**Avanços obtidos na semana**

Mesmo com meus avanços no que se refere à aquisição de conhecimento(o que eu próprio percebo, mesmo não sendo na velocidade com que eu esperava), eu ainda estou a lentos passos na parte de apresentar meus conhecimentos. A maneira com que eu aprendo é obtendo vários conhecimentos que vão sendo organizados de maneira não linear(me ajuda em diversos tipos de provas e me faz realmente entender de várias perspectivas determinado assunto), entretanto isso não fica claro para quem escuta. Fico tendo insights no momento da apresentação e constantemente sinto uma solidificação de conceitos(algo bom), entretanto o momento é inadequado. O professor sugeriu eu construir um fluxograma para ficar graficamente explícito(para eu poder treinar para futuras exposições em eventos).

**Fluxograma da apresentação:**

-O que é o QUIC(abordagem geral)

-Quais problemas ele se propõe a resolver(Relacionar com o HTTP-3, TLS 1.3 e os problemas de aumento de dados na internet além das questões de IOT)

-HANDSHAKE(Possuo um certo domínio)

-CONTROLE DE FLUXO

=====================================================================

**Rfc acompanhadas: 9000, 9001 e 90022**

=====================================================================

**Informações novas obtidas:**

* O MSQUIC é uma biblioteca desenvolvida para o framework .NET, por isso que o mesmo é muito voltado ao SO(windows).
* A biblioteca Quiche(da google) é mais voltada para o protocolo de comunicação da internet(HTTP/3).
* O controle de fluxo é feito pelo RTT(analisado por ele). Existe uma RFC específica para esse tema, que é a rfc 9002. Eu ainda não tenho domínio suficiente para tais conceitos.
* Os assuntos relativos à criptografia(como é feita as trocas de chaves/algoritmos relevantes para o tema). Por exemplo, um tema que eu não vi muito na época em que eu estava na disciplina de segurança(por ela ser mais aplicada e pela própria proposta do curso que era preparar os alunos para o mercado através de uma base), pois o tema vai entrando em âmbitos acadêmicos e muito específico. O algoritmo em questão era o de Diff Helfman.

Tive na reunião passada com Ramon algumas explicações acerca de como funciona o protocolo TLS e o protocolo TCP. Como é feito o controle de fluxo do TCP(quando vê que não há nenhum ACK o fluxo é cortado pela metade, o processo é feito até se chegar numa média), e como é feita a criptografia TLS(a parte assimétrica inicialmente e posteriormente a parte simétrica).