Incentives in Security

Distributed Denial of Service (DDOS)

Egress Filtering - is the practice of monitoring and potentially restricting the flow of information outbound from one network to another. (Implemented by ISP in this example)

This is an example of failure of incentives. Egress Filtering is something easy to implement and could vastly improve security but since there’s no incentives for it on the ISP’s part then no one implements it.

Sony DRM Fiasco

Sony was releasing audio CD’s and they wanted to prevent piracy of said CD’s.

XCP (DRM software)

Media Max v3 and v5 (DRM software)

So for audio CD’s the audio data gets written from the inside out. The DRM software (data) would be written on the CD and would be written from the outside in. If you put the CD in a windows (Mac and Linux wouldn’t auto run so you can rip it as you please) machine it would auto run.

Auto run:

- Display EULA and set approval.
- Since you could still rip the software before accepting the EULA……….. They installed a “temporary” protection mechanism.
- Mechanism that checks against all running processes for known ripping software and would eject the CD.
- Lock CD Tray
- Change Name of Ripping App

- There’s another Temporary protection mechanism that would install Pre-emptively.
- A driver would be installed to do monitoring.
- Not marked to be restarted on reboot.
- Since there was a difference in versions (v3 and v5), the newer version misinterpreted the temporary leftover stuff it would assume the user agreed to the EULA and would permanently install its protection mechanism on the system.
- This would install itself into a world writable directory. This is or could be a huge security exploit, by giving arbitrary users root power.
- Every time you put a CD in the drive with this software it would check the permissions of this world writable drive. So if a smart user had seen this directory change to world write able and changed it back to secure permissions, the CD would complain about not having proper permissions.

The incentive here is for the company making the protection software to get their software on as many computers as possible to market their software/themselves to be put on SONY or other larger companies CD’s.

- To violate the Copyright software you could take a sharpie marker and black out the DRM software portion of the CD. The audio portion would/will still run.

XCP and Media Max must recognize protected CD’s. (They must distinguish between CD’s their supposed to protect and one’s their not supposed to protect)

- Need to mark CD’s somehow arises
- Mark Must be unforgivable
- Mark should be indelible.

One of the companies had a solution: Using a sequence of samples to mark the 3 least significant bits in order to encode some security feature. – This is hard to forge but it’s not indelible.

This became a PR disaster for XCP, Media Max, and Sony because it was making peoples systems less secure.

Their answer to this was an uninstaller.

**Uninstaller Fiasco:**

- You had to install and Active X control
- Run anything you want on my system control. Because after it was done doing its intended purpose any webpage could use this Active X control to install whatever they’d like.
- This lead eventually to a class action lawsuit and a real, better, uninstaller.