Segurança da Informação para Aplicações Interativas no Sistema Brasileiro de Televisão Digital

Thatiane Cristina dos Santos
Universidade Estadual de Campinas (UNICAMP), Campinas, São Paulo, Brasil, eng.thatiane@gmail.com

Vicente Idalberto Becerra Sablón
Centro Universitario Salesiano de São Paulo (UNISAL), Campinas, São Paulo, Brasil, vsablon@sj.unisal.br

Yuzo Iano
Universidade Estadual de Campinas (UNICAMP), Campinas, São Paulo, Brasil, yuzo@decom.fee.unicamp.br

ABSTRACT

This work presents a proposal for transmitting information securely in interactive applications in the Brazilian digital TV. For the creation of interactive applications middleware offers a programming language, which was tested using known vulnerabilities in other systems, enabling the identification of flaws and points where the system becomes unsafe, endangering the information of the user. Applications were exposed vulnerabilities and identified a routine for programming to be done safely.

Keywords: Ginga, Digital Television, Information Security, SBTVD.

RESUMO

Apresenta-se neste trabalho uma proposta para a transmissão da informação com segurança nas aplicações interativas no sistema brasileiro de TV digital. Para a criação das aplicações interativas o *middleware* oferece uma linguagem de programação declarativa que foi testada usando vulnerabilidades conhecidas de outros sistemas, possibilitando a identificação de falhas e pontos onde o sistema se torna inseguro, colocando em risco as informações do usuário. As aplicações foram expostas as vulnerabilidades e identificou-se uma rotina para que a programação seja feita de forma segura.

Palavras chaves: Ginga, Televisão Digital, Segurança da Informação, SBTVD.

1. INTRODUÇÃO

A TV Digital oferece para o usuário não apenas melhor qualidade de imagem e som, mas também uma gama de novos serviços e aplicações de entretenimento e de informações. Assim sendo, a adoção da TV Digital no Brasil aliada ao avanço da tecnologia, permite que serviços e aplicações sejam disponibilizados mesmo em localidades remotas, contribuindo para a universalização e democratização de informações e serviços eletrônicos, permitindo a inclusão social de uma parcela maior da população brasileira.

A interatividade possibilita utilizarmos a televisão digital para fazer transações pessoais, comerciais como se estivesse usando a internet. Isso gera a necessidade de mecanismos de seguranças capazes de identificar ameaças durante a transição de informações através das aplicações interativas.

O *Middleware* do Sistema Brasileiro de Televisão Digital, conhecido como Ginga, proporciona um ambiente onde as transações de informações em aplicações como bancárias (*t-banking*) e de comércio *(t-commerce)* são realizadas, que será melhor explicada na seção 2.3. Nessas transações os dados pessoais dos usuários devem ser protegidos e a proteção das aplicações deve manter a disponibilidade, confiabilidade e a integridade dos dados [1].

O estudo objetiva manter a segurança da informação para aplicações do Sistema Brasileiro de Televisão Digital. Como todos os outros sistemas embarcados, as aplicações precisam ter uma rotina que determina se estas foram desenvolvidas de maneira que assegura que os dados não serão violados.

2. O SISTEMA BRASILEIRO DE TELEVISÃO DIGITAL - SBTVD

O governo brasileiro determinou alguns dos requisitos básicos para o Sistema de TV Digital, como o baixo custo e robustez na recepção, flexibilidade e capacidade de evolução, interatividade e novos serviços, visando promover a inclusão digital e é tratado como um requisito fundamental [2].

A arquitetura proposta baseia-se no modelo de referência da União Internacional de Telecomunicações - UTI [2]. No projeto brasileiro optou-se por representar de forma única as funções de Multiplexação e Transporte, agrupadas na camada de transporte. De forma análoga, a codificação de canal, modulação e transmissão estão representadas em um único módulo. Por fim, o receptor digital foi expandido, para que fosse possível dar uma ênfase maior à sua arquitetura.

O sistema é definido como uma plataforma multimídia capaz de transmitir sinais de áudio e vídeo de alta qualidade, bem como dados, utilizando o sinal de radiodifusão. A capacidade de transmissão de dados, que podem estar vinculados ou não à programação, possibilita o desenvolvimento de novos serviços e aplicações digitais [3].

O sistema atua como uma plataforma de comunicação onde a fonte de conteúdo, representada no diagrama pela produção de conteúdo, e os usuários finais, que fazem uso das aplicações interativas, e está dividido em duas entidades complementares: a difusão e acesso e o terminal de acesso, como mostra a Figura 1.

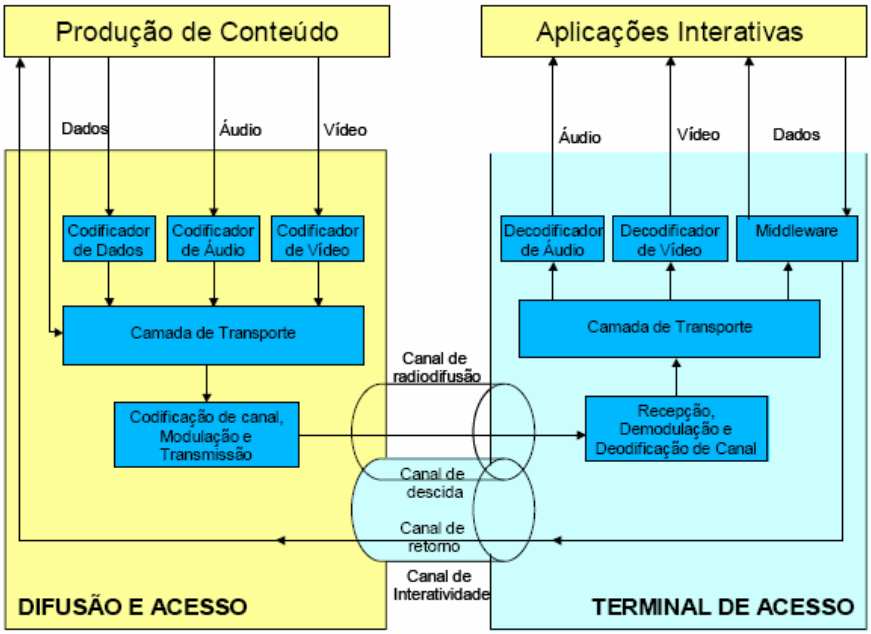

Figura 1 - Diagrama de Fluxo de informação [3]

Desta forma, o sistema é analisado a partir dos seguintes subsistemas e respectivas tecnologias:

- **Transmissão e Recepção:** englobam o módulo Codificação de Canal, Modulação e Transmissão, do lado da Difusão e Acesso, e o módulo de Recepção, Demodulação e Decodificação de Canal, no Terminal de Acesso.
- **Codificação de Sinais Fontes:** este subsistema é dividido em três subsistemas:
  - Codificação de Áudio: composto pelo Codificador e pelo Decodificador de Áudio
  - Codificação de Vídeo: composto pelo Codificador e pelo Decodificador de Vídeo
  - Codificação de Dados: corresponde ao Codificador de Dados.
- **Camada de Transporte:** engloba a Multiplexação e a Demultiplexação.

- ***Middleware*:** presente apenas no Terminal de Acesso, o *Middleware* representa a camada de *software* no lado do Terminal de Acesso.
- **Canal de Interatividade:** compreende o Canal de Descida e o Canal de Retorno, abordando a tecnologia e a estrutura de rede a serem utilizadas.
- **Terminal de Acesso:** devido à sua complexidade, por representar uma estrutura de *hardware* única, responsável pelo funcionamento do sistema no lado do usuário [3].

2.1 PADRÕES ADOTADOS PELO SISTEMA BRASILEIRO DE TV DIGITAL

O sistema de TV digital é composto por um conjunto de padrões que regulam cada uma das etapas descritas na seção 2.

O Sistema Brasileiro de TV Digital adotou os seguintes padrões:

- Para codificação de áudio foi adotado o padrão *Moving Picture Expert Group* – parte 4 - MPEG4 com 2 níveis de perfil para receptores fixos e móveis (*Advanced Audio Coding* - AAC@L4 – para multicanal 5.1 e *High Efficiency Advanced Audio Coding* -HEAAC v1@L4 – para estéreo) e 1 nível de perfil para receptores portáteis (HEAAC v2@L3 – dois canais).
- Para codificação de vídeo foi adotado o padrão MPEG4-AVC com o nível de perfil (alto), *High Profile* - HP@L4.0 para receptores fixos e móveis e o nível de perfil (básico), *Basic Profile* - BP@L1.3 para receptores portáteis.
- Para o sistema de transporte (multiplexação e demultiplexação) foi adotado o padrão MPEG-2 Systems.
- Para o processo de modulação foi adotado o padrão *Band Segmented Transmission Orthogonal Frequency Division Multiplexing* - BST-OFDM/SBTVD-T.
- Para a camada de *middleware* foi adotado o padrão GINGA [3].

Na Figura 2 apresenta-se os padrões de referência e as interações entre eles.

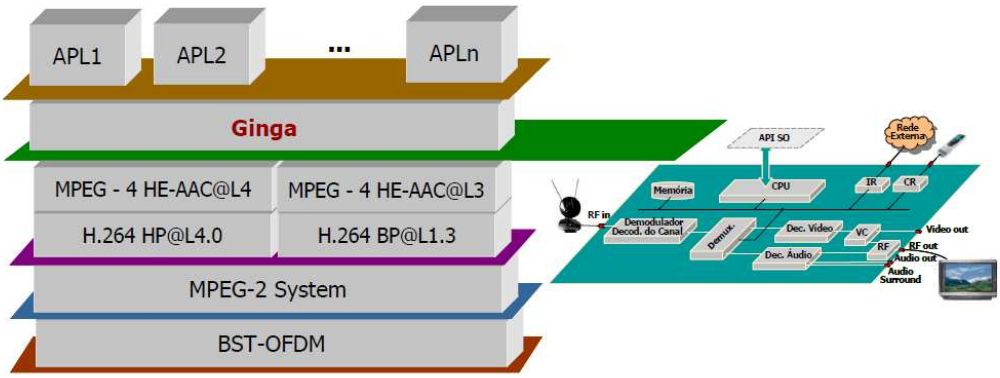

Figura 2 - Padrões de referência do sistema brasileiro de TV digital terrestre. [3]

2.2 CANAL DE INTERATIVIDADE

O canal de interatividade é um meio que possibilita ao usuário, individualmente, interagir encaminhando ou recebendo informações e solicitações das emissoras/programadoras como: provedor de conteúdo, provedor de serviço/aplicações, provedor de interatividade, provedor de rede, programador, distribuidor, outros usuários. Ele é constituído pela interconexão das redes de televisão com as redes de telecomunicação, resultando em dois canais de comunicação: canal de descida e o canal de retorno [4]. A Figura 3 é o diagrama simplificado dos canais.

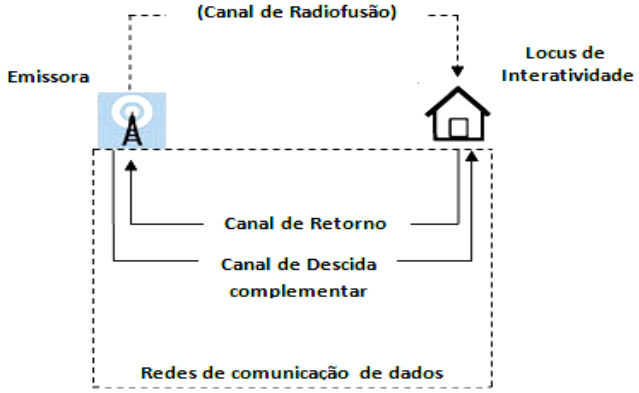

Figura 3 - Diagrama simplificado do sistema canal de retorno [5]

O canal de descida estabelece a comunicação no sentido emissoras/programadoras para os usuários, sendo constituído pelos canais de radiodifusão, podendo ter uma comunicação broadcast (ponto-multiponto), aberta e disponível a todos os usuários ou unicast (ponto a ponto) individualizada. Já o canal de retorno estabelece a comunicação no sentido dos usuários para as emissoras/programadoras, e é composto por qualquer tecnologia de redes de acesso que estabeleça essa ligação. Desse modo, pode ocorrer a transferência e troca de dados, de ambos os lados, permitindo assim a interatividade [6]. Fazendo uma análise sobre um ponto de vista técnico, o grau de interação do usuário com as aplicações, serviços e conteúdos interativos podem ser divididos em três categorias: local, intermitente e permanente [7].

A interatividade local é a mais básica das três categorias. O difusor é composto pelo provedor de serviço de difusão, que gera o sinal dos programas de televisão para que o canal de difusão transmita os fluxos de áudio e vídeo para o receptor doméstico de forma unidirecional. Já na interatividade intermitente ou remota unidirecional, algumas mudanças significativas são realizadas, de forma que, nessa categoria, a comunicação do usuário em direção ao difusor seja possível. O difusor apresenta, além do provedor do serviço de difusão, outro provedor denominado provedor de serviço de interação. A interatividade permanente ou remota bidirecional é considerada uma evolução da interatividade intermitente, na qual a comunicação dos dados no canal de interação deixa de ser unidirecional para se tornar bidirecional, existindo para isso um canal de retorno dedicado no receptor digital [7] [8].

2.2.1 APLICAÇÕES INTERATIVAS

Para o desenvolvimento, estudo, especificações e protótipos de aplicações interativas compatíveis com o padrão de *middleware* do padrão brasileiro de Televisão Digital compreende um conjunto de serviços e aplicações interativas disponibilizados através de um televisor e um decodificador, chamado *Set-top-Box*. A TV interativa permite que o telespectador através dos aplicativos interaja com a programação, como por exemplo, escolhendo a câmera (ângulo) em um jogo de futebol, participando de votações e jogos de auditório, escolhendo suas preferências em aplicativos interativos como previsão de tempo, bolsas de valores, notícias de última hora, etc. [11]

As aplicações para TV digital dão um teor computacional à televisão com conceitos utilizados por um computador. Além de permitir a navegação do usuário pelas informações disponibilizadas através das aplicações, aquelas que são mais avançadas permitem o envio de dados ao provedor do conteúdo utilizando possivelmente a própria infra-estrutura da internet, caracterizando a utilização do canal de retorno. [12]

2.3 O MIDDLEWARE DO SISTEMA BRASILEIRO DE TELEVISÃO DIGITAL - GINGA

2.3.1 ARQUITETURA DO MIDDLEWARE GINGA

Há dois tipos de aplicações, as chamadas declarativas e as procedurais. Um conteúdo declarativo deve ser baseado em uma linguagem declarativa, isto é, em uma linguagem que enfatiza a descrição declarativa do problema, ao invés da sua decomposição em uma implementação algorítmica. Um conteúdo procedural deve ser baseado em uma linguagem não declarativa [9].

Linguagens não declarativas podem ser linguagens baseadas em módulos, orientadas a objetos. Na literatura especializada usa-se o termo procedural para representar todas as linguagens que não são declarativas. Numa programação procedural, cada passo é informado ao computador [10]. Nessa linguagem o programador possui um maior poder sobre o código, estabelecendo o fluxo de controle e execução de seu programa. A linguagem mais usual encontrada nos ambientes procedurais de um sistema de TV Digital é o Java TV [11].

O Ginga-NCL, também chamado de Máquina de Apresentação é um subsistema lógico do Sistema Ginga que processa documentos NCL, conforme mostra a Figura 4. Um componente-chave do Ginga-NCL é o mecanismo de decodificação do conteúdo informativo (NCL formatter), e o mecanismo LUA, que é responsável pela interpretação dos scripts LUA, programação procedural com poderosas construções para descrição de dados baseadas em tabelas associativas e semântica extensível. [12][13].

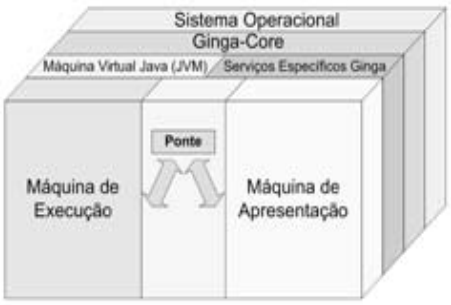

Figura 4 - Arquitetura em alto nível do *middleware* Ginga [10]

3. SEGURANÇA DA INFORMAÇÃO

O termo Segurança da Informação significa proteger uma informação ou um sistema de informação do acesso, uso, divulgação, modificação ou destruição não autorizada; provendo integridade, confidencialidade e disponibilidade. A garantia de integridade significa proteger o conteúdo contra modificação ou destruição imprópria do conteúdo, inclui ainda a garantia da autenticidade da fonte da informação e o não repúdio pelo seu expedidor. A confidencialidade é relacionada à privacidade, restringindo o acesso e divulgação das informações. Já a característica de disponibilidade garante acesso à informação quando esta for necessária de maneira rápida e precisa. A segurança na televisão digital terrestre, nada mais é do que a aplicação destes conceitos aos casos de uso da televisão digital [13].

Os principais objetivos são assegurar a proteção da informação, via mecanismos de controle, contra possíveis ameaças existentes - ataques (ação intencional), acidentes (mau uso), defeitos ou falhas - que ocorram onde a informação estiver sendo criada, processada, armazenada ou transmitida. A Segurança da Informação também possibilita saber o quanto o sistema é resiliente, ou seja, o poder de recuperar-se após uma falha ou um ataque.

Os requesitos da segurança da informação são:

- **Integridade:** tem como objetivo principal a proteção à exatidão e complexidade da informação e dos métodos de processamento. Esse requisito protege a informação contra qualquer alteração não autorizada. A violação da integridade pode ser o primeiro passo de um possível ataque e ainda alterar a confiabilidade do dado e ou sistema;
- **Confidencialidade:** o objetivo desse requisito é assegurar que a informação esteja acessível somente às pessoas autorizadas, refere-se proteção aos dados e sistemas para não serem expostos aos usuários não autorizados. O impacto da violação da confidencialidade das informações ou sistemas podem expor publicamente dados pessoais, corporativos e de governo indevidamente;

- **Disponibilidade**: assegurar aos usuários autorizados o acesso à informação e aos ativos associados. Este se refere ao fato do dado e ou sistema estar liberado para ser acessado pelo usuário no tempo correto;
- **Autenticidade:** é a garantia de que a identidade alegada ou atribuída ao usuário da informação seja verdadeira. A correta identificação do usuário ou ponto de origem (dispositivo) também retrata o requisito autenticidade;
- **Responsabilidade:** permite que as ações de uma determinada entidade em questão sejam rastreadas (imputabilidade) com impossibilidade de sua repudiação, negação ou retratação;
- **Privacidade:** é o direito do usuário em restringir o conhecimento e o acesso aos seus dados pessoais. Uma das formas de preservar a privacidade nas suas transações eletrônicas e ou aplicações é assegurar o anonimato do usuário. A privacidade é considerada como um aspecto de sigilo ou confidencialidade.

3.1 A SEGURANÇA EM SERVIÇOS DA TELEVISÃO DIGITAL INTERATIVA

O usuário pode receber um sinal de áudio e vídeo com qualidade superior, possibilita que ele tenha a interatividade com diversos serviços interativos, associados ou não a programação. São exemplos de aplicações interativas: distribuição de imagem em eventos esportivos, placar em tempo real, legendas e áudios em vários idiomas, previsão do tempo, indicativos financeiros, entre outras.

Para que seja assegurada a proteção do receptor/conversor alguns aspectos devem ser tratados:

a) A segurança dos sistemas embarcados;
b) Segurança em mobilidade (*smartphones*);
c) Segurança na plataforma e computação para transações comerciais.

A Figura 5 apresenta a difusão de Aplicações em televisão digital [14].

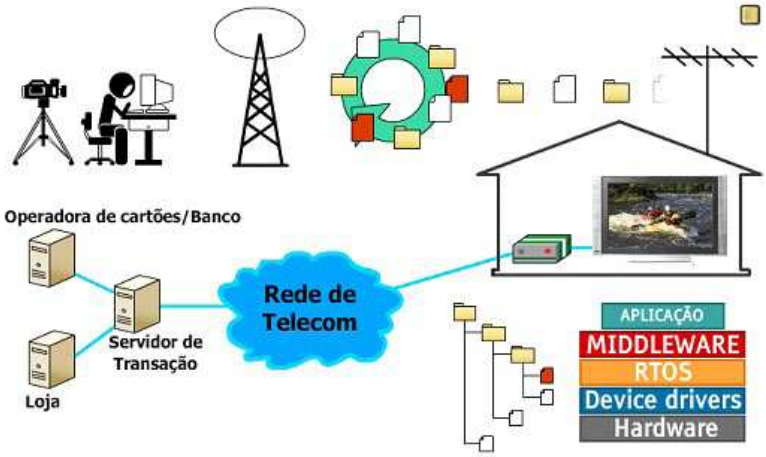

Figura 5 – Difusão de Aplicações em Televisão Digital [14]

As relações comerciais entre empresas por meio eletrônico foram potencializadas pelos cartões de crédito, internet e a globalização. A segurança da troca de informações não é mais preocupação apenas das empresas, mas do cliente ou consumidor. A segurança da informação é parte estratégica do negócio ou serviço podendo traduzir em lucro, aumento de competitividade e fator de redução de perdas.

3.2 AMEAÇAS E VULNERABILIDADES

As vulnerabilidades são pontos em que o sistema é susceptível a ataques. Consideramos aqui também, além das fragilidades do sistema, erros que nele existam. A identificação das vulnerabilidades técnicas nem sempre é trivial, requerendo, em geral, profundo conhecimento de Tecnologia da Informação e de Comunicação.

Os tipos de ameaças e vulnerabilidades irão variar conforme o ambiente interno e externo da organização. A infraestrutura de dados e de comunicação utilizada, a organização dos processos, a cultura de segurança dos

usuários, o apoio da direção à política de segurança da informação, a competitividade do mercado, a visibilidade da organização, tudo isso são fatores a serem considerados.

Identificar os riscos importa em identificar as ameaças e as vulnerabilidades que podem ser aproveitadas por estas aos sistemas de informação envolvidos e o impacto que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos.

Contudo, diversas são as vulnerabilidades associadas a procedimentos ou ao comportamento humano. A questão das senhas é um bom exemplo. É fácil entender que, quanto mais complexas as senhas, mais difícil se torna a descoberta delas. Porém, na mesma proporção, mais difícil se torna decorá-las.

Uma única senha igual para todos os sistemas facilita a memorização, mas por outro lado se traduz em uma vulnerabilidade que afeta todos os sistemas em questão. Outra alternativa encontrada por algumas pessoas quando a senha é muito complexa é anotar a senha em algum papel. A vulnerabilidade da senha é acrescida pela vulnerabilidade do acesso ao papel com a senha.

3.2.1 SISTEMAS DE VERIFICAÇÃO DE VULNERABILIDADES

Sistemas operacionais e demais programas de suporte, tais como o navegador da Internet, máquina Java, frameworks e players, devem ser mantidos sempre atualizados. Normalmente eles possuem algum tipo de controle interno, que pode ser centralizado, informando ou até mesmo atualizando de vez o programa. Incluem-se nesta categoria os programas de proteção, tais como antivírus e *antispywares*. A habilitação da atualização automática de programas pode pesar na rede ou no computador e em alguns casos pode-se considerar uma atualização mais espaçada no tempo.

Existem ainda sistemas capazes de verificar se alguma porta do computador está desprotegida e se a configuração do sistema operacional e da rede está compatível com os requisitos de segurança até então conhecidos [16]. A execução destes programas deve ser feita por quem entende as operações por ele propostas.

A integração entre os próprios sistemas da organização podem prover maior segurança ao conjunto. Se, por exemplo, um funcionário está em gozo de férias, não seria normal que ele viesse a acessar um computador de dentro da empresa.

Os ataques contra a confidencialidade podem ter por resultado a liberação de informação não autorizada para fins de divulgação ou fraude. Ataques contra a integridade irão contra a confiabilidade da informação. E ataques contra a disponibilidade irão contra o suporte ao serviço ou a destruição da informação. Seja como for, com certeza as maiores ameaças estão dentro da própria organização, de forma que um firewall pode não ser suficiente [17].

Cada participante da cadeia de valor da Televisão digital tem a sua necessidade de segurança, desde a produção de hardware, o produtor de conteúdo de televisão até a oferta de serviços interativos ao usuário final. Em cada parte há uma necessidade de segurança, como em qualquer sistema embarcado. A Tabela 1 mostra as partes da cadeia, as vulnerabilidades e as ações de seguranças pertinentes a cada uma delas:

Tabela 1 – Necessidade de Segurança no Sistema de Televisão Digital [17]

Vulnerabilidade	Parte do Sistema de Televisão Digital	Necessidade de Segurança
Transação Fraudulenta- Perda/Roubo de Conteúdo	Usuário Final	Privacidade e integridade dos dados pessoais e execução segura de software baixado e instalado
Pirataria de Conteúdo	Provedor de Conteúdo	Proteção de Conteúdo e Gestão de direitos autorais
Falsificação, violação ou corrupção das aplicações	Provedor de Aplicações	Comunicação segura fim-a-fim Irretratabilidade e autencidade
Uso ilegítimo do serviço	Provedor de Serviço	Acesso seguro a rede
Pirataria de Software e clonagem de Hardware	Fabricante/Integrador de Hardware e Software	Proteção da propriedade Intelectual

4. SISTEMA PROPOSTO

4.1 PROVA DO CONCEITO

O modelo prático que permite provar o conceito de vulnerabilidade é apresentado na Figura 6. A metodologia proposta segue o modelo *top-down*, que envolve a concepção do protótipo, definição dos testes, a conclusão do script e análise dos resultados obtidos.

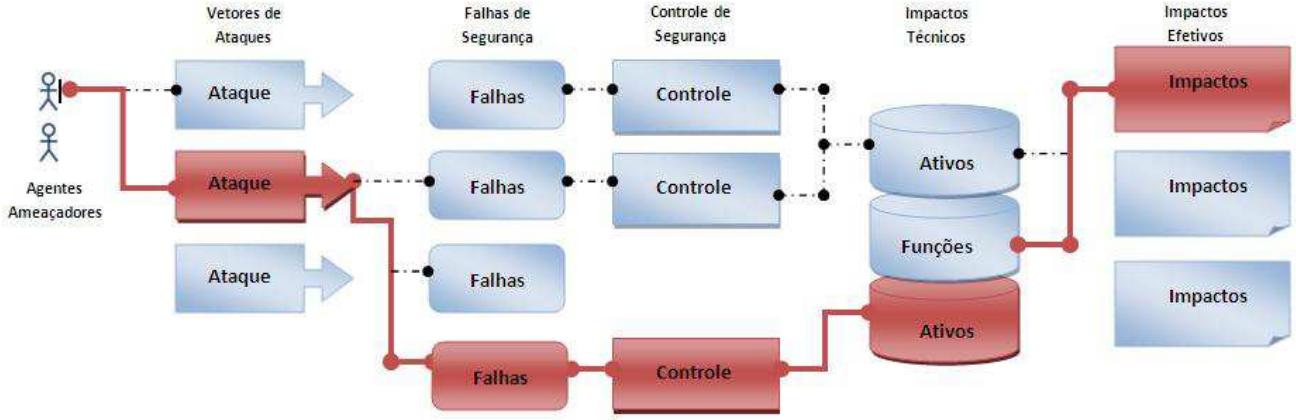

Figura 6 – Metodologia de Identificação de Riscos [18]

Este modelo possibilita provar a viabilidade da metodologia proposta. Para a criação das aplicações interativas, o *middleware* oferece uma linguagem de programação, que foi testada usando vulnerabilidades conhecidas de outros sistemas, possibilitando a identificação de falhas e pontos onde o sistema se torna inseguro, colocando em risco as informações do usuário. As aplicações foram expostas as vulnerabilidades e identificou-se uma rotina para que a programação seja feita de forma segura.

Para determinar o risco, é preciso avaliar a probabilidade associada a cada agente de ameaça, vetor de ataque, e fraqueza de segurança e combiná-lo com uma estimativa do impacto técnico e de negócios.

5. RESULTADOS

5.1 AMEAÇAS E VULNERABILIDADES TESTADAS

As linguagens de programação utilizadas na plataforma de TVDi, o Ginga-NCL e o Lua, foram testadas usando vulnerabilidades já conhecidas e catalogadas pela *Open Web Application Security Project* - OWASP [18].

As rotinas identificadas como vulneráveis na linguagem NCL e Lua são as rotinas do pacote OS (operacionais), de carga e execução de comandos e o pacote IO (entrada e saída de dados). As vulnerabilidades em Lua estão ligadas as rotinas utilizadas nas aplicações. A Tabela 2 mostra as rotinas que deixam o sistema suscetível a ameaças.

Tabela 2 – Rotinas Perigosas [18]

Categoria	Rotina	Tipo de Ameaça ao Sistema
Pacote OS	os.remove() os.rename()	Acesso e modificação do sistema de arquivos.
Carga /execução de código	loadfile() dofile()	Injeção de código malicioso via arquivos.
Pacote IO	io.write() io.read()	Por se tratar de API para acesso a arquivos, é comumente associada a ataques de negação de serviço.

Caso não haja um isolamento das informações todo o sistema será afetado pela rotina maliciosa que manipulará os dados do usuário.

As rotinas perigosas geram inserções de dados na saída modificando a aplicação original e resultado esperado, como a utilização de arquivos não permitidos, a exposição de dados confidenciais e deixando o sistema vulneráveis a ataques de outros programas.

Estas rotinas identificadas se não utilizadas de forma correta podem gerar a injeção de comandos e execução de scripts que obtém as seguintes informações: permissão de escrita e leitura, captura de arquivos ou inserção de arquivos sem proprietário, permissão de arquivos de senhas entre outras.

6. CONCLUSÕES

A segurança da informação para os sistemas de TV Digital, principalmente as aplicações em Ginga-NCL e Lua deve ter parâmetros que assegurem que as rotinas não permitam a invasão indesejada e que protejam os dados dos usuários nas transações realizadas nas aplicações.

O Sistema de Televisão Digital deve ser tratado como os sistemas embarcados e para o desenvolvimento de aplicações seguras é preciso levar em consideração algumas ações, como:

- Planejar a segurança;
- Avaliar a vulnerabilidade de segurança do aplicativo;
- Modelar a ameaça de segurança;
- Avaliar o impacto de segurança;
- Avaliar o risco de segurança;
- Especificar as necessidades de segurança;
- Fornecer informação de segurança;
- Verificar e validar a segurança;
- Monitorar o comportamento de segurança;
- Gerenciar a segurança;
- Garantir a segurança.

As aplicações interativas que manipulam dados confidenciais dos usuários devem ter rotinas de autenticação do usuário e sem essa autenticação não pode ser permitida o acesso e nem a modificação de nenhum dado que o receptor contenha. Desta forma, a confiabilidade, a integridade e disponibilidades estarão asseguradas. A autenticidade, a responsabilidade e privacidade são asseguradas na aplicação segura quando constantemente verificada, validada e monitorada as informações do usuário.

REFERÊNCIAS

[1] PICCOLO, Lara Schibelsky Godoy; BARANAUKAS, Maria Cecília, Desafios de *Design* para a TV Digital Interativa, Universidade Estadual de Campinas, Novembro de 2006.

[2] SCHIEFLER, G. H. C.. TV Digital: A nova ferramenta governamental para a inclusão social. *Google Knol*, 29 jul. 2008.

[3] GIOIA, Francisco. Multiplexação de Sinais, Serviços de Informação (SI) e Transmissão de Dados no Padrão Brasileiro de TV Digital. Escola de Engenharia – Universidade Federal Fluminense (UFF). 2008

[4] BECKER, V.; ZUFFO, M. K.. Desenvolvimento de Interfaces para TV Digital Interativa. In: XIV Simpósio Brasileiro de Sistemas Multimídia e Web, 2008, Vila Velha-ES. Anais: Minicursos - XIV Simpósio Brasileiro de Sistemas Multimídia e Web. SBC, 2008, 2008. p. 49-97.

[5] MANHÃES, Marcus Aurélio Ribeiro; SHIEH, Pei Jen, Canal de Interatividade: Conceitos, Potencialidades e Compromissos, 23 de agosto de 2005.

[6] ZIMMERMANN, Felipi, Canal de Retorno em TV Digital: Técnicas e abordagens para efetivação da interatividade televisiva, Universidade Federal de Santa Catarina, 2007.

[7] OLIVEIRA, Carina Teixeira de, Um estudo sobre o *middleware* para Televisão Digital Interativa, Centro Federal de Educação Tecnológica do Ceará- CEFETCE, julho de 2005.

[8] PATACA, Daniel Moutinho. Tecnologias de Interação Inovadoras: Interatividade na TV Digital, CPQD, 24 de abril de 2008.

[9] MONTEZ, Carlos e PICCIONI, Carlos. Um Estudo sobre Emuladores de Aplicações para a Televisão Digital Interativa. Universidade Federal de Santa Catarina, Florianópolis. 2004.

[10] GHISI, B. C. ; LOPES, Guilhermes Figueredo; Frank Siqueira . Integração de Aplicações para TV Digital Interativa com Redes Sociais. In: Webmedia '10 (Workshop de TV Digital Interativa), 2010.

[11] SOARES, Luiz Fernando Gomes; RODRIGUES, Rogério Ferreira; MORENO, Márcio Ferreira. Ginga-NCL: *the Declarative Environment of the Brazilian Digital TV System. In: Journal of the Brazilian Computer Society*. No. 4, Vol. 13. p.37-46. ISSN: 0104-6500. Porto Alegre, RS, 2007.

[12] PAULINELLI, Fernanda ; OMAIA, D. ; BATISTA, Carlos Eduardo Coelho Freire ; SOUZA FILHO, G. L. . Xtation: um Ambiente de Testes de Aplicações para TV Digital Interativa Baseado no *Middleware* de Referência do Sistema Brasileiro de Televisão Digital. In: WebMedia 2006, 2006, Natal. Anais do WebMedia 2006 - DEMOS AND TOOLS, 2006.

[13] NUNES, Francisco José Barreto; BELCHIOR, Arnaldo Dias; ALBUQUERQUE Adriano Bessa. *Security Engineering Approach to Support Software Security. In: 6th World Congress on Services, 2010, Miami. 6th World Congress on Services*, 2010.

[14] SOUZA FILHO, Guido Lemos de; LEITE, Luiz Eduardo Cunha; BATISTA, Carlos Eduardo Coelho Freire. Ginga-J: *The Procedural Middleware for the Brazilian Digital TV System. In: Journal of the Brazilian Computer Society*. No. 4, Vol.13. p.47- 56. ISSN: 0104-6500. Porto Alegre, RS, 2007.

[15] BATISTA, Carlos Eduardo. TV Digital - Java na sala de estar. Revista Mundo Java, número 17, ano III - Editora Mundo. 2007.

[16] JUCÁ, Paulyne Matthews ; LUCENA, Ubirajara ; FERRAZ, Carlos . Desenvolvendo Aplicações da Televisão Digital. In: Congresso de Tecnologia de Rádio, Televisão e Telecomunicações, 2005, São Paulo, 2005.

[17] BRAGA, A. M. ; Restani, G.S. . *Hacking* Ginga: uma avaliação de segurança da plataforma de aplicações interativas da TV digital brasileira. In: X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, Fortaleza, 2010.

[18] OWASP Top 10 (2010). *The Ten Most Critical Web Application Security Risks*. 2010. www.owasp.org/index.php/Category:OWASP_Top_Ten_Project. Acesso em 01/03/2013.

Authorization and Disclaimer

Authors authorize LACCEI to publish the paper in the conference proceedings. Neither LACCEI nor the editors are responsible either for the content or for the implications of what is expressed in the paper.