**Faculti Summary**
https://faculti.net/security-challenges-and-opportunities-of-software-defined-networking/

This video discusses software-defined networks (SDN), which centralize network management through a controller that makes routing decisions based on flow rather than individual packets. This video provides finer granularity in flow handling and allows for customized network policies based on various constraints like security, performance, and quality of service. However, centralization also introduces vulnerabilities, such as a single point of failure where the controller could become compromised, leading to severe security risks.

Key challenges include the potential for attackers to manipulate the controller by flooding it with false information, leading to denial-of-service attacks, and the need for assurance that the applications running on the controller are secure and operate correctly. Furthermore, the interaction between multiple applications that make routing decisions can result in conflicting outcomes.

To address these issues, the text emphasizes the importance of network-based intrusion detection and the development of robust policies to govern network behavior. Methods such as behavioral modeling and invariants can be used to monitor network integrity. The flexibility of SDN can also support dynamic security measures, allowing for the rerouting of suspicious traffic for analysis rather than immediate termination.

In conclusion, while SDN offers advantages like improved visibility and control over network flows, it also presents significant security challenges that must be tackled with thorough oversight and protective measures against potential intrusions.