Recurring patterns in processes of IPR infringement

Jarmo van Lenthe
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
jarmo@jarmovanlenthe.nl

ABSTRACT
Objective: To find patterns in the criminal process of infringement of intellectual property (IPR), to prevent such crimes from taking place in the future. Methods: By creating models from a study on three police files and verification of this model by conducting two expert interviews with police officers. Conclusions: Patterns are found in the background of the pirates and also in resources and organization of the criminal process. Contribution: Improving knowledge about the criminal process of IPR infringement and providing situational crime prevention analysis.

Keywords
Digital piracy, prevention, cybercrime, patterns, infringement of intellectual property, IPR

1. INTRODUCTION
There is a lot of cybercrime going on in the world right now. For law enforcement purposes, it’s very important to know how digital pirates do what they do and what similarities can be found in several cases, to construct an efficient way to prevent IPR infringement. In this paper, research will be described in the field of digital piracy. Digital piracy can be described as “the illegal reproduction, supply and distribution of copyrighted materials such as music, movies and software”. The goal is to find patterns by studying several cases of digital piracy. These patterns could include matching actors, matching networks or matching facilitations (or facilitators). This study looks into the process one goes through to reveal oneself as a digital pirate and also the process of a piracy attack.

One can commit infringement of IPR in many ways. Filming movies in the cinema and distributing them online is an example. This is not the field on which this research is focused. This research will look into the high tech ways of committing infringement of IPR. This can be done by stealing materials, such as games, movies and music from servers of producers and distributing them online for instance.

This research works in the scope of the Dutch legislation. Downloading is not offending the law on infringement of IPR (to some extent because of the law on the homecopy of Article 16b Aw), while distributing is. A consequence of this is that there are only cases on hacking and distribution of materials with IPR in the Netherlands. Downloading such materials doesn’t bring forth an investigation in the Netherlands.

The main research question is:

Which patterns can be found in the criminal process of infringement of intellectual property (IPR)?

Before an answer to this question can be given, an overview of the field of IPR infringement is needed. To achieve this, a subquestion is formulated.

- How is infringement of IPR, as part of cybercrime, organized?
  - Hopefully, this will result in several explanations. Maybe there are criminal organizations or well-organized individuals behind this, so the following questions can be asked:
    - How do they distribute their files?
    - How do organizations and well-organized individuals hide themselves from law enforcement?

According to Repicky [6], there are five ways of stopping digital piracy: education, public law enforcement, lawsuits from businesses, technology (like fingerprinting [8] and making use of secure Digital Signal Processors (DSP’s) [5]) and lowering of prices of software. Fear is to be induced on criminals, to prevent crimes from being committed again. For public law enforcement, this means that the police has to have an efficient method of catching criminals.

In the United States of America, a new bill is proposed: the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property (PROTECT IP) Act [2]. This bill is an amendment of the controversial and much discussed Combating Online Infringement and Counterfeits Act (COICA) [7], which never became law. The PROTECT IP bill has a proposal for implementing an DNS filter. This measure uses millions of DNS servers to censor domain names who provide illegal content. IPR infringement seems to be very important for the USA, as this measure goes against the security extensions which come with DNSSEC [4]. The PROTECT IP Act is reported by the Senate committee on May 26, 2011. This could affect the future of IPR infringement and its prevention.

To show that certain patterns exist, first presumptions are gathered from case files of the Netherlands’ Police Agency. The presumptions gathered here will be used as basis for interview questions which will be used when interviewing
experts. These experts are police officers who have worked on cases of digital piracy. Then, the results will be stated and discussed.

2. CASE STUDY

First, a background of hackers has to be given. The hackers start out from school. They are students who are interested in IT or IT professionals without enough work, so they find other activities to spend their time on, such as hacking.

The case study consists of two parts: a part about the evolution from script kiddie to hacker and a part about the criminal process of digital piracy. The focus will be on the process, but a little background is useful.

By studying the police files of the Netherlands’ Police Agency, several similarities have been found. The digital pirates questioned in the cases are mostly working with IT or have studied IT. Interest in hacking is developing by boredom at school, low work load or social pressure from (online) friends. After a while, some experience is gained and the pirate is becoming involved in piracy networks, where every pirate has his own specialty.

The hackers in a network help each other. They can communicate over several networks. Amongst these networks are MSN, IRC and ICQ. Because of every pirate having his own specialty, all pirates can carry out small jobs. Those small jobs are carried out separately and are rather inconspicuous. Large companies get attacked multiple times a day, so one attack more will not stand out. When combined, the jobs form the complete hack. In the networks studied, carrying out jobs happens on a voluntary basis. This is less voluntary as it seems, because accomplishing jobs and helping the other hackers give a pirate more status.

A pirate can use exploits to get to administrator passwords, while another can, when the passwords are given to him, create a network map. From this network map, interesting targets are chosen. When a pirate downloads software from a hacked server, another pirate, called a filler, posts it on a torrent site, where it thus can be downloaded by the public.

In one case studied at the Netherlands’ Police Agency, the pirates could skip the step of retrieving a password, because those were already available. Other hackers had already retrieved them, but the questioned hackers did not know where those came from and it was not investigated.

For computer science, the tools which these pirates use are very interesting. For the hacking of the first computer of a network, a program called Acunetix Web Vulnerability Scanner (WVS) is sometimes used. This program crawls a web server and carries out a port scan. Network administrators can use this program to scan their network for vulnerabilities. During the port scan, the applications with version numbers behind these ports are listed. For the respective applications, many exploits to get shell access or executing arbitrary scripts can be found on the internet (for instance www.exploit-db.com and miw0rm).

When hackers use these exploits, easy access to servers is almost granted.

For this research, a WVS scan was carried out on I. C. T. S. V. Inter-Actief, the study association for computer science of the University of Twente. On port 22 (the standard port for SSH) "SSH-2.0-OpenSSH-20061110" was found. This is an up-to-date version of the OpenSSH application for FreeBSD. For an older version (<4.3p1) there are exploits listed on exploit-db.com which cause Denial of Service. Network administrators should therefore always use up-to-date, secure software. Although a scan is carried out for this research, an attack is omitted, as this is illegal. This little experiment shows that it is really easy to find exploits. Had we found "ncftpd < 2.8.5", exploit-db would have provided an exploit to break out of the jail which the FTP daemon is in. This would give access to all files on the server, instead of only the files meant for FTP.

To get to the passwords of an administrator, pirates install a type of keylogger on a hacked computer (they have ‘normal user’ access). This keylogger sends the administrator’s username and password to a pirate. Administrator passwords are likely to be roaming passwords, they work on all computers in a certain domain. An example is MCAF.DLL, this is an DLL file which alters the login process of Windows. This dll-file sends the username and password to a server. Easy does it.

When pirates have full access to a server, it’s likely that they install an FTP server on it. They can then download all files they want from there. They will do this through a proxy, like Proxycap.

In one big case, the software is then given to a filler. A filler isn’t necessarily a hacker, but he is a pirate who has an account on websites where illegal software can be uploaded. From these webpages, the software is accessible by everybody who has the link. The link can be distributed via Instant Messaging, publishing on websites and so on.

What seemed from the case files is that the pirates, after the whole hacking process, are likely to brag about their accomplishments to other hackers on IRC or on their forums. The presumption that pirates do what they do to

3. EXPERT INTERVIEWS
To verify the model constructed in the previous section, expert interviews were held. The two experts interviewed for this research are police officers of the National High Tech Crime Unit (NHTCU) of the Netherlands’ Police Agency, who have all been working on a minimum of one case of digital piracy as digital investigator. These cases are also the cases from whose files the model is constructed. The officers have worked for the NHTCU since its creation in 2006.

The interview consists of two parts, just like the case study: a part about the evolution from script kiddie to hacker and a part about the criminal process of digital piracy. In the second part of the interview, there are five blocks of questions: first some questions about cooperation and communication, then about hacking servers, some about fillers, some about the rewards of IPR infringement and at last some about the hiding and finding of IPR infringement organizations. These questions are fairly common, although some are inspired by what is found in the case files.

The police officers were first asked:

What percentage of pirates is an IT professional?

The respondents could not determine a good estimate, but did have a strong opinion. Certainly not all pirates are IT professionals, they have very different professions, from lawyer to accountant, but also network administrator of a company. All pirates have in common that they have taken an unhealthy interest in computers and hacking. To get a deeper understanding of the development of this interest, the next questions were asked to the respondents:

Is this interest stimulated by peer pressure?

This proved not to be the case. The pirates are roughly to be categorized in two groups, which do not have to be distinct. The first group are the script kiddies who tried some hacking over and over again to finally develop some hacking skills and did not oversee the consequences of their actions until they were in too deep and got caught. The other group is the group consisting of computer geeks, who are socially isolated but have a great skill in hacking. The members of both groups are considered nifty people, who are always trying new things. Of the IT professionals and IT students, it is interesting to know if the work load of their jobs or studies influence them towards hacking. The respondents were therefore asked:

Has the work load of pirates anything to do with whether they are going to hack?

The respondents confirm this question. One respondent has the following example: when the work load is low, network administrators sometimes monitor and scan their own network for security purposes. If they harvest some interesting results, the next step is taken: they scan networks of other companies to check how security is handled there. It’s all on a roll from here. They try an exploit for a security vulnerability and, when all goes as intended, they are inside someone else’s network. It goes from bad to worse and someone downloads files from that network.

Another side of the story is that the IT professionals share their knowledge with other IT professionals. If one has some knowledge of hacking and he shares this knowledge with others, they can be inclined to try it themselves.

The preceding questions give some insight in the profile of a hacker. According to the police officers they are people who have an unhealthy interest for IT and who mostly have stumbled upon hacking accidentally, but found it interesting. They get in too deep before they realize what the consequences are.

Now, for the criminal process. A series of fourteen questions were asked to the police officers. By asking these questions, the features of the criminal process of digital piracy are explored.

From the case files, it seemed that in this process, there’s always some kind of cooperation. This presumption is tested by asking the question:

What percentage of digital piracy cases involves a criminal organization?

The police officers stated that there are many crimes committed by hackers by their own, but that whenever the operation gets bigger, more people are needed, because of different hackers having different specialties. Percentages called were even between 90% to 100%, for serious crimes. This is a really high number, which can be explained by the fact that a lot of specialized knowledge is needed for a big job. Only in a group, this knowledge can be present.

These specialties include retrieving passwords, creating a network map and installing software to download files from a server. The officers also stated that, in an organization, multiple offenders are often in a crime together for sharing knowledge.

It is useful to know if the pirates already know each other beforehand and if they know each other in real life or just digitally. The question asked was as follows:

Do pirates know each other in the real world or just in the digital world?

The police officers said that the hackers mostly only knew each other’s digital identity and mostly through chat applications such as MSN, ICQ and IRC. The officers said that hackers in one case met each other in real life for the first time in the court room or were surprised to see that the gender of the other was not the gender they had expected.

Because of the large scale on which piracy is committed, taken into account the cooperation, one wonders if the actions done by one hacker are distinguishable by security officers. The following question was asked to find out.

Do the separate actions of the hackers in an organization stand out?

The officers explained that companies are often so big, that an attack on one server isn’t something that stands out and that even very large companies that have a huge IT infrastructure are sometimes part of a large botnet. This isn’t the only important part of security flaws. Social engineering is a part of this too, employees tend to
be sloppy when it comes to IT security. An example of this is when a network administrator posts a question on a forum, indicating his name. When a hacker searches for this name on the internet, he could stumble upon the company where the network administrator works. When the hacker calls the helpdesk of that company and impersonates the network administrator and asks to change the administrator’s password, the hacker will own the password. There is no case yet in which this has happened, but the police officers know this happens for a fact.

Because of all the steps used in the criminal process, the next question was asked because of doubt on the necessity of every one of these steps. The question was

Is there a consequent line of work, or can some intermediate tasks skipped during some attacks?

The police officers said that no one, or no step, is indispensable, but for instance the step of running a scan, or making a network chart can make the process more efficient. Therefore, when a job becomes bigger, more steps are involved.

The next question is of a more basal type. It reads

It is necessary to hack a server or can someone commit piracy without doing so?

It turned out that hacking is necessary for committing piracy and, moreover, one police officer explained that mostly servers of large companies and universities are victim to attack. These institutions have servers with a lot of storage space and fast internet connections. Those institutions are therefore popular with pirates.

From the case files, it seemed that there is always some kind of scan involved. From the answers to the next question it can be concluded that this is almost always so.

What percentage of hacks is preceded by a vulnerability scan?

Hackers make vulnerability scans so that they have something to aim their attacks at. These scans are executed quite extensive, as it seems. Some pirates have a directory structure full of scan outputs from Acunetix. This scanner extensively scans a server by opening a lot of connections to a server and probing every port. So extensively even, that when a server is incapable of handling such stream of connections, the scan could be seen as a Denial of Service attack.

The goal of scanning a server is to find vulnerabilities which can be exploited. But in how many cases is an exploit actually used? This question was asked to the officers. They could not give an exact percentage, but claim this is done a lot. It is not the only way to get into a network. For instance social engineering is also often used for this.

The case study revealed that, with big jobs, fillers are involved. These are the pirates who distribute the captured software. Because these people are really involved, but they don’t need hacking skills to do what they do, why are they allowed to the piracy organizations? The first question which is to shed light on this is:

Is software always distributed to people by fillers?

The police officers explained that evolved script kiddies do not use fillers. For them, it’s the fun of succeeding in hacking that counts. In piracy organizations, the responsibilities are well distributed amongst it’s members and fillers are used many times.

The second question on fillers reads:

Are fillers hackers too or do they only put the software online?

In other words: do the fillers have hacking skills? The police officers expect the fillers to have some skill in hacking. They are members of the hacking society, where you are not allowed in if you cannot show some hacking skills first. The respondents are not too sure of this, as not much is known about the fillers.

Where do the pirates post their captured software?

That is the next question asked to the police officers. From the case files and white papers of other investigation agencies, came the picture that they use upload sites like MegaUpload. The officers think that they use a variety of distribution solutions. These solutions include torrent sites, useenet and upload sites like MegaUpload. In September 2003, the Dutch government accepted an amendment in the law of criminal procedures, which allows police officers to claim information from providers to identify the person behind an IP address. This has speeded up the process a lot.

Why do pirates commit piracy acts? What is in it for them? The police officers were asked:

Is there a lot of money to piracy?

They responded that they had not seen this phenomenon yet. They speculated that piracy is committed to just watch movies for free or use software for free. The officers furthermore speculated that when the source of an application or game leaks before the publication date, it is very possible to extort money from the companies whom made the software.

If not for the money, is it fame that drives these criminals? This is what seemed from the case files. The police officers agreed. Especially in the beginning, the hackers want to show who they are and show the other hackers that they have the right stuff. They want to brag about their accomplishments, which you can only do when you really did accomplish something. Furthermore, there are multiple piracy organizations, who vie to be the first who publish new software to the public.

Last but not least, some questions about the organizations were asked. Piracy is done on such great scale, why aren’t many more of those organizations discovered? The answer to that should be given by asking

Do the organizations use techniques to hide themselves from law enforcement?

The police officers explained that the hackers are disguised themselves by taken on an digital, anonymous identity and by protecting their forums with IP blocks for instance. With those IP blocks, only registered IP addresses can access the website. Often, the activity on those websites is only traceable by tapping that website’s connection with the outside world. The problem is, that is only possible for law enforcement when there already is a suspicion.

But how are those organizations found then? The police officers were asked:
Does the police discover these organizations themselves or is she tipped?

The police isn’t looking for these networks proactively, but are guided by reports that are filed by companies who fell victim to piracy or when they get a tip. Sometimes, an informant is involved in this process. It also happens that the investigators stumble upon organizations during an ongoing investigation, from which new investigations start.

4. CONCLUSIONS

From the case files and the interviews, some similarities are found. The background of IT is found in every case and is supported by the interviewed police officers. The problem with this is that it’s only the interest of IT which is found, not a professional or educational background. The assumption that peer pressure is a source of new pirates is wrong, as they are socially isolated people who don’t have many friends to pressure. The work load is a factor though. It enables people to try things, even hacking. Before they know it, they are in too deep. Pirates generally don’t know each other in real life, but communicate by means of chatting.

Organizations show up in many big IPR infringement cases, although small hacks can be committed by hackers on their own. This is because different pirates have different specialties and many aspects of hacking are necessary for accomplishing IPR infringement the high tech way. The different steps don’t stand out on their own in the loads of attacks that companies and universities are victim to. Not every step that is taken is necessary for the capturing of material with IPR. Because it’s easy, big jobs are preceded by vulnerability scans. There is no proof that this is always true, but the experts think it’s almost always the case. By exploiting these vulnerabilities, it’s easy to get into a server.

The organizations use techniques like IP blocks to hide themselves for the outside world. The hackers use digital identities which make them quite anonymous. The police doesn’t track organizations proactively, but is put on their tail by means of filed reports, tips and informants. Sometimes, she stumbles upon new cases of IPR infringement when investigating another case.

Fillers are used in big jobs and not so much in small jobs. They have some hacking skill, which they needed to get into the hackers environment, but they don’t have to use that in their part of the job.

There haven’t been cases in which a lot of money is made on IPR infringement, but it is possible to turn IPR infringement into a large turnover.

The conclusions are listed in Table 1.

<table>
<thead>
<tr>
<th>Part</th>
<th>Table 1. Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background</td>
<td>Interested in IT</td>
</tr>
<tr>
<td></td>
<td>Low work load</td>
</tr>
<tr>
<td>Organizations</td>
<td>Necessary in big cases</td>
</tr>
<tr>
<td></td>
<td>Different specialties</td>
</tr>
<tr>
<td></td>
<td>Easy with scanning and using exploits</td>
</tr>
<tr>
<td></td>
<td>Use techniques to hide themselves from law enforcement</td>
</tr>
<tr>
<td>Fillers</td>
<td>Are common in big jobs</td>
</tr>
<tr>
<td></td>
<td>Need hacking skill to get into an organization</td>
</tr>
<tr>
<td></td>
<td>Don’t need to use hacking skill</td>
</tr>
<tr>
<td>Rewards</td>
<td>Money can be made, isn’t seen yet</td>
</tr>
</tbody>
</table>

This paper could be statistically proved when there are more cases on this field.

4.2 Future research

The part that fillers play in the process of infringement of IPR is not very clear at this moment. They are not the part of the process on which the police focuses. Because of the role they play in the distribution of captured software, it must be stressed that these players have to be taken out of the game.

Another topic for future research is the role of the facilitators of upload sites. The reason for this is twofold. One needs a paid account before one can upload to that site. These websites are used for captured software. It is expected that, because it is just plain illegal to distribute captured software but these websites are used much, that the owners of such websites make a lot of money. So, that’s money from an illegal source!

5. REFERENCES


APPENDIX

In this appendix, a scheme of a situational crime prevention analysis is given. First a general scheme will be presented. Then, a zoom-in of the separate relevant nodes is presented. The subjects for future research are suffixed with an question mark. Law enforcement can prevent this type of cybercrime by preventing the presence of an arrow, preferably the one that occurs most frequently.
Figure 2. Situational crime prevention analysis. The convergence settings include forums, Instant Messaging (IRC, MSN, ICQ, Jabber) and email. The process of figure 1 can be seen as an interpretation of this figure, without the end users.

Figure 3. Zoom-in on the pirate.