ITEA 3

Project Results

ADAX

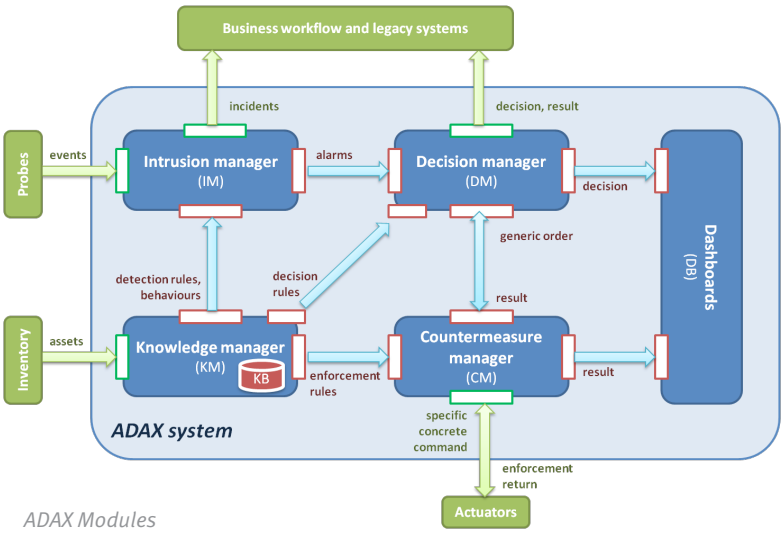
Protecting information systems from complex attacks

Executive summary

Cybersecurity is vital to any person or entity, from consumer to government, involved in conveying information. The key lies in being able to detect attacks and react quickly and efficiently by launching appropriate countermeasures. The ITEA 2 project ADAX has delivered a set of key innovations improving prevention, detection, decision support, countermeasure enforcement and knowledge management to support security operation on complex and critical IT infrastructures.

Project origins

Software-intensive systems can be regarded as targets, assets or threats from a cybersecurity perspective: they are targets for cyberattacks but assets for cyberdefence purposes. While a number of commercial off-the-shelf cyberdefence tools exist, there is a clear need in today's market for detection to be extended with reaction capabilities and support mechanisms to enable security operators to make informed decisions in a dynamic situation. ADAX rose to this challenge by first considering the question: Considering a given attack, can we assess the cost/benefit of each and every possible countermeasure?



ADAX Modules

Technology applied

An interesting innovation in the ADAX project is a hybrid detection technique in which behaviour-based and signature-based detection are combined. The former is a probabilistic approach that helps to identify new attacks (0-day attacks) while the latter is a deterministic approach that is largely applied to known attacks. Combining both techniques helps improve detection rate (true positive), lower false-alarm rate (false positive) and shorten the detection time, saving time and costs for both customers and security service providers in the detection phase. The aim was to improve the detection of new complex attacks and accelerate the detection-to-remediation loop through the development of enhanced decision-support tools with the development of a network simulation tool to enable attack and countermeasure impact to be assessed before implementation on a real IT infrastructure. A new metric, 'Return-On-Response-Investment' (RORI), was set up to calculate the 'cost-benefit' of the different countermeasures that can be implemented to remediate to a particular attack. A reduction in incident resolution time from 3 hours to 90 minutes was achieved. A complete ADAX advanced simulation environment, consisting of different interacting modules supplied by different partners, was delivered and demonstrated in a real environment at YAPI KEDI BANK's office in Gebze, Turkey. The system performed the full detection to remediation cycle in two scenarios: the first involving an APT (Advanced Persistent Threat), the second involving a DDoS (Distributed Denial of Service).

Making the difference

In the ADAX project, four clear markets were identified (UTM, IDS, SIEM, MSSP) along with the markets related to protection against DDoS and APT threats. The main use case was banking, a sector that is targeted by (and vulnerable to) many cyberattacks and it is a sector where decision-makers have a rigorous need to assess impacts before instigating

countermeasures. With interest in cybersecurity protection in Europe growing, the urgency to be prepared with effective defence is starting to take root and regulatory changes regarding infrastructure protection may create a major opportunity to exploit the results of ADAX. European players will undoubtedly benefit, including the ADAX consortium. ADAX is also distinctive in its focus on decision-support and remediation, which are poorly addressed by state-of-the-art systems.

Several developments deriving from the project point to successful exploitation. The RORI metric calculation and the attack and countermeasure volume assessment method have been patented by IMT and is likely to be brought on the market through as a spin-off creation. 6CURE was awarded a contract involving the DDoS mitigation and automatic reaction module resulting from ADAX by a French Internet Service Provider. NETASQ has included ADAX IPS functionality in its new STORMSHIELD NETWORK UTM, reaching more than 10,000 units deployed while P1M1 has been awarded a contract by a major Turkish telecom industry for the detection of VoIP intrusion and another one by a worldwide banking group for the detection of cash transaction anomalies. MasterCard now uses the MAMAT tool, developed within ADAX by its subsidiary PROVUS, to model ATM management systems (PAYS) to analyse and strengthen security. Airbus DS Cybersecurity is in the process of integrating ADAX decision support functionalities in its new version of Cymerius® tool, used for remote security monitoring of many active customers. Finally, licence contracts are under negotiation with the French Army and the Lebanese Ministry of Interior.

Major project outcomes

Dissemination

- 30 publications and 7 theses
- 8 external events & 2 ADAX events (AIDP 2014&2015)

Exploitation (so far)

- 6 new solutions / upgrades:
  - Intrusion prevention mechanism developed by NETASQ, embedded in the new Stormshield Network security appliance, providing mixed-signature detection capability with lower false alarm rate
  - Intrusion detection system marketed by P1M1 providing hybrid detection capability with improved detection rate regarding new attacks
  - Decision support tool developed by IMT, providing RORI and attack volume mechanism to assess the impact of attacks and select the most relevant countermeasures to improve quality and cost of the remediation
  - Decision engine developed by CCS, providing optimised response plan and an automatic UTM reconfiguration mechanism to shorten decision and remediation time
  - Countermeasure enforcement tool developed by 6CURE, providing automated construction, deployment, accounting and deployment of countermeasures to shorten remediation time
  - Model acquisition and maintenance tool developed by PROVUS, providing automated large scale information network modelling capability, saving time for experts in network topology activities
- 5 customer contracts directly linked with project results:
  1 Luxembourgish security service provider, 1 Lebanese Ministry of Homeland Security, 1 Turkish banking corporation, 1 Turkish telecom industry and 1 French telecom operator

Standardisation

- 1 use of AADL standard format in the model acquisition and maintenance tool
- 1 contribution in GS ISI 001-1 standard [6] from ETSI that provides a full set of information security indicators
- 1 contribution in the Payment Card Industry Data Security Standard (PCI DSS)

Patents

- 1 patents approved on Risk on Return Investment (RORI) and attack volume mechanisms
- 1 patent application submitted on an improved version of the above

Spin-offs

- 1 spin-off project to market the RORI engine

ITEA is the EUREKA Cluster programme supporting innovative, industry-driven, pre-competitive R&D projects in the area of Software-intensive Systems & Services (SiSS). ITEA stimulates projects in an open community of large industry, SMEs, universities, research institutes and user organisations. As ITEA is a EUREKA Cluster, the community is founded in Europe based on the EUREKA principles and is open to participants worldwide.

https://itea3.org

ADAX

10030

Partners

France

6cure

Cassidian Cybersecurity

Institut Mines-Télécom

NETASQ

Turkey

Bogazici University

PlusOneMinusOne

Provus A.S.

Yapı ve Kredi Bankası Yapi Kredi Bank

Project start

January 2013

Project end

Aprill 2015

Project leader

Adrien Philippe Bécue,

Cassidian Cybersecurity

Project email

adrien.becue@airbus.com

Project website

http://adax.boun.edu.tr