Aspectos de Segurança da Comunicação Baseada em Papéis usando WebRTC

Victor G. Netto,
Fábio M. Costa

Universidade Federal de Goiás (UFG)

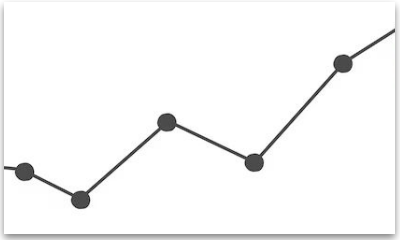
INF
INSTITUTO DE INFORMÁTICA

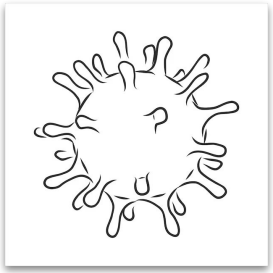
UFG
UNIVERSIDADE FEDERAL DE GOIÁS

BANCO DO BRASIL

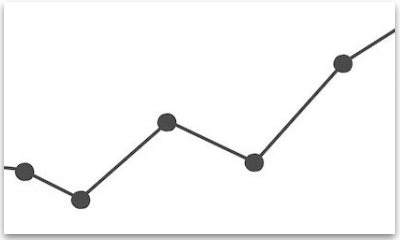
Motivação

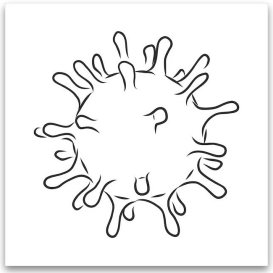
Motivação

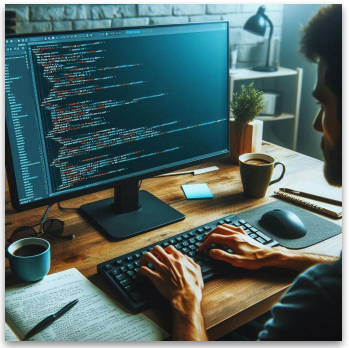




Motivação







Motivação

A Model-Driven Approach for Real-time Role-Based Communication

Marcelo B. Azevedo Vieira[1] , Sérgio T. Carvalho[1] ,
Fábio M. Costa[1] , David Bromberg[2]

[1]Instituto de Informática, Universidade Federal de Goiás
Campus Samambaia, Goiânia-GO, 74690-900 – Brazil

[2]IRISA, University of Rennes 1, Rennes, France

marcelobazevedo@gmail.com, {sergio|fmc}@inf.ufg.br, david.bromberg@irisa.fr

Abstract. *Recent years have seen the inception of many domain-specific modelling languages, enabling to overcome some of the main difficulties found in software development. The use of models has a particular impact on the implementation phase, as models tend to be closer to the problems to be solved than code. This paves the way to enable application construction by non-experts in software development, such as domain specialists. In this paper, we exploit the use of models in the domain of real-time communication, which poses significant challenges for application construction due to the multitude and intricacy of the technologies involved. We propose RBCML, a communication modelling language for the high-level specification of real-time communication sessions based on the roles that users play in the sessions. The language is processed using a combination of partial code generation and dynamic model interpretation, resulting in the construction of fully functional communication applications. The paper describes RBCML and its implementation on top of W3C's Web Real-Time Communication protocols (WebRTC). An evaluation is presented to compare the use of RBCML with code-based development and to characterize*

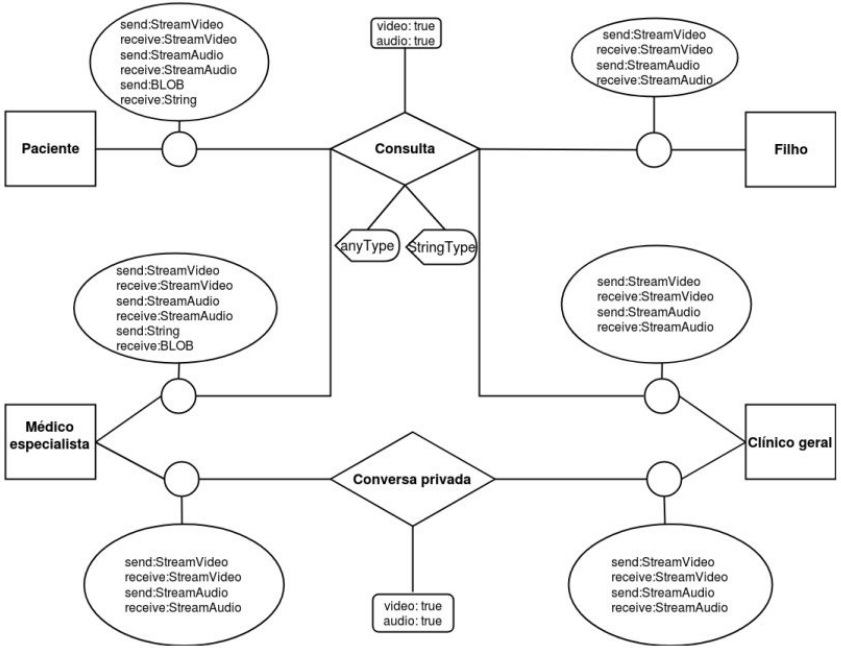


Figura 3.4: *Modelagem do cenário de consulta médica com a G-RBCML.*

SBRC 2020

Motivação

A Model-Driven Approach for Real-time Role-Based Communication

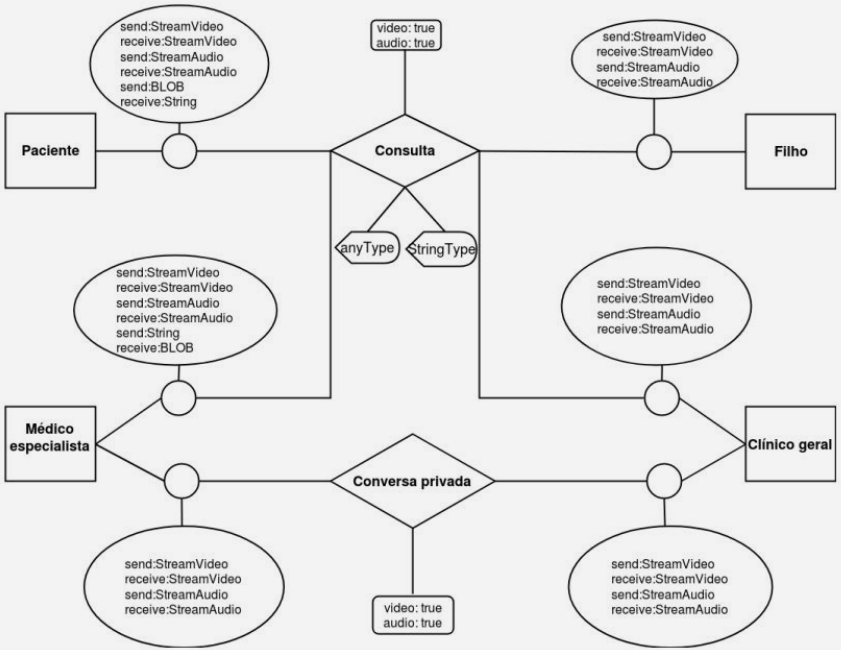
Marcelo B. Azevedo Vieira[1] , Sérgio T. Carvalho[1] ,
Fábio M. Costa[1] , David Bromberg[2]

[1]Instituto de Informática, Universidade Federal de Goiás
Campus Samambaia, Goiânia-GO, 74690-900 – Brazil

[2]IRISA, University of Rennes 1, Rennes, France

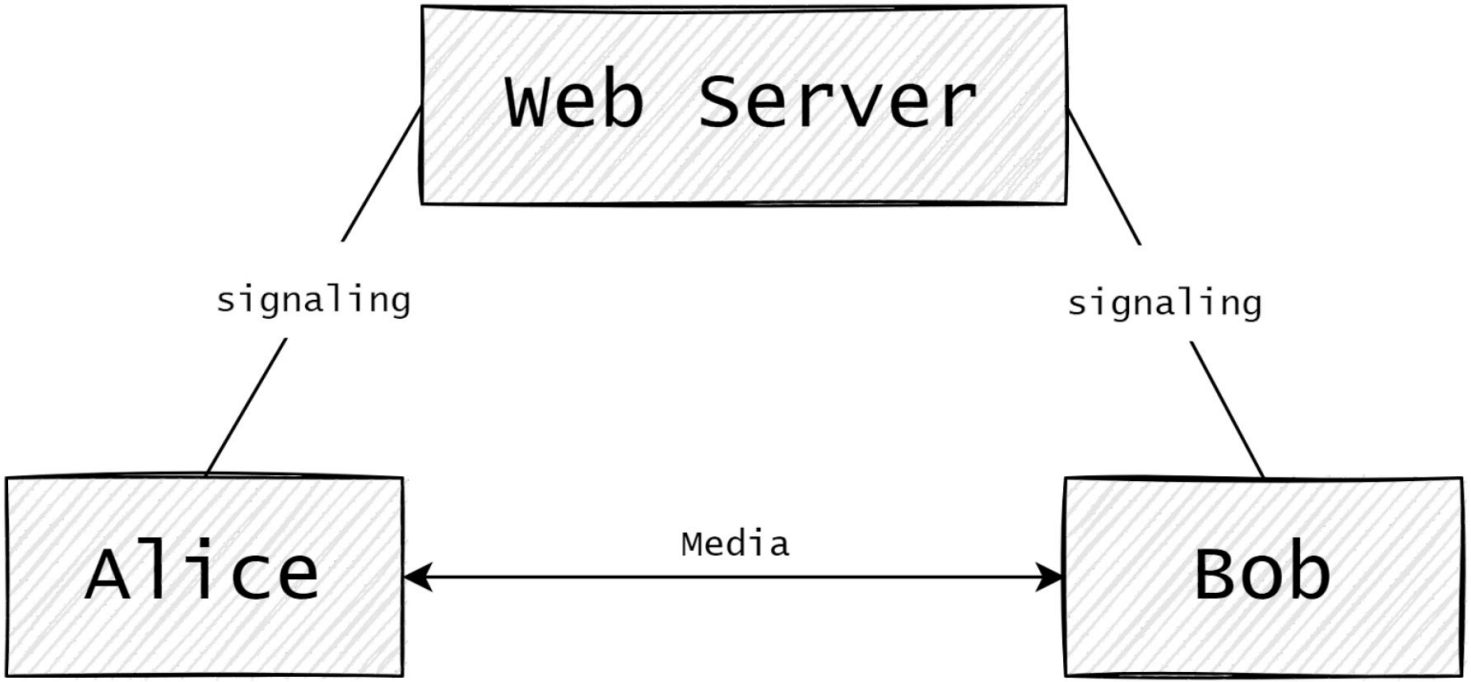
marcelobazevedo@gmail.com, {sergio|fmc}@inf.ufg.br, david.bromberg@irisa.fr

Abstract. *Recent years have seen the inception of many domain-specific modelling languages, enabling to overcome some of the main difficulties found in software development. The use of models has a particular impact on the implementation phase, as models tend to be closer to the problems to be solved than code. This paves the way to enable application construction by non-experts in software development, such as domain specialists. In this paper, we exploit the use of models in the domain of real-time communication, which poses significant challenges for application construction due to the multitude and intricacy of the technologies involved. We propose RBCML, a communication modelling language for the high-level specification of real-time communication sessions based on the roles that users play in the sessions. The language is processed using a combination of partial code generation and dynamic model interpretation, resulting in the construction of fully functional communication applications. The paper describes RBCML and its implementation on top of W3C's Web Real-Time Communication protocols (WebRTC). An evaluation is presented to compare the use of RBCML with code-based development and to characterize*

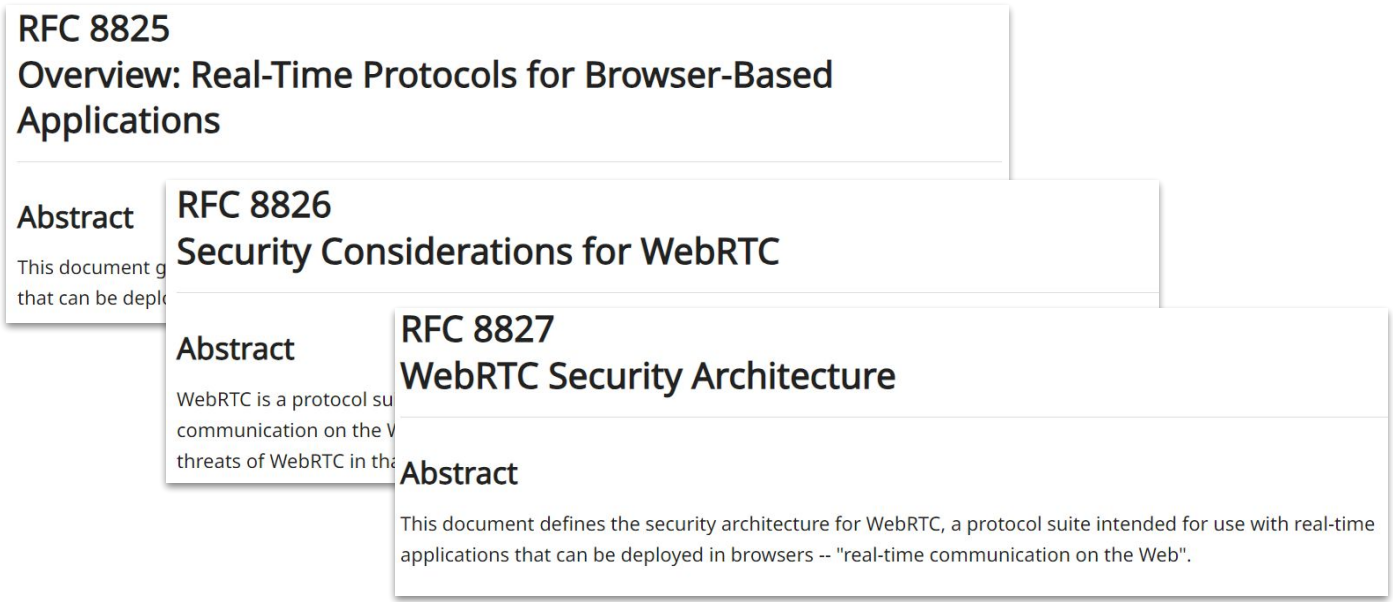


SEGURANÇA?

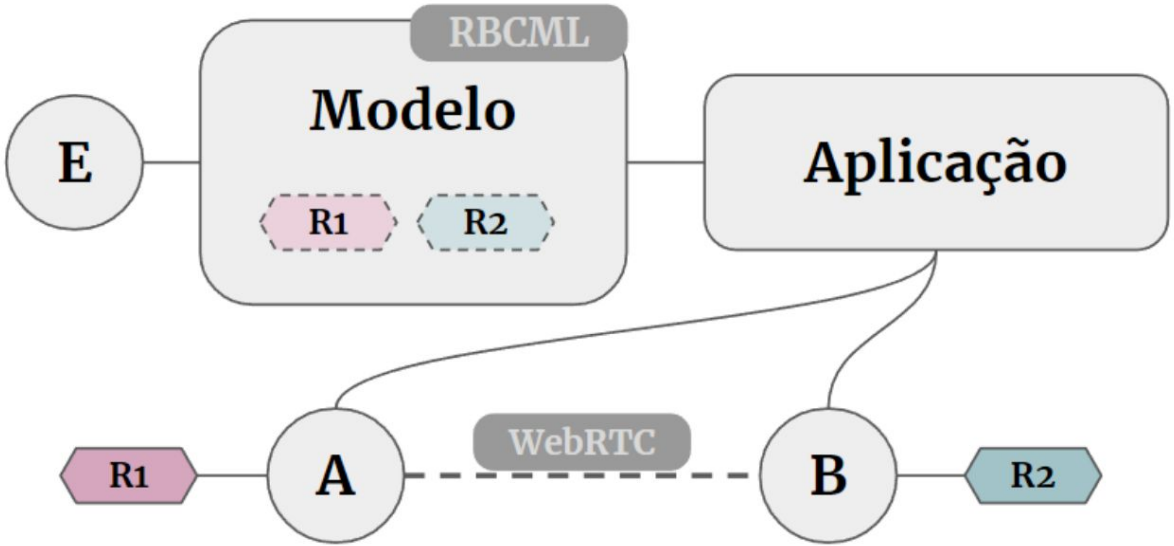
WebRTC



WebRTC

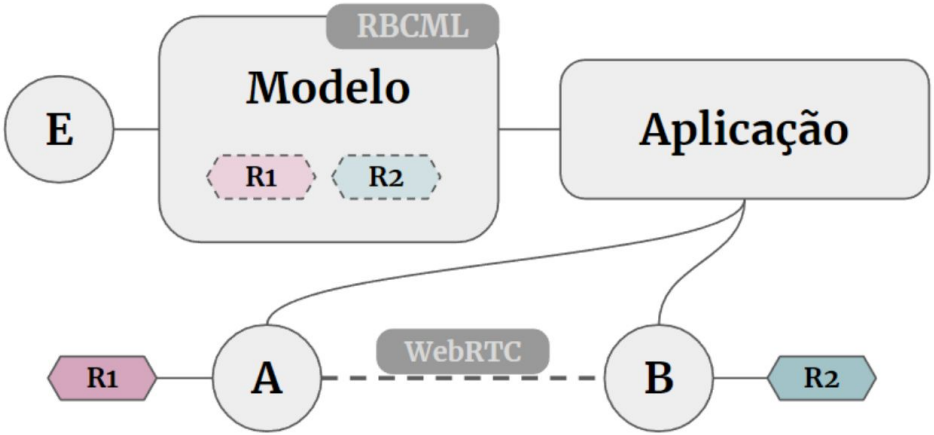

RFC 8825
Overview: Real-Time Protocols for Browser-Based Applications
Abstract
RFC 8826
Security Considerations for WebRTC
Abstract
RFC 8827
WebRTC Security Architecture
Abstract
This document defines the security architecture for WebRTC, a protocol suite intended for use with real-time applications that can be deployed in browsers -- "real-time communication on the Web".

Elementos chaves



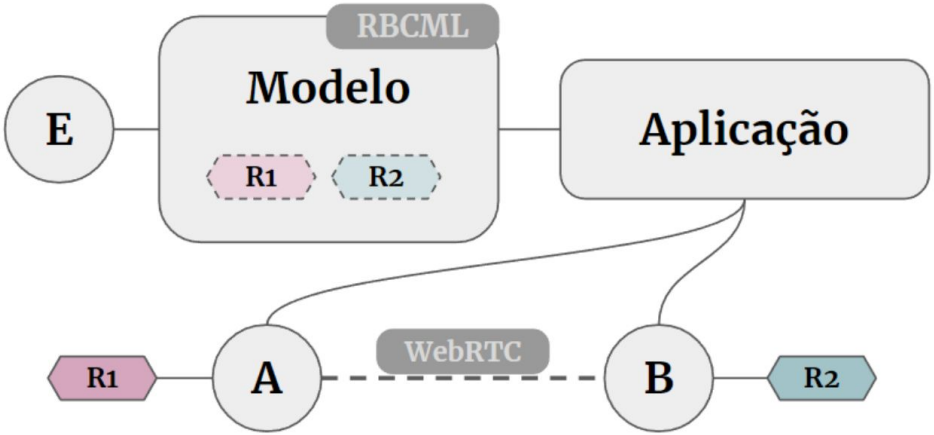
Ameaças

- Violação da Integridade



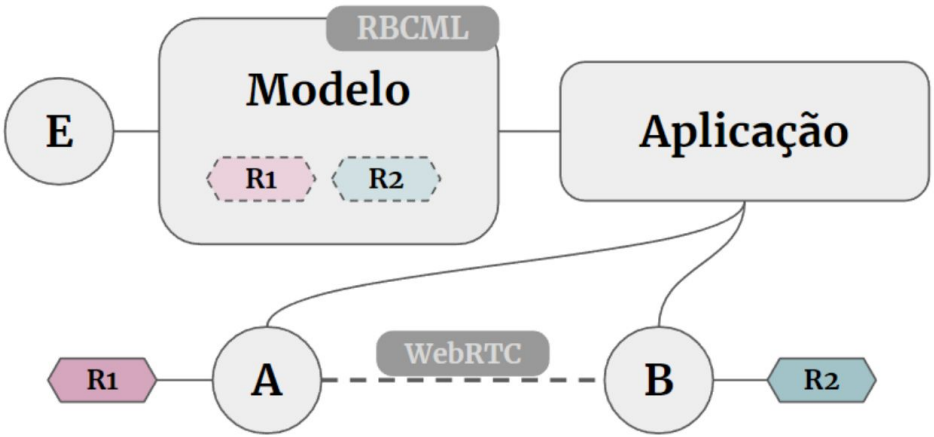
Ameaças

- Violação da Integridade
- Violação da Confidencialidade

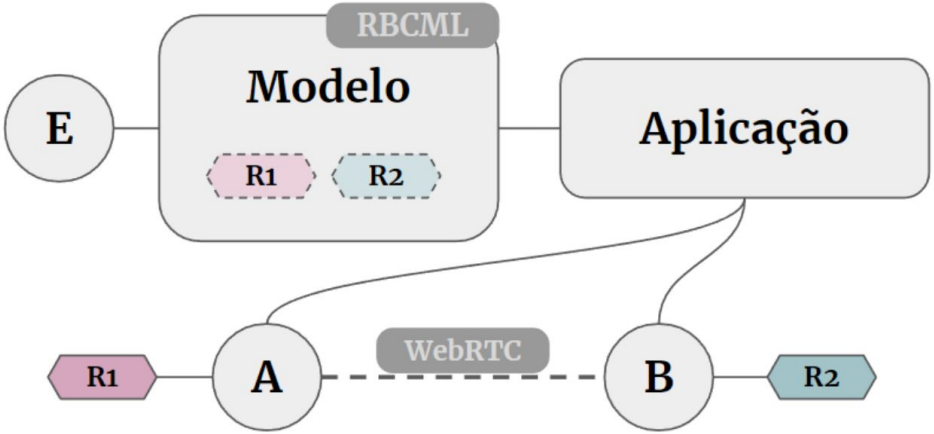


Ameaças

- Violação da Integridade
- Violação da Confidencialidade
- Violação da Autenticação



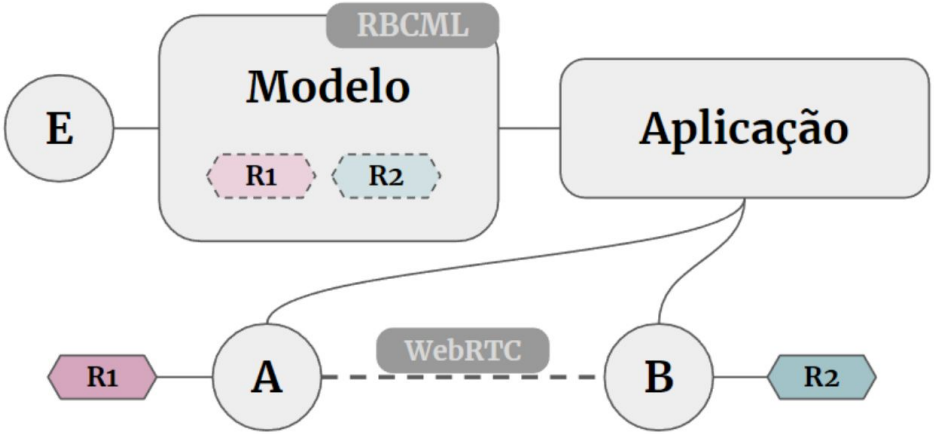
Ameaças



- Violação da Integridade
- Violação da Confidencialidade
- Violação da Autenticação
- Violação da Autorização

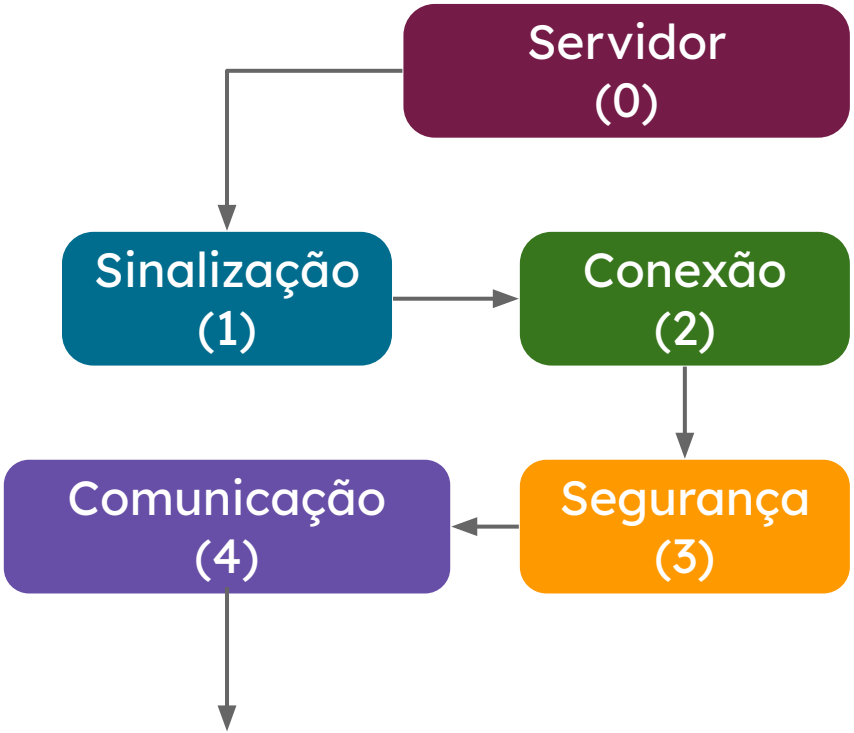
(Papéis RBCML)

Ameaças

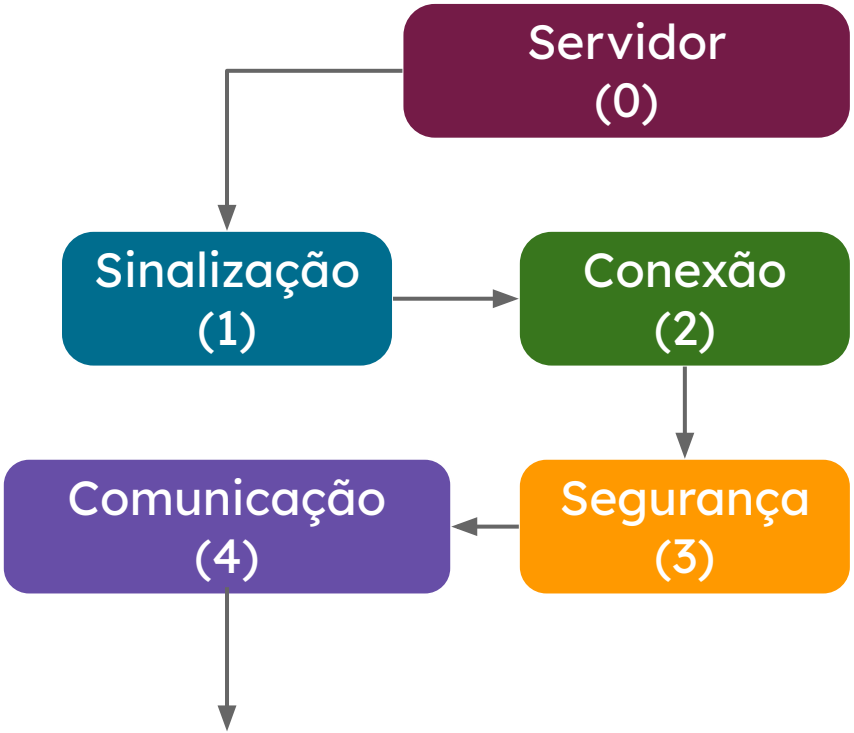


- Violação da Integridade
- Violação da Confidencialidade
- Violação da Autenticação
- Violação da Autorização (Papéis RBCML)
- Violação das restrições de fluxo de mídia impostas pelo modelo RBCML
  - SDP *Munging*
  - Fluxo de dados brutos (“*blobs*”)

Segurança herdada de WebRTC

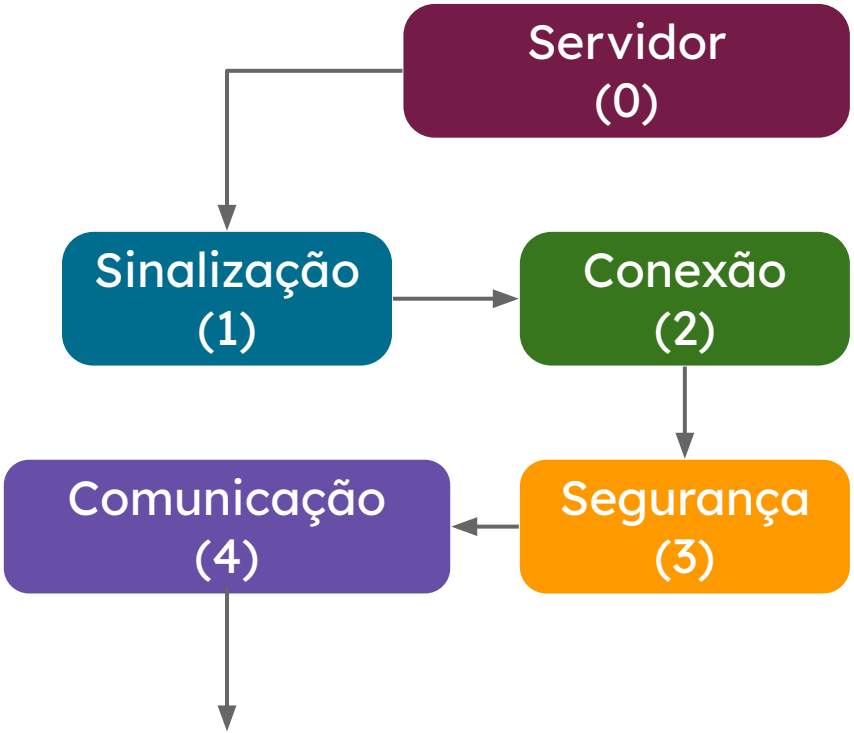


Segurança herdada de WebRTC



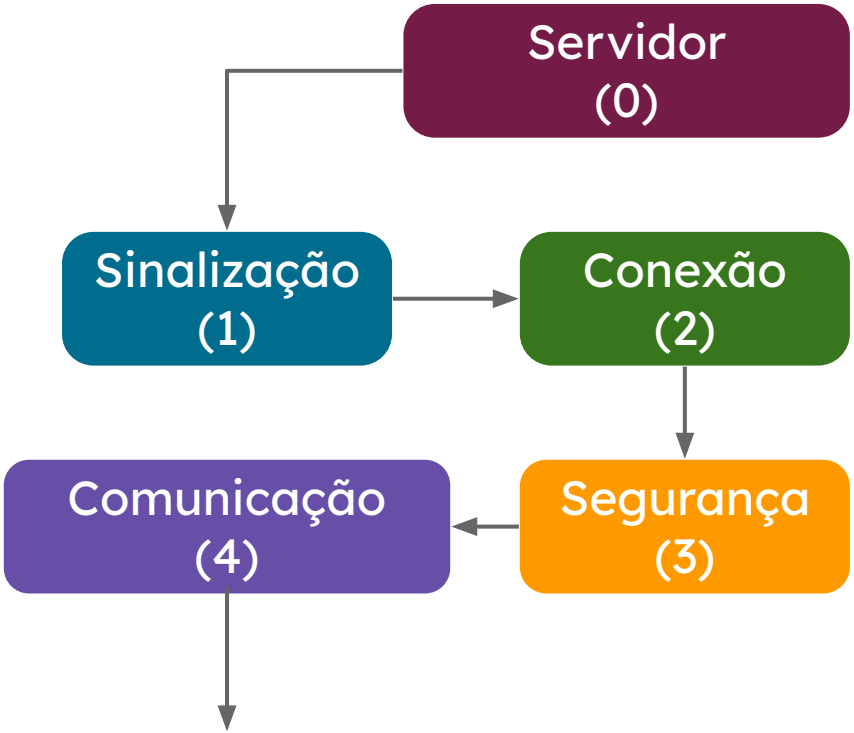
- Integridade após o **Passo 1**

Segurança herdada de WebRTC



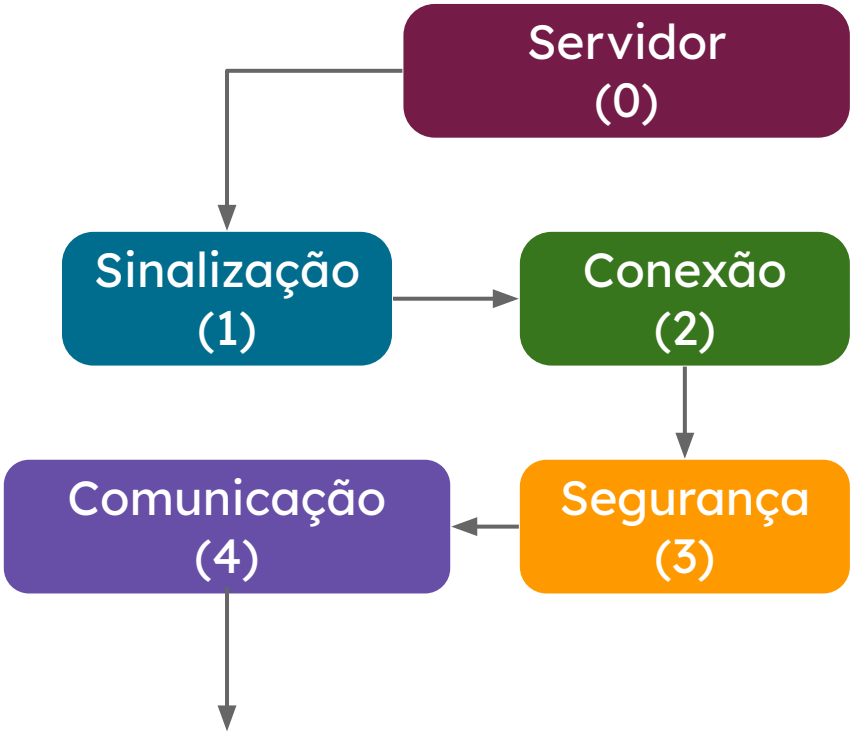
- Integridade após o **Passo 1**
- Confidencialidade após o **Passo 3**

Segurança herdada de WebRTC



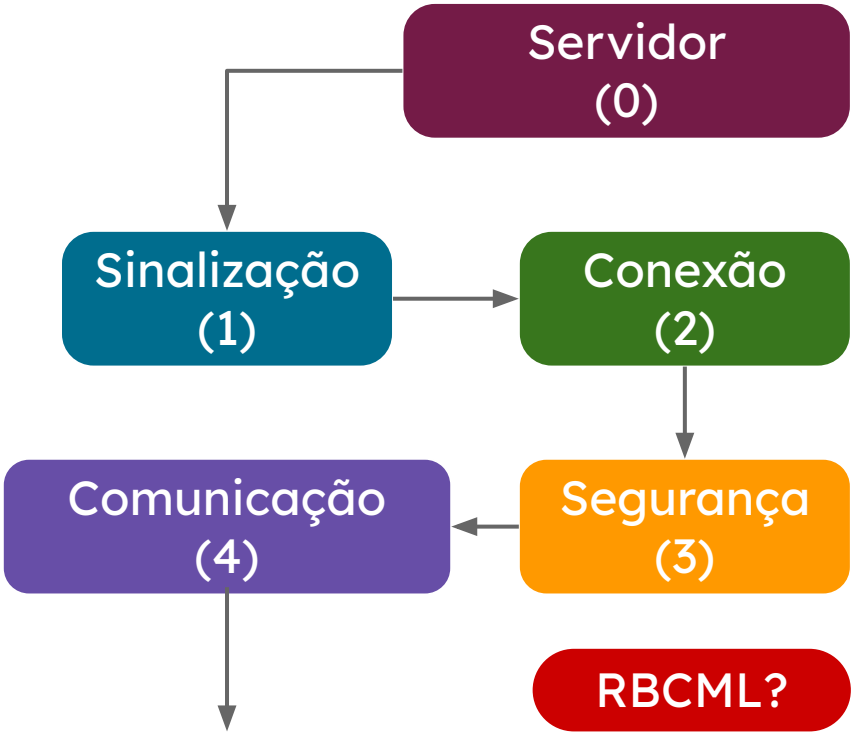
- Integridade após o **Passo 1**
- Confidencialidade após o **Passo 3**
- Autenticação e Autorização após o **Passo 0**

Segurança herdada de WebRTC



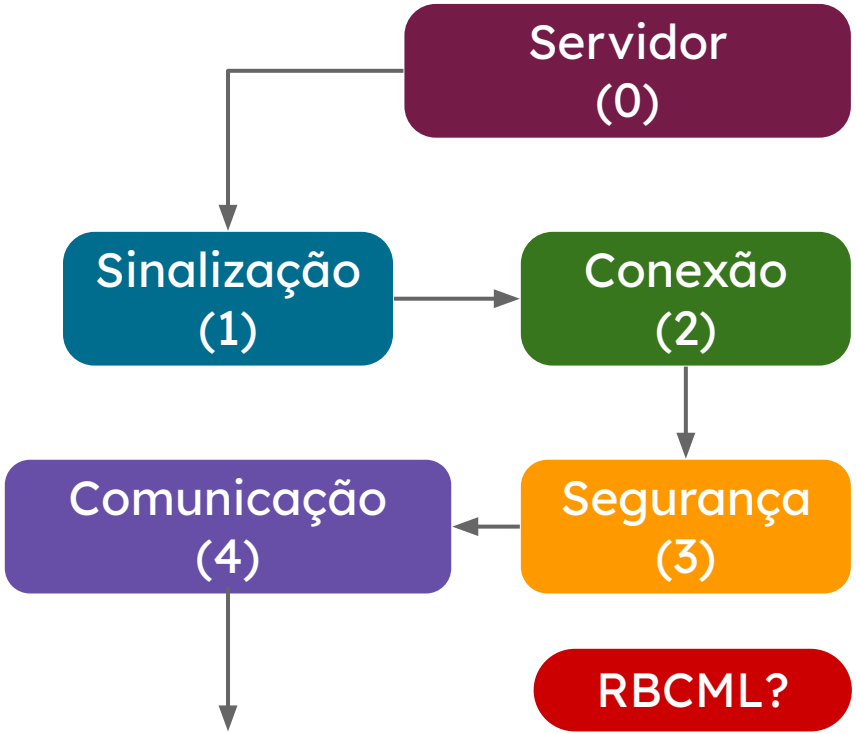
- Integridade após o **Passo 1**
- Confidencialidade após o **Passo 3**
- Autenticação e Autorização após o **Passo 0**
- DoS, Privacidade, [...] com outros medidas do WebRTC

Segurança em sessões RBCML



- Fluxo de Áudio e Vídeo
- Fluxo de dados brutos

Segurança em sessões RBCML

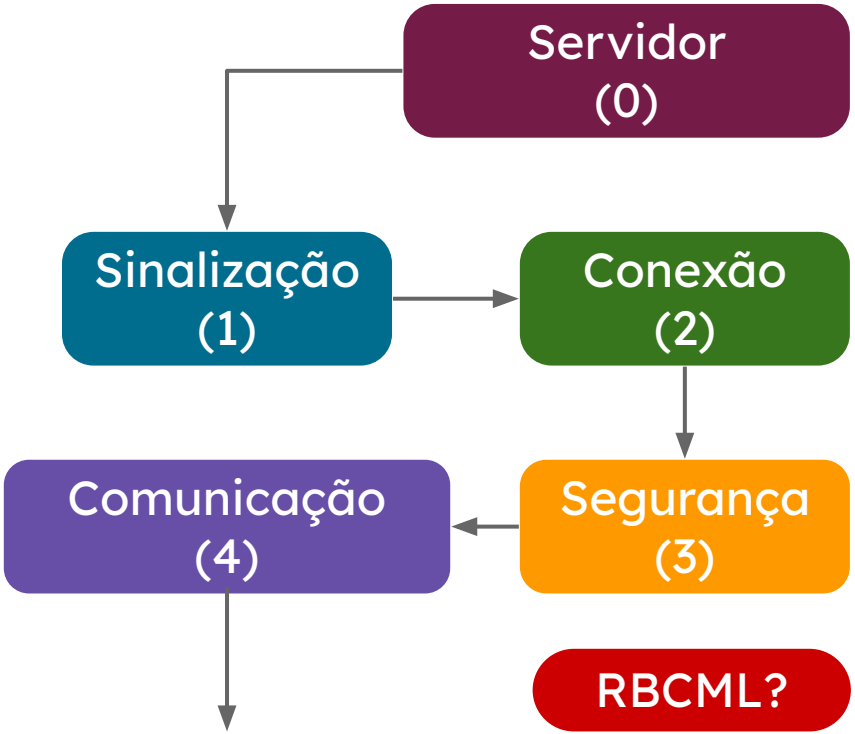


- Fluxo de Áudio e Vídeo
- Fluxo de dados brutos

If a stream is offered as sendonly, the corresponding stream MUST be marked as recvonly or inactive in the answer. If a media stream is listed as recvonly in the offer, the answer MUST be marked as sendonly or inactive in the answer. If an offered media stream is listed as sendrecv (or if there is no direction attribute at the media or session level, in which case the stream is sendrecv by default), the corresponding stream in the answer MAY be marked as sendonly, recvonly, sendrecv, or inactive. If an offered media stream is listed as inactive, it MUST be marked as inactive in the answer.

RFC 3264 (SDP)

Segurança em sessões RBCML

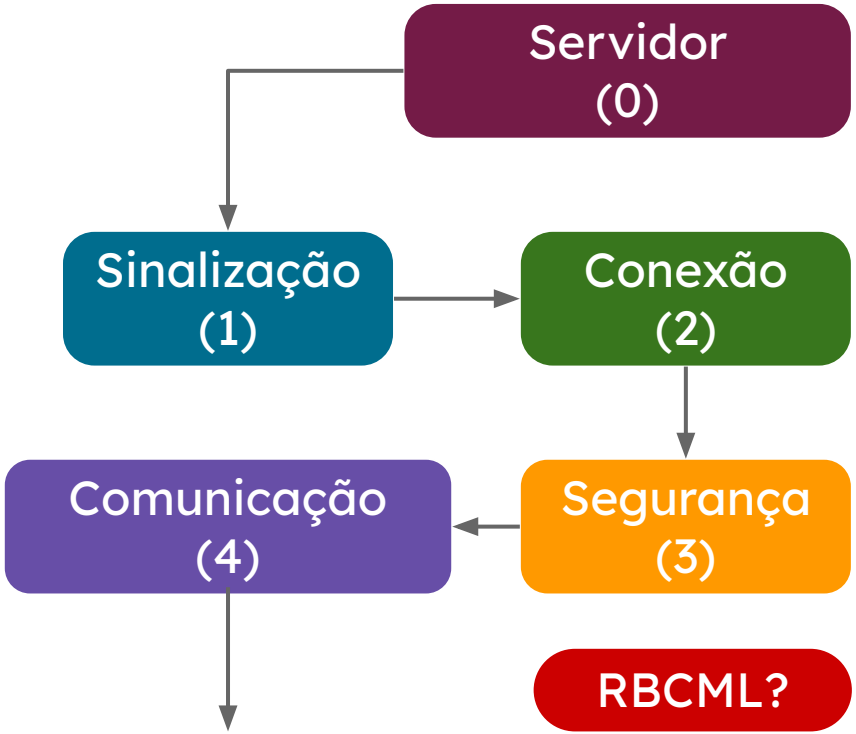


- Fluxo de Áudio e Vídeo
- Fluxo de dados brutos

> Browsers **MAY** permit the formation of data channels without any direct user approval. Because sites can always tunnel data through the server, further restrictions on the data channel do not provide any additional security. (See Section 6.3 for a related issue.)

RFC 8827 (Arq. Segurança WebRTC)

Segurança em sessões RBCML



- Fluxo de Áudio e Vídeo
- Fluxo de dados brutos
  - Assinatura de código
  - Verificação do outro par

> Browsers **MAY** permit the formation of data channels without any direct user approval. Because sites can always tunnel data through the server, further restrictions on the data channel do not provide any additional security. (See Section 6.3 for a related issue.)

RFC 8827 (Arq. Segurança WebRTC)

Próximos passos

- Experimentação dos aspectos de segurança
  - Ataques ao processo de sinalização
  - Formas de controlar o fluxo de dados crus
- Aplicação das medidas de segurança na implementação de sessões RBCML

Trabalhos futuros

- Explorar a segurança de outras aplicações que usam WebRTC
  - Jogos, *Peer-to-peer Distribution Networks* (PDNs), acesso remoto, realidade aumentada etc.
- Identificar outros cenários em que é viável usar RBCML

Referências

- Alvestrand, H. T. (2021). Overview: Real-Time Protocols for Browser-Based Applications. RFC 8825.
- De Groef, W., Subramanian, D., Johns, M., Piessens, F., and Desmet, L. (2016). Ensuring endpoint authenticity in WebRTC peer-to-peer communication. In Proceedings of the 31st Annual ACM Symposium on Applied Computing, SAC 2016. ACM.
- Feher, B., Sidi, L., Shabtai, A., and Puzis, R. (2016). The Security of WebRTC.
- Kohnfelder, L. (2021). Designing secure software. No Starch Press, San Francisco, CA.
- Rescorla, E. (2021a). Security Considerations for WebRTC. RFC 8826.
- Rescorla, E. (2021b). WebRTC Security Architecture. RFC 8827.
- Vieira, M. B. d. A., Carvalho, S. T., Costa, F. M., and Bromberg, D. (2020). A model driven approach for real-time role-based communication. In Anais XXXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2020), SBRC. Sociedade Brasileira de Computação.

INF
INSTITUTO DE INFORMÁTICA

UFG
UNIVERSIDADE FEDERAL DE GOIÁS

BANCO DO BRASIL

Obrigado!

victornetto@discente.ufg.br

fmc@ufg.br