Aakash Saini(2018CSM1001)

March 18, 2019

- **Observations:** Paper proposes an API known as Capsicum for sand boxing the UNIX systems. Capsicum provides the security to the applications by preventing them from the execution of malicious code. Authors refined the four common programs(tcpdump, dhclient, gzip, chromium) of UNIX for the optimal utilization of Capsicum. In tradition systems when user initializes a program, some commands are executed at the same level as of user. Now attackers can use this program is this is prone to vulnerable or arbitrary code. Now Capsisum provides the security by enabling the capabilty mode in which available name space is decreased by heavily restricting the permissions. After entering into the capability mode, process can not remain for the duration of process. Any child process which is in capability mode can have only subset of the paernt process. Capability mode restricts the access to global OS namespaces and thus only delegated permissions are provided to the sandboxes. Capsicum also provides the security by preventing the user from the manipulation of extended files by preventing the files desriptors.
- **Limitations:** Capsisum does not provide any kernel-level security. The primitives defined for the capsicum are not sufficient enough for sand boxing the applications. Security concerns about the network services are not defined for the Capsicum.
- **Conclusions:** Capsisum is based on FreeBSD prototype and provides the extension to the POSIX API. It fulfills the goals of addressing the requirements of applications of sand boxing. Capsicum provide the security improvements by providing the capability mode.
- **Future work:** In future primitives for the capsicum can be improved and by using Bittau's S-thread primitives performance can be enhanced for sandbox creation. Application security mappings can be improved for OS sandboxes which in turn will improve the security of chromium. The approach of Capsicum can be extended to the kernel security.