Major Security Challenges of the Finance Sector & FINSEC Solutions

H2020 FINSEC Project White Paper

November 2020

Authors:

Kyriakos Satlas, INNOV-ACTS LIMITED

Dimitris Drakoulis, INNOV-ACTS LIMITED

Ariana Polyviou, INNOV-ACTS LIMITED

Acknowledgements

The presented solutions have been developed by the H2020 FINSEC Consortium Partners.

This project has received funding from the European Union's Horizon 2020 research and innovation programme 2014-2020 under grant agreement No 786727

1. Security Challenges of the Finance Sector: Lessons Learnt from Recent Security Incidents

Overview

Recent security incidents against banks and financial institutions provide useful insights and lessons on the security gaps and vulnerabilities that should be addressed by emerging security solutions like the ones developed in the scope of the H2020 FINSEC project. Following paragraphs review some recent incidents and outline relevant lessons learnt. In this way, the present white paper serves as a more general-purpose guide for security officers in banks and financial institutions. Moreover, later sections present how FINSEC solutions alleviate some of the root causes of the presented security incidents. The authors would like to underline that the list of incidents is not exhaustive and IT security is a dynamic field. IT security experts should remain vigilant and continuously monitor for new threats, techniques, tactics and procedures.

Bangladesh Bank cyber heist - Lessons Learnt

In 2016 the Bangladesh Central Bank become the victim of one of the biggest cyber heists in history. Fraudsters intruded the SWIFT network of the bank and initiated a US $1 billion transfer to Federal reserve bank of New York out of which $850 million were blocked. Five of the thirty-five fraudulent instructions were successful in transferring $101 million, with $20 million traced to Sri Lanka and $81 million to the Philippines. The attack had its roots in the manipulation of the SWIFT Alliance Access software. It happened sometime between February 4–5, 2016 when Bangladesh Bank's offices were closed.

Lessons Learnt: One of the main lessons learnt from this attack was that SWIFT transactions should be conducted only on computers that are isolated from the rest of the network. Since 2016, banks are using dedicated computers for SWIFT transactions. This is a wider strategy already employed by other firms in the finance sector that are involved in payment networks. Another lesson was that special security measures should be employed for every computing system that accesses the SWIFT computing system. In the case of Bangladesh Bank the malware attack is likely to have been initiated by an insider that was able to override locally installed security software. Other important observations are the need to have certain monitoring mechanisms in place. Monitoring for transactions with suspicious characteristics like significantly high amounts or irregular timing (off-hours or at a bank holiday) are quick steps to protect against malicious actions. Note that in the scope of our earlier White Paper for the FINSEC Reference Architecture[1], scenarios for protecting banks from insider attacks have been presented.

Dridex take down operation and revival - Lessons Learnt

Dridex is a banking malware that has been seen most active between late 2015 and early 2016. At Oct 2015 UK's National Crime Agency (NCA) in cooperation with Federal Bureau of Investigation (FBI) and Europol coordinated a take-down activity by 'sinkholing' infected computers' traffic. According to Europol, before this operation there a £20M of estimated losses in the UK alone took place. The cybercriminals were believed to be based in Eastern Europe and target end users via documents

[1] https://finsecurity.eu/digital-finance-academy-for-security/finsec-ra-whitepaper/

delivered by e-mail addresses that seem legitimate. Despite its declined activity, Dridex malware continues to evolve and remains a serious threat to end users of financial services.

Lessons Learnt: Follow-up attempts to launch Dridex related attacks have taken place based on the establishment of botnets that were used to inject the malware and attack financial institutions. Such attempts have been repelled based on the unprecedented level of collaboration among financial services firms around the world, as well as based on their sharing of information with security experts and law enforcement agencies. The establishment of communities of trust between information security experts that can facilitate prompt exchange of malicious indicators can be proven key contributor to immediate threat prevention. The use of automated procedures based on established data models can further accelerate the effective response. The involvement of law enforcement agencies in the loop can enable the disruption of cybercrime teams, even in cases where they operate from new countries without an established cybercrime profile. The FINSEC project has developed a solution for automated and trusted exchange of security data across financial institutions. Hence, to some extent, FINSEC is contributing to alleviating attacks like Dribex based on effective stakeholders' collaboration.

Attack against the Bank of Valletta

In February 2019 various news outlets wrote about the hack of Bank of Valletta (BOV), one of Malta's biggest banks. Reportedly, the hack took place on February 13, 2019. Using malware planted on the bank's internal servers, hackers transferred €13 million ($14.7 million) from the bank's internal systems to accounts in the UK, the US, the Czech Republic, and Hong Kong. According to security analysts, the EmpireMonkey cybercrime group is believed to be behind this attack. A number of accounts were used to receive those funds, one of them was in the UK and was held in Belfast. Around £800,000 was transferred. From a technical perspective, attackers used macros to manipulate wscript.exe to achieve their target.

Lessons Learnt: This attack shares some common characteristics with the above-listed $81M cyber heist at Bangladesh Bank in 2015. Specifically, it was a case where business processes were compromised, by finding security gaps in money transfer systems. The latter backdoors were then exploited to initiate and conclude unauthorized transfers. Hence, similar considerations and lessons learnt regarding the security and isolation of payment systems can behighlighted. Financial organizations should have a holistic approach and assess the criticality of their IT infrastructure as a whole and not at an ad hoc basis. Following a criticality assessment, the organization should take proper measures to segment and isolate critical systems like those engaged in financial transactions. Nevertheless, this more recent attack also revealed the limitations of current risk assessment approaches, which are in several cases fragmented and oriented to single systems rather than taking a more complete approach. Specifically, it is nowadays suggested that risk assessment evolves to take into account the vulnerabilities of multiple assets (e.g., all possible end-points), including their interdependencies and cascading effects of possible attacks. Furthermore, the importance of being proactive can be underlined. FINSEC is taking a step in this direction based on the use of predictive analytics for implementing early warnings and a predictive security concept.

ECB bring down reporting dictionary

The European Central Bank (ECB) discovered that the Bank's Integrated Reporting Dictionary (BIRD) website 15 August 2019 was breached. ECB issued a relevant report and press release. The breach was discovered after routine maintenance. The BIRD website provides the banking industry with details on

how to produce statistical and supervisory reports. As a result, the contact data (but not the passwords) of 481 subscribers to the BIRD newsletter may have been breached. The affected information may consist of the email addresses, names, and position titles of the subscribers. Hence, an attacker could use this data for further activities (e.g., conduct spear phishing attacks to high-rank officials, management staff) or attempt fraud by abusing spoofed identities.

Lessons Learnt: A rather positive lesson learnt was that BIRD was physically separate from other external and internal ECB systems. This isolation reduces the potential cascading impacts on other more critical systems and it's a good practice that has been suggested in the case of earlier incidents (e.g., SWIFT transactions outlined above). Another important lesson is the existence of a routine maintenance process. This process made discovery feasible at an early stage of the attack and minimized the incident's impact. Financial organizations should have such a routine check process in place that can verify the authenticity and the proper function of the organization's systems and be able to discover possible compromise at an early stage.

Retefe: The 5-year long banking malware

Retefe is a special banking malware that has been seen active between 2014 and 2019. This banking malware is primarily targeting German, Swiss and Austrian individuals. It has been initially discovered in 2014 by Trend Micro. The malware operators used advanced methods to redirect users to spoofed internet banking sites in order to steal banking credentials. Over the course of time, the malware has evolved from using proxies to Tor network and stunnel (secure tunnelling) to redirect users in spoofed sites to achieve its illicit purposes.

In typical Retefe attack scenarios, infected users are directed to fake HTTPS (Secure Hypertext Transfer Protocol) login pages, when trying to access their e-banking. The fake site requires login credentials and/or additional personal data. Users cannot easily understand the fake site, as it looks exactly like the original. Hence, unsuspecting victims can easily be fooled. In principle, it is possible to identify the fake site based on the certificate validation, but this is never easy for the average user.

Lessons Learnt: Retefe is a serious threat for unaware users, as they won't typically review the digital certificate of the HTTS sites that they visit. Hence, users won't verify the certificate issuer, which makes them vulnerable to data and money theft. Banks must therefore make sure that their users become aware of such attacks. For example, all affected UK banks have run awareness campaigns aiming at warning customers on the potential risks. Retefe's example is indicative of the importance of awareness campaigns that will educate users on how to avoid cyber-attacks like phishing, identity theft or credential harvesting. It is also a lesson for IT security teams of the financial organizations to monitor fake sites that imitate the organization using techniques like typosquatting[2], takedown of fake social accounts that imitate the organization and informing the users for their existence.

Cobalt Group Cybergang

Cobalt is a cybergang targeting financial institutions systems (e.g., e-payment systems, ATMs, SWIFT networks) since 2013. The group mainly targets banks in Eastern Europe, Central Asia, and Southeast Asia. Cobalt is likely associated with the Carbanak remote backdoor. According to Europol, Banks in

[2] Typosquatting: Also known as URL hijacking, is a form of cybersquatting (sitting on sites under someone else's brand or copyright) that targets Internet users who incorrectly type a website address into their web browser (e.g., "Gooogle.com" instead of "Google.com").

more than 40 countries have been allegedly attacked by Cobalt group and the overall losses are estimated to be above EUR 1 billion. The leader of the cybergang was arrested in March 2018 following an international operation between Europol, US FBI, the Romanian, Moldovan, Belarussian, Taiwanese and Spanish authorities. One example of attacks launched by Cobalt group is the SpicyOmelette attacks, which uses a vulnerability in JavaScript to grant attackers remote access to infected systems. The infection of the systems is delivered via phishing emails which are accompanied with attachments that look proper, yet when the victim clicks on them is redirected to an Amazon Web Services (AWS) Uniform Resource Locator (URL) controlled by Cobalt. The latter URL installs the SpicyOmelette script, which appears signed by a valid and trusted certificate authority (CA).

Lessons Learnt: The variety of attacks of Cobalt group justifies the need for integrated risk assessments that cover all assets. For example, attacks against the cyber part of the ATM network justify the need for an integrated security strategy for protecting it. Likewise, the importance of building and disseminating cyber-security knowledge that is specific to the financial sector is key to confronting common attacks like SpicyOmelette. Another lesson learned is the stealthy nature of the cybergangs and their malicious software. They tend to continuously evolve their malware to evade detection, highlighting the need for heuristic and predictive technologies in detection tools.

DarkVishnya: Eight banks hacked in Eastern Europe

According to Kaspersky[3], at least 8 banks were hacked from the inside between 2017 and 2018. The attacks, nicknamed DarkVishnya were executed with the use of inexpensive netbooks, Raspberry Pi and Bash Bunny. Attackers didn't use any of the traditional delivery methods like phishing emails. Instead, a visitor pretending to be a courier or a job seeker connected the device to the banks' network. The device offers remote access to the attackers via e.g., a 3G/4G modem. This type of attacks is difficult to detect because there is no infection in the bank's IT equipment

Lessons Learnt: This is yet another attack that reveals the fact that several attacks are launched from insiders. It unveils the importance of inside security measures such as the verification and use of trusted devices only, even when the bank's employees use the banking systems. It is also highlighting the importance of security processes and strict adherence to them. This attack would have been avoided if there was a proper procedure for accompanying external people and the personnel followed it without exception.

Physical Security Attacks: ATM Robbery on a BNP machine in Nanterre[4]

Even though conventional bank robberies incidents are declining when compared to the past, there are still physical security incidents. For example, in 2017, a robbery of 400,000 euros from an ATM (i.e. a BNP machine in Nanterre) took place. In the scope of the attack, an officer in charge of resupplying an ATM, was beaten to the ground and handcuffed, and then threatened with a gun by several individuals disguised as police officers. The officer was placed on the ground and forced to open the airlock, and enter the codes allowing the money to be recovered. The criminals threatened the officer with an electric pistol.

[3] https://securelist.com/darkvishnya/89169/

[4] https://www.lexpress.fr/actualite/societe/fait-divers/nanterre-braquage-d-un-distributeur-automatique-de-billets-a-400-000-euros_1874236.html

Lessons Learnt: Physical security attacks against the banking system are still happening. Technology (e.g., surveillance systems) can boost protection against such incidents, as well as against other security attacks with physical components such as ATM jackpotting attacks. Banks and equipment manufacturers should also monitor ATM equipment for possible vulnerabilities or for the event of tampering its software. Prompt patching and regular verification of original software is key to protect them.

Key Take Aways from the Attacks

Beyond lessons learnt from each attack, the following general remarks can be also drawn:

- The increased use of e-transactions in today's finance leads to more opportunities for cybercriminals. Most of the above-listed incidents concerned cyber-security attacks of different types.
- Organized cybercrime gangs are difficult to dismantle as often the developed malware will be re-used by new cybergangs. Hence, despite catching some of the criminals, their approaches are taken up and evolved from other cybercrime teams.
- Law enforcement operations need international cooperation as often cybergangs are set up worldwide and rely on remote hacked infrastructure for their activities. In this direction, the implementation of automated and trusted data exchanged measures is deemed important for a prompt response to cyberattacks.
- Cybercriminals utilize different techniques to evade detection. In a handful of incidents, we have presented plenty of different approaches. Even more such approaches have been used in other incidents. The presented list of recent security attacks is by no means exhaustive.
- Malicious parties (notably cyber-criminals) evolve their *modus operandi* in accordance with current IT trends. Hence, financial institutions must remain at the forefront of security innovation to be prepared to handle novel and sophisticated cyber-security attacks.
- The continuous evolution of the digital infrastructure creates a vast ground for financially motivated cybercriminals. Digital transformation, cryptocurrency and online marketplaces maximize the attack surface and the opportunities for cybercrimes. A cybergang that developed a crafted attack targeting one region can easily repurpose it for another region e.g. by hiring language skills and local know-how from the underground networks (dark web).
- Physical attacks are evolving to attacks of a hybrid nature with both the digital and the physical network of a financial organization being targeted. Cybercriminals are evolving their modus operandi and use digital skills to maximize their gains as in the example of the ATM jackpotting attacks.
- The cyberthreat landscape is continuously evolving with cybergangs deploying new business models like Ransomware-as-a-Service, DDoS for hire or other as-a-Service attacks. As a result, lower-skilled cybercriminals gain access to stealthy tools maximizing their gains and increasing the losses for financial organizations.
- The growing presence and facilitation of underground markets like deep dark web eases the exchange of know-how between cybercriminals. These creates more powerful and coordinated attacks with bigger damage to the financial organizations.

2. Best Practices and Solution Guidelines

Integrated Cyber and Physical Security Measures and Policies - Cyber Physical Threat Intelligence

Experience from recent security incidents shows that attackers attempt to take advantage of the cyber-physical nature of the critical infrastructures of the financial sector to launch security attacks against them. For example, violation of access control to SWIFT terminals was a prerequisite to launching cyber-attacks against the SWIFT network. Similarly, ATMs are susceptible to jackpotting attacks where attackers use portable computers to physically connect to the machine, while at the same time using malware to target the machine's cash dispenser. Cooperation with a physical attack where a member of the cyber gang is collecting the money is necessary. Thus, jackpotting is another example of a cyber-physical attack. Such incidents motivate the need for Cyber Physical Threat Intelligence (CPTI) towards protecting critical infrastructures of the finance sector. CPTI is at the very core of the FINSEC project, given that the project's platform is essentially enabling the implementation of technical measures for CPTI. Moreover, the FINSEC pilots include CPTI elements as they protect cyber and physical assets alike, while dealing with both cyber and physical incidents.

Best Practices for designing and implementing CPTI include:

- Modelling the Critical Infrastructure as a whole, including both Cyber and Physical assets, their interdependencies and the cascading effects that an attack on one type of assets can have on the other type. This requires improving the cyber defence model from addressing single vulnerabilities to a holistic approach that addresses security gaps in systems and processes.
- Specifying integrated security policies covering both cybersecurity and physical security measures, while fostering their interplay e.g., cyber-security measures triggering physical security measures and vice versa. The policies should be regularly updated and there should be a provision for temporary measures as a response to urgent threats.
- Reengineering the security organization of financial institutions towards boosting the collaboration between physical security teams and cyber-security teams (e.g., CERT - Computer Emergency Response Teams). This reengineering should consider the way these functions are organized and performed (e.g., there are scenarios where physical security is outsourced, while cyber-security is not).

Automated and Trusted Information Sharing - Collaborative Risk Assessment

Some of the presented security incidents (e.g., the Dridex malware-related attacks) have unveiled the importance of the stakeholders' collaboration in confronting complex cyber or cyber-physical attacks. Collaboration is particularly important in services that are delivered in the value chain i.e. services involving multiple organizations. Typical examples of such services are for example SWIFT and SEPA (Single Euro Payments Area) payment services. In the era of PSDII and Open Banking the delivery of multi-stakeholder services across the financial supply chain will proliferate. Hence, there importance of stakeholders' collaboration will increase. In this context, the following best practices are recommended:

- Increase the frequency of information exchange between financial organizations, especially organizations participating in the joint delivery of financial services;

- Automate the process of information exchange based on software systems, including the exchange of cyber-physical information;
- Automate the processing and analysis of the exchanged information towards automatically extracting insights about suspicious behaviours, anomalies and other indicators of security incidents. This can be achieved with the integration of threat exchange platforms and detection tools;
- Implement systems for the trusted and controlled exchange of information as financial organizations want to avoid sharing information that could compromise their reputation and create brand damage. Investing in communities of trust can be a key enabler while putting the necessary frameworks in place (like non-disclosure agreements, operational charter, sponsorships) to maintain trust.

Predictive Security and Early Preparedness

Most of the presented security incidents have been associated with serious financial losses and significant reputation damage for the involved financial institutions. Remedial actions at the technical, organizational and communication levels have alleviated the damage, but the losses remain. Addressing the security incidents in a timely fashion is therefore a best practice that can lead to early preparedness and minimization of loss. In this direction, technology can be exploited to:

- Provide early signs and indicators of security incidents based on predictive analytics.
- Deliver relevant alerts to security teams via user friendly tools like the FINSEC Dashboard.
- Establish organizational measures for proactively confronting incidents i.e. specifying actions to be undertaken in response to identified signs and alerts.
- Aggregate more operational data that can be used for detection and utilize “Big Data” processing methodologies and machine learning to process them for detection.
- Use Techniques Tactics and Procedures modelling of the cybercriminals like Mitre ATT@CK and pattern recognition to detect attacks promptly.
- Deploy innovative techniques in log analysis like sigma rules to improve your detection capability in fileless attacks.

Alleviating Deployment Barriers

Within the context of FINSEC the stakeholders represent a disparate set of organisations from different parts of the financial services sector serving different groups of customers and provide different distinct services to the market. This on its own proves somewhat as a barrier, whilst also requiring that the vision for innovation is ambitious to have the widest possible applicability. Successfully developing and deploying innovations depends on a multitude of internal and external aspects.

Specific Internal Barriers that appear to be prevalent are:

- A restrictive mindset.
- A lack of discovery competences.
- An unsupportive organizational structure.
- Insufficient management support.
- Financial barriers to innovation.
- Skill barriers to innovation.
- A lack of information.
- A lack of technology knowhow.

- Leadership.
- The organization of research and development within the entity and the priority given to it.

Within this context cultural barriers can mean that there is a lack of critical awareness alongside varying degrees of fear, uncertainty, and doubt. Amongst the numerous external barriers, the main ones of interest are regulatory influence and impact, market dynamics, competitor behaviour and wider economic turbulence. Collaborative projects like FINSEC come with the more nuanced challenges of competing requirements and interests, differing levels of technical competency and understanding all of which further contribute to increasing the complexity when it comes to deploying innovations coming from the project.

FINSEC has been driven by innovation at the technology level with the proposition to use Predictive Analytics/Machine Learning to better enable financial institutions and the respective security teams within these organisations to better monitor, manage, mitigate and respond to threats. This proves to be a challenge and a barrier as the technological approach has specific requirements and articulating those requirements to elicit the appropriate input from financial institutions can prove difficult when levels of awareness and technical knowledge differ. Also, a serious barrier to effective deployment will be demonstrating substantive value to the organisation be it by assisting meet regulatory obligations and/or to minimise the risk of business disruption, reputational damage, and financial loss.

FINSEC has solved the challenges to deployment and take-up that any collaborative project with multiple stakeholders faces through several activities:

- Early engagement with stakeholders long before the start of the project.
- A comprehensive set of tasks and activities devoted to knowledge transfer between technical teams and the stakeholders resulting in a bilateral dialogue on both business needs and technical objectives.
- Early identification of ‘project champions’ within the stakeholder organisations who then acts as the intermediary and facilitator for deployment and take-up assisting to overcome some of the intrinsic resistance and risk aversion within stakeholder organisations.
- Dedicated technical support for all the stakeholders to support them in overcoming any technical issues arising with deployment and use of the technologies and services emerging from FINSEC
- Detailed in-depth work on the role of regulation and standards, the implications for each one of the use cases and jurisdictions within which the institutions reside to identify exactly what requirements the technical solution must incorporate to achieve compliance.
- Continuous monitoring of forefront developments in the domain of IT security to maintain excellence and state-of-the-art.
- Study of the evolving threat landscape to maintain competitiveness and stay at the forefront of threats.

3. Overview of Selected FINSEC Solutions

Security Data Collection

One of FINSEC solution provides a Security Monitoring Infrastructure. This solution collects security information from cyber and physical systems and ensures appropriate levels and types of intelligence and adaptability of security monitoring mechanism.

One the FINSEC modules is the Intelligent and Adaptive Data Collection Infrastructure. This solution enables adaptive and intelligent collection of security information, as a means of enabling predictive security analytics for infrastructures of the finance sector. It comprises different security monitoring probes over the cyber and physical security systems. The probes supported by the infrastructure include:

- Collection probes for “Packet-level data”.
- Collection probes for “Flow-level data”.
- Collection probes for “Connection-level data”.
- Collection probes for “Host-level data”.
- Collection probes for “Application-Level Data”.
- Probes from the Skydive Real-Time Network Analyzer.

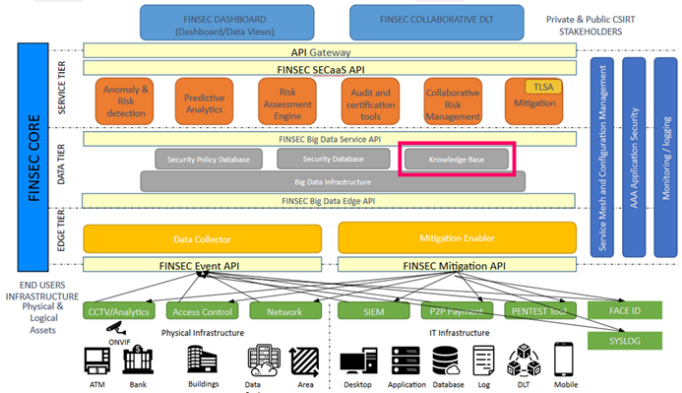
The solution specifies an Actuation API and a Data Collection API, which enable the implementation of additional probes and of actuating functions. In parallel a major step of the security data collection is the creation of a Cross-Layer SIEM (XL-SIEM) for Finance. Cross-Layer SIEM (XL-SIEM) is a Security Information and Event Management (SIEM) solution with added high-performance correlation engine to deal with large volumes of security information.

The FINSEC version of XL-SIEM has been enhanced to support security models and events for the finance sector. This solution is a SIEM system customized to the Finance Sector security. It provides scalability and distribution in security events processing through a cluster of nodes, and capacity to raise security alerts from a business perspective based on events collected from different data sources at different layers. XL-SIEM is ATOS technology built over the Alien Vault Open Source SIEM (OSSIM). It improves the traditional SIEM capabilities offered by OSSIM based on the integration of the Esper high-performance correlation engine.

This solution collects security information from cyber and physical systems and ensures appropriate levels and types of intelligence and adaptability of security monitoring mechanism.

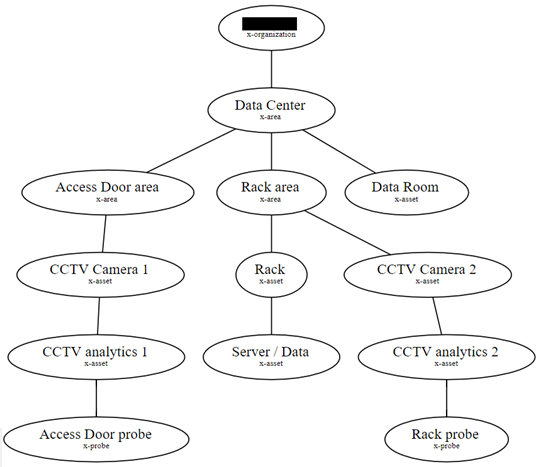
Reference Architecture for Security Solutions

The FINSEC Reference Architecture (RA) provides a blueprint for the development of data-driven systems for integrated cyber-physical threat intelligence over the critical infrastructures of the financial sector. The FINSEC Reference Architecture (RA) illustrates the main components of a data-driven cyber-physical threat intelligence system, as well as the interfaces and the information flows between them. It serves as a blueprint for the development of integrated (cyber/physical) security systems for the critical infrastructures of the



financial sector. It is presented in different views, including logical, process, implementation and deployment viewpoints that address the needs of all security stakeholders in the financial sector. The development of the FINSEC RA was driven by the current security needs of financial institutions including the need for integrated cyber and physical security, the need for collaboration across the stakeholders of the financial services chain, the need for regulatory compliance (e.g., PSD2 and GDPR compliance) and the need for increased automation in developing security solutions as part of the DevSecOps approach.

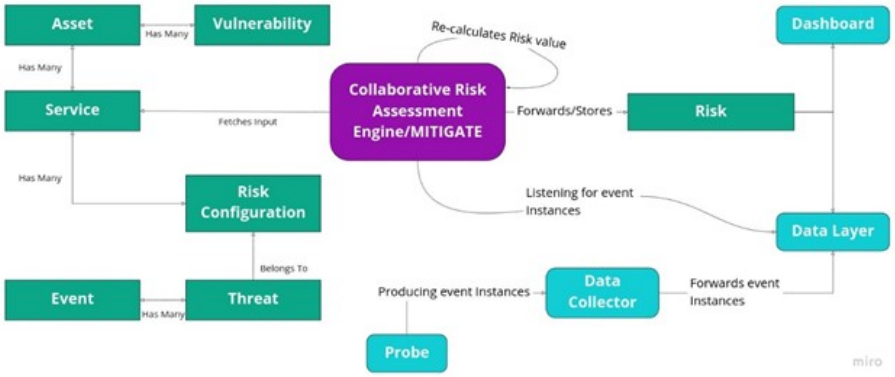
FINSTIX



FINSTIX offers a standard-based approach to model and represent Cyber Threat Intelligence (CTI) and the financial infrastructure assets. Covering both the physical and the cyber world, to the FINSEC Consortium knowledge, FINSTIX is the only data model that allows to represent and exchange Cyber-Physical Threat Intelligence (CPTI). FINSTIX enables modelling of CPTI information, with particular emphasis on cyber and physical security of the critical infrastructures of the financial sector. Using FINSTIX, organizations can collect security data from physical and cyber security systems in the financial sector, as means of applying security analytics, issuing alerts, and activating relevant security policies. Therefore it provides a unique standard-based way for representing security information, facilitating organizations to share information and to implement novel collaborative security functions, such as collaborative assessment of security risks. FINSTIX is also a foundation for representing security knowledge across the systems of the financial services supply chain.

Collaborative Risk Assessment

The Collaborative Risk Assessment Engine provides the means for sharing security information across various stakeholders of the financial supply chain, while at the same time using this information for collaborative risk scoring assessment.

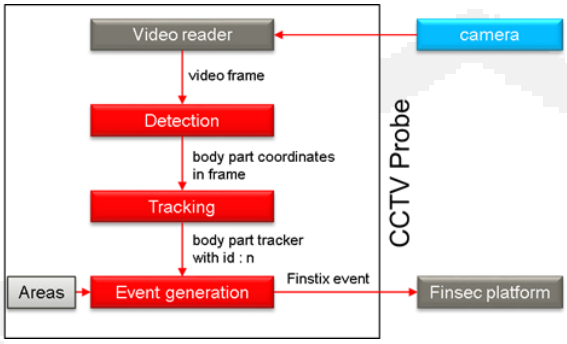


The Collaborative Risk Assessment Engine facilitates stakeholders' collaboration in the financial services supply chain. It is motivated by the fact that financial services infrastructures are nowadays digitally interconnected and hence any attacks on one party affects interconnected parties. This gives rise to stakeholders' collaboration in security processes like risk assessment.

The solution is empowered by an information sharing infrastructure that is based on distributed ledger technologies (i.e. blockchain technologies) and by a risk scoring engine. The engine is capable of performing a higher-level risk assessment based on pre-analysed data and accordingly to run aggregation risk assessments on top of these. Moreover, it consumes Risk Assessment reports from other interconnected organizations that share security information through the data sharing infrastructure.

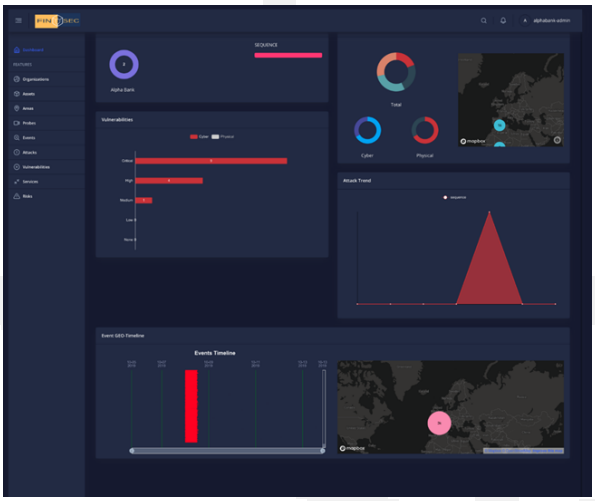
CCTV Analytics

This solution analyses CCTV data and identifies abnormal behaviours in scenarios associated with financial infrastructures like ATM networks. The solution analyzes CCTV observations and produces security-related events linked to human behaviors and physical interactions with other humans and/or the financial infrastructures. The solution detects objects (e.g. people, hands, banking cards, keys, etc.) and capture their interactions with each other and with physical motionless objects (e.g. ATMs or racks). The observations generate events that are provided to FINSEC data analytics services. One of the highlights of the solution is that it provides a privacy-preserving event model for a CCTV Analytics Probe. In particular, the solution does not store any biometric data and does not track individuals across scenes, contexts, and applications, thus safeguarding their privacy.



FINSEC Dashboard

This solution visualizes security information about the critical infrastructures of a financial organization in a human-readable and "security officer friendly" way. It provides a graphical representation of the cyber-physical threat intelligence information in a variety of formats, including trend graphs, pie charts and maps. It containing geo-location information associated with security data, relation graphs, paginated tables, modals that illustrate more details, as well as timeline that display security events occurring in specified intervals. It supports display of information in both pull and push modes. The Dashboard can be flexibly integrated with other security services that are accessible via REST APIs and provide information in-line with the FINSTIX format.



4. FINSEC Resources and More Information

FINSEC Solutions are described in Chapters 2-7 of the Open Access Book: John Soldatos (ed.), James Philpot (ed.), Gabriele Giunta (ed.) (2020), "**Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures", Boston-Delft: now publishers**, http://dx.doi.org/10.1561/9781680836875, available at: https://www.nowpublishers.com/Article/BookDetails/9781680836868

A Series of Presentations and Webinars about the FINSEC Solutions: https://finsecurity.eu/digital-finance-academy-for-security/

Ernesto Troiano, John Soldatos, Ariana Polyviou, Andreas Polyviou, Alessandro Mamelli, Dimitris Drakoulis: **Big Data Platform for Integrated Cyber and Physical Security of Critical Infrastructures for the Financial Sector**: **Critical Infrastructures as Cyber-Physical Systems. ACM MEDES 2019: 262-269**.

Apostolos P. Fournaris, Manos Athanatos, Konstantinos Lampropoulos, Sotiris Ioannidis, George Hatzivasilis, Ernesto Damiani, Habtamu Abie, Silvio Ranise, Luca Verderame, Alberto Siena, Joaquín García-Alfaro: Computer Security - **ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC, Luxembourg City, Luxembourg, September 26-27, 2019, Revised Selected Papers. Lecture Notes in Computer Science 11981, Springer 2020, ISBN 978-3-030-42050-5**


FIN
SEC


Innov-acts
GFT
Atos
Hewlett Packard Enterprise
FUJITSU
UTi GRUP
IBM
sia
Singular Logic
HDI Assicurazioni
nexi
jrc
Liberbank
NR Norsk Regnesentral
NORWEGIAN COMPUTING CENTER
wirecard
Consiglio Nazionale delle Ricerche
CCA
Clear Communication Associates Limited
Assentian Limited
ORT FRANCE
INNOVATION ET DEVELOPPEMENT
FONDAZIONE BRUNO KESSLER
cini
consorzio interuniversitario nazionale per l'informatica
Zanasi & Partners
Security Research and Advisory
ALPHA BANK