

The background is a light blue grid. There are several blue lines and circles: a vertical line on the left, a horizontal line across the top, a horizontal line across the middle, a vertical line on the right, and a horizontal line near the bottom. Small blue circles are placed at the intersections of these lines: one at the top-left, one at the bottom-right, and one at the intersection of the middle horizontal line and the left vertical line.

# Client-side security

# HTTP security extensions

## HSTS

- ◆ HTTP Strict-Transport-Security (**HSTS**) enforces secure (HTTP over SSL/TLS (see lecture 2)) connections to the server.
- ◆ This reduces impact of bugs in web applications leaking session data through cookies and external links and defends against Man-in-the-middle attacks.
- ◆ HSTS also disables the ability for user's to ignore SSL negotiation warnings.

# Cookie Security Policy

## ◆ Uses:

### ■ User authentication

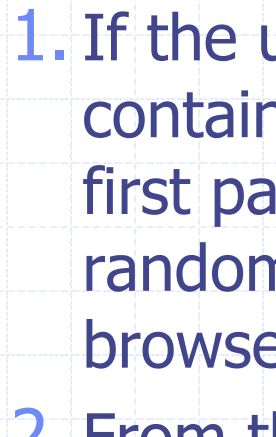
- A Commerce Server cookie contains information about a user visiting the site, such as :  
a logon ID, the date when the user last visited the site.
- Commerce Server uses cookies to identify and authenticate users, and to associate user IDs with the profile information it collects about them.

## ■ Personalization

- Personalization cookies allow the user to access the website with a series of default technical features, based on pre-established criteria on their computer, such as language, browser type, regional settings, etc.

## ■ User tracking

- ◆ Tracking cookies may be used to track internet users' web browsing. This can also be done in part by using the IP address of the computer requesting the page, but cookies allow for greater precision. This can be demonstrated as follows:

- 
1. If the user requests a page of the site, but the request contains no cookie, the server presumes that this is the first page visited by the user; the server creates a random string and sends it as a cookie back to the browser together with the requested page;
  2. From this point on, the cookie will automatically be sent by the browser to the server every time a new page from the site is requested; the server sends the page as usual, but also stores the URL of the requested page, the date/time of the request, and the cookie in a log file.
- ◆ By analyzing the log file collected in the process, it is then possible to find out which pages the user has visited, in what sequence, and for how long.