Systemic Analyser in Network Threats - SAINT

By Latif Ladid, IPv6 Forum President

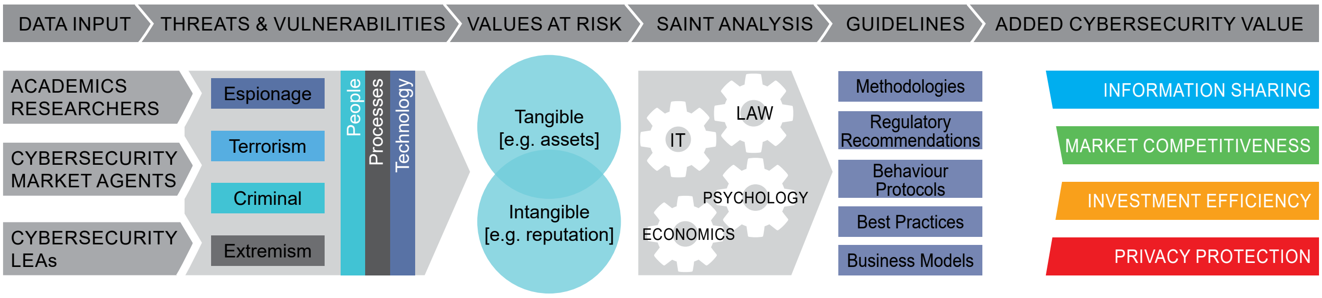
Latif Ladid, IPv6 Forum President

Overall Concept

Systemic Analyser in Network Threats – SAINT proposes to analyse and identify incentives to improve levels of collaboration and information sharing in order to enhance cybersecurity. Based on advanced measurement methodologies of cyber-crime metrics with machine learning algorithms, and by the use of statistical analysis and econometric modelling *SAINT* will develop new research approaches in information sharing, behavioural attitudes, market competitiveness and investment efficiency concerning the cyber-security industry.

SAINT's concept and methodology is depicted graphically in the following diagram. The community of all stakeholders and agents in the cyber-security industry provide important information about cyberthreats and relevant vulnerabilities, from which relevant metric indicators are identified. *SAINT* analyses these cybersecurity data metrics with a multidisciplinary methodology, employing analytic frameworks from various scientific disciplines (IT, Economics, Psychology, Law), resulting in providing clear guidelines to all relevant stakeholders (policy makers, regulators, governmental authorities, law enforcement agencies, relevant market operators) for mutually beneficial cybersecurity information sharing, enhanced privacy protecting behavioural attitude, market competitiveness in the cyber-security industry, and efficiency in cybersecurity investment.

The research and development that comprise the SAINT Analysis methodology, can be categorised into the following



▶ main scientific activities:

- Applied cybersecurity metrics analysis.
- Regulation focused comparative analysis.
- Data mining and data processing automated analysis for the development of machine learning algorithms.
- Economic and behavioural theoretic analysis for the development of econometric and behavioural models.

Objectives

- Establish a complete set of metrics for cyber-security economic analysis, cyber-security and cyber-crime market
- Develop new economic models for the reduction of cyber-crime as a cost-benefit operation
- Estimate and evaluate the associated benefits and costs of information sharing regarding cyber-attacks
- Define the limits of the minimum needed privacy and security level of internet applications, services and technologies
- Identify potential benefits and costs of investing in cyber-security industry as a provider of cyber-security services
- Develop a framework of automated analysis, for behavioral, social analysis, cyber-security risk and cost assessment
- Provide a set of recommendations to all relevant stakeholders including policy makers, regulators, law enforcement agencies, relevant market operators and insurance companies

Application of Cyber-Security Metrics

SAINT will set out a database of cyber-security indicators and metrics about:

a) Information sharing, such as blacklists, cyberattack measurements, malware listing, infected websites, phishing activity, price of digital assets and costs of intangible risks (reputation, non-critical service disruption).

b) Behavioural privacy, such as level of privacy and anonymity provided by privacy-enhancing techniques, limits of traffic analysis of encrypted network data streams.

c) Profitability in the cybersecurity market, such as costs, prices, net present values, internal rates of return.

d) Cybersecurity investment efficiency, such as scalability, efficiency, reliability, security, usability, acceptance and societal compliance.

The definition of these cybersecurity metrics will be based on the identification of practical use cases, related in particular, to commonly occurring incidents.

Data Mining, Data Processing and Automated Analysis

SAINT will develop an automated analysis framework, which will utilise different forms of intelligent information feeds as inputs for identifying current and future threats in the cyberspace and estimating various relations among them as well as to society and economy. The idea behind automated analysis methodology is that the Internet has a multitude of information sources and communications channels which contain huge amount of raw data related to cybersecurity, mostly in a textual form. Such sources of information include cyberprivacy/cybersecurity discussion forums and blocks, security product companies' incident reporting Web pages, bug bounties discussions and reward announcements, as well as public police reports.

Within this framework, we propose the development of the automated analysis framework, which will utilise different forms of intelligent information feeds as inputs for identifying current and future threats in the cyberspace and estimating various relations among them as well as to society and economy. Information extracted from security contests, announced bounties, available cybersecurity updates and bug fixes, price-lists of private security vendors as well as from social networks will be analysed using epidemiological models and machine learning algorithms in order to extract early warning patterns on possible threats.

Economic and Behavioural Theoretic Analysis

SAINT is going to examine the relation between information availability on cyberattacks and security in the cyberspace, by linking measures for knowledge-sharing and relevant training to increased levels of defence against cyberthreats. Along with that, we will investigate the role of cybersecurity information sharing in the investment behaviour. The construction of the methodological framework consisting of these guidelines about information sharing policies will be based on the joint estimation and evaluation of measurable quantitative economic, behavioural and technical variables about the influence of cybersecurity information sharing in the cost structure, the rate of investment, the effective allocation of resources and the overall profitability of each agent.

SAINT research will also investigate the behavioural features of network traffic flow characteristics, for detection of careless and negligent attitude of users, regarding their surfing in suspicious Web pages and the proper application of cybersecurity norms and rules. Based on behavioural psychology theory, we will especially, introduce a more accurate prediction of the cyber-attack detection, by minimising the prediction error on standardised privacy leakage metrics regarding network anomaly detection, represented in daily and weekly patterns. With the use of novel algorithms, the sweep-time parameter for change point detection allows to catch different diurnal and weekly network patterns and smoothly normalise the adjustment of the prediction error on the different counts of events. On the grounds of privacy and cybersecurity, we plan to explain the role of certain individual characteristics of personnel in private and public sector organisations, such as gender, age, education level, and marital status, in shaping cybersecurity behaviour and evaluate the influence of evolving learning over time, on developing people's awareness of cyberthreats.

Moreover, SAINT will perform a thorough analysis on economic factors shaping the conditions for competition and profitability in the cybersecurity industry, assessing effectiveness in the provision of cybersecurity services as it concerns allocation of resources and quality of protection. Using relevant econometric models we will estimate the influence of factors mitigating financial risk exposure against independent and extreme loss events and the relation between vulnerabilities and supply and demand in the cybersecurity market.

Finally, SAINT will analyse the economics of hacking as it concerns what drives the market for profit-motivated hackers to engage in illicit activities in the cyber-space and the ways that their profitability can be affected from cyber-security defending mechanisms, employed by potential cyber-victims.

Expected Impact

- Improved social, institutional and economic comprehension of cyber-security failures
- Improved decision making, governance and investments by stakeholders (e.g. policy makers, regulators, law enforcement agencies, market operators and insurance companies)
- Provision of new models (that take into account cyber-security economics, risks, social and market aspects) for improving institutional and private initiatives in their quest for societal resilience to cyber-security risks
- Facilitated information dissemination and sharing for the public and registered users
- Provide a set of recommendations to fight cybercrime through systemic approach impacting the economic and incentive models of cybercrime

Consortium

Academic Research Partners

- National Centre for Scientific Research “Demokritos” (Greece) as Coordinator
- Computer Technology Institute of the University of Patras (Greece)
- Centre for Security Studies – KEMEA (Greece)
- University of Luxembourg (Luxembourg)
- Mandat International (Switzerland)

Business Partners

- Archimede Solutions (Switzerland)
- Stichting CyberDefcon Netherlands Foundation (Netherlands)
- Montimage (France)
- Incites Consulting (Luxembourg)

Law Enforcement Authority

- Hellenic Police Cybercrime Unit – as part of KEMEA (Greece)

Contact Information

Project website: www.project-saint.eu
Project social media:
Facebook: https://www.facebook.com/saintprojecteu/
Twitter: https://twitter.com/saintprojecteu
LinkedIn: https://www.linkedin.com/in/saintprojecteu/

Project Coordinator:
Integrated System Laboratory
Institute of Informatics & Telecommunication
NCSR “Demokritos”
Dr. Stelios C. A. Thomopoulos
scat@iit.demokritos.gr
Institute Director & Director of Research

Consortium members of the SAINT project.