# Who will tame the Wild West?

David D. Clark

MIT CFP

October 2008

# The issue

- Your computer is constantly under attack.
- You have no right of self-defense.
  - In other words, offense to defend yourself.
- If an attacker can attack repeatedly without deterrence, the attack will eventually succeed.
- Deterrence is ineffective today.
- The public sector has little capability (and no obligation) to defend you.

# Self defense

- IANAL
- Classic self-defense (e.g. shooting the intruder) applies only in case where death or grievous bodily harm is feared.
  - A weak defense if only to protect property.
- If you get into a fight, even though “he started it”, both parties may be charged.
  - The law prosecutes the winner…
- “Active defense” is highly suspect.

# Defending your PC…

- The legality of defending your computer by attacking the attacker has (to my knowledge) never been tested.
- Case law would suggest that the response must no more than match the initial assault, and must be based on a clear assessment by the victim of what his level of peril is.

# The duty of government

- In case of violent crime, they try real hard to “get there in time”.
- They have no obligation to protect.
- In the case of cyber-crime, they have no skills and the timing is all wrong.

# Deterrence

- Even the government, with its instruments of intelligence, is hard-pressed to tell where a sophisticated attack comes from.
- The immediate source of most attacks is an innocent PC that has been subverted.
  - What would it mean to deter this intermediate?

# So what is going to happen?

- (I predict that) there will be a movement toward a position that attacks against computers (both business and consumer) cannot be tolerated at the current levels.
  - “Something has to be done”.
- But what shape might that “something” take?

# Repeated attacks

- I said “attack repeatedly without deterrence…”.
- If we cannot attribute attack, the only remaining deterrence is making the attacks no longer cost-effective.
- Hint:
  - Attacks against business--high value.
  - Attacks against home computer--low value.

# Cost models of attacks

- Researchers are beginning to develop models for the value of a penetrated machine.
  - Going rate for spam proxy: 3-10 cents/host/week.
    - Stefan Savage, talk at NDSS 2005
  - He has lots of other cool facts.
    - Jason Franklin, Vern Paxson, Adrian Perrig and Stefan Savage, *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants*, Proceedings of the ACM Conference on Computer and Communications Security (CCS), Washington, D.C., October 2007.

# Stefan Savage

- His quote: “Chicken Little was an optimist”.
- His formula to control bots:
  - Prevention
    - Improve software quality.
    - Software heterogeneity (including artificial).
    - Rapid software updating.
    - Good hygiene: keep susceptible hosts off the net.
  - Containment
    - Slow down sending
    - Quarantine infested host

# Conclusion:

- If I do not have the right to fight back.
- If the government is essentially useless to defend me.
- If the problem keeps getting worse.
- Then someone will be given the job, and it is going to be (at least in part) the ISP.
  - Refer to  Stefan’s conclusions above.
- Another legal principle (IANAL) : liability should be assigned to the party who is best able to avoid a particular harm.
  - Who better than the ISP? Seriously?

# Another expert

- Dan Geer, *Playing for Keeps, ACM* Queue vol. 4, no. 9 - November 2006
- Only three possible futures
  - Abandon general purpose PCs for server-based applications and thin, fixed function clients.
  - Universal surveillance.
  - Both of the above.

# Across the board

- Consumer
- Industry/govt
- Military
- All are moving toward positioning the (some) responsibility “in the net”.
  - Government to redesign its networks to limit access points for better protection.
    - See Op-Ed by Melissa Hathaway, Cyber Coordination Executive for the Office of the Director of National Intelligence, published by the McClatchy-Tribune News Service on Wednesday, October 8, 2008

# Your choices (you=access ISP)

- Argue that this is not your job.
  - Win for a while, then be required to do it.
- Step up and get ahead of the curve.
  - Work out your preferred role in the ecosystem.
  - Perhaps monetize the solution.
  - (You don’t get paid to conform to regulation.)
- Get your R&D labs working on this
  - …

# Revisit active defense

- Rate limit the attacker.
  - If only to the victim, almost certainly ok. Victim can request.
  - But if to everyone?
- Send a puzzle.
  - If in a protocol and standardized as common practice, probably ok.
- Send attacker some Javascript or otherwise stun it?
- Take it off the net?
  - If this is a part of your terms of service…
    - MIT does this all the time.
  - The ISP can, but another user cannot, certainly.
- Tag traffic with its degree of misbehavior?
  - Blacklisting in all its forms.