Prophylaxis for "virus" propagation and general computer security policy

From biology to the real world of men and computers

by **Dr. Daniel GUINIER**

ACM, IEEE, IACR, EDPAA, IIA member

President OSIA, Inc.

and

Computer Security and Quality Department Chairman
Regional Institute for Promotion of Applied Research (IREPA)

Abstract

Viruses propagate easily with **economic consequences** that are difficult to estimate. Appropriate means of prevention, detection and protection are needed to preserve integrity and availability of computer systems. **Prophylaxis effects** first have to be reasearched to provide data for choice of appropriate measures according to the general security policy. Several models for virus propagations borrowed from biology have been developed in the continuous case to indicate that segregation controls imposed by file value increase the population density of virus.This confirm previous experimental results obtained by F. Cohen on personal computers and mainframes.

Uniform virus prevention is highly recommended rather than segregation by file value which is basically the principle of most of centralized packages. Also, security measures offered by most of the resource access security systems are not effective for virus infections which can **pass high security levels when they are introduced by trusted users.** It is suggested to apply a flexible **management prevention program** adapted to environment, men and virus changes in relation with a **normal use of information systems** which have to play their economic and strategic roles without losses.

Two perspectives are suggested. The first makes reference to the **SRI's real-time Inrusion-Detection Expert System** *(IDES)* based on statistical tests for abnormality, considering deviations from an expected behavior. It works for individual as well as group users or remote hosts. The second proposes the use of **neural networks** as another technical solution actually available. It should work for such an anomaly **detection based on behavior segregation** rather than value.

Keywords : *Disease, Intrusion-detection, Management, Organization, Policy, Prevention, Propagation, Prophylaxis, Protection,Virus*

Mailing address : BP 86
F 67034 STRASBOURG Cedex, (France)

1. Introduction

Computer security losses have an unsupportable annual cost in all computerized countries *(e.g. 2 billion dollars in France declared for 1990).* "Virus, worms & Co." are the newest threats composing the different insecurity agents. Although they appear as *"minor risks"* at a macroeconomic dimension, they can be at the origin of a catastrophe for a single organization or company which has underestimated this problem of security.

A computer virus could be defined as a piece of program code able to self-reproduce when riding on other programs and which cannot exist by itself. The choice of the word Self-Reproducing Program *(SRP)* would be better because it appears to be unambiguous in comparison to the word virus which makes reference to biology. **Protection** is possible by a **better understanding of the computer systems** and their mechanisms of exchanges of data and processes but **prevention first needs a better undestanding of men**, ambiguïties and organizations. Such a study has been presented in Guinier D. (1989).

2. Classification of the illicit objects

A classification from the different illicit objets such as viruses, worms, logical bombs and Trojan horses needs to be done to clarify which measures are appropriate. A simple distinction could be made among the different objects in relationship with the presence or not of one of five criteria which are : an **illicit action** (Act), a **threshold** mechanism (Thr), a **transfer** mechanism (Tra), **auto-replication** process (Aut) and **permanence** (Per) in a host program : (Y : Yes / N: No)

	Act	Thr	Tra	Aut	Per
Virus	Y	?	?	Y	Y
Worm	Y	?	Y	Y	N
Logical bomb	Y	?	N	N	Y
Trojan horse	Y	N	N	N	Y

3. General need for a computer virus strategy

Usually computer virus strategies mix the use of **protection** offered by anti-virus software companies and **emergency procedures** in case of virus invasion after identification of the SRP. Virus warfare directly conducted with anti-virus products can be **more or less well adapted**, depending on the virus, the product used and the organization. Most of the time, **prevention should solve the problems** encountered.

Also, there is a real **need for a general virus policy** in terms of management and organization. This policy should include sensibilisation, education, responsabilities, procedures, training and audit. It should **be integrated into the general computer security policy plan** to ensure full **confidentiality**, **integrity** and **availability** of computer systems and data.

Prophylactic measures are those taken to avoid disease and form part of the prevention and cure. Choice of such measures requires theoretical studies on the **propagation** of virus inside a system and on the direct effects of the different measures proposed. The goal of such a study is to verify the correctness of the appropriate treatment before its application so as to avoid inadapted countermeasures or to make a better choice **according the general security policy**. Recall that **security is first a management responsibility** which calls for a real strategy in answer of the temptation to try the last offer technical solution to avoid **false alerts** or **real lacks of security**. The benefit of this action will be a higher degree of assurance that the information systems will play their **role in the overall strategy in an organization.**

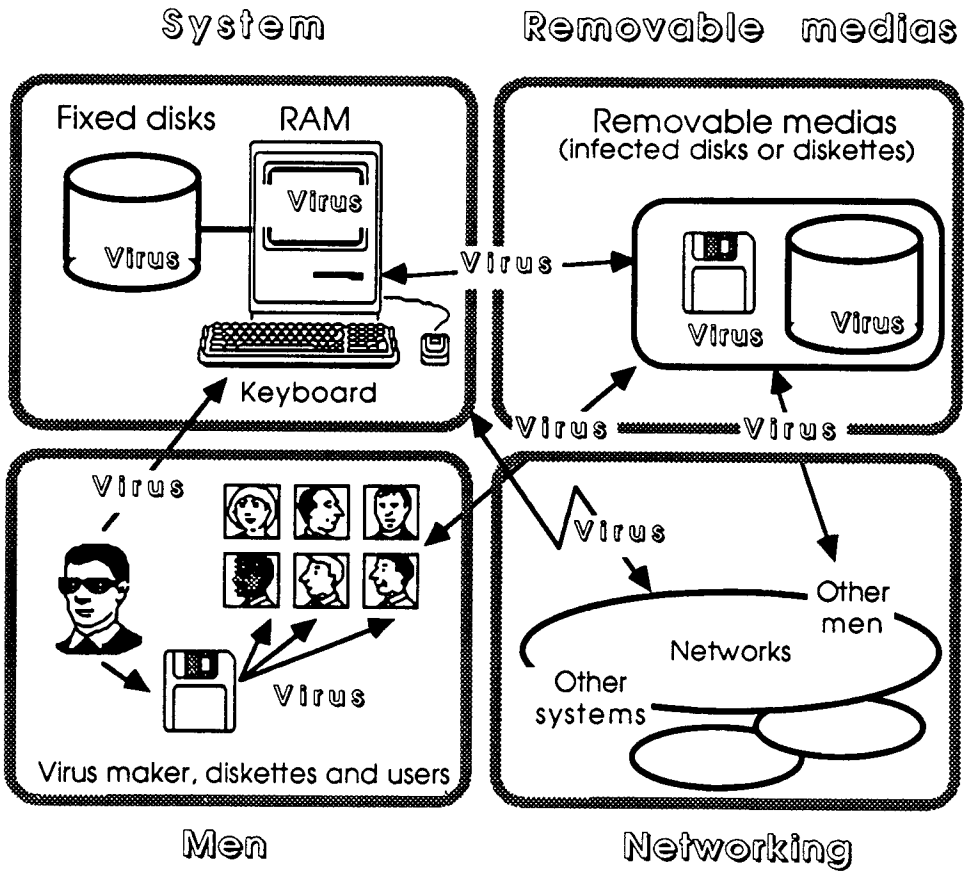
4. Virus propagation mechanisms

External and internal propagations should be distinguised. External propagation consists of entering from one system or media to another and, internal propagation evolves inside a system or media.

> ***Propagation*** *refers to the multiplication or a progression by expansion*
> ***Contagion*** *refers to the transmission from an infected entity to another, originally uninfected*
> ***Contamination*** *is the action which permits the infection*
> ***Infection*** *refers to a penetration inside a system and resulting troubles, caused by a* ***contamination****.*

As expressed in the different definitions : external propagation refers more to contagion and, propagation is the general word referring the mechanism of expansion whether the reference is to an external or to an internal model.

Fig.1 : External propagation : A physical model

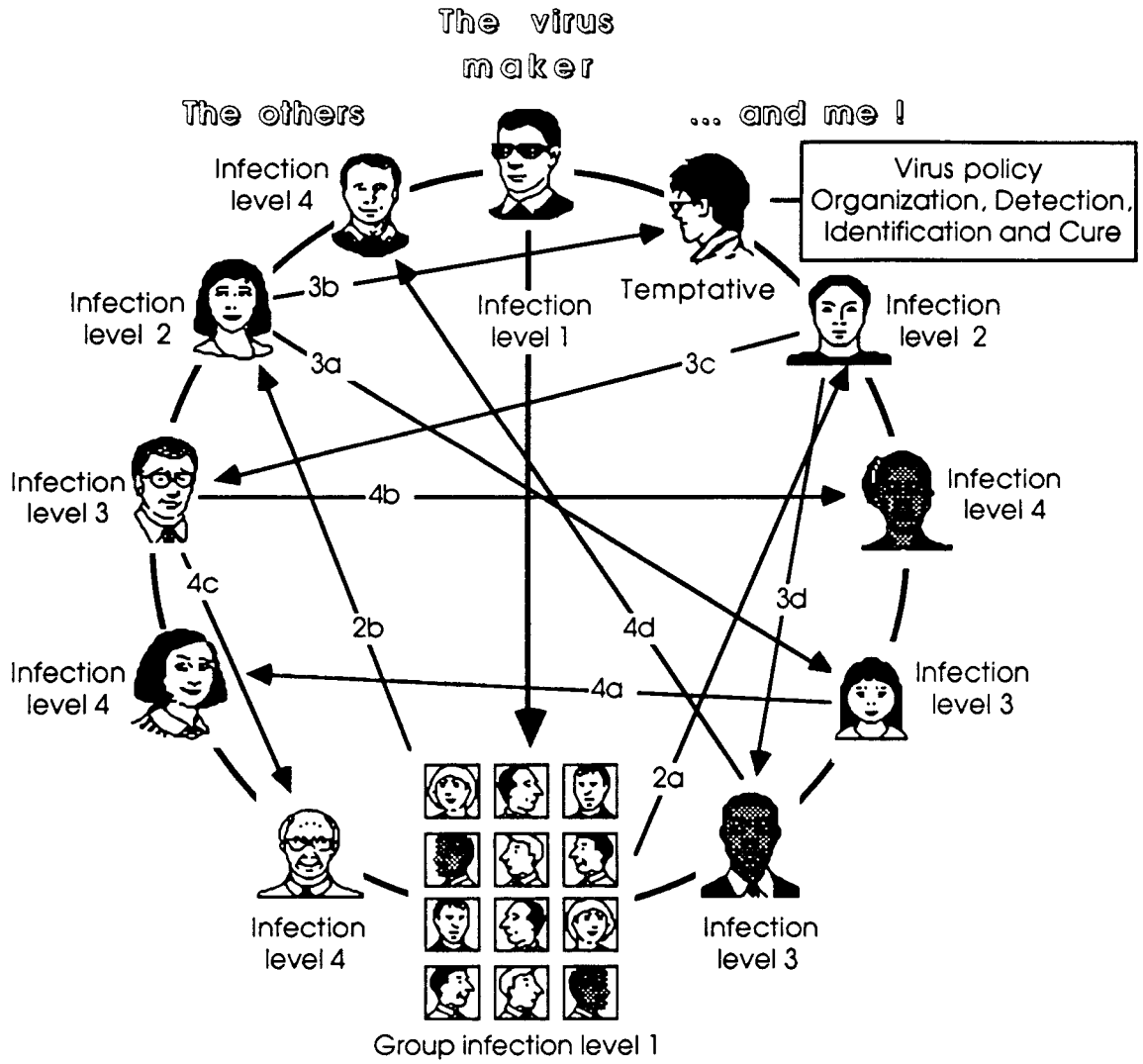


4.1. External propagation

Mechanisms of external propagation are linked with **the environment** and can involve **macroeconomical consequences** through a **vector of infection** :

Infected diskette exchanges	*(infected copy exchanges, freeware, software, ...)* *(e.g. A very recent occurrence in France concerned 70000 diskettes sent by Soft&Micro, a computer newspaper, including the 4096 virus alias Frodo ! (source : Stratégie Sécurité no.3, May, 1991)).*
Networking	*(infected file exchanges, electronic bulletin board,...)*
Sabotage	*(malicious behavior, unhappy or ex-employees, competitor, ...)*

Fig. 2 : External propagation : *"The virus maker, the others and me !"*



Number of infected sites by "one-to-two" contamination <= $2^{\text{Number of levels}}$

External propagation is easy...

According to Mr. Miao Daoqi, from the Peoples Republic of China, at the Helsinki meeting, June 1990, 50 % of the micro computers have been infected by the "Jerusalem virus", *(some few others by Vienna, Brain and Yankee-doodle,coming from Bulgaria).* Because of the low level of priority given to this problem, around **125,000 microcomputers** have been infested ! A uniform propagation from one-to-two requires less than **17 levels of exchanges** for this case of contagion.

... and economic consequences are difficult to estimate !

The 2 November 1988 Internet worm losses have been evaluated at **0.2 million** dollars by G. Spafford from Purdue University, less than **10 millions** by C. Stohl and less than **96 millions** according to J. McFee from the Computer Virus Association! Also, a method of risk evaluation especially dedicated to virus threads would be a very efficient tool to help in decision-making. In this case, it is necessary the evaluate the system and its environment *(customers, suppliers, competitors, ...).*

4.2. Internal propagation

Internal propagation begins after the virus has been introduced inside the system. Mechanisms for internal propagation are linked to the **dynamics of the homogeneous population** of viruses present in the system or on the disks. These mechanisms involve more complex interactions depending on the characteristics of :

The virus
The files to be infected after activation (load and execute function)
The infected files
The measures in place playing the rôle of the ***virus predator***

However, real-world problems such as those involving virus propagation, interactions with security measures and men **are never completely continuous but combine different continuous and discrete situations** *(e.g. Illicit action from the virus which makes the system unavailable).* Fundamental interactions can occur between continuously and discretly changing states such as a continuous state achieving a threshold value may cause a discrete event to occur or a discrete event can cause a discrete change in the value of a continuous state variable. In this essay on dynamics of computer virus populations. We now consider a continuous model of competition between the virus population inside the system and the security measures. This theoretical essay will be **useful for a better understanding** of the propagation dynamics.

5. Essay on the dynamics of computer virus population

There is an immediate possible transcription of biological mechanisms to the evaluation of the dynamics of computer virus populations. All the laws applied here will be derived from biology for homogeneous virus population and issued from the law of mass action. The law of mass action says that the rate of interaction is a direct function of the product of the concentrations of the interfaced reagents involved in the kinetics reaction*(programs and virus).* The population needs to be considered as homogeneous and described by a single variable representing the population density. By analogy with the law of mass action, it is also assumed that the rate at which objets interact with each other by competition, parasitism or predation is a direct function of the product of the densities of populations involved.

Fig. 3 : Internal propagation model and different concerns in the real world

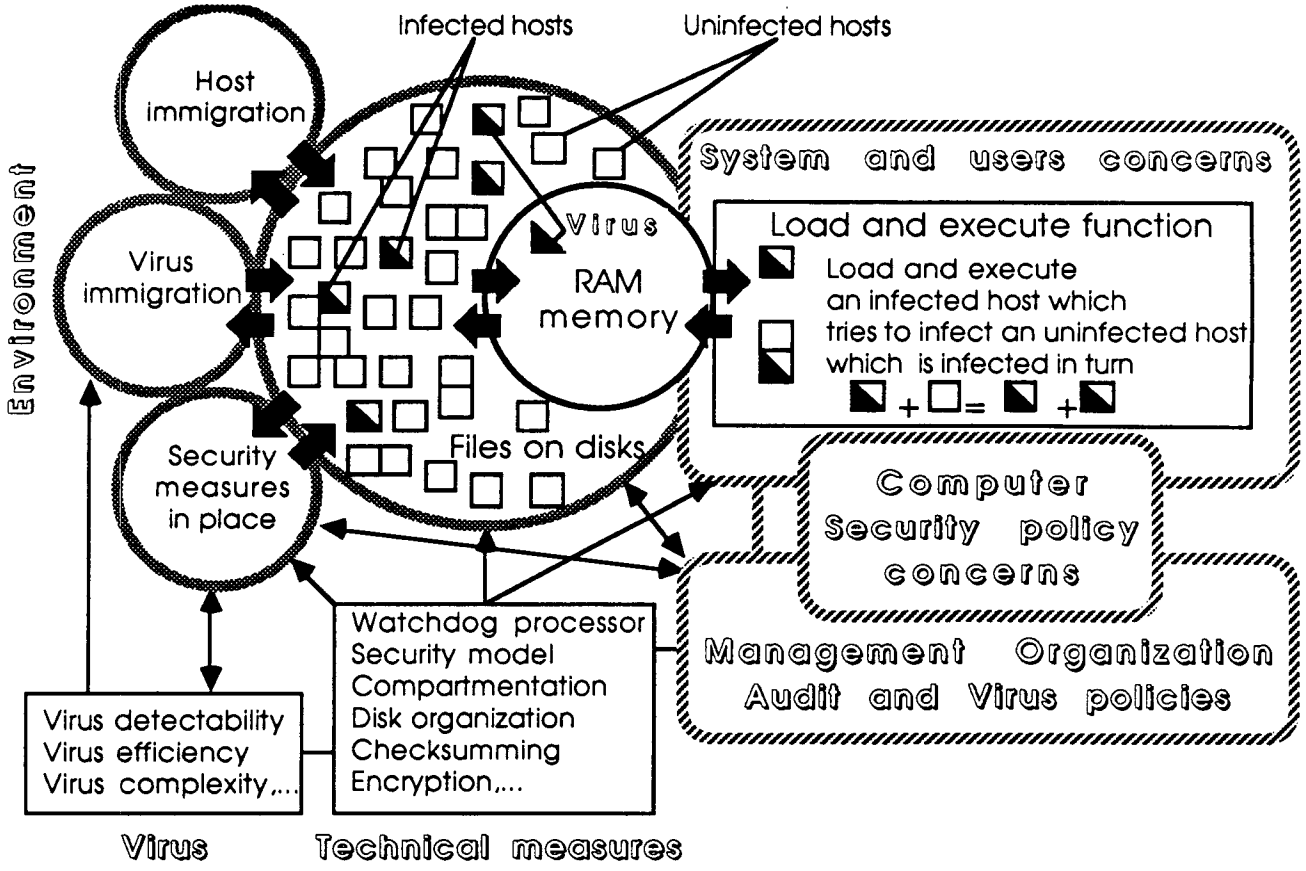
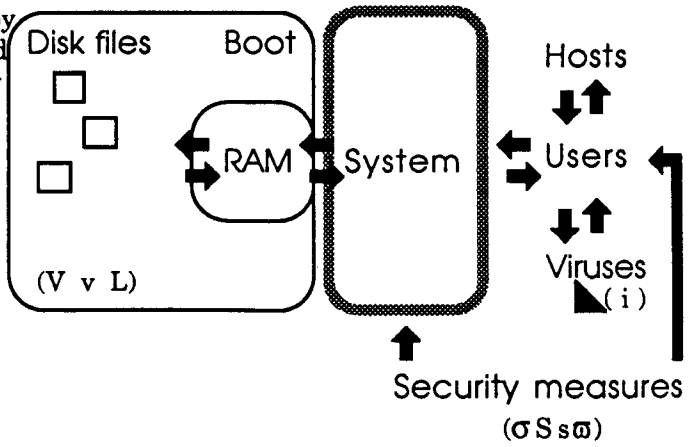


Fig. 4 : Proposal for a simplified logical model applied to the present essay

σ	Efficiency of security measures represented by ratio security measures/nbr viruses destroyed
ϖ	Number of virus to security carrying capacity
i	Immigration rate of virus inside the system
L	Virus population natural density limit also named the carrying capacity
s	Intrinsic rate constant for security measures
S	Security measure density
v	Intrinsic virus net growth rate constant
V	Virus population density



5.1. Virus propagation in an unlimited system

In a theoretically unlimited environment, the growth rate of a virus ***(uninhibited model)*** is expressed by $dV/dt = k.V$ or $\mathbf{dV/dt = v.V/L}$ when $k=v/L$. It is possible to rebuild the equation for the "J-shape" population growth curve by a single integration :

$$Vt = Vo.e^{vt/L}$$

5.2. Virus propagation in a limited system

While in a limited environment, the growth rate of a virus ***(inhibited model)*** is expressed by $dV/dt = k.V.(L-V)$ or $\mathbf{d\,V/dt = v.V.(\,L-V)/L}$ when $k=v/L$. It is also possible to rebuild the equation for the "S-shape" sigmoïd population growth curve by integration :

$$Vt = Vo.L / (Vo + (L - Vo.e^{-vt}))$$

the equation corresponds to the **Verhulst-Pearl model** proposed by Verhulst (1938) and developped by Pearl. It is also called the *"logistic model"*. The growth rate dV/dt can be rewritten under more typical forms such as :

if $k=v/L$

$$dV/dt = k.V.(\,L-V\,) \quad (1)$$
$$dV/dt = v.V.(\,L-V\,) / L \quad (2)$$
$$\mathbf{dV/dt = v.V - v.V^2/L} \quad (3)$$

Comments on equation (3) $dV/dt = v.V - v.V^2/L$:

the first part	$v.V > 0$	corresponds to the uninhibited model *(dV/dt = k.V)*
the second part	$-v.V^2/L < 0$	is a function of V-square. It corresponds to a loss resulting from a "**crowding effect**" of virus in interaction one on another.

The **virus population density approaches** to steady-state equilibrium conditions in which the increment is exactly balanced by the negative feedback part which is a density dependent decrement. **Interpretation of the "crowding effect"** can be either as an increase of the mortality rate or a decrease in the virus apparition rate. A decline of the population size of the uninfected host programs cause a decline in the rate of infection.

5.3. Introducing security measures in the system

While introducing a "**virus predator**" which is represented by **security measures** in a **limited environment**, the virus growth rate ***(inhibited model with predator)*** is expressed by the two equations proposed by Leslie and Gower (1960) :

$$dV/dt = v.V.(\,1 - V/L - \sigma.S\,) \quad (4)$$
$$dS/dt = s.S\,.\,(\,1 - S/(\varpi.V)\,) \quad (5)$$

The "mortality" term of the equation is in part $(\,1 - S/(\varpi.V))$. At equilibrium :

$dV/dt = dS/dt = 0$, also : $\quad v.V.(\,1 - \sigma.S\,) - v.V^2/L = s.S - s.S^2/(\varpi V)$

In this case predator and virus are dependent on each other, and the predator is self-reproducing. It could be a kind of *"virus anti-virus"* corresponding to advanced automated security measures. In reality, only equation (4) will be considered, with the last term represented by the *"predation term"* issued from a supposed constant **security measures** flow.

5.4. Introducing virus immigration

Equation (4) can be rewritten as : $dV/dt = v.V.\ (\ 1 - V/L - \sigma.S\ ) + i$, while including a last term **i** to represent the **immigration rate of virus from outside the system**. At equilibrium :

$$v.V.\ (\ 1 - V/L - \sigma.S\ ) + i = 0$$

that is : $\mathbf{V = i\ /\ v.(\sigma.S - (1 - V/L))}$ (6) implying $\sigma.S - (1 - V/L) > 0$ that is : $\sigma.S > 1 - V/L$

6. Effects of prophylaxis based on value segregation

Equal high level of security in all the parts of a system is costly and classification of the resources (objects) and the people having authorization for access these resources (subjects) make part of some risk analysis methodologies. Results issued from such methodologies can be used for a better understanding of the system in use and to help decision making to establish parameters of the operating system or the resource access and control facilities system in use, **under management responsability**. We have to see the consequences for such a segregation involving viruses.

New threats created by new enhenced viruses force the system to be out from the equilibrium situation and need new security measures. Some decisions are in relationship with **some arbitrary choice** for the organization mostly based **on segregation by file value**. When virus propagation is considered as continuous, parameters attached to security measures (σ,**S**) and to virus propagation (v,V) are assumed to be random variables due to this decision. Such a consideration of eventual **variations involve a bias** in the expected value for V.

Introducing the term Δ corresponding to the bias between the expected value for V at the equilibrium (**E**) and the average value **V**, we have :

$$\mathbf{E}\ (1/V) = 1/\mathbf{V} + \Delta$$

that is : $1/\mathbf{V} = v.(\sigma.S - (1 - V/L))/\ i\ - \Delta$ which can be rewritten as :

$$\boxed{\mathbf{V = i/\ (v.\sigma.S - (v.(1 - V/L) + i.\ \Delta))}}$$

to show that the **average virus population density** (V) **will increase while security measures are segregated**. And, as suggested by S.K.Jones, C.E. White (1990) using a simplified model, the covariances of V and the security parameters are inversely related : $Cov\ (V) \approx Cov\ (1\ /\ s)$. In this case, **the density of virus will be in the inverse progression to the degree of segmentation among files**.

7. Conclusion

Considering these first results limited to continuous models, the approximation in the propagation of virus : **a uniform virus prevention could be highly recommended rather than segregation**. Also, security measures offered by most of mainframe protection systems and resource access and control security systems *(ACF2, MULTICS, RACF,...)* **are not effective for virus infections** which can pass high security levels! when they are introduced by the least privilege user *(which is normally considered as the "most dangerous")* **as well by trusted** *(and highly trusted)* **users**. In this case, a virus could be also considered as another category of user*(unauthorized)* introduced by an authorized user. This confirm experimental results presented by F. Cohen (1988) for personal computers and mainframes.

8. Actual solutions

It might be suggested to apply a **management prevention program** based on **organizational policy** in relation with education, economic consequences, technical measures and **normal use of information systems** which have to play their economic and strategic roles without losses. Also, a flexible strategy for adoption of **combined countermeasures mixing prevention and protection** will be adapted to the **changing nature** of "virus & Co", **men** and **environment**.

Knowledge on viruses using databases for **investigation** (D. Guinier (1989b)) or **classification** (K. Brunnstein (1989)), **viruses description languages** such as the Threat Description Language for Viruses (TDL/V) (M.G. Swimmer (1990)) from the VTC (Virus Test Center (Hamburg) created by K. Brunnstein)) and virus/anti-virus products evaluations (Highland J. (1990)) **contribute to the overall approach** and give enough detail **to identify** possible virus attacks.

Policy models dedicated to virus threats need to be developed and implemented. Software **fault tolerance systems** could be also employed. Various additional solutions are presented in the following bibliography (G.I.Davida, V.G. Desmedt, B.J. Matt (1989), D.E. Denning (1987), R.M. Greenberg (1989) and A. Mahmood, E.J. McCluskey (1988)).

9. Perspectives using segregation by behavior

The SRI International's real-time Inrusion-Detection Expert System (IDES) (H.S. Javitz, A. Valdes (1991)) has been designed to observe behavior on a monitored system and to **learn adaptively what is "normal" for an individual as well as group users and remote hosts**. In fact, IDES maintains a statistical profiles database corresponding to the description of subjects behavior *(frequency tables, means, and covariances)*. An observed behavior will be flagged as a **potential intrusion** if it triggers a rule in the expert-system rule database. The deductive process is based on statistics controlled by adjustable parameters, specific for a given subject. The statistical knowledge is automatically updated every day and IDES learns subjects' behavior patterns. Such an experimental **anomaly detector** based on statistical tests for abnormality considering deviations from an expected behavior could be applied **in the case of a virus attack**. because there is nor segregation by object nor by subject value but only by behavior deviation. This direction should be very promising because it is also *"adapted to changing nature of virus & Co, men,...".*

Because of the analogy of such patterns and those encountered in others areas, **we hardly think that neural networks should be another technical solution actually available.** It is easy to experiment and efficient to implement when used with multi-transputeror neurons boards. Considering the learning process made in parallel and, outside from the original system, it should not decrease performance of the computer system. Neural networks are efficient for classification, they could work for such an **anomaly detection based on behavior classification**.

10. Bibliography

Brunnstein K. (1989) : Zur Klassifikation von Computer-Viren : Der "Computer Virus Catalog", Proceed of the 19th. German Computer Science Association, Ann Conf.

Cohen F. (1988) : On the implications of computer viruses and methods of defense. Computer & Security. Vol.7, pp.167-184.

Davida G.I., Desmedt Y.G., Matt B.J. (1989) : Defending Systems Against Viruses through Cryptographic Authentification, IEEE Symposium on Security and Privacy, May 1-3rd., Oakland, Proceedings, pp.312-318.

Denning D.E. (1987) : An Intrusion-Detection Model, IEEE Trans Soft Eng., Vol. SE-13, No. 2., pp.222-232.

Greenberg R.M. (1989) : Flu_shot+ (TM) : Anti-Trojan / Anti-Virus Protection, Version 1.6, January, Software Concepts Design.

Guinier D. (1989) : Biological *versus* Computer Viruses, A better understanding for a better defense. ACM SIGSAC *REVIEW*, Special Interest Group on Security Audit and Control. Vol.7, No.2, pp.1-15.

Guinier D. (1989 b) : Proposal for a "C-Virus" database dedicated to SRP's, Worms, Trojan horses,... ACM SIGSAC *REVIEW*, Special Interest Group on Security Audit and Control. Vol.7, No.3, pp.13-16.

Highland H.J. (1990 : Computer virus handbook. Elsevier Advanced Technology. pp.1-375.

Javitz H.S., Valdes A. (1991) : The SRI IDES Statistical Anomaly Detector. IEEE Symposium on Security and Privacy, May, Oakland, to appear in the Proceedings (11 pages).

Jones S.K.,White C.E. (1990) : The IMP model of computer virus management. Computer & Security, No.9, pp.411-418.

Mahmood A., McCluskey E.J. (1988) : Concurrent Error Detection Using Watchdog Processors - A Survey, IEEE Trans Comp, Vol. TC-37, No. 2., pp.160-174.

Swimmer M.G. (1990) : Response to the Proposal for a "C-Virus" database.ACM SIGSAC *REVIEW*, Special Interest Group on Security Audit and Control. Vol.8, No.1, pp.1-5.