# Estudo e análise de vulnerabilidades de segurança na tecnologia Bluetooth

**Érico Santos Rocha, Gaspare Giuliano Elias Bruno**

Ciência da Computação – Centro Universitário Lasalle (UNILASALLE)
Av. Victor Barreto 2288 – 91.501-970 – Canoas – RS – Brasil
ericomsr@gmail.com, gaspare@inf.ufrgs.br

***Resumo.*** *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.*

## 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 tais necessidades, surgiram inúmeras tecnologias com este propósito. Entre elas destacam-se a IrDA (*Infrared Data Comunications*) (SEEK, 2005), a UWB (*Ultra Wide Band*) (UWBG, 2005), a *Home* RF (SYSTEM, 2000) 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* (ROUSSEAU, 2001). 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. (GEHRMANN, 2004).

Partindo deste cenário e suas respectivas vulnerabilidades, este trabalho vem a contribuir com as questões de segurança desta tecnologia através de propostas que alteram os processos de autenticação e *paring.* O artigo esta estruturado da seguinte maneira: Seção 2 aborda a arquitetura de segurança Bluetooth; seção 3 apresenta as propostas de melhorias; seção 4 avalia as propostas e a seção 5 traz os trabalhos futuros e as considerações finais deste estudo.

## 2. Arquitetura de Segurança

Os serviços de segurança bluetooth abrangem a confidencialidade, a integridade e a disponibilidade. Estes serviços são garantidos por meio da utilização de procedimentos de criptografia, autenticação e autorização (VANIO, 2000). 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 (KARYGIANNIS, 2002).

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 (BLS, 2003). 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 (GEHRMANN, 2004).

Após o *paring***,** as partes envolvidas terão a certeza de que poderão estabelecer uma conexão segura entre as mesmas (BLS, 2003).

Referindo-se às vulnerabilidades, apesar da tecnologia Bluetooth apresentar determinado grau de segurança, possui um número considerável de falhas, que podem ser verificadas em pesquisas como JAKOBSSON (2001), ARMKNECHT (2002) e LEVI (2004). 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. Outros fatores que contribuem para o surgimento de vulnerabilidades são as falhas de implementação bem como a flexibilidade do padrão que oferece autonomia aos fabricantes para definição de diversos procedimentos relacionados a criprografia e autenticação (GEHRMANN, 2004).

## 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.

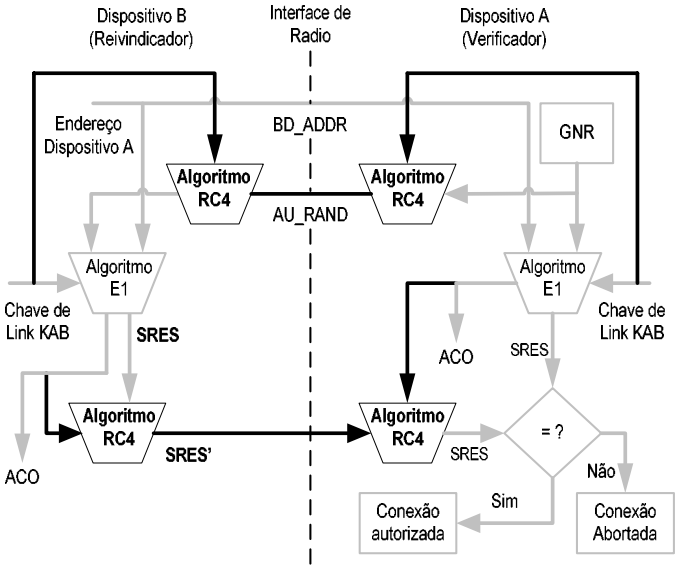



Figura 1a: Modificação no sistema de Autenticação

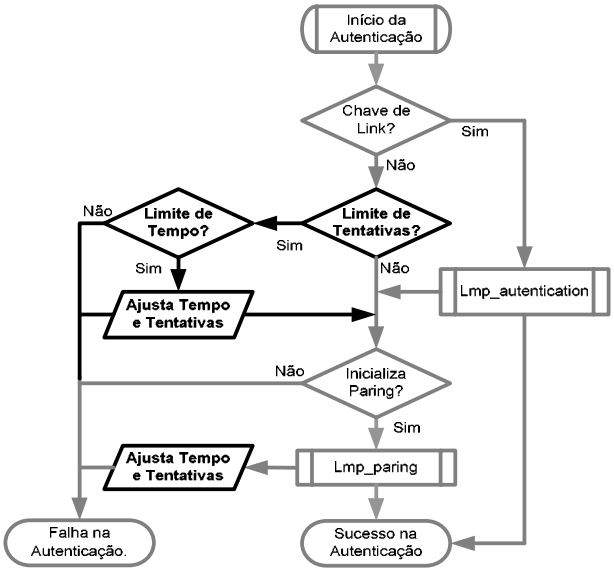



Figura 1b: Modificação no sistema de *paring*

Fonte: Autoria própria,2006

Partindo deste ponto, a seção 3.1 apresenta nova proposta para o processo de autenticação, e 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 trabalha 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*

Em 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. O mesmo 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 a falha

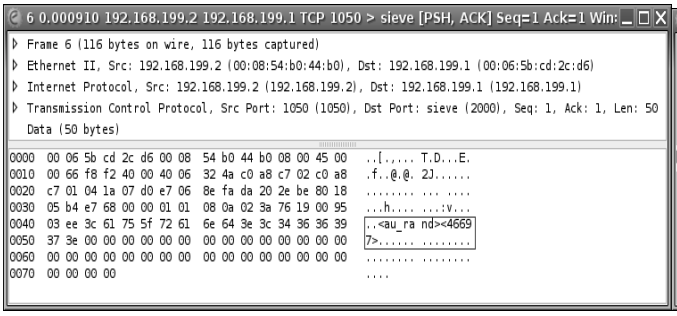
deste procedimento. Quando o número de tentativas sem sucesso chegar ao limite, o controle de tempo é ativado.

Neste momento, o dispositivo entra no modo de bloqueio e somente aceitando apenas novas conexões originadas por dispositivos confiáveis para o qual este já obteve sucesso no processo de *paring* anteriormente.

## 4. Avaliação das propostas

Para avaliar os procedimentos propostos foram utilizados dois métodos distintos, tendo como base o desenvolvimento de um protótipo para a simulação dos processos de *paring* e autenticação no modelo atual e no modelo proposto.

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 tráfego 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.



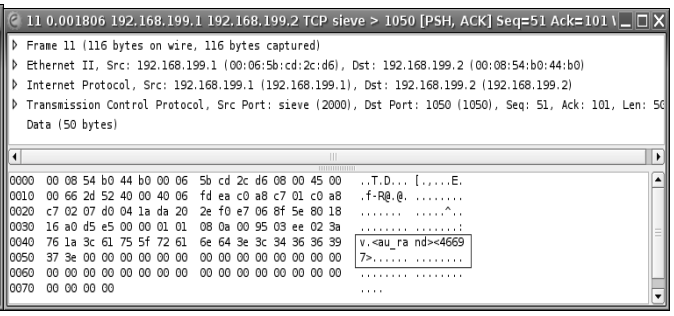




Figura 2a: AU_RAND – Modelo atual Figura 2b: AU_RAND – Proposta RC4

Fonte: Autoria própria,2006

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 proposta obteve êxito ao evitar a quebra do PIN de forma on-line.

## 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 apresentaram 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 estudo proporcionou uma 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, a atualização do módulo BlueHoc pertencente ao NS-2, ou o desenvolvimento de um novo simulador facilitará estudos futuros relacionados a tecnologia Bluetooth.

## Referências


ARMKNECHT, F. (2002) A Linearization Attack on the Bluetooth Key Stream Generator. Disponível em <http://www.scholar.google.com>.

BLS, (2003) “Specification of the Bluetooth System Version 1.2”, www.bluetooth.org.

GEHRMANN, C., Persson, J. e Smeets B. (2004) “Bluetooth Security”, Boston: Artech House.

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

KARYGIANNIS, T. Owens L. (2002) “Wireless Network Security 802.11, Bluetooth and Handheld Devices”, http://citeseer.ist.psu.edu.

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.

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

SEEK, D. (2005) “IrDA”, www.definitionseek.com.

SYSTEM, A. (2000) “Bluetooth Whitepaper”, www.palowireless.com.

UWBG. (2005) “About UWB”, www.uwbgroup.ru, acesso em 20/09/2005.

VANIO, J. (2000) “Bluetooth Security”, www.niksula.cs.hu.fi/~jiitv/bluesec.html.