusted Device to Secure a Bluetooth Piconet", em: Proc. of Gemplus Developer Conference, Paris, França.

[5] GEHRMANN, C., Persson, J. e Smeets B. (2004) "Bluetooth Security", Boston: Artech House.

[6] VANIO, J. (2000) Bluetooth Security: hyttp://www.niksula.cs.hu.fi/~jiitv/bluesec.html - visitado em abril de 2006. 2006.

[7] KARYGIANNIS, T. Owens L. (2002) Wireless Network Security 802.11, Bluetooth and Handheld Devices: http://citeseer.ist.psu.edu/582974.html – visitado em abril de 2006. 2006.

[8] BLS, (2003) Specification of the Bluetooth System Version 1.2: https://www.bluetooth.org – visitado em maio de 2006. 2006.

[9] JAKOBSSON, M., Wetzel, S. (2001) “Security Weaknessess in Bluetooth”, em: The Cryptographers Track at RSA Conference, San Francisco, CA.

[10] ARMKNECHT, F. (2002) A Linearization Attack on the Bluetooth Key Stream Generator. www.scholar.google.com – visitado em abril de 2006. 2006.

[11] LEVI, A., Cetintas, E., Aydos, M., Koc, C., e Caglayan, M. (2004) “Relay Attacks on Bluetooth Authentication and Solutions”, em: Computer and Information Sciences – ISCIS 2004: 19Th International Symposium, Kemer-Antalya, Turkey.

[12] BUROWS, M.; ABADI, M.; NEEDHAN, R.: A Logic of Authenication, ACM Transactions on Computers Systems, Vol.8, n. 1, p.18-32,fev.1990.