MITSUBISHI ELECTRIC CORPORATION
PUBLIC RELATIONS DIVISION
7-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo, 100-8310 Japan

FÖR OMEDELBAR PUBLICERING **Nr 3649**

Det här pressmeddelandet är en översättning av den officiella engelskspråkiga versionen. Det publiceras endast som praktisk referens för användaren. Läs den ursprungliga engelska versionen för information. Vid skillnader mellan texterna är det den engelska versionen som gäller.

Kundförfrågningar

Information Technology R&D Center
Mitsubishi Electric Corporation

www.MitsubishiElectric.com/ssl/contact/company/rd/form.html

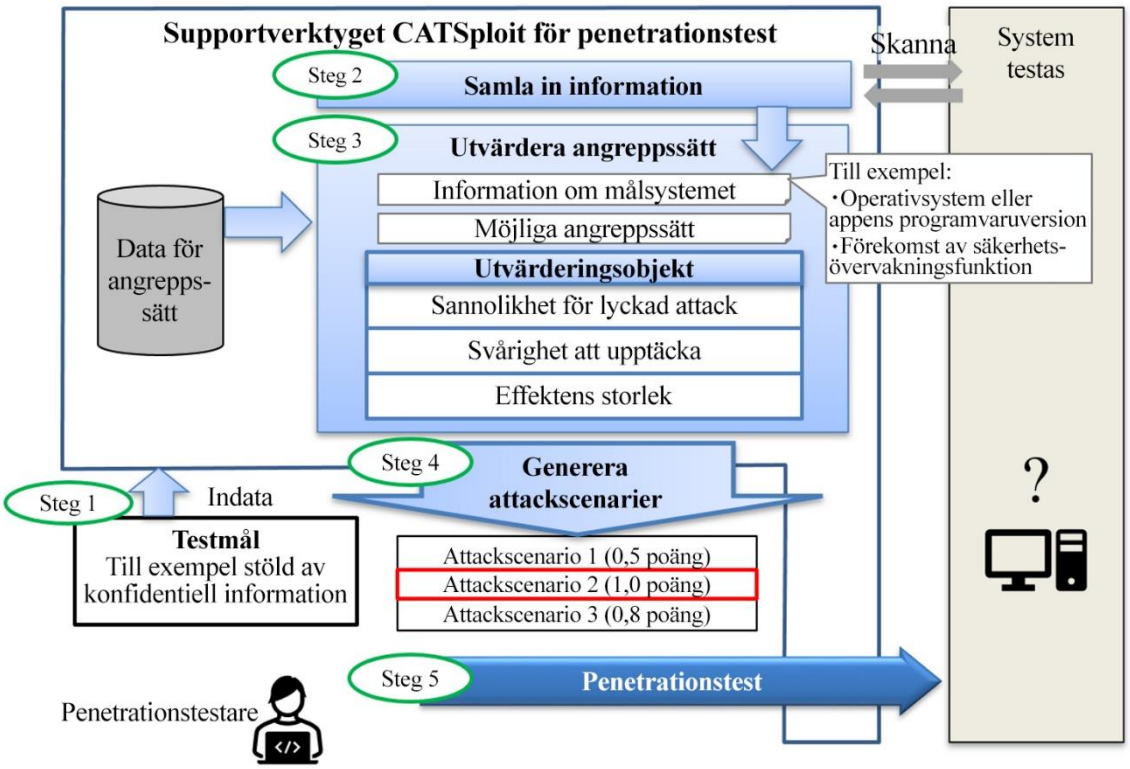
Medieförfrågningar

Public Relations Division
Mitsubishi Electric Corporation

prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

Mitsubishi Electric utvecklar världens första supportverktyg för penetrationstest som genererar attackscenarier från en hackares perspektiv

Det förväntas förbättra motståndet mot cyberattacker hos alla nätverksanslutna produkter



Exempel på användning av supportverktyget under penetrationstest

TOKYO, 5 december 2023 – Mitsubishi Electric Corporation (TOKYO: 6503) meddelade idag att företaget har utvecklat världens första[1] supportverktyg för penetrationstest[2], CATSploit, som automatiskt genererar attackscenarier baserade på en penetrationstestares testmål, t.ex. stöld av konfidentiell information, för att utvärdera hur effektiva testattacker är. Med hjälp av attackscenarierna och de efterföljande testresultaten (poäng) kan även oerfarna säkerhetstekniker enkelt utföra penetrationstester.

Under de senaste åren har styrsystem som till exempel infrastruktur och fabriksutrustning allt oftare anslutits till nätverk, vilket ökar risken för störningar, såsom strömavbrott eller nedstängning av kollektivtrafik, på grund av cyberattacker. Behovet av att implementera säkerhetsåtgärder i sådana system har blivit brådskande. Dessutom krävs det enligt standarderna ISA/IEC 62443[3] att fuzzing[4] och penetrationssäkerhetstester utförs på system och utrustning för att utvärdera deras motstånd mot cyberattacker, inklusive sårbarheter på grund av implementerings- eller konfigureringsfel. Penetrationstesterna är mycket sofistikerade och det krävs att etiska hackare[5] attackerar systemet eller produkten som testas, men sådana personer måste ha mycket hög expertis, och de är få och svåra att hitta.

Mitsubishi Electric har, genom att fokusera på de faktorer som etiska hackare tar hänsyn till när de väljer attackvektorer, utvecklat ett supportverktyg för penetrationstest som genererar listor över möjliga attackscenarier och deras effektivitet (uttryckt i siffror).

Information om verktyget presenteras 6 december (kl. 11 lokal tid) under Black Hat Europe 2023 Arsenal i London, som äger rum 6 och 7 december.

Egenskaper

1) Genererar automatiskt attackscenarier utifrån etiska hackares perspektiv

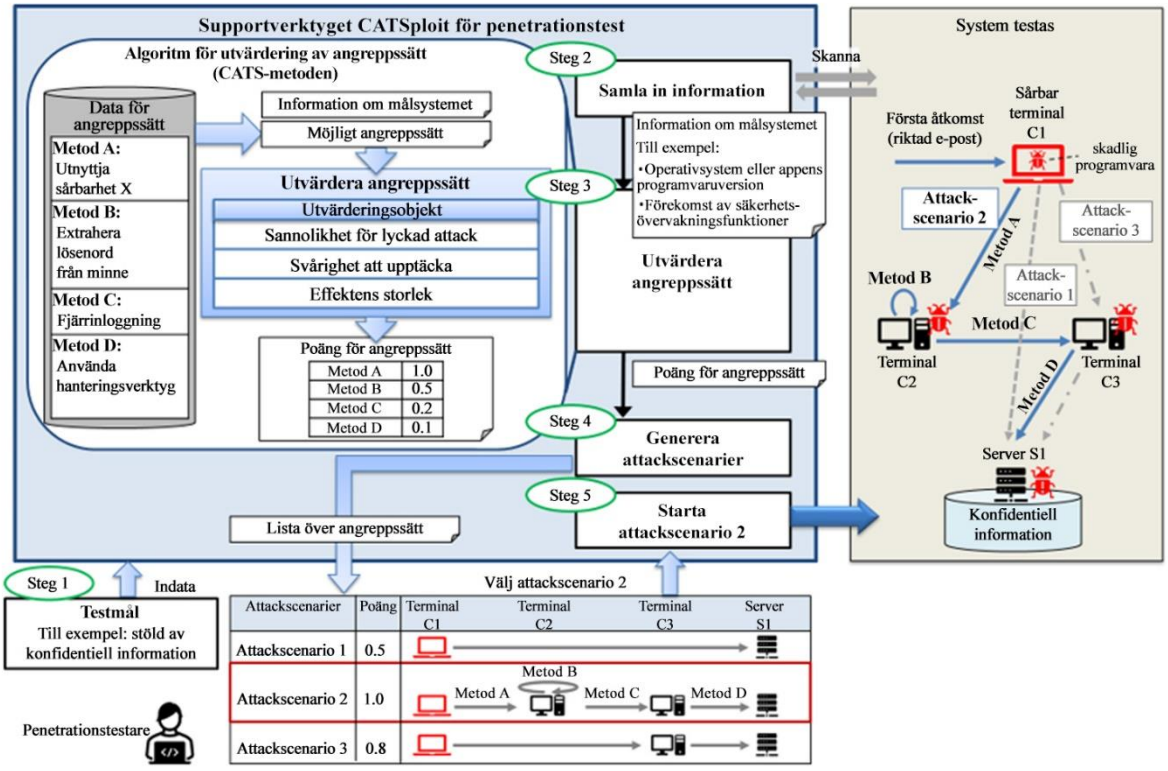
- Mitsubishi Electric fokuserade på faktorer som etiska hackare tar hänsyn till när de väljer angreppssätt, till exempel sannolikheten för en lyckad attack, svårigheten att upptäcka attacken och hur stor effekten är. Genom att justera för målen för specifika tester kan systemet automatiskt generera scenarier som visar de steg som krävs för att genomföra en attack för att uppnå dessa mål.

2) Optimala tester utvärderar hur effektiva attackscenarierna är ur en etisk hackares perspektiv

- Mitsubishi Electrics egenutvecklade metod CATS[6] beräknar hur effektivt varje angreppssätt är (uttryckt med en siffra) utifrån en etisk hackares perspektiv, och baserat på det föreslås en lista med attackscenarier så att det mest effektiva scenariot (högsta poäng) kan väljas.
- CATS-utvärderingen tar inte bara hänsyn till känd systeminformation, som operativsystem, appversion och säkerhetsövervakningsenheter, utan även saknad systeminformation, som hjälper till att förverkliga attackscenarier som noggrant replikerar en faktisk angripares perspektiv.
- Den automatiska utvärderingen av attackscenarier som sannolikt kommer att användas av etiska hackare gör det enkelt för mindre erfarna säkerhetstekniker att utföra penetrationstester.

---

[1] Enligt studier från Mitsubishi Electric från den 5 december 2023
[2] Testa för att bekräfta att om ett system eller en utrustning kan skadas av en faktisk attack
[3] Säkerhetsstandarder för industriella styrsystem
[4] En testmetod för upptäckt av programvarufel eller sårbarheter genom att ange ogiltiga eller felaktiga data
[5] Etiska hackare som använder avancerad kunskap och datorteknik för att identifiera säkerhetsproblem, osv.
[6] Poäng på cyberattacktekniker: Mitsubishi Electrics egenutvecklade metod för att utvärdera effektiviteten hos attackvektorer



Supportverktyget CATSploit för penetrationstest

Framtida utveckling

För att ytterligare förbättra motståndet mot cyberattacker hos system och enheter som utvecklats av Mitsubishi Electric kommer företaget att fortsätta att undersöka och utveckla det nya verktyget med målet att använda det för faktiska säkerhetstester av företagets produkter senast 2026.

###

Om Mitsubishi Electric Corporation

Mitsubishi Electric Corporation (TOKYO: 6503) har mer än 100 års erfarenhet av att tillhandahålla tillförlitliga och högkvalitativa produkter och är en erkänd global ledare inom tillverkning, marknadsföring och försäljning av elektrisk och elektronisk utrustning som används i behandling av information och kommunikation, rymdteknik och satellitkommunikation, konsumentelektronik, industriteknik, energi-, transport- och byggutrustning. Mitsubishi Electric berikar samhället med teknik i enlighet med företagets motto, ”Changes for the Better”. Företaget noterade en omsättning på 5 003,6 miljarder yen (37,3 miljarder* dollar) under räkenskapsåret som avslutades den 31 mars 2023. Mer information finns på www.MitsubishiElectric.com

*Amerikanska dollarbelopp har omvandlats från yen med kursen ¥134=1 USD, den ungefärliga kursen på Tokyobörsen den 31 mars 2023.