Análise dos Processos de Segurança em Sistemas Móveis de 3ª Geração

Fabrício Jorge Lopes Ribeiro[1], Jaime Cesar Ribeiro Lopes[1]
Aloysio de Castro P. Pedroza[1]

[1] Grupo de Teleinformática e Automação (GTA)
Universidade Federal do Rio de Janeiro
Programa de Engenharia Elétrica – Poli-COPPE/UFRJ
Caixa Postal. 68504 – CEP 21945-970 – Rio de Janeiro – RJ - Brasil

{fabricio, jaime, aloysio}@gta.ufrj.br

Resumo. *Este artigo apresenta um estudo dos processos de segurança em Sistemas Móveis de Terceira Geração (3G), através do emprego de uma técnica de descrição formal utilizando a linguagem LOTOS. Estes protocolos são parte integrante de uma camada de serviços da arquitetura de um sistema móvel 3G, que provê mecanismos de Segurança. Os protocolos em estudo são empregados em atividades de consulta, que vão desde requisitos de confiabilidade que o sistema pode especificar até acordos de chaves de autenticação para usuários. A arquitetura utilizada para a implementação destes protocolos tem suas premissas definidas no fórum de discussão de 3G.*

Abstract. *This paper presents a study of security processes in 3rd Generation Mobile Systems using a formal description technique based on the LOTOS language. These protocols are part of a service layer of the architecture of a 3G mobile system, which provides security mechanisms. The protocols in study are used in information querying, such as reliability system provisioning capabilities and users authentication keys agreement. The architecture used in this implementation is well defined in the 3G-discussion forum.*

1. Introdução

A necessidade de confiabilidade e segurança é preocupação constante em todos os ambientes, mas, na telefonia pública, o atendimento aos seus requisitos torna-se um grande desafio. Por outro lado, com o desenvolvimento da telefonia móvel celular, que propiciou a universalização nas comunicações de voz, a comunicação móvel de dados recebeu igualmente impulso no sentido de atingir sua ubiqüidade.

Se a segunda geração (2G) trouxe a telefonia móvel para o mercado em geral, espera-se que a arquitetura de terceira geração (3G) estenda-se-á além da telefonia e abranja o fornecimento de comunicação de dados em alta velocidade e permita recursos multimídia. Essa arquitetura de terceira geração vem sendo desenvolvida pelo grupo de trabalho 3GPP (Third Generation Partnership Project).

A arquitetura de terceira geração deverá ser baseada em uma rede IP, já que este protocolo tornou-se o protocolo universal para comunicações em rede. O uso de pacotes IP na estrutura de transporte e sinalização vem se tornando naturalmente o caminho para a convergência entre as redes fixas e móveis. Esta convergência acontecerá pela

padronização de uma arquitetura totalmente baseada no protocolo IP, que incluirá o sistema celular, as redes fixas e as redes locais sem fio. Sendo assim, muitos dos requisitos de confiabilidade e segurança atualmente existentes, ou em definição, deverão também seguir os aspectos já adotados nas redes convencionais e deverão balizar o desenvolvimento dos seus análogos para redes móveis.

O desenvolvimento de um modelo padrão para protocolos de confiabilidade e segurança de terceira geração deverá basear-se, necessariamente, nos protocolos que compõe a arquitetura de segurança IP (IPSec) [Kent e Atkinson 1998] para garantir às redes sem fio a interoperabilidade aos serviços já utilizados nas redes atuais. A arquitetura necessária ao desenvolvimento de tais garantias deve ser organizada em camadas, cada uma delas provendo parte da segurança requerida. Tais camadas apresentarão um protocolo de sinalização e funções diversas de monitoramento no domínio da operadora, e cada uma delas terá seus requisitos definidos com base em padrões de confiabilidade desejados. Por outro lado, uma restrição importante é que, pelas limitações dos sistemas sem fio no que tange à vulnerabilidade dos canais, a sinalização deve apresentar alta complexidade e gerar pequeno volume de tráfego adicional.

Nesse sentido, mostraremos uma arquitetura de estudo das características e aspectos de integração deste processos de segurança. A especificação e a verificação de protocolos envolvidos nos processos de garantia de confiabilidade e segurança deve ser orientada por técnicas de descrição formal, empregando mecanismos e linguagens apropriados. As técnicas de descrição formal, por serem métodos de definição do comportamento de um sistema com o uso de uma sintaxe formal e uma semântica, permitem uma implementação de protocolos sem ambigüidades, precisa e completa. Além disso, provêem uma base bem definida para a verificação e validação desses protocolos, entendidas como a avaliação de conformidade dos mesmos com relação ao comportamento esperado [Fernandez, Garavel et al. 1996], [Bolognesi e Brinksma 1987].

O restante deste artigo está organizado nas seguintes seções: na seção 2, mostramos a importância da aplicação da técnica de descrição formal na verificação de segurança em protocolos de comunicação. Na seção 3, apresentamos os fundamentos da arquitetura de segurança de terceira geração que empregamos em nosso trabalho. A seção 4 apresenta a conclusão e temas para trabalhos futuros.

2. Comunicações Seguras dos Sistemas Móveis de 3ª Geração

Segurança, autenticação e controle de acesso são características vitais que devem ser encontradas nas comunicações em rede. Por outro lado, com a ênfase recentemente dada a novas aplicações baseadas em multimídia, levar em conta requisitos de confiabilidade tornou-se necessário à correta especificação de novos sistemas de comunicação. Estas necessidades são maiores em sistemas de comunicações móveis sem fio devido às restrições inerentes de largura de banda. Este meio geralmente é considerado não confiável, pois as mensagens estão sujeitas a perdas e interceptação durante a comunicação e restrições do meio.

Uma análise do comportamento dos protocolos que promovem as garantias de confiabilidade e segurança deve estar de acordo com os requisitos determinados pelo sistema. Um processo de verificação formal para protocolos se adequa a este esforço de

se atestar a confiabilidade e segurança de um sistema sem fio de comunicação. A especificação de um protocolo com o conceito de entidades confiáveis e não confiáveis torna-se viável devido à flexibilidade dos tipos de dados abstratos, que permitem a descrição de grande parte das operações seguras baseada no processo de modelagem do esquema clássico de segurança [Germeau e Leduc 1997].

O processo de validação e a formalização das propriedades de segurança definem uma ordem de estados que acarreta em uma comunicação segura, sendo esta ordem avaliada através das propriedades que são capazes de se expressar como eventos de segurança. No entanto, este processo pode acarretar modelos infinitos, sendo assim, necessário efetuar alguma simplificação.

O modo de transformação de método que acarreta estados infinitos em um sistema de estados finitos depende da limitação de números arbitrários das entidades envolvidas. A estrutura da especificação é composta por vários processos que interagem entre si através das portas de comunicação existentes neste protocolo. Cada entidade envolvida no protocolo é modelada pelo processo que descreve o seu exato comportamento.

Há um grande número de mecanismos de segurança, mas poucos deles são usados nos protocolos atuais. A análise dos tipos de mecanismos demonstra a confiabilidade e segurança de um protocolo [Leduc 2001]. O nível de abstração provido pelas técnicas de descrição formal e sua relativa simplicidade na definição do comportamento confiável e seguro de um protocolo são de grande valia na verificação de aspectos de segurança.

Muitas propriedades seguras podem ser verificadas [Pecheur, Zanetti et al. 1998]. Estas propriedades são estados que no protocolo podem acontecer sem prejuízo da segurança no sistema. A autenticação, o controle de acesso, a integridade e a aceitação são propriedades de segurança mas também são propriedades de confiabilidade. Cada um desses serviços de segurança necessita de um estado particular que pode acontecer ou não. A especificação formal permite, de um modo abstrato, a obtenção de todos os detalhes dos mecanismos de segurança. Assim, podemos focar somente nos serviços realmente seguros. A verificação de que todos os eventos no protocolo são seguros atesta a confiabilidade e a segurança deste protocolo.

3. Modelo UMTS para Domínios Seguros de Rede

Uma fraqueza identificada no sistema de 2a geração é a falta de segurança no núcleo da rede. Isto não foi tratado como um grande problema pois os sistemas de 2a geração eram compostas por sistemas proprietários e controladas por um número reduzido de instituições. Agora, com a introdução no backbone GPRS do IP [Rautpalo 2000], não somente usado para o tráfego de sinalização mas também para o tráfego de usuários, isto se traduz em novas ameaças e riscos para o sistema.

Os serviços seguros tem necessidade de confiabilidade, integridade, autenticação. Isto será assegurado com procedimentos padronizados e baseados em técnicas de criptografia, que possibilitam a implementação dos domínios seguros [Kent e Atkinson 1998].

Estes domínios são gerenciados por uma única autoridade que define a política de segurança que será implementada. O controle dos níveis de segurança é determinado

por esta política e implementado pelos dispositivos de borda (Security Gateways - SEGs). Os SEGs são responsáveis pela integridade e a autenticação dos dados de origem.

O domínio de rede UMTS deve ser dividido logicamente e fisicamente em domínios seguros. Este controle dos domínios seguros deve corresponder ao núcleo da rede e a sua separação deve ser realizada pelos roteadores de borda.

3.1. Roteadores de Borda Seguros

Os SEGs são entidades na borda dos domínios seguros que serão usados pelos protocolos baseados em IP [Rautpalo 2000], controlando as comunicações entre domínios diferentes (interface Za) e entre SEGs e entidades de rede internas no domínio (interface Zb).

Todo tráfego IP dos domínios seguros de rede deve passar por estes roteadores de borda antes de entrar ou sair dos domínios seguros, sendo o número destes dispositivos dependente do equilíbrio entre a necessidade de acessibilidade externa e o balanceamento de carga, para evitar um único ponto de falha. Eles são responsáveis por executar a política de segurança nas comunicações entre as redes (vide figura 1).

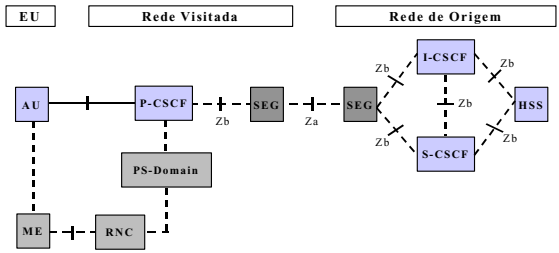

Figura 1: Arquitetura de Segurança entre Domínios Seguros

No modelo de segurança proposto para os sistemas de 3a geração, estes dispositivos de borda devem ter capacidade de oferecer armazenamento seguro das chaves de autenticação, o que pode ser assegurado com a utilização de parte dos processos existentes no protocolo IKE (Internet Key Exchange – IKE) [Harkins e Carrel 1998].

Na arquitetura UMTS, o estabelecimento das SAs (Security Associations), poderá ser realizado pelo protocolo de troca de chave da Internet [Harkins e Carrel 1998]. Este protocolo tem como objetivo principal negociar, estabelecer e manter associações seguras.

Em uma típica comunicação segura entre dois SEGs, o gerenciamento e a distribuição das chaves também poderão ser baseados no protocolo ISAKMP (Internet Security Association and Key Management Protocol) [Maughan, Schertler et al. 1998], que é fundamental para o estabelecimento das duas associações IPSec.

O protocolo ISAKMP é um protocolo de transação, definido para prestar um serviço necessário ao atendimento a requisitos de troca de chaves criptográficas. Durante esta sessão de estabelecimento, os SEGs trocam informações para

estabelecimento de associações seguras. Há dois modos de operação (principal e agressivo) para estabelecimento destas associações. As características de segurança variam com a simples mudança no modo de operação.

Em muitos trabalhos de análise de protocolos, onde a criptografia é a base da garantia de segurança, verificamos que o ponto fraco se encontra justamente durante o processo de estabelecimento e negociação das características de segurança a serem adotadas entre as partes envolvidas. É neste ponto onde procuramos a vulnerabilidade nos processos seguros.

O número e a complexidade das mensagens compostas por cada estabelecimento, influenciam diretamente na ação de intrusos durante a interceptação, modificação e retransmissão de mensagens. O grande problema que encontramos é que, quanto maior a robustez de um sistema, mais difícil se dá a sua implementação devido a sua alta complexidade. Achar este equilíbrio é cada vez mais uma necessidade, levando em consideração a rápida evolução dos sistemas como o de 3a geração.

Os resultados obtidos com a verificação do comportamento do protocolo, em relação ao modelo do serviço, sugerem que a análise do número de estados, transições e rótulos do protocolo pode ser utilizada para aferir a sua maior eficácia em estabelecer comunicações seguras. A grande diferença encontrada na expansão dos estados e rótulos é que determina o grau de vulnerabilidade dos modos em relação a interceptações das mensagens.

4. Conclusão e Trabalhos Futuros

Neste trabalho apresentamos um processo de validação e a formalização de segurança, empregada na estrutura de uma camada de serviços, pertencente à arquitetura de sistemas móveis de terceira geração (3G). A validação tem como base a verificação da complexidade e robustez dos protocolos de segurança.

A análise da quantidade dos estados e a confirmação das propriedades observacionais permitem concluir que, pela modelagem formal de um protocolo, podemos aferir as suas propriedades de segurança e, através dos estados do protocolo, verificar eventuais falhas no procedimentos executados. As equivalências devem ser definidas para garantir que o protocolo modelado apresente, em termos observacionais, o mesmo comportamento seguro que se espera do serviço modelado.

Concluímos que a vulnerabilidade a ataques em algumas fases específicas do processo tem relação com a complexidade das mensagens e as variações de estados. Isto significa que, quanto maior a complexidade, maior a dificuldade de interceptação e replicação das mensagens por um intruso.

O resultado obtido coloca a descrição formal como ferramenta de grande contribuição para a validação de confiabilidade e segurança dos protocolos. Pode-se afirmar que trabalhos neste sentido serão fundamentais para o estabelecimento desta nova filosofia de comunicação no sistema móvel de terceira geração. Ao nosso ver, estaremos contribuindo com uma metodologia de trabalho e com a validação de protocolos de confiabilidade e segurança que ainda não foram testados no sistema móvel de terceira geração e assim verificando as garantias do atendimento aos requisitos de segurança que sejam necessários.

Referências

Bolognesi, T. e Brinksma, E. (1987) “Introduction to the ISO specification language LOTOS”, Computer Networks and ISDN Systems, 14: 25–59.

Fernandez, J. C., Garavel, H., Kerbrat, A., Mateescu, R., Mounier, L. e Sighireanu, M. (1996), in: Alur, R. e Henzinger, T. (Eds.), “CAESAR/ALDEBARAN Development Package: a protocol validation and verification toolbox”, Proceedings of the Eighth Conference on Computer-Aided Verification, LNCS, Springer Verlag, Berlin.

Germeau, F. e Leduc, G. (1997) “Model-based Design and Verification of Security Protocols using LOTOS”.

Harkins, D. e Carrel, D. (1998) “The Internet Key Exchange (IKE)”, IETF RFC 2409.

Kent, S. e Atkinson, R. (1998) “Security Architecture for the Internet Protocol”, IETF RFC 2401.

Leduc, G. (2001) “Verification of two versions of the Challenge Handshake Authentication Protocol”.

Maughan, D., Schertler, M., Schneider, M. e Turner, J. (1998) “Internet Security Association and Key Management Protocol (ISAKMP)”, RFC 2408.

Pecheur, C., Zanetti, D., Koerner, E., Leduc, G., Léonard, L. e Bonaventure, O. (1998) “Model-based Design and Verification of Security Protocols using LOTOS”.

Rautpalo, J. (2000) “GPRS Security - Security Remote Connections over GPRS”.