

## COMP 3410 – I.T. in Electronic Commerce

### eTrading 2. Key Technology Issues

Roger Clarke

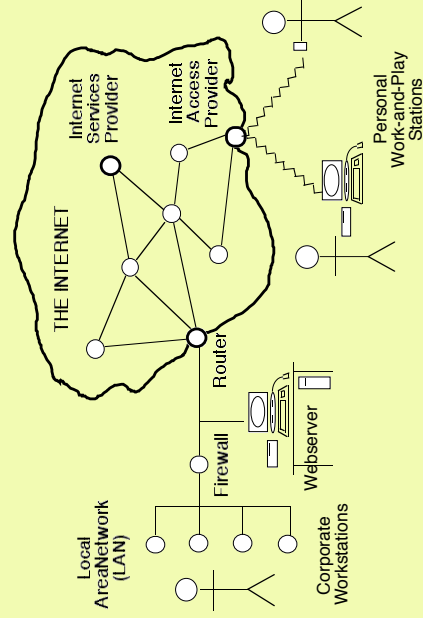
Xamax Consultancy, Canberra  
Visiting Professor, A.N.U. and U.N.S.W.  
<http://www.rogerclarke.com/EC/> ...  
ETIntro.html, OhdsET2.ppt

ANU, September 2009

## E-Trading Some Key Technology Issues

### Agenda

1. Mobile Commerce (Internet and Cellular)
  - Access Devices
  - Access Channels
2. Malware



## User Devices

- **Capacity** (now rivals Hosts)
- **Diversity** (vast, expanding) desktops, laptops, handhelds, smartcards, ... phones, PDAs, cameras, iPods, iPhones, ... car buretters, fridges, ... RFID tags, 'Things' Parallel Divergence and Convergence, ongoing

## User Connections

- **Wired Connectivity** (now mostly Broadband)
- **Wireless Connectivity** (now mainstream)

## The Rich Variety of Wireless Comms

- **Wide Area Networks – Satellite** (Geosynch; Low-Orbit) GS is Large footprint, very high latency (c. 2 secs)
- **Wide Area Networks – Cellular** (50m to 10km cell-radius, with increasing capacity per user, particularly with 3G)
  - 1 – Analogue Cellular, e.g. AMPS, TACS
  - 2 – Digital Cellular, e.g. GSM, CDMA
  - 3 – '3G' – GSM/GPRS, CDMA2000 and UMTS/HSPA
- **Wide Area Networks – IEEE 802.16 (WiMAX), 802.20 (MobileFi)** (3-10 km per cell, high-capacity per user, but a local monopoly?), and proprietary options such as **iBurst**
- **Local Area Networks – 'WiFi'** (10-100 m radius) primarily IEEE 802.11x, x=b,g,n
- **Personal Area Networks** (1-10 metres) e.g. Bluetooth (or beamed infra-red)

## Mobile 1 – Variable-Location Rather Than Fixed-Point

- Faxes (for printouts) and Phones (e.g. for spoken email)
- Wifi / iBurst / WiMax wireless connection
- 3G cellular services (GSM/GPRS, CDMA2000, UMTS/HSPA) to an Internet Access Provider (IAP)
- Provides a temporary IP-address
- Device is inherently locatable to the cell it's in
- Potentially more accurately locatable (MOLI, transceiver direction, signal analysis, triangulation, GPS self-reporting)
- May involve one or multiple 'nynms' (IMSIIs)
- Used in some circumstances by fixed-location devices e.g. in sparsely-populated regions, and to hide

## Mobile Type 2 – Device - in - Transit Device, Channel Capacity and Motion Issues

- **Mobile Device Capacity Constraints** (processor, memory, storage, display, power) e.g. may be unable to support web-browsers
- **Bandwidth Constraints**, partly inherent, partly because of web-designers' ignorance, excessive enthusiasm, inadequate self-discipline
- **Mobile Phone Handoff between cells is poor**
- **Internet Handoff is worse.** When a device moves to a new sub-net, it loses its IP-Address and has to get a new one from its new sub-net

## Generic Solutions re Device and Channel Capacity

- A 'Mini-Browser'
- A Complete Alternative Protocol Stack (cf. HTTP, TCP, IP) and an alternative ML (cf. HTML, XHTML, XML) [WAP tried, but failed]
- **Device-Independent Web-Pages:** "W3C is dedicated to ensuring that the Web universe is not fragmented. Interoperable languages and protocols, and single-authored content should prevail"

### HTTP/TCP/IP

1. → TCP SYN
2. ← TCP SYN, ACK of SYN
3. → ACK of SYN, Data Request
4. ← ACK of Data
5. → Reply
6. ← ACK of Reply
7. → Data Request
8. ← ACK of Data
9. → Reply
10. ← ACK of Reply
11. → Data Request
12. ← ACK of Data
13. → Reply
14. ← ACK of Reply
15. → TCP FIN
16. ← TCP FIN, ACK of FIN
17. → ACK of FIN

### WSP/WTP/UDP

1. → Data Request
2. ← ACK, Reply
3. → ACK, Data Request
4. ← ACK, Reply
5. → ACK, Data Request
6. ← ACK, Reply
7. → ACK

**Bold packets contain payload**  
Non-bold items are overhead

Typical Handset Session — 3 Requests, 3 Responses	
HTTP/TCP/IP	WSP/WTP/UDP
17 packets	7 packets
65% Overhead*	14% Overhead*

\*does not account for DNS, SSL, Authentication or Cookies

## A Solution to the Device Motion Problem

### 'Mobile IP'

- Messages are directed to a specific, stable IP-Address (which could be thought of as a 'care-of' address)
- A home agent on the home subnet of the mobile device performs re-direction of the traffic
- Sending nodes only ever send to the home IP-Address
- There is a delay in the notification by the device of a new IP-Address, so messages in the interim need to be managed
- Is implementation proceeding quickly enough?

## Malware, Informally

- Software that does harm
- Recognisable in retrospect as early as 1971
- The term 'virus' was borrowed from biology in 1983
- Transferred by floppy disk:
  - initially among Apple micros in 1981
  - major infections on 'IBM PCs' from the late 1980s
- Network transmission dominant since the mid-1990s

## Foundational Concepts

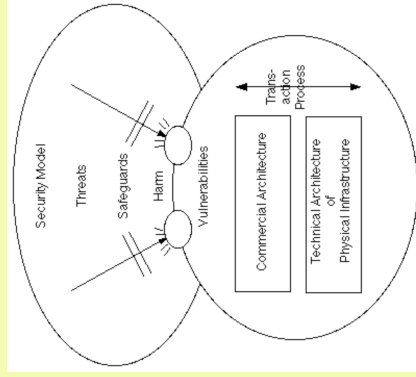
- **Undesired Content**  
spam, email-attachments (e.g. pornography), web-browser and P2P downloads (e.g. ads)
- **Malbehaviour**  
'social engineering' to enveigle users into providing the means, e.g. 'phishing', 'free anti-virus software'
- **Malware**  
Undesired Content in the form of software

## Challenges in Defining Malware

- **Code:** executable, or interpreter-dependent
- **Dependence:** hardware, system s'ware, or app
- **Form:** program, program-fragment, or -feature
- **Execution:** conscious, implied, or auto
- **Storage:** locally stored, or executed without storage
- **Operation:** invoked or latent
- **Harm:** harm, or no harm
  - **Category:** type(s) of harm caused
  - **Sufferer:** who or what the harm is caused to
  - **Intention:** harmful intent ('malicious'), accidental harm ('malprogrammed') or beneficial intent

## Malware

- **Software**, or a software component or feature that
  - is capable of being **Invoked** on a device and that
  - on invocation, has an **Effect** that is:
    - **Unintended** by the person responsible for the device; **and**
    - **Potentially Harmful** to an interest of that or some other person



## Malware from the Viewpoint of the Conventional IT Security Mode

- Malware external to a device is a Threat
- An attempt to migrate it to a device is an Attack
- An Attack depends on existing Vulnerabilities
- Malware internal to a device as a result of a successful Attack is a new Vulnerability
- Once invoked, installed Malware may:
  - do Harm
  - create additional Vulnerabilities

## Categorisation of Malware

Malware

- (1) uses a '**Vector**'
- (2) to deliver a '**Payload**' which performs
- (3) a function that is '**Invoked**' by some means and is harmful to some party

## Criterion 1 – Vector

The means whereby undesired content reaches a device  
The alternatives, viewed broadly:

- **Unit Storage Proliferation:** copying from portable storage that is directly-connected to the device (diskette, CD, DVD, solid-state electronic 'drive')
- **Network Transmission:** transmission or download from another device on a local area network, or from a device on a remote network

## Network Vectors – 1

- **file transfer** (FTP get or put)
- **email-attached executable** (push):
  - default auto-invocation
  - manual settings-change to auto-invocation
  - remote settings-change to auto-invocation
  - manual invocation
- **social engineering** using an email-message, chat/IM, bulletin-board, Web-pages or P2P, to entangle a user into downloading a file (pull)
- **the Web and P2P**, using a variety of features ...

## Network Vectors – 2 The Ever-Extending Malicious Web

- Features of HTTP (e.g. additional Methods, esp. the Microsoft invention 'XMLHttpRequest')
- Features of HTML
- Features of Javascript
- Server-side capabilities
- Associated protocols and standards

### The Result:

File-download to the user device, based on a user-performed trigger, but without an intentional request or an informed response to a request

## Network Vectors – 3 Host Control over Remote Devices

- **AJAX**
  - Use of Malicious Web features to construct a platform-independent 'engine' within the browser-space
- **ActiveX Controls within / .NET**
  - Absence of a Sandbox
  - Unsafeguarded Computing Resources
- **'Drive-By Download'**

## Criterion 2 – Payload

- The carriage capacity of aircraft (1930s)
- The content of a communication (1970s)
- **The active code delivered to the target device in order to perform some function or functions**
- The scope may extend to functions ancillary to the ultimate purpose, e.g. means of obscuring the existence or operation of the malware

## Categories of Payload

- Operations on Data:**
- data creation (entries in control files)
  - data deletion or directory-entry deletion
  - data modification (security-settings, parameter-settings, port-settings)
  - data capture (spyware), generally surreptitious, e.g. keystroke logging, adware
  - data disclosure
- S'ware installation or mod, to:**
- establish a 'backdoor', for remote control
  - install a 'rootkit', to obscure malware ops
  - upgrade malware payload
  - undermine anti-malware software
- Downloading of Files, e.g.**
- large malware apps
  - adapted malware payload
  - detection of a triggering event

## Trojan

### Vector-Based Interpretation:

- Malware that reaches a device by means of an intentional act by an authorised user, as a result of a social engineering exploit

### Payload-Based Interpretation:

- Malware with unexpected functionality that facilitates unauthorised remote access to the device

### Preferred Usage:

- A **Trojan** is any malware whose vector is an intentional act by an authorised user, as a result of a social engineering exploit that involves convincing the user that the software is beneficial
- A **Backdoor Trojan** is a Trojan whose payload is a means of facilitating remote access to the device

### Criterion 3 – Invocation

- The causing of the code to run in the target device
- This encompasses various categories of code:
  - native to the instruction-set of the target device
  - in a form that requires a compiler, an interpreter or a run-time interpreter
  - embedded, such as macros within word processing and spreadsheet documents
- The device's system software may include safeguards against unauthorised invocation of programs, e.g. permissions limitations. Malware seeks to circumvent or subvert such safeguards

### Forms of Invocation – 1. Human Triggered

- **An Authorised User's explicit, intentional action:**
  - directly acting on the device
  - remotely, through a user-account
- **An Authorised User's implicit, unintentional action:**
  - invocation of a macro, by opening a document
  - a request from a web-browser which triggers a 'website application attack':
- **An act by someone other than an Authorised User:**
  - directly acting on the device
  - remotely, through a user-account
  - remotely, using a 'bot'

### Forms of Invocation – 2. Auto-Triggered

- **Automated Invocation of Stored Software**  
e.g. inclusion in the list of start-up routines  
e.g. timed action, as for 'run the backups at midnight'
- **Auto-Download and Immediate Invocation**  
e.g. system software version updates and patches  
e.g. protection software updates and virus signatures
- **Pushing of Malware by a Remote Device**  
taking advantage of existing device vulnerabilities

### Web-Site Application Attack An Important Special Case of an Authorised User's implicit, unintentional action

A web-browser request triggers the delivery of malware to the device running the web-browser:

- with delivery directly by the web-server; OR
- with indirect delivery, through invocation by the web-server of a component from another site

In each case, the delivery may arise:

- by intent of the web-server manager; OR
- through a connivance by another party

### Bots, Zombies and Botnets

- A **Bot** is any malware that is capable of being invoked remotely in order to perform a particular function
- Typical functions include emailing spam and distributed denial of service (DDOS) attacks
- A **Zombie** is any device on which a bot is installed
- A **Botnet** is a set of devices on which bots are installed
- A **Botnet Master** or **Botnet Herder** is any person who can exercise control over a botnet

### But 'Bot' has an Alternative Usage Bot / Robot / Agent

- **Software that interacts with other software or human users as though it were a human, and in some sense at least on behalf of a human**
  - Web crawler or spider
  - Re enquiries / requests / incident reports
    - Auto-acknowledgement
    - Auto-response
  - Automated Trading
  - Online Games

## Malware Persistence

- Briefly memory-resident and then terminates
  - Memory-resident and active
  - Memory-resident but dormant; pending some trigger  
Such software is commonly referred to as a 'daemon' or in Microsoft environments a 'Windows service'
- Memory-resident malware can perform functions that a one-time program cannot  
e.g. to take advantage of ephemeral data, or a communications channel that is only open briefly

## E-Trading Some Key Technology Issues Agenda

1. **Mobile Commerce**  
(Internet and Cellular)
  - Access Devices
  - Access Channels
2. **Malware**  
Vector cf. Payload cf. Invocation  
Diversity of Phenomena  
Diversity of Language  
undermines Countermeasures

## Virus ... Worm

- A **Virus** is a **block of code that replicates itself by seeking out other executable files and inserting copies of the block of code into them.** (It commonly carries a payload, and it commonly delays the invocation of the payload, in order to avoid early detection. It may be limited to specific contexts, hence, for example, 'boot sector virus' and 'macro virus')
- A **Worm** is a **program that propagates copies of itself over networks.** It does not infect other programs.
- Viruses and Worms flourish because of:
  - the naiveté of users
  - inadequate care by I.T. professionals
  - OS and apps distributed in a culpably insecure state

## Spyware

- **Software that surreptitiously:**
  - **gathers data within a device; and**  
e.g. about its user, or the uses made of it
  - **makes it available to one or more other parties**  
(The data may be extracted from files on the device, may reflect the behaviour of a device and /or the user of the device, and /or may reflect the behaviour of other devices on the same network)  
(The data may then be transmitted to a remote device)
- Key applications:
  - keystroke logger (esp. for passwords)
  - monitoring of consumer behaviour ('adware')
  - monitoring of uses of copyright works

## Backdoor / Trapdoor

A feature, possibly software, that enables unauthorised remote access to a device, bypassing or subverting authentication and other security safeguards.

(The access is usually contrived to have a high level of privileges)

...

## Remote Administration Tool (RAT)

Software that enables remote access to a device, with a high level of privileges, and with the capacity to monitor user behaviour, adapt the device's software configurations, and install and/or invoke software

(RATs are essential for the provision of remote management and support. But unauthorised use represents a serious threat because of the power they provide over the device)

## Rootkit

(Literally software that allows an intruder to gain access to a device with the highest level of privileges available, i.e. associated with the root or system-administrator account. By extension:)

**Software that assists in obscuring the existence of malware on a device, and/or establishes an obscured environment within which malicious code can be executed**

## Drive-By Download

**A technique whereby malware is downloaded to a device as a result of a user action, but such that the user is unaware that they are triggering the download.**

(The user is probably also unaware during and after the download that they have triggered it)

## Exploit

- An Exploit is an established way of performing an attack on a vulnerability
- Standard techniques are supported by guidelines and programming code, which circulate on the Internet
- Code that enables easy performance of an exploit is expressed in a **Script**
- **Script Kiddies** is a derogatory term for relatively unskilled crackers who rely on techniques and program code developed and published by others

## Bug

- An error in systems software (esp. MS Windows) or applications (esp. MS IE and MS Office)
- It is impossible to produce software without bugs
- Less prevalent in MS products than previously, but MS products remain the primary target
- Bugs may create vulnerabilities
- The vulnerabilities may be attacked by crackers
- This gives rise to the need for urgent patches
- Which give rise to risks of new bugs
- ...

## Social Engineering (1) Phishing

- Sending people e-mail messages in order to lure them into divulging sensitive data
- The data sought is commonly passwords and credit-card details
- The sender commonly assumes a relatively highly trusted identity e.g. a fin/1 institution
- The data is commonly keyed into a web-form on a site that purports to be operated by the trusted identity
- Phishing is not Malware, but Phishing may be supported by Malware

## Social Engineering (2) Incitement to Download and/or Invoke

The use of social engineering to manipulate a person into downloading and/or invoking malware

A common example: free 'anti-virus software'