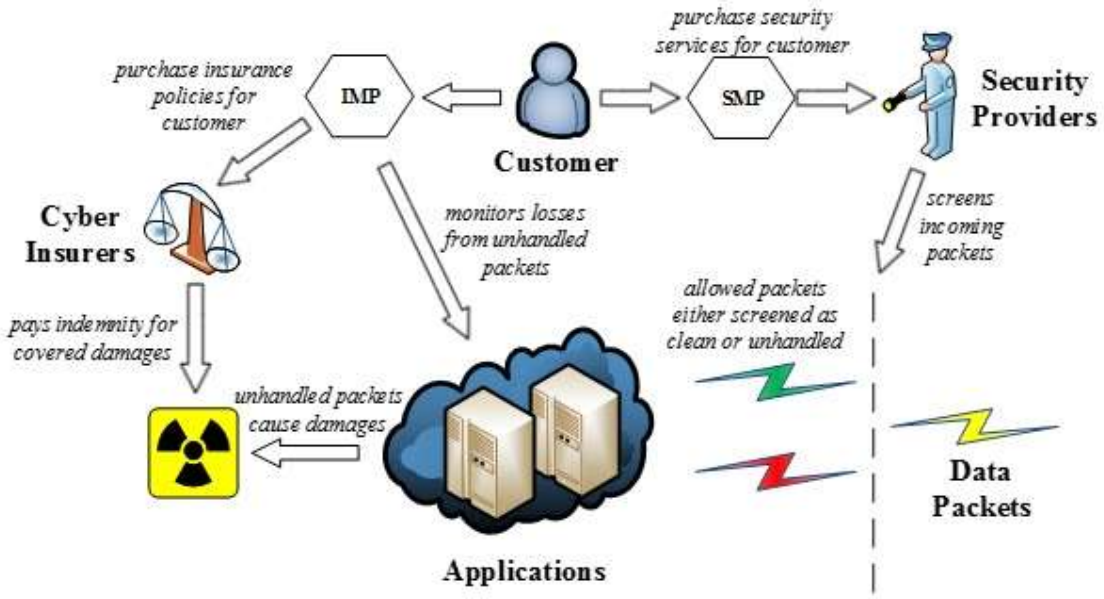
A Joint Optimization Approach to Security-as-a-Service Allocation and Cyber Insurance Management

Security-as-a-Service (SECaaS), pay-per-use cloudbased services that provides information security measures via the cloud, are increasingly used by corporations to maintain their systems' security posture. Customers often have to provision these SECaaS services based on the potential subscription costs incurred. However, these security services are unable to deal with all possible types of threats. A single threat (e.g. malicious insiders) can result in the loss of valuable data and revenue. Hence, it is also common to see corporations (i.e. cloud customers) manage their risks by purchasing cyber insurance to cover costs and liabilities due to unforeseen losses. A balance between service allocation cost and insurance is often required but not well studied.

We proposed an optimized SECaaS framework that consists of two major processes, i.e. subscription and insurance management processes. The processes apply an optimal solution from solving the optimization model that jointly minimizes the costs of security services handling application packets and cyber insurance policies covering unhandled risks from malicious packets. Our model was derived by stochastic programming with three-stage recourse for dealing with uncertainties including fluctuating prices of security services and insurance premiums, unpredictable security service demand, and the uncertain number of unhandled cyber threats. . Simulations were conducted to evaluate this optimization model. We exposed our model to several uncertain information parameters and the results are promising – demonstrating an effective approach to balance customers' security requirements while keeping service subscription and insurance policy costs low.

For our future work, the objective function and constraints of our stochastic programming model will be tested with real life environments. Actual insurance packages, service-level agreements, and performance metrics (e.g., communication and computation overheads of security services) will be taken into account. Interdependent risks (e.g., risks from two or more applications that can be correlated) will be considered. Honeypots will be deployed in public clouds for capturing unhandled packets arriving at certain applications associated with security services. From the honeypot data, a scenario tree with its probability distribution can be constructed and practically used by the optimization model. Computational complexity of the optimization model will be evaluated and approaches to addressing the complexity will be explored.



Principal Investigators	Assoc. Prof. Dusit Niyato *(SCSE)* Assoc. Prof. Wang Ping *(SCSE)*
Student	Mr. Jonathan Chase
School / Dept	School of Computer Science & Engineering
Collaborator	Sivadon Chaisiri Ryan Ko