This video goes over the history of security for routing protocols. It seems that security was not a factor all the way back in the 70s when these routing protocols were created/updated. This brought the talk to discuss a route leak that occurred in 2019 that deterred traffic from the original AS that Cloudfare owned to another imposter network. An AS was leaked that contained networks that were a part of Cloudfare. An attacker advertised that network under a smaller network mask and made all the incoming traffic route to that subnet instead of Cloudfare. It seems that this new AS route to a bogus network was created by a route optimizer. The same optimizer also could have caused the AS leak in the company that Cloudfare was serving. Apparently, what happened is it was a series of bugs that happened to cause an unfortunate event of leaking routes. This could have happened when that specific company sent routes to a transit provider and filtering was not up to par that day and leaked the routes. This video has showed me that route-maps and route filtering in general is VERY important. I can see it through this real world example and also in Lab 3 with sending/receiving specific traffic based on the label (transit, customer, peer).