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

Outline

- Designing Web Pages
- Implementing Security for EC
- Introduction to Cryptography
- B2B EC Frameworks
- Active Server Pages

Designing Web Sites

- Web Usability
  - Page Design
  - Content Design
  - Site Design
  - Intranet Design
  - *Accessibility for Users with Disabilities*
  - *International Users*

Designing Web Sites

- Web Usability
  - "Designing Web Usability": Jakob Nielson: New Riders Publishing (2000)
    - **H**igh-quality Content
    - **O**ften Updated
    - **M**inimal Download Time
    - **E**ase of Use
    - **R**elevant to Users' Needs
    - **U**nique to the Online Medium
    - **N**et-centric Corporate Culture

Designing Web Sites

- Web Usability
  - What metrics will you use to measure the success of your Web Site?
    - Unique hits?
    - Total hits?
    - Return visits?

Designing Web Sites

- Page Design
  - Avoid fixed width text for material that may need to be printed
    - Narrow columns are wasteful and annoy users
    - Wide columns that do not fit the page are even more frustrating
    - 600 pixels is 8.3 inches at 72 pixels per inch
      - Allowing for printer margins, this exceeds standard letter paper
  - Do not force users to scroll horizontally!

Designing Web Sites

- "Creating Killer Web Sites": David Siegel: Hayden Books (2nd Edition 1997)
  - 3rd generation design
  - Use (but don't overuse) metaphor
  - GIF, JPEG, GIF89a, etc.
    - Transparency
  - Compress images to reduce download times

Designing Web Sites

- 3rd Generation Design
  - Entry points (splash screens)
    - Load quickly
    - Capture users
    - Tell them where they are and what's happening
  - Fish Food
    - Free goodies
  - The Core Page
    - Can be more than one
    - Guide users – offer choices but also suggestions
    - Avoid endless vertical lists of links
  - Exits
    - A well-marked exit entices users to stay!
    - Keep users within the site
    - Collect feedback?

Designing Web Sites

- David Siegel:
  - Control vertical space
  - Banish horizontal rules
  - In text, use proper indentation rather than extra space to delineate paragraphs
    - Don’t indent initial paragraph, or after white space
  - Use proper margins
  - Avoid long lines of text – they slow the reader down (10-12 words is ideal)

Designing Web Sites

- David Siegel:
  - Use tables with invisible cells to control page layout
    - Turn off borders
    - Insert a single space at the end of text in each column (but a soft carriage return at the end of text in the final column) to help break up text for users with old (non-table) browsers
  - The single-pixel gif trick
    - Scaling controls vertical or horizontal spacing
    - Should become less important as designers gain more control over browser behavior

Designing Web Sites

- David Siegel:
  - If you use frames, remember to add a No-Frames page
    - Useful for index or other links you want to keep visible during scrolling
  - Frame navigation is more complex and requires care
    - Don’t load new pages within old frames

Designing Web Sites

- David Siegel's Deadly Sins:
  - Blank line typography
  - Horizontal rules
  - Background images that interfere
  - The Slow Load
  - Illegal use of the third dimension
  - Aliasing, dithering and halos

Designing Web Sites

- Some additional references:
  - "Universal Web Design": Crystal Waters: New Riders Publishing (1997)
    - Creating accessible Web Sites
  - "Web Concept & Design": Crystal Waters: New Riders Publishing (1996)
    - Creating effective Web Sites

Designing Web Sites

- Designing Web Graphics.3": Lynda Weinman: New Riders Publishing (3rd Edition1999)
  - Preparing Images and Media for the Web
- RGB color v. CMYK color
  - CMYK
    - Subtractive
    - Printing
  - RGB
    - Additive
    - Computer screens
    - Hexadecimal colors (#FFFFFF)

Designing Web Sites

- Browser-Safe Colors
  - 216 common from palettes of 256 for Mac, Windows, Windows 95
  - Formed from hex 00, 33, 66, 99, CC and FF
    - Multiples of 51 for decimal-thinkers!
- sRGB
  - Microsoft/HP proposal
- Background colors and background images (tiles)
  - Use transparency

Designing Web Sites

- Some graphics software:
  - Adobe Photoshop
  - Paint Shop Pro
  - The Gimp
  - DeBabelizer

Designing Web Sites

- Many, many other things we have not discussed . . .
  - Image maps
  - Cascading style sheets (CSS)
  - DHTML
  - Shockwave
  - Video, audio, etc.

Designing Web Sites

- Content Design
  - Short text
  - Plain language
  - Users tend to scan rather than read
  - Titles/headers
  - Put the conclusion near the top!
  - Page chunking
  - Hypertext – non-linear design

Designing Web Sites

- Site Design
  - Splash screens should die
  - Use metaphor effectively but sparingly
    - Shopping carts
  - Navigation
    - Where am I? Where have I been? Where can I go?
    - Breadth v. depth
    - Site structure
  - Don’t include searches of the whole web on your site
  - URL design
    - Users guess!

Designing Web Sites

- Intranet Design
  - General principles apply, but
    - Users are employees rather than customers
    - There are typically many more pages
    - More advanced browsers features may be safely used if reasonable presumptions can be made about the facilities that users will have available

Implementing Security for EC

- Protecting Electronic Commerce Assets
  - Secrecy & Privacy
  - Integrity
  - Availability
  - Key management
  - Nonrepudiation
  - Authentication

Implementing Security for EC

- Intellectual Property and Privacy
  - Department of Justice: Computer Crime and Intellectual Property Section
  - Many other active bodies
  - Watermarks, ect.
  - WebSide Story
    - Cookie demonstration

Implementing Security for EC

- Protecting Client Computers
  - Monitoring active content
    - Digital certificates
      - VeriSign, etc.
    - Microsoft Explorer: Authenticode
    - Netscape
  - Antivirus software
  - Forensic experts

Implementing Security for EC

- Protecting Electronic Commerce Channels
  - Transaction Privacy
    - Encryption
    - Algorithms and Standards
    - Secure Sockets Layer Protocol
    - S-HTTP
  - Transaction Integrity
    - Hash Functions
    - Digital Signatures (encrypted hash functions)
  - Transaction Delivery

Implementing Security for EC

- Protecting the Commerce Server
  - Access Control and Authentication
  - Operating System Controls
  - Firewalls

Introduction to Cryptography

- No longer only the domain of the military
- Important business Issue
  - Financial transactions
  - Limiting distribution
  - Keeping important documents or transmissions confidential
- Issues of Government restrictions and economic well-being of US firms

Motivation for Cryptography

- General Reasons
  - Open data gives the Internet power
  - Authenticity in a very simulated environment!
  - Sharing information is important

Motivation for Cryptography

- Economic Reasons
  - Selling to comfortable customers
  - Currency transactions!
  - Monitor copying, etc.
  - Easy access to business information does not mean easy access by your competitors!

Basic Terms

- Plaintext or cleartext
- Encryption
- Ciphertext
- Cryptography
- Public key crypto systems (asymmetric)
- Private key crypto systems (symmetric)

Basic History

- Caesar Cipher: rotation of alphabets
- Alan Turing and his team: cracked the German Enigma in the early 1940s
  - Used the ACE computer
- C. Shannon at Bell Labs, 1940s
  - Showed the One-Time-Pad is the only "unbreakable code"
- Diffie-Hellman and the asymmetric or public key codes

History

- Rivest, Shamir and Aldeman: RSA public key cryptography
  - Found a good use for apparently very hard mathematical problems!
  - Unless there is a great mathematical breakthrough, the RSA and its relatives are VERY costly to break
- The US Government forbids export of this technology for now

Caesar Cipher

- ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Mapped to
- DEFGHIJKLMNOPQRSTUVWXYZABC
- Example: “GIVE ME TEN”
- Becomes: “JLYH PH WHP”
- Attacks: probability of letters occurring in English

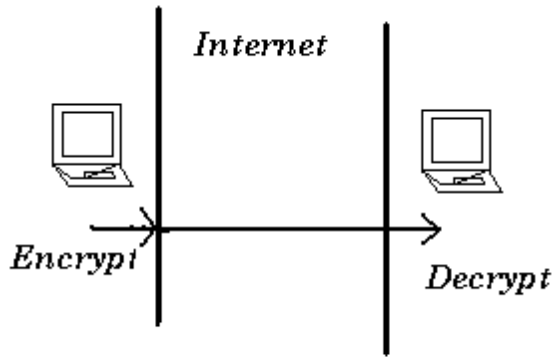
One-Time Pad

- Classic example: military frequency hopping
- Pre-agreed encryption key, like Gettysburg Address “Four Score and Seven Years Ago...” becomes the key to work from
- If the enemy discovers the pre-agreed key we loose!
- Only use this pre-agreed key once!

Pros and Cons of One-Time Pad

- Mathematically unbreakable!
- Good for one-off messages (very few Internet transactions are one-offs!)
- Have to have pre-agreed encryption key
- Can only use each encryption key only once!
- If pre-agreed encryption key is in files, then it is vulnerable!

Encrypt-Decrypt



Intercepting Messages or Packets?

- Ethernet
- Hubs
- Routers
- CPU Trace Cycles
- Screen
- Invasive: break in and copy/steal disks!

Public Key and RSA

- Why so popular?
  - Anyone can send messages and without trusting anyone else with your private key!
  - The mathematical problems that are at work are very well known to be very hard!
  - Extremely well trusted!
  - Easily integrated into present software systems

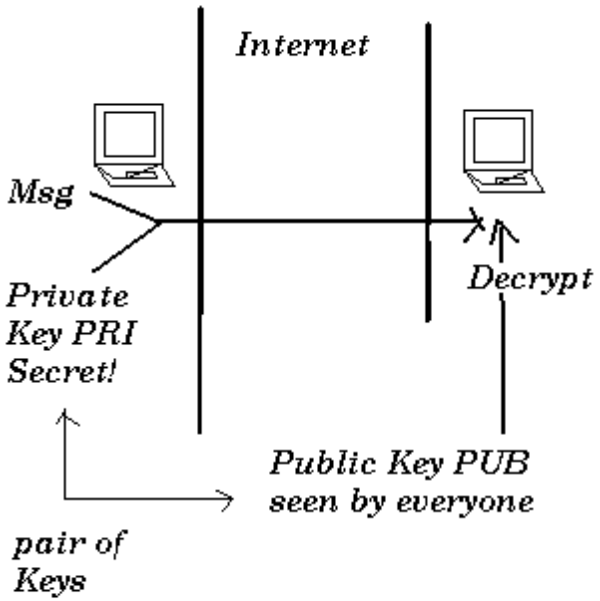
Public Key: How To

- Public Key PUB is seen by everyone!
- Private Key PRI is seen only by us
- PUB and PRI are inverses of each other
- From PUB you cannot determine PRI!
- Transaction type 1 (secret transmission):
  - I Encrypt message M with YOUR PUB and email PUB(M) to you. The only way to decrypt it is using your (secret) PRI key!

Public Key: How To

- Transaction type 2: Authentication
  - You encrypt M with your (secret) key PRI and email me PRI(M).
  - I use your public key PUB to decode PRI(M) verifying that the message was from you

Public Key (RSA)



A few uses

- Transactions
  - Secrets
  - Verifications
- Digital signatures
- Trusted companies or sites
- Digital cash!

DES, the NSA and all that

- Data Encryption Standard
- Symmetric
- First from IBM for a NBS Call for Proposals
- 40 bits, 56 bits and now 128 bits
- Why more bits over time?
- It apparently costs $200,000 to crack 56 bits in 4.5 days: 1998 Electronic Frontier Foundation

DES, the NSA and all that

- 8 bits allows how many keys?
- $2^8 = 256$ keys
- 100 bits? 2^{100}, a giant amount of keys!
- Shamir applied differential analysis and partially cracked DES

Attacks

- The notion of randomness as good cryptography
- Ciphertext only attack
- Known Plaintext attack
- Chosen Plaintext attack
- Man-in-the-middle
- Correlation attack

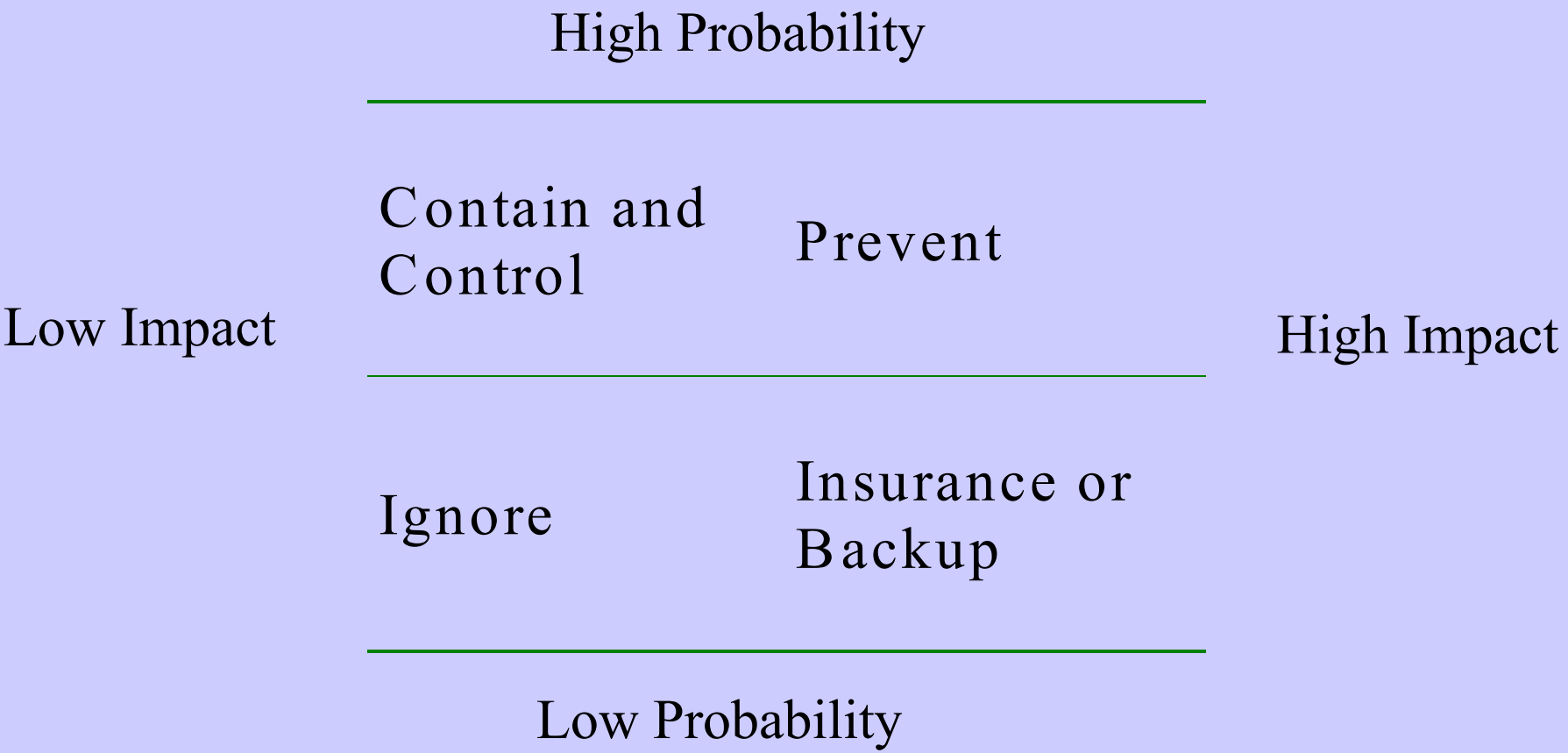
Security on the Internet

- Morris's worm: exploited the send-mail server, 3-Nov.-1988
  - Affected 10% of the internet (NSF Net)
  - Cost: $24 million in denial, $40 million to bring back
  - Total cost between $64 and $100 million
- The Internet is central to business now
- Business impacts would dwarf the NFS Net costs

More Security on the Internet

- Check out CMU's http://www.cert.org/
- Classical business parallels
  - Phone transactions
  - Mail transactions
- Logical and physical security
  - Countermeasures
  - Dealing with security threats

Risk Analysis



Risk Analysis Explained

- Why does “Low Probability” and “Low Impact” get “Insurance” or “Backup”?
- What does this mean for security?

Security in Pieces

- Secrecy: disclosure and authenticity
- Integrity: modifications
- Necessity: delays or denials
- Intellectual property: copyright, patents, etc.
- Should you have a privacy policy?
  - Why?
  - Where?
  - How to implement?

Evaluation of your Security

- Testing, testing, testing!
- Start with the “commerce chain”
- Active Content
  - JavaScript, ActiveX, CGI, VBScript, Java
- Email attachments: viruses and Trojan Horses
- Cookies
- What if you get too many security alerts?

Security in Pieces

- Sniffer programs
- Site hopping
- Click-trails
- Anonymizers
  - anonymizer.com
  - enonymous.com
- Cyber vandalism

Security in Pieces

- Masquerading or spoofing
- Necessity, delay or denial
  - Direct
  - Indirect
- Always provide the least privileges to do a job
- Super users on Unix, Administrator in NT and Windows

Security in Pieces

- The more passwords the better?
- Anonymous ftp, etc.
- Key economic tradeoff issue:
  - The more complex the security . . .
  - . . . the more costly it is to do anything!

Implementing Internet Security

- Planning testing, cycle
- Is the legal system prepared?
- Some businesses are Internet only!
- Robust security and trusted security is necessary for the Internet to flourish
- Digital signatures, digital watermarks
- Search! Use search engines for copyright, trademark and patent violations

Additional References

- S. S. Y. Shim V. S. Pendyala, and J.Z Gao: “Business-to-Business E-Commerce Frameworks”, Computer, 40-47, Oct. 2000.
- U. Varshney, R. J. Vetter and R. Kalakota: “Mobile Commerce: A New Frontier,” Computer, 32-29, Oct. 2000.

B2B EC Frameworks

- B2B is becoming much larger than B2C
  - Fewer customer interactions to sell large B2B unit
  - More standards necessary
- Tech standards not compatible: EDI in different countries
- Consider business as a set of processes
  - Process engineering streamlines and automates processes to improve efficiency

B2B EC Frameworks

- Defining Frameworks
  - Make all protocols between business partners have the same protocol
  - Standards:
    - data format
    - security
    - ontology
    - content management

B2B EC Frameworks

- Open Buying on the Internet (OBI)
  - High-volume and low-value B2B transaction
  - Infrastructure robustness supporting many users reliably and securely
  - Use digital certificates and optional digital signatures
  - Dynamic interoperable trading web. Many participants and easy to join
  - Chain reaction for making firms join

B2B EC Frameworks: OBI

- Work distributed among buyers and sellers; unlike e-Bay
- Complement EDI by overcoming its drawbacks
- Current implementation CGI and HTML
- Future? XML

B2B EC Frameworks: OBI

- Main Benefits
  - Simplicity
  - Security, reliability and robustness
  - Customizable catalogues based on digital certificates

B2B EC Frameworks: eCo

- From CommerceNet: consortium of reps from more than 35 firms
- Interoperability as a set of levels, eCo uses XML documents to describe APIs
- Businesses can define, publish and exchange metadata descriptions
- Layered approach to defining and maintaining interactions

B2B EC Frameworks: eCo

- Extensibility: unforeseen requirements
- Gateway web page for search engine needs
- A simple set of compliance rules
- Allow the discovery of EC systems and markets

B2B EC Frameworks: RosettaNet

- XML business standards for supply chain management
- Interoperable EC standards for high-tech firms
- Business process and tech spec building
- Framework for guidelines for trading partners in the supply chain
- Guidelines: PIPs - Partner Interface Processes

B2B EC Frameworks: RosettaNet

- Business dictionary: use the same language
- Protocol for exchanging messages securely
- Generic organization independent business process model
- Business process model, dictionary and implementation framework are inputs to the PIPs

B2B EC Frameworks: RosettaNet

- Benefits
  - In depth support for business process
  - Addresses security issues
  - Supports agent protocols

B2B EC Frameworks: cXML

- From Commerce XML
- Joint effort of more than 40 firms
- cXML is open Internet based standard for
  - Easy exchange of catalogue content
  - Easy exchange of transaction information
  - Made of ‘light weight’ DTDs
- Request/response model and asynchronous model

B2B EC Frameworks: cXML

- Uses HTTP and/or URL formed encodings based communication
- Web browser acts as an intermediary
- cXML focus on maintenance, repair and operating services (MRO).
- Allows us to define parts of business processes
- Simple to use and easy to implement

B2B EC Frameworks: BizTalk

- Leverages existing standards
- Application integration to facilitate EC
- It serves as a platform to quick migration to XML
- A firm's XML schemas are:
  - Validated
  - Versioned
  - Stored

B2B EC Frameworks: BizTalk

- Benefits
  - Schema versioning, better schema control
  - XML with support for non-XML data
  - Transition Planning for legacy EDI

B2B EC Frameworks: Comparison

- Industry targeting
- Architecture
  - XML?
  - With EDI?
  - Replace EDI?
- Security
- Protocols: most HTTP, one CGI

Active Server Pages

- Microsoft innovation
- Server-generated pages that can invoke other programs (e.g., to access a database)
- Use server-side scripting with support for VBScript or Jscript
- Many other software tools now supported
- Runs more efficiently than CGI scripts

Active Server Pages

- Has been used extensively
  - E.g., Amazon.com
- Now available on non-Microsoft servers
- Although HTML is the default output, could also be XML
- Not use of <& . . . &> pairs for server-side scripts
- *N.B. Now there is JSP too!*

Active Server Pages

```
<%
    dim BrowserType
    set bc = Server.CreateObject("MSWC.BrowserType")
    if bc.browser="IE" then
      BrowserType = "MSIE"
    elseif bc.browser="Netscape" then
      BrowserType = "Netscape"
    elseif bc.browser="Lynx" then
      BrowserType = "Lynx"
    end if
%>
```

Active Server Pages

```
<%
    select case BrowserType
    case "Lynx"
      Response.Write("You're using Lynx! How do you manage to live
      without 3-D backgrounds and endless download times? Whatever!")
    case "MSIE"
      Response.Write("You're using Internet Explorer! Thank you for helping
      keep Microsoft afloat!")
    case "Netscape"
      Response.Write("You're using Netscape! And you're wearing those
      great pink pants! ASP knows everything about you!")
    case else
      Response.Write("You're using some other browser I don't know
      about.")
    End select
%>
```