

**Alexander Gausdal**

**120927**

**Obligatory exercise #1**

**2014-09-03**

**Trusted Path**

**SAK i Linux**

SAK (Secure Attention Key) ble implementert på grunnlag av det som står i "the Orange Book" (en datasikkerhetsstandard) om at det må være en måte for brukeren å initiere en login-sekvens som er fri for login-simulatorer.

Dette er en metode i Linux som aktiverer/bruker en trusted path. Dette ble implementert med versjon 2.2 av Linux kjernen. Om du trykker på et bestemt sett av knapper på tastaturet vil SAK settes igang (kjent fra Windows: ctrl+alt+del). I Linux brukes tastekombinasjonen ctrl+alt+pause, eller SysRq+K. Når denne tastekombinasjonen eksekveres sørger Linux-kjernen for at den genuine login prompten dukker opp. Det skal da være garantert at login prompten ikke kommer fra noe annet program (trojaner) som prøver å lure til seg brukernavn og passord. SAK garanterer også at inputen (brukernavn og passord) vil bli lest av det ekte login programmet, og ikke noe annet program som ligger i bakgrunnen å lytter etter input. For å realisere dette kjøres en kill kommando på alle prosesser som lytter på terminalenheten til login-programmet (program med /dev/console åpnet).

**Kilder:**

Secure attention key. URL: [http://en.wikipedia.org/wiki/Secure\\_attention\\_key](http://en.wikipedia.org/wiki/Secure_attention_key)

*Real World Linux Security: Intrusion Prevention, Detection, and Recovery.* Forfatter: Bob Toxen. URL: [http://books.google.no/books?id=bv2n6o\\_6LaQC&pg=PA330&dq=sak+linux&hl=no&sa=X&ei=xs39U7ugM4TmyQPruIHQBA&redir\\_esc=y#v=onepage&q=sak%20linux&f=false](http://books.google.no/books?id=bv2n6o_6LaQC&pg=PA330&dq=sak+linux&hl=no&sa=X&ei=xs39U7ugM4TmyQPruIHQBA&redir_esc=y#v=onepage&q=sak%20linux&f=false)

*Linux 2.4.2 Secure Attention Key (SAK) handling.* Forfatter: Andrew Morton. URL: <https://www.kernel.org/doc/Documentation/SAK.txt>