Introduction to the Training Workshop
Notorious Security Incidents in the Finance Sector

January 14th, 2021

John Soldatos, FINSEC Project

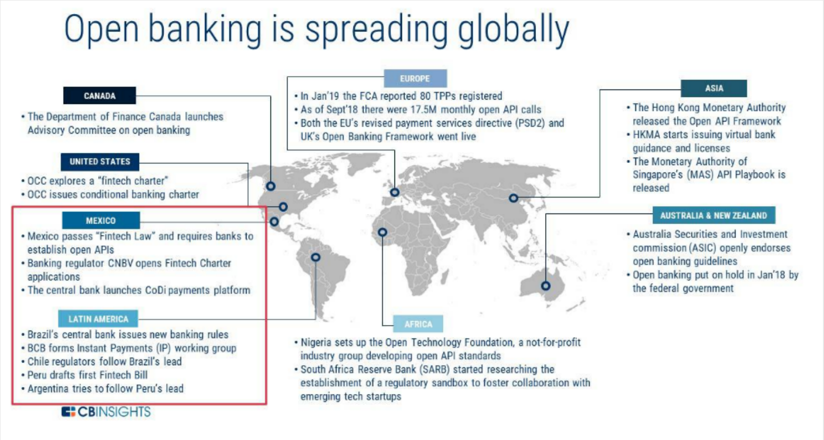
Background & Motivation

Stakeholders & Critical Infrastructures of the Finance Sector are densely Interconnected

- Financial Supply Chain Services (e.g., SWIFT/SEPA Transactions, Trading)
- PSD2 & Open Banking increase the number of interconnected (supply chain) services
- Security Incidents on one organization can impact interconnected organizations (incl. possible cascading effects)

Critical Infrastructures in Finance are large scale Cyber-Physical Systems

- Cyber Assets (e.g., networks, computers, software systems)
- Physical Assets (e.g., buildings, data centres, ATM devices)
- Cyber-Physical Interconnection



Open banking is spreading globally

CANADA
- The Department of Finance Canada launches Advisory Committee on open banking

UNITED STATES
- OCC explores a "fintech charter"
- OCC issues conditional banking charter

MEXICO
- Mexico passes "Fintech Law" and requires banks to establish open APIs
- Banking regulator CNBV opens Fintech Charter applications
- The central bank launches CoDi payments platform

LATIN AMERICA
- Brazil's central bank issues new banking rules
- BCB forms Instant Payments (IP) working group
- Chile regulators follow Brazil's lead
- Peru drafts first Fintech Bill
- Argentina tries to follow Peru's lead

EUROPE
- In Jan'19 the FCA reported 80 TPPs registered
- As of Sept'18 there were 17.5M monthly open API calls
- Both the EU's revised payment services directive (PSD2) and UK's Open Banking Framework went live

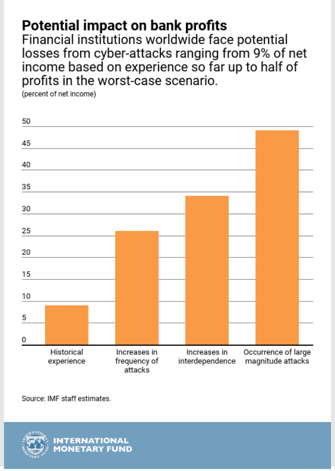
AFRICA
- Nigeria sets up the Open Technology Foundation, a not-for-profit industry group developing open API standards
- South Africa Reserve Bank (SARB) started researching the establishment of a regulatory sandbox to foster collaboration with emerging tech startups

ASIA
- The Hong Kong Monetary Authority released the Open API Framework
- HKMA starts issuing virtual bank guidance and licenses
- The Monetary Authority of Singapore's (MAS) API Playbook is released

AUSTRALIA & NEW ZEALAND
- Australia Securities and Investment commission (ASIC) openly endorses open banking guidelines
- Open banking put on hold in Jan'18 by the federal government

CBINSIGHTS

9% of Profits at Risk due to Cyber-Attacks (source: IMF)



Potential impact on bank profits

Financial institutions worldwide face potential losses from cyber-attacks ranging from 9% of net income based on experience so far up to half of profits in the worst-case scenario.

(percent of net income)

Source: IMF staff estimates.

INTERNATIONAL MONETARY FUND

Bangladesh Bank cyber heist

- The Incident:
  - Bangladesh Bank's offices closed (February, 2016)
  - Fraudsters intruded the SWIFT network of the bank and initiated US $1 billion to Federal reserve bank of New York out of which $850 million were blocked
  - 3/35 fraudulent instructions → transferring $101 million: $20 million traced to Sri Lanka & $81 million to Philippines
- **Attack had its roots in the manipulation of the SWIFT Alliance Access software**
- **One of the biggest cyber heist in history**

Dridex take down operation and revival

- Dridex is a banking malware : most active 2015 - 2016
- At Oct 2015 UK’s National Crime Agency (NCA) in cooperation with Federal Bureau of Investigation (FBI) & Europol coordinated a take-down activity by ‘sinkholing’ infected computers’ traffic
- Cybercriminals were believed to be based in Eastern Europe and target end users via documents delivered by e-mail addresses that seem legitimate.
- **£20M of estimated losses in the UK alone took place**
- **Dridex malware continues to evolve and remains a serious threat to end-users of financial services**

Bank of Valetta Attack

- February 13, 2019 hack of Bank of Valetta
- malware planted on the bank's internal servers
- Security analysts believe that EmpireMonkey cybercrime group is believed to be behind this attack
- From a technical perspective, attackers used macros to copy wscript.exe to another file
- **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**

Retefe: The 5 year long banking malware

- Retefe is a special banking malware that has been seen active between 2014 and 2019
- Banking malware that is primarily targeting German, Swiss and Austrian individuals
- Malware operators used advanced methods to redirect users to spoofed internet banking sites in order to steal banking credentials
- Malware evolved from using proxies to Tor network and stunnel (secure tunneling) to redirect users in spoofed sites to achieve its illicit purposes

Typical Retefe attack scenario:

- infected users are directed to fake HTTPS login pages, when trying to access their e-banking
- fake site requires login credentials and/or additional personal data
- unsuspecting victims can easily be fooled

DarkVishnya: Eight banks hacked in Eastern Europe

- At least 8 banks were hacked from the inside between 2017 and 2018
- Executed with the use of inexpensive netbooks, Raspberry Pi and Bash Bunny
- Didn’t use any of the traditional delivery methods like phishing emails but a visitor pretending to be a courier or a job seeker connected the device to the banks’ network
- Device offers remote access to the attackers via e.g. a 3G/LTE (Long Term Evolution) modem
- Difficult to detect because there is no infection in the banks IT equipment

Cobalt Group Cybergang

- Cybergang targeting financial institutions (e-payment systems, ATMs, SWIFT)
- Cobalt is likely associated with the Carbanak remote backdoor
- banks in more than 40 countries have been allegedly attacked by Cobalt group: losses are estimated to be above EUR 1 billion

Example:

- SpicyOmelette attacks: vulnerability in a JavaScript script to grant attackers remote access to infected systems.
- Infection of the systems delivered via phishing emails
- Once the victim clicks on them he/she is redirected to an Amazon Web Services (AWS) Uniform Resource Locator (URL) controlled by Cobalt
- installs the SpicyOmelette script, which appears signed by a valid and trusted certificate authority (CA)

Europe Physical Security Attacks: ATM Robbery on a BNP machine in Nanterre

- BNP ATM machine in Nanterre 2017
- officer in charge of resupplying an ATM was beaten to the ground and handcuffed and threatened with a gun by several individuals disguised as police officers
- Forced to open the airlock, and enter the codes allowing the money to be recovered
- Robbery of 400,000 euros

Cyber Security Incidents & Lessons Learned

Incident	Lessons Learned
Bangladesh Bank cyber heist	• SWIFT transactions should be conducted only on computers that are isolated from the rest of the network • Special security measures should be employed for every computing system that accesses the SWIFT computing system
Dridex take down operation and revival	• Collaboration among financial services firm around the world • Sharing information information with security experts & law enforcement agencies, enable the disruption of cybercrime teams
Attack against the Bank of Valletta	• Risk assessment to account the vulnerabilities of multiple assets, interdependencies and cascading effects of possible attacks • Need for becoming more intelligent & proactive
Retefe: The 5 year long banking malware	• Users won't verify the certificate issuer → vulnerable to data and money theft • Banks must therefore make sure that their users become aware of such attacks

Cyber Security Incidents & Lessons Learned

Incident	Lessons Learned
Cobalt Group Cybergang	• Beed for integrated risk assessments that cover all assets • Importance of building and disseminating cyber-security knowledge that is specific to financial sector
DarkVishnya: Eight banks hacked in Eastern Europe	• Several attacks are launched from the inside • Importance of inside security measures such as the verification and use of trusted devices
ATM Robbery on a BNP machine in Nanterre	• Physical security attacks against the banking system are still happening • Technology (e.g., surveillance systems) can boost protection against such incidents

Extending the Lessons Learned for the Finance Sector

Increased use of e-transactions today:

More opportunities for cybercriminals

Developed malware re-used by new cybergangs

→ Catching the criminals is not the solution, their approaches evolve

Law enforcement operations need international cooperation:

→ Implementation of automated and trusted data exchanged

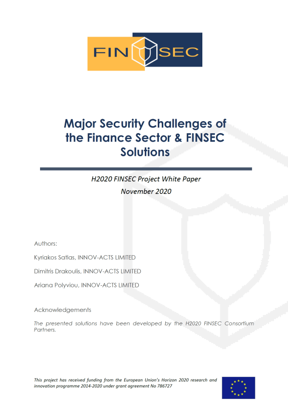
Cybercriminals utilize different techniques to evade detection

Malicious parties evolve their approaches in accordance to current IT trends

→ Financial institutions must remain at the forefront of security innovation

More Information - Free Downloads (Finsecurity.eu)

White Paper: “Major Security Challenges of the Finance Sector & FINSEC Solutions”: https://finsecurity.eu/digital-finance-academy-for-security/major-security-challenges/



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

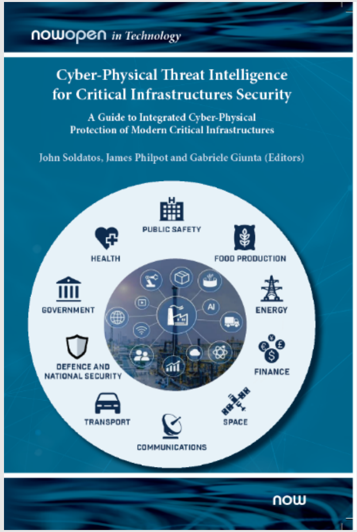
Ariana Polyviou, INNOV-ACTS LIMITED

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

Open Access Book (free download): 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
Download at:
https://www.nowpublishers.com/Article/BookDetails/9781680836868



nowopen *in Technology*

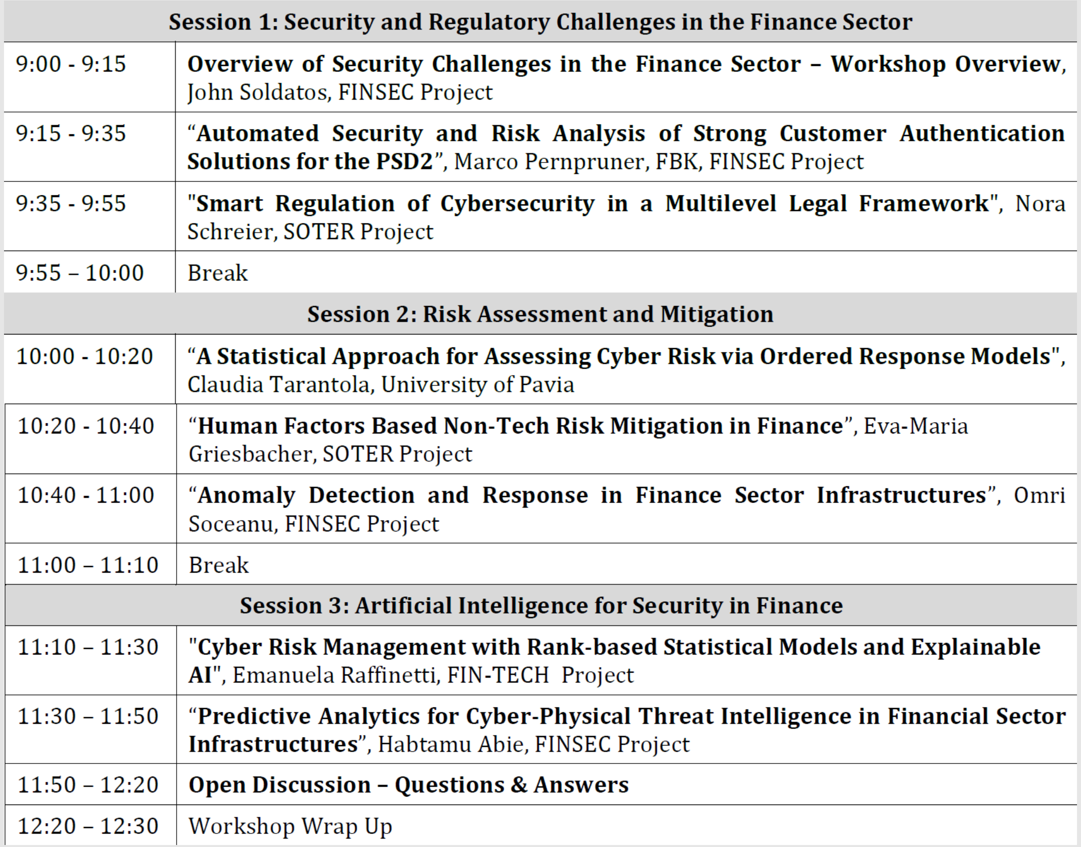
Cyber-Physical Threat Intelligence for Critical Infrastructures Security

A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures

John Soldatos, James Philpot and Gabriele Giunta (Editors)

now

Agenda



Session 1: Security and Regulatory Challenges in the Finance Sector	
9:00 - 9:15	**Overview of Security Challenges in the Finance Sector – Workshop Overview**, John Soldatos, FINSEC Project
9:15 - 9:35	"**Automated Security and Risk Analysis of Strong Customer Authentication Solutions for the PSD2**", Marco Pernpruner, FBK, FINSEC Project
9:35 - 9:55	"**Smart Regulation of Cybersecurity in a Multilevel Legal Framework**", Nora Schreier, SOTER Project
9:55 – 10:00	Break
Session 2: Risk Assessment and Mitigation	
10:00 - 10:20	"**A Statistical Approach for Assessing Cyber Risk via Ordered Response Models**", Claudia Tarantola, University of Pavia
10:20 - 10:40	"**Human Factors Based Non-Tech Risk Mitigation in Finance**", Eva-Maria Griesbacher, SOTER Project
10:40 - 11:00	"**Anomaly Detection and Response in Finance Sector Infrastructures**", Omri Soceanu, FINSEC Project
11:00 – 11:10	Break
Session 3: Artificial Intelligence for Security in Finance	
11:10 – 11:30	"**Cyber Risk Management with Rank-based Statistical Models and Explainable AI**", Emanuela Raffinetti, FIN-TECH Project
11:30 – 11:50	"**Predictive Analytics for Cyber-Physical Threat Intelligence in Financial Sector Infrastructures**", Habtamu Abie, FINSEC Project
11:50 – 12:20	**Open Discussion – Questions & Answers**
12:20 – 12:30	Workshop Wrap Up