Teach Your Children Well, Part II

This is informal research

- Answers were freeform
- Answers overlapped
- Answers were shared/copied!

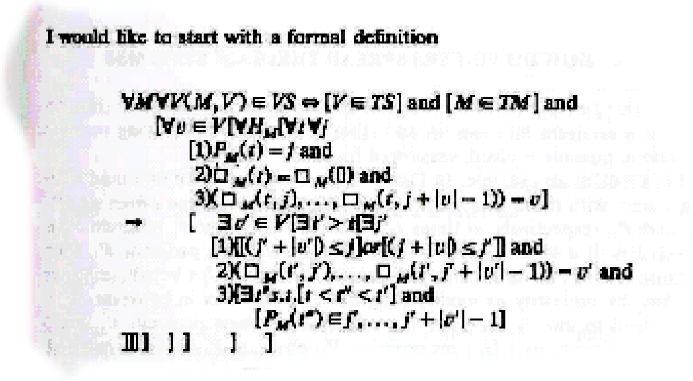
Real Value of the Exercise

- The group discussions that followed
- A snapshot of security awareness among small but disparate groups of young people
- Laying a basis for further research
- Highlighting popular issues and misconceptions

Do you know what a virus is?

- – Yes!
- – Programming Code
- – Hacks into [kills] PCs
- – Infection
- – Replication
- – A program attachment
- – Definition by effect
- – Definition by example

The Irresistible Definition



I would like to start with a formal definition

$$\forall M \forall V (M,V) \in VS \Leftrightarrow [V \in TS] \text{ and } [M \in TM] \text{ and}$$
$$[\forall v \in V [\forall H_M [\forall t \forall j$$
$$[1) P_M(t) = j \text{ and}$$
$$2) \square_M(t) = \square_M(0) \text{ and}$$
$$3)(\square_M(t,j),\ldots,\square_M(t,j+|v|-1)) = v]$$
$$\rightarrow \quad [\ \exists v' \in V [\exists t' > t [\exists j'$$
$$[1)[[(j'+|v'|) \leq j] \text{ or } [(j+|v|) \leq j']] \text{ and}$$
$$2)(\square_M(t',j'),\ldots,\square_M(t',j'+|v'|-1)) = v' \text{ and}$$
$$3)[\exists t'' \text{ s.t. } [t < t'' < t'] \text{ and}$$
$$[P_M(t'') \in j',\ldots,j'+|v'|-1]$$
$$]]]\ ]]\ \ ]\ \ ]$$

Have you ever been affected by a virus?

– About half said no.

– About half said yes.

– Two said yes, frequently, one said yes, once.

– One said “Yes, off a file-sharing program (limewire)”.

– One said “No – I have anti-virus security software.”

– One said “Yes, but sometimes you can’t tell if you have them.”

– One null response.

What are the effects of a virus?

- Crashing or destroyed programs
- Performance issues
- Data/file corruption/deletion
- Screw up PC
- Doesn’t do anything
- Takes control of your computer
- Virtually anything.”
- Don’t know.
- Changes your boot sector
- Spread quickly.
- Eat up your hard drive.

Do you click on every link in an email and open every attachment you receive?

- – Most said no [one said because of viruses]
- – Yes
- – Yes, but scan first
- – Yes, if they look important
- – Yes, because I want to look to see what it is.
- – "Only if it's someone I know." "Depends on the sender."
- – "Download file."

Do you use an easy password?

- – Two said yes.
- – Rest said no: one said “Complicated: contains numbers and letters”; four said “No, otherwise easily discovered.”

How can you surf on the Internet safely?

- Go only on sites you know you can trust
- Use Google “Safesearch” option
- About 50% said “Use anti-virus software”.
- One said “Internet Security”, another said “Security Software”.
- One said “Never click on pop-ups”. One said use a pop-up blocker.
- Three mentioned anti-adware and/or spyware filtering.
- “I don’t know. My AV and firewall doesn’t seem to have any effect.”
- One null response.
- “Don’t click on suspicious links.”
- Don’t give personal details to strangers
- Common sense.
- Going through search engines.

What do you think of virus writing or hacking?

- Disapproval
- Extreme disapproval
- Stupid/foolish/ridiculous/pointless [5]
- Admiration [sometimes grudging]
- Should get tougher sentences and be more tightly controlled.
- Shouldn’t write viruses because it can wreck people’s work and computers.
- Depends on motivation

UK Follow-Up Assignment Questions

Task – Internet Intrusion

- Name at least three types of “viruses” and give an example of each type.
- How do viruses get passed onto your computer?
- Why would someone send a virus across the Internet?
- What must individuals and firms always do to be prepared for the threat of viruses?
- What does the term “social engineering” mean?
- Name three types of web scams
- Create a newsletter (using newspaper column layout) to write about all of the above to be presented to new staff in a company. Give your newsletter an appropriate title and use headings and clipart.

Name at least three types of “viruses” and give an example of each type.

- Macro
- File
- Boot
- Multipartite
- Polymorphic
- Stealth
- Worms
- Trojans
- Backdoor
- Melissa/Michelangelo/Form
- “Normal viruses”

How do viruses get passed onto your computer?

- Email – 25% – one specifically mentioned attachments.
- Downloads – one person mentioned downloads but didn’t specify further.
- Attached to [downloaded] document
- Instant Messaging – surprisingly, given how commonly this seems to be used within that age group, only one respondent mentioned this.
- Browsing
- Internet connection (3)
- Malicious web site
- Filesharing (kazaa, limewire, emule, edonkey, exeem, kiwi alpha, limewire pro, iTunes)
- Floppy disk boot sector

Why would someone send a virus across the Internet?

- As a research project
- Prank
- Vandalism
- To attack the products of specific companies
- To send out a political message.
- To take down a network or a standalone system such as a home PC
- To get hacking access, or to allow the hacker to see your screen (described in this case as a “backdoor virus”).
- Get recognition for their achievement as a virus writer.
- To feel in control of a very large company.
- Disliking someone to the point of wanting to destroy their PC.
- To affect more people and maybe bring down an ISP.
- Revenge

What must individuals and firms always do to be prepared for the threat of viruses?

- Most mentioned anti-virus software. One distinguished between desktop and server AV. One mentioned Norton Internet by name, and one mentioned the need for frequent updates.
- Almost as many mentioned firewalls, but didn’t display much understanding of how firewalls actually work, or the differences between software and corporate firewalls. One or two seemed to confuse firewalls with email filtering, and none distinguished between the types of malware that a firewall might protect against.
- Two mentioned backup.

What does the term "social engineering" mean?

- Suggests a very wide range of definitions, even if you ignore the use of the term in a non-perjorative/sociological/anthropological sense

Name three types of web scams

- Most responses variation on FTC “Dirty Dozen”

Findings

- A search engine doesn’t discriminate between good and bad info
- Children can be
  - Uncritical of what they read
  - Unscrupulous in what they plagiarize

Would an adult do better?

The “Dark Side of the Internet” Presentation

- The significant differences between forms of malicious code were discussed in some detail, including some of the more relevant sub-classifications and -mechanisms.
- Viruses
- Worms
- Trojan horses
- Adware and Spyware
- Bots/botnets

Some more issues we discussed

- "If you can only tell that you have a virus because your anti-virus tells you so, does it matter if it's there or not?"
- "What's the difference between a hacker and a virus writer?"
- "Can a virus damage hardware?"
- "Is virus writing illegal? Is hacking? Is spamming?"
- "What's good/bad about virus writing?"

And…

- “Is there such a thing as a good virus?”
- “How many viruses are there, and how many of them do you need to worry about?”
- Mass-mailers and popular fallacies that surround them

General spam issues

- UCE/UBE
- SPIM
- Text spam
- Fraud
  - Advance fee fraud
  - Phishing/Pharming/Moneylaundering
  - Pyramid schemes et al
  - Cellphone fraud
  - Auction fraud
  - Money mule recruitment
- Hoaxes, chain letters

Why do kids need to know about criminal activity aimed at adults?

- May have part time jobs and be close to school-leaving age
- Anyone is old enough to be exposed to the material
- May have access to own or others’ financial facilities
- May be able to mislead/educate their elders

Other risk areas

- Texting
- IM
- Hoaxes and chainmail

No pr0n discussed here

- Lots of research on the subject already
- Google SafeSearch as an introduction to filtering problems
- Paedophilia – important topic, but no time to discuss at length

Other areas for follow-up studies and discussions

- Countermeasures against:
- Malware, Spam, Adware/Spyware
- Online fraud
- Wi-fi/broadband/bluetooth vulnerabilities

More topics…

- Encryption and authentication
  - What is it, and how does it work?
  - Where is it appropriate?
  - What is an effective password?
  - What alternative means of authentication are there?
  - Is an encrypted object always safe and secure?

And more topics…

- Anonymity
- IT ethics/morality
- Personal abuse & netiquette
- ID Theft
- Piracy & file-sharing

Implications for Educators

- Teachers and autonomy
- Teaching material based on poor or out-of-date information

The Misinformation Superhighway

- Misinformation that passes exams
- Are children more or less vulnerable than adults?
  - More use of contexts of maximum exposure
  - Vulnerable to predatory attacks on juveniles
  - Inexperience

The Generation Gap

- The “children are IT experts” fallacy
- Failure of moral/ethical grounding
- Talking up the expertise of the black hat increases its glamour

Eddy’s conclusions revisited

- Children of that age don’t seem to know very well what computer security is!
- We must start ethical computer education at a much earlier age, if we want to change people’s behaviour and reduce the attractiveness of becoming a virus-writer, hacker or spyware-writer.
- Incorporate this information inside the MEGA/DARE project
- Bringing in more psychological elements and Re-evaluation next year
- Investigate if this can be done elsewhere .. worldwide?

Thinking Globally

- Conflicting info
- Official Misinformation
- Need for:
  - A trusted environment
  - Security information filtering
  - Access to expert advice
  - Early warning of threats
  - Strategic decision support
  - Improved awareness

Any questions?

- david.a.harley@gmail.com,
- Eddy.Willems@be.noxs.com
- jharley@Bohunt.Hants.sch.uk