黑客用來尊重字

許多黑客從他的憤怒，恐懼和貪婪陷入陰暗面

社會的決定，以保護從黑暗的工程師用戶

Security Wars
Light Side and dark side of Hacker Power

Ikuo Takahashi

小故事1 黑客暗黑面

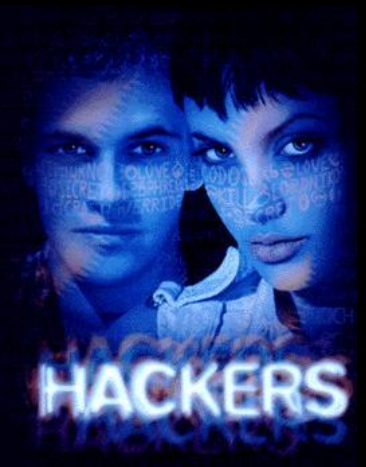
Episode 1

Dark Side of Hackers

Dark side of Hackers

- Definition-Hacker
  - A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular.
  - As if manipulate computers “wizard”
- Force
  - Source of power of Jedi
  - “field of energy”
- Refer; dark side of force
  - The Force has a "dark side", which feeds off emotions such as anger and fear from“wikipedia”

黑客尊称-暗黑面 墮落 怒・恐感情



The Lost Twenty

二〇 暗黒卿－暗黒客

- Star Wars

"The Lost twenty, as they have been known since Dooku joined their number,are remembered with both honor and regret among Jedi; their images, sculpted from bronzium, stand enshrined in the Temple archives."

- We can count famous or notorious hackers as follows;
  - Pakistan brain virus(1986)
  - Internet Worm(1988)
    - Robert T. Morris
  - Melissa Virus(1999)

“Office” case in JP

- Kawai (handle name “Office”)
  - office found the CGI vulnerability of webpage ASKACCS（copyright. privacy BBS） operated ACCS
  - stolen the personal information of 1,200 people, including their names, addresses and phone numbers, from the Association of Copyright for Computer Software Web site between Nov. 6 and 8.
  - office unauthorised access at least four times using above way
  - On Nov.8,2003,Office taught people attending an event in Tokyo how to gain unauthorized access to computers at”A.D.2003”
  - explained the way of attack with ppt slide with actual personal information
  - Above ppt slide was downloaded by 12 persons
  - noticed the vulnerability to ACCS by e-mail in the evening of his presentation
  - Asahi newspaper reported on Jan.4,2004. “warning to vulnerability”
  - Police arrested Kawai on suspicion of breaking into computer and obstructing business.

ACCS黒客事件
表於討論会
「侵入」事件公

Hacking method-Office

侵入手法

- cgi vulnerability
  - ACCS page’s posting form used the cgi for the confirming the contents of posting.
  - cgi’s vulnerability reveal the source of cgi when put the cgi into parameter.
  - confirm the file name where the excel file is stored.
  - If put the file name into cgi parameter,the contents of excel file is revealed.

Issues in Office's case

題 不正侵入禁止法適用、脆弱性情報公開手法、公媒体対応問

- applicability of Unauthorized access prohibition law
  - preparing the file,finally he put the file name to address bar.
- obstructing the association's business-not prosecuted
- freedom of expression and vulnerability information
- ACCS as webhosting user
- crisis communication of Kyoto university
- injunction

Sentenced guilty

有罪判決

- Tokyo district court March25,2005
  - “Access administrator didn’t authorise any people by this access activity.”
  - Viewing of cgi and this case log file were access controlled.”
- *Don’t misunderstand*
  - He actually broke into computer.
  - He was not prosecuted in the security symposium presentation.

Tsunami hacker case in UK

英国津波黑客事件

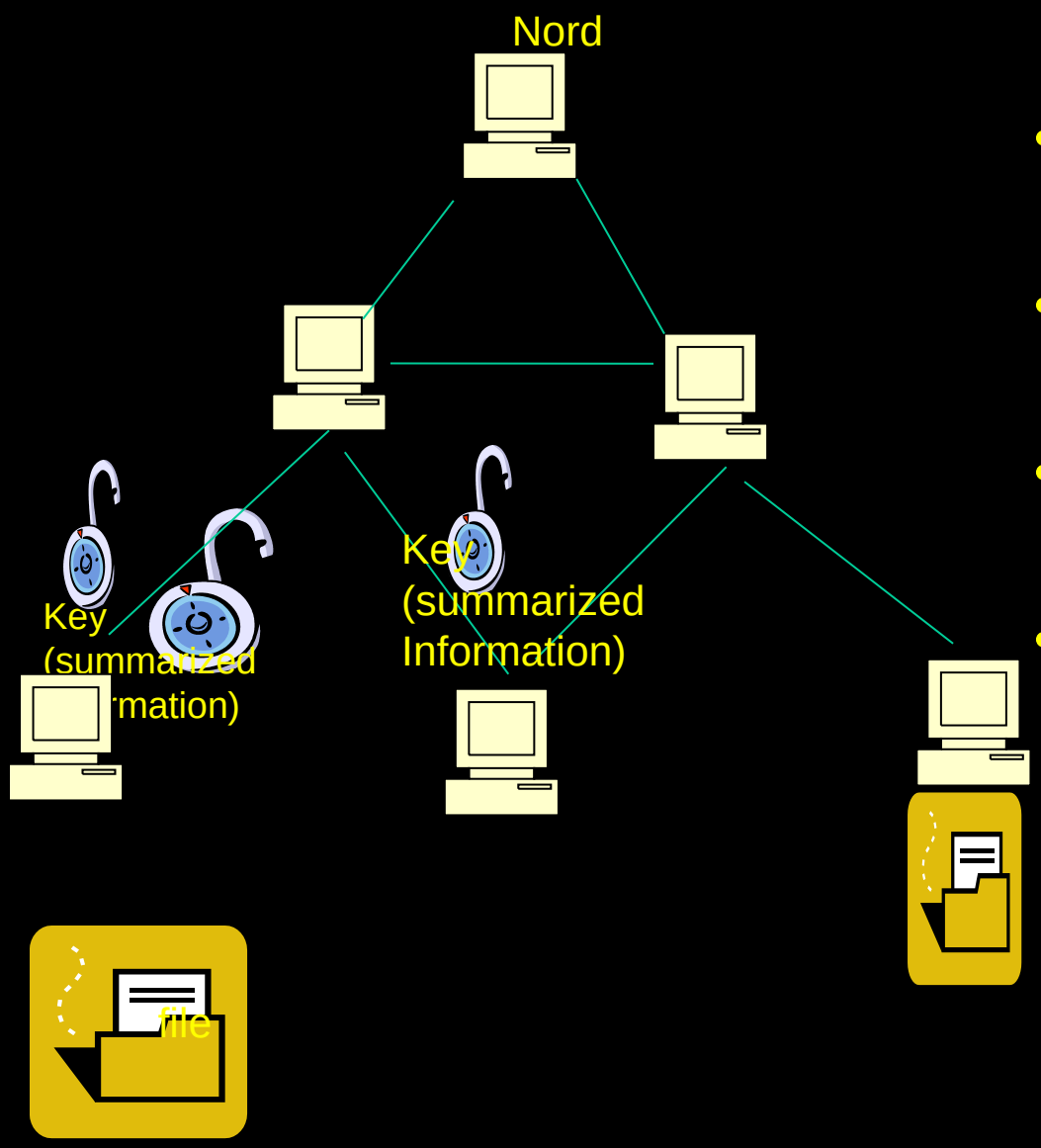
- Daniel Cuthbert
  - security consultant at ABN Amro, lecturer at Westminster and Royal Holloway universities
- December 31, 2004, Cuthbert became concerned that a website collecting credit card details for donations to the Tsunami appeal could be a phishing site.
- After making a donation, and not seeing a final confirmation or thank-you page, Cuthbert put ../../../ into the address line.
- Alarm of Intrusion Detection System at BT‘s offices and call the police.
- convicted of breaking the Computer Misuse Act, fined £400, and ordered to pay £600 in costs.

Tsunami hacker case difficulties in criminal sanction

- motivation of inputting ../../../
  - confirm the site's
- limitation of terminology of Computer Misuse Act 1990
- Daniel understand that he was unauthorised.

- CMA 1990 section 17
  - (5) Access of any kind by any person to any program or data held in a computer is unauthorised if— .
    - (a) he is not himself entitled to control access of the kind in question to the program or data; and .
    - (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

Winny Case-Winny Network



- Application of Pure P2P network
- Each nord duplicate file at back ground
- Retrieve file via “Key file” which is encrypted.
- Difficult to find first sender

Winny事件 P2P電網 暗号化 匿名性特徴 背後複製

Winny programmer criminal case

- Principals case (Kyoto district court Nov.30,2004)
  - Two Winny users guilty for Winny to distribute twenty-eight movies and games (violation of copyright law).
- Mr.Kaneko, programmer, was prosecuted
- Cause of prosecution
  - Aiding and abetting two users
  - provide above two users to download the Winny2.Oβ 6.47

正犯者事件 軟件作者刑事事件
「提供行為」違法性認定

Kaneko's allegation

- not guilty
  - merely experimenting with a new technology
  - not intend to promote any illegal activity

軟件作者 無罪主張

Kyoto District court Dec.13,2006

- Guilty convicted fined \1,500,000- ($14,400)
- mens rea
  - Recognition and admission
    - recognized
      - the program was used for transmitting copyright protected works by general public widely
    - admit
      - above situation and intentionally upload Winny program to the public.

一五〇万円罰金
主観面－当時状況認識・認容
配布提供

Osaka high court-Oct. 8,2009 Not guilty

大阪高等裁判所　無罪

(1) technical evaluation of Winny

Neutral in value. (not intend to criminal purpose)

(2)Criticize against standard by district court

- It's difficult to understand the situations of copyright infringement by file sharing software and district court standard is ambiguous

(3)Standard by appeal court

- If the court admit the abet offense in providing value neutral software, provider may face the possibility of offense as long as third party may make a offense using the software.
- The court should be prudent in criminal responsibility from the aspect of principle that offences should be created by legislature (principle of legality).
- The court have the opinion that it is not enough that the provider of software had the recognize and allow possibility and probability that unspecified or mass person may make an offense, it is necessary for an offense that provider recommend the software for only or mainly the illegal activity.

Supreme Court-Dec.19,2011
Sustain-High court decision(Not guilty)

最高裁判所無罪維持

- Distributing value neutral software via Internet constitute aiding and abetting only when there is actual (copyright)infringement beyond general possibility and distributor recognize such situation.
  - (1)Software distributor publish and distribute the software for which is misused for the actual copyright infringement and recognized such situation.
  - (2) Based on the software's nature, objective use situation and method of distribution, high probability is required that not exceptional portion of the person use the software for copyright infringement. Distributor publish and provide the software recognizing such situation. Principal use the software for copyright infringement.

Comments

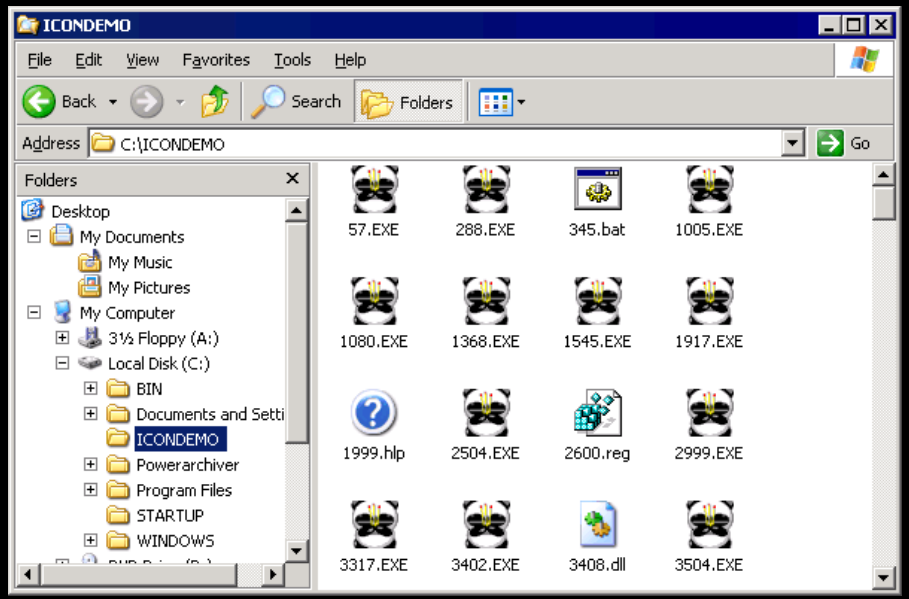
- accused activity
  - providing the software
  - not making, developing
  - often misunderstood
- misuse of anonymity
- no software forensic technique in trial
- Scope is not so wide

分析 配布行為 違法性 軟件分析手法 狭射程距離

Panda Virus case

大熊猫病毒事件

- Fujacks worm (also known as Worm.Whboy) (2006)
  - converted icons of infected programs into a picture of a panda burning joss-sticks
  - stole usernames and passwords from online games players



- Li Jun,
  - four years in prison
  - profiting from the worm he created,
- offered a job paying a million yuan ($133,155) salary.
- Jushu Technology
  - Hangzhou City
  - the firm being itself a victim of the worm.

“Trap” for engineers

技術者罠

- Social justification -Academic importance of discovery and publication
  - disclosure is important for vulnerability preparedness
  - efficient P2P is progression in technology.
- How to overcome with conflict issue
  - attitude with society
  - “fame” by evil challenge to existing rules.
    - “efficient” way for his tech spread over the world.

Society's Combat

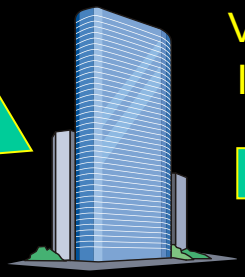
社会努力・闘

- Society have to combat against high tech crime.
  - In general, "Integrity" is most important security element.
- Vulnerability
  - Responsible disclosure /Coordinated disclosure
- Cyber crime convention "hacker tool"
  - Dual tool issue

Information Security Early Warning Partnership

- Control the occurrence of computer security incidents through effective cooperation with related organizations
- Built the international cooperation structure for vulnerability handling among JPCERT/CC, CERT/CC, and NISCC
- Closed down many websites which announce vulnerability information
- Have already received 120 pieces of vulnerability information since July, 2004

Discoverers of Vulnerability



IPA

Vulnerability Information

Cooperation

Foreign CSIRTs (CERT/CC, NISCC, etc.)

Coordination

IT Vendors

System Integrators

Vulnerability Information
Countermeasures

Vulnerability Information
Countermeasures

Countermeasures

Countermeasures

Users (System Administrators, Individual Users, etc.)

from METI presentation

Cyber Crime Convention

- article 6 dual use
  - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
  - a. the production, sale, procurement for use, import, distribution or otherwise making available of:
    - i. a device, including a computer program, designed or adapted ***primarily*** for the purpose of committing any of the offences established in accordance with Article 2 - 5;

止 電網犯罪条約六条 黒客道具禁

guidelines for the application of Computer Misuse Act.

- Prosecutors dealing with dual use articles should consider the following factors in deciding whether to prosecute:
  - Does the institution, company or other body have in place robust and up to date contracts, terms and conditions or acceptable use polices?
  - Are students, customers and others made aware of the CMA and what is lawful and unlawful?
  - Do students, customers or others have to sign a declaration that they do not intend to contravene the CMA?

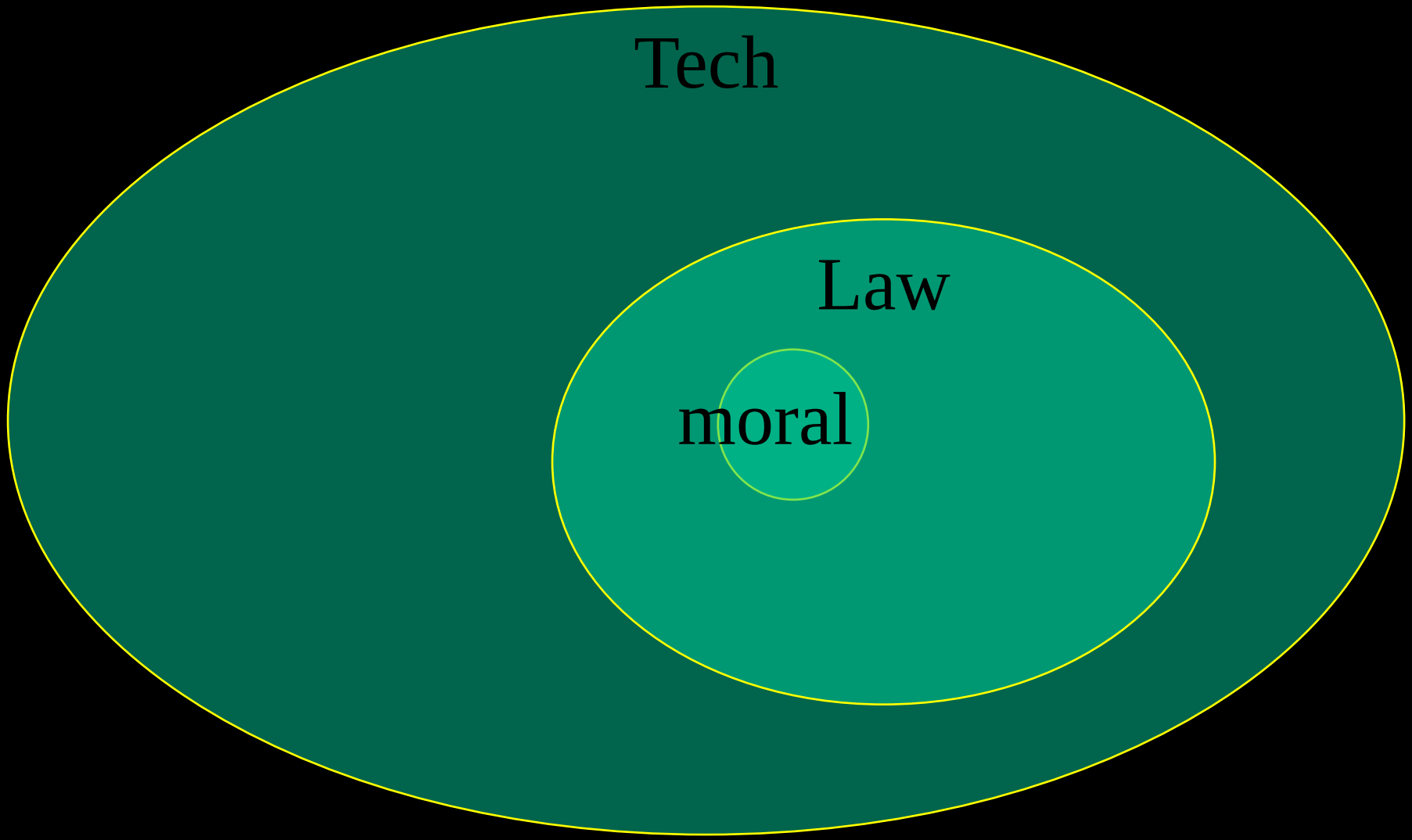
英国 電脳不正使用法適用 解釈手引

Importance of power of community

共同体 重要性、修行

- Force
  - Luke studied and felt the ethics of Jedi under the Master Yoda’s tutorials.
  - Padaone (apprentice) live in Jedi Temple.
- Hacker
  - Information ethics
  - Leading professor suggests the appropriate usage of information techniques.

Ethics,Law,Technology



Security Wars

episode 2

Attack of anonymous troops

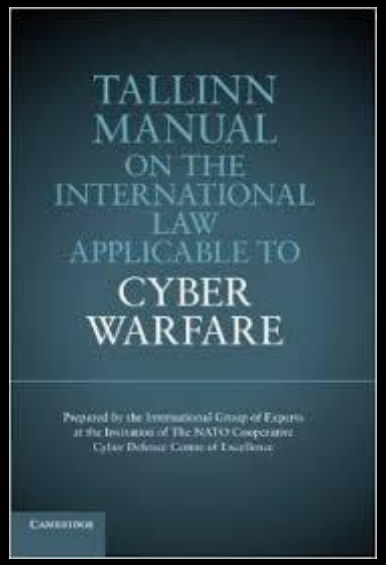
小故事二 匿名軍団攻撃

Security Wars

episode 3

Revenge of State

小故事三　国家逆襲



deep grief “No”

深的悲伤

- Vador didn’t intend to kill Padome.
  - “I’m very sorry, Lord Vador.(..) It seems in your anger, you killed her”
- “No…no. it is not possible” (ep3)
  - Darth Vader

Does not intend to regulate “Freedom of speech” concepts

How to control?
What control?
Who control?
Who pay for costs?

Fin.

- Only Force can solve the information security problems.

- “May the Force be with you”

Special thanks to

- Alan Lee for Light Sabre.