ARE WIDELY USED SECURITY SYSTEMS INADEQUATE?

G. Futschek, Chr. Weninger

Institute for Software Technology, Vienna University of Technology
A-1040 Vienna, Resselgasse 3, Austria

Abstract. The aim of any security system is the prevention of unauthorized access to or use of data or programs. To circumvent any security measure specific knowledge about the functionality of the attacked system is essential. Since the information on the functionality of popular and widely used computer systems is accessible, these systems are the primary target for security attacks. The usually higher effectiveness (e.g. cost, compatibility, reliability etc.) of widespread systems is decreased by loss of security. Consider e.g. the widespread PCs and the enormous security efforts that are required to prevent virus infection and to recover data. A dynamic model was created to calculate the correlation between security, effectiveness and the degree of distribution. It shows that it is better to provide specific security systems for each user, even if these systems are relatively simple, than to provide all users with a single very sophisticated system.

Keywords. data security, security systems, trusted systems, computer viruses, virus epidemology

INTRODUCTION

An extensive increase in system penetration indicates that there is no perfect software system to prevent such attacks. Therefore it is necessary to realize that only the efforts to penetrate these systems vary. Specific knowledge of protection measures is an obvious prerequisite to the security violation effort. The probability of successfully attacking a security system is usually higher for a widely used popular system than for a specific system used in few computers. Hence the question arises whether or not a sophisticated standard security system is preferable to rather simple but specifically designed systems.

Data stored in computers are threatened by the loss of

- data confidentiality
  = unauthorized access to information
- data integrity
  = unauthorized modification of information
- data availability
  = unauthorized impairment of system functionality

(Zentralstelle für Sicherheit in der Informationstechnik, 1989).

Several technical and organizational methods are applicable to prevent the loss or modification of data. Organizational procedures like

- training and informing employees
- forming a group of security specialists
- consulting independent specialists

are always necessary. They supplement technical measures like the

- use of security software (i.e. encrypting methods)
- use of biometric systems (i.e. finger prints, retina check)
- use of other electronic surveillance systems (i.e. chip-card based systems)

Most of these technical methods are very cost intensive, biometric systems in particular, so that only few people will derive benefit from them. Since the application of security software has evolved to become the most commonly used technique to protect data, it will be given special attention in this paper. First of all it has to be understood that there is no possibility, no matter what measures are applied, to build a system which is absolutely secure.

Unauthorized modification of protected data requires specific knowledge about the structure of the system protection mechanism. Hence, attacking a widely used popular system is more likely to succeed than trying to beat a specifically designed system. In the following we will come to the conclusion that applying a single highly sophisticated protection system for all users is not as effective as providing each user with a specific and even simple system.

A serious threat, of which PC users especially have become aware of recently, is caused by computer viruses. A virus is defined in Cohen (1987) as

'a program that can infect other programs by modifying them to include a possibly evolved copy of itself.'

Virus infection causes the loss of data integrity and data availability. Only the execution of an infected program can increase the number of infected programs or systems. In order to prevent virus infection, program modifications have to be detected as soon as possible. A security program that runs in the PC-Dos environment was developed by the authors, which is able to detect unauthorized modifications of data and programs (Weninger, 1991). A test of this system in a virus-infected environment showed its resistance against any security attack, but a good knowledge of the internal structure of this specific security system would make successful violations possible.

Assuming that a virus is intended to make use of a specific flaw in a protection mechanism (which means that the virus can only penetrate systems employing the same protection mechanism), it has to be realized that, if it was intended by the programmer of the virus to infect as many systems as possible, he would certainly have chosen to attack a widely used security system. If every user employs a specific security system, virus propagation will be almost impossible. The following models will describe the correlation between security, effectiveness and the degree of virus propagation.

UNRESTRICTED VIRUS PROPAGATION

The basic model on virus propagation considers the number of infected and clean systems and the probability of virus infection.

x ... rate of currently infected systems ($0 \leq x \leq 1$)
$1 - x$ rate of clean systems
a ... probability of infection of a clean system

The rate of infected systems increases proportional to the probability that a clean system will become infected by exposure to an infected system. This result is the well known differential equation for unrestricted virus propagation (Solomon, 1990; Murray, 1989)

$$dx/dt = a(1-x)x \qquad (1)$$

with the solution

$$x(t) = x_0 / (x_0 + (1 - x_0)\, e^{-at}) \qquad (2)$$

The rate of infected programs tends to 1 (the state when every system is infected) from every starting point $x_0 > 0$.

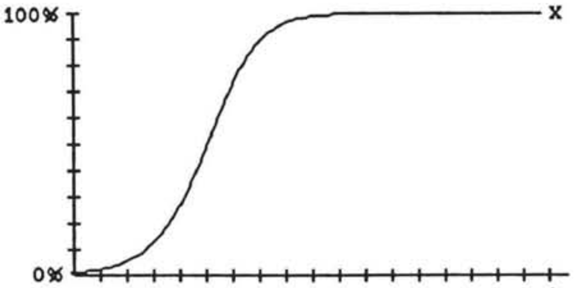

Fig. 1 Model (1), $a = 0.1$, $x_0 = 0.01$

If we assume that viruses are detected and removed from some systems, the virus propagation is reduced by a term which is proportional to x.

$$dx/dt = a(1-x)x - ex \qquad (3)$$

e ... probability of detection and removal

The function $x(t)$ tends to 0, if $e \geq a$ (see Fig. 2). Otherwise $x(t)$ tends to $1 - e/a$, so the probability that a system is clean tends to e/a (see Fig. 3).

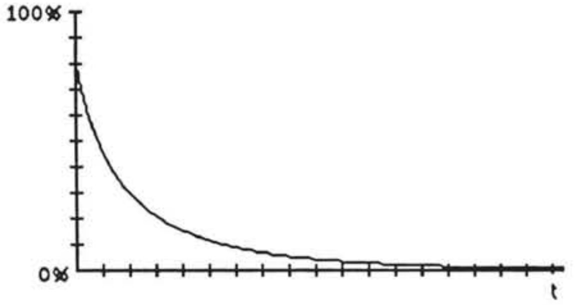

Fig. 2 Model (1), $a = 0.05$, $e = 0.07$, $x_0 = 0.8$
Countermeasures beat the virus infection

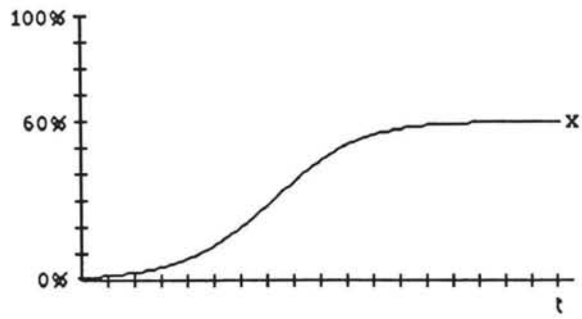

Fig. 3 Model (1), $a = 0.1$, $e = 0.04$, $x_0 = 0.01$
60% of all systems remain infected

USE OF A PERFECT PROTECTION SYSTEM

Now we assume that we use perfect protection systems, that make any virus infection impossible.

y ... rate of currently protected systems ($0 \leq y \leq 1$)
p ... probability of newly protecting an unprotected system

The infected and protected systems are disjoint ($0 \leq x \leq x + y \leq 1$).

$1 - x - y$ ... rate of not protected and clean systems

The increase of protected systems is proportional to the rate of infected systems x.

$$dy/dt = p\,x \tag{4}$$

The number of protected systems y increases by the protection of not infected $(1 - x - y)$ or infected systems.

$$p = d\,(1 - x - y) + e \tag{5}$$

d ... probability of newly protecting a clean system
e ... probability of newly protecting an infected system

$$dx/dt = a\,(1 - x - y)\,x - e\,x \tag{6}$$

$$dy/dt = d\,(1 - x - y)\,x + e\,x \tag{7}$$

We assume that every time a system is newly protected all viruses are removed. Therefore the term $- e\,x$ is added to (6).

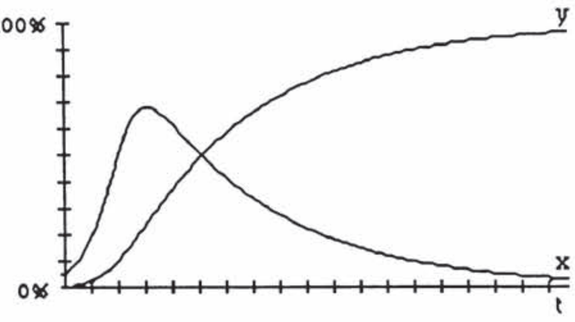

Fig. 4 Model (6, 7), $a = 0.2$, $d = 0.01$, $e = 0.02$
$x_0 = 0.05$, $y_0 = 0$

We see that all systems will be protected (y converges to 1 whenever $d > 0$ and $e > 0$ holds) and no virus will remain.

If we reduce the number of protected systems whenever the number of viruses decreases, we will get the following differential equation system:

$$dx/dt = a\,(1 - x - y)\,x - e\,x \tag{8}$$

$$dy/dt = d\,(1 - x - y)\,x + e\,x - c\,(1 - x)\,y \tag{9}$$

$c\,(1 - x)$ ... probability of removing a protection system

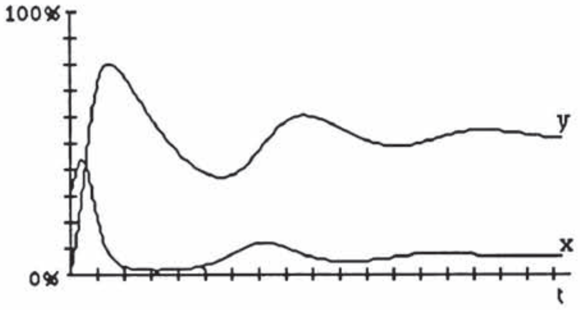

Fig. 5 Model (8, 9), $a = 0.5$, $c = 0.03$, $d = 0.02$
$e = 0.2$, $x_0 = 0.3$, $y_0 = 0$

The behavior of this system is similar to a predator-prey model. A decrease of the virus rate reduces the number of protection systems, so that the viruses can spread again, which increases the rate of protection systems again.

NOT PERFECT PROTECTION SYSTEMS

No virus protection system is perfect. If the virus knows the specific protection procedures it can circumvent the system or misuse the procedures for its own purpose. In order to model this situation, we add a third variable z and a factor b to model (8, 9).

z ... rate of protected but infected systems
b ... probability of infection of a protected system

Usually b has a smaller value than a. We have

$y - z$ ... rate of protected & clean systems
$x - z$ ... rate of not protected & infected systems
$1 - x - y - z$ ... rate of not protected&clean systems

$$dx/dt = a\,(1 - x - y - z)\,x + b\,(y - z)\,x - e\,(x - z) \tag{10}$$

$$dy/dt = d\,(1 - x - y - z)\,x + e\,(x - z) - c\,(1 - x)\,y \tag{11}$$

$$dz/dt = b\,(y - z)\,x \tag{12}$$

Equation (12) says that z increases proportional to the probability that a protected and clean system becomes infected by exposure to an infected system. This amount must also be added to (10).

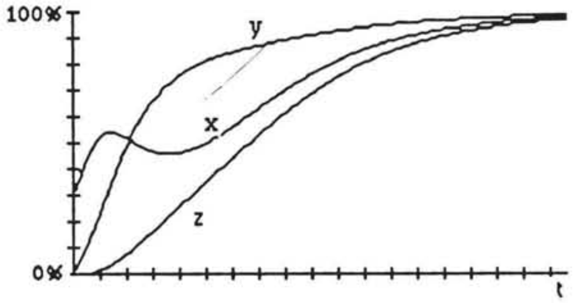

Fig. 6 Model (10-12), a = 0.2, b = 0.04, c = 0.01, d = 0.02, e = 0.05, x_0 = 0.3, y_0 = 0, z_0 = 0

All protected systems become infected in this example. The existence of some infected systems increases automatically the number of protected & infected systems.

The use of a protection system may make the detection and removal of viruses easier, so that some of the protected & infected systems will become clean. This can be modeled by a term – f z which is added to (10) and (12).

f ... probability that a protected & infected system is cleaned

$$dx/dt = a(1-x-y-z)x + b(y-z)x - e(x-z) - fz \quad (13)$$

$$dy/dt = d(1-x-y-z)x + e(x-z) - c(1-x)y \quad (14)$$

$$dz/dt = b(y-z)x - fz \quad (15)$$

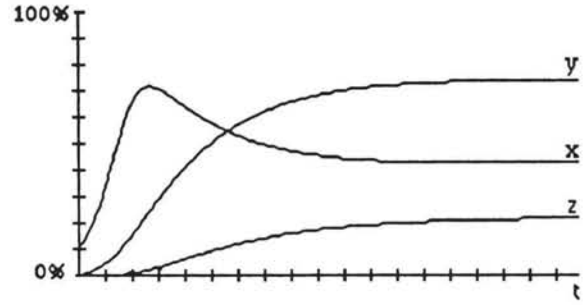

Fig. 7 Model (13-15), a = 0.2, b = 0.02, c = 0.01, d = 0.01, e = 0.02, x_0 = 0.1, y_0 = 0, z_0 = 0

The behavior of this system is equivalent to the use of a widespread but not perfect protection system.

A widespread protection system is only sufficient, if it is perfect. Otherwise it can only slow down virus propagation.

DIFFERENT PROTECTION SYSTEMS

The basic idea: Every virus makes use of a specific flaw of a protection system in order to infect it. Therefore a virus can only infect systems which use the same protection mechanism.

In the following we will try to find out to what extend the number of different protection systems that are used worldwide may influence the rate of infected systems.

We assume that there exists a variable number n of different protection systems and these protection mechanisms are equally distributed amongst all these systems. The rate of systems, that use the same protection mechanism corresponds to 1/n.

The rate of infected systems x is increased proportionally to the probability that a clean system gets infected by exposure to an infected system, which has the same protection mechanism. e x equals the part of infected systems, which introduce new protection mechanisms.

$$dx/dt = a(1-x)x/n - ex \quad (16)$$

$$dn/dt = enx/(1-ex) \quad (17)$$

Equation (17) can be calculated on the assumption that all protection mechanisms remain equally distributed. After the introduction of Δn new protection mechanisms we have a rate of $\Delta n/(n + \Delta n)$ of newly protected systems, which should be equal to ex. From $ex = \Delta n/(n + \Delta n)$ follows that $dn/dt = e n x / (1 - e x)$.

For e = 0 we have a constant number n of protection systems and the model (16, 17) is reduced to model (1). So a constant number of not perfect protection systems leads in principle to the same drastic increase in virus infection as the unrestricted virus propagation.

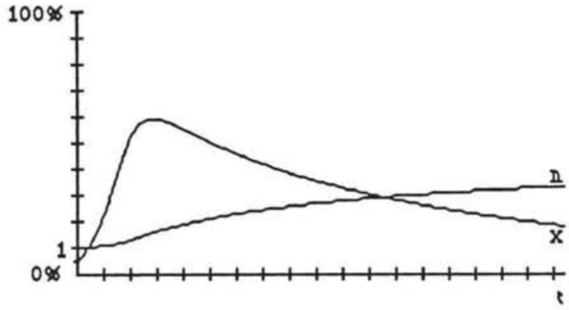

Fig. 8. Model (16, 17), a = 0.3, e = 0.08, x_0 = 0.05, n_0 = 1

The rate of infected systems converges to 0 whenever the number of different protection systems exceeds a/e.

Now we assume that the use of many different protection mechanisms leads to an average reduction of the quality factor efficiency.

Efficient protection mechanisms are characterized by:

- highly reduced virus propagation
- high detection & removal rate

Instead of a constant probability of infection a, we use $(1 - h / n)\, a$, which is minimal for $n = 1$ and tends to a for a high value of n.

The detection & removal rate is assumed to be g / n. This is a very defensive assumption. The efficiency of one system is n times higher than that of n systems

$(1 - h / n)\, a$ ... probability of infection
g / n ... probability of detection & removal

$$dx/dt = (1 - h / n)\, a\, (1 - x)\, x / n - e\, x - (g / n)\, x \qquad (18)$$

$$dn/dt = e\, n\, x / (1 - e\, x) \qquad (19)$$

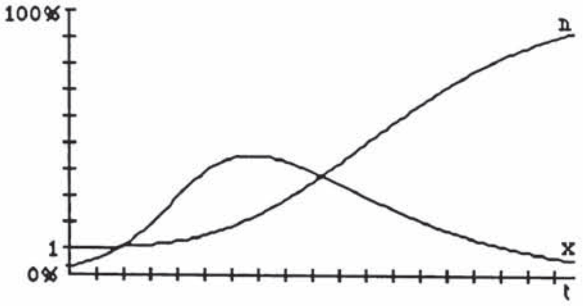

Fig. 9 Model (18, 19), $a = 0.3$, $e = 0.05$, $h = 0.5$, $g = 0.02$, $x_0 = 0.03$, $n_0 = 1$

Again all infected systems become clean, whenever the number of different protection systems becomes large enough.

CONCLUSION

The discussed models show that the use of many different protection systems can be more effective than the use of a single very sophisticated and efficient system. It is necessary to develop new and further develop existing protection systems or the battle against computer virus propagation will be lost.

REFERENCES

Cohen, F. (1987). Computer Viruses, Theory and Experiences. *Computer & Security, 6*, 22-35.

Futschek, G. (1991). Experiments with Self-Reproductive Logo Programs. *Proceedings of the 3rd European Logo Conference*, Parma.

Murray, J. D. (1989). *Mathematical Biology*. Springer.

Solomon, A. (1990). Epidemology and computer viruses. *Virus News International, 9*,.15-21.

Weninger, Chr. (1991). *Betrachtungen zur Virenproblematik und Implementierung des PC- Antivirenprogramms PROTECTOR (Germain).* Diplomarbeit, TU-Wien.

Zentralstelle für Sicherheit in der Informationstechnik (1989). *IT-Sicherheitskriterien - Kriterien zur Bewertung der Sicherheit von Systemen der Informationstechnik (IT).* Bundesanzeiger Verlagsges.mbH., Köln.