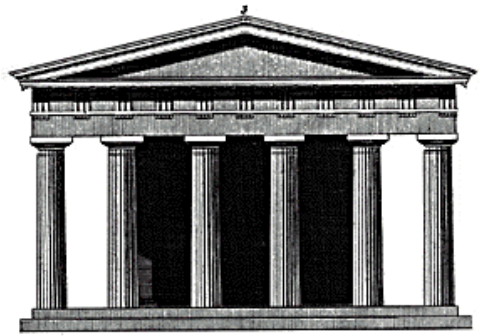
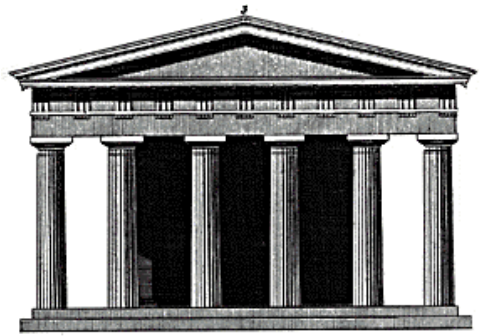
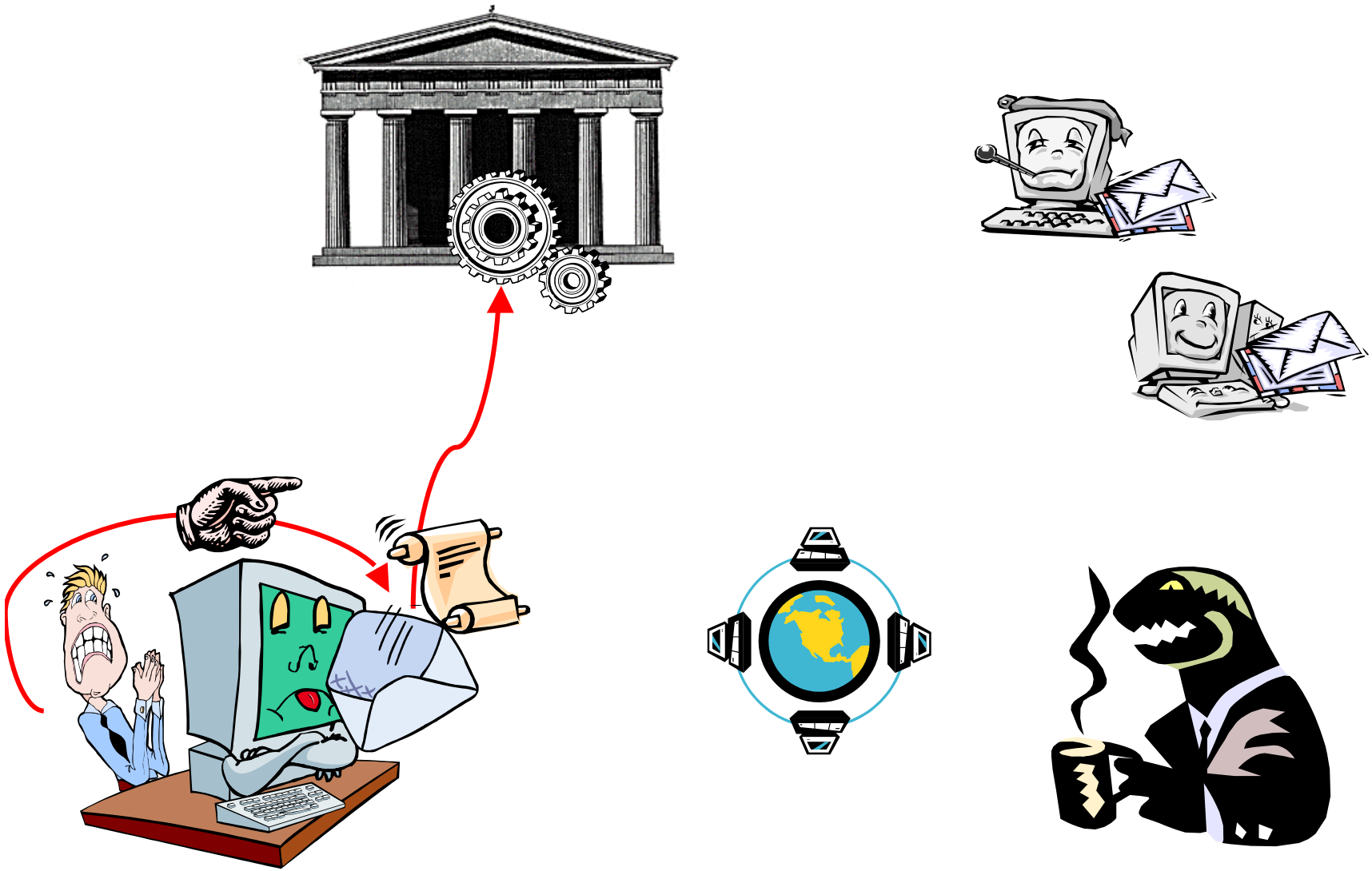
I (Server-Side) Cross-Site Scripting (1)



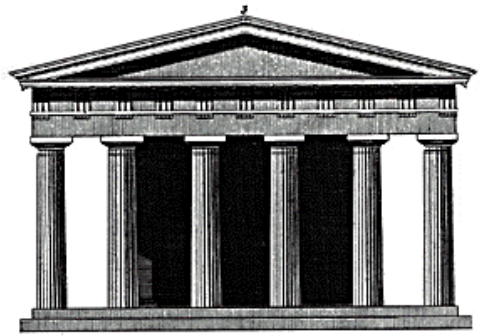
I (Server-Side) Cross-Site Scripting (2)



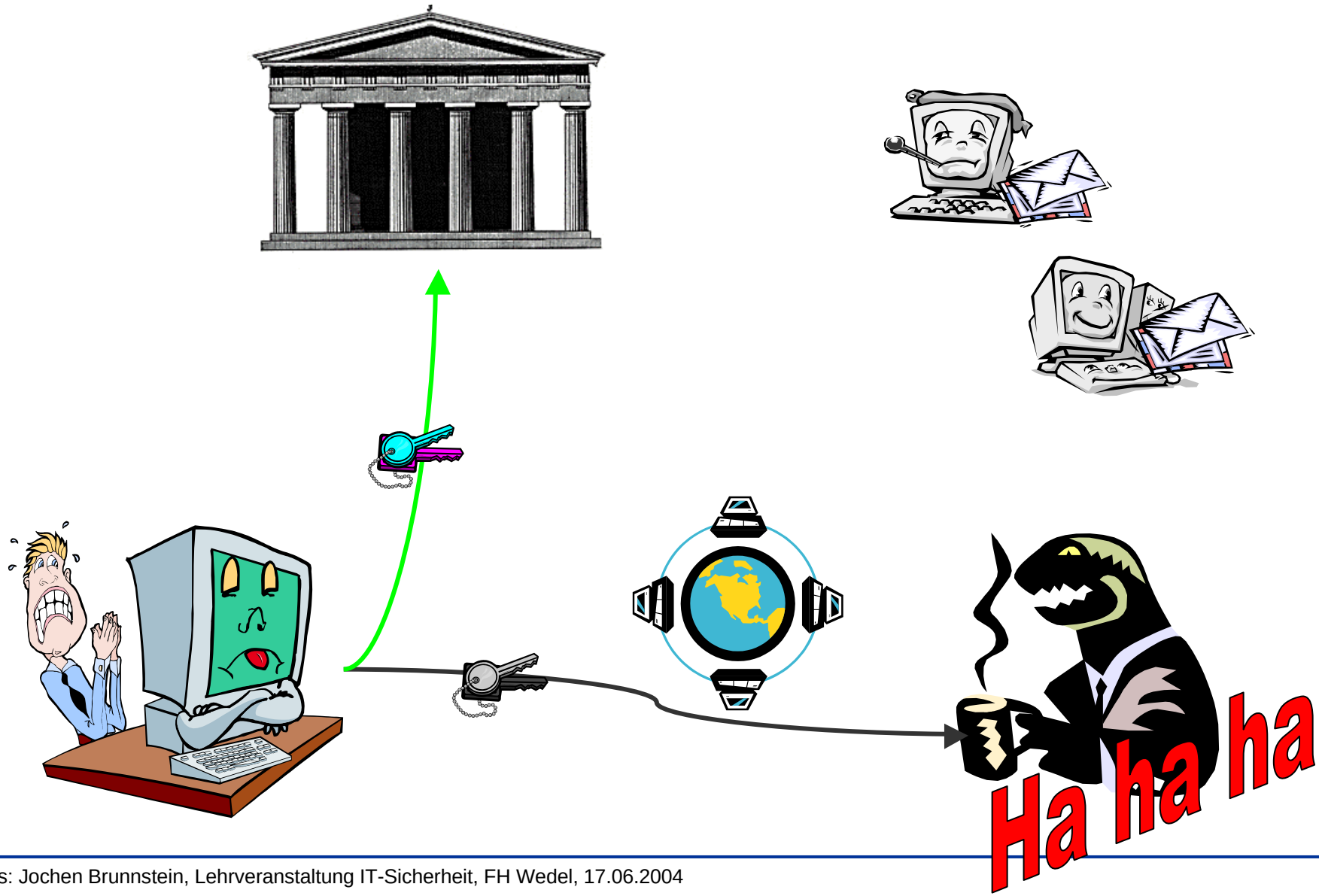
I (Server-Side) Cross-Site Scripting (3)



I (Server-Side) Cross-Site Scripting (4)



I (Server-Side) Cross-Site Scripting (5)



I (Server-Side) Cross-Site Scripting - Ablauf (1)

- **Benutzer klickt auf einen Link in eMail/ Web-Seite/ Posting**
  - Im Link ist böswilliger JavaScript-Code verborgen.
  - Der Link verweist auf eine vertrauenswürdige Site mit unsicherer Web-Seite.
- **Die Site:**
  - nimmt in der Web-Seite Benutzereingaben entgegen
  - prüft diese jedoch unzureichend gegen nicht ordnungsmäßige Daten, wie z.B.:
    - "**<script>alert('Test')</script>**" statt **<Login-Name>**
  - generiert dynamisch eine Antwort-Seite, welche die Benutzer-eingaben (bzw. das eingeschleuste Script) enthält
  - und sendet diese an den Benutzer zurück.

I (Server-Side) Cross-Site Scripting - Ablauf (2)

- **Typische Web-Seiten mit beschriebener Schwäche:**
  - Suchmaschinen, welche die eingegebenen Suchworte anzeigen
  - Fehlermeldungen, welche die fehlerhafte Zeichenkette enthalten
  - Formulare, deren Benutzereingaben nochmals angezeigt werden
  - Nachrichten in Web Message Boards oder Gästebüchern
- **Das Script wird auf dem Rechner des Benutzers ausgeführt, der die Web-Seite abruft und hat dort vollen Zugriff auf die darin enthaltenen Daten. Der Angreifer kann so z.B.:**
  - vertrauliche Informationen (Benutzername, Passwort) ablauschen
  - Cookies manipulieren oder stehlen
  - Anfragen für einen anderen Benutzer erzeugen
  - maliziösen Code auf dem Client ausführen