DEFCON402 Presentation

3/11/2025

Notes, feedback, and questions posed from Ryan’s Presentation on Tuesday

Comment 1: Current Legislation on Anti-Trust & Systematic Lists

The participant mentioned that existing legislature and anti-trust laws are primarily focused on consumer-harm (monopolistic pricing, lack of competition). He mentioned the idea of creating systematic lists as opposed to just focusing on laws that are centered towards evaluating competition for the consumer and those impacts.

Notes:

By systematic lists, I understood him to mean creating lists that would classify software that could pose systemic threats. The lists would then be adopted industry-wide. It would be interesting to see how defining the risk thresholds would look. This falls into supply chain risk management that is heavily used by NIST.

Comment 2 : EU Product Liability Directive (PLD) & Software Accountability

The participant is a practicing attorney in Omaha, he mentioned the EU’s PLD that allows consumers to seek damages against software companies.

Notes:

After looking into it a bit more, The Product Liability Directive allows consumers the ability to sue software companies for the damages caused by defects. I think the EU has even expanded liability to digital services and AI. It seems like software liability has always been pretty limited (User End Agreements usually disclaim liability for failure). It’s an interesting catch because it’s completely flipping the system around in terms of how it’s always been done. It could have a waterfall effect on prioritizing security, redundancy, and resilience metrics in products before they’re ever released.

Comment 3: Amadeus Airline Data

The participant made a comment about all airline data being held in software called Amadeus, after Ryan had mentioned CrowdStrike’s oopsie and the effects on major airline companies’ servers.

Notes:

It looks like Amadeus is a global distribution system that centralizes airline, bookings, pricings, and scheduling data. I assumed that he brought this up to serve as an additional example of a single point of failure having the ability to cause industry wide effects in the event Amadeus failed or was compromised.

Comment 4: Specific Industry Focus & Resilience Layers

The participant offered a suggestion that would narrow the scope of our project to one specific area rather than generalizing across multiple industries. He mentioned examples like AWS and Azure outages that if a whole cloud region went down it could be disruptive even with failover mechanisms or multiple availability zones. He expanded more on the importance of implementing multiple layers of redundancy in single point of failure vulnerabilities. The participant then gave an example if 14 fiber lines went down in Miami, what would the impact be on the internet?

Notes:

It was a great point that he made and the question brings up a lot of different possibilities. I think the point that he was getting at is that the physical vulnerability layers in digital infrastructure can have a completely different resilience planning process than one of a cloud-based system like AWS. But, both can have catastrophic consequences on commerce, food supply, critical infrastructure, etc. He was animating just how wide the scope could be narrowed when trying to do research on a topic that has two different industries of focus.

Comment 5: Question Forcing Market Segregation vs Open Market Maximization

The participant raised the question about how to enforce market diversity when companies prioritize profit maximization in a legal way?

Notes:

I think the participant was agreeing that limiting consolidation in critical software should be done, but most markets function where companies seek market dominance to maximize profitability. Does this punish top corporations that practice free market capitalism the best?

Comment 6: Cybersecurity Challenges for Small Companies & MSPs

The participant made a comment about how small companies and MSP’s (Managed Service Providers) cannot afford large cybersecurity budgets or investments.

Notes:

I believe he was referring to the huge security gap that exists with smaller companies that rely on third-party software and cloud services. Are those types of companies assuming huge amounts of risk just because only a few, dominant cloud providers control the market? It would kill small businesses. It forces the dilemma of companies having to choose between spending funds on expensive infrastructure (killing their bottom lines) or relying on a handful of dominant cloud providers, which exposes them to systemic risks, potential vendor lock-in, and disruptions beyond their control. Smaller companies essentially must either sacrifice financial stability or accept operational vulnerabilities.

Comment 7: Outdated Software in Critical Infrastructure

The participant cited a huge security concern in the use of outdated operating systems (Windows 10, 11, and XP) in workstations in critical sectors. He stated that in the company he is employed by 941 devices still run on Windows XP. Also, referred to Southwest allegedly still running Windows 95 on their system. Shows just how many critical industries still use legacy systems and are just massive areas of vulnerability in itself.