DOWNLOAD SEGURO EM RÁDIO DEFINIDO POR SOFTWARE (RDS)

VICTOR GODOY VEIGA
BRUNO GUIMARÃES

Universidade de Brasília (UnB)
Departamento de Engenharia Elétrica (EnE)

e-mail: vgveiga@apis.com.br - bruno@ene.unb.br

RESUMO

Com o rápido avanço da tecnologia de comunicações sem-fio, surge um novo paradigma de terminais baseado na capacidade de reconfiguração das funções de rádio por software: o conceito de Rádio Definido por Software (RDS). Neste contexto, o processo de download seguro do software em terminais RDS é fundamental para a viabilização desta tecnologia. Este artigo apresenta uma visão geral dos requisitos para a realização do download seguro em terminais RDS.

ABSTRACT

Within the fast advance in the wireless communication technology, a new model of terminals based on the capability of reconfiguration of the software radio functions rises: the concept of Software-Defined Radio (SDR). In this context, the download of the software in a secure manner to SDR terminals is fundamental to the viability of this technology. This paper presents an overview of the requirements for a secure download in SDR Terminals.

Keywords: Software Defined Radio (SDR), Mobile Fourth Generation, Secure Download.

1. INTRODUÇÃO

Os sistemas de comunicações móveis atuais estão diversificados em vários padrões (UMTS, CDMA-2000, IS-136, DECT, SC-CDMA, entre outros), limitando a área de atuação de seus terminais, cuja compatibilidade é muito depende do próprio *hardware*. É neste contexto que surge a necessidade de se produzir rádios com alto nível de flexibilidade, capazes de se adaptar aos diferentes padrões existentes. O objetivo é garantir sua interoperabilidade através de uma simples atualização de *software*. A reconfigurabilidade do sistema é a principal meta (Mitola, 2000) desta tecnologia definida como Rádio Definido por Software (RDS).

Do ponto de vista comercial, a viabilidade dos RDS implica na redução significativa dos custos em sistemas de comunicação móvel. Rádios Definidos por *Software* evitariam que a evolução de padrões de comunicação gerasse desperdício do investimento massivo anteriormente aplicado aos terminais. Atualmente, devido à incapacidade de atualização, os terminais móveis são geralmente descartados.

Do ponto de vista militar, operações envolvendo vários grupos distintos, cada qual operando de forma isolada e portando padrões específicos de rádios, poderiam com a tecnologia RDS convergir para uma total interoperabilidade.

As atualizações serão realizadas em RDS com o objetivo de disponibilizar novas técnicas de modulação, componentes criptográficos, aplicações, entre outros, através de um simples *download* de novos componentes de *software*.

A segurança do GSM na telefonia móvel, por exemplo, apresentou certas vulnerabilidades notadas apenas após a sua implementação comercial, mantendo as mesmas vulnerabilidades de forma duradoura. Conseqüentemente, seu nível de segurança (Mynttinen, 2000) é atualmente questionado e uma evolução simplesmente exigiria a substituição dos terminais. Por outro lado, um RDS permitirá substituir seu conjunto de algoritmos criptográficos, chaves simétricas e assimétricas, protocolos, técnicas de codificação, mecanismos de proteção e outros fatores que compõem a segurança de um sistema de comunicação.

Dado que a flexibilidade de RDS permite total controle sobre os modos de operação, incluindo freqüência e potência de transmissão/recepção, é de fundamental

importância um mecanismo de alta segurança no processo de *download* de seu código, pois erros nesta etapa podem comprometer a confiabilidade e a disponibilidade de todo o sistema.

A atualização do código, sem o nível adequado de segurança, gera desde uma mera indisponibilidade momentânea de um dado serviço oferecido a um terminal móvel e, em outros casos, interferências eletromagnéticas sobre outros dispositivos, como os terminais ou servidores responsáveis por serviços críticos (emergência).

O problema de segurança da informação em RDS não é trivial e sua solução final ainda permanece am aberto (SDR Forum[1], 2002). Os avanços já obtidos na segurança do *download* na Internet e para as tecnologias sem-fio não são suficientemente capazes de apontar uma solução final para *download* seguro de RDS. Esta situação decorre de complexidades extras não enfrentadas pela Internet ou pelos atuais sistemas de comunicação móvel. Talvez, a principal destas complexidades diga respeito ao fato de que terminais RDS possuem limitação quanto à capacidade de processamento, quantidade de memória e consumo de energia.

A arquitetura de *hardware* no RDS terá papel relevante na segurança da informação, pois comparativamente com os sistemas anteriores uma revolução será proposta. Neste sentido, o modo de operação em RF, mecanismos e componentes lógicos da segurança e a camada de aplicações serão definidos em grande parte por *software*.

A seção 2 deste documento amplia o conceito de RDS, apresenta as principais instituições no mundo e no Brasil que lideram a pesquisa em RDS e, mais adiante, as tendências desta tecnologia no futuro. A seção 3 analisa os requisitos teóricos e conclusões já alcançadas associadas ao problema do *download* seguro em RDS. Uma breve comparação será apresentada sobre técnicas de *download* seguro existente na Internet em relação aos requisitos do RDS. Por último, a seção 4 apresenta uma breve conclusão acerca do tema.

2. RÁDIO DEFINIDO POR SOFTWARE (RDS)

Esta seção apresenta o conceito de Rádio Definido por Software (RDS), analisando, em seguida, algumas características de *hardware* relevantes no projeto de segurança de RDS. Finalmente, discorre sobre as instituições de pesquisa que impulsionam esta tecnologia. Em suma, ressalta a importância de RDS no futuro das comunicações móveis, mostrando a influência na segurança da informação gerada pelas tendências de *software* e de *hardware* que atualmente guiam as pesquisas desta tecnologia.

2.1 Conceito

O SDR Forum define o termo Rádio Definido Software (RDS) como uma coleção de tecnologias de *hardware* e *software* que permite sistemas com arquitetura reconfigurável para redes sem-fio e terminais móveis. Ainda segundo o SDR Fórum, a tecnologia RDS provê solução eficiente e comparativamente barata para o problema de construir dispositivos sem-fio, multi-modo, multi-banda e multi-funcionais que podem ser adaptados, atualizados e/ou melhorados através da atualização de seu conjunto de *software*.

2.2 Considerações na arquitetura de RDS

Um sistema que possui mecanismo seguro de *download* pode ter comprometido sua segurança se o dispositivo não contiver proteções contra ataques físicos. Em Uchikawa, 2002, é proposto um sistema de *download* seguro com a presença de mecanismos *tamper-proof* (àprova de violação física) capazes de proteger áreas críticas dos terminais (regiões de memória onde são armazenadas senhas, chaves criptográficas, entre outros componentes de segurança).

Do ponto de vista de poder computacional, o avanço é notável e crescente na área de processamento digital de sinais, especialmente em dispositivos FPGA (Cummings, 1999 e Reed, 2002) e DSP (Efstathiou, 1999).

De uma forma geral, as tecnologias disponíveis para uso em RDS são: FPGA, DSP e ASIC (*Application Specific Integrated Circuits*).

A figura 1 exibe o compromisso entre flexibilidade e desempenho destes dispositivos (Ahlquist, 1999 e Reed, 2002).

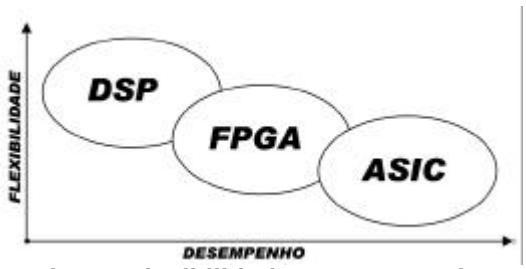

Fig. 1 - Flexibilidade x Desempenho entre dispositivos DSP, FPGA e ASIC.

Diversos protótipos bem sucedidos alcançaram resultados positivos (Lackey, 1995 e Shiba, 2002), ratificando a previsão de viabilidade técnica dos RDS para os próximos 10 ou 15 anos. O protótipo de Lackey, 1995, por exemplo, substitui 15 rádios militares por um único dispositivo.

[1] SDR Forum – http://www.sdrforum.org

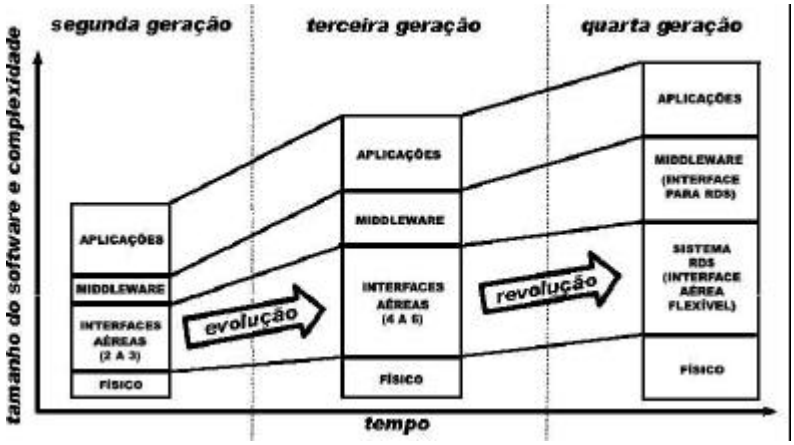

Fig. 2 – Evolução da telefonia e a inserção da tecnologia de Rádio Definido por *Software* (RDS).

O autor destaca, neste caso, que o principal fator limitante foi o baixo poder de processamento disponível naquela época. O DSP adotado em Lackey, 1995 foi o Quad-C40 MCM de 200 MFLOPS (milhões de operação em ponto flutuante) e 1100 MFIPS (milhões de operações em ponto fixo). Para ilustrar o avanço, atualmente a linha TMS320C6000 de DSP da Texas Instruments chega a alcançar 5760 MFIPS e 1350 MFLOPS.

Segundo Cummings, 1999, a tecnologia baseada em FPGA é a mais promissora para os sistemas de RDS, pois vem demonstrando evolução contínua e significativa quanto ao poder computacional, capacidade de armazenamento, aumento de flexibilidade / desempenho e redução no consumo de potência. Avanços significativos em DSP também foram observados.

O uso híbrido de FPGA e DSP pode se tornar uma boa solução nos projetos de RDS, pois aproveita as vantagens de cada dispositivo e explora o paralelismo computacional necessário ao funcionamento do sistema. A atual preferência ao redor da tecnologia FPGA a colocará em destaque nos projetos de RDS futuros.

A figura 3 mostra a evolução da capacidade da tecnologia nos últimos anos (Xilinx, 1998).

De acordo com Baab, 2002, a quarta geração (4G) deverá empregar técnicas de RDS. A figura 2 exibe esta tendência de evolução no sentido de buscar uma maior flexibilidade. Pesquisas em uma geração futura, identificada como 4G (posterior a 3G, B3G e NG (*Next Generation*)) de sistemas de comunicação móvel encontram-se em seus estágios iniciais e seus primeiros produtos surgirão no mercado em cerca de 10 ou 15 anos.

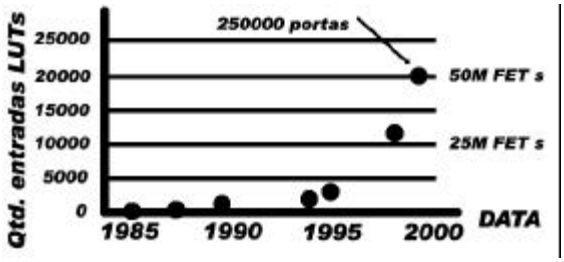

Fig. 3 – Evolução na densidade de portas (*poder de processamento e capacidade de armazenamento*) das famílias de chips FPGA - fabricante Xilinx.

2.3 Futuras gerações de telefonia móvel e a importância da tecnologia de RDS

Desde 1980, um crescimento exponencial de sistemas de telefonia móvel foi observado, produzindo em todo o mundo uma grande variedade de padrões analógicos e digitais. A competição industrial em 2000 entre Ásia, Europa e América promoveu um caminho muito difícil em torno da definição de um padrão único para sistemas móveis, embora as análises de mercado ressaltem os benefícios da implantação de um sistema global único. Neste contexto, o conceito de Rádio Definido por Software emerge como uma solução pragmática.

A segunda geração (2G) de tecnologia sem-fio consiste em uma grande variedade de padrões incompatíveis e o principal objetivo em desenvolvimento, a terceira geração (3G), é a compatibilidade entre esses padrões. Mesmo se esses padrões de celulares convergirem globalmente, sistemas 3G requerem sistemas multi-modo e modo de seleção automático de operação.

2.4 Instituições associadas à tecnologia de Rádio Definido por Software (RDS)

As grandes motivações baseadas em interesses militares e comerciais fazem com

que grande parte da pesquisa seja desenvolvida em instituições governamentais e privadas ou de interesse privado, como o departamento de defesa americano, Sony, Samsung, Motorola, Siemens, Nokia, entre outras.

Dentre as instituições de caráter público, o SDR Forum ocupa papel de destaque no incentivo a pesquisa e padronização da tecnologia RDS. Em especial, ele atualmente aloca esforços consideráveis sobre o problema da segurança no *download* em RDS.

Grupos de telefonia móvel na Europa também avançam em suas pesquisas contribuindo para o desenvolvimento da telefonia móvel, entre eles: ITU (*International Telecommunication Union)*, ETSI (*European Telecommunications Standards Institute*) e GSM *Association*. Todos possuem departamentos, grupos de pesquisa ou parcerias na busca e padronização das soluções de segurança da informação.

O grupo 3GPP[2] (*Third Generation Partnership Project*) e seu subordinado ramo MExE (*Mobile Execution Environment*) atuam na padronização de ambientes de execução para a telefonia móvel. A grande motivação do MExE, encontra-se no sucesso da Internet como ambiente de proliferação de diversos tipos de aplicações compatíveis com as mais diferentes arquiteturas de *hardware* de computadores pessoais. O MExE almeja padronizar protocolos para que os mais variados aparelhos de comunicação móvel futuros (desde *hand-sets,* celulares, e até mesmo estações de trabalho), usufruam dos mesmos aplicativos, ou seja, multi-plataforma associada àcamada de aplicações.

A abordagem proposta pelo MExE é extremamente importante no que se refere ao futuro da tecnologia RDS, pois todo e qualquer esquema de segurança da informação a ser adotado deverá assumir que o funcionamento dos terminais irá operar corretamente em multi-plataforma, situação extremamente diferente da atual segunda geração (2G) e obviamente mais complexa.

O Projeto 4G Brasil é uma das iniciativas de pesquisa conjunta, reunindo várias instituições nacionais e internacionais na pesquisa de RDS. A Universidade de Brasília (UnB) também possui grupo de pesquisa em RDS.

3. SEGURANÇA DA INFORMAÇÃO NO DOWNLOAD DE SOFTWARES EM RDS

Esta seção aborda os requisitos teóricos necessários à segurança do processo de reconfiguração de sistemas RDS. Além disso, retrata o problema do *download* seguro de sistemas RDS comparativamente ao *download* da Internet e em tecnologias de comunicação móvel/sem-fio.

A segurança em sistemas de comunicação móvel é fundamental e de interesse público. Exemplos evidentes estão ligados a situações onde a segurança das pessoas depende diretamente da transmissão e recepção de chamadas e informações de emergência, podendo significar a diferença entre a vida e a morte.

3.1 Requisitos de segurança da informação nas telecomunicações em geral

Os desafios de segurança da informação nas telecomunicações, em geral, podem ser divididos em 6 categorias: operação confiável do sistema, autenticação, autorização, integridade, privacidade e irretratabilidade.

Estes requisitos gerais de segurança são similares para diferentes tipos de sistemas de comunicação, sem-fio ou não.

A indústria trabalha na busca de soluções de segurança nas mais variadas plataformas, comumente envolvendo todos os requisitos acima citados. O exemplo mais atual é a própria Internet.

3.2 Tópicos sobre a segurança de sistemas sem-fio

A liberdade de movimento derivada da introdução de sistemas de comunicação sem-fio trouxe novos paradigmas no cenário da segurança da informação. Novos requisitos incluem: proteção das estruturas de controle do sistema, uso malicioso, interceptação de mensagem, roubo de propriedade intelectual e até uso de serviços ilegalmente.

O nível de vulnerabilidade é superior em sistemas de comunicação sem-fio, especialmente pelo advento da transmissão diretamente na atmosfera. Já é possível observar que as redes sem-fio começam a sofrer ataques notáveis. Em 2001, por exemplo, (SDR FÓRUM, 2002) o Japão sofreu um ataque onde *e-mails* maliciosos alcançaram 13 milhões de usuários de telefonia móvel. Ao abrir o *e-mail*, o dispositivo de comunicação discava o número do serviço de emergência durante 20 minutos consecutivos. Obviamente informações importantes como agendas, números de cartões de crédito e senhas podem estar vulneráveis diante de ataques desta natureza.

[2] 3GPP (3rd *Generation Partnership Project)* - http://www.3gpp.org

Tabela 1 – Comparação entre o *download* na Internet e na no RDS.

Questões de Segurança		*Download* em RDS	*Download* na *Internet*
Requisitos Principais	- integridade - autenticidade - confidencialidade - irretratabilidade	sim sim sim sim	Sim algumas vezes algumas vezes algumas vezes
Partes envolvidas	- usuário - provedor - autoridade certificadora	sim sim obrigatório	Sim sim opcional
Primitivas criptográficas	- chaves simétricas - funções *hash* (integridade) - autenticação	sim sim sim	Sim sim sim
Requisitos da arquitetura RDS	- proteção física (*tamper-proof*) - baixa utilização de recursos computacionais	sim sim	Não opcional

Uma das tecnologias sem-fio comumente difundidas é o padrão IEEE 802.11 atuando em redes locais. Este padrão propõe o algoritmo WEP (*Wired Equivalent Privacy*) como mecanismo de proteção. Sua cifração é baseada no RC4. Entretanto, sérias deficiências foram identificadas até o momento (Borisov, 2001). A fraqueza deste sistema encontra-se no tamanho relativamente pequeno de seu vetor de inicialização (VI). O protocolo WEP usa 24 bits para seu VI e uma chave secreta de 40 bits. Para citar o nível de vulnerabilidade atual, um aluno de graduação da *Rice University* chamado Adam Stubbefield, com apenas 20 anos de idade, foi capaz de quebrar a cifração do WEP.

O exemplo acima ilustra que o nível de segurança em RDS não pode incorrer em deficiências graves como a observada no WEP.

3.3 Requisitos de segurança do download na Internet e em Rádio Definido por Software

O *download* na Internet é difere do *download* em RDS e suas principais diferenças encontram-se nos requisitos de segurança, vide tabela 1.

Apesar do avanço nos mecanismos de segurança já bastante evoluídos ao longo dos últimos anos na Internet, pontos obrigatórios específicos de RDS aumentam a complexidade do *download* seguro, como a autenticidade do código e sua aprovação junto à agência r eguladora de telecomunicações local.

3.4 A segurança em dispositivos RDS

Quanto maior as complexidades dos dispositivos de comunicações, maiores são suas vulnerabilidades e mais complexo se torna o desafio evitá-las. Dispositivos que operam em diversos sistemas de comunicação simultaneamente são, em geral, mais complexos que dispositivos RDS. Entretanto, diferentemente destes dispositivos, os dispositivos RDS necessitam atualizar *software* de plenamente segura.

O desafio enfrentado pelo sistema de segurança da tecnologia RDS é, portanto, mais complexo do que o dos sistemas dos dispositivos de comunicação móvel existente atualmente. Os principais problemas e ataques relacionados à tecnologia RDS são:

- Interferência no canal de comunicação gerada por equipamentos com defeito;
- Uso ilegal ou comprometimento de canais de segurança pública (canais reservados para órgãos governamentais);
- Ataques de personificação (tanto do usuário, como do servidor);
- Ataques de negação de serviço;
- Ameaças àintegridade do sistema e dos *softwares*;
- Escuta nos canais de comunicação ameaçando a privacidade de usuários.

4. AGRADECIMENTOS

Agradecemos ao Prof. Eduardo Wolski pelo apoio e dedicação para a viabilidade deste trabalho e ao Prof. Leonardo Menezes pela iniciativa e incentivo à pesquisa em RDS na Universidade de Brasília.

5. CONCLUSÃO

A evolução da tecnologia de Rádio Definido por *Software* (RDS) mostra-se promissora no futuro das comunicações móveis e a solução segura do processo de *download* em terminais RDS foi enfatizada como um fator essencial para a viabilização da tecnologia. Esta é uma área de importância crescente em nível de pesquisas tanto na área acadêmica como em áreas comerciais e militares.

Este artigo apresenta uma visão geral do problema de download seguro em RDS, com o foco nos requisitos necessários já amplamente debatidos na comunidade científica.

A definição técnica final para o problema de download seguro ainda é uma questão em aberto. Dado o estado atual de pesquisa no ramo do download seguro, a implementação prática das metas de segurança propostas pelo SDR Fórum passarão ainda por vários níveis de evolução até alcançar um padrão final, capaz de tornar o global o uso da tecnologia de RDS. Destarte, esforços contínuos de pesquisa serão fundamentais para atingir o objetivo do *download* seguro nos terminais RDS.

6. REFERÊNCIAS BIBLIOGRÁFICAS

AHLQUIST, Gregory C.; RICE, Michael e NELSON, Brent. *Error Control Coding in Software Rádios: An FPGA Approach.* IEEE Personal Communications, agosto de 1999.

BABB, D.; BISHOP, C. e DODGSON, T. E. *Security Issues for Downloaded Code in mobile phones.* IEEE Eletronics & Communication Engineering Journal, outubro de 2002.

BORISOV, N.; GOLDBERG, I.; WAGNER, D. *Intercepting Mobile Communications: The insecurity of 802.11*, 2001.

CUMMINGS, MARK e HARUYAMA, SHINICHIRO. "FPGA in the Software Radio". IEEE Communications Magazine, pp. 108 a 112, fevereiro de 1999.

EFSTATHIOU, Dimitrios; FRIDMAN, Jose; ZVONAR, Zoran. *Recent Developments in Enabling Technologies for Software Defined Radio.* IEEE Communications Magazine, agosto de 1999.

LACKEY, Raymond; UPMAL, Donald. *Speakeasy: The Military Software Radio.* IEEE Communication Magazine, maio de 1995.

MYNTTINEN, Juha. *End-to-end security of mobile data in GSM*. Tik-110.501 Seminar on Network Security, 2000.

MITOLA, Joseph. *Software Radio Architecture: Object Oriented Approaches to Sem-fio Systems Engineering.* John Wiley and Sons, 2000.

REED, Jeffrey H. *Software Radio: A Modern Approach to Radio Engineering.* Prentice Hall PTR, 2002. ISBN 0-13-081158-02002.

SDR FORUM. *Report on Issues and Activity in the area of security for Software Defined Radio* SDRF-02-0003-V0.00, setembro de 2002.

SHIBA, Hiroyuki; SHONO, Takashi; SHIRATO, Yushi; TOYODA, Ichihiko; UEHARA, Kazuhiro; *Software Defined Radio Prototype for PHS and IEEE 802.11 Sem-fio LAN*. IEICE Transaction Community, VOL.E85-B, NO. 12, dezembro de 2002.

XILINX. *The Programmable Logic Data Book*, San Jose, Califórnia CA, 1998.

UCHIKAWA, Hironori; UMEBAYSAHI, Kenta; KOHNO, Ryuji. *Secure Download System based on software defined radio composed of FPGA.* Yokohama National University, IEEE PIMRC 2002.

7. BIOGRAFIAS

Bruno Guimarães. Formado em Engenharia de Redes de Comunicação pela Universidade de Brasília (UnB) em 2003. Trabalha na empresa Link Data Informática.

Victor Godoy Veiga. Formado em Engenharia de Redes de Comunicação pela Universidade de Brasília (UnB) em 2003. Trabalha na empresa Z Tecnologia.