......

.....

ITEA Success Story

From technical leadership to business excellence in cybersecurity

The ADAX project started in early 2013, aiming at developing advanced capabilities for cyber-Attack Detection And Countermeasures Simulation. The consortium was comprised of 8 partners from France and Turkey including 2 large enterprise, 4 SMEs, 2 academics. Airbus DS Cybersecurity (Cassidian CyberSecurity SAS) acted as Project Coordinator while Yapi Kredi Bank acted as pilot end user. The project duration was 30 months for a total effort of 86 person-years.

A key success factor for this project has been the continuous assessment of the innovativeness of our developments versus the state of the art. Cybersecurity being a very fast evolving discipline, we had to keep an eye on both the evolution of threats and the market solutions landscape to make sure the technology outputs from ADAX would make the difference. For example, we started the project with a set of developments targeting improved detection of DDoS attacks (Distributed Denial of Service) because at this stage, the banking sector was still under shock of the large DDoS on global payment system, which occurred in 2010. This massive attack carried out by the "Anonymous hacktivists group" had caused major disruptions of services to powerful transaction and banking champions like VISA, MASTERCARD or PAYPAL. So we reassessed the market and found out that there was a lack of available solutions for incident response to emerging APTs (Advanced Persistent Threat). An APT named "Pitty Tiger" was discovered by Airbus DS Cybersecurity on the IT network of a monitored customer, using a spear phishing e-mail, a corrupted word document and several RATs (Remote Access Tools) in order to disclose company-confidential information. Consequently, we focused our second batch of experiments on response to APT threats. This continuous adaptation to changing conditions of the attacker-defender game helped us stay nearest to the end-user needs and capture key customer contracts throughout the project execution thanks to a fast integration of ADAX developments into the portfolio.



Another success factor was the effective involvement of Yapi Kredi Bank as an onboard end user, pilot owner and specification authority. This kept us away from the very dreadful temptation to do engineering for engineers. It also drove us in a direction that was slightly different from our first intuition. As security operators, we have been from the start very focused on the objective to shorten time to response, and this would mean the sum of detection, investigation, decision and remediation time. From a banking perspective however, the challenge appeared to be rather on optimising response to the lower cost. This would mean that not only the cost of damages caused by the attack, but also the cost of countermeasures should be assessed for rational decision making. Putting those two objectives in balance, we found out that the most demanding process in both time and cost was decision making. Hence we have put significant efforts in developing an advanced decision support tool, proposing optimised response plans to security operators and quantified metrics for business owners to make appropriate decisions. A mechanism to assess the impact of attacks and countermeasures on multiple criteria (Attack Volume Mechanism) and to quantify the Return On Risk Investment (RORI) was developed and patented by Institut Mines-Télécom. Attack generation and countermeasure simulation engines were developed by Airbus DS Cybersecurity to perform the calculation of optimised response plans and a dedicated

module was added to Cymerius® security supervision software for exploitation by security operators.

Last but not least, the project was driven by a multidisciplinary team of excellent mindset, with a balanced care for scientific, technical, economic, contractual, social and business aspects. Academic partners (IMT & Bogazici University) have fostered intensive research activities, leading to the production of no less than 30 articles, 7 theses, 2 patents and 2 conference events. SMEs have delivered key innovations which are being largely adopted by the market like a hybrid attack detection system for which P1M1 was awarded contracts with 2 major telecom and transaction companies, a mixed-signature based intrusion prevention system, which has been deployed by Stormshield on more than 10 000 appliances, a dynamic knowledge and model acquisition tool, which was sold by Provus to a world leader in payment systems, a remote countermeasure enforcement tool, which has been operated by 6Cure to protect a European champion in telecom services. Airbus DS Cybersecurity has integrated all ADAX developments into its commercial version of Cymerius® security supervision tool, sold to 5 customers from financial, military, retail, space and oil & gas sectors, providing a unique advantage to their security operators by simulation-supported incident response. Yapi Kredi Bank has implemented the full ADAX system on its IT

network in Gebze (Turkey), supporting 5000 users. A total of 12 customer contracts have been reported directly linked with the project results, addressing diverse vertical markets like finance, military, retail, space or oil & gas. Further developments include the exploitation of ADAX results for a new product to be marketed by Airbus DS Cybersecurity, supporting financial quantification of cyber-exposure for risk managers. A marketing announcement will be issued by the end of 2016.

All the above choices that have led this project to a success would not have been fruitful without the effective mentoring, steering and support from ITEA. Getting back to the words of Rudolf Haggenmüller: "innovation, business impact, fast exploitation, seizing the high ground and happiness"; I'd like to say that is a quite unique formula in the research & technology community, and a probable reason for ADAX's success. Beyond the scientific and technical excellence, beyond the project management quality, beyond the business relevance, happiness has been a key driver to success of ADAX project, and I'd like to thank ITEA as well as our partners from Bogazici University, Yapi Keredi Bank, Provus, P1M1, Institut Mines Telecom, Stormshield & 6Cure for that.

More information:

Adrien Bécue adrien.becue@airbus.com