



Veilige communicatie met DECT-compatible oplossingen.

Plantronics biedt de enige DECT-compatible headsetapparaten en gestroomlijnde gecentraliseerde managementsoftware ter wereld.

Digitally Enhanced Cordless Telecommunication (DECT) is een technologie van 1.9 Ghz, die gebruikmaakt van een specifiek deel van het draadloze spectrum om een hoog niveau van beveiliging en geluidskwaliteit in kantoor- en thuisomgevingen te bieden. DECT-technologie wordt vaak aangeduid als "storingsvrij" omdat het geen spectrum deelt met andere technologieën zoals wifinetwerken.

Beveiliging is één van de vele sterke punten van DECT-technologie. Het gebruikt Time Division Multiple Access (TDMA) digital radio en dynamische kanaalselectie over 10 carrier-frequenties en 24 time slots, gekoppeld met een meerlaags beveiligingssysteem. Dit gelaagde systeem met een abonnement, encryptie en authenticatie, beschermt tegen af luisteren. Bepaalde branches, zoals de gezondheidszorg en de financiële sector, vereisen DECT-gebaseerde draadloze communicatie vanwege de beveiliging en vertrouwelijkheid.

VOORZIEN IN VERBETERDE DECT-BEVEILIGING

De draadloze DECT-oplossingen van Plantronics zijn 's werelds enige producten die zowel aan de standardeisen voldoen als aan de verbeterde veiligheidseisen van de DECT-standaard, zoals die zijn opgesteld door het European Telecommunications Standards Institute (ETSI).

De vraag naar verbetering van de DECT-standaard bleek in 2009, toen een groep white-hat hackers, bekend als de DeDECTed Group, een artikel publiceerde waarin de veiligheidslekken van standaard DECT-producten werden uiteengezet. De hackergroep ontmaskerde de dreiging zodra DECT-producten geen gebruikmaken van de standaardcontrole en codering zoals beschreven in de ETSI-normen. Plantronics DECT-producten beschikken altijd over controle en codering.

Het DECT Forum, waarvan Plantronics lid is, beoordeelde de bevindingen van de DeDECTed Group en lanceerde in 2013 als reactie daarop het officiële DECT Security Certification Programme (DECT-beveiligingscertificaatprogramma). Het programma zorgt dat producten afzonderlijk zijn getest en gecontroleerd door een erkend laboratorium.

ALLEEN PLANTRONICS BIEDT UITGEBREIDE DECT-BEVEILIGING

De nieuwe DECT-normen bieden richtlijnen voor verbeteringen in vier nieuwe gebieden (zie hieronder), waarmee het totale aantal beveiligingscategorieën op acht komt te staan. In feite is Plantronics de eerste aanbieder in de draadloze productenindustrie die volledig voldoet aan de veiligheidsnormen van het DECT Forum. De Plantronics CS500-serie begon in oktober 2013 met de verbeterde beveiligingsfuncties.

Met ingang van januari 2016 beschikken de Plantronics Savi 400- en Savi 700-series over verbeterde DECT-beveiliging en maken daarmee de Plantronics DECT-portefeuille compleet. Alle Plantronics DECT-producten voldoen aan de acht beveiligingsfuncties van het DECT Forum. Plantronics is daarmee nog steeds de enige aanbieder van draadloze oplossingen die volledig voldoen aan deze DECT-standaard:

STANDAARD DECT-BEVEILIGINGSFUNCTIES

1. Registratieprocedure en tijdsbestek voor het instellen van een 64-bits verificatiecode - het basisstation staat niet langer dan 120 seconden 'open voor registratie'. De registratie van een headset met het basisstation kan daardoor alleen plaatsvinden wanneer de gebruiker de registratie heeft gestart, en voltooid binnen 120 seconden.
2. Activatie van codering (basisstation en headset): zowel het basisstation als de headset ondersteunen coderingsactivering en het basisstation activeert deze voor alle oproepen. Voorheen activeerden DECT-apparaten de codering niet bij alle oproepen.
3. Uitgezonden sleuteltoewijzing: het basisstation maakt een 64-bits gebruikersverificatiecode (user authentication key, UAK) aan en wijst deze toe wanneer de headset is geregistreerd. Dit beschermt het basisstation en de headsets tegen man-in-the-middle-aanvallen. Zowel het basisstation als de headset gebruiken de verificatiecode in hun communicatie.
4. Authenticatie van de headset: het basisstation kan verifiëren of de headset origineel is en geen indringer of een poging tot het imiteren van de originele headset. Deze functie zorgt ervoor dat er geen communicatie kan plaatsvinden tussen de headset en het basisstation als zij onderling niet zijn geverifieerd.

VERBETERDE DECT-BEVEILIGINGSFUNCTIES

5. Verbeterde willekeurige getal generator: een sterker algoritme om dubbele soortnummers bij het genereren van coderingssleutels te vermijden. Deze verbetering maakt het onmogelijk om het willekeurige getal te achterhalen met opeenvolgende pogingen om vervolgens te worden gebruikt bij het maken van sleutels.
6. Evaluatie van gedrag aan gelijke zijden met betrekking tot time-outwaarden van de codering bij de activering van een oproep: als een zijde zich anders gedraagt dan verwacht, bijvoorbeeld wanneer de codering niet tijdig wordt gestart, beschouwt het apparaat het als een poging tot overtreding van de beveiliging, waarna de oproep wordt beëindigd.

Elke hackpoging zou in ieder opzicht perfect moeten zijn, aangezien elke communicatie tussen een headset en het basisstation buiten het verwachte patroon om ervoor zorgt dat de verbinding wordt beëindigd.
7. Snelle codering: garandeert onmiddellijke coderingsactivering nadat verbinding tot stand is gebracht, voordat protocolberichten uit hogere lagen worden uitgewisseld, waaronder bellers-id, gekozen nummers, enz. Er wordt geen informatie uitgewisseld zonder codering.
8. Procedure voor het opnieuw versleutelen met een nieuw verkregen coderingssleutel tijdens een oproep: de coderingssleutel die wordt gebruikt door het coderingssysteem wordt ten minste eenmaal per minuut bijgewerkt, waardoor iedere poging tot het kraken van de codering met brute technieken, zoals supercomputing, wordt verijdeld.

DECT 101: De voordelen van Plantronics DECT

GEKOPPELDE VERIFICATIE

Basisstations en andere apparaten worden op elkaar afgestemd zodat zij elkaar eenvoudig kunnen herkennen. Een geheime verificatiecode wordt berekend met het DECT Standard Authentication Algorithm (DSAA). Alleen fabrikanten van de apparatuur weten wat de werking van dit algoritme is. De duur waarin apparaten gekoppeld zijn, is beperkt vanwege extra beveiliging.

CONTROLE

Beide apparaten controleren of de juiste verificatiecode wordt gebruikt en ontcijferen de coderingssleutels (die worden gebruikt om de gegevens te coderen die via de ether worden verzonden) met behulp van de DECT Standard Cipher (DSC). De definitie van dit algoritme wordt alleen ter beschikking gesteld aan fabrikanten van apparatuur.

CODERING

De 64-bits coderingssleutel wordt gebruikt om spraakgegevens, die via de ether worden verzonden, digitaal te coderen. Aan de ontvangende kant wordt de sleutel uit de verificatiefase, gebruikt om de gegevens te decoderen.

DYNAMISCHE CHANNEL AGILITY

Als onderdeel van het DECT-protocol zullen apparaten, zodra er sprake is van interferentie, dynamisch naar nieuwe zenders gaan. Omdat de timing en de bestemming van deze overstap onvoorspelbaar is, wordt een beveiligingslaag voor de transmissie toegevoegd.

DYNAMISCHE VERMOGENSREGELING

De Plantronics DECT-producten van de Savi®-serie en CS500-serie maken gebruik van een aangepaste vermogensregeling, door de radiofrequentie van vermogensniveaus te verlagen die zijn vereist voor communicatie wanneer de gebruiker zich dicht bij de basis bevindt. Potentiële cyberaanvallers zouden zich binnen dit bereik moeten bevinden of high-gain richtantennes moeten gebruiken om te kunnen af luisteren, waardoor dergelijk risico wordt beperkt.

VOLDOET AAN SARBANES-OXLEY

Plantronics DECT-apparaten voldoen aan Sarbanes-Oxley (2002) sec. 404. Deze verklaring is gebaseerd op de coderingsmaatregelen, zoals opgenomen in het product met de eisen van het VS-reglement 45 CFR 164.312(a)(2)(iv).

EENVOUDIGE IMPLEMENTATIE EN BEHEER VOOR ONDERNEMINGEN

Naast de headsets van de Savi 400- en Savi 700-serie, die worden geleverd met de nieuwste DECT-functionaliteit, kunnen bestaande Plantronics-headsets worden uitgebreid met een firmware-update. IT-organisaties kunnen dit eenvoudig bereiken met Plantronics Manager Pro, een cloudgebaseerde softwaretoepassing die ongeëvenaard beheer van audio-apparatuur, bewaking, beleidsvoering en gebruikersondersteuning biedt.

Als onderdeel van het softwareportfolio Plantronics Spokes biedt Plantronics Manager Pro IT-managers gebruiksvriendelijke tools voor het configureren van instellingen en het bijwerken van software en firmware voor audioapparaten van eindgebruikers binnen de onderneming. Plantronics Manager Pro is uitgerust met rapportagetools die IT-beheerders helpen hun DECT-omgeving beter te begrijpen en ervoor te zorgen dat alle headsets voldoen.

Belangrijke functies zijn:

- Apparaatinstellingen in- of uitschakelen om aan het bedrijfsbeleid of de voorschriften te voldoen
- Individuele gebruikers op een geschikt tijdstip de gelegenheid geven om de DECT-instellingen te upgraden en de verantwoordelijkheid te vergroten
- Gebruik en instellingen van audioapparaten bijna realtime beheren
- Voorraad- en gebruiksrapporten genereren om het gebruik van bedrijfsmiddelen te controleren
- Voorraad van alle apparaten weergeven, inclusief niet-Plantronics apparaten

Plantronics is de enige aanbieder van managementsoftware voor de versnelde implementatie van DECT-technologie, waardoor gebruikers productief blijven en een conforme headsetconfiguratie wordt behouden. Deze mogelijkheden, samen met 's werelds enige verbeterde DECT-productfuncties, maken Plantronics marktleider op het gebied van beveiligde draadloze communicatie.

Meer informatie vindt u op plantronics.com

¹ Eerdere Savi 400- en Savi 700-modellen kunnen worden bijgewerkt naar de nieuwste DECT-beveiligingsfuncties via een firmware-update.

Niet van toepassing op de CS500-serie.

©2016 Plantronics, Inc. Alle overige handelsmerken zijn het eigendom van hun respectievelijke eigenaren. 5.16