

Draadloze beveiliging

maart 2007

Whitepaper

Beveiliging van de DECT™-headset

De draadloze DECT-producten van Plantronics (CS60™, CS70™ en SupraPlus® Wireless) maken gebruik van digitale technieken en voldoen aan de beveiligingseisen van de DECT-standaard, zoals vermeld in ETSI EN 300 175-7.

Beveiliging is een van de vele sterke punten van een DECT-systeem dat gebruik maakt van TDMA/TDD digitale radiosignalen en dynamische kanaalselectie. Bovendien is het systeem voorzien van een drielaags beveiligingssysteem. Dit drielaagse systeem van gekoppelde verificatie, codering en controle biedt een uitstekende bescherming tegen afluisteren:

1. 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 de fabrikanten van de apparatuur weten wat de werking van dit algoritme is.

2. Codering

De coderingssleutel wordt gebruikt om gegevens te coderen die via de ether worden verzonden.

3. Controle

Beide apparaten controleren of de juiste verificatiecode wordt gebruikt en ontcijferen de coderingssleutels (die wordt gebruikt om de gegevens te coderen die via de ether worden verzonden). De DSC-codering (DECT Standard Cipher) wordt gebruikt; alleen de fabrikanten van de apparatuur weten wat de werking van dit algoritme is.

RF-protocol

Het RF-protocol heeft dynamische kanaaltoewijzing en biedt zelf een bepaald beveiligingsniveau, met kanalen en tijdsintervallen die steeds veranderen, aangezien de omgeving geschikt is voor meer dan tien draagfrequenties en 12 tijdsintervallen per drager (voor beide communicatierichtingen).

Beveiliging van de Bluetooth®-headset

Ondanks de vele persberichten over beveiligingslekken bij Bluetooth-apparaten, zoals telefoons en PDA's, is de audioverbinding tussen een telefoon en een Bluetooth-headset van Plantronics erg veilig. Er wordt namelijk gebruik gemaakt van geavanceerde algoritmen voor codering en controle.

Headsets hoeven slechts korte tijd 'waarneembaar' te zijn (zichtbaar voor andere apparaten), wanneer deze worden geïnstalleerd voor gebruik met een nieuw apparaat (bijvoorbeeld een mobiele telefoon). Tijdens dit proces (ook wel 'afstemmen' genoemd) wisselen de twee apparaten informatie uit om een 'veilige' verbinding tot stand te brengen. Het basisstation van het Plantronics Voyager™ 510-systeem, dat wordt aangesloten op een bureautelefoon, kan nooit worden herkend.

Na het afstemmen, zijn de Plantronics-headsets niet zichtbaar voor andere apparaten en worden alle overdrachten gecodeerd.

Het afstemmen

Voor het afstemmen wordt de volgende informatie uitgewisseld:

1. Het Bluetooth-adres van elk apparaat
2. De pincode die de gebruiker heeft ingevoerd
3. Een unieke tijdstempel die wordt gegenereerd van de mobiele telefoon

Deze items worden gecombineerd om een beveiligingssleutel van 128 bits te genereren, die wordt gebruikt voor mogelijke verbindingen tussen de headset en de telefoon (of het Voyager-basisstation). De tijdstempel kan later erg moeilijk worden geraden, zelfs als het adres en de pincode al bekend zijn bij een potentiële afluisteraar.

Omdat voor alle communicatie tussen Bluetooth-apparaten gebruik wordt gemaakt van een systeem dat radiogolven uitzendt met behulp van de Frequency Hopping Spread-Spectrum-technologie, is de communicatie uiterst moeilijk te onderscheppen.

Veilige gesprekken

De Plantronics-headsets met DECT-technologie gebruiken de coderingssleutel van 128 bits om audiosignalen tussen de headset en de telefoon (of het Voyager-basisstation) digitaal te coderen. Dit lijkt erg op de methode waarbij de GSM-radiosignalen tussen de mobiele telefoon en het basisstation worden gecodeerd.

Veel van de gepubliceerde zwakke plekken van Bluetooth gelden niet voor de headsets, maar u kunt de beveiliging van uw telefoon wel verbeteren. Het belangrijkste is dat u de afstemmodus van de telefoon uitschakelt.

De afstemmodus uitschakelen

Plantronics raadt aan om de verborgen of 'niet-afstemmodus' in te schakelen voor een betere beveiliging, tenzij een gebruiker regelmatig visitekaartjes via Bluetooth uitwisselt. De telefoon hoeft niet in de afstemmodus te staan om te kunnen werken met een Plantronics-headset. De headset staat altijd in de niet-afstemmodus, behalve bij het afstemmen.

Het op deze manier 'verbergen' van uw telefoon vermindert ook het risico op 'Bluesnarfing' (het stelen van contactinformatie van een Bluetooth-telefoon of PDA, NIET van Plantronics headsets. Deze gegevens zijn namelijk niet op de headsets opgeslagen).

Bij juist gebruik zijn Bluetooth-headsets en de telefoons waarop deze zijn afgestemd uiterst moeilijk aan te vallen. Hackers zijn echter heel vindingrijk, wat betekent dat geen enkel apparaat volledig veilig is.

Het lage bereik van Bluetooth (meestal 10 meter) maakt het voor iemand die wil afluisteren echter moeilijker om de veilige verbinding te 'hacken'. Ze zullen zelfs meer succes hebben door gewoon zelf te luisteren naar wat er wordt gezegd.