

Obefogade farhågor om säkerhet

En av de pådrivande krafterna bakom DASH-initiativet (Desktop and mobile Architecture for System Hardware) är DMTF (Distributed Management Task Force). Syftet med initiativet är att ersätta leverantörsspecifika IT-nätverkslösningar med en öppen branschstandard som främjar informationsutbyten mellan IT-administratörer, en effektiv fjärrhantering och en flexibel programmeringsmiljö.

DASH-initiativet bygger på en gränsöverskridande CIM-modell (Common Information Model) som hanteras på en webbplattform. Plattformen gör att IT-administratörer kan fjärrstyra systemuppgifter i realtid. Det går att fjärrstyra omstarter eller att bekräfta programuppdateringar vilket både förenklar och effektiviserar nätverkshandlingen. Säkerhet är ett ämne som ofta dyker upp i diskussioner om fjärrhantering. Många uppfattar själva fördelen, fjärråtkomsten, som ett säkerhetsproblem. Säkerhet är självklart mycket viktigt vid systemhantering och en faktor som IT-administratörer alltid tar med i beräkningarna. CIM-modellen innebär att det är en utmaning att dela och ge användare tillgång till nätverksinformation inom ett individuellt nätverk med öppen standard och

samtidigt förhindra att informationen kan missbrukas. Tidigare erfarenheter har därför fått IT-administratörer att ifrågasätta nivån och pålitligheten för nätverkssäkerhet i DASH-initiativet och i DASH-kompatibla nätverkslösningar.

Leverantörsägda nätverkslösningar har allmänt ansetts vara mycket säkra och pålitliga. Patent och licenser har begränsat möjligheterna att få åtkomst till data och att förändra systemen. Men flexibilitet är inte synonymt med bristande säkerhet. Det går att säkerställa datasäkerheten genom interna IT-principer där exempelvis endast användare med administratörsrättigheter kan anpassa nätverksinställningarna. Och i motsats till vad många tror så klarar DASH-initiativet av säkerhetskraven genom att definiera säkerheten i flera nivåer. DASH-kompatibla IT-lösningar innehåller procedurer för autentisering och auktorisering som gör att IT-administratörer kan fjärrstyra sina nätverk i realtid. De kan även kontrollera att användarna inte har tillgång till konfidentiella data eller att de är begränsade till uppgifter på administratörsnivå.



Säkerhet och sekretess

DASH-kompatibla datorer hanterar två säkerhetstyper, klass A och B. Klass A kräver inte datakryptering, men det gör klass B. Klass B tillgodoser IT-administratörernas krav i fråga om sekretess och konfidentialitet för kunddata och erbjuder samtidigt ytterligare säkerhetsnivåer.

Bakgrundsinformation

DMTF (Distributed Management Task Force, Inc.) är en branschorganisation som leder utveckling, främjande och acceptans av gränsöverskridande standarder och initiativ för IT-administration. DMTF omfattar drygt 4 000 aktiva medlemmar som representerar 44 länder och nästan 200 företag. Under de senaste 15 åren har DMTF:s administrationstekniker blivit avgörande för gränsöverskridande hantering av system, verktyg och lösningar från många olika leverantörer inom ett företag. Genom att välja lösningar som följer DMTF:s standarder kan IT-ansvariga driftsätta en blandning av system och lösningar som bäst passar användarnas behov, och samtidigt minska hanteringskomplexiteten och den totala ägandekostnaden. Mer information om DMTF:s tekniker och verksamhet finns på www.dmtf.org.

“För video och kameraövervakning kan det vara oerhört viktigt att paket inte tappas, då det kan orsaka pixelfel, eller att bilden hoppar till och viktiga detaljer försvinner.”

MELVYN WRAY,
ALLIED TELESIS



DASH-INITIATIVET

En annan av säkerhetsfunktionerna i DASH är hanteringen av nätverkskort. Nätverkskortet innehåller inbyggda krypteringsfunktioner och en fast krypteringsprocessor för kryptering och dekryptering. Det förhindrar inte bara att obehörig personal får åtkomst till privilegierade data utan frigör även vårdprocessorn att hantera andra IT-administrationsuppgifter. Det innebär kortare administrationstider i nätverket och att IT-administratörer alltid kan skicka och ta emot skyddade data med högsta möjliga anslutningshastighet. Allied Telesis nätverkskort AT-2812FX för Fast Ethernet över fiber kan till exempel öka säkerheten genom att använda säkra IP-protokoll som kallas IPSec (IP Security). Med IPSec måste alla IP-datapaket i en dataström autentiseras och/eller krypteras. AT-2812FX stöder även protokollen IPSec AH (Authentication Header) och ESP (Encapsulation Security Payload) för upp till 32 SA (Security Associations) vilket skapar en pålitlig och säker dataöverföring, från början till slut.

Användarvänligt

DASH-standarden är gränsöverskridande och den gör det enklare för IT-administratörer att dela information över Internet vilket skapar en flexiblare, mer anpassningsbar och användarvänlig nätverkshantering. En av de allra viktigaste funktionerna är att obehöriga användare inte får åtkomst till driftshanteringsverktyg eller personlig information. Tack vare att säkerheten hanteras i flera nivåer, och med IPSec och en rad andra autentiseringsprotokoll, har IT-administratörer fullständig kontroll över driften vid fjärrövervakning av de DASH-kompatibla datorerna. Det är viktigt att IT-administratörer använder olika IT-principer för olika verksamheter. Det är bra för DASH-initiativet som redan innehåller de säkerhetsfunktioner som krävs för att göra det meningsfullt att ha en flexiblare fjärrövervakning.

DASH för video

Hur förhåller sig DASH till tjänster som streaming video och video on demand? Administratörer som använder sig av kameror och andra produkter som stödjer DASH-standarden har fördelen att via ett gemensamt interface kunna kommunicera med sina enheter. Detta kan innebära en förenkling i hur kameror och andra produkter med video streaming-möjlighet kan hanteras via samma gränssnitt. En annan viktig fråga är QoS, quality of service, alla bitarna måste fram till mottagaren i en jämn stadig ström annars hoppar bild och ljud. I ett nätverk där flera typer av tjänster används, så måste det gå att säkerställa kvalitén på genomflödet av de olika tjänsterna i nätverket. För video och kameraövervakning kan det vara oerhört viktigt att paket inte tappas, då det kan orsaka pixelfel, eller att bilden hoppar till och viktiga detaljer försvinner. Med hjälp av QoS kan vi bestämma hur trafiken och tjänsterna i nätverket skall prioriteras, då nätverket börjar belastas till sin yttersta kapacitet. Med QoS kan vi se till att tjänster som t ex video alltid får prioritet över andra tjänster som vanlig dataöverföring. Börjar kapaciteten ta slut i nätverket, så ser ex Allied Telesis avancerade switchar till att den trafik eller tjänst med lägst prioritet begränsas först och video fortsätter att flyta på som det skall.



SRH840 är Shure's referenslur och är konstruerad speciellt för kristisk lyssning och professionell inspelning. Med dess exakta frekvensgång kan den leverera korrekt ljud i krävande studiomiljöer.
Rek pris 2 595,-



PROFESSIONAL SOUND FROM EAR TO EAR.

I över 80 år har Shure försett marknaden med professionella audioprodukter med legendarisk prestanda. Denna totala hängivenhet till att ständigt utveckla funktion och kvalitet på sina produkter gäller i högsta grad de nya professionella hörlurarna i SRH-serien. Det är bara en sak som gäller för dessa lurar: det som kommer in måste komma ut! Designen, med dess höga fokus på att hålla emot vardagligt slitage, gör dessa lurar till det perfekta valet för professionella musiker - för inspelning, monitorlyssning, och vanlig lyssning.

SHURE
LEGENDARY
PERFORMANCE™