Az IPv6 protokoll bevezetésével kapcsolatban gyakran felmerül a kérdés, milyen újítást hoz az új protokoll az informatikai biztonság területén. Korábban ezt a kérdést gyorsan letudták azzal, hogy az IPv6-ban kötelező az IPSec, így a protokoll sokkal biztonságosabb. A helyzet azonban ennél sokkal bonyolultabb. Az IPSec korántsem annyira univerzális, és széleskörben használt, mint az korábban cél volt. A két protokoll közötti különbségek sokkal rejtettebbek.

Az előadás elemzi az IPv6 és az IPv4 közötti különbségeket biztonsági szempontból. Az IPv6 újdonságait: a címzési architektúrát, az autokonfigurációt, a megváltozott csomagszerkezetet, és más további tulajdonságokat a kockázatelemzés módszerét felhasználva összehasonlítja az IPv4-ben alkalmazott megoldásokkal. Bemutatja a jellemző eltéréseket, és azokat a pontokat, amelyek alapján biztonsági szempontból különbség észlelhető a két protokoll között. Ilyenek például a címtér nagysága, amely a felderítés egyszerűségét befolyásolja, vagy az autokonfiguráció és a Szomszédfelmérési protokoll, amelyek különböző támadási felületet nyújtanak.

Nem jelenthető ki, hogy egy bizonyos tulajdonság vagy újdonság miatt az IPv6 egyértelműen biztonságosabb, mint az IPv4, de külön-külön vizsgálva megállapítás tehető a protokoll egészére. Figyelembe véve az implementációk állapotát is, várható, hogy hosszútávon az IPv6 biztonságosabbnak tekinthető az IPv4-hez képest.