CSE468
Information Conflict

Lecturer: Dr Carlo Kopp, MIEEE, MAIAA, PEng

Lecture 10

Information Conflict - Copyright, Privacy, Spam, Espionage, Surveillance, Hacking and Cyberwar, Viruses/Worms, and Identity Theft

Reference Sources

- Prof Dorothy Denning (formerly Georgetown)
  - **COSC 511 Information Warfare: Terrorism, Crime, and National Security**
  - http://www.cs.georgetown.edu/~denning/cosc511/fall02/index.html
  - http://devost.typepad.com/cosc511/

- Carlo Kopp - APA IW Topics Archive:
  - http://www.ausairpower.net/OSR-1296.html
  - http://www.ausairpower.net/OSR-0297.html
  - http://www.ausairpower.net/OSR-0200.html
  - http://www.ausairpower.net/OSR-0300.html
  - http://www.ausairpower.net/moore-iw.pdf
  - http://www.ausairpower.net/_JIW-2002-1-CK-S.pdf

Taxonomy of IW Categories

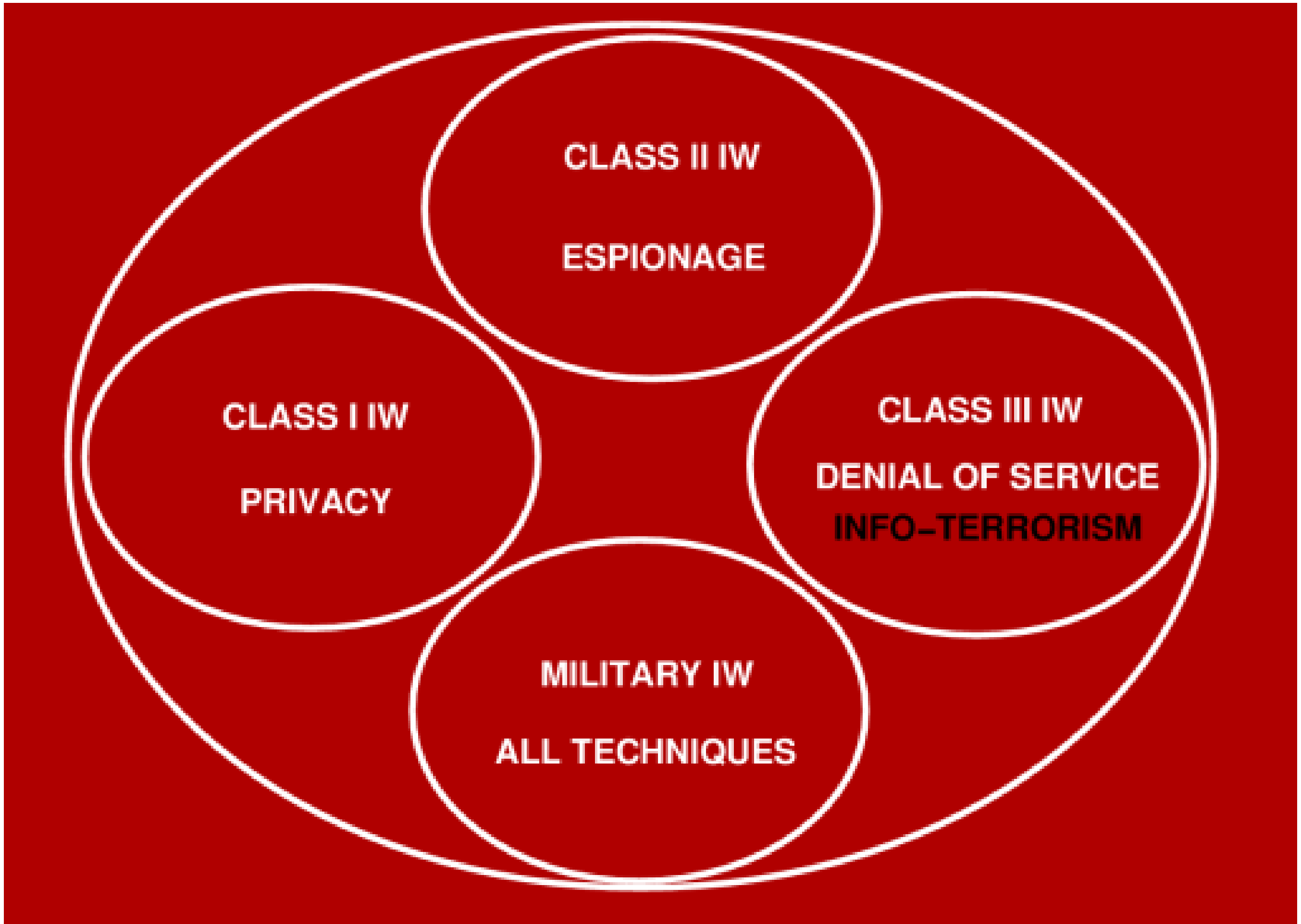
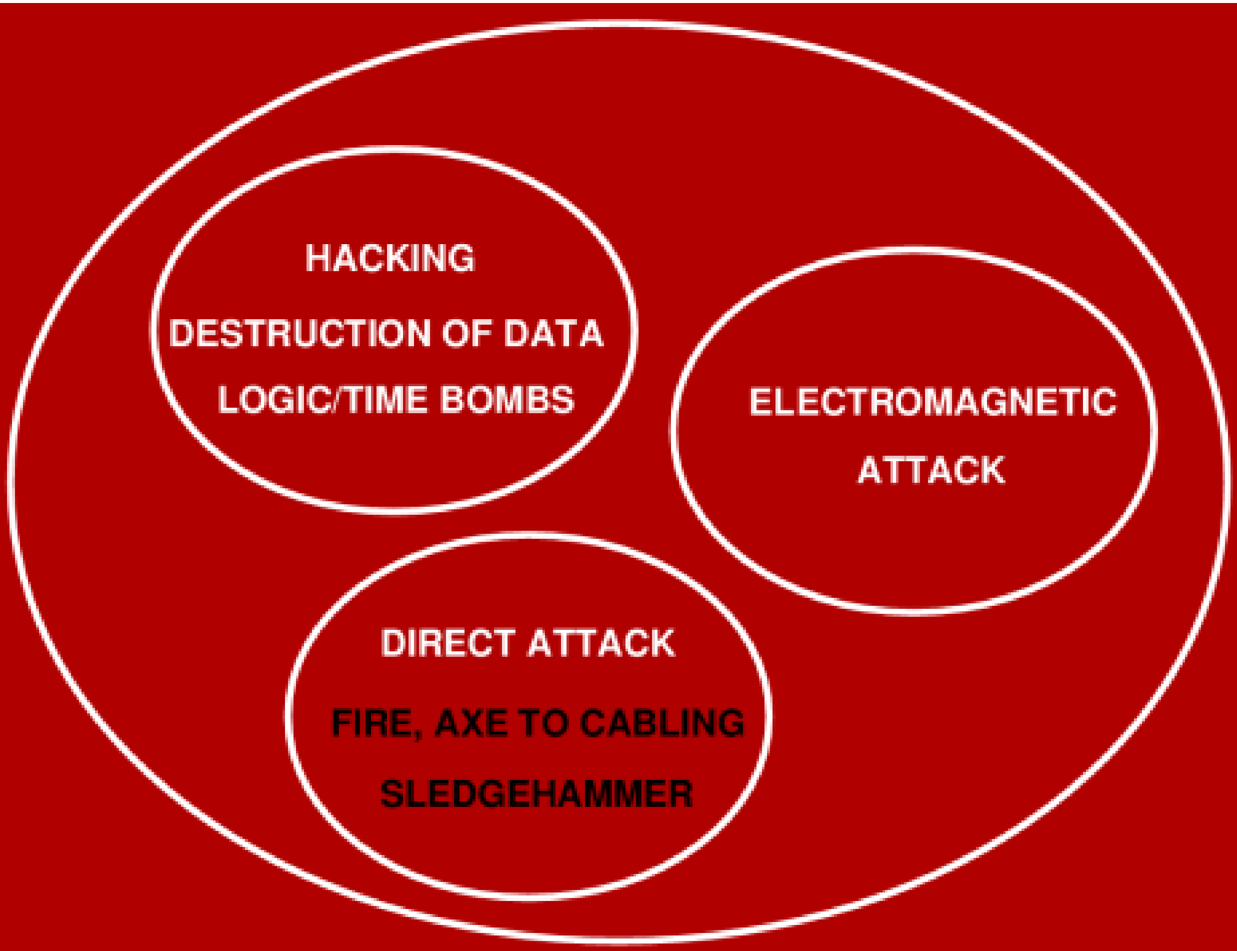


FIG.1 INFORMATION WARFARE

Denial of Service Attacks



HACKING

DESTRUCTION OF DATA

LOGIC/TIME BOMBS

ELECTROMAGNETIC

ATTACK

DIRECT ATTACK

FIRE, AXE TO CABLING

SLEDGEHAMMER

FIG.2 IW – DENIAL OF SERVICE

Offensive vs Defensive IW

- In any IW engagement there is an offensive player or *attacker*, and a defensive player or *defender*.
- Strategic planners and managers will typically play the defender’s game. Their role is to ensure that the organisation’s infrastructure can resist IW attacks – starting with Class I, and then Class II and III IW. Class IV attacks are usually the responsibility of governments.
- Given the diversity of ways in which IW attacks can be mounted, concentrating on established security techniques is not enough – it will protect against hackers and physical Denial of Service attacks, but not against viruses and worms or other forms of attack.
- If an organisation depends on websites for billing, notifications and support, losing that website even temporarily could inflict significant monetary losses.
- Resistance to IW attacks must be planned for from the outset when developing and planning infrastructure. Attempting to add defensive measures to production systems can be very expensive.

Practioners of IW Technique

- Malicious hackers and worm/virus writers inflict damage for amusement or peer group approval. They can attack globally.
- Hackers, Phrackers and Whackers may steal bandwidth by penetrating networks or manipulating accounts.
- Criminals may hack to acquire information, such as credit card numbers, confidential information etc, or threaten DoS attacks to extort money from a victim organisation such as a bank or telco.
- Industrial and commercial espionage may be performed to steal proprietary information such as manufacturing techniques for financial gain.
- Espionage against government departments, esp police and military, may be performed to gain access to national secrets, operational or technical. Foreign governments or contracted hackers may be involved.
- [Info-]Terrorists may perform DoS attacks to promote their cause by inflicting economic or political damage. A car bomb deployed against a stock exchange, national bank, media site or central telephone exchange qualifies as an IW attack.

Moore’s Law, Bandwidth Law vs IW

- Moore’s Law predicts monotonic growth in computing power over time, the Bandwidth Law predicts monotonic growth in network bandwidth over time. Both laws are well validated empirically [Kopp]
- Rapid growth and commodification of hardware and software have dual effects on IW:
  - The cost of computer systems and tools capable of use for IW declines and these become more available, globally.
  - The cost of defensive measures and encryption technology declines over time, making defensive measures more affordable.
- *It is necessary to look at IW as an evolutionary game – as better defensive measures are created, better offensive measures evolve to overcome these.*
- Strategic planning and budgeting must allow for evolutionary growth in defensive measures to account for increasing capabilities for IW over time.
- Senior management in many organisations may not appreciate these issues and will need to educated, often despite their resistance.

Privacy and Copyright Considerations

- Individual privacy and corporate client privacy are important considerations. Legislation exists in most developed nations – including Australia – intended to protect privacy.
- Many types of IW attack violate privacy and the onus is upon the carrier or provider to protect against such attacks. Failure to provide proper protection could see a carrier or provider criminally and commercially liable for damages.
- Privacy becomes critical where financial transactions, medical records and private correspondence are involved.
- If a hacker steals such information, he/she may never be caught. The damaged party could launch legal action against the provider or carrier on the basis of inadequate protective measures being implemented, or file charges with a law enforcement agency.
- In some nations privacy violation is automatically considered a criminal offense and carriers or providers are held responsible.
- Copyright violations are a special case since the material is available to the public, but its distribution is controlled. Such violations have become a major political and commercial issue globally, especially in the entertainment industry.

Copyright and Intellectual Property

- Illegal or unauthorised reproduction of digital materials is a major problem.
- With cheaply available networking, hard disk, CD-R and DVD burner technology, almost any materials can be reproduced, often in bulk quantities, for little material expense.
- This has led to the growth of illegal ‘pirate’ industries which steal and market digital materials, especially software products, and entertainment products such as cinema, music and publications. The result is significant losses to the owners of the intellectual property in the products.
- Weak legislation in some nations allows these to become ‘havens’ for such industries.
- It is important that organisations carefully assess the origins of any digital materials used internally to ensure that these are not pirate copies.
- A good example would be software tools used within an organisation. Using pirated copies or unwittingly distributing such materials opens the organisation to civil litigation over copyright violation or criminal charges.

SPAM

- SPAM is unauthorised and unsolicited distribution of marketing materials via email, in bulk quantities. Spammer violate the privacy of spam recipients.
- Spammers will market everything from pornography, discount pharmaceuticals, junk stocks, dubious home loans, consumer products, to pirated software and CD/DVD.
- Spam is also used to distribute propaganda on behalf of political and religious movements.
- Modern spamming techniques use tools which use digital archives (usually harvested off the web on CD-ROM) of victim addresses, and which usually forge the sender address by using another victim address.
- Spam is not illegal in most nations since legislation was injudiciously adopted which does not require prior consent by the recipient when being spammed.
- It is likely that anti-spam legislation will be adopted in the developed world over coming years since spam often accounts for a significant fraction of bandwidth used causing economic losses globally.

Privacy on the Web

- The internet creates many opportunities for privacy violations.
- Many websites use the cookie mechanism to retain state information and identity information. Cookies allow the web server to recognise systems accessing a site. In turn this information can be stored to produce profiles of visitor accesses on a site, and thus divine visitor interests or agendas.
- Such information can be used to support marketing activities directed at visitors. An example is a website which uses such statistics to adaptively present advertising material to visitors.
- Most web servers collect access statistics which allow operators to track which visitors are making what accesses and when. While this can be used for legitimate purposes, it also allows profiles of specific visitors to be produced.
- Cookies and server statistics are usually gathered silently and visitors are unaware of their existence or possible/actual uses.
- Website owners often compromise their own privacy by putting materials on websites which are not intended for distribution, but forgetting to disable read access.
- Online directories now allow gathering of significant materials on individuals such as addresses, phone numbers, email addresses and other details. While most users are legitimate, criminals and terrorists also have access.

Espionage and Intelligence Gathering

- Espionage and intelligence gathering – the second oldest profession - has a long history. The advent of digital communications has made some aspects of this craft easier, and some more difficult.
- Practicioners may be acting on behalf of governments – illegally or as part of law enforcement, political movements and parties, religious movements, commercial organisations or individuals.
- Most espionage or intelligence gathering amounts to covert collection of information or materials without the consent or knowledge of the victim.
- This can be performed by acoustic eavesdropping, visual/video surveillance, electronic eavesdropping of analogue or digital channels (SIGINT), hacking into computers (CyberWAR), breaking into offices, filing cabinets or safes (HUMINT), or by unauthorised reproduction of accessible materials (HUMINT).
- While most intelligence gathering and espionage is performed by governments against other governments, industrial espionage is also common. The latter is of interest to managers since it can result in significant losses. Target information can vary from technical data on products or processes, to marketing plans, costing information and tender proposal documents.

Surveillance Techniques

- Surveillance can be performed using acoustic (microphone ‘bugs’ or phone tap), visual (film or video camera) or electronic (radio/mobile phone/wireless network) intercepts.
- In most nations surveillance is only lawful if performed by a law enforcement or intelligence agency ie government entities.
- Commercial operators are usually permitted to use video surveillance of publicly accessible areas ie banks, ATMs, carparks, foyers etc.
- An large scale example of such surveillance is the CCTV network in London used to apprehend terrorists after the recent attempts to bomb public transport.
- Law enforcement agencies rely heavily on acoustic and visual surveillance to gather intelligence or evidence.
- Managers need to be aware of the potential for unlawful surveillance and plan infrastructure to make it difficult to perform.
- Counter-surveillance technologies may be illegal in some nations – for instance voice scramblers for telephone links.

SIGINT/COMINT – Signals/Communications

- The interception of radio signals and communications has been practiced since the advent of wireless communications. It is mostly practiced by the military and law enforcement due to the cost of the complex equipment required.
- The advent of cheap radio ‘scanners’ has opened up opportunities for individuals and organisations to intercept unencrypted or unscrambled wireless voice traffic.
- Intercepts may be targeted, ie a single individual or site is monitored on a specific channel, or they may be performed en masse by recording swaths of the radio spectrum for later semi-automated or manual analysis by human operators.
- Wireless channels without strong encryption must be therefore considered insecure and should never be used to transmit information which is sensitive – either from a privacy perspective, commercial perspective, or where sensitive government traffic is involved. GSM mobile phones are a good example.

Network Sniffers

- Network sniffers are a vital tool for legitimate traffic analysis and network maintenance tasks. They can also be used to perform lawful and unlawful surveillance and monitoring of specific users or sites on a network.
- A sniffer is a software/hardware device which collects and decodes network packets, and can often reassemble traffic flows.
- Network protocols with weak or absent encryption will allow the user of a sniffer to collect accounts/password information, email traffic, file transfers and web traffic.
- Sniffers with wireless network interfaces allow penetration of wireless networks without having physical access to a network port or cable.
- Network planning needs to account for unlawful surveillance by users of sniffer equipment. Active network ports in publicly accessible areas are not acceptable, and wireless channels must use the strongest available encryption techniques.
- ‘Insider attacks’ by staff using sniffer software on internal systems are a real possibility. Superuser access on computers should be carefully controlled.

Van Eck Radiation

- Van Eck radiation is defined as Unintended Emissions (UE) in the radio-frequency bands.
- Computer monitors and to a lesser extent keyboard or poorly impedance matched network cables will radiate signals as a result of the digital or analogue modulations they are carrying.
- Specialised receivers can be used to collect UE – the typical example cited is equipment which can reconstruct what is being displayed on a computer monitor from outside the building housing the computer.
- UE surveillance and intelligence gathering is expensive and usually limited to governments and law enforcement.
- The US NACSIM 5000 Tempest series of standards defines design specifications and techniques for computer equipment to prevent the emission of Van Eck radiation.
- Managers in government organisations need to understand the risks arising from UE and ensure that computer equipment used for classified or highly sensitive material is suitable for such use.

Psychological Warfare (Psywar) Techniques

- Psywar is used most frequently in wartime (radio/leaflets), but is often seen in commercial or political mass media advertising.
- Psywar techniques aim to amplify existing anxieties in a target/victim population to disrupt their behaviour, and disrupt the cohesion of an organisation or group.
- A prerequisite for successful ‘Psyops’ is that the target or victim population has an existing anxiety or prejudice over some issue.
- Statements or claims which reinforce such anxieties or prejudices will produce distress or anger in the victim population.
- Examples are political advertising emphasising issues like job losses or interest rate increases, or commercial advertising pointing out bugs or vulnerabilities in computer products. Commercial foodstuff advertising alleging weight gains, cancer or heart disease also qualifies as Psywar.
- The internet and mass media are the preferred channels for Psywar attacks.
- Most nations have inadequate legislation regulating this area.

Censorship

- Censorship is a mechanism used to control access to information. It typically involves denying access or punitive criminal legislation intended to deter distribution.
- In developed nations censorship is mostly directed at entertainment products with explicit or violent content. In wartime censorship is used to deny an opponent knowledge of sensitive developments. Many nations apply political censorship to control public and political debate. Internet censorship exists in some nations to deny access to a wide range of materials not deemed suitable for public access.
- Censorship is a double edged sword, since it can increase the attractiveness of the censored material to a potential audience.
- Censorship remains a controversial issue in Western democracies since the criteria used to determine exclusion are often difficult to achieve consensus on.
- Managers operating in a global market or across national boundaries need to be sensitive to censorship legislation since criminal law is often used to enforce it.

Hacking, Cybercrime, Cyberwar (HCC)

- Hacking is the term used to describe unauthorised access to computer systems. The term originally applied to programmers who worked on operating system kernels but the media and entertainment industries popularised the currently accepted use of the term.
- Cybercrime is the use of ‘hacking’ techniques to commit criminal offences, usually theft of money or intellectual property.
- Cyberwar is the use of ‘hacking’ techniques to perform denial of service attacks or intelligence gathering for political or military purposes.
- HCC relies on poor password security and security ‘holes’ in computer operating systems.
- Phracking (Phone Hacking) is hacking into telephone networks mostly to steal bandwidth.
- Whacking (Wireless Hacking) is hacking into wireless networks mostly to steal bandwidth.
- Hacking remains a controversial issue. In most developed nations it is a criminal offence, frequently punished by long jail terms.

Techniques for Gaining Unauthorised Access

- A wide range of techniques exist for ‘hacking’ into computer systems.
- Passwords may be stolen by sniffing, or by entering offices and reading paper notes. Passwords may also be guessed using robots, or ‘purchased’ from unethical staff members. Unsecured terminals left logged in may be exploited.
- Trojan horse or backdoor entry code may be inserted into systems where a hacker has access to the original source code.
- Sophisticated attackers may perform identity spoofing by replacing real network packets with substitutes.
- Security holes in some network applications may permit remote entry by driving the application with messages known to expose the vulnerability.
- Software tools developed for security testing of networks can also be used to expose security holes for unauthorised entry.
- Robust firewalling and system security audits are essential to protect against unauthorised site entries.

Viruses and Worms

- Viruses are malicious programs which embed themselves in file systems, operating systems or applications upon which they propagate themselves via removable storage media or networks to other systems.
- Viruses may be benign or destructive in effect, and can be used to compromise security by propagating password files or email address lists.
- Worms are malicious programs which consume system resources to the point where a system becomes unusable.
- Highly integrated mailer and word processor programs are the most common targets of viruses and worms since they permit easy entry and propagation between systems. Some proprietary systems are considered the most vulnerable, cf Linux, BSD and commercial Unix systems.
- Managers and strategic planners need to be sensitive to risks which may arise from using some commodity software products known to be susceptible to such attacks.

Identity Theft and Fraud

- Identity theft is an increasing problem in the computer and communications industry.
- The simplest examples involve theft of mobile phones and credit cards for profit.
- Spammers today mostly forge return and sender email addresses by using addresses of other spam victims held in digital archives.
- Internet newsgroups have also seen identity thefts where hoaxers pretend to be actual or fictional persons. An example was a hoaxer on rec.aviation.military impersonating a retiree, who was actually bedridden in a nursing home suffering from severe stroke impairment.
- Validation of subscriber identity for web accessible services can present genuine issues, especially where sites are used to effect financial transactions.
- Bogus websites set up to visually emulate actual bank websites have been used to steal electronic banking passwords, in turn to fraudulently access accounts.
- ‘Nigerian scams’ involving impersonations are now of epidemic proportions in the spammer community.

Denial of Service Attacks vs Extortion

- Denial of Service attacks can be used as a tool to extort money from victims.
- Organisations which rely on uninterrupted computer operation to effect financial transactions, or which rely on web servers for client access, are the most common targets of such attacks.
- The attacker will cause repeated service loss and then extort money by promising to cease attacks.
- *Cyber attacks* - as the attacker may be located on another continent, in a nation with weak or absent cybercrime legislation, major problems arise with identifying the attacker, and with prosecuting the attacker.
- *Radio-frequency / electrical attacks* – the attacker will be geographically local but may not leave a detectable signature or footprint permitting law enforcement to apprehend or prosecute.
- Usually DoS extortionists prey on organisations with poor expertise levels in computer/network administration and security.
- In general DoS attacks can be difficult to prove and prosecute.

Tutorial

- Q & A
- Case Studies Discussion