Web Attacks and Security

Classroom Code:o7l60yk

Outline

- Browser Attacks
- Web Attacks Targeting Users
- Email Attacks
- Demonstrations (Demo) of Attacks

Browser Attacks

Man-in-the-Browser:

- A **man-in-the-browser** attack is an example of malicious code that has infected a browser.
- Code inserted into the browser can read, copy, and redistribute anything the user enters in a browser.
- The threat here is that the attacker will intercept and reuse credentials to access financial accounts and other sensitive data.

Browser Attacks

Man-in-the-Browser:

- A **man-in-the-browser** attack is an example of malicious code that has infected a browser.
- Code inserted into the browser can read, copy, and redistribute anything the user enters in a browser.
- The threat here is that the attacker will intercept and reuse credentials to access financial accounts and other sensitive data.

Browser Attacks: Man-in-the-Browser

Man-in-the-browser example: Trojan horse that intercepts data passing through the browser.

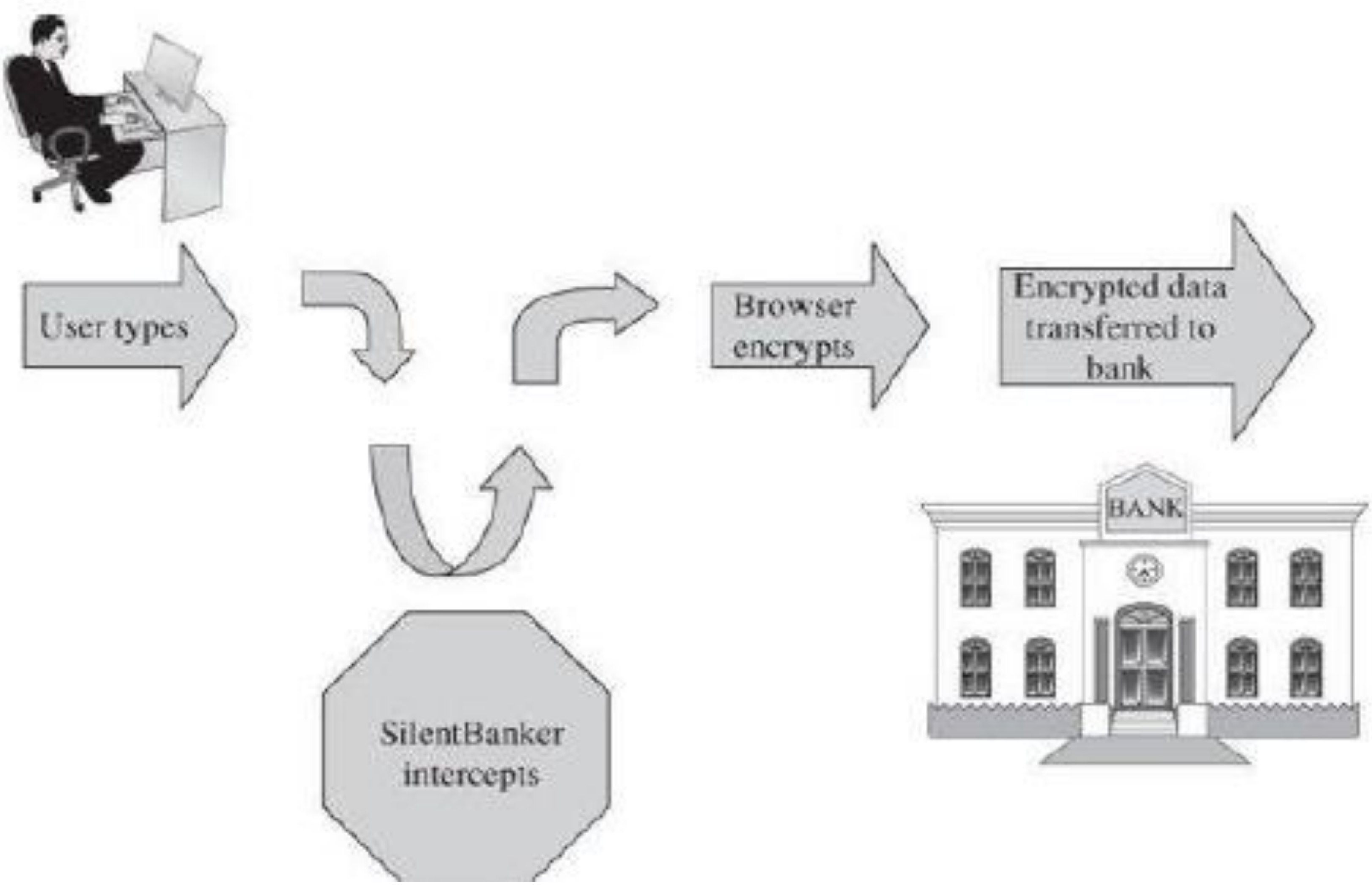
- In January 2008, a new Trojan horse is detected and named as SilentBanker. This code linked to a victim's browser as an add-on or browser helper object; in some versions it listed itself as a plug-in to display video.
- As a helper object, it set itself to intercept internal browser calls, including those to:
- receive data from the keyboard, send data to a URL,
- generate or import a cryptographic key,
- read a file (including display that file on the screen),
- or connect to a site; i.e. everything a browser does.

Browser Attacks: Man-in-the-Browser

Man-in-the-browser example: SilentBanker

- SilentBanker started with a list of over 400 URLs of popular banks throughout the world.
- Whenever it saw a user going to one of those sites, it redirected the user's keystrokes through the Trojan horse.
- These recorded customer details that it forwarded to remote computers.
- **CRYPTOGRAPHY/ ENCRYPTION??**

SilentBanker



User types

Browser encrypts

Encrypted data transferred to bank

SilentBanker intercepts

Browser Attacks

- If intercepting details such as name, account number, and authentication data were not enough.
- SilentBanker is also capable to change the effect of customer actions.
- For example : if a customer instructed the bank to transfer money to an account at bank A, SilentBanker converted that request to make the transfer go to its own account at bank B, which the customer's bank duly accepted as if it had come from the customer.
- When the bank returned its confirmation, SilentBanker changed the details before displaying them on the screen. Thus, the customer found out about the switch only after the funds failed to show up at bank A as expected.

Other Browser Attacks on users

- **Keystroke Logger:** A **keystroke logger** (or **key logger**) is either hardware or software that records all keystrokes entered.
- **Page-in-the-middle:** A **page-in-the-middle** attack is another type of browser attack in which a user is redirected to another page.
- **Program Download Substitution:** Coupled with a page-in-the-middle attack is a download substitution. In a **download substitution**, the attacker presents a page with a desirable and seemingly innocuous program for the user to download, for example, a browser toolbar or a photo organizer utility.
- **User-in-the-middle:** Taking unwilling help of independent and innocent users by spammer to solve CAPTCHA. How? n Why?

Web Attacks beyond User Side

- **Cross Site Scripting (XSS): Injecting Script from server side.**
- **Session Hijacking: it can be done at network level.**
- **Other Attacks at network level like Wiretapping.**

XSS

- The introduction of scripting languages allowed webpages to become more dynamic.
- Server-side scripting languages such as PHP and ASP enabled web developers to interact with resources that reside on the server such as files and databases.
- Client-side scripting languages, e.g. JavaScript, execute in the user's web browser and provide similar functionality on the client computer.
- As with anything else in computing and networking, the addition of more capabilities raised a security concern.

XSS

- XSS attacks are essentially code injection attacks into the various interpreters in the browser.
- These attacks can be carried out using HTML, JavaScript, VBScript, ActiveX, Flash, and other client-side languages.
- These attacks also have the ability to gather data from account hijacking, changing of user settings, cookie theft/poisoning, or false advertising is possible.

XSS Types

- **Type 0:** The first type of XSS vulnerability is also known as local or DOM-based XSS.
- This exists in the client-side script which resides in the code for a particular website. JavaScript code often uses objects which are provided by the browser as part of the Document Object Model (DOM). Examples of such objects include "document.URL" and "document.location."
- If such a script uses these document objects to write HTML code to the page without properly encoding the HTML entities, a vulnerability may be present.
- This is because the output of the script is then reinterpreted by the browser, and the contents could include an additional client-side script

XSS Types

- Type 1: The next type of vulnerability is the most common type of XSS vulnerability.
- It is sometimes referred to as a reflected or non-persistent vulnerability.
- This occurs when data provided by a web client is immediately used by scripts on the server to generate results which are displayed to the user, as is commonly seen with search engines.
- If the user-supplied data is not validated, some of the results could include a client-side script that is executed in the browser instead of HTML

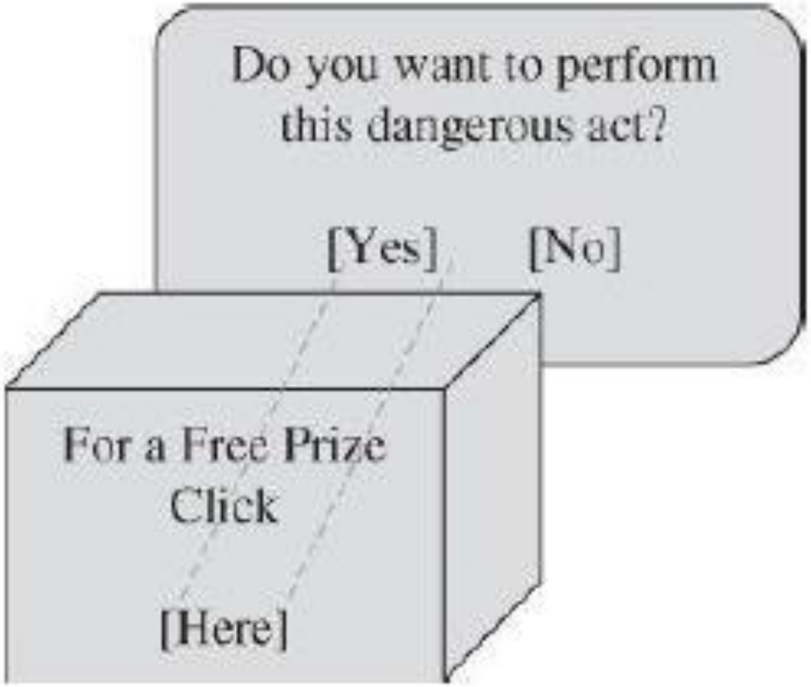
XSS Types

- Type 2: The last type of vulnerability allows the most powerful attacks, though these attacks may arguably be the easiest to deploy.
- Known as the persistent, stored, or second-order XSS vulnerability, it occurs when user-provided data is stored on a web server and then later displayed to other users without being encoded using HTML entities.
- This can be found on message boards or online social networking sites, where users are allowed to post HTML-formatted messages for others to see.

Web Attacks Targeting Users

Web Content:

- False/ Misleading Content
- Defaced Web Site
- Malicious Web Content
  - Clickjacking
  - Drive-By Download
  - Substitute Content on a Real Web Site (link to fake executable of popular tools).



Email Attacks

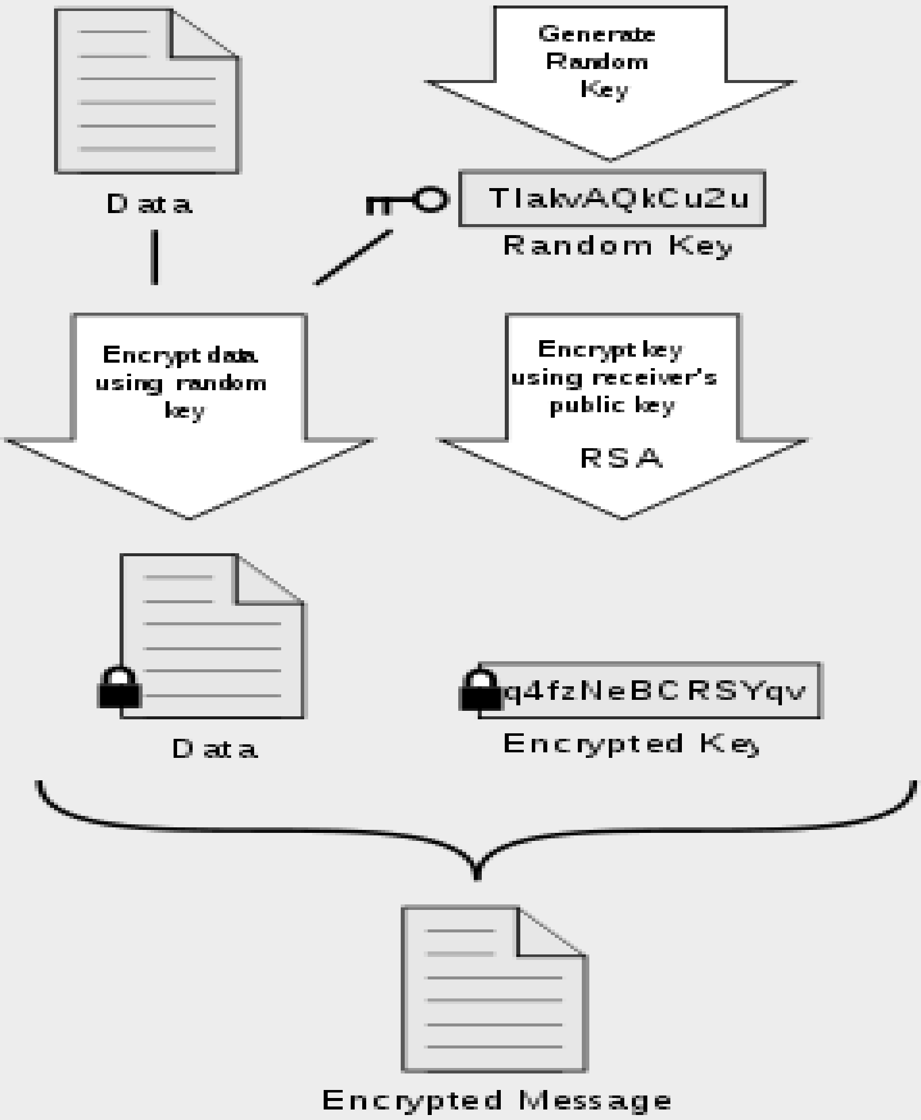
Fake Email

- Fake email messages as spam
  - Advertising
  - Pump and Dump
  - Phishing

Protection against email attacks

- **Pretty Good Privacy (PGP):** is an encryption program that provides cryptographic privacy and authentication for data communication.
- PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications
- **S/MIME:** An Internet standard governs how email is sent and received. The general MIME specification defines the format and handling of email attachments. **S/MIME** (Secure Multipurpose Internet Mail Extensions) is the Internet standard for secure email attachments.

Encrypt



Data

Generate Random Key

TlakvAQkCu2u

Random Key

Encrypt data using random key

Encrypt key using receiver's public key

RSA

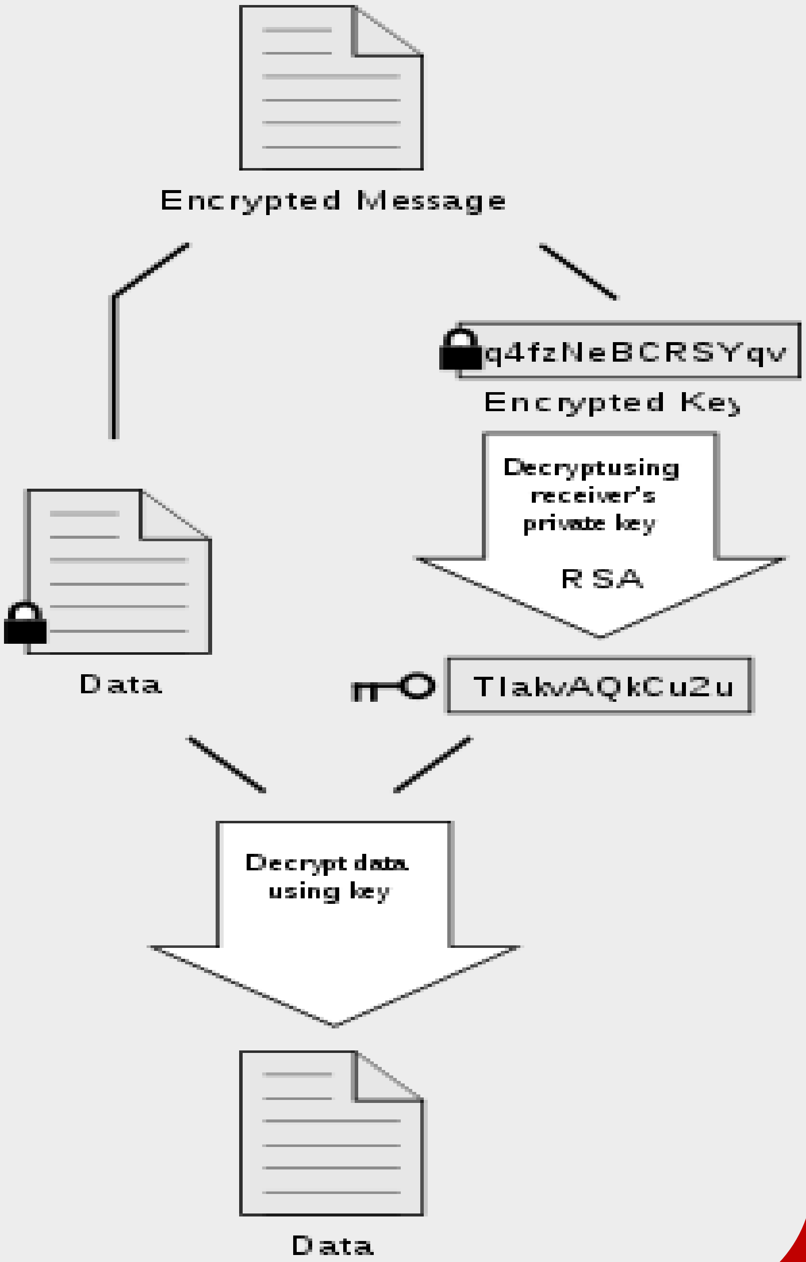
Data

q4fzNeBCRSYqv

Encrypted Key

Encrypted Message

Decrypt



Encrypted Message

q4fzNeBCRSYqv

Encrypted Key

Decryptusing receiver's private key

RSA

Data

TlakvAQkCu2u

Decrypt data using key

Data

Attack Demo Time

https://www.google.com/intl/am_AD/about/appsecurity/learning/xss/

Thank you, for your time and attention!

The LNMIIT: Where young dreams take shape …..