Enigma XXI w?

#Przemysł zbrojeniowy #Strategia i polityka 15 stycznia 2009

EADS Defence & Security (EADS DS) ujawniła wczoraj nowy system kryptograficzny, który ma - według producenta - zrewolucjonizować elektroniczny przesył danych. Ściśle tajne informacje będą mogły być przekazywane zwykłymi łączami internetowymi.

Dotychczas wykorzystywane systemy kodowania informacji rządowych i korporacyjnych, nie gwarantują odpowiedniego stopnia tajności. W związku z tym, do przesyłania informacji elektronicznych, wykorzystuje się odrębne od zwykłego Internetu łącza, co jest rozwiązaniem drogim i wymagającym ciągłego monitorowania linii przesyłowych. Co więcej, stopień skomplikowania systemów zabezpieczających, doprowadza do spowolnienia przekazywania danych, na tyle, że praktycznie nie jest możliwe przekazywanie na bieżąco np. obrazów video.

EADS DS ujawnił, że po 5 latach prac w ośrodku Newport South Wales, grupie naukowców i informatyków, udało się stworzyć system niezawodny i stosunkowo prosty, nazwany Ectocryp. Według producenta, pozwala on na wykorzystanie zwykłych łączy internetowych - system wykorzystuje ponad milion linii certyfikowanego kodu, co ma wyeliminować możliwość złamania szyfru. Ponadto, odczytania danych jest bardzo szybkie, co umożliwia przesyłanie dużych plików, także video, w czasie zbliżonym do rzeczywistego.

Przedstawiciele EADS DS twierdzą, że Ectocryp jest XXI-wiecznym odpowiednikiem maszyny szyfrującej Enigma. Wypada w tym miejscu przypomnieć, że nie jest to zbyt dobry przykład. Mechaniczna Enigma - nawet we współczesnej dobie komputerów, dysponujących ogromnymi mocami przeliczeniowymi - stwarza tak olbrzymie możliwości kodowania, że odczytanie utajnionej wiadomości i dzisiaj trwałoby miesiące, a nawet lata. Mimo tego jej kod został stosunkowo szybko złamany, przy fundamentalnym udziale wywiadu II Rzeczypospolitej i naszych matematyków. W istocie, Enigma - która dla Niemców wydawała się absolutnym zabezpieczeniem dla przekazywania informacji - stała się przyczyną wielu ich militarnych niepowodzeń, szczególnie od końca 1942, kiedy brytyjski wywiad był w stanie odczytywać depesze w kilka godzin po ich nadaniu.

Dotychczas wykorzystywane systemy kodowania informacji rządowych i korporacyjnych, nie gwarantują odpowiedniego stopnia tajności. W związku z tym, do przesyłania informacji elektronicznych, wykorzystuje się odrębne od zwykłego Internetu łącza, co jest rozwiązaniem drogim i wymagającym ciągłego monitorowania linii przesyłowych. Co więcej, stopień skomplikowania systemów zabezpieczających,

doprowadza do spowolnienia przekazywania danych, na tyle, że praktycznie nie jest możliwe przekazywanie na bieżąco np. obrazów video.

EADS DS ujawnił, że po 5 latach prac w ośrodku Newport South Wales, grupie naukowców i informatyków, udało się stworzyć system niezawodny i stosunkowo prosty, nazwany Ectocryp. Według producenta, pozwala on na wykorzystanie zwykłych łączy internetowych - system wykorzystuje ponad milion linii certyfikowanego kodu, co ma wyeliminować możliwość złamania szyfru. Ponadto, odczytania danych jest bardzo szybkie, co umożliwia przesyłanie dużych plików, także video, w czasie zbliżonym do rzeczywistego.

Przedstawiciele EADS DS twierdzą, że Ectocryp jest XXI-wiecznym odpowiednikiem maszyny szyfrującej Enigma. Wypada w tym miejscu przypomnieć, że nie jest to zbyt dobry przykład. Mechaniczna Enigma - nawet we współczesnej dobie komputerów, dysponujących ogromnymi mocami przeliczeniowymi - stwarza tak olbrzymie możliwości kodowania, że odczytanie utajnionej wiadomości i dzisiaj trwałoby miesiące, a nawet lata. Mimo tego jej kod został stosunkowo szybko złamany, przy fundamentalnym udziale wywiadu II Rzeczypospolitej i naszych matematyków. W istocie, Enigma - która dla Niemców wydawała się absolutnym zabezpieczeniem dla przekazywania informacji - stała się przyczyną wielu ich militarnych niepowodzeń, szczególnie od końca 1942, kiedy brytyjski wywiad był w stanie odczytywać depesze w kilka godzin po ich nadaniu.
