

E-commerce

Security cnt.

User Experience



Nov 26, 2004 www.dcs.bbk.ac.uk/~gmgoulas/teaching.html 1

E-commerce Security-cnt

- Internet security issues (last week)
- Security for client computers (last week)
- Security for the communication channels between computers
- Security for server computers

Nov 26, 2004 www.dcs.bbk.ac.uk/~gmgoulas/teaching.html 2

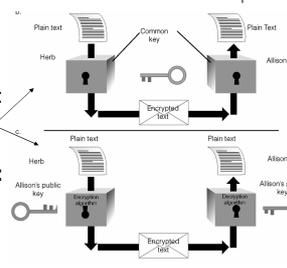
Protecting Communication Channel- Encryption Solutions

- **Encryption:** Using a mathematically based program and a secret key to produce a string of characters that is unintelligible
- **Cryptography:** Science that studies encryption. It has four basic parts
 - Plain text: the original text in human-readable form
 - Cipher text: the plain text after it has been encrypted
 - Encryption algorithm: the mathematical formula that encrypts the plaintext into cipher text and vice versa
 - Key: the secret key used to encrypt and decrypt a message. Different keys produce different cipher text when used with the same algorithm.

Nov 26, 2004 www.dcs.bbk.ac.uk/~gmgoulas/teaching.html 3

Protecting Communication Channel-1

- **Public key (asymmetric encryption):** Freely distributed to the public at large.
- **Private key (symmetric encryption):** Belongs to the key owner, who keeps the key secret.



Nov 26, 2004 www.dcs.bbk.ac.uk/~gmgoulas/teaching.html 4

Protecting Communication Channel-2

Public key cryptography

Theory: belongs to a class of NP-complete problems known as **knapsack problem**

This is the problem of selecting numbers from a collection so that the sum of the selected numbers is a particular value.

Solution: try all possible combinations systematically until a solution is found.

Nov 26, 2004 www.dcs.bbk.ac.uk/~gmgoulas/teaching.html 5

Protecting Communication Channel-3

How it works

1. Define a list of numbers: let's say
191 691 573 337 365 730 651 493 177 354
2. Represent a message as a string of bits (using ASCII or Unicode)
3. Break the string into segments of n-bits (let's say 10 bits because we have 10 numbers in our list) each and represent each 10-bit segment by a single number. This number is obtained by adding the values from the list that occupy the positions of the 1s in the 10-bit segment. For example, the 10-bit segment 1001100001 would be represented by 1247

Example: 10011000010010011010 → 1247 2131

Nov 26, 2004 www.dcs.bbk.ac.uk/~gmgoulas/teaching.html 6

Protecting Communication Channel-4

	[0 0 1 0 0 1 1 0 1 0]
Bit pattern	1 0 0 1 1 0 0 0 0 1
	↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
Knapsack values	191 691 573 337 365 730 651 493 177 354
	↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
Sum	1247=191 + 337+365 + 354
	[2131= 573 + 730+651 +177]

2^n (number of values is $n=10$) possible combinations

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmgoulas/teaching.html

7

Ensuring Transaction Integrity with Digital Signatures

- Anyone could intercept a purchase order: alter the shipping address and quantity ordered; re-create the message digests; send the message and new message digest on to the merchant
- Digital signature: An encrypted message digest

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmgoulas/teaching.html

8

Sending and Receiving a Digitally Signed Message

1. The sender creates a phrase (e.g. John Smith) and encrypts it with her **private key**;
2. The phrase is attached to the message and the combined message is encrypted with the **recipient's public key**;
3. Upon receipt the message is decrypted with the **recipient's private key**;
4. The signature phrase is decrypted with the **sender's public key**;
5. If the phrase is successfully decrypted then the recipient knows that the message could have only been sent by the holder of the sender's private key.

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmgoulas/teaching.html

9

Protecting the web server-Firewalls1

- Computer and software combination installed at the Internet entry point of a networked system
- Provides a defense between
 - Network to be protected and the Internet, or other network that could pose a threat
- All corporate communication to and from Internet flows through firewalls

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmgoulas/teaching.html

10

Protecting the web server-Firewalls2

- Characteristics
 - All traffic from inside to outside and from outside to inside the network must pass through firewall
 - Only authorized traffic is allowed to pass
 - Firewall itself is immune to penetration
- Trusted
 - Networks inside the firewall
- Untrusted
 - Networks outside the firewall

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmgoulas/teaching.html

11

Protecting the web server-Firewalls3

- **Packet-filter firewalls:** Examine data flowing back and forth between trusted network and the Internet
- **Gateway servers:** Firewalls that filter traffic based on the application requested
- **Proxy server firewalls:** Firewalls that communicate with the Internet on the private network's behalf

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmgoulas/teaching.html

12

User experience (this week)

- User-centred design/Usability
- Web usability
- Usability guidelines
- Gathering user requirements
- Usability techniques
- Example: online shopping (ASDA, Iceland, Sainsbury, and Tesco)

Nov 26, 2004

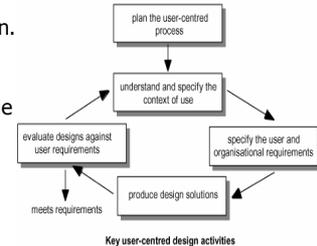
www.dcs.bbk.ac.uk/~gmgoulas/teaching.html

13

Usability

Usability is a very broad concept in system design. It is concerned with:

- designing software applications which people find convenient and practicable for use
- how usable or user-friendly the product, service, or system is.



Nov 26, 2004

www.dcs.bbk.ac.uk/~gmgoulas/teaching.html

14

Web usability-1

Facts

- 79% of users **scan the page** instead of reading word-for-word;
- Reading from computer screens is 25% slower than from paper;
- Web content should have **50% of the word count** of its paper equivalent

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmgoulas/teaching.html

15

Web usability-2

Fundamental errors on web design levels

- **Business model:** treating the web as a brochure (it's a new way to conduct business)
- **Project management:** as any other corporate project (fails to look at customer needs)
- **Information architecture:** the site mirrors the structure of the company (should mirror users' tasks and their view of the information space)

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmgoulas/teaching.html

16

Web usability-3

Fundamental errors on web design levels

- **Page design:** creating internal demos (does not expose the difficulties a novice user will have; it is not realistic; does not suffer the response time delays)
- **Content authoring:** use a linear style (user scan text, need very short pages, use hyperlinks for secondary information)
- **Linking strategy:** no well designed entry point for other to link to; no links to other websites (use hypertext; no site is an island)

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmgoulas/teaching.html

17

Usability guidelines-1

- **Sun Microsystems'** guidelines can be used to ensure that users can read content on a site with ease. <http://www.sun.com/980713/webwriting/>
- **Stanford Web Credibility Research** has produced ten guidelines to ensure that web sites are seen as credible and trustworthy. <http://www.webcredibility.org/guidelines/>
- **The National Cancer Institute** has lists of design guidelines, where each one is accompanied by an indication of the supporting research. <http://www.usability.gov/guidelines/index.html>
- **The W3C Web Accessibility Initiative's** guidelines are frequently relevant to usability as well as accessibility, and are the standards recommended by UK government. <http://www.w3.org/TR/WCAG10/full-checklist.html>

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmgoulas/teaching.html

18

Usability guidelines-2

Guidelines for Web Credibility (from www.webcredibility.org)

1. Make it easy to verify the accuracy of the information on your site.

You can build web site credibility by providing third-party support (citations, references, source material) for information you present, especially if you link to this evidence. Even if people don't follow these links, you've shown confidence in your material.

2. Show that there's a real organization behind your site.

Showing that your web site is for a legitimate organization will boost the site's credibility. The easiest way to do this is by listing a physical address. Other features can also help, such as posting a photo of your offices or listing a membership with the chamber of commerce.

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmagouas/teaching.html

19

Usability guidelines-3

Guidelines for Web Credibility (from www.webcredibility.org)

3. Highlight the expertise in your organization and in the content and services you provide.

Do you have experts on your team? Are your contributors or service providers authorities? Be sure to give their credentials. Are you affiliated with a respected organization? Make that clear. Conversely, don't link to outside sites that are not credible. Your site becomes less credible by association.

4. Show that honest and trustworthy people stand behind your site.

The first part of this guideline is to show there are real people behind the site and in the organization. Next, find a way to convey their trustworthiness through images or text. For example, some sites post employee bios that tell about family or hobbies.

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmagouas/teaching.html

20

Usability guidelines-4

Guidelines for Web Credibility

5. **Make it easy to contact you:** A simple way to boost your site's credibility is by making your contact information clear: phone number, physical address, and email address.

6. **Design your site so it looks professional (or is appropriate for your purpose):** people quickly evaluate a site by visual design alone. When designing your site, pay attention to layout, typography, images, consistency issues, and more. Of course, not all sites gain credibility by looking like IBM.com. The visual design should match the site's purpose.

7. **Make your site easy to use – and useful:** sites win credibility points by being both easy to use and useful. Some site operators forget about users when they cater to their own company's ego or try to show the dazzling things they can do with web technology.

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmagouas/teaching.html

21

Usability guidelines-5

Guidelines for Web Credibility

8. **Update your site's content often (at least show it's been reviewed recently):** People assign more credibility to sites that show they have been recently updated or reviewed.

9. **Use restraint with any promotional content (e.g., ads, offers):** If possible, avoid having ads on your site. If you must have ads, clearly distinguish the sponsored content from your own. Avoid pop-up ads, unless you don't mind annoying users and losing credibility. As for writing style, try to be clear, direct, and sincere.

10. **Avoid errors of all types, no matter how small they seem:** Typographical errors and broken links hurt a site's credibility more than most people imagine. It's also important to keep your site up and running.

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmagouas/teaching.html

22

User requirements

Gathering users' requirements is often done at the beginning of a project. But **users' needs and expectations change and evolve** (as do your competitors), so efforts to understand needs should be ongoing.

There are many **ways to gather requirements** from users, including surveys, interviews, focus groups, informal chats and observation.

User-Centred Requirements handbook:

<http://www.jiscinfonet.ac.uk/Resources/external-resources/user-centred-requirements-handbook/view>

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmagouas/teaching.html

23

Usability techniques-1

- **Heuristic evaluation:** interface is scrutinised against a set of recognised usability principles, or 'heuristics'
- **User Testing:** evaluation that involves users to assess usability issues.
- **Log analysis:** analysis of user interactions, searching and navigation in order to generate hypotheses about user's behaviour.

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmagouas/teaching.html

24

Usability techniques-2

Heuristic evaluation (see <http://www.humanfactors.com/>)

- Visibility of system status
- Match between system and the real world
- User control and freedom
- Consistency and standards
- Error prevention
- Recognition rather than recall
- Flexibility and efficiency of use
- Aesthetic and minimalist design
- Help users recognise, diagnose and recover from errors
- Help and documentation

Nov 26, 2004

www.dcs.bbk.ac.uk/~gnagoulas/teaching.html

25

Example: online shopping-1



Example: online shopping*-2

Heuristics	
H1	Visibility of system status
H2	Match between system and the real world
H3	User control and freedom
H4	Consistency and standards
H5	Error prevention
H6	Recognition rather than recall
H7	Flexibility and efficiency of use
H8	Aesthetic and minimalist design
H9	Help users recognise, diagnose and recover from errors
H10	Help and Documentation
Additional Heuristics	
H11	Support and extend the user's current skills
H12	Pleasurable and respectful interaction with the user
H13	Protect the personal information

* For details on this application example, please refer to [Chen, S. Y. and Macredis, R. D. (forthcoming) Assessment of the User Interface of Electronic Shopping: a Heuristic Evaluation. International Journal of Information Management]

Nov 26, 2004

www.dcs.bbk.ac.uk/~gnagoulas/teaching.html

27

Example: online shopping*-3

Heuristics	Interface Considerations	Purposes
H1: Visibility of system status	To highlight current option selected To breakdown steps required to complete tasks, and highlight current step reached in interaction process To display all options pertinent to the users tasks during interactions To display messages if observable delays are longer than 10 seconds.	To identify current location in interaction process During all tasks, to indicate to users how much more longer there is to go. At every time during the interaction, to indicate to users what options are available and the alternatives for action To keep users informed of the systems progress
H2: Match between the system and the real world	To provide easily identifiable icons when needed To use clear, simple language for question and answer To arrange task/menu choices in a logical order according to natural sequences To provide meaningful menu choices	To make information easy to remember and identify To decrease cognitive load on users. To allow menu choices to be readily understood
H3: User control and freedom	To provide mechanisms for undoable menu levels To provide undo functions for every action/group of actions To provide back options on every page where a user is completing tasks. To provide users with customisation of system, session and screen defaults	To allow users to go back to previous menus To allow users to reverse their actions and change earlier choices To give users the freedom to select and sequence their own tasks where possible. To allow users to set their own preferences
H4: consistency & standards	To follow company formatting standards. To match menu structure to task structure To provide vertical/horizontal scrollbars in all windows to be viewed To follow consistent standards for interaction design To use consistent location for online instructions	To maintain consistency throughout the site To reduce cognitive load on user To allow all information in every window to be viewed. To facilitate easy interactions with the system To help users easily find instructions
H5: Help users recognise, diagnose & recover from errors	To show meaningful error messages To provide suggestion actions when users make errors. To show constructive, brief, unambiguous messages To highlight the field in error in data-entry fields	To suggest the causes of the problems To allow users to recover from the error To imply that the user is in control To attract attention on the particular field in error

Heuristics	Interface Considerations	Purposes
H6: Error prevention	To provide default values when users fill out the forms To put less frequently used options in least convenient positions To show way out for users to exit the system To put function keys causing serious consequences far way from low consequence and high use keys To show warning message if users are about to make serious error	To reduce the likelihood of errors occurring To use the screen effectively To ensure users cannot get stuck To prevent errors To make sure user has not selected an option in error
H7: Recognition rather than recall	To group items in logical zones with headings To place prompts where eye is likely to be looking To use colours to group related elements To distinguish emphatic data and de-emphasize data with different colours	To distinguish between different groups of items/zones To make prompts clearly visible to users To distinguish between groups of elements To draw attention to important data. To make less important information not distracting.
H8: Flexibility and efficiency of use	To allow user to save partially filled forms To provide multiple levels of detail To allow tasks to be resumed after a short period of time To provide shortcuts for high-frequency actions	To allow flexibility for users to return to their work at a later time. To cater for the different needs of novice and expert users To speed up interactions for users
H9: Aesthetic and minimalist design	To display only essential decision-making information on screen To show brief and clear title for each screen To separate meaningful groups of items by using white space	To increase visibility of essential information To make immediately apparent the nature of content within each screen To increase visibility of different groups of items
H10: Help and documentation	To maintain consistent help system interface To provide option to switch between help and work To provide additional explanatory information for ambiguous options To allow work to be resumed from where left off after accessing help	To ensure consistent standards applied throughout the site. To allow users to easily switch between help and their work To provide further help where it is most likely to be needed without having to search through the help system. To anticipate the users' expectations
H11: Skills	To make important keys larger than other keys To allow users to initiate actions	To make important options highly visible To anticipate users' expectations To ensure users can actively take actions rather than respond to the

Example: online shopping*-5

Heuristics	Asda	Sainsbury
1. Visibility of system status	Strength: During tasks, users can always tell how much more longer there is to go. Weakness: The system does not tell the user the state of the system and the alternatives for action.	Strength: The user can easily determine when they are and what options are available. Weakness: When the system requires in additional steps are not large portions of the system's progress.
2. Match between the system and the real world	Strength: Icons are easy to identify and readable. Weakness: The system does not anticipate the user's expectations at each step.	Strength: Task menu choices are ordered in the most logical way. Weakness: System does not anticipate user's expectations at each step.
3. User control and freedom	Strength: Users can easily reverse actions. Weakness: No undo function for any group of actions. Users cannot set up their own defaults.	Strength: For multiple menu levels, a back button allows users to go back to previous menu choices. Weakness: No undo function for the active group of actions.
4. Consistency and standards	Strength: Consistent formatting standards have been applied throughout the site. Weakness: Vertical and horizontal scrolling can work in all windows.	Strength: Online instructions appear in a consistent location across systems. Weakness: Optional data entry fields are inconsistently marked.
5. Help users recognise, diagnose, recover from errors	Strength: Prompts are brief and constructive. Weakness: Error messages do not provide appropriate, immediate information.	Strength: Error messages do not provide constructive information. Weakness: Some messages are not helpful and distracting.
6. Error prevention	Strength: Fields on data entry screens and dialogue boxes contain default information when appropriate. Weakness: Users are stuck if a sensor is not detected.	Strength: Error messages do not provide constructive information. Weakness: Some messages are not helpful and distracting.
7. Recognition rather than recall	Strength: The same colour is used to group related elements. Weakness: Principles, cues and icons are not obvious.	Strength: The system provides options for multiple menu levels. Weakness: Only information essential to actions leading to developed actions.
8. Flexibility and efficiency of use	Strength: None. Weakness: Users cannot be interrupted at all.	Strength: The system provides options for multiple menu levels. Weakness: Only information essential to actions leading to developed actions.
9. Aesthetic and minimalist design	Strength: Each screen has a short, clear, distinctive title. Weakness: Some irrelevant information is included in with the rest of the site.	Strength: The system provides options for multiple menu levels. Weakness: Only information essential to actions leading to developed actions.
10. Help and documentation	Strength: It is easy to access and content from the help system. Weakness: The help system interface is inconsistent with the rest of the site.	Strength: Additional explanatory information is provided when ambiguous menu choices are selected. Weakness: Users cannot easily switch between help and their work.
11. Skills	Strength: The system performs data transactions for users. Weakness: The help system interface is inconsistent with the rest of the site.	Strength: The system provides options for multiple menu levels. Weakness: Only information essential to actions leading to developed actions.
12. Pleasurable and respectful interaction with the user	Strength: Content is used with discretion. Weakness: Exclusive window hovering is required.	Strength: Very effective use of colours. Weakness: Protected areas can be accessed with certain passwords.
13. Privacy	Strength: None. Weakness: Password functions are ineffective.	Strength: Protected areas can be accessed with certain passwords. Weakness: None.

Nov 26, 2004

www.dcs.bbk.ac.uk/~gnagoulas/teaching.html

30

Summary

Customer needs are central to services a company provides → poor usability results in lost revenue.

A usable web site:

- allows users to easily and quickly do their tasks
- offers functionalities that are easy to remember
- prevents the user from making mistakes, and ensures any mistakes made can be corrected
- tries to maximise user's subjective satisfaction.

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmagouas/teaching.html

31

Next week

SEMINAR- From E-commerce to E-business: current developments and future directions

Dr Natasha Papazafeiropoulou, Brunel University

E-commerce started as a tidal wave in the 1990's affecting the majority of companies and industry sectors. It has changed the way companies do business by creating new channels for customers and redefining supply chain relationships. These effects were either revolutionary (Dell.com) or rather catastrophic (DotComs failures). While managers are still trying to cope with e-commerce challenges they now have to familiarise themselves with the next stage of this business evolution, which is e-business. E-business is the complex fusion of business processes, enterprise applications and organisational structure necessary to create a high-performance business model.

In this seminar we take a **technology-oriented** as well as **strategy-oriented** approach to e-commerce/business phenomenon, analysing cases studies from various industry sectors, while giving projections for the future of the e-commerce era. You are expected to participate in an active discussion about the pros and cons of e-commerce practices, comment on case studies and even give your ideas for successful application of e-commerce endeavours.

Nov 26, 2004

www.dcs.bbk.ac.uk/~gmagouas/teaching.html

32