Cryptologic Methods Used in Computer Viruses

Vesselin Bontchev

National Laboratory of Computer Virology Bulgarian Academy of Sciences

The paper describes the various cryptographic and cryptanalytic techniques, which the author has observed as being used in computer viruses and other malware. Most of what the anti-virus people call "encryption" is not really encryption but encoding. The paper emphasizes this difference in terminology and describes in detail only the techniques that can correctly be classified as "cryptographic" and "cryptanalytic" from a cryptographer's point of view. Various techniques like authentification, asymmetric encryption, error correcting codes and brute-force cryptanalysis are considered.

Key words: Computer viruses, Malware, Cryptography, 94A60

Introduction to NISL

Kr. Markov[1], Kr. Ivanova[1], I. Mitov[2]

[1] *Institute of Mathematics and Informatics, Bulgarian Academy of Sciences*

[2] *Institute of Information Theories and Applications FOIITHEA, e-mail: info@foibg.com*

The Numbered Information Spaces Language (NISL) is aimed to serve the access to information bases using the numbered information spaces. It has three main sub-languages:

- Numbered Information Spaces Definition Language (NISDL)
- Numbered Information Spaces Manipulation Language (NISML)
- Numbered Information Spaces Query Language (NISQL)

The NISL follows the possibilities of the Milti-domain Information Model presented in [Markov 2004].

The NISL main information structures are:

- basic information elements - arbitrary long strings of machine codes (bytes) which may represent information structures of any kind. When it is necessary the strings may be parceled out by lines. The length of the lines may be variable.
- numbered information spaces of different ranges,
- indexes,
- meta-indexes.

The basic elements are organized in numbered information spaces with variable ranges. There is no limit for the ranges the spaces. Every element may be accessed by correspond multidimensional space address (coordinates) given via coordinate array. At the first place of this array the space range needs to be given. So, we have two main constructs of the physical organizations - numbered information spaces and elements, and two additional - indexes and meta-indexes.

The NISL main operations with basic information elements are:

- reading a part or a whole element;
- writing a part or a whole element;
- appending a string to an element;
- inserting a string into an element;
- removing a part of an element;
- replacing a part of an element;
- deleting an element;
- returns the length of the element in bytes.

The numbered information spaces are ordered and main operations within spaces take in account this order. So, from given space point (element or subspace) we may search the previous or next empty or non empty point (element or subspace). It is convenient to have operation for deleting the space as well as for count its nonempty elements or subspaces.

The logical operations are based on the classical logical operations - intersection, union and supplement, but these operations are not so trivial. Becausc of complexity of the structure of the spaces these operations have at least two principally different realizations based on codes of information spaces' elements and on contents of those elements.

The information operations can be grouped in sets corresponding to the main information structures: elements, spaces, indexes and meta-indexes. Information operations are context depended and need special realizations for concrete purposes. Such well known operations are, for instance, transferring from one structure to another, information search, sorting, making reports, etc.

At the end there exist several operations which serve information exchange between archives (files) such as copying and moving spaces from one to another archive.

Bibliography

[Markov 2004] K. Markov. Multi-Domain Information Model. Int. Journal "Information Theories and Applications", 2004, Vol. 11, No. 4, pp. 303-308

Key words: 68N15 Programming languages, Numbered Information Spaces Language, NISL

Visualization of Association Rules

Georgi Simeonov[1], Ivan Koychev[2], Jean-Christophe Bennavail

[1] *Institute of Mathematics and. Informatics. Bulgarian Academy of Sciences*

[2] *Faculty of Mathematics and Informatics, Sofia University*

[3] *Retail-Analytics ltd. Birmingham, UK, e-mail: jch@retai.l-analytics.com*

Visualization techniques have been very useful in managing and displaying data and knowledge in a comprehensible and intuitive way. The visual exploration can be of great asset for data mining systems where complex models have to be displayed in an easy to understand way to facilitate the decision-making process

New Trends in Mathematics and Informatics

Jubilee International Conference 60 years
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences

A B S T R A C T S

Sofia, Bulgaria
6-8 July, 2007

CEI
CENTRAL EUROPEAN INITIATIVE

"New Trends in Mathematics and Informatics"
ISBN 978-954-8986-26-7