Nowoczesne koncepcje kryptograficznej ochrony transmisji danych

Wszędzie tam, gdzie istnieje problem komunikacji między rozproszonymi terytorialnie jednostkami organizacyjnymi, najefektywniejszą formą komunikacji między nimi jest wykorzystanie rozległych sieci teleinformatycznych. Budowane są one najczęściej w oparciu o łącza dzierżawione, nad którymi dysponent nie ma kontroli i nie jest w stanie zapewnić ich bezpieczeństwa w zakresie poufności i integralności przesyłanych informacji. Nawet w pełni własna, rozległa infrastruktura sieciowa nie gwarantuje bezpieczeństwa transmitowanych danych. Problem narasta, gdy między jednostkami zachodzi potrzeba przesyłania informacji niejawnych.

Polskie prawo wymaga, żeby sieci (systemy teleinformatyczne), w których przetwarzane są informacje niejawne, posiadały akredytacje Agencji Bezpieczeństwa Wewnętrznego lub Służby Kontrwywiadu Wojskowego. Akredytacja jest możliwa tylko dla systemów, w których zastosowane zostały właściwe mechanizmy bezpieczeństwa, m.in. kryptograficzne zabezpieczenie danych poprzez zastosowanie urządzeń kryptograficznych (szyfratorów), posiadających certyfikat ochrony kryptograficznej ABW lub SKW.

Urządzenia kryptograficzne I oraz II generacji

Wśród istniejących rozwiązań kryptograficznych najpopularniejsze są te, realizujące szyfrowanie informacji lokalnie (typu *off-line*). W dobie upowszechnienia Internetu i rozwoju innych sieci rozległych, nieodzowne stały się systemy szyfrowania współpracujące z publiczną siecią transmisji danych (*on-line*). Kryptograficzną ochronę informacji niejawnych w sieci teleinformatycznej najlepiej realizują szyfratory zapewniające ochronę przesyłanych danych w czasie rzeczywistym. Mogą to być np. scramblery, szyfratory liniowe lub szyfratory protokołu IP. Szyfratory wyższych warstw sieci budowane są w oparciu o popularne architektury mikroprocesorowe, typu komputery PC z ogólnodostępnymi systemami operacyjnymi. Jednak tego typu rozwiązania nie mogą zapewnić właściwego poziomu bezpieczeństwa, z przyczyn *grzechu pierworodnego*, jakim jest ich jawna i ogólnie dostępna architektura. Jak pokazuje praktyka ostatnich 10 lat, są one podatne na wiele typów ataków. Zastosowanie gotowych komponentów mikroprocesorowych (karty interfejsowe: Ethernet, USB, FireWire; płyt głównych itp.) wprowadza ponadto zagrożenie braku rzeczywistej kontroli nad możliwością nieautoryzowanych kontaktów ze światem zewnętrznym, na przykład poprzez niekontrolowane aktualizacje firmware'u.

Nowoczesne koncepcje kryptograficzne – urządzenia III generacji

Dzięki szybkiemu rozwojowi układów programowalnych FPGA w ostatniej dekadzie, stała się możliwa fizyczna realizacja teoretycznego, doskonale bezpiecznego modelu sprzętowej platformy kryptograficznej. W dużym skrócie, bezpieczeństwo platform III generacji zapewnione jest na dwóch poziomach. Po pierwsze, całe oprogramowanie jest ściśle dedykowane zadaniu szyfrowania transmisji danych, a po drugie, platforma sprzętowa jest zbudowana wyłącznie do realizacji funkcji szyfratora. Oznacza to, że w szyfratorach III generacji nie może się znaleźć *obce* oprogramowanie o nieznanej funkcjonalności, a platforma sprzętowa realizuje wyłącznie zadania zdefiniowane przez producenta. Główną zaletą, poza niepenetrowalnością architektury przy użyciu zaawansowanych technik hackerskich, jest możliwość osadzania własnego algorytmu kryptograficznego przez instytucje uprawnione do definiowania polityki kryptograficznej państwa. Rozwiązania w całości oparte na dedykowanej platformie w technologii FPGA są w stanie zapewnić przepustowość rzędu kilkunastu, a w przyszłości również kilkudziesięciu Gb/s.

System KRYPTON K2

Aktualnie, jedynymi urządzeniami III generacji spełniającym wymagania nowej polityki kryptograficznej ABW z sierpnia 2011, są urządzenia systemu KRYPTON K2. Jest to kompleksowe rozwiązanie umożliwiające ochronę informacji niejawnych o klauzuli *Poufne*. Jego elementami są: szyfratory IP KRYPTON K2, Bezpieczny Moduł Sprzętowy KRYPTON HSM2, aplikacja zarządzająca KRYPTON AZ oraz centrum certyfikacji KRYPTON CA. Wszystkie wymienione komponenty systemu przeszły złożony proces badań w ABW, a urządzenia uzyskały *certyfikaty ochrony kryptograficznej Typu*, ważne do 2018.

Głównym elementem systemu, realizującym funkcje poufności i integralności przesyłanych danych jest szyfrator IP KRYPTON K2. Posiada on imponujące parametry zarówno w zakresie bezpieczeństwa, jak również funkcjonalności. KRYPTON K2 zapewnia szyfrowanie przesyłanych danych na poziomie 1 Gb/s. Umożliwia zestawienie jednocześnie do 1024 tuneli IPSec,

Szyfrator IP KRYPTON K2

co odpowiada możliwość połączenia 1024 lokalizacji (przy zastosowaniu architektury połączenia *każdy z każdym*). Każdy tunel IPSec zestawiany jest w czasie poniżej 1 sekundy. Dodatkowo, wartym podkreślenia jest fakt, że szyfrator nie wprowadza w sieci opóźnień, co jest bardzo istotne w przypadku zestawiania wideokonferencji lub połączeń telefonicznych z wykorzystaniem protokołu VoIP. Szyfrator jest całkowicie *przeźroczysty* dla usług działających powyżej warstwy 3 w modelu ISO/OSI.

Obsługa każdej sieci, a w szczególności sieci szyfratorów służących ochronie informacji niejawnych wymaga sprawnego zarządzania. I tu z pomocą przychodzi aplikacja zarządzająca KRYPTON AZ, która z centralnego miejsca w sieci (tzw. centrum zarządzania) umożliwia m.in. monitorowanie wszystkich szyfratorów, ich zdalną konfiguracje oraz zdalny odczyt rejestrów zdarzeń. Dotychczasowi użytkownicy systemu KRYPTON K2 podkreślają łatwą i intuicyjną obsługę aplikacji KRYPTON AZ.

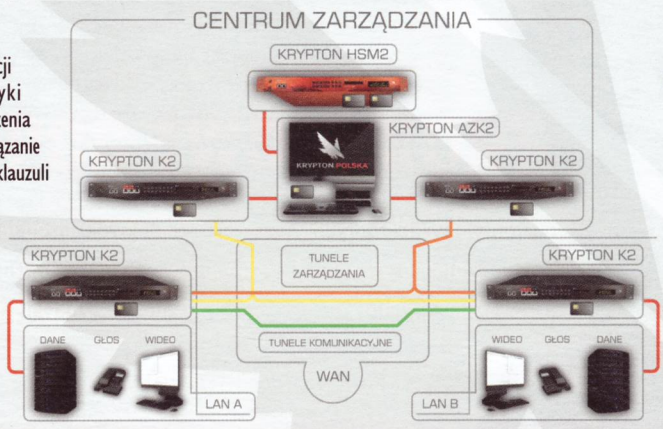
Bezpieczny Moduł Sprzętowy KRYPTON HSM2

Dodatkowy poziom bezpieczeństwa w systemie KRYPTON K2 wprowadza Bezpieczny Moduł Sprzętowy KRYPTON HSM2, wraz z centrum certyfikacji KRYPTON CA. Komponenty te, poprzez infrastrukturę PKI, zapewniają silne uwierzytelnienie wszystkich elementów systemu. Dostosowana dla systemu KRYPTON K2 infrastruktura PKI nie wprowadza, jak inne systemy, uciążliwości związanych z zarzadzaniem certyfikatami i wszelkimi innymi operacjami narzucanymi przez PKI.

To dopiero początek...

Na koniec należy podkreślić, że powyższe nowoczesne urządzenia zostały w całości opracowane przez polską firmę. Ambitny cel, jaki postawili sobie na starcie Właściciele spółki oraz jej kierownictwo – zbudowania polskiego rozwiązania kryptograficznego – został spełniony. Wykorzystanie najnowszych technologii, układów FPGA, sprzętowej implementacji logiki urządzeń i kryptografii, umożliwiło uzyskanie przez Szyfrator IP KRYPTON K2 i Bezpieczny Moduł Sprzętowy KRYPTON HSM2 wysokiej wydajności oraz ponadstandardowych parametrów bezpieczeństwa. Rozwiązania te są innowacyjne nie tylko w skali kraju, ale również świata, co zauważane było przez licznych gości na wystawach i targach w kraju i za granicą, a także przez obecnych Użytkowników.

Przed Krypton Polska stoją nowe wyzwania. Trwają prace nad kolejnymi projektami, które poszerzą ofertę firmy o urządzenia do ochrony IN o klauzuli *zastrzeżone* (KRYPTON K1) i *tajne* (KRYPTON K3) oraz dedykowane na rynek wojskowy.



Przykładowa infrastruktura systemu KRYPTON K2

KRYPTON POLSKA

Michał Czmoch
Dyrektor Generalny
Krypton Polska