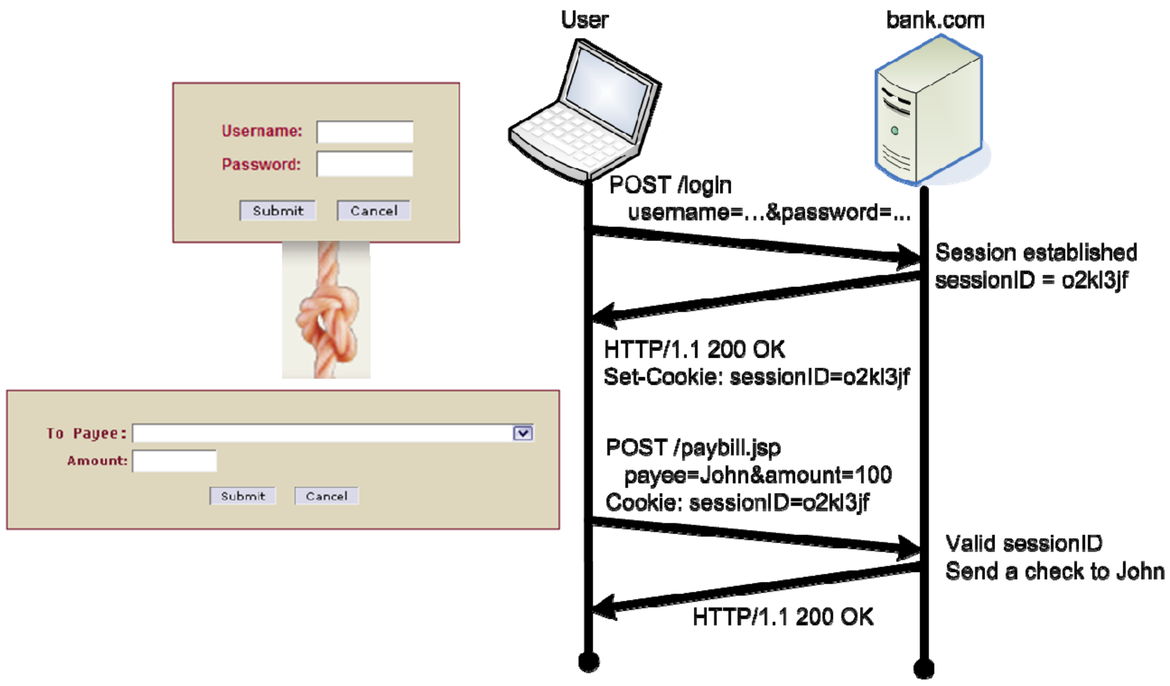
CERIAS

the center for education and research in information assurance and security

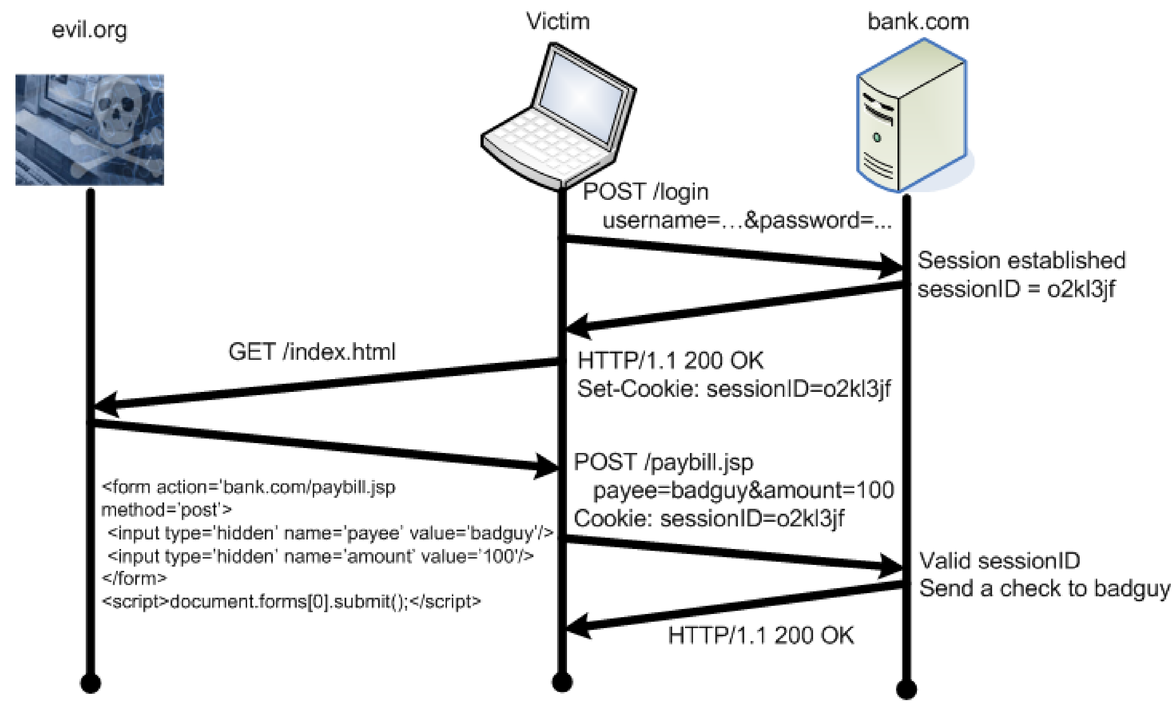
Defeating Cross-Site Request Forgery Attacks with Browser-Enforced Authenticity Protection

Ziqing Mao, Ninghui Li, Ian Molloy
CERIAS, Purdue University

Session maintenance on web



The CSRF attack



The weakness


Sends cookies if present


Authorizes the request if the cookie is valid


Direct the browser to send a request

A real threat

Gmail by Google BETA — Add a filter to forward emails

PURDUE UNIVERSITY — Delete web email; edit biography

PEFCU Purdue Employees Federal Credit Union — Transfer money; add accounts

- **Diagnosis**
  - No every request reflects the user's intention
  - Browser should NOT *always* attach auth tokens
- **Proposal**
  - *only intended requests carry auth tokens*
- **A Browser-Based Solution**
  - infer whether a request reflect the user's intention
  - infer whether an auth token is sensitive
  - strip sensitive tokens from unintended requests
- **Implementation**
  - A Firefox Extension available at mozilla.org

- **Design Details**
  - Infer the user's intention
    - User-interface actions
    - Ancestor web-pages
  - Infer the auth token's sensitivity

	GET		POST
	HTTP	***HTTPS***	Sensitive
Session	Not Sensitive	Sensitive	
Persistent	Not Sensitive		
HTTP Auth Header	Sensitive		

Paper published in Financial Crypto and Data Security 2009

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center