

Network Security Monitoring of Smart Home Systems

Mgr. Radek Krejčí

Abstract

With growing number of security threats we gradually take network security questions seriously into account. The main focus of nowadays security methods and tools is to protect desktop and servers and usually large high-speed networks. Home networks stay underestimated in a security perspective. Considering a concept of smart homes and intelligent buildings that are incoming trend of a modern living, the area of the security of Small Office/Home Office (SOHO) networks and interconnected building automation systems with sensor networks increases its importance.

We propose to use network monitoring and behavior analysis as tools to understand what is happening inside the network. The intents of my Ph.D. thesis are to adapt current network security monitoring methods for the specific needs of the SOHO networks and interconnected building automation and sensor networks. These methods are currently used for security monitoring of large-scale network. The research will further include fingerprinting of benign and malicious behavior of various network devices or the detection of unexpected and potentially dangerous devices inside the network.

We can use with advantage experiences and knowledge of high-speed networks security monitoring acquired during the Liberouter research project. Mainly FlowMon, a flow monitoring probe developed as part of the Liberouter research activity, can serve as a base for the development of network behavior monitoring tools and methods for SOHO and building automation system networks.

Abstrakt

S rostoucím počtem bezpečnostních hrozeb již začínáme brát otázky síťové bezpečnosti vážněji. Hlavní oblastí dnešních metod a nástrojů pro zajištění síťové bezpečnosti je na jedné straně ochrana serverů a pracovních stanic uživatelů a na druhé straně bezpečnost zejména rozsáhlých sítí poskytovatelů připojení k Internetu. Oblast domácích sítí je z bezpečnostního hlediska podceňována. Právě oblast domácích sítí, sítí automatizačních systémů a senzorových sítí, však ve spojení s nastupujícím trendem chytrých domácností a inteligentních budov, nabývá na důležitosti.

Plánujeme využít metody a nástroje pro monitorování sítě a analýzu chování síťového provozu, které poskytují náhled na to, co se uvnitř sítě skutečně děje. Záměrem disertační práce je upravit v současnosti používané nástroje a metody monitorování sítí pro potřeby a omezující požadavky domácích sítí a sítí automatizačních systémů včetně senzorových sítí. Tyto metody se v současnosti využívají zejména v rozsáhlých sítích. Výzkum bude dále zahrnovat identifikaci a vytváření profilů běžného a škodlivého chování síťových zařízení anebo detekci neznámých a potenciálně nebezpečných zařízení v síti.

V disertační práci lze s výhodou využít zkušenosti a znalosti z oblasti bezpečnostního monitorování vysokorychlostních sítí nabyté během řešení projektu Liberouter. Zejména jeho část FlowMon, sonda pro monitorování síťových toků, může sloužit jako základ při vývoji nástrojů monitorujících chování sítí v rámci systémů inteligentních budov.