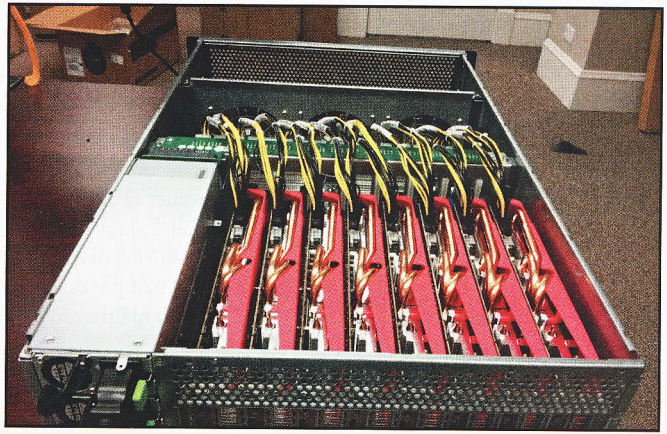
KLUSTER KNÄCKER LÖSENORD PÅ LÖPANDE BAND

En säkerhetsexpert vid namn Jeremi Gosney har visat ett datorkluster som kan gissa 350 miljarder lösenord per sekund. Klustret är uppbyggt av fem servrar och 25 grafikkort. Det bildar ett mycket kraftfullt beräkningskluster med hjälp av mjukvaran Virtual OpenCL. Denna mjukvara använder så kallad GPGPU-teknik som drar nytta av beräkningskraften i grafikprocessorerna.

För att knäcka lösenorden används så kallad offline-teknik, med lösenordslistor som stulits från servrar av hackare. Dessa listor är krypterade med olika metoder och det går generellt inte att matematiskt ta fram det ursprungliga lösenordet med hjälp av det krypterade. För att knäcka lösenorden låter man istället systemet gissa lösenord. När ett nyskapat lösenord matchar ett lösenord i listan vet man också vad det ursprungliga lösenordet var.

Siffran 350 miljarder lösenord per sekund gäller när systemet används mot lösenord krypterade med Microsofts NTLM-algoritm, som använts sedan Windows Server 2003. Detta innebär i praktiken att systemet kan gå igenom samtliga möjliga lösenord på åtta tecken (med små och stora bokstäver, siffror och symboler) på cirka 5,5 timmar. Handlar det istället om den äldre LM-algoritmen tar det inte mer än cirka sex minuter.

Fram till dess att bättre krypteringsrutiner införs gäller det alltså att inte använda för korta lösenord. Rekommendationen är nu minst nio tecken, men gärna fler. Det ska naturligtvis inte heller vara ett ord, namn eller liknande som kan återfinnas i en ordlista.



En del av det GPGPU-kluster som kan gissa 350 miljarder lösenord i sekunden.