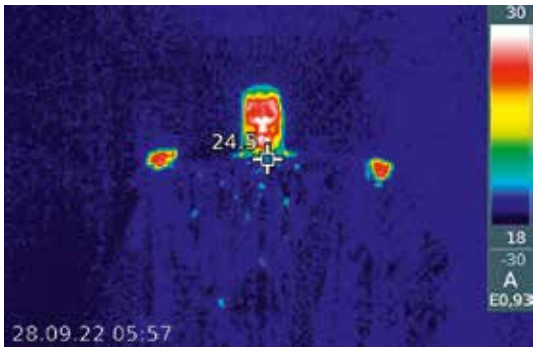
IoT-data som bevis i brottsutredningar

Av Ulf Seijmer, Induo och AKKR8

Ulf Seijmer är innovationschef på Induo samt CTO och medgrundare till hårdvaruföretaget AKKR8. Han är också styrelsemedlem i EUTECHs IoT Alliance. År 2012 skrev han en av de första artiklarna om 5G, en artikel som publicerades i Elektroniktidningen. Ulf är en frekvent anlitad föreläsare inom trådlös teknik för LPWAN och 5G.



Under de senaste tio–femton åren har våra byggnader fått en puls. Sensorer, loggar och styrsystem producerar en ständig ström av data som beskriver vad som faktiskt sker. Den här utvecklingen har gjort fastighetsautomation till en allt viktigare källa för forensiskt arbete.

Byggnaden som brottsplats är inte längre bara en plats där ett brott sker, utan något mer – en plats att undersöka, ibland med en historia, sann eller förvanskad. Byggnaderna är vittnen, vittnen som kan tala om man vet hur man skall fråga. De är system med historik, tidsserier och mätvärden som kan bidra till att rekonstruera händelseförlopp. Men till skillnad från mänskliga vittnen är detta tekniska konstruktioner, med kända begränsningar och ibland okända svagheter.

Byggnaden som stöd i brottsutredningar, Forensik i uppkopplade byggnader, skiljer sig fundamentalt från traditionell IT-forensik. Här handlar det om att analysera tidsserier från sensorer och styrsystem: PIR-detektorer, CO_2-nivåer, temperaturer, magnetkontakter och styrsignaler till aktuatorer.

Sensorer och aktuatorer i ett fastighetsautomationssystem är vanliga hjälpmedel för att ge stöd till exempelvis drifts- och underhållsplanering, styrning av inomhusklimat och energioptimering, men sällan designade med forensiskt bevisvärde i åtanke. Samplingsfrekvenserna är ofta låga, tidsstämplar och dataformatering kan skilja sig mellan system och loggning är i första hand avsedd för drift och felsökning, inte för metodisk rekonstruktion i efterhand. Därför är tester och metodik centrala för att avgöra vad som går att lita på.

I den forskning som bedrivits kring forensik i uppkopplade byggnader har fokus legat på att systematiskt pröva vilken tillförlitlighet vanliga fastighetssensorer faktiskt har som beviskälla. Utgångspunkten är enkel men ofta förbisedd: sensorer i byggnader är inte konstruerade för att fastställa sanningen om en händelse, utan för att trigga funktioner eller optimera drift.

I experimentella studier och forskning jag har tagit del av har Johnny Bengtsson, IT-forensiker vid Nationellt forensiskt centrum (NFC) fördjupat sig i hur sensorer som PIR, CO_2 och magnetkontakter reagerar på kontrollerade stimuli, hur lätta de är att påverka, och vissa fall manipulera, samt hur deras data beter sig över tid. Resultaten visar att sensordata sällan är binär eller entydig. Samma händelse kan ge olika avtryck, vilket innebär att mätvärdena i sig kan inte betraktas som objektiva, utan måste tolkas som tekniska vittnesmål med kända osäkerheter.

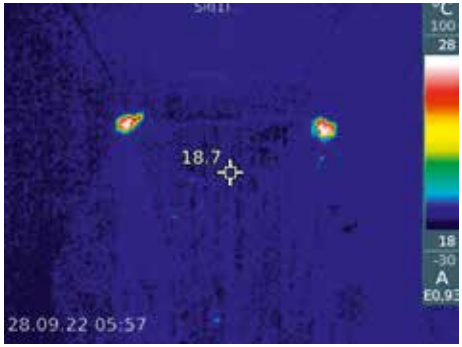
När avsiktliga och oavsiktliga händelser blandas i en uppkopplad byggnad genereras data av tre kategorier av händelser, avsiktliga stimuli, oavsiktliga händelser och rena olyckor. En magnetsensor reagerar när en dörr öppnas, ett röstkommando till en smart högtalare tänder lampan och om en vattenläcka träffar en läckagesensor så triggar den en kulventil som stänger inkommande vatten. Alla dessa skeenden skapar digitala spår som i teorin kan användas för att rekonstruera en tidslinje vid brott eller olycka. Frågan man måste ställa sig är om sensordata manipulerats och därmed ger en felaktig bild av vad som hänt, eller om mätningarna faktiskt är korrekta? Fungerade sensorn som den skulle och hur var den monterad? För forensiskt arbete är det avgörande att skilja mellan vad systemet registrerade och vad som faktiskt hände.

Genom att andas i en luftmadrass går det att undgå upptäckt av CO_2-sensorer.

Manipulation och oavsiktliga bieffekter

Ett centralt resultat i forskningen är att manipulation av sensorer inte nödvändigtvis kräver intrång i systemen. I många fall räcker det med att påverka den fysiska miljö som sensorn tolkar. Forskningsresultat visar att det går att skapa både falska positiva och falska negativa utslag med relativt enkla medel. Frånvaron av en sensors registrering av data kan alltså inte automatiskt tolkas som frånvaro av aktivitet.

Ett av de mest illustrativa testen i Johnnys forskning gäller PIR-sensorer, vanliga i kontor och trapphus för närvarodetektering. PIR reagerar på förändringar i infraröd strålning – i praktiken värme – och reagerar inte enbart på mänsklig värme. Detta gör dem känsliga för värmekällor som inte är mänskliga. Genom att flyga en liten drönare inom-



PIR-sensorer reagerar på förändringar i infraröd strålning – i praktiken värme. De är tänkta att reagera på mänsklig värme men kan luras av en drönare eller andra värmekällor.

hus kunde man skapa tydliga falska positiva utslag: systemet tolkade drönaren som mänsklig rörelse. Försöket visar hur enkelt felaktiga spår kan skapas och hur snabbt en utredning kan ledas fel.

Lika viktigt var försöken att uppnå falska negativa resultat; med en nödfilt med metallbestrykning gick det delvis att maskera kroppsvärme och därmed undgå rörelsedetektering. I praktiska tester med rörelsestyrd belysning på toaletter kunde registrering helt utebli. Det gick att gå in på toaletten och stanna där en ansenlig stund utan att sensorerna registrerade rörelse.

När man testade CO_2-sensorer uppvisade de högre robusthet; människans andningsavtryck är svårt att kapsla in över tid men genom att andas i luftmadrasser gick det ändå att lösa, även om det är svårt och kanske inte så praktiskt. Här är det snarare i mätfrekvensen som CO_2-sensorn uppvisar brister. CO_2-sensor mäter med olika frekvens, vissa mäter så sällan som var tionde minut, och det betyder att dataluckor uppstår, små tidsfönster kan utnyttjas av en angripare eller av en person som vill undvika upptäckt.

Begränsat bevisvärde och kontexten

Sensordata i uppkopplade byggnader bör därmed sällan betraktas som primär bevisning. I stället fungerar den bäst som stödjande information, som kan stärka eller ifrågasätta andra iakttagelser.

Ett återkommande tema i forskningen är att kombinationer av flera sensortyper ger ett betydligt robustare underlag än enskilda mätpunkter. Om man lägger samman flera dataset ökar sannolikheten att se oegentligheter, som att data verkar vara korrupt eller kan ha manipulerats. I exemplet ovan kanske inte PIR-sensorn triggats, medan CO_2-sensorn registrerat att någon kan ha andats i lokalen. Sensorernas begränsade upplösning i tid, deras känslighet för installation och miljö samt bristen på standardiserad loggning gör att de sällan kan ge exakta svar på vad som hänt – men de kan ge goda indikationer på vad som kan ha hänt.

Detta ska dock inte tolkas som att mer data eliminerar osäkerheter. Tvärtom, nya tolkningsproblem introduceras när flera tidsserier med olika upplösning, samplingsfrekvens och tidsstämpling ska vägas samman. Det stora forensiska värdet ligger inte i just mängden data, utan i förståelsen för hur olika sensorer samverkar – och var de inte gör det.

Tekniska skillnader

Förutom höga krav på hur data samlas in, säkras och analyseras så måste man understryka vikten av att analysera sensorernas tekniska förutsättningar lika noggrant som själva mätvärdena. Utan kunskap om hur ett system är uppbyggt riskerar även korrekt insamlad data att misstolkas. En CO_2-sensor med en viss tolerans, teknisk konstruktion och placering kan inte rakt av jämföras med ett annat fabrikat med andra tekniska förutsättningar eller annan monteringsplats.

Forensiskt arbete kräver metodik

För att dra trovärdiga slutsatser behövs en ▶▶

strukturerad arbetsgång som speglar traditionell forensik men med en extra ingenjörsdimension. Tidsstämplar kan vara osynkade, samplingsfrekvenser för låga och loggnivåer anpassade för drift snarare än bevisinsamling.

Den mänskliga faktorn är också kritisk; kognitiv bias, förväntningar och grupptänk riskerar färga tolkningen. NFC:s praxis att arbeta två personer vid analys är ett sätt att minska risken för förhastade slutsatser.

Cyberangrepp och hybridhot

När fastighetsautomation och IoT kopplas upp ökar också angreppsyta och attraktionskraft för illasinnade aktörer. Motivbilden spänner från ekonomisk vinning och utpressning till sabotage och mer komplex hybridpåverkan där samhällskritiska funktioner eller produktionskapacitet påverkas negativt eller sätts ur spel. Effekterna kan vara att driftpersonal stängs ute, att sensorer manipuleras eller att inomhusmiljöer förändras för att orsaka fysisk eller personell skada eller skapa missvisande forensiska data. Förebyggande åtgärder måste därför kombinera klassisk säkerhetsarkitektursegmentering, nätavskiljning, uppdateringsrutiner med operationella rutiner: incidentplaner, ansvarskedjor och tydliga procedurer för hur loggar och artefakter ska säkras vid misstanke om intrång.

Ur ett forensiskt perspektiv pekar forskningen inte i första hand på behovet av fler sensorer, utan på bättre kontroll över data. Det handlar om tillförlitlig tidsstämpling, spårbarhet i systemförändringar och möjlighet att i efterhand återskapa ett systems tillstånd vid en given tidpunkt.

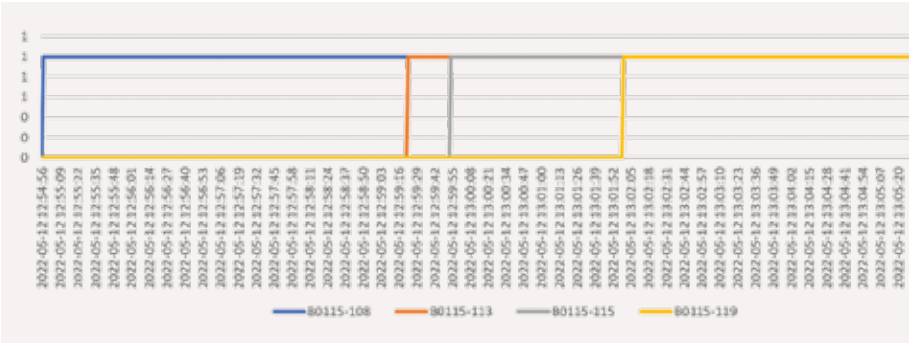
I praktiken innebär detta att smarta byggnader behöver utformas med analys i åtanke, inte bara automation. System som kan frysa loggar, bevara historik och tydligt visa hur data genererats har ett avsevärt högre forensiskt värde än system som enbart presenterar aktuella mätvärden. Här blir systemarkitekturfrågor minst lika viktiga som sensorval.

Digitala tvillingar och bevarande av scenarier

Ett möjligt verktyg i detta sammanhang är digitala tvillingar: kontinuerligt uppdaterade kopior av byggnadens tillstånd som kan användas både för simulering av angrepp och för att frysa ett incidentögonblick. Genom att kombinera lidar, GPS, tidsloggar och sensordata går det att skapa en tidsmässigt synkroniserad bild som underlättar rekonstruktion. Digitala tvillingar kan också vara ett verktyg för testmiljöer där man proaktivt tränar på angrepp och försvar utan att riskera produktion. För att detta ska fungera i forensiskt syfte krävs dock designbeslut som prioriterar bevisvärde: säkra loggar, klocksynkronisering, högre samplingsfrekvenser där det är relevant och en arkitektur som möjliggör bevarande av snapshot-data.

När byggnaden blir ett vittne

Det som gör området så angeläget är kombinationen av teknisk potential och praktiska begränsningar. Data från sensorer kan, rätt hanterad, hjälpa utredare att förstå händelseförlopp; de kan också vilseleda om systemen inte är robusta eller om aktörer medvetet manipulerar dem. För IoT-branschen innebär detta ett ansvar: att designa lösningar som inte bara optimerar drift och energieffektivitet utan också tar hänsyn till forensisk spårbarhet. Våra uppkopplade byggnader lämnar fler spår än någonsin, men för att använda dem måste vi veta hur vi tolkar och bevarar dem. ■



Diagrammen visar hur sensorerna registrerat drönarens rörelser.