Should We Teach Virus Writing?

Dr. Vesselin Bontchev, anti–virus researcher
FRISK Software International
Thverholt 18, IS-105 Reykjavik, ICELAND
E–mail: bontchev@f-prot.com

***Abstract**: In late spring 2003, Prof. Ken Barker, head of the Department of Computer Science at the University of Calgary decided that, as part of a set of courses on Computer Security, his students had to be taught how to write viruses. He even went as far as widely advertising this idea of his on the Web and seems firmly convinced to implement it, despite the uniformly negative feedback he has received from the professionals in this field. This paper examines in details everything that is wrong with the particular proposal, as well as with the general idea of teaching students how to write viruses and other malicious code. Finally, we propose some ideas how to educate students properly on this subject.*

1.Introduction

In May 2003, it was brought to our attention that Prof. Ken Barker, head of the Department of Computer Science of the University of Calgary, Canada, has decided to create a new course for his students. By itself, this fact would have hardly been worth of notice – new courses for students are created at the universities around the world all the time. The peculiar thing about this particular course, however, was that it was supposed to teach the students how to write viruses. Furthermore, its author had made a lot of noise about it and had posted a text, defending his idea, on one of the University of Calgary's Web pages. (The full text of this Web page is given in Appendix A.) In fact, this course was advertised so widely, that an article about it even made it to the pages of an airline magazine ([Scanorama03]). The original content of this page was even published by Prof. Barker in Virus Bulletin ([Barker03]), in defense of his idea to create such a course.

Since then, the idea behind this course has been criticized very widely throughout the anti-virus industry ([Kuo03], [Skulason03], [VB03]). In a panel discussion published in the July issue of "Information Security" ([IS03]), 9 of the 10 participants stated negative opinions about the idea of teaching students how to write viruses. The position of the only dissenting participant is probably understandable, given that this was Prof. Fred Cohen – the person who invented computer viruses in 1984 and who created several of them

(in order to research them and their behavior in laboratory conditions) during his work on his Ph.D. thesis ([Cohen86]).

Despite the severe criticism, the author of the course, Prof. Ken Barker, seems unswayed and determined to proceed forth with his idea. We do not harbor the illusion that, by publishing this paper of ours, we shall change his mind. However, it seemed useful to us to collect and systemize in a single paper the arguments against this idea in general, against its proposed particular implementation by the University of Calgary, as well as some suggestions regarding what is the proper way to teach students about computer viruses.

2.What Is Wrong With the Particular Proposal

The statement of the University of Calgary (see Appendix A) contains a lot of logical errors, contradictions, false assumptions and other untruths. In this section we shall try to examine and debunk them in detail.

> *The course will prepare the newest computer professionals with the expertise needed to work in a computing environment which includes more than 80,000 computer viruses and other forms of malware.*

The author incorrectly assumes that knowledge of how to create viruses is necessary in order to prepare the aspiring computer professionals for working in a computing environment where viruses are widespread. What these computer professionals really need is knowledge how to *detect*, *analyze* and *remove* computer viruses – not knowledge how to create them.

> *A critical element of a complete education for the graduating professional computer scientists must include knowledge about viruses, their nature, and their destruction.*

The above statement is correct. However, the Prof. Barker makes the implicit conclusion that learning how to *create* viruses will provide such knowledge. This conclusion is false. It is true, that once one learns about computer viruses enough in order to analyze and destroy them effectively, it is quite likely that this knowledge could be applied to create them as well – if nothing else, then at least by combining bits and pieces from the known viruses one has analyzed. However, this is a side-effect of this education – not its primary goal. And the opposite is not true – if one is taught how to create viruses, one might still not have sufficient knowledge to fight them effectively.

The skills required from a virus writer and an anti-virus researcher are *very* different – even if the subject of interest of both is computer viruses. Prof. Barker would do well to consider what is the reason that there are hundreds of virus writers – but only a

handful of competent anti-virus researchers. Nowadays it is extremely easy to write a virus - in fact, there are virus construction kits which allow even an unskilled person with no knowledge of programming or computer viruses to create rather sophisticated viruses. As opposed to that, there are no such kits permitting the automatic creation of anti-virus programs.

A virus writer usually concentrates on a single (often rather simple) idea and often doesn't care how well his virus will work. As opposed to that, an anti-virus researcher needs to have wide expertise in various computer security fields; must be capable of unconventional thinking, must have a lot of imagination – and, at the same time, a lot of discipline and pedantism, in order to perform his or her job in a satisfactory manner. He or she must carefully design and test their anti-virus program in all kinds of environments, in order to ensure that it is compatible, effective, and does not cause any unintentional damage. Those are all goals, which are usually completely foreign to the virus writer; goals which he neither cares about, nor would have had the expertise to fulfill, even if he did care about them.

> *It is time for critics to take their heads out of the sand and work with us to start developing the next generation of computer professional who will be proactive in stopping computer viruses.*

Being proactive in stopping computer viruses does not mean creating them before they come all by themselves. It means setting up defenses which would work even before the viruses have attacked. The ability to create viruses does not help even one little bit for the achieving of the latter objective.

There are three main kinds of anti-virus programs ([Bontchev98]) – *known-virus scanners*, *behavior blockers*, and *integrity checkers*. The first of these three kinds is the one which is the most commonly used nowadays – but it is not proactive. The other two *are* proactive – but they are not widely used. The reason why they are not is that, unlike the first kind, they do not provide simple and easy-to-understand reports to the user. Instead of "Found and removed the XYZ virus" (the kind of reports that the known-virus scanners produce), they produce reports like "Attempt to write to file FOO.EXE, allow or deny?" (behavior blockers) or "File BAR.EXE has changed since the last check" (integrity checkers). Both viruses and legitimate actions (file copying or installation of new software) can cause such reports. The burden to decide whether they are caused by a virus or not is left to the user – and most users simply do not have the expertise to make a competent decision in such a situation and neither are they interested in acquiring it. After all, what they want is to do their primary job; all this security stuff is incomprehensible and uninteresting to them and, besides, isn't that why they bought an anti-virus product – in order to take care of such stuff for them?!

Future computer professionals should try to make such decision simpler and automatable – and this can be achieved by studying how to write better anti-virus programs; not by studying how to write viruses.

The current approach of reacting to the viruses is simply not working.

To a certain degree the above is correct (but only to a certain degree – if the current approach wasn't working at all, we wouldn't have a multi-billion anti-virus industry successfully selling it to the users). However, one of the reasons why it is not working is explained above. This reason is most definitely *not* the lack of people who know how to write viruses. Therefore, it cannot be made to work by teaching virus writing.

(The other reason why it is not working is because, according to our research – see [Bontchev01] – more than 97% of the users simply do not care whether their machine is infected or not. However, educating the users is a rather hopeless task (especially given the fact that most of them do not *want* to be educated on this subject), so the possible solution should be aimed at improving the anti-virus programs; not at educating the user.)

Let's be honest: any reasonably intelligent individual can get this information from the internet without having to spend four years at University.

This, again, is correct. However, it is completely irrelevant as an argument supporting the idea that the University of Calgary should teach its students how to write viruses. In fact, it is an argument *against* it. And, indeed, if such information is easily available and readily accessible (which is indeed the case), then what is the point of wasting time and money teaching it to the students?! In the unlikely case that they ever need it, they can easily obtain this information from the Internet – precisely as Prof. Barker says.

It is naïve and dangerous to think that virus writers can be stopped without a better understanding of how they operate.

Stopping the virus writers, as stopping any other kind of criminals, is the job of the law enforcement – not of the computer science graduates. The job of the latter is to stop the *creations* of these criminals – not the criminals themselves. And for that they need to know how to write anti-virus programs, how to analyze viruses and how to stop a virus attack – they do not need to know how the virus writers operate.

Some detractors claim that teaching students about viruses is "wrong" or "dangerous" because this kind of software is bad.

I am not aware of anybody who criticizes Prof. Barker's idea and who makes the above silly argument – so, either Prof. Barker has misunderstood the argument or he is erecting a straw-man here. Teaching students *about* viruses is *not* "wrong" or "danger-

ous". What *is* wrong and dangerous is teaching them how to write viruses. The difference between the two is huge, as explained earlier in this section.

> *The simple fact is that viruses and malware exist. It is an undeniable fact of the modern computing environment.*

This fact is by no means an excuse to create more of them, however!

> *We are interested in producing computer professionals who have the expertise necessary to stop computer viruses.*

The proper way to achieve the above goal is to teach people how to stop viruses – not how to create them. Primarily, in order to achieve the above goal, the students have to be taught how to develop and deploy sound security policies, as well as the basics of anti-virus software (that is – what kinds of anti-virus programs exist, what are their main advantages and limitations, in what situations it is proper to use each one of them and so on). Unless the goal is to train anti-virus researchers, it is not even necessary to teach the students how to analyze viruses. It is perfectly possible to stop computer viruses without being able to analyze them in detail. In any case, teaching how to write viruses is *never* necessary.

> *Further, a critical element of being able to stop these viruses is to have sufficient knowledge about them to be able to write them.*

The above statement is given without any supporting arguments. This is hardly surprising, because there aren't any – the statement is simply false. The knowledge about computer viruses that is sufficient to be able to stop them includes only knowing what kinds of viruses exist, what they are capable of doing, and what the proper ways of detecting and eradicating them are. The knowledge how to write them is completely unnecessary. Furthermore, it is also insufficient – that is, a person who knows how to write a virus does not necessarily know how to stop it. There are multiple examples of virus writers who, when caught, have come up with the excuse that they had not realized how easy their virus could "escape" and have been unable to prevent its spread.

> *That will come as no surprise to IT professionals who understand that to solve a computer problem it helps to understand what caused the problem.*

The above is correct but the implied conclusion from it is wrong. In fact, the above argument does not support the idea that students have to be taught how to write viruses, in order to learn how to stop them. In order to solve the problems posed by the various criminal acts, it helps to understand what is causing them; what are the main motives of the criminals and why they have been able to commit their crimes. It most defi-

nitely does not help, however, if the person studying the problem starts committing crimes himself.

> *It is clear that anyone who claims they understand computer viruses well enough to stop them also understands them well enough to write them. Anyone who claims otherwise is simply wrong.*

The above statement is simply false and saying "anyone who disagrees is wrong" without providing proper arguments to support such a notion does not make it true – in fact, it is an extremely flawed and counter-productive way of conducting arguments; a fact which Prof. Barker, as member of the academia, really ought to know. In most big corporations nowadays there are people whose job is to ensure that the corporation's computers remain virus-free. These people rarely know how to write a virus – but that does not prevent them from performing their job quite well. With the risk of repeating ourselves, we must stress again that completely different (and often incompatible and contradictory) kinds of skills are required for writing viruses and for stopping them.

> *This course is not about creating new viruses but about understanding how they function with the ultimate goal of stopping them.*

If Prof. Barker honestly subscribes to the above statement, then he clearly must drop the idea of teaching his students how to write viruses. After all, as he clearly says himself, it is not relevant to the intended goal of the course!

> *A necessary step in stopping viruses is that the computer professional could also write one so we are using the "writing" of computer viruses as a teaching method.*

The above statement is utterly false and it shows perhaps in a most concentrated form what is wrong with Prof. Barker's idea. You do not need to teach somebody how to write a virus, in order to teach them how to stop one.

> *Is there another way to teach about stopping viruses without providing adequate knowledge so that the students could write a virus? The answer is simple: No.*

The above question is clearly meant as a rhetorical one – however, the answer provided to it is wrong. *First* of all, it is perfectly possible to teach about stopping viruses without providing adequate knowledge so that the students could write a virus. Many of us in the anti-virus industry, when we still had the time to educate corporate users on proper anti-virus practices did just that. *Second*, while it might be true that if the students are taught a lot about computer viruses (not just how to stop them but also how to analyze them and many other things; when the goal is to train anti-virus researchers; not just peo-

ple who know how to stop viruses), they could use the acquired knowledge to write a virus, this by no means must be the primary goal of such a course; at most it should be a side-effect. If one gives the students the knowledge mentioned above, one does not need to give them the knowledge how to write viruses; one must leave it to them to infer it themselves (stressing all the while that it is something they **must not** do).

> *Anyone who claims they can fight a virus but could not write one is either uninformed or trying to mislead for other reasons.*

Again, the above statement is utterly false. It does not provide any arguments in defense of the thesis stated; instead, intentionally strong words are used in the hope of discouraging anyone who would normally argue against it. The truth is that there are many people in many companies all over the world – people whose job is to fight viruses (and who are quite capable of performing these jobs successfully) – yet who are not capable of writing viruses.

> *We have to wonder why the anti-virus software companies are so opposed to development of software that could prevent viruses from proliferating.*

The anti-virus companies are doing nothing of the sort. Just the opposite – it is quite difficult for them to find capable people to hire as anti-virus researchers and they welcome any educational institution's efforts to produce such people. The technical people at these (otherwise competing) companies often collaborate with each other and help each other with the various issues related to fighting viruses. The author of this paper has published a Ph.D. thesis ([Bontchev98]), which has successfully been used as a textbook for training anti-virus researchers at several anti-virus companies. Just like the goal of the physicians is to make illnesses disappear and the goal of the law enforcement officers is to make criminality disappear, it is our goal to make viruses disappear – despite the fact that our revenues are directly related to their existence.

Had Prof. Barker simply announced that he intended to teach his students how to develop software that could prevent viruses from proliferating, none of us would have objected. Just the opposite – we would have supported his efforts to the best of our abilities. However, he has announced that he is going to teach his students how to write viruses. *This* is what the anti-virus companies are strongly opposed to.

Prof. Barker then goes on to describe what steps will be taken to protect the learning environment. While many of the described steps are commendable (albeit obvious), it is difficult for us to evaluate how appropriate such a protection would be without seeing how it is implemented in practice and without examining it carefully on-site. Suffice it to say that in our long career as an anti-virus researcher we have seen many virus protection policies that looked just fine on paper but which had turned out to be utterly ineffective in

practice – mostly due to some implementation flaw that was not foreseen by the designer of the protection policy. Still, we would like to make a couple of comments on the guidelines provided in Prof. Barker's statement.

> *No removable media will be taken out of the laboratory once it is brought in so there is no risk of viruses leaving on a floppy or removable hard disk.*

The above statement suggests that Prof. Barker seriously underestimates the challenge that securing such a lab provides – as well as the fact that he does not seem to be up-to-date with the latest developments in hardware and software.

Firstly, there are devices with the size of a keychain which can be plugged in the USB port of any contemporary PC and which can store several megabytes of data. It would be trivial for a student to smuggle such a device in the Lab and use it to transport virtually any protected data they want. Only a full-body strip search at the door of the Lab would prevent such an attack. However, we very much doubt that Prof. Barker would be willing to submit his students to such a procedure – or that they will tolerate it, for that matter.

Secondly, instead of trying to control the *media* that will be allowed (or not) to be taken out of the Lab, it would be much more effective to control what media the computers in the Lab would be allowed to access. With the contemporary operating systems, it is relatively trivial to forbid the machine from accessing floppy disks and FLASH disks connected to the USB ports – while in the same time forbidding the user (by setting up a security policy) from installing device drivers for the purpose of accessing such (or any other) devices.

Thirdly, it is not the media taken out of the Lab that is of primary concern. A much more serious problem will be the knowledge and information residing in the heads of the students. Even if they are successfully prevented from taking the viruses they have developed out of the Lab on a floppy disk (or other removable media), there is no way to prevent them from using the acquired knowledge to re-create these viruses on their own outside the Lab and outside Prof. Barker's or the University of Calgary's control. We seriously doubt that Prof. Barker has invented a way for searching the thoughts of his students.

> *When the course ends - the computers used will be completely cleaned by having all removable media destroyed and all hard disks completely scrubbed down to the BIOS.*

The phrase "scrubbed down to the BIOS" again suggests that the technical knowledge of Prof. Barker is somewhat on the lacking side. As anybody with serious computer

knowledge knows, the BIOS is a program recorded in PROM, EPROM, EEPROM or FLASH memory and residing on the motherboard of the computer – not on its hard disk. A hard disk simply *cannot* be "scrubbed down to the BIOS" – because there *is* no BIOS on it to be scrubbed down to. ☺

We shall conclude with a few final comments.

> *Anti-virus community: We have been in contact with members of the anti-virus community and they have offered to help us in delivering the course and in developing its curriculum. Most of this community accepts the argument that stopping viruses requires sufficient knowledge to also write a virus so they are willing to work with us.*

Everybody in the anti-virus community whose opinion on Prof. Barker's idea we are aware of (which, for all practical purposes, is just about anyone in the anti-virus community that matters) is strongly opposed to the idea of teaching the students how to write viruses. Yes, many of us would be glad to help Prof. Barker in delivering a course that teaches the students *about* computer viruses, teaches them how to design anti-virus software, and how to develop sound security policies. But this must not be understood as suggesting that anyone of us supports the idea of teaching the students how to write viruses. The author of this paper also very strongly doubts that "most" members of the anti-virus community are indeed as ignorant as to think that stopping viruses requires the knowledge to also write them.

> *The bottom line: We can pretend that the problem will be solved with old methods, or we can take on the problem to a new level of understanding and action to stop virus. It may not make for a good media story, but it should make sense to anyone who owns a computer.*

We are not opposed to seeking new methods for solving the computer virus problem. However, writing more viruses is most definitely not such a method. The virus writers have been using this method for about 15 years already and the only result is that the computer virus problem has become worse. As far as the media is concerned, apparently the fact that the University of Calgary would be teaching their students how to write viruses has attracted the attention of the media – if we have read about it even in the airline magazines([Scanorama03]).

3.What Is Wrong With the General Idea

Even if Prof. Barker's proposal did not contain all the logical flaws and other errors that were discussed in detail in the previous section, we still maintain that the general idea of teaching the students how to write viruses is wrong. In the in this section we shall

consider some general flaws of the idea – flaws which remain no matter how it is implemented.

3.1It Encourages Virus Writing and Legitimizes It

Research has shown that one of the most effective ways to reduce a particular kind of anti-social behavior is via peer pressure. That is, a public opinion should be widely established among the group of people from which the perpetrators usually originate, according to which opinion the anti-social behavior in question is considered "uncool" – i.e., frowned upon; unacceptable by the group. In the past, such tactic has helped to greatly reduce the driving under the influence of alcohol among the young people.

However, such a tactic would have no hope of success, if a serious educational institution begins to endorse the anti-social behavior – i.e., virus writing in this particular case. Scores of young people will grasp at the excuse that they are "doing research" when they engage in this form of electronic vandalism. Little attention will be paid to the details – e.g., whether the same precautionary measures are taken to avoid the virus from escaping the research environment. People are likely to pay attention only to the essence – i.e., "the University of Calgary teaches it, so it must be OK".

3.2It Decreases Employment Opportunity

The anti-virus company that the author of this paper works for, just like most other anti-virus companies, has a very strong policy against hiring virus writes. This is necessary, because we are operating in an environment where trust is essential. We have constantly been plagued by accusations what we are the ones who write all the viruses – accusations, stemming from the rather trivial consideration that we owe our income from the existence of computer viruses. (The authors of such accusations tend to forget that the members of the medical and the law enforcement professions have similar apparent "conflicts of interest" – yet they are not accused to be the source of illnesses or crimes.) We simply cannot afford to give any credence to these accusations – therefore, the strict policy against hiring of virus writers.

It is worth noting that it does not matter to us whether the virus writers are still active or have already "reformed" and stopped writing viruses. Once a virus is created and released out of its author's control, it exists forever in the virus collections. Even if the environment in which it is capable of replicating no longer exists, we are still forced to implement detection, recognition, identification and removal of it. The virus definitions databases of our scanners must still contain the proper entries for handling this virus, despite the fact that it is no longer a threat. This is because our products are often tested and evaluated against "zoo collections" of viruses from various sources – viruses,

which are not necessarily the ones currently posing a threat to the users. And since, from our point of virus, a virus, once created and distributed, lives forever, for us there is no such thing as a "former" virus writer. If somebody has written and released even a single virus in the past, this person is "tainted" as far as we are concerned and we cannot afford to hire them.

As a consequence of the above, the students who attend a virus writing course are automatically denying themselves the opportunity to be hired by most anti-virus companies. This is rather deplorable, given that one of the stated goals of such a course is to prepare people for dealing with the computer virus problem. Sadly, they will have no chance of doing that in the anti-virus industry – and only because the course they have attended teaches virus writing.

In reality, the situation is even worse. Job applicants rarely list in detail on their résumés which particular course they have taken at the educational institution(s) they have attended. If it is known that a particular educational institution teaches a virus writing course, we would be automatically prejudiced against **all** students who have graduated from this particular educational institution. Therefore, the professor who chooses to teach a virus writing course damages the future not only of his students but of all other students who have graduated from his university or college during the time the virus writing course has been taught.

3.3It Brings Legal Responsibilities

In some countries virus writing is considered illegal. Students, who have attended a virus writing course, can have legal troubles if they ever enter such a country.

In addition, what if one of the students who graduate from the course starts writing viruses and releasing them into the wild? It is quite likely that if the public learns about such a case, the educational institution that has taught such a course will find itself on the receiving end of a class action lawsuit.

We are not, however, experts in legal matters, so we shall leave this matter without further comment. Still, any educational institution that allows a virus writing course to be taught on its grounds should give serious considerations to the possible legal implications.

3.4There Are No Good Viruses

Sometimes the proponents of the idea to teach virus writing use the argument that it is legitimate academic research – research, which might lead to some useful results, like the ability to use computer viruses for some beneficial purpose. The detailed debunk-

ing of this flawed misconception is outside the scope of this paper. We have presented all the necessary arguments against it in a paper of ours ([Bontchev94]) which, although written way back in 1994, is still perfectly actual and all the arguments presented there are still valid. To summarize the conclusion of this paper – there is no such thing as a "good" computer virus.

4.How to Do It Properly

Let us assume, for the sake of argument, that the true goal of Prof. Barker is indeed to train computer professionals capable of developing and deploying efficient anti-virus defenses (instead of, say, the creation of publicity for his course by coming up with a controversial proposal). Under such an assumption, in this section we shall present some guidelines about how to achieve this goal while using proper means.

4.1Study Solutions, Instead of How to Create Problems

The proper way of training people how to handle a particular problem is most definitely *not* by training them how to *cause* it. The proper way is to have them study the known solutions for it, and to train them how to develop such solutions on their own.

It is immensely more difficult to develop a good anti-virus program than to write a virus. After all, a computer virus is a rather simple program which has one main, rather simple task – that of self-replication. An anti-virus program, on the other hand, is a very complex project. Its author has to make it able to cope with the various multitude of operating environments in existence, has to make it able to correctly detect and stop (or remove) a great multitude of viruses (which use many different replication methods, the handling of which requires many – often contradictory – approaches), and, not in the last place, has to make it *usable* by the unsophisticated user.

Contrary to popular opinion, the anti-virus programs do not simply look for a large number of scan strings (or "virus signatures", as they are often incorrectly called) in the files. If nothing else, this is a rather slow and inaccurate process. Many modern virus scanners do not use scan strings at all – or use them only to trigger their more powerful and more accurate virus identification algorithms.

Even the design of a good (and fast!) known-virus scanner is by far not a trivial process. But this is by far not the only kind of anti-virus programs in existence. The design of a good behavior blocker or a good integrity checker is a difficult task on its own – with completely different sets of challenges typical for it. The students could learn a lot while trying to design such an anti-virus program and then observe how their creation behaves in practice, how fast it is (or not) and how easy-to-use the users find it.

Such a learning process would teach the students many things about stopping viruses and about developing anti-virus solutions – things, which the teaching of them how to write viruses would never achieve.

But the development of anti-virus programs is by far not the only thing the students of such a course should be taught. No less important is the knowledge how to develop and deploy sound security policies – policies, which will be actually usable and enforceable, and which would be able to keep effectively computer viruses (and often – many other kinds of intruders) at bay. In fact, just such a knowledge alone would do a great deal to prepare computer professionals who are able to tackle the virus problem – even if they don't learn how to develop anti-virus programs. Needless to say, the knowledge how to write viruses is completely irrelevant (i.e., neither necessary, now sufficient) for this purpose.

4.2Teach Virus Analysis, Instead of Virus Writing

In order to understand how computer viruses work, and in order to create efficient defenses against them, it is again neither necessary nor sufficient to know how to create them. Instead, it is much better to know how to analyze viruses.

We have observed the "production" of several virus writers and they, almost without exception, tend to concentrate on just a few simple ideas. If the students are taught virus writing, this (a few simple ideas) is all that they will learn, too. If, instead, they are taught how to analyze viruses, how to understand what makes them work, how they infect, and how to stop them and to reverse their effects on the infected system, the students will learn much, much more.

It is simply impractical to teach them all the different tricks used in computer viruses – because there are so many of them and, even worse, new ones are created all the time. No matter how well the students are taught to write viruses, it is likely that, in their practical experience, they will encounter a virus, using ideas that haven't been told about – for instance, simply because those ideas were not known at the time the students have taken their virus writing course. If, however, they are trained to analyze viruses, they will have no trouble to understand how the new virus works and how to handle it efficiently.

In addition, of course, such an approach will have the added benefit that it will not increase the number of known viruses and that it will train anti-virus people, instead of virus writers.

Certainly, after the students have analyzed a few dozen viruses, they will know enough, in order to be able to write a virus on their own – if nothing else, at least by combining bits and pieces of the viruses they have seen. But this will be only a side-effect

from a much more extensive and important body of knowledge. Teaching virus writing alone cannot give them the rest of this required knowledge. Virus writing cannot and must not be the primary goal (any goal, actually) of their education. Of course, even the training in virus analysis must be accompanied with the proper ethical education – in order to prevent them from misusing the abilities, which they will acquire as side-effects of such training.

4.3Use Existing Viruses, Instead of Creating New Ones

We readily admit that, in the process of education, the students will have to be exposed to real viruses – e.g., in order to analyze them, in order to observe how they behave in a controlled environment, and so on. However, we maintain that it is completely unnecessary to write new viruses for such a purpose – one should simply use some of the tens of thousands of existing ones.

There is already a large enough number of viruses in existence – and they employ various enough ideas and tricks. The pool of existing viruses is perfectly sufficient to train the students in any needed intricacies of virus analysis. It is completely unnecessary (and even dangerous, let alone unethical) to create new ones – even for educational purposes. We are reasonably certain that no matter how hard they try, neither Prof. Barker, nor any of his students will be able to come up with the idea of a virus that has not already been tried before in an already existing virus – in one form or another.

4.4Create Viruses for a Virtual Environment

The only legitimate case of virus writing that we are aware of is when computer viruses did not exist and when the person who invented them – Dr. Fred Cohen – needed to write some, in order to perform various experiments with them and to prove in practice the various theoretical results about them that he had deduced. In the unlikely case that the students have similar needs, we have a constructive proposal for them. Namely, instead of writing viruses for the existing operating environments, simply create a virtual, simulated environment and write viruses that are able to spread only under that environment.

Such an approach would guarantee that the created viruses will not escape and will not cause any damage. It will have various other benefits, too. For instance, creating a virtual, simulated computer, with virtual infectable programs and media for it is a rather difficult task. By fulfilling it, the students will learn a lot about computers and programming in general – which will further enhance their education as computer science professionals. In addition, they would be able to give the created environment the exact proper-

ties they need – properties, which might be difficult (or even impossible) to obtain when experimenting with real computers.

One possible problem with this approach is that, because of its difficulty, it might not be suitable for integration into a single-year training course on computer viruses. However, it should be possible to fit it with the other courses the students take during the years they spend at the University. The skills, learned from completing such a project would be quite useful to someone who is studying computer design, operating systems, hardware, or compiler design.

5.Conclusion

We hope that we have been able to expose in detail that there are many things, which are wrong with the University of Calgary's decision to teach their computer science students how to write viruses. In fact, that there are several things, which make the idea of teaching virus writing in general a flawed one. We have also provided some guidelines about what and how to teach, if one's goal is to train capable and competent anti-virus researchers.

We do not harbor any illusions that this paper of ours will change Prof. Barker's mind – our communication with him has convinced us that he is quite stubbornly decided to go forth with his idea, that he refuses to listen to proper reasoning, and that he has some rather basic flaws in his logical reasoning – flaws, which he is seemingly unable to perceive. However, if we have managed to convince others how flawed his idea is and not to repeat it, the time and efforts we have spent writing this paper would not have been wasted.

6.References

[Barker03] Ken Barker, "*To Teach or Not To Teach*", Virus Bulletin, July 2003, pp. 17-18.

[Bontchev94] Vesselin Bontchev, "*Are Good Viruses Still a Bad Idea?*", Proc. EICAR'94 Conf., pp. 25–47.

[Bontchev98] Vesselin Bontchev, "*Methodology of Computer Anti-Virus Research*", Ph.D. Thesis, University of Hamburg, 1998.

[Bontchev01] Vesselin Bontchev, "*Anatomy of a Virus Epidemic*", Proc. 11th Int. Virus Bull. Conf., 2001, Prague, pp. 389-406

[Cohen86] Fred Cohen, *PhD. Thesis*, University of South California, 1986.

[IS03] "*Is there ever a legitimate purpose for creating a virus?*", Information Security, July 2003, pp. 18-19.

[Scanorama03] "*Know the Enemy*", Scanorama, September 2003, p. 75.

[Skulason03] Fridrik Skulason, "*Open Letter to the University of Calgary*", Virus Bulletin, July 2003, pp. 18-19; also available from

[VB03] "*School without Thought*", Virus Bulletin, June 2003, p. 3.

[Kuo03] Jimmy Kuo, "*Alberta Strikes Again*", Virus Bulletin, July 2003, p.2.

Appendix A. University of Calgary's Announcement

The following is the full text of the original announcement of the University of Calgary's intent to set up a virus writing course for their students. It used to be available from http://www.cpsc.ucalgary.ca/News/virus_course.html. However, at the present time this Web page is no longer available and the text on it cannot be found anywhere on the University of Calgary's Web site. According to Prof. Barker, this was caused by a re-organization of the University's Web site and because the announcement was no longer actual, given that the course had already begun.

Computer Viruses and Malware

As a part of a set of courses on Computer Security the University of Calgary is offering fourth year students - and fourth-year students only - a course on computer viruses and malware. The course will prepare the newest computer professionals with the expertise needed to work in a computing environment which includes more than 80,000 computer viruses and other forms of malware. A critical element of a complete education for the graduating professional computer scientists must include knowledge about viruses, their nature, and their destruction.

It is time for critics to take their heads out of the sand and work with us to start developing the next generation of computer professional who will be proactive in stopping computer viruses. The current approach of reacting to the viruses is simply not working. The University of Calgary continues to take a leadership role in this area and this course is another example of the cutting edge research and education undertaken in the Department of Computer Science at the University of Calgary.

Let's be honest: any reasonably intelligent individual can get this information from the internet without having to spend four years at University. There are easier and cheaper ways for them to wreak havoc. It is naïve and dangerous to think that virus writers can be stopped without a better understanding of how they operate.

This course sets viruses within a professional ethical framework, discusses legal factors, and fully considers the environment within which malware exists in the modern computing systems.

The course addresses three primary areas:

1. Knowledge is critical. Some detractors claim that teaching students about viruses is "wrong" or "dangerous" because this kind of software is bad. The simple fact is that viruses and malware exist. It is an undeniable fact of the modern computing environment. We are interested in producing computer professionals who have the expertise nec-

essary to stop computer viruses. Further, a critical element of being able to stop these viruses is to have sufficient knowledge about them to be able to write them. That will come as no surprise to IT professionals who understand that to solve a computer problem it helps to understand what caused the problem.

It is clear that anyone who claims they understand computer viruses well enough to stop them also understands them well enough to write them. Anyone who claims otherwise is simply wrong. This course is not about creating new viruses but about understanding how they function with the ultimate goal of stopping them. A necessary step in stopping viruses is that the computer professional could also write one so we are using the "writing" of computer viruses as a teaching method.

Is there another way to teach about stopping viruses without providing adequate knowledge so that the students could write a virus? The answer is simple: No. Anyone who claims they can fight a virus but could not write one is either uninformed or trying to mislead for other reasons. We have to wonder why the anti-virus software companies are so opposed to development of software that could prevent viruses from proliferating.

2. Protecting the Learning Environment. A valid and critical concern is constraining any viruses studied in the laboratory. The University has taken several steps to ensure any viruses developed or studied are constrained within the laboratory:

- Students must be in the fourth year of our program and are only permitted into the program with the consent of the Department of Computer Science.
- The laboratory will be housed in a secure laboratory that is locked 24 hours per day 7 days per week. Student access will be monitored and limited to only students taking the course.
- No removable media will be taken out of the laboratory once it is brought in so there is no risk of viruses leaving on a floppy or removable hard disk.
- No "wireless access" point will be used within the laboratory so nothing can "leak" out through the air.
- No "wired" access to the computers in the laboratory will exist. Although the computers in the laboratory will be networked together, it will be impossible for a virus to leave the laboratory as no wired connection will exist to outside computers.
- When the course ends - the computers used will be completely cleaned by having all removable media destroyed and all hard disks completely scrubbed down to the BIOS.

3. We are willing to work with the wider community to ensure the best possible education for our students. At least three groups of people have been contacted, and are willing to work with us, to develop this course:

- Anti-virus community: We have been in contact with members of the anti-virus community and they have offered to help us in delivering the course and in developing its curriculum. Most of this community accepts the argument that stopping viruses requires sufficient knowledge to also write a virus so they are willing to work with us.
- Ethics training: Philosophers, lawyers, and business professionals will be included in the curriculum so students will have a full professional training in all aspects of computer viruses and malware.

The bottom line: We can pretend that the problem will be solved with old methods, or we can take on the problem to a new level of understanding and action to stop virus. It may not make for a good media story, but it should make sense to anyone who owns a computer.

Ken Barker, Head and Professor, Department of Computer Science