ΠΑΡΟΥΣΙΑΣΗ
ΔΙΔΑΚΤΟΡΙΚΗΣ ΔΙΑΤΡΙΒΗΣ

ΗΜΕΡΟΜΗΝΙΑ: Τρίτη, 18 Ιουνίου 2019

ΩΡΑ: 13:00

ΑΙΘΟΥΣΑ: Αίθουσα Σεμιναρίων Κτήριο Τμήματος Μηχανικών Η/Υ & Πληροφορικής

ΟΜΙΛΗΤΗΣ: Ιωσήφ Πολενάκης

Θέμα
«Algorithmic Techniques for Detection and Classification of Digital Objects»

Επταμελής Εξεταστική Επιτροπή:
1. Σταύρος Δ. Νικολόπουλος, Καθηγητής Πρώτης Βαθμίδας, Τμήμα Μηχανικών Η/Υ και Πληροφορικής, Πανεπιστήμιο Ιωαννίνων (Επιβλέπων).
2. Λεωνίδας Παληός, Καθηγητής Πρώτης Βαθμίδας, Τμήμα Μηχανικών Η/Υ και Πληροφορικής, Πανεπιστήμιο Ιωαννίνων.
3. Λουκάς Γεωργιάδης, Αναπληρωτής Καθηγητής, Τμήμα Μηχανικών Η/Υ και Πληροφορικής, Πανεπιστήμιο Ιωαννίνων.
4. Χρήστος Νομικός, Επίκουρος Καθηγητής, Τμήμα Μηχανικών Η/Υ και Πληροφορικής, Πανεπιστήμιο Ιωαννίνων.
5. Ιωάννης Σταματίου, Καθηγητής Πρώτης Βαθμίδας, Τμήμα Διοίκησης Επιχειρήσεων, Πανεπιστήμιο Πατρών.
6. Αριστειάδης Παγουρτζής, Αναπληρωτής Καθηγητής, Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Εθνικό Μετσόβιο Πολυτεχνείο.
7. Δημήτριος Τσώλης, Επίκουρος Καθηγητής, Τμήμα Διαχείρισης Πολιτισμικού Περιβάλλοντος και Νέων Τεχνολογιών, Πανεπιστήμιο Πατρών.
In this PhD Thesis there have been studied the algorithmic techniques for the detection and classification of digital object. In the area of digital objects, this Thesis focuses mainly on the investigation of designing and proposing algorithmic techniques that detect and classify (in terms of indexing) a specific category of digital objects, the one of software, and more precisely the malicious software, providing finally an integrated algorithmic framework for protection against malicious software.

It is well known that malicious software consists a security threat of major importance. Especially the last years, where almost every device supports networked operations, several malicious attacks have been deployed targeting on the infringement of Confidentiality, Integrity and Availability of data stored into information systems or any other computing device. Hence, this thesis mainly focuses on the design and the development of efficient graph-based algorithmic techniques that detect malicious software samples and further classify them into known malware families, while on the other hand, the proposal of graph-based strategies for early warning, effectively prevent the pandemic spread of malicious software between interconnected mobile devices. The structure of the thesis is developed over two axes, namely, the design and development of protection techniques against the malicious software, regarding the detection and classification of malicious samples, and the development of graph-based techniques for pandemic prevention, regarding the definition of the maximum time required for a countermeasure to suppress malware’s spread.

Malicious authors, in order to avoid traditional detection methods, have developed sophisticated practices focusing on mutating their produced malicious samples, incorporating mutation engines that mutate the structure of the generated malicious samples (i.e., polymorphism and metamorphism). On the first development axis of this thesis, the research focuses on the design and the proposal of a mutation tolerant graph-based representation of malicious software sample’s behaviour (behavioural graph) resulted from System-call Dependency Graphs, or, for short ScDG, a Directed Acyclic Graph produced through Dynamic Taint Analysis of the executed sample. So, in the first state we propose the Group Relation Graph, or, for short GrG, a Directed Weighted Graph that is an abstraction of ScDG resulting after grouping disjoint vertices of it, utilizing the property that system-calls can be merged into groups based on their similar functionality. Further, we extent this approach by proposing the Coverage Graph, or, for short CvG, where we investigating the dominating relations among the vertices of GrGs regarding the vertex weight and degree. Additionally, extending the potentials of the above graph-based representations, we also propose the Temporal Graphs, that actually depict the structural evolution of the previously proposed graphs (i.e., GrG and CvG) by depicting their structures through instances captured over specific periods. Among others, we propose a set of similarity metrics that utilize quantitative, relational and qualitative characteristics of the above graph-based representations of malicious
software sample’s behaviour, utilizing them in order to experimentally evaluate the detection and classification potentials of our model.

Moreover, since the usage of mobile devices exhibits a wide spread, throughout this thesis, it has also been studied the development of graph-based algorithmic techniques that would integrate the overall algorithmic framework for protection against malicious software by investigating graph-based strategies for suppressing and finally avoiding potential pandemics caused by malware’s spread. More precisely, we propose a set of graph-based techniques for modelling the topology of towns-planning, the node mobility patterns as also the propagation behaviour, incorporating them to develop an algorithmic technique that defines the maximum permitted time required by a counter-measure to take effect removing the malware from an infected device (i.e., response time) in order to finally the pandemic spread. Finally, the precision of the proposed approach is tested throughout a series of repetitive series of experiments of various epidemic models and set of factors that affect the malware’s spread.