TRABALHO DO SEMESTRE PARA A DISCIPLINA MODELOS E TÉCNICAS COMPUTACIONAIS PARA ANÁLISE DE REQUISITOS DE SEGURANÇA (SAFETY E SECURITY)

Aplicação da STPA na Análise de Vulnerabilidades de um Sistema de Autenticação e Autorização Baseado em Papéis (RBAC)

Última atualização: 19/05/2025

1. Introdução

Em sistemas de software modernos — especialmente aqueles que lidam com informações sensíveis ou funcionalidades críticas — mecanismos de autenticação e autorização desempenham um papel essencial. Esses mecanismos asseguram que apenas usuários autenticados e com permissões adequadas possam acessar recursos específicos ou executar determinadas ações no sistema. Uma abordagem amplamente adotada para implementar autenticação e autorização é o Controle de Acesso Baseado em Papéis (RBAC), no qual os usuários recebem papéis, e os direitos de acesso são concedidos com base nesses papéis.

Para ilustrar um sistema web típico de autenticação e autorização baseado em papéis, recomenda-se assistir ao seguinte vídeo no YouTube, intitulado *"Demonstração da aplicação web para o hostel Sparkling Water"*:

https://tinyurl.com/mw292ebe (5min)

Cabe ressaltar que o vídeo serve apenas como exemplo de um sistema RBAC. Assim, a análise STPA a ser concluída neste trabalho **não deve** se basear em um sistema específico, mas ser projetada para contemplar **qualquer** sistema de autenticação e autorização baseado em papéis.

2. RBAC e CIA

O **Controle de Acesso Baseado em Papéis (RBAC)** é um método amplamente adotado para gerenciar o acesso a recursos nos sistemas de informação de uma organização. Em vez de atribuir permissões diretamente a cada usuário, o RBAC associa permissões a papéis, e os usuários recebem papéis de acordo com suas funções na organização. Essa abordagem oferece diversas vantagens, como o aumento da segurança, a conformidade com políticas organizacionais e a simplificação da administração dos direitos de acesso.

Ao considerar o RBAC no contexto da tríade **CIA** — **C**onfidencialidade, **I**ntegridade e **D**isponibilidade — torna-se evidente como esse modelo contribui para os principais pilares da segurança da informação:

- **Confidencialidade**: O RBAC reforça a confidencialidade ao garantir que os usuários tenham acesso apenas às informações e recursos necessários para o desempenho de seus papéis. Ao limitar o acesso com base em funções predefinidas, reduz-se o risco de visualização indevida de dados sensíveis por usuários não autorizados. Por exemplo, em uma organização de saúde, o RBAC pode assegurar que apenas profissionais médicos tenham acesso a registros de pacientes, protegendo, assim, a confidencialidade das informações clínicas.
- **Integridade**: O RBAC desempenha um papel crucial na preservação da integridade dos dados, ao impedir que usuários realizem alterações fora de sua competência. A atribuição de permissões com base em papéis facilita a aplicação do princípio do menor privilégio, garantindo que modificações sejam feitas apenas por indivíduos autorizados e dentro de seu escopo de responsabilidade. Isso reduz a probabilidade de alterações acidentais ou maliciosas, contribuindo para a confiabilidade das informações.
- **Disponibilidade**: O RBAC também colabora com a disponibilidade ao assegurar que os recursos estejam acessíveis a usuários autorizados sempre que necessário. A definição clara de papéis e permissões previne contenção indevida de recursos e tentativas de acesso não autorizado que possam comprometer o desempenho do sistema ou interromper serviços. Além disso, o RBAC simplifica a administração de acessos, permitindo ajustes rápidos e seguros nas permissões sem comprometer a continuidade dos serviços.

Em síntese, o RBAC alinha-se diretamente aos princípios da tríade CIA, oferecendo uma abordagem estruturada e eficaz para o gerenciamento de direitos de acesso. Ao incorporar esses princípios, o RBAC contribui para a mitigação de riscos e o fortalecimento da postura de segurança das organizações.

3. Motivação do Trabalho — O Novo Passo 4 da STPA e a MicroSTAMP

Executar o Passo 4 da STPA — Identificar Cenários de Perdas — é uma tarefa reconhecidamente complexa. Embora existam diretrizes descritas no *STPA Handbook* e na obra *Engineering a Safer World*, muitos analistas de segurança ainda consideram esse passo carente de um método mais sistemático e rigoroso que os auxilie de forma mais efetiva.

Em 2024, o professor John Thomas, membro da equipe da professora Nancy Leveson no MIT, apresentou no STAMP Workshop os resultados de anos de pesquisa dedicados ao desenvolvimento de uma nova abordagem para o Passo 4 da STPA. A apresentação, intitulada *STPA: Formally Developing Loss Scenarios*, está disponível no link a seguir:

https://www.youtube.com/watch?v=hp-KBjIBmrI

Como vocês puderam observar no exercício *Level Crossing System*, elaborar uma análise STPA não é uma tarefa trivial. Nessas circunstâncias, o uso de ferramentas de apoio torna-se fundamental para facilitar o processo. Embora o foco do trabalho deste semestre **não** seja o uso de ferramentas STPA, é importante destacar que o curso de Ciência da Computação da UNIFAL-MG tem atuado ativamente no desenvolvimento de uma ferramenta *web* destinada a auxiliar analistas de segurança na aplicação da STPA.

Esse esforço resultou na criação da **MicroSTAMP**, uma ferramenta livre e de código aberto, compatível com a STPA, desenvolvida com base em uma arquitetura de microsserviços. O projeto foi apresentado no **STAMP Workshop 2024**, por meio do trabalho *MicroSTAMP: Towards a Free and Open-Source STPA-Compliant Web Tool Based on Microservices Architecture*.

A seguir, estão disponíveis alguns recursos relacionados à MicroSTAMP:

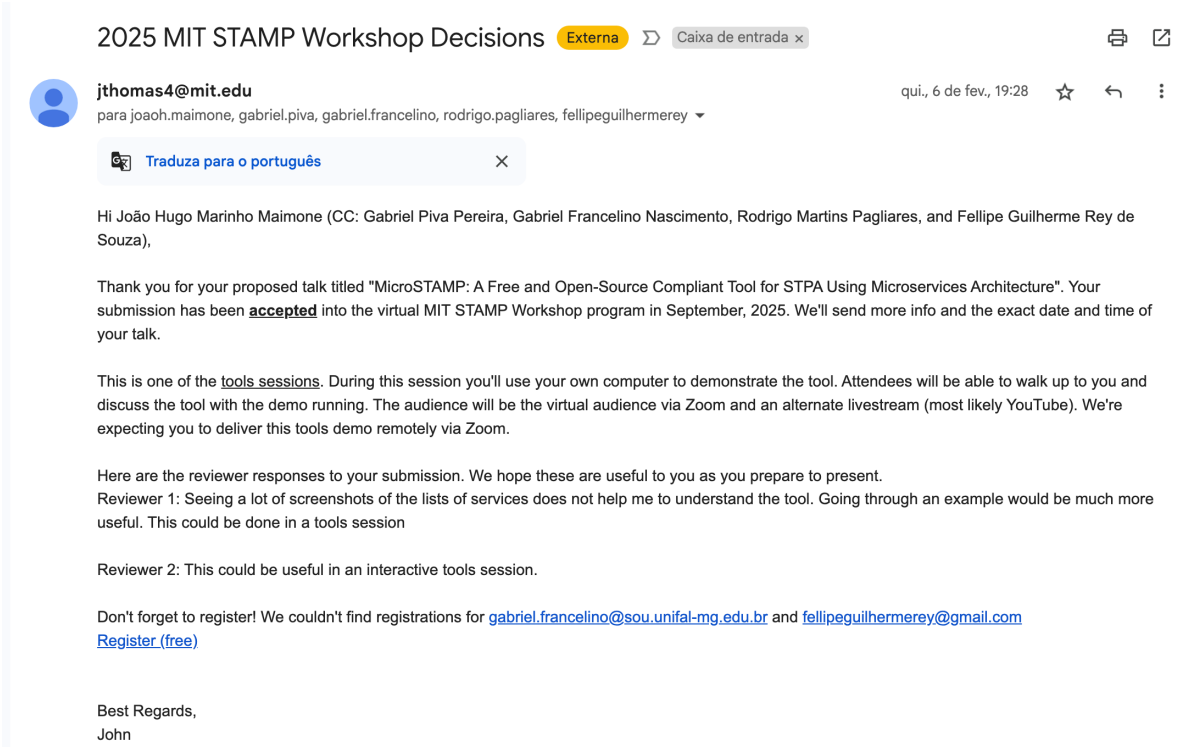
Página do evento com os slides da apresentação

Apresentação do nosso ex-aluno João Hugo (~20min)

Tutorial introdutório ao uso da MicroSTAMP (~10min)

Repositório no GitHub com o código-fonte da MicroSTAMP

Para nossa satisfação, tivemos mais uma vez um trabalho aceito para apresentação na edição de setembro de 2025 do **MIT STAMP Workshop**. Nesta ocasião, a proposta contempla um novo microserviço voltado ao suporte do **Passo 4 da STPA**, já incorporando a abordagem recentemente proposta pelo professor **John Thomas**.



2025 MIT STAMP Workshop Decisions Externa Caixa de entrada ×

jthomas4@mit.edu qui., 6 de fev., 19:28

para joaoh.maimone, gabriel.piva, gabriel.francelino, rodrigo.pagliares, fellipeguilhermerey

Traduza para o português

Hi João Hugo Marinho Maimone (CC: Gabriel Piva Pereira, Gabriel Francelino Nascimento, Rodrigo Martins Pagliares, and Fellipe Guilherme Rey de Souza),

Thank you for your proposed talk titled "MicroSTAMP: A Free and Open-Source Compliant Tool for STPA Using Microservices Architecture". Your submission has been **accepted** into the virtual MIT STAMP Workshop program in September, 2025. We'll send more info and the exact date and time of your talk.

This is one of the tools sessions. During this session you'll use your own computer to demonstrate the tool. Attendees will be able to walk up to you and discuss the tool with the demo running. The audience will be the virtual audience via Zoom and an alternate livestream (most likely YouTube). We're expecting you to deliver this tools demo remotely via Zoom.

Here are the reviewer responses to your submission. We hope these are useful to you as you prepare to present.
Reviewer 1: Seeing a lot of screenshots of the lists of services does not help me to understand the tool. Going through an example would be much more useful. This could be done in a tools session

Reviewer 2: This could be useful in an interactive tools session.

Don't forget to register! We couldn't find registrations for gabriel.francelino@sou.unifal-mg.edu.br and fellipeguilhermerey@gmail.com
Register (free)

Best Regards,
John

Figura 1. E-mail com aceite de nosso trabalho para este ano

4. Enunciado do Trabalho do Semestre – O Novo Passo 4 da STPA

Neste semestre, vocês terão a oportunidade de aprender e aplicar o novo Passo 4 da STPA em uma análise de vulnerabilidades (*security*) de um sistema de autenticação e autorização baseado em papéis (RBAC).

Para isso, será disponibilizada uma análise previamente desenvolvida com os três primeiros passos da STPA. A tarefa de vocês será estudar essa análise e completá-la com a aplicação do novo Passo 4, conforme proposto recentemente pelo professor John Thomas, do MIT.

A análise que servirá de base para o trabalho foi utilizada no TCC intitulado *"A Method Based on Behavior Driven Development (BDD) and System-Theoretic Process Analysis (STPA) for Verifying Security Requirements in Critical Software Systems"*, apresentado por mim em abril de 2024 na conferência ITNG, realizada em Las Vegas, Nevada – EUA.

A leitura do artigo não é obrigatória para a realização do trabalho, mas poderá ser útil para os(as) estudantes que desejarem se aprofundar no tema. O artigo está disponível na Seção "**Publicações**" da página principal da disciplina no Moodle. Também aproveito para compartilhar os seguintes links de interesse:

- Programação do evento
- Página do artigo na editora Springer

5. Cronograma do Trabalho e do Restante do Semestre

O trabalho de vocês será desenvolvido em partes semanais, conforme cronograma preliminar apresentado a seguir. Qualquer alteração será comunicada com antecedência.

Semana 10: 19/05/2025 – 23/05/2025 (Enunciado do trabalho + Análise STPA)

- Leitura do enunciado do trabalho (este documento).
  Esforço estimado: *1h*
- Estudo dos três primeiros passos da análise STPA de segurança, desenvolvida pelos discentes Alice Batista e Vitor Rubatino durante o TCC e utilizada como base no artigo apresentado no ITNG.
  Esforço estimado: *3h*
- Tempo reservado para estudos para a primeira avaliação.
  Esforço estimado: *4h*

Semana 11: 26/05/2025 – 30/05/2025 (Avaliação presencial + O novo passo 4 da STPA)

- **Avaliação presencial**.
  Esforço estimado: 2h
  - Data, local e horário: **Segunda-feira, 26/05/2025 – Sala UE-B-202 – das 19h00 às 20h50**
- Assistir ao vídeo do professor John Thomas sobre o novo Passo 4 da STPA.
  Esforço estimado: *6h*

Semana 12: 02/06/2025 – 06/06/2025 (Avaliação Especial + Aplicação do novo passo 4 da STPA)

- **Avaliação especial presencial** (somente para estudantes que não realizaram a avaliação da semana 11).
  - Data, local e horário: Segunda-feira, 02/06/2025 – Sala UE-B-202 – das 19h00 às 20h50
- Finalizar a análise fornecida na semana 10, incorporando os resultados da aplicação do **novo Passo 4 da STPA**.
  Esforço estimado: *8h*

Semana 13: 09/06/2025 – 13/06/2025 (O novo passo 4 da STPA produz melhor resultados? + MicroSTAMP)

- Contrastar os **resultados** obtidos com o **novo Passo 4 da STPA** com os **resultados** gerados pela **abordagem tradicional** (conforme vídeos assistidos na disciplina e o *STPA Handbook*).
    - Os resultados da abordagem tradicional serão disponibilizados nesta semana.
- Ler o artigo ao **MicroSTAMP: Microservices for Steps 1 and 2 of the System-Theoretic Process Analysis (STPA) Technique**
    - O artigo está disponível na Seção "**Publicações**" da página principal da disciplina no Moodle. Também aproveito para compartilhar os seguintes links de interesse:
        - Programação do evento
        - Página do artigo na editora Springer

Semana 14: 23/06/2025 – 27/06/2025 (Especificação de requisitos de segurança + Seminário)

- Elaborar um **documento de especificação de requisitos de segurança** com base na análise STPA do sistema RBAC.

  Esforço estimado: *4h*

- Produção e entrega de um vídeo (duração entre 30 e 60 minutos) comparando os resultados obtidos por vocês com o novo Passo 4 da STPA aos resultados fornecidos pela abordagem tradicional.

  Esforço estimado: *4h*

Semana 15: 30/06/2025 – 04/07/2025 (Encerramento da disciplina)

- Divulgação das notas finais da disciplina.
- Retrospectiva e encerramento da disciplina.

Data da Prova Final (Para quem não atingiu nota mínima 6 durante o semestre)

- Data, local e horário: Segunda-feira, **14/07/2025** – Sala UE-B-202 – das 19h00 às 20h50

6. Instruções

- Formem grupos de **3 a 7 estudantes** para a realização do trabalho.
- A atividade valerá **6 pontos na média final da disciplina**, distribuídos da seguinte forma:
    - 3 pontos: Análise com aplicação do novo Passo 4 da STPA.

- **3 pontos**: **Seminário em vídeo** apresentando e discutindo os resultados obtidos no trabalho.

6.1 Documento de Análise STPA (PDF)

- Prepare um documento PDF com sua análise STPA para com da uma das quatro etapas (você não precisa alterar os 3 primeiros passos na análise fornecida). O passo 4 deverá ser baseado no **Novo Passo 4 da STPA** e **NÃO no passo 4 tradicional** discutido nas vídeo-aulas e nos livros-texto.

6.2 Requisitos de segurança obtidos a partir da Análise STPA (PDF):

- Elabore um **documento em PDF** contendo os **requisitos de segurança** identificados na análise STPA.
- Os requisitos devem ser extraídos a partir da própria análise realizada com o novo Passo 4 da STPA.
- **Dica:** Os requisitos podem estar distribuídos pelas quatro etapas da análise. Sua tarefa é identificar na análise o que é um requisito (a ser incluído no documento PDF) e o que não é (a não ser incluído no documento PDF). Sinta-se à vontade para revisar as aulas sobre Requisitos no início do curso, em especial a aulas sobre Especificação de Requisitos (Requirements Specification)

6.3 Seminário (Vídeo)

- Grave uma apresentação em vídeo resumindo sua análise STPA.
- O vídeo deve ser entregue apenas na data de entrega da análise STPA
- O vídeo deverá focar na solução com o novo Passo 4 da STPA.
- O vídeo deve ter entre 30 e 60 minutos de duração, no máximo, e deve ser apresentado por qualquer número de membros do grupo.
- O vídeo deve ser publicado no YouTube.
- Certifique-se de que o vídeo comunique efetivamente suas descobertas e recomendações.

6.4 Entrega do trabalho

- 1 discente do grupo deverá ficar responvável por eviar o documento de análise STPA completa, incluindo o novo Passo 4 (em formato PDF) e o documento de requisitos (em formato PDF) para o endereço de e-mail pagliares@bcc.unifal-mg.edu.br
- Inclua os nomes de todos os alunos que trabalharam ativamente do trabalho.
- Para a apresentação em vídeo, envie apenas o link do vídeo do YouTube.

6.5 Critérios de Avaliação

- Este trabalho será avaliado com base nos seguintes aspectos:
  - **Minúcia e coerência da análise STPA** realizada com **o novo Passo 4**.
  - **Qualidade da apresentação em vídeo**, considerando clareza na exposição dos resultados, estrutura da apresentação e argumentação.

- **Clareza e precisão dos requisitos de segurança extraídos da análise STPA**, preferencialmente utilizando uma ou mais formas de especificação apresentadas nos vídeos sobre a **Área de Conhecimento "Requisitos de Software"**, discutidos no início do curso.

6.6 Prazos

- **Entrega até 27/06/2025**, por e-mail para: **pagliares@bcc.unifal-mg.edu.br**
- O e-mail deve conter os seguintes itens em anexo:
  - Documento em PDF com a **análise completa**, incluindo **o novo Passo 4 da STPA**.
  - Documento separado com a **especificação de requisitos** extraída da análise.
  - Link ou arquivo da **apresentação em vídeo**

Bom trabalho!