# Flow of Presentation

## 0) INTRODUCTION

1. Introduce presenters
2. Introduce topic
3. Give outline of presentation
   1. Handout

## 1) HISTORY

1. History of security
   1. Early
   2. Middle
2. Learning from history

## 2) CURRENT EFFORTS

1. People who are teaching malware
   1. George Ledin
   2. John Sullins
   3. John Aycock
2. Importance of ethics in education in malware
   1. Reasons why
   2. Example methods
3. Example course outline
   1. George Ledin Course
   2. John Aycock Course
      1. VIDEO: John Aycock talking about malware course
4. Sucker activity

## 3) CONCLUSION

1. Review/summary of history and current efforts.
   1. Going Forward
2. Major roadblocks
   1. Fear of danger
   2. Fear of complicity
   3. Lack of preparedness
3. Hopes for the future

# Conclusion

#### Going Forward

In the past the response to threats has been inefficient, patching holes in the defenses after the holes were found, usually by a malicious party. Solutions for malware attacks rarely pre-empt the attack, and for the victims they often come too late. Those that would do good remain in the dust of those that would do evil.

Other fields of study have adopted the practice of examining how threats work through close examination of those threats in safe, supervised environments. Computer science has been reluctant to adopt the same methodology.

While educators like John Sullins, George Ledin, John Aycock, and others are certainly laying the base layer for the road to conquering this shortcoming there are still some major roadblocks to overcome.

#### Major Roadblocks

First major roadblock is the fear that students will use the knowledge gained in a course about malware to go out and perpetuate malicious software. It is the worry that knowledge will tempt students into unethical actions.

The second roadblock has a significant effect on institutions as well as educators, and that is the fear of complicity. That should our first fear be well founded, the institution or educator will be seen as aiding or abetting the criminal acts of an offending student.

Finally, these first two roadblocks lead to a lack of knowledgeable educators and properly equipped institutions.

#### Fear of Danger

Many feel that teaching how malicious software is developed will lead to its students using such knowledge to develop more viruses or worms, or any other malicious code. Similar fears have, in the past, prevented development in medical science, most notably with the ban on dissection of human cadavers for research. Within the computer science field itself that barrier existed around cryptography but has since been overcome and is one of the things commonly taught in classes on security. Often times however these classes are still elective and amount to mostly history classes without any examination of actual source code.

#### Fear of Complicity

Many institutions, and educators, are worried that teaching students how malicious code is made could be considered aiding and abetting should one of those students go on to use that knowledge to commit crimes. The same concern could be applied to medical research, or in chemistry. In those fields most people would agree educators would not be held responsible for the independent decisions of an individual student to abuse the knowledge they were taught.

It is important we overcome these two fears as have other fields of study. As technology finds its way into more aspects of our lives it becomes increasingly important that we can trust this technology to not be compromised. Once we being to move past these two fears we can begin addressing the final roadblock.

#### Lack of Preparedness

Many educators currently have little to no experience with malicious software, after all they have gone through the same education system as their students. Sometimes this lack of familiarity is involuntary, and some educators would may wish to teach courses on malware but due to the previously discussed fears many institutions have not the resources to set up new courses for examining and teaching malware.

#### Hopes for the Future

It is important to continue and build upon the work being done by the current educators teaching malware-focused courses like the ones we have discussed today. They have set a precedence, provided a running start and we should not squander the momentum.

As courses in malware become more common so too should the topic become less taboo. The worries of ethical violations will lessen as it has in the medical research field as more students complete these courses and go on to not be terrible people.

With the topic become less taboo in the tech world the discussion should become more mainstream, causing the knowledge to diffuse to the general public. We have seen that happen again within medical research in the form of hygiene.

Ultimately it is hoped that studying malware become a standard component in computer science courses in universities and colleges. This will create a better-prepared generation of software developers and programmers applying security approaches that not only patch the holes in our defenses that are already known, but better anticipate future attacks and can adequately defend against them. Improved understanding of how various malware works should result in better personal security practices of the average user, like improved understanding of germ theory resulted in better personal hygiene.

# References

Ledin, George Jr. (2005). Not teaching viruses and worms is harmful. *Communications of the ACM, 48*(1), 144.

# First Malware

There were some malware for other platforms before 1986, but in 1986 appeared first malware for PC. It was virus called Brain.A. Brain.A was developed in Pakistan, by two brothers -Basit and Amjad. They wanted to prove that PC is not secure platform, so they created virus that was replicating using floppy disks. It infected booting sector of floppy drive and booting sector of every inserted floppy disk. So anytime infected floppy would be inserted into PC, it would infect its drive, so the drive would infected again every disk inserted. Computer security Page 2 of 11 History of malware.

This virus did no harm, and authors were signed in code, with phone numbers and address [2]. Intention of early malware writers was to point on problems, rather than make some harm or damage. But later of course malware become more and more destructive.

[2] Brain: Searching for first PC Virus, Mikko Hypponnen, F-Secure, 2011.