SECURITY IN COMPUTING, FIFTH EDITION

Chapter 4: The Web—User Side

Chapter 4 Objectives

- Attacks against browsers
- Fake and malicious websites
- Attacks targeting sensitive data
- Injection attacks
- Spam
- Phishing attacks

Browsers

- Our focus here is on the user or client side: harm that can come to an individual user interacting with Internet locations.

- Browsers - the software most users perceive as the gateway to the Internet.

- Browser is software with a relatively simple role:
  - connect to a particular web address, fetch and display content from that address, and transmit data from a user to that address.

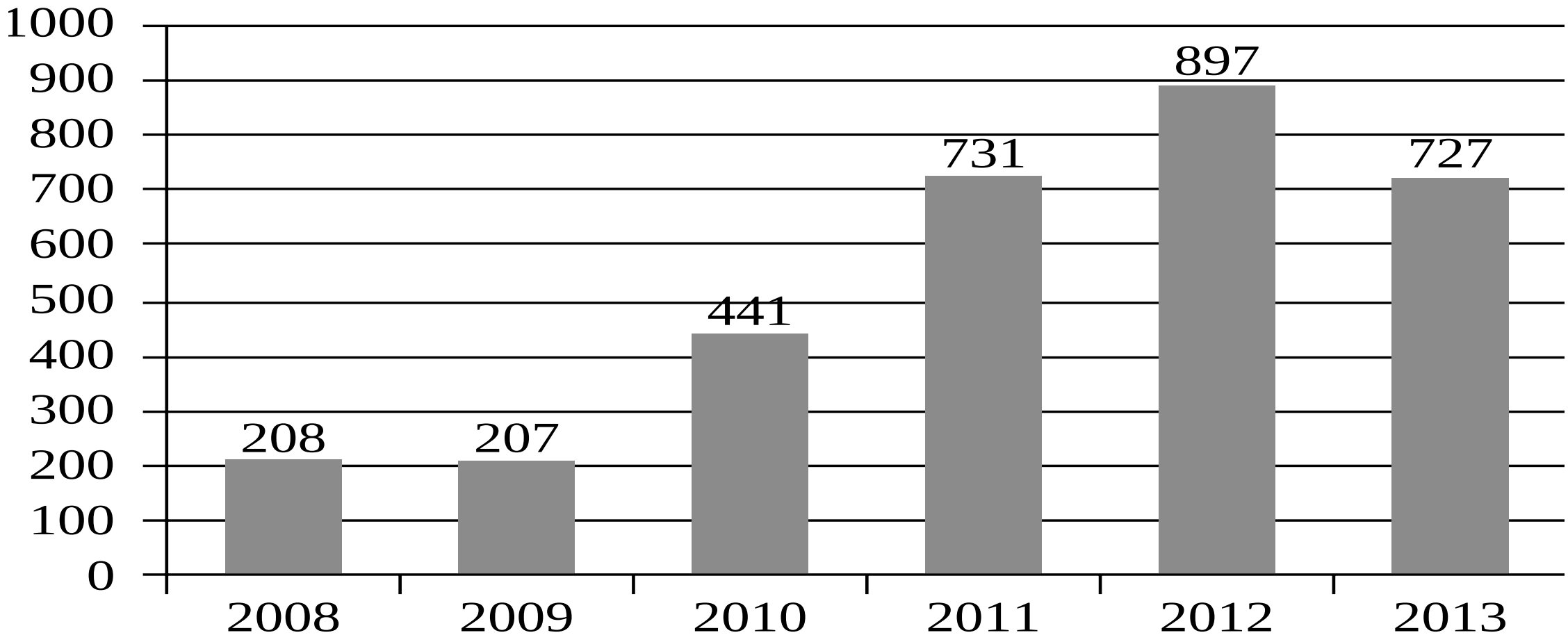
Browsers

- Security issues for browsers
- A browser often connects to more than the one address shown in the browser's address bar.
- Fetching data can entail accesses to numerous locations to obtain pictures, audio content, and other linked content.
- Browser software can be malicious or can be corrupted to acquire malicious functionality.
- Popular browsers support add-ins, extra code to add new features to the browser, but these add-ins themselves can include corrupting code.

Browsers

- Data display involves a rich command set that controls rendering, positioning, motion, layering, and even invisibility.
- The browser can access any data on a user's computer (subject to access control restrictions); generally the browser runs with the same privileges as the user.
- Data transfers to and from the user are invisible, meaning they occur without the user's knowledge or explicit permission.
- **Browsers connect users to outside networks, but few users can monitor the actual data transmitted**

Browser Vulnerabilities



Browser Attack

There are three attack vectors against a browser:

- Go after the operating system so it will impede the browser's correct and secure functioning.
- Tackle the browser or one of its components, add-ons, or plug-ins so its activity is altered.
- Intercept or modify communication to or from the browser.

Browser Attack Types

- Man-in-the-browser
- Keystroke logger
- Page-in-the-middle
- Program download substitution
- User-in-the-middle

Man-in-the-Browser

User types

SilentBanker intercepts

Browser encrypts

Encrypted data transferred to bank

Man-in-the-Browser

Man-in-the-Browser

- SSL encryption is applied in the browser; data are vulnerable before being encrypted.
- As you can see, man-in-the-browser attacks can be devastating because they represent a valid, authenticated user.
- The Trojan horse could slip neatly between the user and the bank's web site, so all the bank's content still looked authentic.
- SilentBanker had little impact on users, but only because it was discovered relatively quickly, and virus detectors were able to eradicate it promptly.
- Nevertheless, this piece of code demonstrates how powerful such an attack can be.

Keystroke Logger

- Hardware or software that records all keystrokes
- May be a small dongle plugged into a USB port or can masquerade as a keyboard
- May also be installed as malware
- The logger either retains these keystrokes for future use by the attacker or sends them to the attacker across a network connection.

Keystroke Logger

- Such devices can capture passwords, login identities, and all other data typed on the keyboard.
- Not limited to browsers

Page-in-the-Middle

- User is directed to a different page than believed or intended
- Similar effect to a man-in-the-browser, where attacker can intercept and modify user input
- As an example, when the user clicks “login” to go to the login page of any site, the attack might redirect the user to the attacker’s page, where the attacker can also capture the user’s credentials.

Page-in-the-Middle

The difference

- The man-in-the-browser action is an example of an infected browser that may never alter the sites visited by the user but works behind the scenes to capture information.

- In a page-in-the-middle action, the attacker redirects the user, presenting different web pages for the user to see.

Program Download Substitution

- Attacker creates a page with seemingly innocuous and desirable programs for download
- Instead of, or in addition to, the intended functionality, the user installs malware
- for example, a browser toolbar or a photo organizer utility.
- This is a very common technique for spyware
- **A user agreeing to install a program has no way to know what that program will actually do.**
- In this attack, the user knows of and agrees to a download, not realizing what code is actually being installed.

User-in-the-Middle

- A different form of attack puts a human between two automated processes so that the human unwittingly helps spammers register automatically for free email accounts.
- Using click-bait to trick users into solving CAPTCHAs on spammers' behalf

How Browser Attacks Succeed: Failed Identification and Authentication

- The central failure of these in-the-middle attacks is faulty authentication.
- If A cannot be assured that the sender of a message is really B, A cannot trust the authenticity of anything in the message.

- **Human Authentication :** authentication is based on something you know, are, or possess.
- Human-to-computer authentication uses sophisticated techniques such as biometrics and so-called smart identity cards.
- These human factors can affect authentication in many contexts because humans often have a role in authentication, even of one computer to another

How Browser Attacks Succeed: Failed Identification and Authentication

- The central failure of these in-the-middle attacks is faulty authentication.
- If A cannot be assured that the sender of a message is really B, A cannot trust the authenticity of anything in the message.

- **Computer Authentication**: Fully automated computer-to-computer authentication has additional difficulties

Computer Authentication

- When a user communicates online with a bank, the communication is really user-to-browser and computer-to-bank's computer.
- Although the bank performs authentication of the user, the user has little sense of having authenticated the bank.
- **Your bank takes steps to authenticate you, but how can you authenticate your bank?**
- The system needs assurance that the user is authentic, but the user needs that same assurance about the system.
- This second issue has led to a new class of computer fraud called phishing, in which an unsuspecting user submits sensitive information to a malicious system impersonating a trustworthy one.

Computer Authentication

Authentication is vulnerable at several points:

- Usability and accuracy can conflict for identification and authentication: A more usable system may be less accurate. But users demand usability, and at least some system designers pay attention to these user demands.
- Computer-to-computer interaction allows limited bases for authentication. Computer authentication is mainly based on what the computer knows, that is, stored or computable data. But stored data can be located by unauthorized processes, and what one computer can compute so can another.

Computer Authentication

Authentication is vulnerable at several points:

- Malicious software can undermine authentication by eavesdropping on (intercepting) the authentication data and allowing it to be reused later. Well placed attack code can also wait until a user has completed authentication and then interfere with the content of the authenticated session.
- Each side of a computer interchange needs assurance of the authentic identity of the opposing side. This is true for human-to-computer interactions as well as for computer-to-human.

Successful Authentication

- The attacks listed above are largely failures of authentication Can be mitigated with

- **Shared secret** – e.g. mother's maiden name, secret verification number, Street on which you grew up, first school attended, and model of first car are becoming popular.
- **One-time password** – e.g. SecurID token, google authenticator, SMS etc.
- **Out-of-band communication** – e.g. Bank card PINs, phone call,

Continuous Authentication

- Encryption can provide continuous authentication, but care must be taken to set it up properly and guard the end points.
- If two parties carry on an encrypted communication, an interloper wanting to enter into the communication must break the encryption or cause it to be reset with a new key exchange between the interceptor and one end.
- These mechanisms—signatures, shared secrets, one-time passwords and out-of-band communications—are all ways of establishing a context that includes authentic parties and excludes imposters.

Web Attacks Targeting Users

- **False or Misleading Content**
- The first kind involves false content, most likely because the content was modified by someone unauthorized; with these the intent is to mislead the viewer.

- **Malicious Web Content**
- The second, more dangerous, kind seeks to harm the viewer.

Web Attacks Targeting Users

- **False or Misleading Content**
  - It is difficult to tell when an art work is authentic or a forgery
  - An incoherent message, a web page riddled with grammatical errors, or a peculiar political position can all alert you that something is suspicious, but a well-crafted forgery may pass without question.
  - The falsehoods that follow include both obvious and subtle forgeries.
- **Defaced Web Site**
  - a website defacement, occurs when an attacker replaces or modifies the content of a legitimate web site.
  - these attacks attempt to defeat the integrity of the web page.
  - to prove a point or embarrass the victim
  - to make a political or ideological statement
- **Fake Website - The attacker can get all the images a real site uses; fake sites can look convincing.**

Fake Website

Fake Code

Protecting Web Sites Against Change

- **Integrity Checksums**
  - It a checksum, hash code, or error detection code is a mathematical function that reduces a block of data (including an executable program) to a small number of bits.
  - Using a checksum, you trust or hope that significant changes will invalidate the checksum value.
  - **Integrity checksums can detect altered content on a web site.**
  - To detect data modification, administrators use integrity-checking tools, of which the Tripwire program is the most well known.
- **Signed Code or Data**
  - Using an integrity checker helps the server-side administrator know that data are intact; it provides no assurance to the client.
  - A digital signature can vouch for the authenticity of a program, update, or dataset. The problem is, trusting the legitimacy of the signer.

Malicious Web Content

- Arbitrary code could be delivered to an unsuspecting site visitor.
- It could be either nonmalicious or malicious.
- someone could rewrite a web site in a way that would embarrass, deceive, or just poke fun —the defacer's motive may not be obvious.
- Substitute Content on a Real Web Site

Download important things to read:

Studies of low-order even primes	pdf file
How to cheat at solitaire	pdf file
Making anti-gravity paint and what to store it in	pdf file
101 things to do with string	pdf file

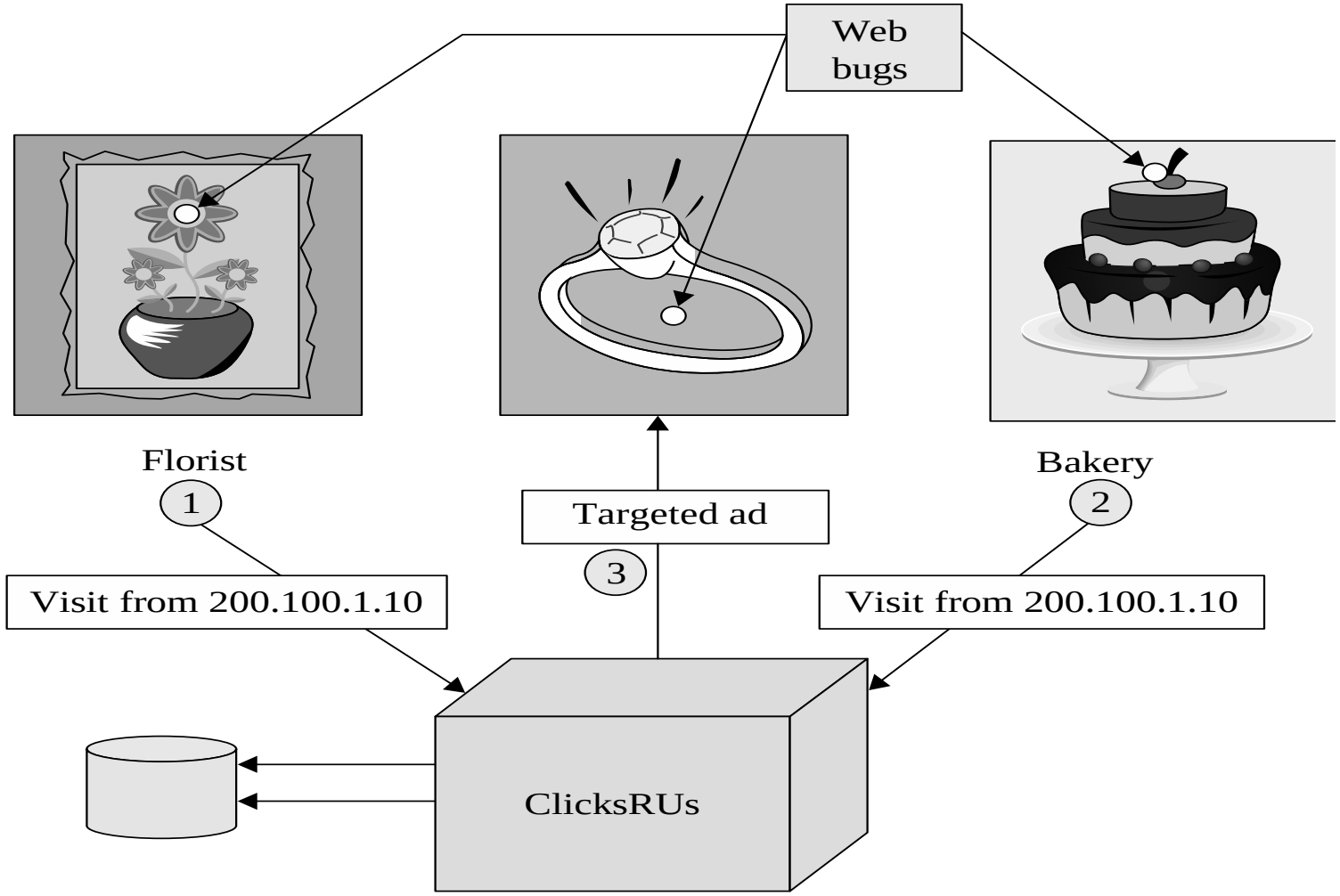
Download my infected version of Adobe Reader here

FIGURE 4-11 Malicious Code to Download

Web Bug

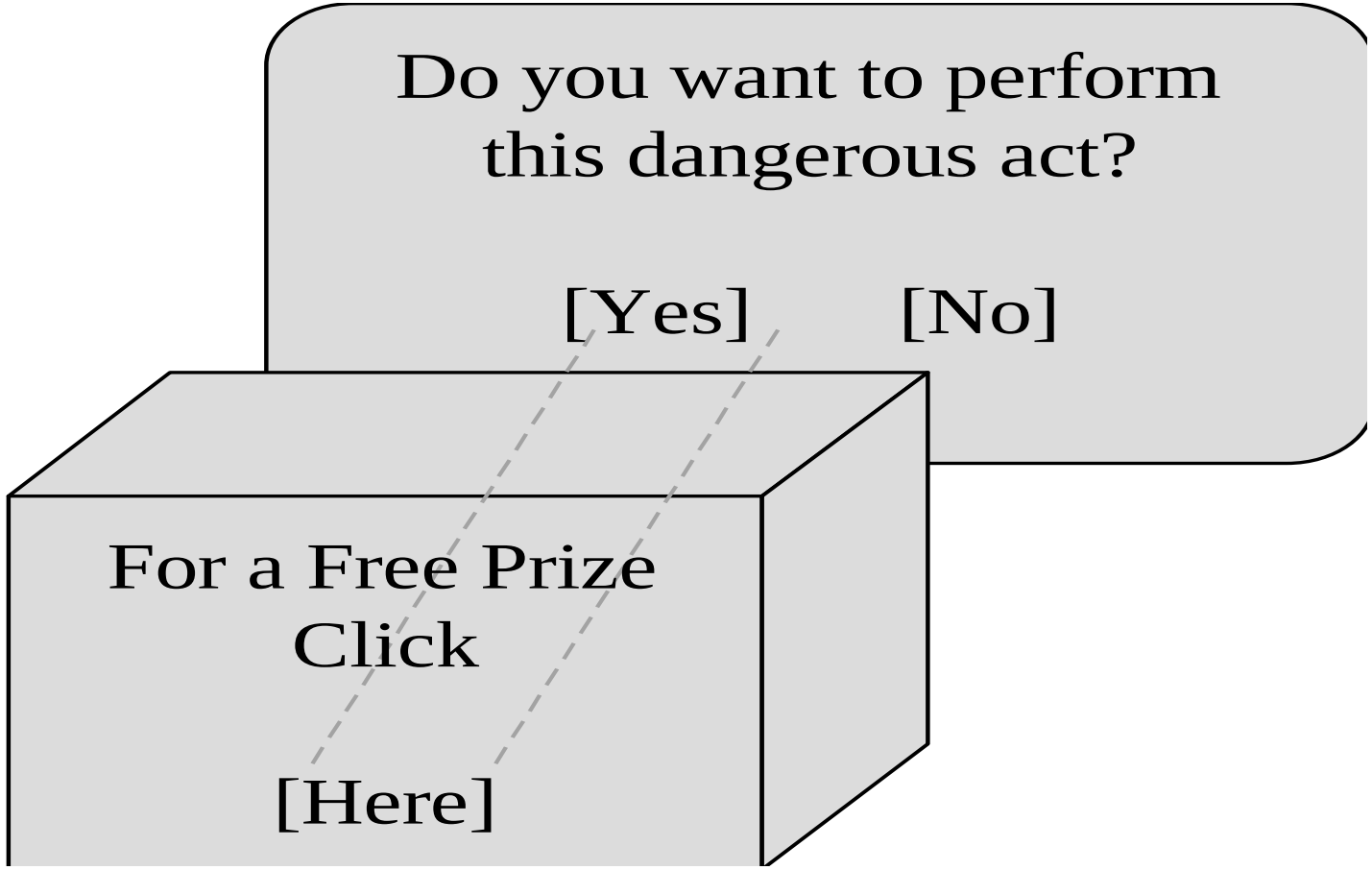
- Tiny action points called web bugs can report page traversal patterns to central collecting points, compromising privacy.
- When a remote file is fetched for inclusion, the request also sends the IP address of the requester, the type of browser, and the content of any cookies stored for the requested site.
- These cookies permit the page to display a notice such as “Welcome back, Elaine,” bring up content from your last visit, or redirect you to a particular web page.
- Is a web bug malicious? Probably not, although some people would claim that the unannounced tracking is a harmful invasion of privacy.

Tracking Bug



Clickjacking

Clickjacking: Tricking a user into clicking a link by disguising what the link points to



Drive-By Download

- Code is downloaded, installed, and executed on a computer without the user's knowledge
- May be the result of clickjacking, fake code, program download substitution, etc.
- Drive-by download: downloading and installing code other than what a user expects

Protecting Against Malicious Web Pages

- The basic protection against malicious web content is access control.
- In some way we want to prevent the malicious content from becoming established or executed.
- Access control accomplishes **separation.**
- Users download code to add new applications, update old ones, or improve execution.
- Although some operating systems require administrative privilege to install programs, that practice is not universal.
- And some naïve users run in administrative mode all the time.

Protecting Against Malicious Web Pages

- The other control is a responsibility of the web page owner: Ensure that code on a web page is good, clean, or suitable.
- good (secure, safe) code is hard to define and enforce.
- User vigilance can reduce the likelihood of accepting downloads of such code, and careful access control can reduce the harm if malicious code does arrive.
- But planning and preparedness for after-the-infection recovery is also a necessary strategy.