Intrusion Detection, Mobile Code

Prepared By : Yousef Aburabie
Supervised By : Dr. Lo'ai Tawalbeh

New York Institute of Technology (NYIT),
Amman's campus-2006

Outline of Presentation

- Defining Mobile Code
- Mobile Code Paradigms
- Types of Mobile Code
- Problems with Mobile Code
- Technologies to solve the Problems
- Summery

What is Mobile Code

- **What is Code ?**

  Code is a series of commands, and (usually) contains no or little information.

  Examples: Programs, applications, operating systems, games and viruses.

What is Mobile Code

- **What is mobility ?**

  Mobility in general is the ability and willingness to move or change.

  Data mobility : as we use the internet to download, read, send, receive information to others. Data has been mobilized.

What is Mobile Code

- **Now，What is Mobile Code ?**
  - "Mobile Code" is code sourced from remote, possibly "untrusted" systems, but executed on your local system.
  - Mobile code is the term used to describe general-purpose executables that run in remote locations.
  - In almost all situations, the user is not aware that mobile code is downloading and executing in their workstation
- **Malicious mobile code** is mobile code that makes your system do something that you do not want it to do .

What is Mobile Code (Cont'd..)

- Mobile code can also download and execute in the client workstation via email. It can be downloaded via an email attachment or via an HTML email body (e.g., JavaScript). For example, the ILOVEYOU, TRUELOVE, viruses/worms all were implemented as mobile code.
- The Concept is not new ,so what is the new !!

- What's new and revolutionary about the current uses of mobile code is that web browsers now come with the ability to execute general-purpose executables.

Mobile Code Examples

- Examples of mobile code include :
  - Scripts (JavaScript, VBScript)
  - ActiveX controls
  - Dynamic e-mail
  - Viruses, Trojan horses, worms

Mobile Code Examples

ActiveX controls

- A software component based on Microsoft's ActiveX technology that is used to add interactivity and more functionality, such as animation or a popup menu, to a Web page. An ActiveX control can be written in any of a number of languages, including Java, C++, and Visual Basic.

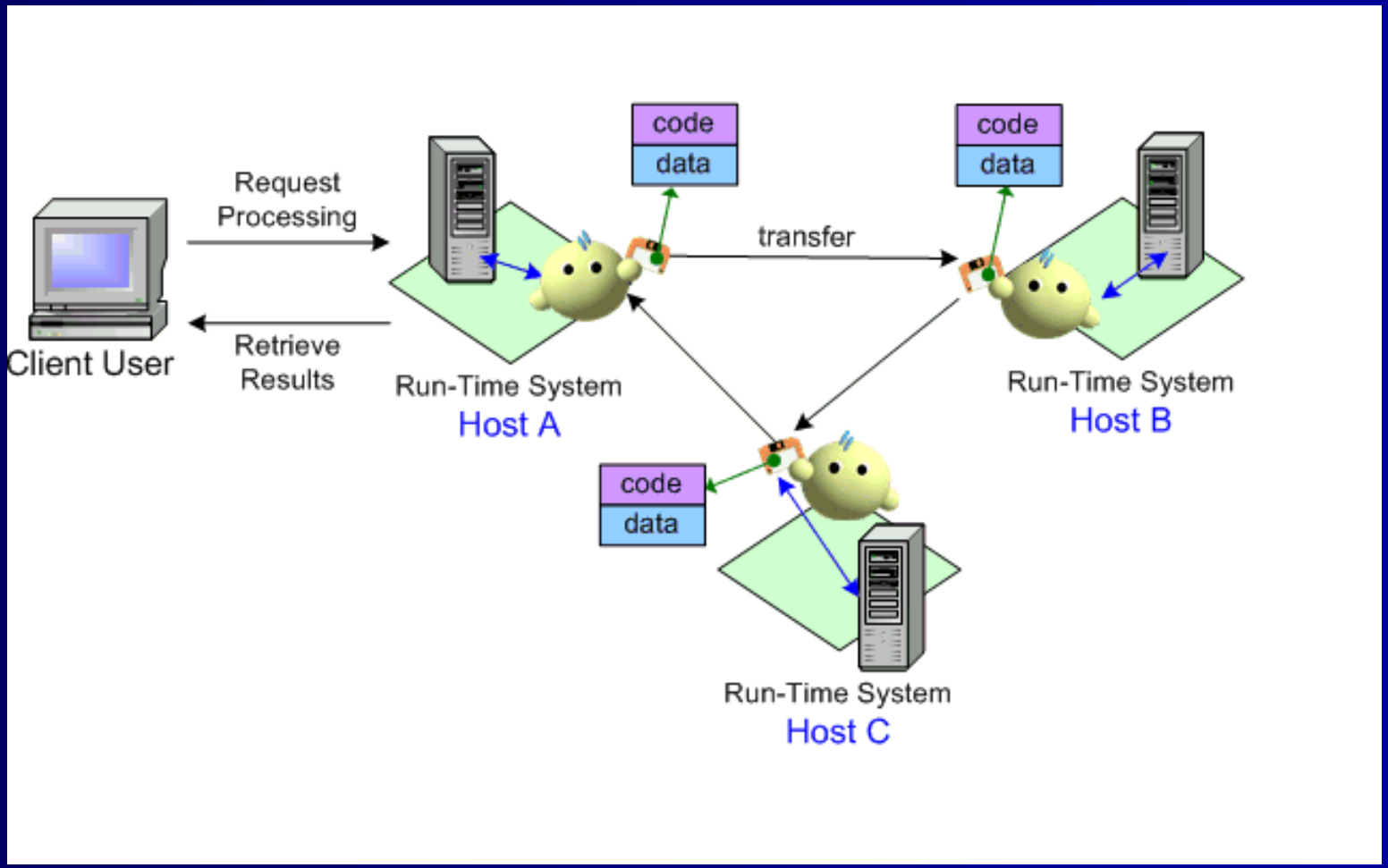
Mobile Code Paradigms

- **Mobile code technologies can be used to support three different paradigms :**
  - Mobile Agents
  - Code on Demand
  - Remote Evaluation

Mobile Code Paradigms

- **Mobile Agents :**
  - Mobile agent is a composition of computer software and data which is able to move from one computer to another autonomously and continue its execution on the destination computer .
  - When the term mobile agent is used, it refers to a process that can transport its state from one environment to another, with its data intact, and still being able to perform appropriately in the new environment.

Mobile Code Paradigms (Mobile Agent)



Mobile Code Paradigms (Mobile Agent)

- **Some advantages of mobile agents :**
  - Move computation to data, reducing network load.
  - Asynchronous execution on multiple heterogeneous network hosts (no synchronization between the connection and the computation)
  - Dynamic adaptation - actions are dependent on the state of the host environment

    For example, if the host signals shutdown, the agent can pick up and go to another host to continue its work. Groups of agents can distribute themselves among hosts to achieve maximum efficiency.
  - Tolerant to network faults – if something is going wrong at one location, they have a chance to escape and continue at another .

Mobile Code Paradigms

- **Code on demand :**

Code on demand is a general term for any technology that sends executable software programs from a server computer to a client computer upon request from the client's software.

Code on demand is a specific use of mobile code. A well-known example for the code on demand paradigm are java applets : An applet's program code lies inactive on some web server until a user (client) requests a web page that contains a link to the applet using his web browser. Upon this request, the web page and the applet are transported to the user's machine using HTTP. When the page is displayed, the applet is started in the browser and executes locally, inside the user's computer until it is stopped (e.g. by the user leaving the applet's web page).

Mobile Code Paradigms

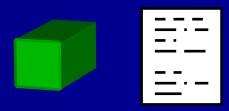
- **Remote Evaluation :**

  Remote evaluation is a general term for any technology that involves the transmission of executable software programs from a client computer to a server computer for subsequent execution at the server. After the program has terminated, the results of its execution are sent back to the client.

A Chocolate Cake Example

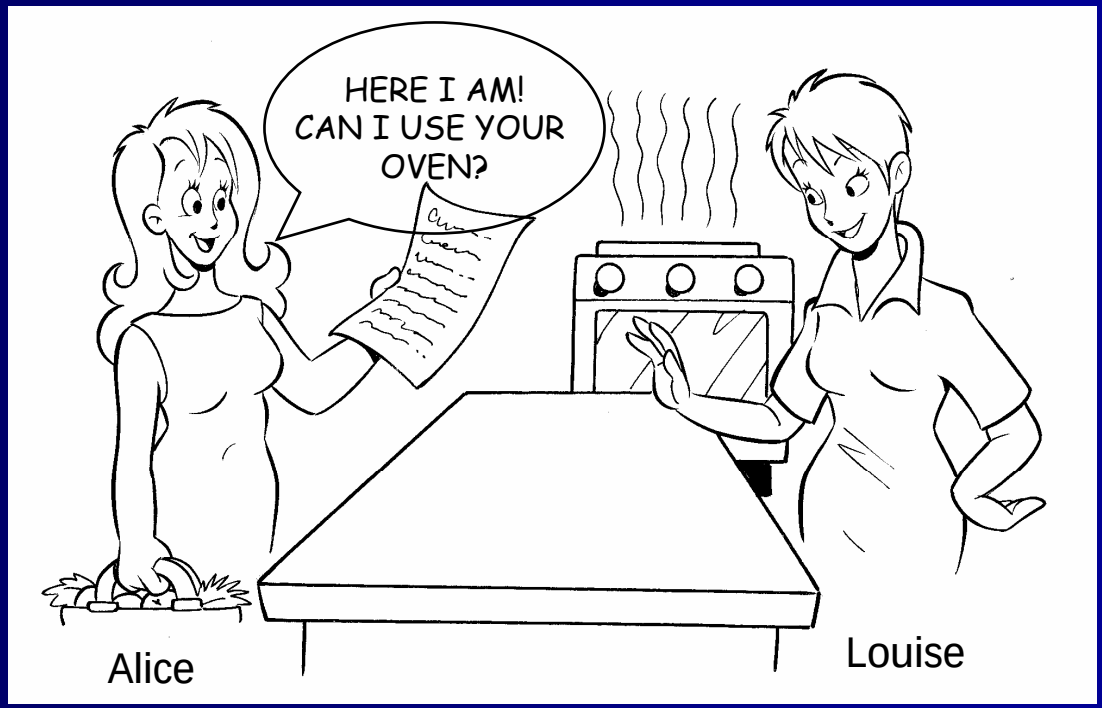
A Chocolate Cake Example

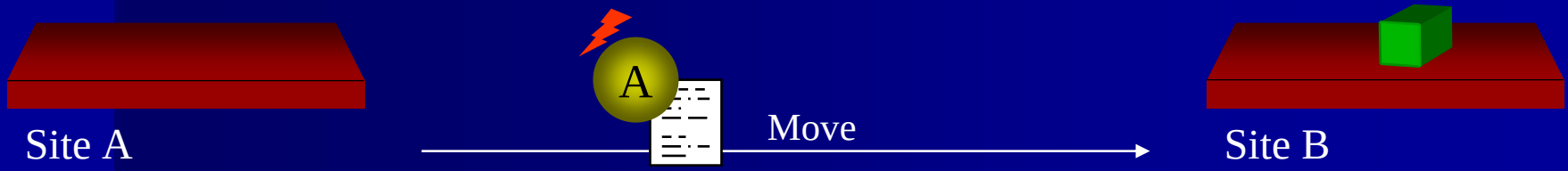
- *Components*
  - Resource components (Data, devices, code)
  - Computational components
    - Execution state
    - Private data
    - Bindings to other components (e.g., code)
- *Sites*
  - Support execution



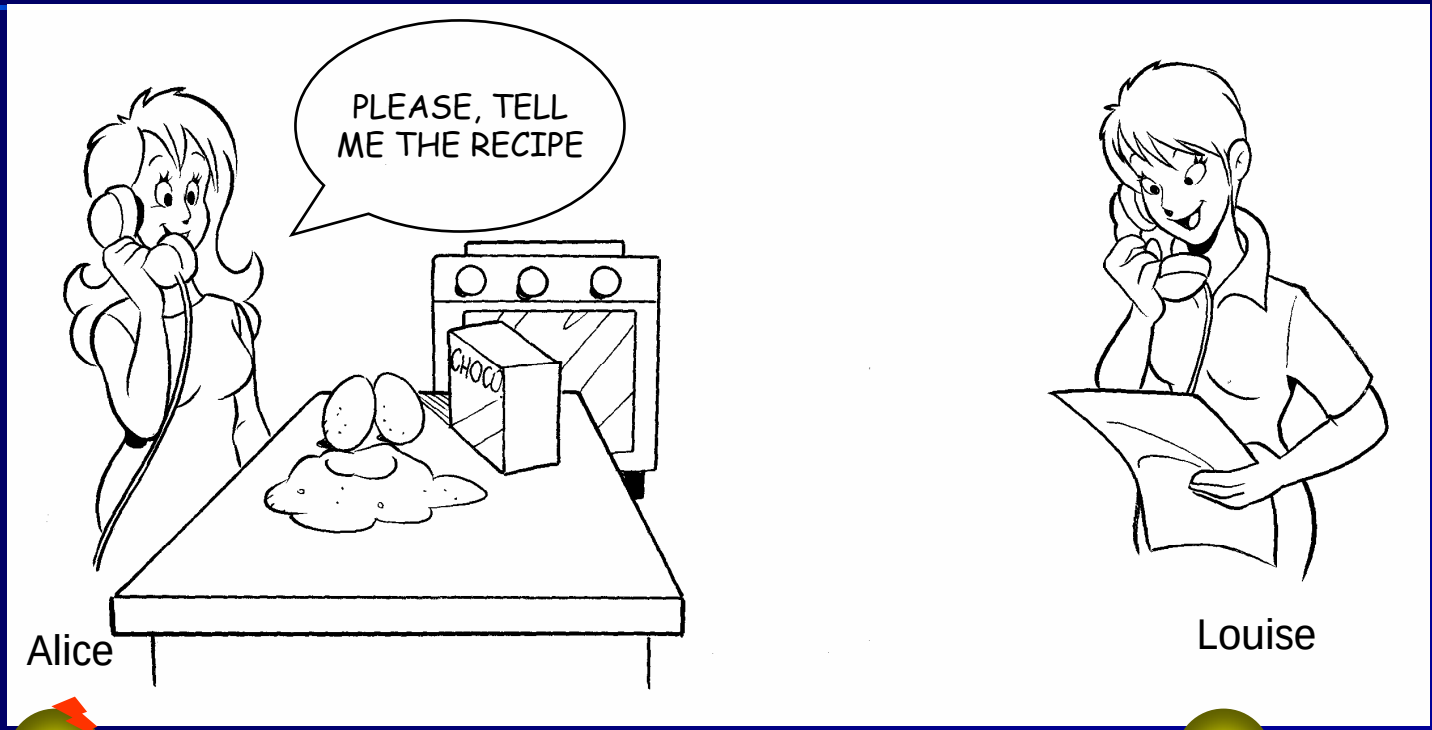
Site Y

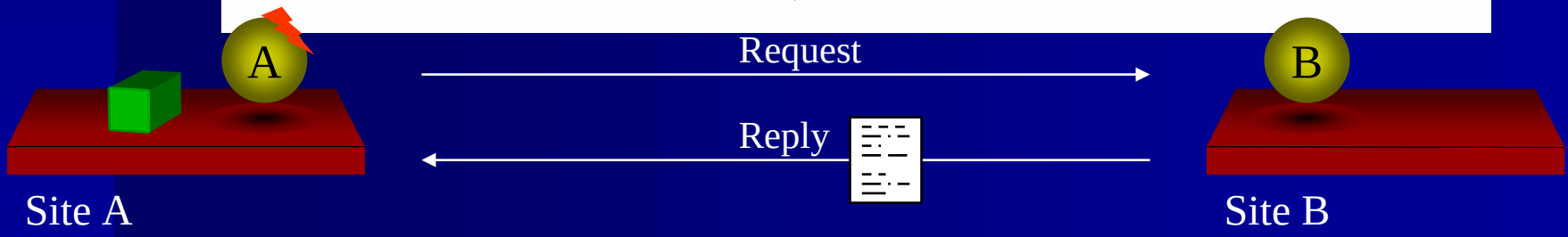
Mobile Agent



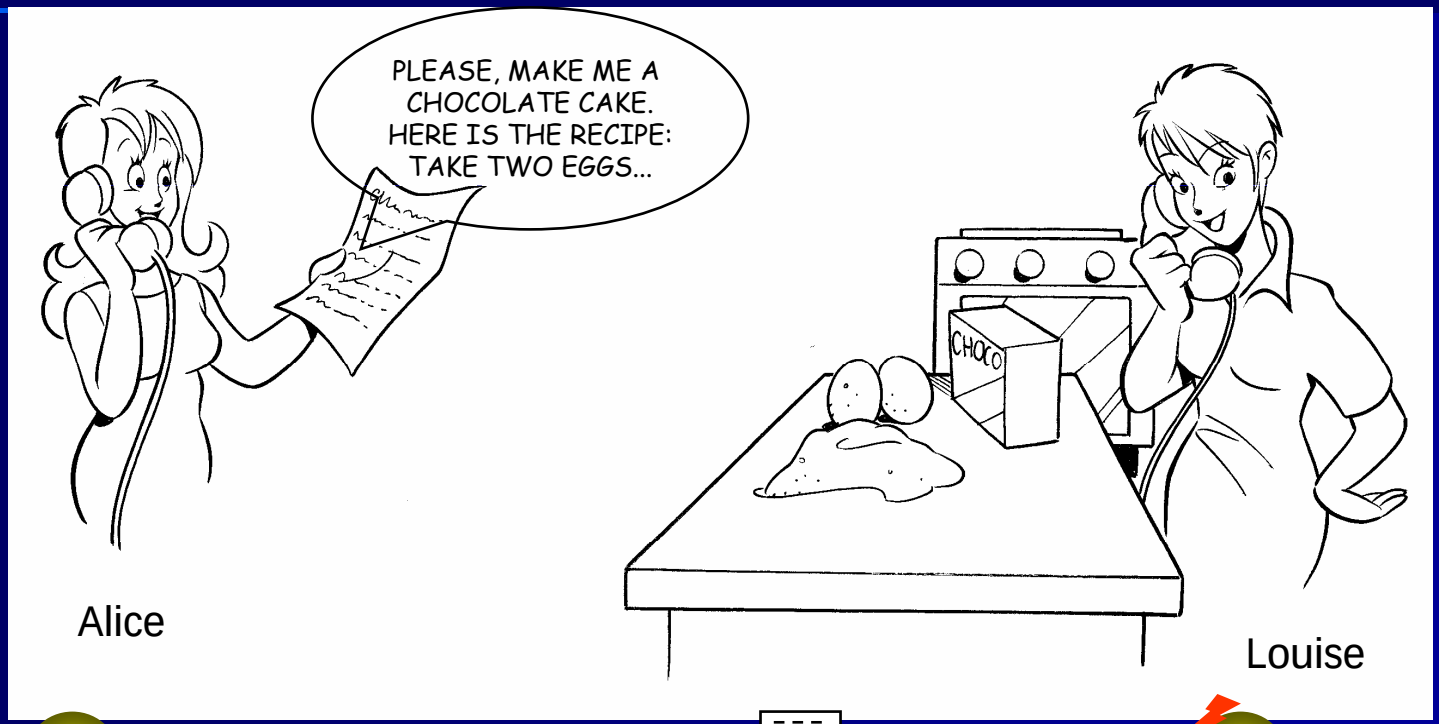


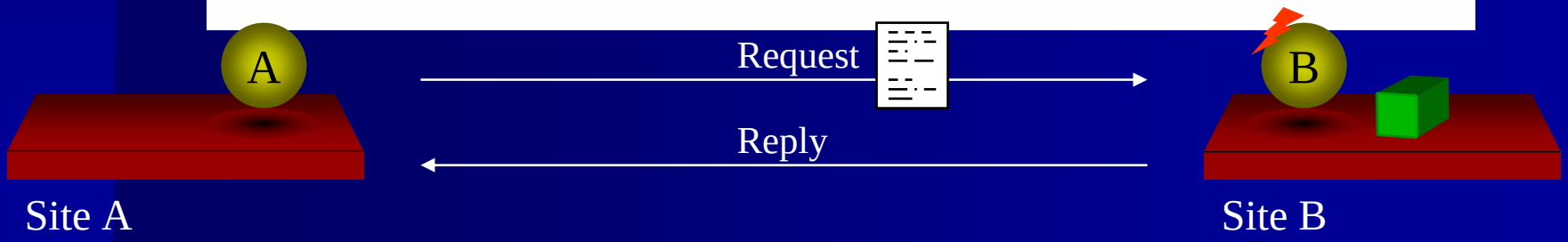
Code On Demand





Remote Evaluation





Types of Mobile Code

Types Of Mobile Code include :

- One-hop Agents (weak mobility)*, e.g.* Java applets.
  Sent on demand from a server to a client machine and executed. After execution, the agent's results or agent itself is returned to the agent owner that sent it.

- Multi-hop Agents (strong mobility) ,
  Sent out on the network to perform a series of tasks. .These agents may visit multiple agent platforms and communicate with other agents.

Problem with Mobile Code

- **The types of attacks which need to be guarded against include:**
  - denial of service
  - disclosure of confidential information
  - damage or modification of data
  - annoyance attacks

Problem with Mobile Code

- Mobile Code Security :
  - **Malicious Code Problem** (executing useful applets while protecting systems from malicious ones)

    We must protect a host from malicious mobile code
  - **Malicious Host Problem** (protect agents from malicious servers)

    Protect a mobile code from a malicious host

Techniques to prevent malicious code

- **Techniques to prevent malicious code :**
  - Code blocking approaches
  - Authentication through Code Signing
  - Sandboxing

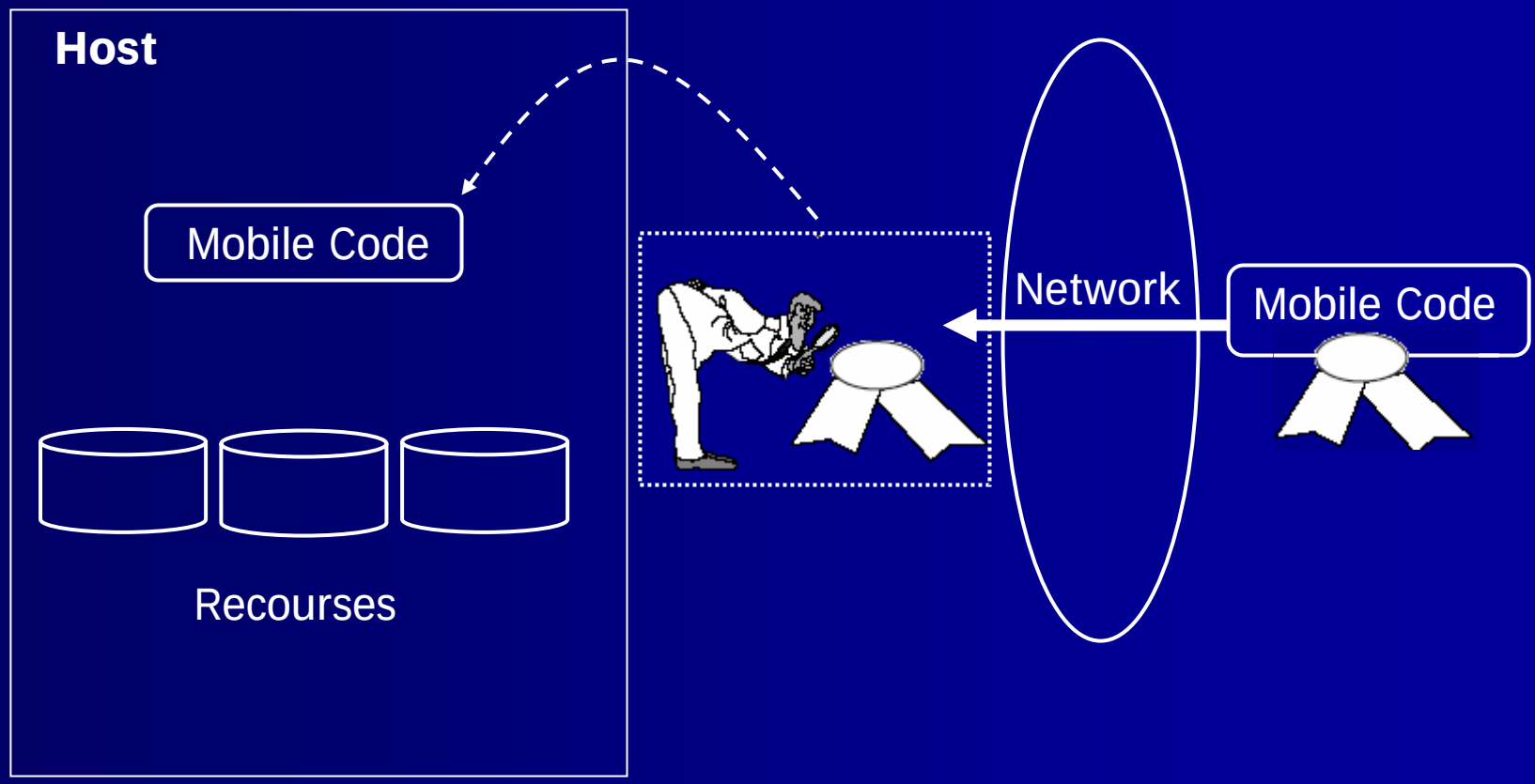
Techniques to prevent malicious code

- **Techniques to prevent malicious code :**
  - Code blocking approaches:
    - ✓ Disabling applications
      - o E. g. switching off Java in Java- enabled browsers.
      - o Relies on users complying with security policy.
    - ✓ Filtering
      - o E. g. firewalls to filter out Web pages containing applets.
      - o Useful functionality at many popular web sites is denied to users.

Techniques to prevent malicious code

- **Authentication through Code Signing**
  - Achieved through code signing
  - based on the assurance obtained when the source of the code is trusted on receiving the mobile code, client verifies whether it was signed by an entity on a trusted list
  - used in JDK 1.1 and Active X
  - once signature is verified, code has full privileges
  - Trusted third party can be used to allows developers to digital sign their code like Verisign

Techniques to prevent malicious code

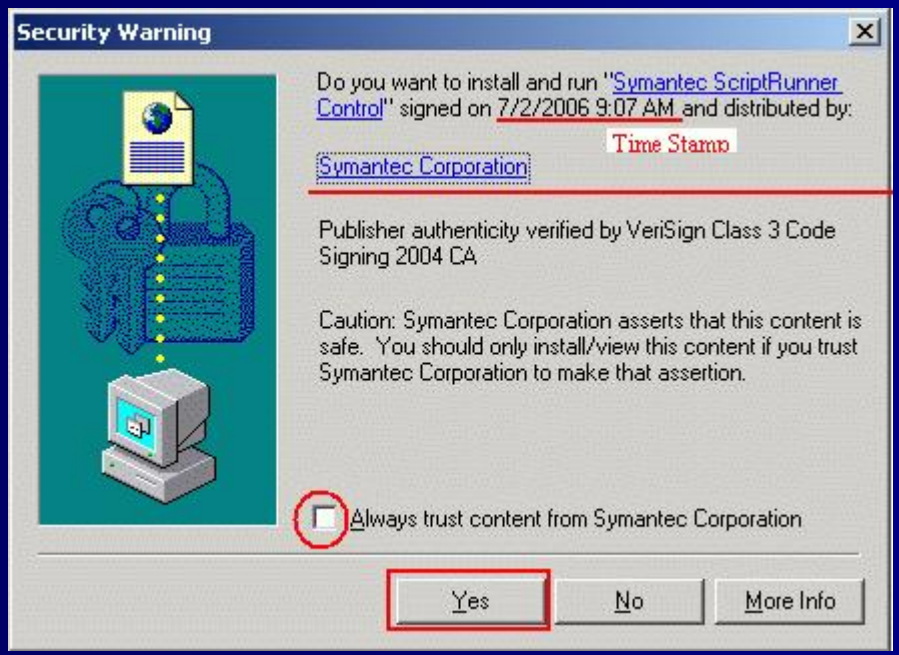


Code Signing

Techniques to prevent malicious code

- Problems
  - A signed code is either granted full access to the resources of the code consumer, or not executed at all. This choice is left to the end- user who, even without administrator privileges, can put the entire host security at risk.
  - Limits users (the untrusted code may be useful and benign)
  - No protection if the code from a trusted source is malicious

Techniques to prevent malicious code



Techniques to prevent malicious code

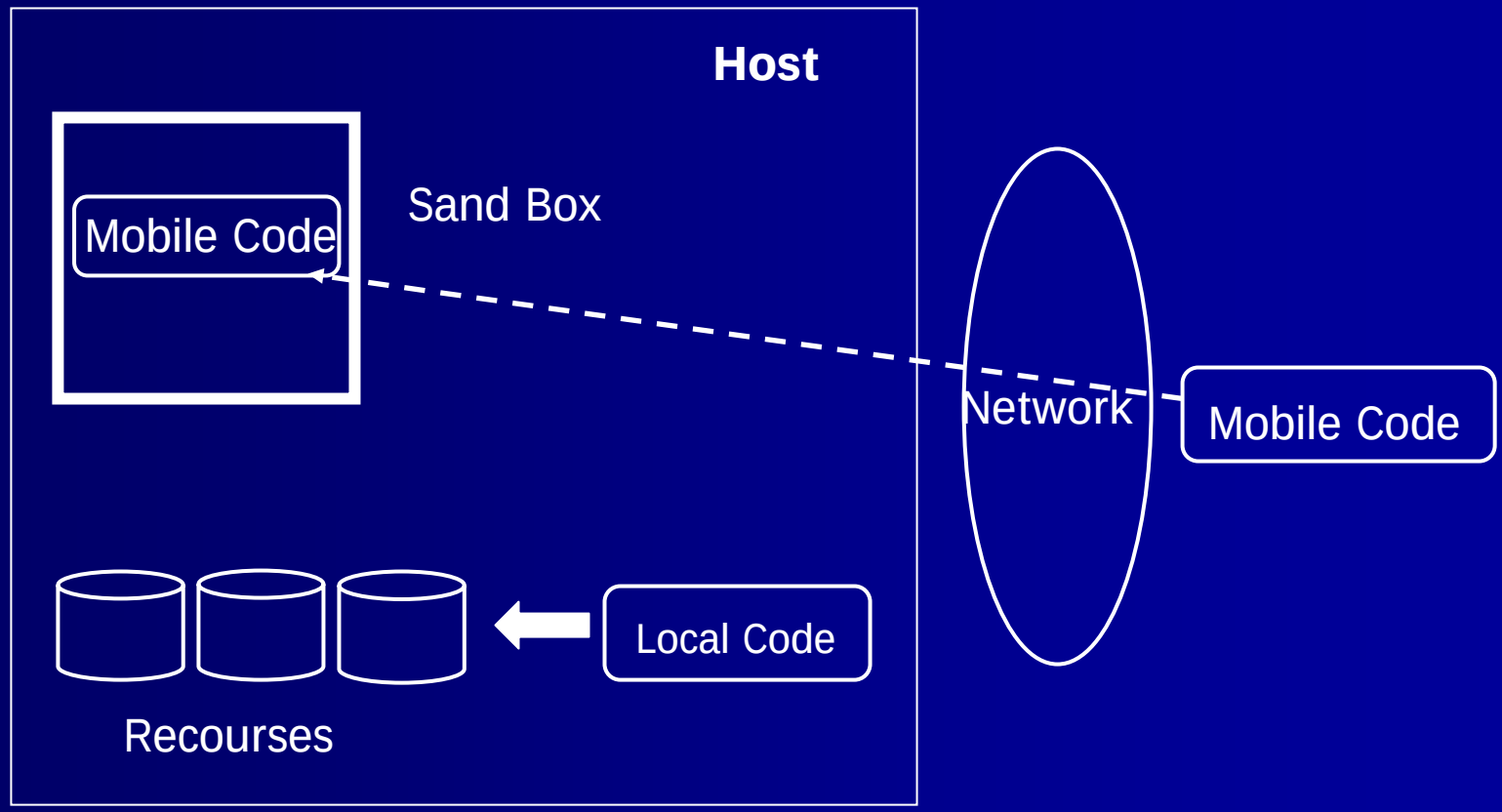
- **Sandboxing :**

Sandboxing consists in running a mobile code in a restricted environment called the “sandbox”.

It is often used to execute untested code, or programs from unverified third-parties, suppliers and untrusted users.

Network access, the ability to inspect the host system or read from input devices is usually disallowed or heavily restricted.

Techniques to prevent malicious code



Techniques to prevent malicious code

- Some examples of sandboxes are:
  - Virtual machines.
  - Jails are a special kind of resource limit imposed on programs by the operating system.

Protection From a Malicious Host

- **Malicious Host Problem:**

- The problem of protection from a malicious host has been studied only recently, and is intrinsically more difficult because the environment gets a total control over the mobile code (otherwise, host protection would not be possible!).

- When protecting a mobile code from a potentially malicious host, code mobility implies that the program will be run under total control of the host. This means the following threats:
  - spoofing through impersonation of code owner theft and secrecy
  - violation through unauthorized disclosure integrity
  - violation through subversion of code semantics

  To prevent all three cases, data segments as well as code semantics must be protected.

Protection From a Malicious Host

- **Data Protection**
  - The integrity of the data collected by a mobile agent might be protected using a cryptographic technique.

Summery

- Increased interest in mobile code technology.
- Mobile Code have advantages not only problems.
- Considerable progress in solving the malicious code problem.
- Research in solving the malicious host problem is still in its infancy.