22:010:622
Internet Technology and E-Business

Dr. Peter R. Gillett

Associate Professor

Department of Accounting & Information Systems
Rutgers Business School – Newark & New Brunswick

Overview

- Review of Last Week?
- Client Threats
- Data Collection and Analysis
- Internet Pricing
- Security Issues
- Firewalls and Related Technology
- Simple Game Theory

The Big Issues

- Turban et al. quote a Georgia Tech. survey (97-98) of the most significant issues facing the Internet:
  1. Censorship (privacy issues)
  2. Privacy
  3. Navigation (not really privacy)
  4. Taxation
  5. Encryption

Domain Names

- Cybersquatting
- Name changing
- Name stealing

Client Threats

- Active Content
  - Java applets
  - ActiveX Controls
  - JavaScript
  - VBScript
- Cookies
- Trojan Horses
- Zombies
- Viruses
- Worms
- Steganography

Big Issues

- Privacy and the World
  - The Internet is global
  - Different views:
    - US: privacy is balanced against the needs of society
    - Europe: privacy a constitutional right
- General Issues
  - Accuracy
  - Property
  - Accessibility and verifiability

Data Collection on the Web

- Primary types collected on Web Sites
  - Domains
  - Countries, companies
  - IP address, browser type, etc.
- Timing Records
  - How long on web site?
  - How long to a purchase?
  - When?
  - Repeat visits?

Data Collection on the Web

- Time Series of data
  - Descriptive: what happened
  - Predictive: anticipate what will happen next
  - Explanation: why this lead to a sale.
- Seasonality effects: E-marketing and winter holiday season. Day and night.
- Periodic: weekends
- Trends: increasing sales overall, decreasing sales per minute visited
- Whose property are the predictions?

Data Analysis

- Where can we get the data about our web site?
- Types of statistical analysis
- A time series is stationary if it has no periodic variation and no trend and no change in variance
- Looking for trends

Competitive v. Cooperative Marketing

Competitive Marketing	Cooperative Marketing
Frontal Assault (Amazon.com vs. BN.com)	Joint Venture (Microsoft)
Flank Attack (e*Trade vs. Schwab)	Value Chain partnership (Dell, ingredient marketing)
Raise Structural barriers (lots of costly development or marketing)	Lower Desire for attack (joint marketing programs)

Internet Firms Raising Prices!

- Why?
  - People seem willing to pay more
  - Costs are higher
  - Not able to buy in bulk like larger brick-and-mortar stores
  - Equity markets no longer willing to support money-loosing enterprises
- What is the cardinal rule of pricing?
- Why have Internet firms focused on price?

Internet Pricing

- **X looses $1 on each unit they sell, but that is OK since they make it up on volume!**
- How? Primary and secondary data
  - Controlled Experiments
  - Conjoint Surveys
  - Market Intelligence

Advantages of Internet Pricing?

- Speed
- Audience
- Experiments
  - Fast
  - Large
- Market Intelligence

Key Security Issues

- Authentication
- Secrecy
- Data
  - Firm's data
    - Customer data
    - Internal data
- Hierarchy of Security

Security

- Extranets are harder to secure than intranets
  - Must deal with lots of other systems
  - Outer firewall protects from gross misuse
  - Perhaps the best way: packet filtering firewall
- Intranets generally have more tight security
  - More sensitive information
  - ORB: Object Request Broker model
    - Sending your Objects (data) where?
    - Not keeping things totally secured

Security: Flavors

- SecurID: One-Time Pad
  - Risks?
    - Lost or stolen
- Hashing or finger-printing as an ID
  - What is hashing?
  - Hashing: many to fewer

Bellcore's S/Key System

- Start with a secure password
  - Using the same algorithm
    - Host and local server generate many one-time passwords
    - Use passwords sequentially
    - After each use, dispose of passwords
- Like One-Time Pads
- Like SecurID's hardware tokens

PPP, PAP, & CHAP

- PPP: point to point protocol
  - Secure links
  - Secure the transmission and exchange
  - Transmit passwords, User Ids, etc.
  - Allows challenges of authentication
    - Things change
    - Packets intercepted, etc.
- PAP:
  - Password Authentication Protocol
  - Clear text id and password pairs
  - Acknowledgements
- CHAP
  - Three-way handshake protocol using hashing

Other Security Methods

- Business: different needs
- RADIUS: Remote Authentication Dial In User Service
- TACACS: Cisco's server security protocol
  - Administers
    - Authentication
    - Authorization
    - Account information for users

TACACS and Cisco

- Uses a centralized server to hold all information
  - Why not distributed?
- Sends all data in cleartext (TACACS+ uses encryption for sending)
- Can handle a few other protocols!
- Business issues?

SSL

- Secure Socket Layer
- History
  - Unix Sockets and Pipes
  - Sockets and TCP/IP
- Internet Engineering Task Force and Netscape
- Goal: “privacy and reliability between two communicating applications”

SSL Goals

- Secure crypto connection between 2 parties
- Interoperability with different programs
- Extensibility: add new cryptographic methods as they appear
- Relative efficiency

SSL

- Two Layers
  - Low Level: Record Protocol (build on TCP/IP) encapsulates higher level protocols
  - Top Level Protocol: Handshake Protocol
    - Server and client authenticate each other
    - Negotiates encryption algorithms and keys
  - Top Level: Various Application Protocols
    - Different programs
    - Netscape, IE, etc.

SSL

- Private connection (via a socket)
- Authentication can use asymmetric encryption (RSA)
- Encryption used after initial handshake
  - Symmetric encryption is used for transmission (like DES)
- The connection must be reliable (TCP/IP) often over a socket

Firewall FAQ

- http://www.interhack.net/pubs/fwfaq/firewalls-faq.pdf
- Filter in/out access control
- Access control consistency
- Covers bad application protocols
- Cost/service benefit
- Network level
- Application level
  - ftp
  - Proxy
  - Direct

Firewall FAQ

- Allow only what is necessary
- Consider space between Extranet and Intranet to be “DMZ”
- Try to isolate single points of failure
- There are few technical solutions for social problems
- Watch out for:
  - ICMP re-directs
  - Proxies and mirrored data
  - DNS spoofing: IP hijacking, etc.

Firewall FAQ

- Watch for:
  - Port Scans
  - Sniffing
    - Password (use RSA, etc.)
    - Clear Text Sniffing
- Preventives
  - Use sniffers yourself
  - Monitor traffic
  - Anomaly detection

Firewall Heuristics

- Increase the level of security as you “go into your network site”
- In other words: inner fire-walls “stronger” than outer fire-walls
- Why?
- Partition Intranet and Extranet into security zones, possibly orthogonal to each other
- Include an experienced human in the loop

Other Methods

- PGP: protocol, see http://www.pgp.com/
- Secure MIME (Multipurpose Internet Mail Extensions): a hierarchical approach
- Cyber Cash
- SSL: get a secured link (socket)

System Penetration

- Reconnaissance
- Probe and attack
- Toehold
- Advancement
- Stealth
- Listening post
- Takeover

E-Commerce and Business

- On-line shopping grew by 300% Between 1997 and 2000
- On-line shopping grew by 600% in the last year
- Security made this possible
- IBM: “e-business is the transformation of key business processes through the use of Internet technologies”

ATM: Asynchronous Transfer Mode

- http://www.npac.syr.edu/users/mahesh/homepage/atm_tutorial
- http://www.iec.org/tutorials/atm_fund/topic01.html
- Integrates Voice, Video and Data
- Uses short fixed length packets called cells
- Not guaranteed delivery: best effort
- Bandwidth on demand: define circuit then get bandwidth
- Once a path is found from source and destination:
  - Then virtual circuit is established
  - All cells travel this path

ATM Design Questions

- Fixed length cells (48 bytes + 5 byte header)
  - Why? What does this have to do with Video, etc.
- Cells are delivered in order (though some can be lost)
- VPC: Virtual Path Connection: which path to take, that is for virtual circuits
- VCC: Virtual Channel Connection or a Virtual Circuit
- ATM network focuses on the VPC (the block of common start and destination virtual circuits)
  - Why is this good? Failure?

ATM Flavors

- Five service classes
  - constant bit rate (CBR)
  - variable bit rate–non-real time (VBR–NRT), uses statistical multiplexing
  - variable bit rate–real time (VBR–RT)
  - available bit rate (ABR)
  - unspecified bit rate (UBR)
- In what business sense are these useful?

ATM: Benefits

- ATM is between Circuit Switching and Packet Switching
- Uses “Statistical Multiplexing” for fast switching technology
  - Multiplexing: joining data for the trip
  - Gives high bandwidth use
- Very high speed
- Integrated types of traffic (Voice, Data, Video)

ATM General Design: PROS

- Not hardware or software specific
- Covers both LANs and WANS
- Super-scalability:
  - Number of users (multiplexing)
  - Geographic distance
- Consistent speed achievable by keeping same circuit

ATM General Design: CONS

- High overhead for each cell (lots of descriptive information)
- Packet loss possible: best effort, not guaranteed cell arrival (like TCP).
- Quality-of-service hard to guarantee

ATM: LAN or WAN?

- Can perform both broadcast and point-to-point
- Can use IP protocol
- Can use
  - 144 to 150 Mbps: OC3
  - 622 Mbps: OC12
  - 2.5 Gbps: OC48
  - Others…

VPNs

- Virtual Private Networks
  - Private networks constructed within a public network infrastructure such as the global Internet
  - Communications environments in which access is controlled to permit peer connections only within a defined community of interest, and is constructed through some form of partitioning of a common underlying communications medium, where this underlying communications medium provides services on a non-exclusive basis

VPNs

- Link layer
- Network layer
- Transport layer
- Application layer

Simple Game Theory

- Zero Sum Games
- General Sum Games: all equilibriums don't have the same payoffs!
  - Maximizing I does NOT necessarily Minimize II
  - Pure Strategy: can have no equilibriums!
  - Mixed Strategy
- Nash's Theorem: General Sum Pure Strategy Games Always Have Mixed Strategy Equilibriums!

Simple Game Theory

- The **Prisoner's Dilemma** shows how Pure Strategy can be locally optimal, but not globally optimal!
- Nash Equilibrium: (max payoff)
- In Nash Equilibrium iff for all s_i' we have:
- $g_i(s_1,\ldots,s_i',\ldots s_n) <= g_i(s_1,\ldots,s_i,\ldots s_n)$
- Depends on other player's choices

Prisoner's Dilemma

A_1 \ A_2	C	D
C	(3,3)	(0,4)
D	(4,0)	(1,1)

Lessons

- Nash Equilibrium: neither player has an incentive to move their position
- Rigid row and column issue!
- Not zero sum: no cooperation means not necessarily globally optimal
- What to do?