SAINT-PETERSBURG STATE POLYTECHNICAL UNIVERSITY
Department of Computer Systems and Software engineering

# ESSAY

for second lecture
Discipline: "Information security"

Performed: student gr. 53501/2
Ponomarev M.A

Teacher
Vilegzanina K.D

Saint-Petersburg
2015

## Essay cover three themes:

- Improving Efficiency of Spam Detection using Economic Model
- Enterprise Risk Assessment Based on Compliance Reports and Vulnerability Scoring Systems
- Protecting Enterprise Networks through Attack Surface Expansion

# 1 First theme

The first theme ensures us about significant impact of email spam on our life. As well as that, it states that econimic lifts and declines lead to increasing or, opposite, decreasing threats of email spamming. One of way to detect email spamming is to include a novel economic metric, based on the underlying spam economic system, to assist detectors in keeping their false positives at bay by associating detection accuracy to the spammer's cost.

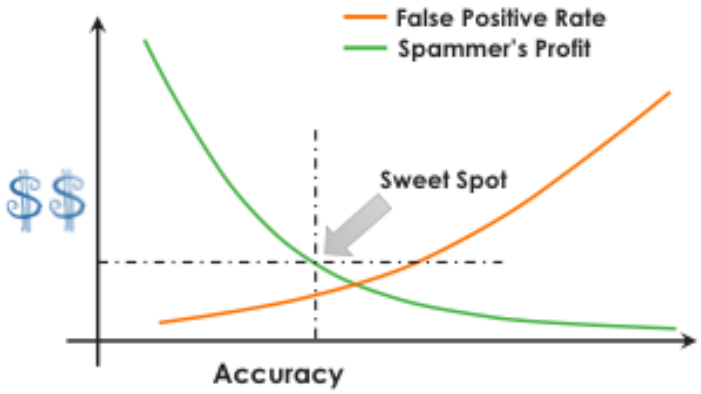


Figure 1: Economic metric

Main idia is that spammer program spend some money to achieve some desired utility. Constraining the economic model using the detection features provides a relationship between detection accuracy and spammer's cost. So that spam detectors suffer from the inherent tradeoff between accuracy and efficiency. Since, spam is all about earning money, to deal with it:

- **Created** an economic metric by associating the detection accuracy of the detectors with the spammer's cost.
- **Developed** a mechanism to identify effective spam detection features (like IDT) using K directed divergence analysis, followed by the use of ROC curves to evaluate the performance of IDT based detector
- **Developed** a spam economic model that calculates the spammer utility in terms of the number of spam emails sent by the spammer. Fur- ther constraining this utility with the IDT feature, we have added a cost sense into the detector to focus on increasing spammer's cost rather than just the detection accuracy.

## 2 Second theme

The second theme is about risk assessment. Risk assessment aims to provide consistent recommendations to maximize the protection of organization assets. There are two main documents to provide standarts of risk management:

- **The Security Content Automation Protocol (SCAP)** provides standard specifications to communicate security information.
- **The Extensible Configuration Checklist Description Format (XCCDF)** specifies a language to describe security checklists and collect com- pliance results of targeted systems.

Risk models define the risk factors to be assessed and the relationships among them. Typical risk factors include threat, vulnerability, impact, likelihood of exploit, and predisposing condition. Risk model defines the risk in terms of:

- The exploitability and impact scores reported by the vulnerability scoring systems.
- Hosts' exposure that takes into con- sideration the network configuration and the vulnerabilities distribution.
- The assets distribution in the network.

To calculate risk is used the total impact subscore and the integrity impact base score as in the case of Infidelity. The Risk of a particular host h formally is:

$$Risk(h) = A(h) * B(h) * \sum_{v} (\frac{\$[v, E]}{10} * \$[v, I]) \tag{1}$$

where $A(h)$ is the asset value of the host $h$.

This work investigates the feasibility of using security compliance reports along with universal vulnerability scores and network configuration in assessing the risk of cyberattacks.

## 3 Third theme

The third theme declares that it is critical to protect the enterprise assets from being stolen or compromised by internal and external attackers. Attack surface is a valuable metric that help administrators of enterprise networks to evaluate the risk and security of the entire network.

Current theme is about research efforts usually focus on reducing the attack surface observed by the attackers. Attacks are devided by:

- **Internal attack surface (IAS)** - the attack surface observed by the defenders
- **External attack surface (EAS)** - the attack that can be observed by the external unauthenticated attackers

A system's attack surface is the set of ways in which an adversary can enter the system and potentially cause damage. There are three main ways of expanding Attack Surface:

- using Virtual Identities
- using Dynamic Virtual Networks
- using Secret Moving Proxy