Myndigheten för samhällsskydd och beredskap

FORSKNING

RIOT: Hur vi gör sakernas internet säkrare

RIOT: Hur vi gör sakernas internet säkrare

Tidsperiod: 2019–2024
Utförare: Chalmers Tekniska Högskola och Uppsala universitet
Ansvarig: forskare/författare Magnus Almgren, Christian Rohner

Kort sammanfattning: Denna rapport sammanfattar forskningsprojektet RIOT, där forskare och doktorander har undersökt hur vi kan göra uppkopplade enheter, som används i allt från hem till industrier, säkrare och mer robusta. Här beskrivs de utmaningar vi mötte och de resultat som kan bidra till att göra framtidens teknik tryggare.

MSB:s Kontaktpersoner: Erik Sundström, 010-240 5371

Text: professorerna Magnus Almgren, Chalmers,
och Christian Rohner, Uppsala universitet
Produktion: Advant

Publikationsnummer: MSB2526 – december 2024

MSB har beställt och finansierat genomförandet av denna forskningsrapport.
Författarna är ensamma ansvariga för rapportens innehåll.

Förord

Arbetet med projektet RIOT har varit en givande resa. Projektet har låtit oss fördjupa oss i ett område med stor samhällsrelevans – säkerheten hos uppkopplade enheter, något som ofta diskuteras i nyheter och påverkar allt från hem till samhällsviktig infrastruktur. Under projektets gång har vi haft förmånen att se doktorander utvecklas från studenter till självständiga forskare, en process som varit både inspirerande och lärorik.

Vi vill tacka MSB för stödet och medlemmarna i referensgruppen för era värdefulla frågor och perspektiv. Tack också till alla studenter som bidragit genom att undersöka olika aspekter av våra frågeställningar. Slutligen ett tack till våra familjer – ert stöd har varit ovärderligt under en period då arbetet ibland tagit över vardagen.

Göteborg, 2024-11-22

Magnus Almgren, Christian Rohner

Innehåll

INTRODUKTION 5

FÖRBÄTTRAD AUTENTISERING 6
Bakgrund 6
Utmaningar 6
Insikter från vår forskning 6

SKYDDA DATA ÄVEN OM EN ENHET KOMPROMETTERAS 7
Bakgrund 7
Utmaningar 7
Insikter från vår forskning 7

ATT UPPTÄCKA ATTACKER 8
Bakgrund 8
Utmaningar 8
Insikter från vår forskning 8

SAMSPEL AV ATTACKDETEKTIONSSYSTEM 9
Bakgrund 9
Utmaningar 9
Insikter från vår forskning 9

ATTACKDATA OCH KUNSKAPSDELNING 11
Bakgrund 11
Utmaningar 11
Insikter från vår forskning 11

SAMMANFATTNING 12

BIBLIOGRAFI 13

Introduktion

Sakernas internet (IoT) består av uppkopplade enheter som samlar in data med sensorer, utför lokala beräkningar och kommunicerar med varandra eller med mer kraftfulla resurser i molnet. Dessa enheter, som ofta också kan aktivera funktioner som ställdon, används i allt från smarta städer och industriell automation till sjukvård och energihantering. IoT:s potential är enorm, men dess framväxt har också skapat nya och komplexa säkerhetsutmaningar.

IoT-enheter är ofta små och resursbegränsade, vilket gör dem särskilt utsatta för cyberattacker. En angripare kan utnyttja en sårbar enhet för att manipulera data, störa funktioner eller använda enheten som en del av en större attack. Trots dessa risker är IoT avgörande för samhällskritiska funktioner, och systemen måste förbli motståndskraftiga även om enskilda enheter blir komprometterade. Detta kräver både bättre skydd för enheterna och robusta mekanismer för att upptäcka och hantera angrepp.

Projektet RIOT har undersökt hur IoT kan göras säkrare och mer motståndskraftigt genom tre huvudsakliga fokusområden:

- **Utveckling av algoritmer och prototyper:** Vi har tagit fram nya algoritmer och tekniska lösningar för att skydda resursbegränsade enheter och deras data, samtidigt som vi balanserat komplexa avvägningar mellan prestanda, säkerhet och energieffektivitet.
- **Säkerhet genom dataresiliens:** Vi har studerat hur insamlade data kan skyddas mot manipulation, även när enskilda enheter blir utsatta för attacker, bland annat genom blockkedjor och smarta kontrakt.
- **Tvärvetenskaplig samverkan:** Vi har arbetat med industrin, studenter och forskare från andra discipliner för att lyfta säkerhetsfrågorna och skapa en bredare förståelse för IoT:s utmaningar och möjligheter.

En viktig del av RIOT har varit att skapa dialog mellan olika samhällssektorer och forskningsområden. Genom workshops, presentationer och utbildning har vi fört ut resultaten till allt från tekniska experter och studenter till gymnasieklasser och yrkesverksamma utanför datavetenskapen. Även om samverkan varit en central del av projektet ligger denna rapports fokus på de tekniska och forskningsmässiga resultaten.

Rapporten består av flera kapitel som speglar olika aspekter av IoT-säkerhet. I de inledande kapitlen behandlas arbetet med att stärka säkerheten på enhetsnivå, upptäcka attacker och skydda insamlade data. De senare kapitlen tar upp mer teoretiska aspekter av säkerhet, som hur flera detekteringsmetoder kan kombineras, samt praktiska utmaningar som att skapa data för att träna algoritmer.

Förbättrad autentisering

Bakgrund

Autentisering, det vill säga att säkerställa att en person eller en enhet är den de utger sig för att vara, är en central del av cybersäkerhet. Det är grunden för att skydda information och förhindra att obehöriga får tillgång till känsliga system. Ända sedan datorns barndom har autentisering varit en svår utmaning, och lösenord är fortfarande det vanligaste sättet att identifiera sig på nätet. Trots detta har lösenord många svagheter, och när det gäller sakernas internet – där små och uppkopplade enheter blir allt vanligare – förstärks problemen ytterligare.

Utmaningar

Ett av de största problemen med lösenord är att människor ofta återanvänder samma lösenord på flera system. Detta innebär att en läcka i ett system kan ge angripare tillgång till andra tjänster där samma lösenord används. För IoT-enheter, som ofta är små och resursbegränsade, är detta särskilt allvarligt. Dessa enheter saknar ofta tillräcklig datorkraft, minne och energi för att använda moderna och säkra metoder för lösenordshantering.

Moderna lösningar för lösenordssäkerhet bygger ofta på så kallade envägsfunktioner – matematiska omvandlingar som gör lösenord omöjliga att återskapa från den lagrade informationen. Algoritmer som *Argon2* (Biryukov, Dinu, Khovratovich, & Josefsson, 2021) är designade för att vara svåra att knäcka, även för angripare med kraftfulla datorer. Men de kräver också stora resurser, vilket gör dem svåra att använda på små IoT-enheter. Dessutom kan de tunga beräkningarna utsätta servrar för överbelastningsattacker, där många inloggningsförsök skickas samtidigt för att dränera systemets kapacitet.

Insikter från vår forskning

För att adressera dessa problem har vi utvecklat Clipaha – en metod som flyttar den resurskrävande beräkningen från servern till användarens egen enhet. (Riera, Almgren, Picazo-Sanchez, & Rohner, 2023) Genom att använda Clipaha kan även resursbegränsade IoT-enheter dra nytta av moderna och säkra autentiseringsmetoder utan att riskera överbelastning eller kompromissad säkerhet. Clipaha bygger på avancerade lösningar som Argon2, men vår metod gör det möjligt att hantera autentisering effektivt även på små enheter.

Våra tester visar att Clipaha inte bara är säkrare utan också snabbare än många tidigare lösningar. Genom att fördela arbetsbördan mellan klient och server minskar risken för överbelastning, samtidigt som det blir möjligt att använda moderna säkerhetsmetoder även i miljöer med begränsade resurser.

Skydda data även om en enhet komprometteras

Bakgrund

I sakernas internet är data kärnan i många applikationer – från att styra smarta städer till att övervaka sjukvårdspatienter eller optimera energiförbrukning. För att sådana system ska fungera krävs att insamlade data är korrekt och spårbar, även om enskilda IoT-enheter blir utsatta för attacker. Om data manipuleras eller förfalskas kan det få allvarliga konsekvenser, särskilt i kritiska system. Detta gör det viktigt att inte bara skydda enheterna utan också säkerställa att den data som används är tillförlitlig.

Utmaningar

En återkommande utmaning, som vi redan nämnt i tidigare avsnitt, är att IoT-enheter ofta är små och resursbegränsade, vilket gör det svårt att implementera avancerade säkerhetslösningar. Samtidigt samarbetar dessa enheter ofta i nätverk, vilket innebär att en attack mot en enda enhet kan sprida felaktiga data till hela systemet. Dessutom är många IoT-enheter inte kontinuerligt uppkopplade, vilket ytterligare försvårar traditionella metoder för att verifiera och skydda data.

Insikter från vår forskning

För att säkerställa att data är tillförlitliga och spårbara har vi undersökt användningen av blockkedjor och smarta kontrakt. Blockkedjor fungerar som digitala loggböcker där varje ny post verifieras och länkas till tidigare poster, vilket gör det svårt för en angripare att manipulera data utan att bli upptäckt. Genom att använda blockkedjor kan vi skydda data från komprometterade enheter och garantera dess spårbarhet.

En av våra lösningar gör det möjligt för resursbegränsade IoT-enheter att lagra och signera transaktioner lokalt när de saknar nätverksanslutning. Transaktionerna kan sedan verifieras via en blockkedja, vilket gör enheterna självständiga och säkerställer att data är spårbara och tillförlitliga (Profentzas, Landsiedel, & Almgren, 2019).

Vi har också utvecklat metoder där smarta kontrakt används för att automatisera och säkra interaktionen mellan IoT-enheter. Detta är särskilt användbart i miljöer där många enheter samarbetar, exempelvis i smarta städer eller industriella system, för att förhindra manipulation och säkerställa att regler följs (Profentzas, Almgren, & Landsiedel, 2020).

Sammantaget visar vår forskning att blockkedjor och smarta kontrakt effektivt kan säkerställa pålitliga och spårbara data, även i resursbegränsade IoT-miljöer.

Att upptäcka attacker

Bakgrund

Även med förbättrade säkerhetsåtgärder kan hot mot sakernas internet (IoT) inte alltid undvikas. Det är därför avgörande att snabbt identifiera och hantera attacker. Dessa kan syfta till att stjäla data lokalt eller använda komprometterade enheter för att utföra större attacker. Den ökända *Mirai*-attacken (Antonakakis, et al., 2017) visade hur miljontals sårbara IoT-enheter kunde användas för att slå ut stora delar av internet, vilket underströk vikten av att snabbt upptäcka misstänkt beteende.

Utmaningar

Att upptäcka attacker kräver effektiva analysmetoder för att tolka data från IoT-enheter. Traditionella verktyg som Snort (Roesch, 1999) använder mönsterigenkänning för att identifiera kända hot men har svårt att hantera nya och okända angrepp. Djupinlärning erbjuder en lösning genom att upptäcka komplexa mönster, men kräver mycket datorkraft, vilket är svårt att implementera på små IoT-enheter. Dessa enheter är ofta beroende av molnservrar, vilket skapar energikostnader och integritetsproblem.

Insikter från vår forskning

Vi har undersökt hur maskininlärning kan anpassas till IoT-enheters begränsningar. Genom att optimera ramverk som uTensor och TF-Lite-Micro har vi visat att lågströmsenheter kan upptäcka hot i realtid utan att förlita sig på molnet. Detta skyddar både integritet och minskar energibehovet (Profentzas, Almgren, & Landsiedel, 2021).

För att hantera förändrade förhållanden och nya användningsområden har vi utvecklat MicroTL, en metod för så-kallad *transfer learning* på IoT-enheter. MicroTL (Profentzas, Almgren, & Landsiedel, 2022) gör det möjligt att anpassa befintliga modeller till nya miljöer och förhållanden med minimal resursanvändning. Som en vidareutveckling av detta har vi tagit fram MiniLearn, en mer generell metod för lokal inlärning. MiniLearn (Profentzas, Almgren, & Landsiedel, 2022) låter IoT-enheter uppdatera sina modeller lokalt, vilket gör dem flexibla och motståndskraftiga mot förändringar utan att kompromissa med användarens integritet. Dessa metoder är särskilt värdefulla i dynamiska och känsliga miljöer som sjukvård eller industri.

Sammantaget visar vår forskning att IoT-enheter kan upptäcka hot och anpassa sig till nya attacker, samtidigt som integritet och energieffektivitet bevaras.

Samspel av attackdetektionssystem

Bakgrund

Intrångsdetekteringssystem (IDS) är grundläggande för att säkra IoT-nätverk genom att upptäcka ovanliga aktiviteter eller policyöverträdelser. Som svar på den ökande komplexiteten i cyberhot har **sammansatta IDS** – system som integrerar flera detektionskomponenter – ramträtt som ett lovande tillvägagångssätt. Genom att kombinera olika detektionsmetoder syftar dessa system till att förbättra motståndskraft och anpassningsförmåga.

Att utvärdera sammansatta IDS är inte enkelt. Traditionella prestationsmått misslyckas med att fånga samspelet mellan enskilda komponenter. För att lösa denna utmaning antog vi ett informationsteoretiskt perspektiv för att analysera hur individuella IDS-komponenter bidrar till systemets robusthet. Det möjliggör en uppdelning av den totala systeminformationen i redundanta, unika och synergistiska bidrag, vilket ger värdefulla insikter i komponenternas interaktion.

Utmaningar

IDS står inför två stora utmaningar som försvårar deras design och utvärdering. Den första utmaningen är den så kallad *base-rate fallacy* (Axelsson, 2000), ett problem som uppstår på grund av den låga förekomsten av faktiska intrång i förhållande till legitima händelser. Denna obalans snedvrider systemets prestationsmått, vilket gör det svårt att optimera både så-kallade true-positives, som indikerar framgångsrik upptäckt av angrepp, och false-positives, som speglar falska larm. Det gör att systemet inte fungerar så effektivt eller bra som det skulle kunna göra.

Den andra utmaningen härrör från adaptiva angripare, som kontinuerligt utvecklar sina attackstrategier för att undvika att bli upptäckta. Sådana angripare kan skapa manipulerade data – små förändringar som lurar säkerhetssystemen att inte upptäcka ett angrepp. Denna dynamiska och ständigt föränderliga hotmiljö kräver IDS som inte bara är mycket exakta utan också motståndskraftiga mot avancerade strategier för att undvika upptäckt av attacker. Komplexiteten i sammansatta IDS gör detta ännu svårare, eftersom samspelet mellan komponenterna inte alltid är väl förstått. Utan en tydlig bild av hur komponenter bidrar hela systemet blir det svårt att effektivt integrera och optimera dem för robust prestanda.

Insikter från vår forskning

För att hantera dessa problem skapade vi ett verktyg som analyserar hur olika delar av säkerhetssystemen samarbetar för att upptäcka hot, via *partial information decomposition* (PID). Detta tillvägagångssätt gav värdefulla insikter om bidragen från enskilda systemkomponenter och deras interaktioner. Genom att dela upp

information kunde vi tillskriva systemets prestanda till tre olika typer av bidrag. *Redundanta* bidrag representerar den information som delas mellan flera komponenter, vilket förbättrar tillförlitligheten men potentiellt leder till ineffektivitet om det överbetonas. *Unika* bidrag, å andra sidan, tillhandahålls exklusivt av enskilda komponenter och är avgörande för att identifiera specifika, sällsynta attackmönster. Slutligen uppstår *synergistiska* bidrag endast genom samspelet mellan flera komponenter och möjliggör upptäckt av mer komplexa och koordinerade attackstrategier.

Våra resultat visade att synergi spelar en avgörande roll för robustheten hos sammansatta IDS, särskilt mot avancerade attacker. När interaktionen mellan komponenter optimerades skapades nya förmågor som överträffade summan av deras individuella bidrag. Dessutom erbjöd vårt arbete praktisk vägledning för att optimera systemdesign. Till exempel förbättrade justeringen av tröskelvärdena för enskilda IDS baserat på deras bidragstyp den övergripande systemprestandan. Vi visade också vikten av att noggrant överväga tillägg av nya klassificerare, eftersom deras integration kan ha betydande påverkan på redundans och synergi.

Genom fallstudier med redan existerande IDS-data lyfte vi fram de kompromisser som är involverade i att optimera sammansatta system. Studierna visade att för att systemet ska fungera bra behöver det både minimera falska larm och kunna stå emot manipulativa angrepp. Utöver IDS visade vår forskning att PID är ett kraftfullt verktyg för att utvärdera robustheten hos andra komplexa system, såsom IoT-nätverk och maskininlärning. Möjligheten att kategorisera bidrag som redundanta, unika eller synergistiska erbjuder en ram för att förstå och förbättra designen av olika sammankopplade system (Mages, Almgren, & Rohner, 2022).

Attackdata och kunskapsdelning

Bakgrund

IoT-nätverk är mål för skadlig aktivitet som kan påverka integritet, robusthet, prestanda och affärsverksamhet. Exempel på angrepp inkluderar överbelastnings-angrepp, manipulation av enheter eller data, och injicering av falsk information. Intrångsdetekteringssystem (IDS) är en kritisk del av en effektiv cybersäkerhets-strategi, men utmaningen ligger i att förutsäga nya angrepp. Maskininlärning är en lovande metod för att designa IDS, men dess framgång hämmas av två huvud-sakliga faktorer: begränsad datatillgång och integritetsproblem vid datadelning.

Utmaningar

Begränsad datatillgång har att göra med att angrepp är relativt sällsynta och det finns inte alltid relevanta loggar som kan användas för att träna ett IDS. Ofta skulle man kunna lära sig av andra aktörer som har genomgått angrepp, men att dela data är känslig då den även kan innehålla känslig information om aktörens nätverk eller affärstransaktioner.

Insikter från vår forskning

För att säkerhetssystemen ska bli bättre skapade vi en simulator som genererar data om olika typer av attacker. Detta gör systemen mer förberedda på nya hot som de tidigare inte observerat. Vi delar *kunskap* i stället för rådata mellan aktörer i form av maskininlärningsmodeller. Vi använder en teknik (*federated learning*) som låter flera system dela information utan att behöva samla all data på ett ställe. Det gör att säkerheten kan förbättras utan att kompromissa med integriteten hos känslig data.

Vi visar att modeller som tränats på specifika angreppstyper eller nätverks-konfigurationer inte generaliserar till nya scenarier, vilket understryker behovet av förbättrade metoder. Datadelning visade sig vara mycket effektiv men kräver ömsesidigt förtroende mellan aktörer, medan den integritetsskyddande metoden presterade bra för angreppsvariationer men var mindre robust i scenarier med varierande topologier. Forskningen ger värdefulla insikter för att förbättra IDS-prestanda genom att utnyttja samarbetande inlärningstekniker samtidigt som integritetsbegränsningar hanteras, och lägger grunden för framtida utveckling av mer adaptiva och skalbara IDS-lösningar anpassade för dynamiska IoT-miljöer (Kaveh, Rohner, & Johnsson, Impact of Attack Variations and Topology on IoT Intrusion Detection Model Generalizability, 2024) (Kaveh, Pettersson, Rohner, & Johnsson, 2023).

Sammanfattning

IoT, sakernas internet, har på kort tid blivit en central del av samhällsviktig infrastruktur, från sjukvård och energi till vattenförsörjning och smarta städer. Det som gör IoT unikt är dess uppbyggnad av små, resursbegränsade och ofta billiga enheter, vilka tillsammans utgör basen för insamling och hantering av data. Trots framsteg inom cybersäkerhet för traditionella system kräver IoT särskilda säkerhetslösningar eftersom dess sårbarheter kan påverka inte bara enskilda enheter, utan hela nätverk och kritiska system. Med den växande användningen av IoT blir det allt viktigare att adressera dessa utmaningar.

Denna rapport sammanfattar delar av forskningen från projektet RIOT, som har fokuserat på att stärka säkerheten och motståndskraften i IoT-system. Vi har utvecklat algoritmer som kan användas för att förbättra säkerheten på enhetsnivå, upptäcka och hantera attacker, samt skydda data även om enheter komprometteras. Vissa av dessa resultat är tillämpbara nästan direkt i industrin, medan andra bidrar med teoretiska insikter som kan styra forskningen framåt. En viktig del av projektet har också varit att skapa data som möjliggör och förenklar framtida forskning inom området.

Rapportens innehåll speglar bredden av forskningen i RIOT – från praktiska lösningar som kan förbättra säkerheten i dagens IoT-system till långsiktiga teoretiska framsteg som lägger grunden för framtida innovationer. Tillsammans visar resultaten hur viktigt det är att kombinera teknisk utveckling med ett strategiskt och forskningsdrivet angreppssätt för att möta de säkerhetsutmaningar som IoT innebär.

Bibliografi

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., . . . Zhou, Y. (2017). Understanding the Mirai Botnet. *26th USENIX Security Symposium.*

Axelsson, S. (2000). The base-rate fallacy and the difficulty of intrusion detection. *ACM Transactions on Information and System Security (TISSEC)*, 186–205.

Biryukov, Dinu, Khovratovich, & Josefsson, 2. (2021). Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications (RFC 9106). *RFC 9106*. Internal Research Task Force (IRTF).

Kaveh, A., Pettersson, A., Rohner, C., & Johnsson, A. (2023). On the Impact of Blackhole-Attack Variations on ML-based Intrusion Detection Systems in IoT. *NOMS 2023 - IEEE/IFIP Network Operations and Management Symposium.*

Kaveh, A., Rohner, C., & Johnsson, A. (2024). Impact of Attack Variations and Topology on IoT Intrusion Detection Model Generalizability. *2024 IEEE 21st International Conference on Mobile Ad-Hoc and Smart Systems (MASS).* IEEE.

Mages, T., Almgren, M., & Rohner, C. (2022). q. *Computers & Security*.

Profentzas, C., Almgren, M., & Landsiedel, O. (2020). TinyEVM: Off-Chain Smart Contracts on Low-Power IoT Devices. *IEEE International Conference on Distributed Computing Systems.*

Profentzas, C., Almgren, M., & Landsiedel, O. (2021). Performance of deep neural networks on low-power IoT devices. *CPS-IoTBench '21: Proceedings of the Workshop on Benchmarking Cyber-Physical Systems and Internet of Things.*

Profentzas, C., Almgren, M., & Landsiedel, O. (2022). MicroTL: Transfer Learning on Low-Power IoT Devices. *2022 IEEE 47th Conference on Local Computer Networks (LCN).*

Profentzas, C., Almgren, M., & Landsiedel, O. (2022). MiniLearn: On-Device Learning for Low-Power IoT Devices. *International Conference on Embedded Wireless Systems and Networks.*

Profentzas, C., Landsiedel, O., & Almgren, M. (2019). IoTLogBlock: Recording Off-line Transactions of Low-Power IoT Devices Using a Blockchain. *Proceedings of the 44th IEEE Conference on Local Computer Networks (LCN).*

Riera, F. B., Almgren, M., Picazo-Sanchez, P., & Rohner, C. (2023). Clipaha: A Scheme to Perform Password Stretching on the Client. *Proceedings of the 9th International Conference on Information Systems Security and Privacy*, (pp. 58–69).

Roesch, M. (1999). Snort – Lightweight intrusion detection for networks. *Proceedings of LISA '99: 13th Systems Administration Conference (Usenix).*

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publikationsnummer MSB2526 – december 2024