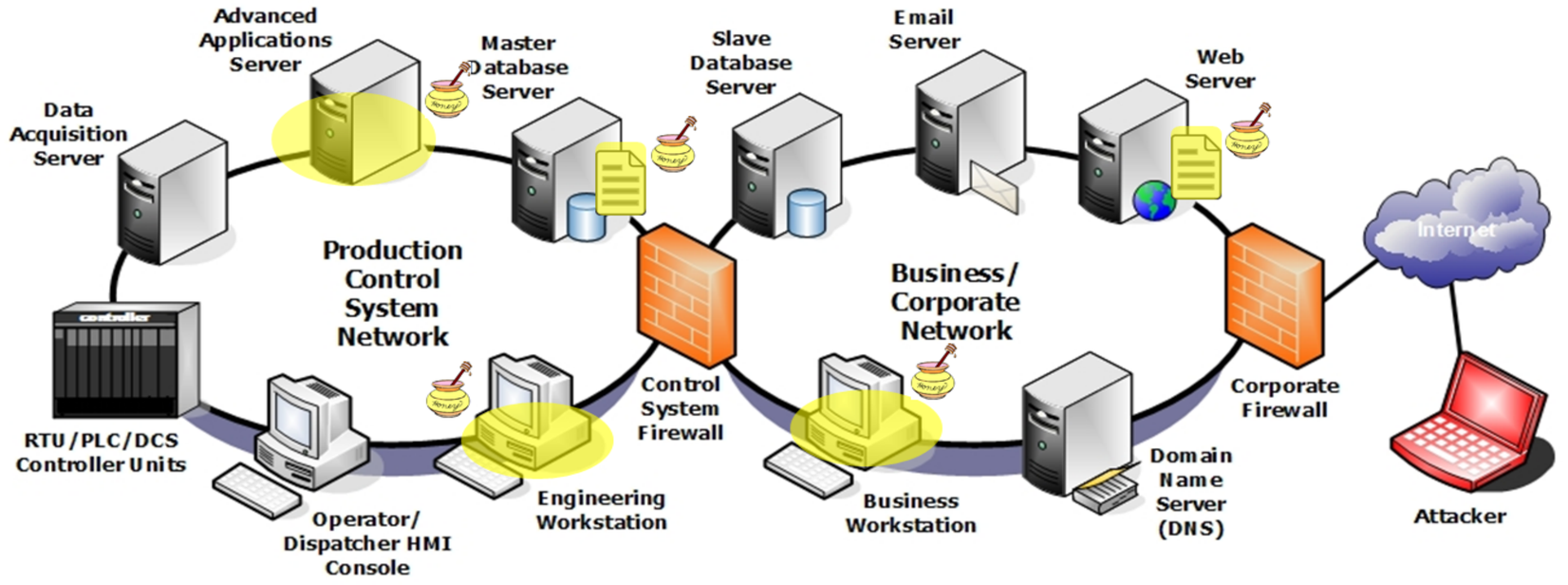
Protecting Critical Infrastructures against Targeted Attacks
Kritikus infrastruktúrák védelme célzott támadások ellen

The goal of the project is to develop a security framework that allows for the detection of targeted cyber attacks against critical infrastructures, and that supports the recovery from such attacks, incident handling, as well as forensic analysis aiming at determining the root causes and the impact of the incident.

A projekt célja egy olyan biztonsági keretrendszer kifejlesztése, mely alkalmas kritikus infrastruktúrák ellen intézett célzott informatikai támadások detektálására, valamint a támadásokból származó incidenskezelés és az azt követő forensic analízis támogatására.



The targeted attacks that have occured in recent years (e.g., Stuxnet, Duqu, Flame, etc.) clearly show that the protection of our critical infrastructures against cyber threats is not sufficiently effective. The framework to be developed in the project aims at filling this gap. It will be based on honeypot technology, it will use static and dynamic malware analysis tools, and it will support threat information sharing. The originality of the project lies in the novel ways in which we combine known security mechanisms and tools into a common framework, also taking into account the constraints of critical infrastructures.

Az utóbbi években feltárt célzott támadások (Stuxnet, Duqu, Flame, stb.) egyértelműen bizonyítják, hogy kritikus infrastruktúráink informatikai védelme nem hatékony. A kifejlesztendő biztonsági keretrendszer ezt a hiányt igyekszik pótolni. A keretrendszer honeypot technológiára, statikus és dinamikus program-analízis eszközök alkalmazására, valamint anonimizált incidens információ megosztásra épül. A projekt újdonságtartalma abban áll, hogy ismert biztonsági technológiákat és mechanizmusokat kombinálunk újszerű módon figyelembe véve a kritikus infrastruktúrák sajátosságait.

Project leader:
Dr. Levente Buttyán, CrySyS Lab, Budapest

A projekt témavezetője:
Dr. Buttyán Levente, CrySyS Lab, BME

During 2011 and 2012, the CrySyS Lab participated in the analysis of several targeted malware, and obtained a unique know-how in the field. In September 2011, the CrySyS Lab discovered and named Duqu, a previously unknown malware, and performed its detailed technical analysis, which resulted in the conclusion that Duqu has striking similarities to the infamous Stuxnet worm. Later, the CrySyS Lab discovered the dropper of Duqu, an MS Word document, with a 0-day Windows kernel exploit in it. In May 2012, the CrySyS Lab participated in the analysis of another targeted malware, which became known as Flame.

A CrySyS Lab 2011 és 2012 folyamán részt vett több célzott támadást megvalósító malware analízisében, és ennek kapcsán jelentős és unikális know-how-ra tett szert. 2011 szeptemberében a CrySyS Lab fedezte fel a Duqu trójait, valamint elvégezte a Duqu részletes analízisét, mely során kiderült, hogy az nagy mértékben hasonlít a Stuxnet nevű hírhedt féreghez. Később a CrySyS Lab találta meg a Duqu dropper komponensét, egy MS Word fájlt, és megmutatta, hogy az egy 0-day kernel szintű exploit-ot tartalmaz. 2012 tavaszán a csoport részt vett egy másik célzott malware, a Flame elemzésében, és publikálta a Flame részletes technikai analízisét.

A projekt a Magyar Kormány támogatásával, a Nemzeti Fejlesztési Ügynökség kezelésében, a Kutatási és Technológiai Innovációs Alap finanszírozásával valósul meg.

Az EITKIC_12-1-2012-0001 számú projekt a Magyar Kormány támogatásával, a Nemzeti Fejlesztési Ügynökség kezelésében, a Kutatási és Technológiai Innovációs Alap finanszírozásával valósul meg.
The EITKIC_12-1-2012-0001 project is supported by the Hungarian Government, managed by the National Development Agency, and financed by the Research and Technology Innovation Fund