Lore: Ett verktyg för att automatisera cyberangrepp

Lore är ett verktyg utvecklat av FOI som automatiserar cyberangrepp. Lore har använts för att automatisera angrepp i cybersäkerhetsövningar sedan 2019, och nyttjar regler för att identifiera tillämpbara handlingar och tränade modeller för att prioritera dessa handlingar. Vi arbetar nu med att anpassa verktyget för andra tillämpningsområden, i synnerhet tekniska penetrationstester.

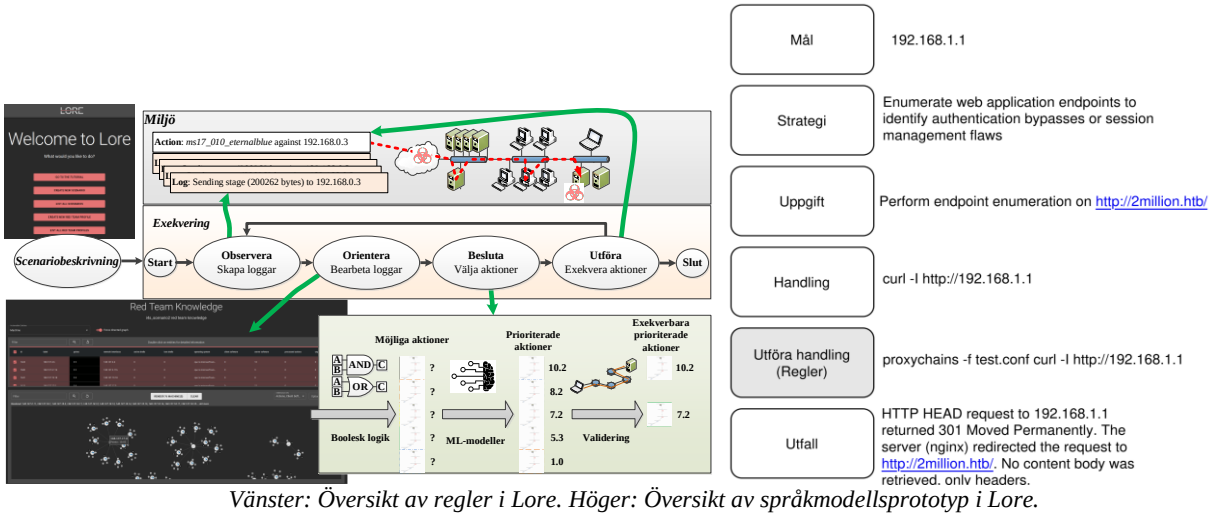
Lore skapades mellan 2018 och 2025 inom ramen för två FoT-projekt. Syftet var att öka möjligheten att bedriva övningar gällande logganalys och incidenthantering, där simulering av cyberangrepp i regel är en av de större kostnaderna för att bedriva övning.

När Lore använts för att simulera hotaktörer i övningar har den upplevda realismen varit likvärdig med när en mänsklig expert designat och genomfört angreppen. Övningarna har också upplevts som ungefär lika lärorika.

Under 2026 har arbetet inriktats mot att automatisera penetrationstester. Dessa ställer andra krav än övningar. Exempelvis är urvalet av handlingar av större vikt, då avbrott i regel inte är acceptabelt för operativa system. Det finns även ett större behov av kreativitet, såsom att granska skript unika för den testade miljön.

Framtida forskning inom projektet (2026–2028) bedöms huvudsakligen omfatta stora språkmodeller som komplement till regelstyrningen som idag nyttjas i Lore. Regelstyrning är väl lämpat för att lösa vanliga kända problem, såsom publicerade mjukvarusårbarheter och svaga lösenord. Det krävs dock tid för att skriva regler, och regler är inte väl tillämpbara för okända och ovanliga sårbarheter.

Andra forskare har visat att stora språkmodeller har förmågan att utföra cyberangrepp, och förmågan för stora språkmodeller att lösa cybersäkerhetsutmaningar har ökat mycket på kort tid. Det har dessutom utvecklats en prototyp inom projektet som trots stora begränsningar redan medför att Lore kan lösa många specialiserade utmaningar som dess regler inte omfattar.



Vänster: Översikt av regler i Lore. Höger: Översikt av språkmodellsprototyp i Lore.

Kontaktinformation
hannes.holm@foi.se

FOI Memo: FOI Memo 9275
Forskningsområde: Cyberförsvar och cybersäkerhet
Godkänd av: Pauline Ärlebäck

2026-04-17

Publika rapporter som kan laddas ner via www.foi.se:

- Holm H. (2026) Verktyg och teknik för CNO-övningar: Slutrapport, FOI-R--5817--SE
- Holm, H., Helgeson, L. (2024) Utvärdering av verktyg som emulerar hotaktörer, FOI Memo 8662
- Karlsson, J.O., Holm, H. (2024) Förstärkningsinlärning för cyberangrepp, FOI-R--5533--SE
- Holm, H. (2021) Automatisering av cybersäkerhetsövningar: Vidareutveckling och evaluering av Lores beslutsprocess. FOI-R--5148--SE.

Publika rapporter i fackgranskad litteratur:

- Holm, H., Helgeson, L. (2026) An Empirical Study of Automated Adversary Emulators, Hawaii International Conference on System Science
- Holm, H., & Sommestad, T. (2025). Realistic and balanced automated threat emulation. Computers & Security.
- Holm, H. (2022). Lore a red team emulation tool. IEEE Transactions on Dependable and Secure Computing.