Revista TEMÁTICA www.insite.pro.br

Identificação de Usuário em Aplicativos Interativos para a TVDi

Regiane Helena Monteiro ZOLEZI[1]
Marcos Antonio CAVENAGHI[2]
Renata S. LOBATO[3]
Roberta SPOLON[4]
Maria Lúcia AZEVEDO[5]
João Pedro ALBINO[6]

Resumo

Analisar os requisitos de segurança da informação para identificação de usuários na televisão digital interativa (TVDi). Dentre os diversos cenários emergentes das aplicações interativas, categorizamos as aplicaçoes em classificações. Para cada classificação são analisados os requisitos de segurança para a identificação do usuário.

Palavras-chave: Autenticação. Identificação. Televisão digital. Interatividade. Segurança.

Introdução

No cenário da televisão digital, com o advento da televisão digital *anywhere*, *anytime*, *anyscreen*, a informação poderá ser acessada em qualquer lugar, a qualquer hora e por qualquer pessoa em qualquer dispositivo. Não importa se o telespectador está assistindo televisão em sua casa, pelo seu televisor ou pelo seu dispositivo móvel. A segurança do conteúdo televisivo acessado ou recebido é de extrema importância neste contexto.

A autenticação do telespectador, já podendo ser chamado usuário, no cenário da televisão digital, será necessária em diversas aplicações. Alguns cenários de utilização

[1] Mestranda do Programa de Pós-Graduação em Televisão Digital da Faculdade de Arquitetura, Artes e Comunicação da Estadual Paulista "Júlio de Mesquita Filho" – UNESP, *campus* de Bauru. Analista de Sistema da Plasútil Indústria e Comércio de Plásticos Ltda. , Bauru – SP - rzolezi@hotmail.com
[2] Professor Doutor do Departamento de Ciências da Computação da Faculdade de Ciências da Universidade Estadual Paulista "Júlio de Mesquita Filho" – UNESP, *campus* de Bauru - marcos@fc.unesp.br
[3] Professora Doutora do Departamento de Ciência da Computação e Estatística do Instituto de Biociências Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", *campus* de São José do Rio Preto - renata@ibilce.unesp.br
[4] Professora Doutora do Departamento de Ciências da Computação da Faculdade de Ciências da Universidade Estadual Paulista "Júlio de Mesquita Filho" – UNESP, *campus* de Bauru - roberta@fc.unesp.br
[5] Mestranda do Programa de Pós-Graduação em Televisão Digital da Faculdade de Arquitetura, Artes e Comunicação da Estadual Paulista "Júlio de Mesquita Filho" – UNESP, *campus* de Bauru. Professora da ETEC Extensão Christino Cabral e ETEC Bauru Rodrigues de Abreu. Bauru –SP -maluazevedobru@hotmail.com
[6] Professor Doutor Departamento de Ciências da Computação da Faculdade de Ciências da Universidade Estadual Paulista "Júlio de Mesquita Filho" – UNESP, *campus* de Bauru - jpalbino@fc.unesp.br

dessas aplicações incluem adquirir novos conteúdos, compras on-line, cursos à distância, marcar uma consulta médica, solicitar o resultado do seu exame médico, acessar sua conta bancária, oferecer votação eleitoral pela televisão sem ter que sair de casa, gravar conteúdos selecionados no conversor digital. Em alguns desses cenários não é suficiente somente a autenticação do usuário sendo necessária, também, a sua identificação.

Para Huntington (2009), a autenticação é o processo de determinar se um usuário ou entidade é quem afirma ser. Ela é realizada usando algo que o usuário conhece (por exemplo, senha), algo que o usuário tem (por exemplo, o *token*[7] de segurança) ou algo que o usuário possui (por exemplo, o dado biométrico).

Conforme o NIST, a identificação é o meio pelo qual um usuário fornece uma identidade declarada para o sistema sendo que a autenticação é o meio de estabelecer a validade dessa alegação.

A presente pesquisa busca analisar os requisitos de segurança para autenticação da identidade do usuário em aplicações interativas para TVDi por meio do reconhecimento facial.

Trabalhos Correlatos

Nesta seção serão abordados trabalhos correlatos em autenticação e requisitos de segurança.

Salini e Kanmani (2011) propõem um framework aplicado a sistemas de comércio on-line que segue o modelo de processo de espiral. Esse framework é interativo e todas as fases de engenharia de requisitos são abordadas no âmbito de engenharia de requisitos de segurança. Os autores (SALINI; KANMANI, 2011) ainda expõem que se os requisitos de segurança forem levantados antes do estágio de desenvolvimento permitirá um sistema mais robusto e com maior desempenho.

Gucowski (2011) apresenta um middleware para auxiliar no desenvolvimento de softwares seguros na linguagem Java com base na norma ISSO/EIC 15408 permitindo garantir a segurança da informação para os desenvolvedores de softwares.

[7] *Token* de segurança (também conhecido como um *token* de *hardware*, *token* de autenticação ou *token* criptográfico) é um dispositivo físico dado a usuários autorizados para acessar serviços de informática que os auxiliam na autenticação. Fonte: http://en.wikipedia.org/wiki/Tokens.

Para a televisão digital, Costa et. al. (2010) e Wang et. al. (2011) elaboraram um sistema para autenticação de conteúdos no lado do Difusor de Acesso.

Costa et. al. (2010) propôs um sistema de autenticação para conteúdos específicos para o Sistema Brasileiro de Televisão Digital SBTVD, chamado AUTV, com base na assinatura digital da aplicação utilizando atributos e certificados de chaves públicas. O autor (Costa et. al., 2010) menciona os requisitos de segurança para serviços interativos para televisão digital que vão desde o oferecimento do serviço até o desenvolvimento da aplicação. Costa et. al. (2010) propõe também, um sistema para proteção de conteúdo com relação a direitos autorais.

Já Wang et. al. (2011) apresenta um método de autenticação de conteúdo com base em assinatura digital e na sintaxe ASN.1[8] (*Abstract Sintax Notation One*). A proposta desse método consiste em um protocolo de empacotamento e transmissão das informações assinadas para realizar a autenticação de conteúdo na televisão digital garantindo a validade e a integridade do conteúdo para a televisão digital.

Ainda para a televisão digital, mas focando no lado do Terminal de Acesso, podemos mencionar Wei-Bin, Hsing-Bai e Ching-Chih (2010) e o CPqD (2012).

Wei-Bin, Hsing-Bai e Ching-Chih (2010) demonstram um esquema que permite ao assinante receber o conteúdo em qualquer conversor ou *set-top-box*. A autenticação é realizada através de *smart-cards* e biometria. Essa pesquisa baseia-se no teorema de geração de chaves criptográficas a partir de uma característica biométrica.

Já o CPqD (2012) divulgou, recentemente, recomendações de segurança para aplicações interativas para TVDi. Essas recomendações são direcionadas para o receptor, para o desenvolvimento de aplicações seguras que devem atender aos requisitos de Confiabilidade, Integridade e Disponibilidade (CID) e para aplicações interativas que necessitam de transação comercial.

Transmissão da Informação na Era da Televisão Digital

O contexto da Televisão Digital gera uma mudança de paradigma. A televisão digital, além de proporcionar melhor qualidade de som, imagem e vídeo, poderá oferecer um novo tipo de mídia, o conteúdo interativo.

[8] http://www.itu.int/ITU-T/asn1/introduction/index.htm

Mediante esse cenário, o telespectador ou usuário deixa de ser apenas um usuário reativo e passa a ser um usuário pró-ativo podendo interagir com o conteúdo televisivo.

O Sistema Brasileiro de Televisão Digital Terrestre (SBTVD), conforme Alencar (2007, p. 239) menciona "É uma plataforma capaz de transmitir e receber sinais de áudio e vídeo, bem como dados utilizando para isso o sinal de radiodifusão".

O SBTVD pode ser dividido em dois blocos principais: 1) Difusão e Acesso e 2) Terminal de Acesso. O bloco de Difusão e Acesso é o bloco do lado das emissoras ou das provedoras de conteúdo enquanto que o Terminal de Acesso é o bloco do lado dos usuários.

Os receptores, chamados de conversores digitais, podem ser *full-seg* ou *one-seg*. Os dispositivos *full-seg* decodificam áudio, vídeo e dados aplicados aos conversores digitais. Já os dispositivos *one-seg* decodificam áudio, vídeo e dados aplicados aos receptores portáteis como, por exemplo, o celular e *tablet*, entre outros.

> Entre os dois blocos se encontram o Canal de Radiodifusão e o Canal de Interatividade. Por meio do Canal de Radiodifusão os sinais de áudio, vídeo e dados são transmitidos. O Canal de Interatividade é composto pelo Canal de Descida e pelo Canal de Retorno, que possibilita a integração do usuário final com a Produção de Conteúdo, permitindo-lhe receber ou enviar solicitações ou informações (ALENCAR, 2007, p. 239).

As informações na televisão digital antes de serem transmitidas são comprimidas, codificadas e empacotadas pelo bloco de Difusão de Acesso. O bloco Terminal de Acesso é responsável pelo processo inverso conforme apresentada na Figura 1.

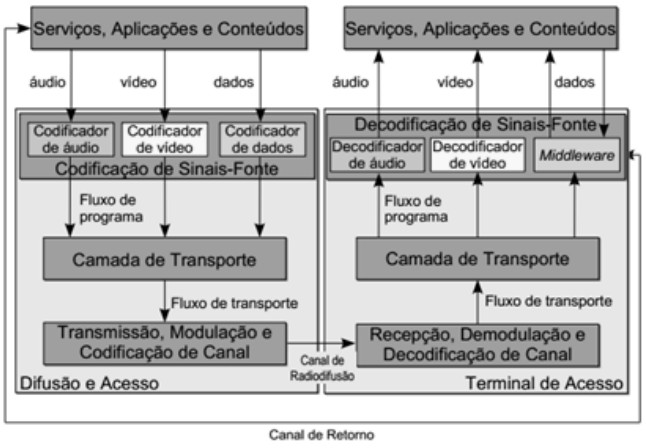

Figura 1 – Representação esquemática de sistema de televisão digital terrestre.
Fonte: Funttel, 2006.

De acordo com a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2011), em sua norma técnica NBR-15607-1, a arquitetura de rede recomendada para o SBTVD é baseada em rede no padrão TCP/IP com servidores em qualquer localidade com acesso a internet. Essa norma direciona os padrões para o canal de interatividade.

Segundo Alencar (2007), o *middleware* é o responsável em decodificar as informações e executar a aplicação, permitindo que dessa forma os aplicativos interativos sejam exibidos na televisão digital. O *middleware* é uma camada de software que intermedeia o sistema operacional residente no Terminal de Acesso e a aplicação interativa. Ginga é o nome dado ao *middleware* específico para o SBTVD.

O *middleware* é uma camada de suma importância para a execução da aplicação tornando-a independente da plataforma do conversor digital. Essa camada é importante devido à diversidade de fabricantes de conversores digitais, sendo que cada conversor tem a sua peculiaridade.

Os aplicativos interativos podem ser transmitidos das produtoras de conteúdos para os usuários, via Carrossel de Dados ou pelo Canal de Interatividade citado anteriormente. O Carrossel de Dados é conceituado conforme Alencar (2007, p.251) como "Um mecanismo de transporte que possibilita a transmissão periódica de um conjunto de dados em um sistema de radiofusão".

A distinção entre um serviço e uma aplicação para TVDi é exposta como:

> Um serviço refere-se a um canal lógico, fluxo de vídeo mais código binário – software. [...] O *software* transmitido juntamente com o conteúdo audiovisual é chamado, na TV digital, de aplicativo ou aplicação. (BECKER, 2007, p. 74, 76).

Portanto, é por meio do aplicativo interativo que o usuário poderá comunicar-se com o provedor de conteúdo ou com a aplicação comercial.

Identificação através da Biometria Facial

A Biometria (do Grego bio, "vida", e metria, "medida") é o estudo estatístico das características físicas ou comportamentais dos seres vivos[9]. Biometria é um método de reconhecer as pessoas por meio de suas características biométricas que podem ser

[9] Fonte: Wikepdia: http://pt.wikipedia.org/wiki/Biometria

físicas ou comportamentais. Dentre essas características podemos citar a impressão digital, a voz, a face, a retina e a veia.

Ashbourn (2003) define biometria como uma característica fisiológica ou comportamental que pode ser medida e, posteriormente, identificada para confirmar uma identidade individual.

Cada pessoa tem uma característica única. Os sistemas biométricos baseiam-se em duas fases: a de Registro (matrícula) e a de Reconhecimento. A Fase de Registro consiste em capturar a característica biométrica por meio de um dispositivo ou sensor. Em seguida, a tal característica é convertida num modelo ou característica de consulta (*template*) e armazenada, podendo ser em uma base de dados ou em disco.

O reconhecimento biométrico pode ser realizado de dois modos pela verificação ou pela identificação.

> Na verificação apresenta-se uma identidade e uma característica biométrica de consulta [...]. Ela tem a finalidade confirmar ou negar a identidade declarada. A identificação compara uma característica biométrica fornecida com as características biométricas armazenadas em uma base de dados [...]. (FORNAZIN, 2008, p. 9)

A verificação, também denominada de autenticação, é o processo da biometria que determina a validade da identidade. É um processo um para um (1:1), ou seja, a biometria de consulta é comparada com a característica biométrica modelo que foi previamente adquirida na Fase de Registro.

Já a identificação é o processo da biometria que reconhece uma pessoa. É um processo um para muitos (1: N), ou seja, a característica de consulta é comparada com todas as características modelos armazenadas em uma base de dados.

Várias são as características que as pessoas podem utilizar em sistemas biométricos. Podemos citar muitas técnicas de biometria como, por exemplo, a impressão digital, o reconhecimento facial, o reconhecimento da íris, o reconhecimento da retina, o reconhecimento da voz e a geometria das mãos.

Requisitos para Identificação de Usuários em Aplicações Interativas

A comunicação digital, na sociedade contemporânea, é cada vez mais indispensável tanto para as empresas como para uso pessoal. Para que essa comunicação

digital se concretize há a necessidade de transmitir a informação em rede, como já acontece hoje com a internet.

A preocupação na segurança dessas informações compartilhadas por meio da internet é um tema de extrema importância, já que a mesma é considerada um canal de comunicação inseguro por ser uma rede pública.

Com o advento da televisão digital essa preocupação não será diferente. Essa mídia emergente permitirá que os usuários interajam com os provedores de conteúdo ou com aplicações comerciais, sendo de grande preocupação a segurança do fluxo dessa informação.

Diante do exposto, a informação trafegada entre a aplicação interativa e o provedor de conteúdo ocorrerá por meio do canal de interatividade que poderá ser a internet.

Ressaltando a importância da informação segura para aplicativos para TVDi, o CPqD (2012) divulgou as ameaças para a televisão digital e as recomendações para o tratamento dessas ameaças relatadas pelo CPqD (2012) conforme apresentado no Quadro 1.

.

Ameaças	Componentes da Cadeia de Valor em TV Digital	Recomendações de Segurança da Informação
Pirataria de software e clonagem de hardware.	Fabricante, Montador, Integrador de hardware/software.	Proteção da propriedade intelectual (DRM).
Uso ilegitimo ("pirataria") do serviço.	Provedor de Serviço.	Colocar controles de acesso aos programas *login*, senha, criptografia e outros (exemplo: *Smart Card*).
Falsificação, violação ou corrupção de aplicações.	Provedor de aplicações.	Comunicação segura fim-a-fim, irretratabilidade e autenticidade.
Uso ilegítimo ("pirataria") de conteúdo.	Provedor de conteúdo.	Proteção do conteúdo e gestão dos direitos digitais (DRM).
Transação fraudulenta, perda, roubo ou violação de dados dos usuários.	Usuário final.	Proteção a privacidade, confidencialidade, integridade e disponibilidade dos dados pessoais e execução segura de software baixado e instalado.

Quadro 1 – Recomendações de segurança para os componentes da cadeia de valor em TV Digital.
Fonte: CPqD, 2012.

Deparando-se com a diversidade de aplicações para TVDi, optou-se por categorizar as aplicações de acordo com as classificações propostas por Bertini (2005)

para serviços prestados ao governo. O autor (Bertini, 2005) propõe uma classificação para aplicativos interativos conforme requerimentos técnicos:

- **informativo**: que não exige canal de retorno e exige pouco investimento;
- **interativo**: que exige canal de retorno, médio prazo e exige investimento médio;
- **transações**: que exige canal de retorno médio prazo, investimento médio e exige funções de segurança.

Os requisitos de segurança para identificação de usuários por meio do reconhecimento facial serão analisados conforme a classificação proposta por Bertini (2005). A identificação segura do usuário deve ser concretizada nas três classificações. Exemplificando as aplicações interativas de acordo com cada classificação podemos citar:

- **classificação informativa**: previsão do Tempo, EPG *(Eletronic Programming Guide*), Jogos.
- **classificação interativa:** marcar consulta médica, simulação de credito imobiliário, TV Social, Jogos.
- **classificação transação:** transação bancária, declaração de imposto de renda, conteúdo personalizado, júri virtual.

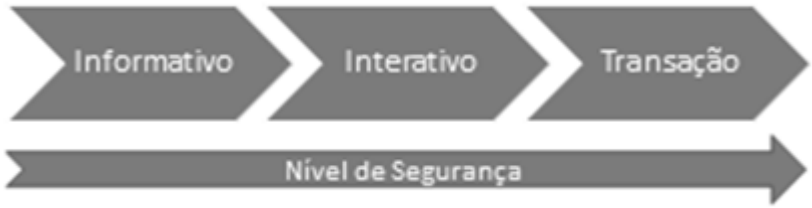

Figura 2 – Representação do nível de segurança de acordo com a classificação.
Fonte: Elaboração nossa.

Verificando-se a Figura 2, a classificação de Transação exige nível de segurança mais forte e mais robusto em relação aos outros níveis e, para esse estudo, os requisitos de segurança necessários para cada classificação serão pesquisados.

Conforme Salini e Kanmani (2011), os requisitos de segurança podem ser definidos como restrições sobre as funções do sistema. Tais restrições operacionalizam um ou mais objetivos de segurança.

A análise de requisitos de segurança será embasada na norma ISO/IEC 15408 *Evaluation Criteria for IT Security* também conhecida como *Common Criteria for Information on Technology Security Evaluation* (Critérios Comuns para Avaliação de Segurança de Tecnologia da Informação). Essa norma descreve os conceitos necessários para a segurança em sistemas de informação contendo os Requisitos Funcionais de Segurança e os Requisitos de Garantia de Segurança.

O *Common Criteria for Information on Technology Security Evaluatin* (CC) consiste em três módulos. O primeiro módulo descreve a introdução e o modelo geral. O segundo módulo especifica os componentes funcionais de segurança. O terceiro e último módulo especifica os componentes da garantia da segurança. O foco desta pesquisa concentra-se no segundo módulo onde constam as regras para os requisitos de segurança.

O CC define que o *Target of Evaluation* (TOE) é o sistema, *hardware* ou *firmware* que está sendo avaliado. Já o *Security Target* (ST) é a especificação de segurança para que o TOE possa ser considerado seguro. Os requisitos funcionais são necessários para definir o comportamento desejado do TOE.

O interesse geral do CC consiste na avaliação dos requisitos de segurança para produtos e sistemas. O CC consiste em três grupos: o TOE consumidor, o TOE desenvolvedor e o TOE avaliador.

Os consumidores podem utilizar os resultados da avaliação para ajudar na tomada de decisão se um TOE cumpre as suas necessidades de segurança. Estas necessidades de segurança são identificadas como resultado da análise de risco e direção política. Os consumidores também podem utilizar os resultados da avaliação para comparar diferentes TOE.

O CC destina-se a apoiar os desenvolvedores em dar suporte na preparação e na avaliação do TOE que está sendo implementado. Também, visa identificar se os requisitos de segurança estão sendo satisfeitos no desenvolvimento do sistema.

Já para os avaliadores, o CC contém critérios para contribuir no julgamento sobre a conformidade do TOE em relação aos requisitos de segurança. O CC descreve o conjunto de ações gerais que o avaliador deve realizar e especifica os procedimentos a serem seguidos na realização dessas ações.

O TOE que está sendo avaliado na presente pesquisa é a identificação de usuário por meio do reconhecimento facial para aplicativos interativos para a televisão digital e serão analisados requisitos de segurança para a autenticação e identificação do usuário.

O CC organiza os requisitos de segurança em hierarquia de **classes, famílias e componentes** conforme apresentado na Figura 3.

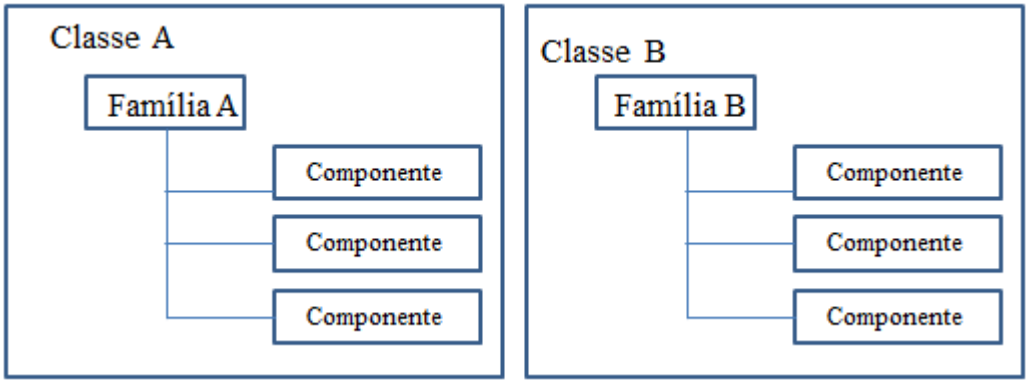

Figura 3 – Representação da estrutura hierárquica dos requisitos de segurança.
Fonte: Adaptado do CC. Elaboração nossa.

A classe é um termo utilizado para o agrupamento mais genérico dos requisitos de segurança. Todos os membros de uma classe compartilham um foco comum. Os membros de uma classe são denominados famílias.

A família é um conjunto de requisitos de segurança que compartilham objetivos de segurança, podendo ser diferente em ênfase ou rigor. Os membros da família são denominados componentes.

O componente descreve um conjunto específico de requisitos de segurança e é o menor conjunto selecionável de requisitos de segurança definido na estrutura do CC. Os componentes são definidos como elementos individuais e são considerados como o menor nível de se expressar um requisito de segurança, por isso são considerados elementos atômicos.

Conforme o CC, os componentes funcionais de segurança são a base para os requisitos de segurança funcional definida em um Perfil de Proteção (*Protection Profile* - PP) ou Alvo de Segurança (*Security Target* - ST).

A avaliação TOE está preocupada, principalmente, com a garantia de que um conjunto definido de Requisitos Funcionais de Segurança, *Security Functional Requirements* (SFR), seja aplicado sobre os recursos propostos pelo TOE.

A parte de segurança do TOE é denominada de TOE *Security Functional* (TSF) e o TSF define as funcionalidades do TOE que serão avaliadas.

A classe de família que especifica os requisitos de segurança para a autenticação e identificação do usuário no sistema é denominada *Family Identification and Authentication* (FIA). Os atributos que regem as regras para a identificação e a autenticação são: FIA_AFL (*Authentication failures*), FIA_ATD (*User attribute definition*), FIA_SOS (*Specification of secrets*), FIA_UAU (*User authentication*), FIA_UID (*User Identification*) e FIA_USB (*User subject binding).*

Uma breve descrição de cada família da classe FIA será exposta.

A família FIA_AFL (*Authentication Failure*), Falhas de Autenticação, define os requisitos para definir os valores em números para as tentativas de autenticação falhas e as ações que o TSF deve executar para essas falhas.

A família FIA_ADT (*User Attribute Definition*), Definição do Atributo do Usuário, define os requisitos para associar os atributos de segurança válidos do usuário para reforçar a tomada de decisão de segurança do TSF.

A família FIA_SOS (*Specification of Secrets*), Especificação de Segredos, define os requisitos para mecanismos que definem métricas de qualidade em relação ao segredo prestado e gerar os segredos que satisfaçam o que foi definido.

A família FIA_UAU (*User Authentication*), Identificação do Usuário, define os mecanismos de autenticação do usuário suportados pelo TSF. Essa classe também define os atributos requeridos nos quais os mecanismos de autenticação de usuário tem que se basear.

A família FIA_UID (*User Identification*), Identificação do Usuário, define as condições sob as quais os usuários devem identificar-se antes de realizar qualquer outra ação a ser mediada pelo TSF e que requer a identificação do usuário.

A pesquisa em questão visa analisar os requisitos de segurança para cada componente da família FIA sendo o TOE uma aplicação interativa para a televisão digital que permita a identificação do usuário, por meio do reconhecimento facial para cada classificação mencionada anteriormente: Informativa, Interativa e Transação.

A seguir, demonstra-se os atributos de segurança da família FIA_ATD para cada classificação.

O primeiro requisito definido para a família FIA_ATD foi exibir a **data e a hora do último acesso**. Esse requisito foi definido como prioridade alta para todas as

classificações. O usuário ao interagir com a aplicação se souber a data e a hora do último acesso gera uma maior confiabilidade na aplicação.

O segundo requisito definido foi o **tempo de duração do último acesso**, sendo que o mesmo foi definido como prioridade baixa para a Classificação Informativa, prioridade média para a Classificação Interativa e prioridade alta para a Classificação Transação. Considera-se necessário informar a duração do acesso, principalmente na Classificação Transação. Supondo-se que o sistema seja a votação pela televisão digital, o tempo de duração do acesso é de extrema importância para essa aplicação.

O terceiro requisito definido foi a **autenticação por meio do reconhecimento facial** que é o foco da presente pesquisa sendo atribuída prioridade alta para as três classificações.

O quarto requisito definido foi denominado **requisito específico da aplicação**. Este requisito foi definido como prioridade baixa para a Classificação Informativa, prioridade média para a Classificação Interativa e prioridade alta para a Classificação Transação.

Como exemplos de aplicação dos requisitos específicos citamos: para sistema médico pertencente à Classificação Interativa, o número do convênio médico; para a Classificação Transação, o protocolo de votação da última eleição; para o sistema de T-Voto, o número da agência bancária, o número da conta corrente e a posição atual do saldo para o sistema de *T-Banking*.

Ressalta-se que pelo fato desta pesquisa estar em andamento, serão ainda levantados e analisados os requisitos funcionais de segurança para toda a classe FIA.

Considerações finais

Na era da televisão digital, a autenticação e a identificação do usuário poderão ser utilizadas nos aplicativos interativos em grande escala. A biometria como forma de identificação foi exposta neste artigo e o método utilizado para a identificação de usuário no estudo presente é o reconhecimento facial.

Resgatando-se o objetivo de pesquisa em que se analisa os requisitos de segurança para identificação de usuários por meio do reconhecimento facial para cada classificação, isto é, informativa, interativa e transação, vê-se que tal análise está sendo embasada na norma ISO/IEC 15480, também conhecida como CC.

Espera-se que os resultados obtidos, a partir da referida análise de requisitos de segurança, possam contribuir para um maior nível de segurança em aplicativos para a televisão digital. Além disso, essa análise realizada previamente, aumenta a robustez e o nível de segurança do sistema, colaborando para que os sistemas propostos e desenvolvidos para a televisão digital tenham maior confiabilidade e integridade.

Além disso, outro ponto a ser destacado é que a análise de requisitos gera documentação do sistema contribuindo para que a implementação, a análise, a implantação e consumo do sistema sejam mais eficazes.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 15607-1:** televisão digital terrestre - Canal de Interatividade - parte 1: protocolos, interfaces físicas e interfaces de software. 2 ed. Rio de Janeiro, 2011.

ALENCAR, M. S. de. **Televisão digital**. São Paulo. Ed. Érica. 2007.

ASHBOURN, J. **Practical biometrics:** from aspiration to implementation. [S. l.] Springer Professional Computing, 2003.

BECKER, V.. **Convergência tecnológica e a interatividade na televisão**. Comunicação & Sociedade, São Bernardo do Campo, v. 29, n. 48, p. 63-81, set. 2007.

BERTINI, P. **Designing accessibile t-government services**. DTT**:** a technological challenge to create an info-inclusive information society. Itália, [s. n.], 2005.

COMOM CRITERIA. **Common criteria for information technology security evaluation:** ISO/IEC 15408. Disponível em: http://www.commoncriteriaportal.org/. Acesso em: 04 jun. 2012.

COSTA, L. C .P. et al. A digital television software authentication mechanism. In: International Conference on Consumer Electronics (ICCE), 2010, Las Vegas. **Digest of Technical Papers**... Las Vegas: IEEE, 2010. p. 91.

CPqD. **Recomendações em segurança da informação para TVDi:** versão 1.0. [S.n.t.], 2012.

FORNAZIN, M. **Análise de desempenho do criptossistema fuzzy vault em aplicações reais.** 2008. 90 f. Dissertação (Mestrado em Ciência da Computação) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto. Disponível em: acesso em 30 set. 2011.

GUCOWSKI, B. C. **Middleware para fornecimento de serviço de segurança em conformidade com a ISO/IEC 15.408.** 2011. 78 f. Monografia (Trabalho de Conclusão de curso em Ciência da Computação) - Universidade Regional de Blumenau, Blumenau. Disponível em: http://www.bc.furb.br/docs/MO/2011/347275_1_1.pdf. Acesso em: 12 out. 2011.

HUNTINGTON, G.. **The business of authentication:** 27 de Junho de 2009. Disponível em <http://www.authenticationworld.com/>. Acesso em: 23 maio 2012.

NIST. **An introduction to computer security:** the NIST handbook: special publication 800-12. Disponível em: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf. Acesso em: 01 fev. 2012.

SALINI, P.; KANMANI, S. **A model based security requirements engineering framework applied for online trading system**. In: IEEE - INTERNATIONAL CONFERENCE ON RECENT TRENDS IN INFORMATION TECHNOLOGY (ICRTIT), 2011, p. 1195-1202.

WANG, L. et al. A content authentication method for digital television. In: international Asia conference on Informatics in control, automation and robotics, 2., 2010. **CAR'10 Proceedings…** Piscataway: IEEE Press, 2010. v.1, p.445-447.

WEI-BIN, L.; HSING-BAI, C.; CHING-CHIH, **C. Secure communication between Set-top Box and Smart Card for Fair Use in DTV broadcasting**. IN: IEEE INTERNATIONAL CONFERENCE ON INTELLIGENCE AND SECURITY INFORMATICS (ISI), 2010, p.156-158.