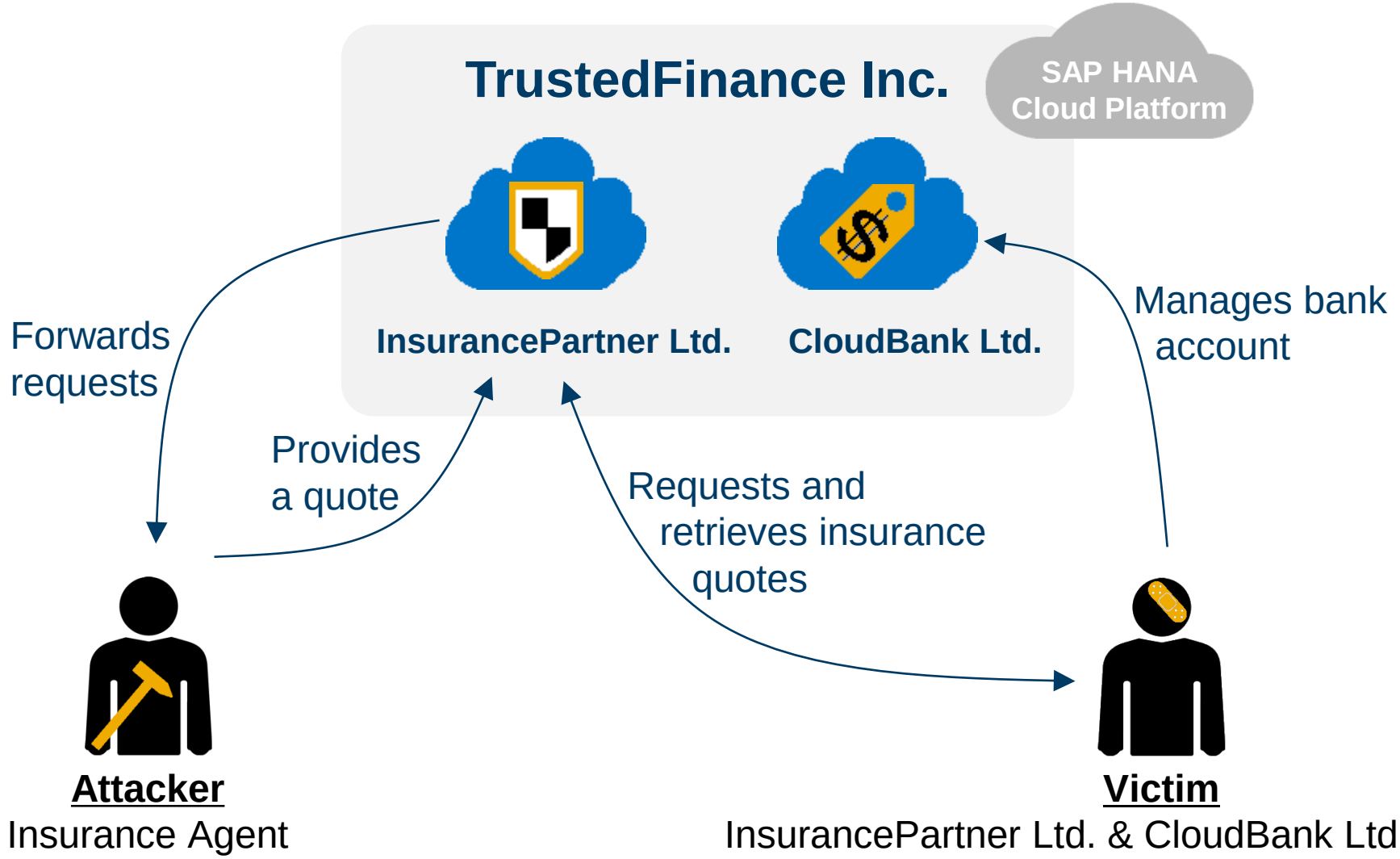
Week 3 Unit 2: **Protecting Against CSRF Attacks**

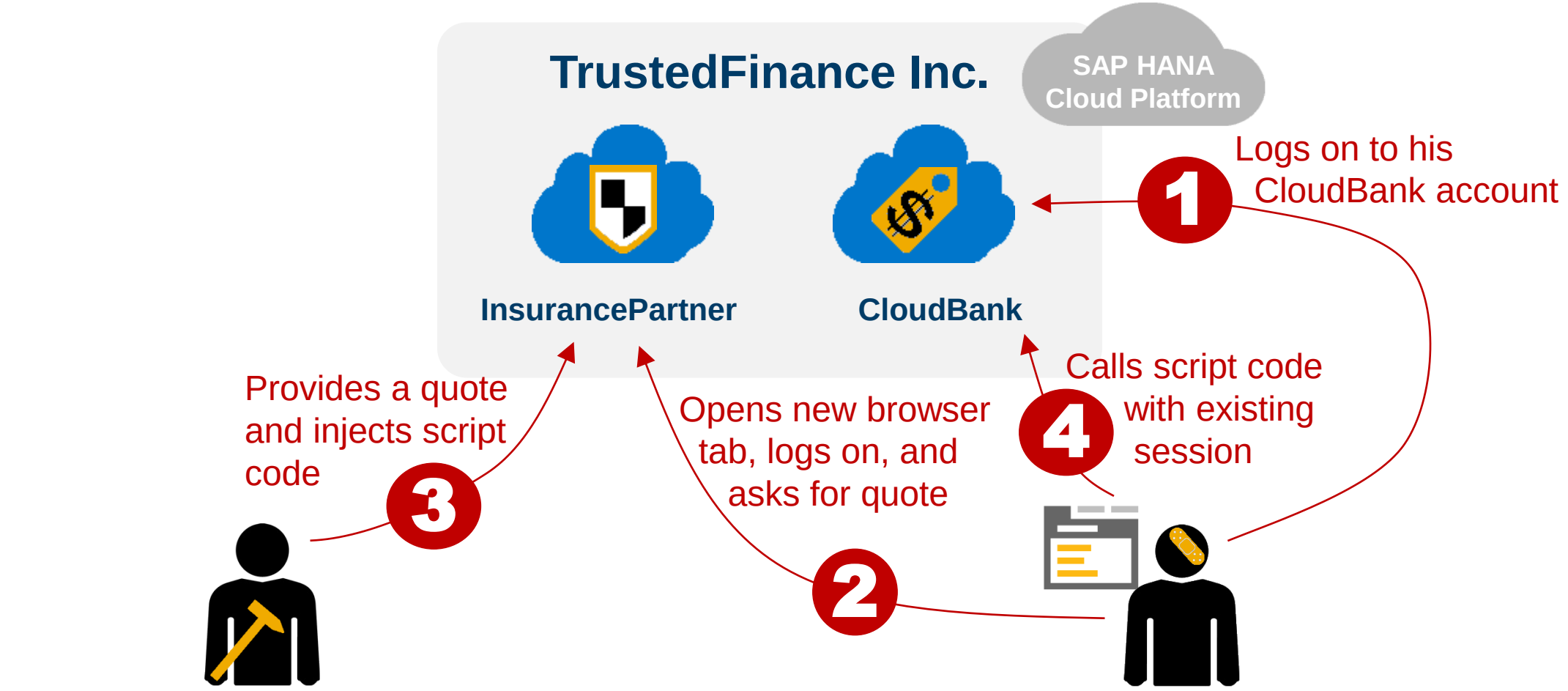
Protecting Against CSRF Attacks

A business scenario (1/2)



Protecting Against CSRF Attacks

A business scenario (2/2)



Protecting Against CSRF Attacks

Strategies to protect against CSRF attacks

- CSRF = cross-site request forgery
- Make your application's URLs unpredictable!
- Use randomly generated tokens with each request that are associated with the user's current session
- Use a CSRF filter provided by the HCP runtimes
  - Java: `org.apache.catalina.filters.RestCsrfPreventionFilter`
  - SAP HANA XS: `prevent_xsrf` keyword in `.xsaccess` file
  - HTML5: CSRF must be taken care of by the consumed (REST) services

Protecting Against CSRF Attacks

What you've learned in this unit

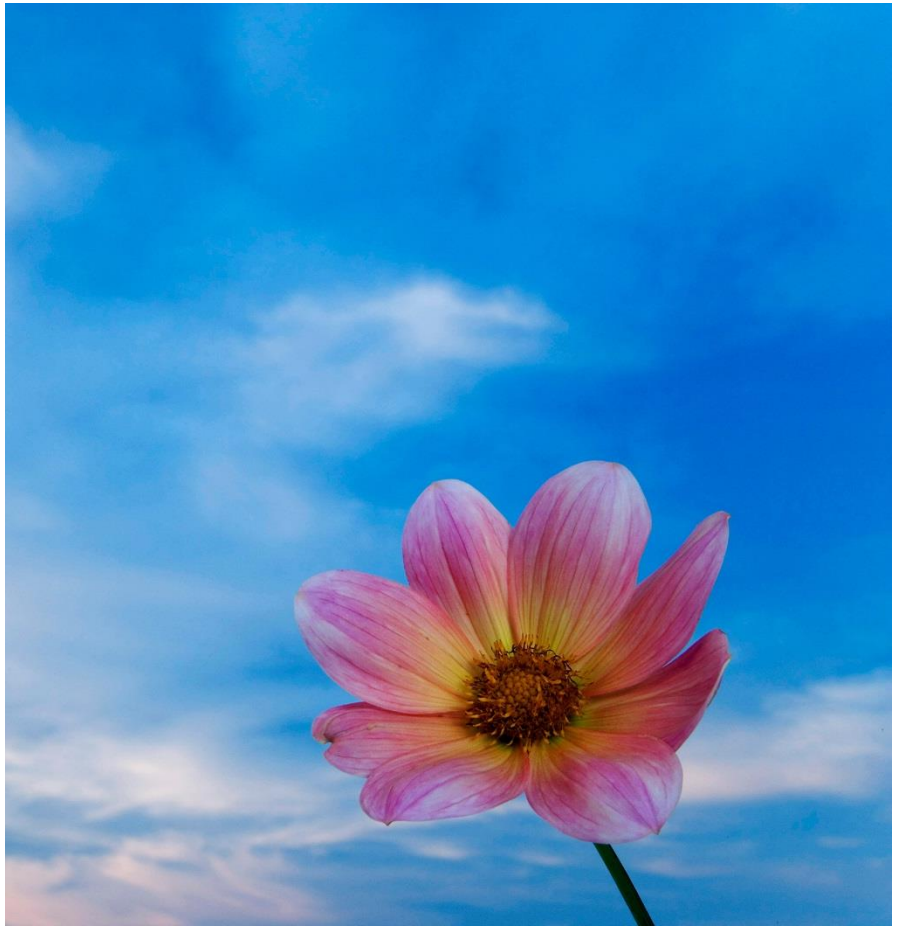
- CSRF is (still) a serious Web attack.
- Protection against it is YOUR responsibility.
- HCP offers a protection mechanism based on a token (a nonce value) generated on each request and stored in the session.

Protecting Against CSRF Attacks

Further reading

Additional Material

- Using the Apache Tomcat CSRF Prevention Filter: https://help.hana.ondemand.com/help/frameset.htm?e5be9994bb571014b575a785961062db.html



Thank you

Contact information:

open@sap.com

openSAP

© 2016 SAP SE or an SAP affiliate company. All rights reserved.