DDOS támadások és azok veszélye az ipari kommunikációra

Dr. Gyányi Sándor
Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar

A számítógépes hálózatok elterjedésével és népszerűvé válásával megjelent az igény, hogy kiváltsuk vele az egyéb célokra létrehozott hálózatokat – például a telefon, a kábeltévé szolgáltatásokat. A helyi hálózatok mellett a nagyobb távolságú kommunikáció megvalósítására a publikus IP [1] hálózat, az internet használata vált általánossá, amely az üzemeltetési költségeket drasztikusan csökkentette. A csomagkapcsolt, kapcsolatmentes IP használata gazdaságos átviteli csatornát biztosít az adatátvitel számára, emiatt napjainkban a gyártók igyekeznek mindenbe integrálni a megfelelő hálózati csatolókat. A háztartási eszközök mellett az iparban használt különböző szenzorok és adatgyűjtő eszközök is képessé tehetők internetes kommunikációra, azonban a publikus hálózat alkalmazása veszélyforrásokat hordoz magában. A triviális biztonsági problémák – illetéktelen hozzáférés, adatmódosítás – mellett egyre jobban terjed az eszközök működését lassító vagy akár lehetetlenné tevő támadási forma, az elosztott túlterheléses támadási módszer, vagy angol nevén, a Distributed Denial of Service (DDoS) [2]. Az ilyen támadások során a támadó egyszerre nagy mennyiségű támadó végpontot használva generál akkora mértékű adatforgalmat, ami a célpontok normál, üzemszerű működését megnehezíti vagy működésképtelenné teszi. A különböző, intelligens IoT – Internet of Things – eszközök fenyegetettsége kettős: célpontok is lehetnek, vagy egyéb támadási módokkal kombinálva akár az elkövetés eszközei is.
Az előadás áttekinti a gyakoribb DDoS támadási módszereket, bemutat néhány nagyobb léptékű támadást.

Hivatkozások
[1] RFC 791 Internet Protocol, https://www.rfc-editor.org/rfc/rfc791
[2] What is a DDoS attack? https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/