

METHODS AND MEANS FOR PROTECTION OF SOFTWARE CRITICAL INFRASTRUCTURES

EUGENE NICKOLOV, PROF. DSC. CEO,
DIMITRINA POLIMIROVA, PHD,
NATIONAL LABORATORY OF
COMPUTER VIROLOGY – BAS



- Wireless Security
- Data Security
- Cryptographic Security
- Computer Security
- Steganographic Security
- Communication Security
- Mobile device Security
- Operating System Security
- Application Security
- Web Security
- Emission Security
- Email Security

25-26 Mar 2010, Sofia, Bulgaria

GMES OPERATIONAL CAPACITY WORKSHOP

GMES 2010



National Laboratory of Computer Virology – BAS

1. DEFINITIONS

- 1.1. Infrastructures
- 1.2. Critical Infrastructure
- 1.3. Software Critical Infrastructure



1.1. INFRASTRUCTURES

 National Laboratory of Computer Virology – BAS

- According to "Etymology online" ^[1] a definition for the global infrastructure exists since 1927 and means: "The installations that form the basis for any operation or system.". Originally the term was used by the military.

[1] Online Etymology Dictionary, Douglas Harper, Historian,
<http://dictionary.reference.com/browse/infrastructure>

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
3



1.1. INFRASTRUCTURES

 National Laboratory of Computer Virology – BAS

- Usually the term "infrastructure" refers to the technical structures that serve citizens. These are roads, water supply, sewage system, electrical network management systems in a flood, communications (internet, telephone lines, radio, television), etc. In the past these systems were usually owned and managed by local and central government authorities. These elements can be summarized as civil infrastructure, municipal infrastructure, or simply referred to as public facilities, although they can operate and develop in both the private sector and in state enterprises.

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
4



1.2. CRITICAL INFRASTRUCTURE

 National Laboratory of Computer Virology – BAS

- The term "critical infrastructure" is used for those elements of infrastructure that if damaged severely or destroyed, would cause serious disruption of the depended system or organization. Storm, flood or earthquake leads to the loss of key transport routes in the cities (e.g. bridges). This can prevent people to evacuate or rescue teams to do their work; these roads can be referred to critical infrastructure. Similarly, online registration systems can be critical infrastructure for airlines.

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
5



 National Laboratory of Computer Virology – BAS

- The notion of infrastructure lies not only on the public sphere and its facilities, but also on the working methods, management practices and policy developments in the direction of interaction between them all on the one hand, on the other - taking into account with the social needs and assuagement of public transport communications (for people and goods), providing drinking water and industrial water, safe waste disposal, energy supply and the need for dissemination of information among the population [2].

[2] Infrastructure for the 21st Century, Washington, D.C., National Academy Press, 1987

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
6



- IT infrastructure is an integral part of critical infrastructures and to achieve an effective protection of these critical infrastructures should primarily ensure the protection of critical information infrastructures from malicious acts caused intentionally or unintentionally.



1.3. SOFTWARE CRITICAL INFRASTRUCTURE

- As software critical infrastructure will note a set of specific software solutions designed to operate and manage the relevant critical information infrastructures.
- In most cases, when talking about infrastructure security is understood security of critical infrastructures such as airports, railway highways, hospitals, bridges, network communications, media, power grid, dams, nuclear reactors, seaports, oil refineries and water systems.



1.3. SOFTWARE CRITICAL INFRASTRUCTURE

National Laboratory of Computer Virology – BAS

Below when talking about the protection of critical infrastructure software will mind the following points:

- protection during the design of the software solution;
- protection during the build of the software solution;
- protection during the test of the software solution;
- protection during the execution of the software solution;

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
9



1.3. SOFTWARE CRITICAL INFRASTRUCTURE

National Laboratory of Computer Virology – BAS

To protect critical software infrastructure must be taken into account following:

- to analyze and identify threats;
- to reduce vulnerabilities in software critical infrastructure;
- to reduce to a minimum the amount of possible injuries;
- to minimize to a minimum the time for reaction while trying to attack, and the time of response reaction and recovery of the caused damages;
- to analyze the causes of damages and the attack source (human action, incorrectly written source code, etc.);

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
10



2. THE CURRENT SITUATION

- 2.1. Information attacks groups
- 2.2. Objects groups
- 2.3. Protection groups



GROUPS OF INFORMATION ATTACKS, METHODS OF PROTECTION AND INFORMATION OBJECTS

INFORMATION ATTACKS

MALWARE

MALATTACKS

METHODS OF PROTECTION

DEPENDING ON
ENVIRONMENT

DEPENDING ON
CLIENT-SERVER ARCHITECTURE

DEPENDING ON
CPU CHARACTERISTICS

INFORMATION OBJECTS

DIRECTLY EXECUTABLE

INDIRECTLY EXECUTABLE



2.1. INFORMATION ATTACKS GROUPS MALWARE

National Laboratory of Computer Virology – BAS

I. BROWSERS	(1) ActiveX; (2) BHO; (3) Cookie; (4) Prefix of URL; (5) Related Info; (6) Scumware; (7) Ticker;
II. METADATA	(8) ADS (Alternate Data Streams); (9) Binder; (10) Downloader (Trojan Downloader); (11) Dropper;
III. CRACKING	(12) Cracking; (13) Password Cracker;
IV. SPYING	(14) Spyware; (15) GUID; (16) IRC Bots; (17) Phishing; (18) Error Reporting Tool; (19) Smart Links; (20) Sniffing; (21) Toolbar; (22) nPnP; (23) WebBug; (24) GSM Pointer; (25) WAP Access Link;
V. DoS, DDoS	(26) Flooder; (27) Mail Bomber; (28) Nuker; (29) Spoofing; (30) Bacterium;

05-06 March 2010,
Sofia, Bulgaria

Dimitrina Polimirova, PhD, NLCV-BAS
Prof. DSc Eugene Nickolov, NLCV-BAS

13



2.1. INFORMATION ATTACKS GROUPS MALWARE

National Laboratory of Computer Virology – BAS

VI. EXPLOITS	(31) Exploit;
VII. SCANNERS	(32) Port Scanner (IP Scanner); (33) Probe Tools; (34) RAT (Remote Administration Tool); (35) Riskware;
VIII. KEYBOARD MODIFIERS	(36) Ansi Bomb; (37) Keylogger; (38) Mouselogger; (39) Screenlogger;
IX. COMPUTER TROJAN HORSES	(40) Computer Trojan Horse;
X. COMPUTER BACKDOORS	(41) Computer backdoor;

05-06 March 2010,
Sofia, Bulgaria

Dimitrina Polimirova, PhD, NLCV-BAS
Prof. DSc Eugene Nickolov, NLCV-BAS

14



2.1. INFORMATION ATTACKS GROUPS MALWARE

National Laboratory of Computer Virology – BAS

XI. COMPUTER WORMS	• (42) <i>Computer worm</i> ;
XII. COMPUTER VIRUSES	• (43) <i>Computer virus</i> ; (44) <i>Logic Bomb</i> ;

05-06 March 2010,
Sofia, Bulgaria

Dimitrina Polimirova, PhD, NLCV-BAS
Prof. DSc Eugene Nickolov, NLCV-BAS

15



2.1. INFORMATION ATTACKS GROUPS MALATTACKS

National Laboratory of Computer Virology – BAS

XII. USING ACCESSIBLE INFORMATION	• (45) <i>Audit Trail</i> ; (46) <i>Traffic Analysis</i> ;
XIV. OVERFLOW	• (47) <i>Buffer Overflow</i> ;
XV. VULNERABILITIES	• (48) <i>CGI (Common Gateway Interface)</i> (49) <i>Packet Attacks</i> ;
XVI. CONTENT	• (50) <i>Content Attacks</i> ;
XVII. DATA ENCAPSULATION	• (51) <i>Data Driven</i> ;

05-06 March 2010,
Sofia, Bulgaria

Dimitrina Polimirova, PhD, NLCV-BAS
Prof. DSc Eugene Nickolov, NLCV-BAS

16

2.1. INFORMATION ATTACKS GROUPS MALATTACKS



National Laboratory of Computer Virology – BAS

XVIII. DENIAL OF SERVICE

- (52) DDoS (Distributed Denial of Service); (53) Flooding;

XIX. SPOOFING

- (54) DNS Spoofing; (55) EFT Spoofing; (56) Ethernet Spoofing; (57) IP Spoofing; (58) Screen Spoofing; (59) SET Spoofing; (60) TCP Dump Spoofing; (61) Trace Route Spoofing; (62) Tunnel Spoofing;

XX. CRACKPASSWD

- (63) HTCrackPasswd;

XXI. ZOMBIE COMPUTERS

- (64) Zombies

05-06 March 2010,
Sofia, Bulgaria

Dimitrina Polimirova, PhD, NLCV-BAS
Prof. DSc Eugene Nickolov, NLCV-BAS

17

2.2. OBJECTS GROUPS DIRECTLY EXECUTABLE



National Laboratory of Computer Virology – BAS

ARCHIVED AND COMPRESSED

- Archived; Compressed; Archived and compressed; Packages; Other (unnamed)

SCIENTIFIC

- Computer-aided design; Electronic design automation; Geographic information system; Signal data objects, non-audio; Financials/Stocks; Chemical file objects;

DATA

- Database; Document/Text file object; Spreadsheet; Tabulated data; Presentations; Page description language;

INTERNET RELATED

- Static web page; Dynamic web page;

BINARIES

- Object code or Object file; Executable objects; Shared and dynamically-linked libraries; Script; Source code for computer programs;

VIRTUAL MACHINE

- Microsoft Virtual PC/Virtual Server
• EMC VMware ESX/GSX/Workstation/Player

OTHER

- Font files; Windows File Objects; Communication File Objects; Printer File Objects; Hardware File Objects;

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
18



2.2. OBJECTS GROUPS INDIRECTLY EXECUTABLE

 National Laboratory of Computer Virology – BAS

GRAPHICS

- *Raster graphic; Vector graphic; 3D graphics;*

MUSIC AND AUDIO

- *Uncompressed audio; Compressed lossless audio; Lossy audio; Playlist objects; Other music file objects;*

MOVIES

- *Video; Video game data; Video game ROM*

25-26 March 2010,
Sofia, Bulgaria

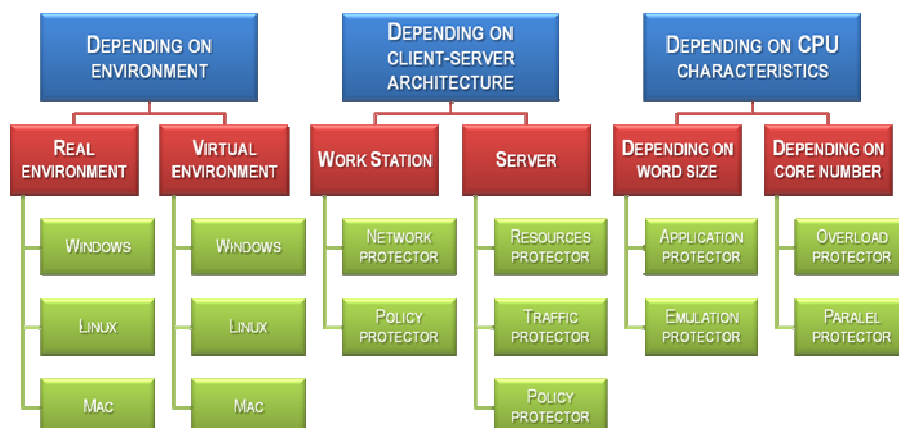
Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
19



2.3. PROTECTION GROUPS

 National Laboratory of Computer Virology – BAS



25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
20



2.3. PROTECTION GROUPS

PROTECTION TYPES DEPENDING ON ENVIRONMENT:

 National Laboratory of Computer Virology – BAS

- In case of **real environment**. It is protected by:
 - real-time memory protectors;
 - real-time registry protectors;
 - real-time media (disk, CD/DVD, flash, etc.) protectors;
- The most commonly used **operating systems in a real environment** and their protection types are:
 - **Windows real environment**. The protectors include:
 - real-time Windows memory protectors;
 - real-time Windows registry protectors;
 - real-time Windows media (disk, CD/DVD, flash, etc.) protectors;
 - **Linux real environment**. The protectors include:
 - real-time Linux memory protectors;
 - real-time Linux registry protectors;
 - real-time Linux media (disk, CD/DVD, flash, etc.) protectors;
 - **Mac real environment**. The protectors include:
 - real-time Mac memory protectors;
 - real-time Mac registry protectors;
 - real-time Mac media (disk, CD/DVD, flash, etc.) protectors;

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
21



2.3. PROTECTION GROUPS

PROTECTION TYPES DEPENDING ON ENVIRONMENT:

 National Laboratory of Computer Virology – BAS

- In case of **virtual environment**. It is protected by:
 - virtual memory protectors;
 - virtual registry protectors;
 - virtual media (disk, CD/DVD, flash, etc.) protectors;
- The most commonly used **operating systems in a virtual environment** and their protection types are:
 - **Windows virtual environment**. The protectors include:
 - virtual Windows memory protectors;
 - virtual Windows registry protectors;
 - virtual Windows media (disk, CD/DVD, flash, etc.) protectors;
 - **Linux virtual environment**. The protectors include:
 - virtual Linux memory protectors;
 - virtual Linux registry protectors;
 - virtual Linux media (disk, CD/DVD, flash, etc.) protectors;
 - **Mac virtual environment**. The protectors include:
 - virtual Mac memory protectors;
 - virtual Mac registry protectors;
 - virtual Mac media (disk, CD/DVD, flash, etc.) protectors;

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
22



2.3. PROTECTION GROUPS

PROTECTION TYPES DEPENDING ON CLIENT—SERVER ARCHITECTURE:

 National Laboratory of Computer Virology – BAS

- On behalf of **Workstation** the following protections can be referred:
 - **Network protector.** These type protections analyze the TCP/IP packets and recognize malware content;
 - **Policy protector.** A user profile, threat assessment and security policy choice is made;
- On behalf of **Server** the following protections can be referred:
 - **Resources protector.** They protect single shared resources (memory, disk, periphery);
 - **Traffic protector.** Protection aims to prevent unusual, abnormal traffic;
 - **Policy protector.** A Work Station's profile is created, a malware content is recognized and correct security policy is chosen for each Work Station.

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
23



2.3. PROTECTION GROUPS

PROTECTION TYPES DEPENDING ON CPU CHARACTERISTICS:

 National Laboratory of Computer Virology – BAS

- Depending on **word size** the following protectors can be observed:
 - **Application protector.** They must be conformable to the application's word size as taking into account the relationship between the operating system and the word size;
 - **Emulator protectors.** These protections include defense against unwanted or incorrectly selected emulations of processes, applications and resources.
- Depending on **core's number** the following protectors can be observed:
 - **Overload protector.** They include protection against overloading of dataflow with respect to one or more cores;
 - **Parallel protectors.** They include protection against malicious or accidental breach of parallel processing of the information by the single cores.

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
24



3. AVAILABLE INFORMATION FOR ACCOMPLISHED ATTACKS

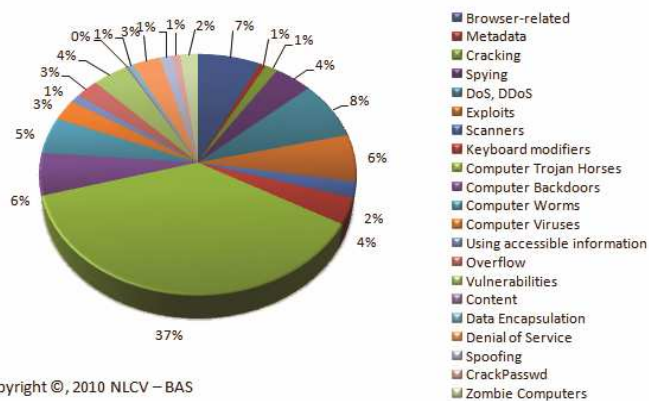
25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
25



PERCENTAGE DISTRIBUTION OF ACCOMPLISHED ATTACKS' GROUPS

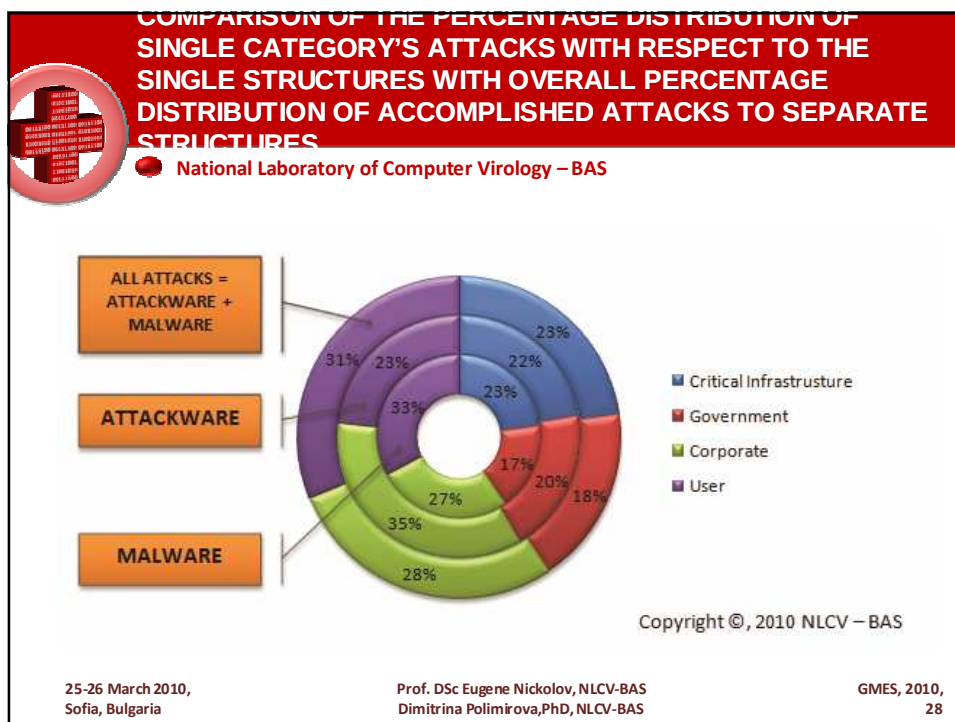
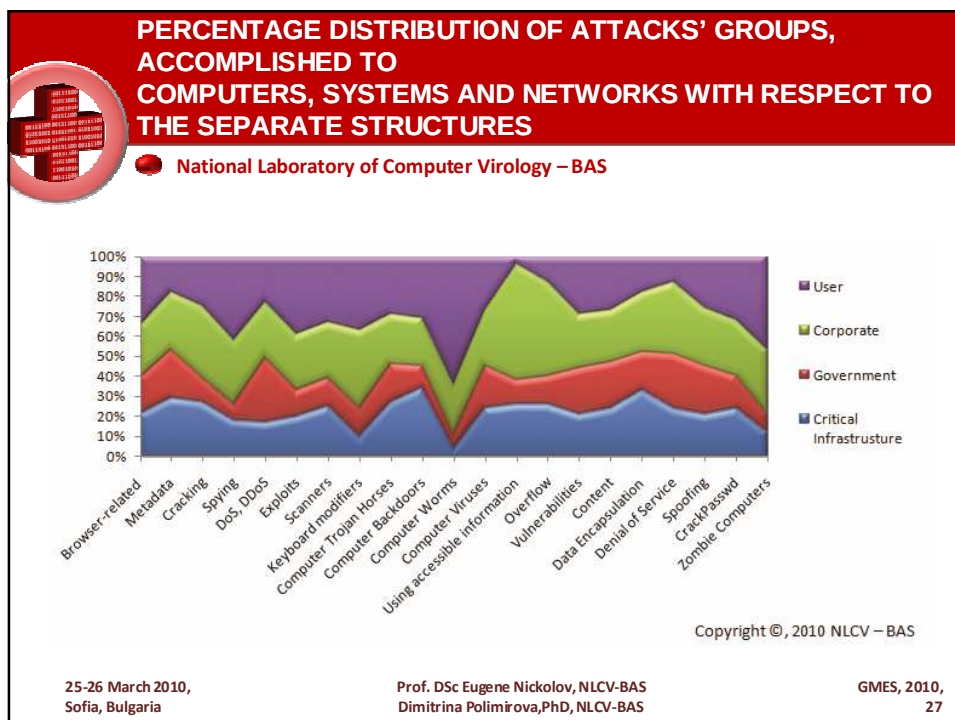


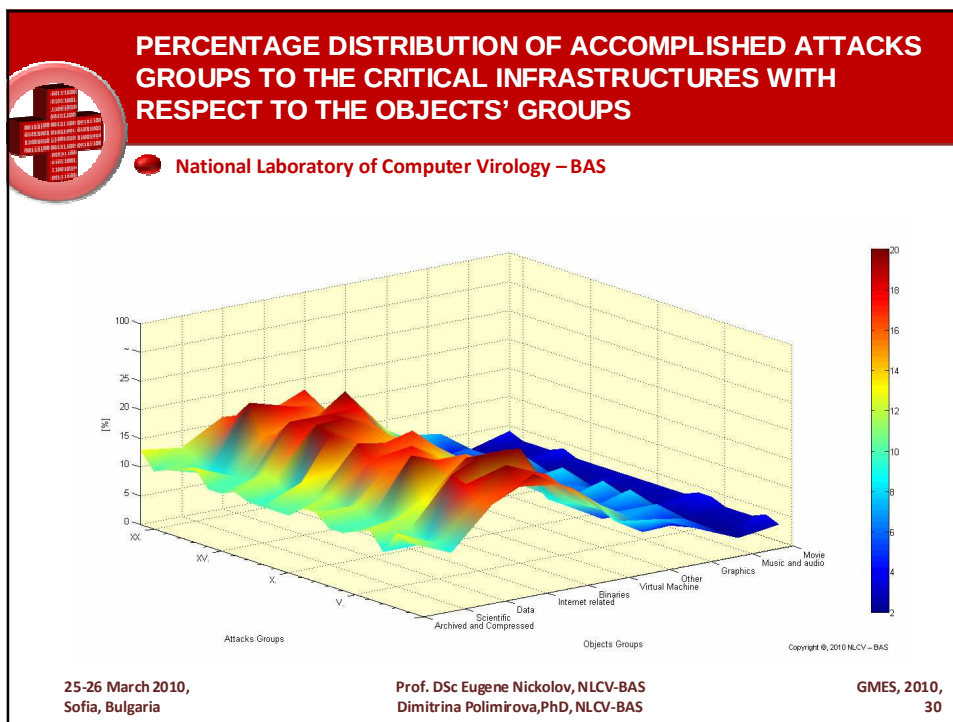
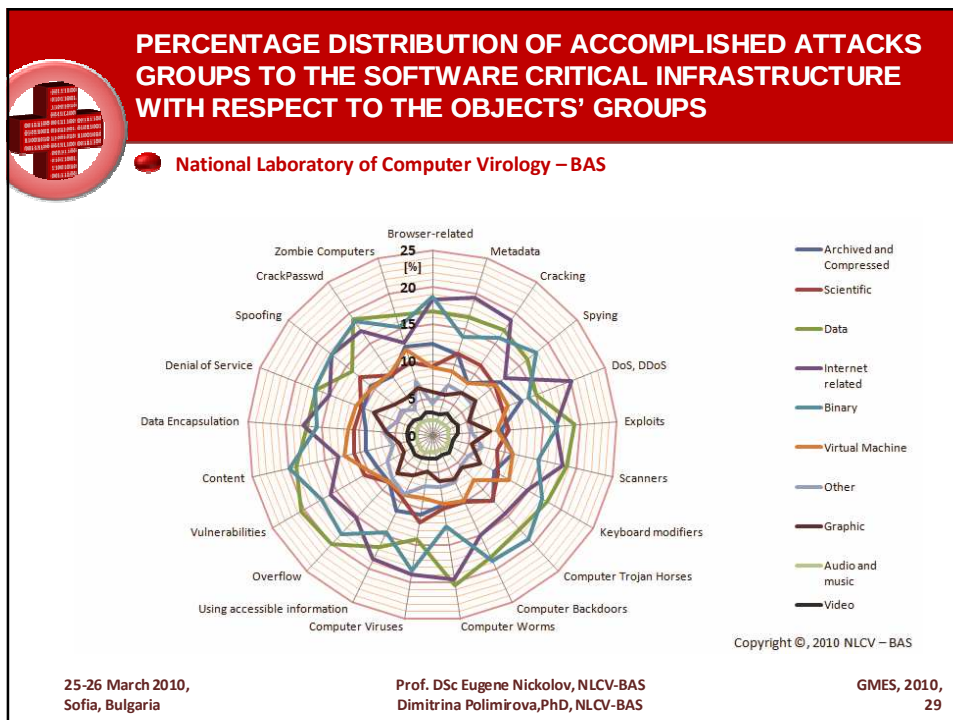
Copyright ©, 2010 NLCV – BAS

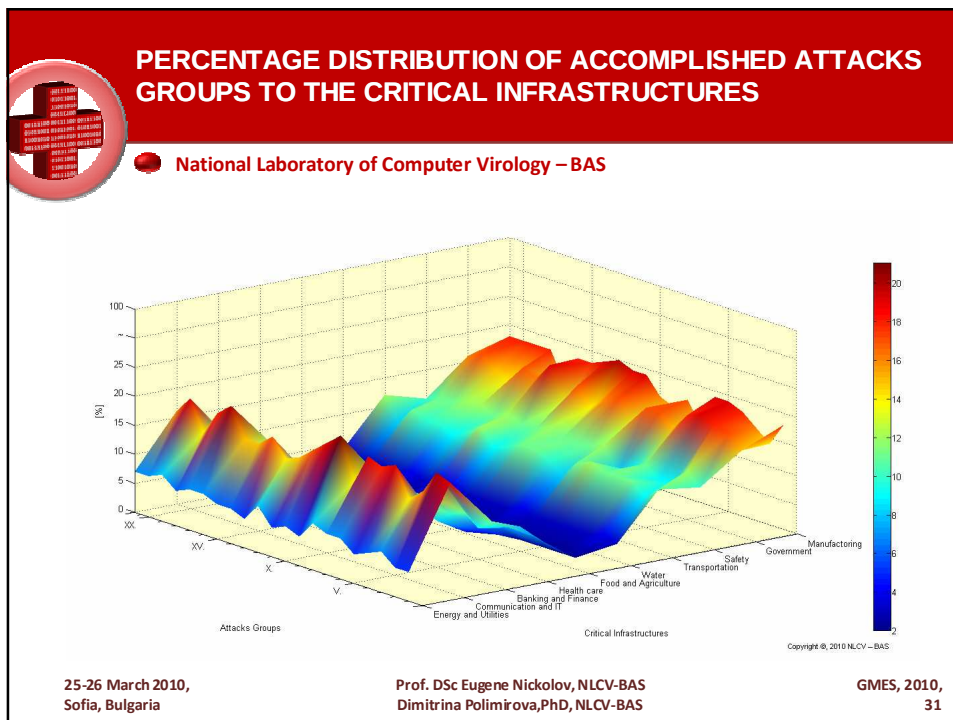
25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
26







 **National Laboratory of Computer Virology – BAS**

4. METHODS OF PREVENTION, PROTECTION AND RECOVERY

- 4.1. Methods of prevention
- 4.2. Methods of protection
- 4.3. Methods of recovery

25-26 March 2010,
Sofia, Bulgaria

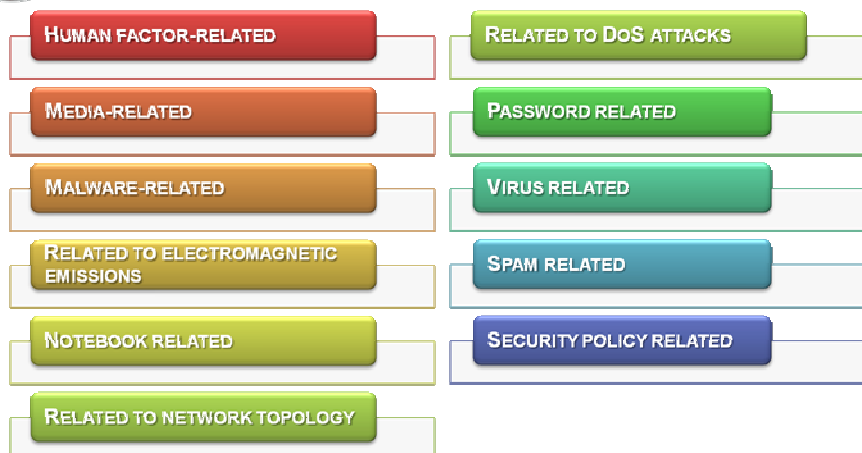
Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
32



4.1. METHODS OF PREVENTION

National Laboratory of Computer Virology – BAS



25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
33



4.2. METHODS OF PROTECTION

National Laboratory of Computer Virology – BAS

BASIC FUNCTIONS

- The problem with absolute malignant software protection is practically impossible to solve but **in order to protect a computer system we have to guarantee**: 1) Intrusion protection; 2) Resource inaccessibility; 3) Inaccessibility of information in the working terminals; 4) Cryptographic protection.

BASIC TASKS

- The **security protection** of a company should **have the following abilities**: 1) Identify the attack; 2) Act on the attack; 3) Discover the attacks; 4) Reflect the attack; 5) Transparent work.

BASIC ELEMENTS

- The methods for computer system protection include the following basic elements: 1) Threat analysis; 2) Access control; 3) Authentication; 4) Confidentiality; 5) Data integrity; 6) Denial inability; 7) System reliability;

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
34



4.2. METHODS OF PROTECTION

National Laboratory of Computer Virology – BAS

BASIC PRINCIPLES

- 1) Smallest privileges; 2) Deep protection; 3) Protection diversity; 4) Default denial; 5) Security by ambiguity.

BASIC METHODS

- 1) Data and file encoding; 2) Methods for server antimalware protection; 3) Methods for workstation antimalware protection; 4) Methods for hoaxes protection; 5) Methods for DDoS attack protection; 6) Methods for protection against e-mail and spam bombings and IP spoofing; 7) Protection against Sniffing; 8) Protection against kernel level Rootkits; 9) Protection against Smurf or Fraggle attacks; 10) Protection against SYN Flood attacks; 11) Protection against DNS attacks; 12) Methods for wireless network protection; 13) Methods for VPN protection; 14) Methods for browser protection; 15) Methods for mobile device protection (laptops, table computers, PDA etc.)

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
35



4.3. METHODS OF RECOVERY

National Laboratory of Computer Virology – BAS

COMMON PRELIMINARY MEASURES

PRELIMINARY MEASURES FOR BIG COMPUTER SYSTEMS

PRELIMINARY MEASURES FOR COMPUTER NETWORKS

COMPUTER INCIDENT REACTION METHODS

COMPUTER SYSTEM RECOVERY METHODS

RECAPITULATION AFTER RECOVERY FROM THE ATTACK

RECOVERY AFTER DoS ATTACKS

POST-VIRUS ATTACK RECOVERY

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
36



5. ASSESSMENTS AND CONCLUSION



ASSESSMENTS

- Sharp **increase the importance of security** for software critical infrastructures.
- Sharp **increase of price in establishing** the software critical infrastructures.
- Sharp **increase in the complexity** of establishing a software critical infrastructures.
- Sharp **increase in vulnerabilities** in the creation of software critical infrastructures.



CONCLUSIONS

 National Laboratory of Computer Virology – BAS

- Need for increased funding, **new methods for reducing the complexity, new methods of reducing vulnerabilities** to ensure adequate security of society in creating software critical infrastructure.

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
39



 National Laboratory of Computer Virology – BAS



THANK YOU!

**PROF. DSC EUGENE NICKOLOV,
CEO,**

PHD, DIMITRINA POLIMIROVA,

National Laboratory of
Computer Virology – BAS

1113 Sofia, Acad. G. Bontchev St., Building 8,
Tel. 359.2.973.3398, Fax 359.2.971.3710,

25-26 March 2010,
Sofia, Bulgaria

Prof. DSc Eugene Nickolov, NLCV-BAS
Dimitrina Polimirova, PhD, NLCV-BAS

GMES, 2010,
40