Linux Security Summit og Linux Plumbers Conference

Morten Linderud

Linux Foundation arrangerer årlig flere konferanser rundt Linux mellom USA, Europa og Asia. Konferansene er organisert med varierende mål og størrelse, med alt fra formål om å støtte opp under den kommersielle biten av Linux, samt open-source miljøet og utviklere som jobber på Linux kernelprosjektet.

Personlig er jeg mest interessert i tematikken som omhandler hvordan vi kan gi brukere bedre sikkerhetsverktøy på Linux, samt hvordan Linux distribusjoner samarbeider på tvers med hverandre. To konferanser som er relevante for dette er “Linux Security Summit” og “Linux Plumbers”.

Linux Plumbers arrangeres annethvert år i USA og Europa, men blir samlokalisert med Open-Source Summit, Kernel Maintainer Summit og diverse andre større konferanser. Dette trekker til seg et større galleri av mennesker som jobber med, i og rundt Linux-kjernen, samt tilhørende teknologier.

Under Open-Source Summit arrangeres også en mindre konferanse som er målrettet mot sikkerhet rundt Linux, Linux Security Summit. Dette er en litt mindre konferanse med færre deltagere og består av “main track” som varer over to dager.

Kombinasjonen av disse to foredragene, og mengden folk alle arrangementene tiltrekker gjør det til en ypperlig mulighet for å sosialisere med bidragytere i open-source miljøer, lære noe nytt og finne nye problemer som må løses.

Uken i Wien startet med Linux Security Summit som inneholdt flere spennende talks. René Mayrhofer og Mario Lins tar oss igjennom xz-bakdøren fra tidligere i år. Denne bakdøren var et prosjekt over flere år hvor en ukjent person fikk nok støtte til å bli med på å vedlikeholde kompresjonsverktøyet xz. Igjennom en del tid ble ondsinnet kode tilsatt i byggesystemet som til slutt endte inn i openssh som lot en spesiell nøkkel sende kommandoer til serveren. René og Mario går igjennom hvordan dette angrepet ble til, samt flere forslag for hvordan denne type leveringskjedeangrep kan forhindres.

Andre foredrag som er verdt å nevne er Lennart Poettering sitt foredrag om ny funksjonalitet for Trusted Platform Module (TPM) i systemd prosjektet. En TPM er en form for kryptoenklaver som kan lage nøkkler og utføre kryptografiske operasjoner. Dette gjør at man kan ha et tydelig skille mellom hvordan man håndterer nøkler. Dette er praktisk for ting som diskkryptering eller mer

avanserte tjenester som plattformattestering. Systemd har i de siste årene jobbet med å tilby bedre funksjonalitet for TPMer for Linux distribusjoner som bidrar til økt sikkerhet for brukere.

Günther Noack holdt også et foredrag om landlock i Linux. Dette er relativt ny funksjonalitet som lar applikasjoner implementere sandkasser i kjøretid. Dette bidrar til økt sikkerhet for kritiske prosjekter og er lettere å implementere da andre løsninger krever eksterne prosjekter for å implementere sandkasser.

Sosialt under Linux Security Summit organiserte ikke Linux Foundation noe. Derfor ble det middag med diverse open-source utviklere som førte til spennende diskusjoner. Det var også trivelig å møte René som jeg har jobbet med litt tidligere.

De siste 3 dagene i Wien til å delta på Linux Plumbers Linux Plumbers er en konferanse for utviklere og bidragsytere “plumbingen” rundt Linux. Dette strekker seg fra API-laget i selve kernelen, til userspace verktøy, dokumentasjon og organisering rundt prosjektet.

Konferansen organiserer 30 spor med innhold som handler om flere forskjellige temaer. Blant annet Rust i kjernen, eBPF og andre subsystemer, nettverk og diskusjonsrunder kjent som “Birds of the Feather” (BOF). Det holdes flere hundre foredrag og det er vanskelig å få med seg alt. Foredragene er korte, gjerne 10-20 minutter, og mer tekniske enn konferanser flest. Dette gjør at problemer blir diskutert blant folk med samme interesse som fører til konkrete løsninger og ny kode.

“Kernel <-> Userspace/Init/System Management boundaries and APIs MC” var et spor på konferansen som varte en halv dag. Dette sporet ble organisert av utviklere bak systemd og inneholdt flere spennende foredrag. Mickaël Salaün snakket om hvordan man kan forhindre kode eksekvering på sikre systemer hvor man f.eks ikke er klar over hvor kildekoden kommer fra. Lennart Poettering førte en samtale med et bredere publikum om hvordan vi kan gjøre den initielle bootingen av Linux systemer tryggere ved å revidere initrd mekanismen.

Linux Plumbers organiserer som nevnt også flere BOFer. Dette er åpne diskusjonsforaer på en time hvor man setter seg sammen og diskuterer felles problemer eller større tematikker. Jeg deltok på en som var en diskusjon mellom kernel utviklere og distribusjoner om hvordan man skal håndtere den nye mengden sikkerhetsanmerkninger som publiseres fra Linux. Dette fører til mye ekstra arbeid og folk ønsker en lettere prosess.

Sosialt var det bedre her enn på Linux Security Summit. Det merkes at det er en større konferanse med bedre sponsorer da det ble servert all-inclusive middager to av kveldene på konferansen. Dette førte til god snakk under god mat. Jeg fikk truffet noen av utviklerne jeg har sendt patcher til rundt. Samt fikk jeg møte en person som nylig ble ny utvikler i Linux distribusjonen jeg jobber på.

Alt i alt var dette en engasjerende og trivelig tur som jeg ser frem til å gjenta!

Utvalg Foredrag

- The Critical Path to Implant Backdoors and Potential Mitigation Techniques: Learnings from XZ - René Mayrhofer & Mario Lins, Johannes Kepler University Linz
- Update on Landlock: IOCTL Support - Günther Noack, Google
- Systemd & TPMs - Lennart Poettering, Microsoft
- Linux CVEs Open Discussion - MELOTTI, Damiano
- Closing the script execution control gap - SALAÜN, Mickaël
- Revisiting How Kernels Invoke initrds - POETTERING, Lennart