UISA: User Interface Security Assessment

Sarah Abdellahi and Heather Lipford, University of North Carolina at Charlotte
Carrie Gates and Jeremiah Fellows, Bank of America

UNC CHARLOTTE
College of Computing and Informatics

BANK OF AMERICA

What is UISA?

While organizations have independent, mature processes for evaluating the usability of their software as well as security threats and risks for their assets, methods at the intersection of these two concerns are still missing.

Design → User Behavior → Security

UISA is a method for designers and developers to use to **assess the security implications of a particular user interface design**, based on how users will interact, and in particular, behave in unexpected and unintended ways.

Why UISA?

- Help designers evaluate the security risks of a particular design or application
- Prioritize aspects of a design that may need improvement
- Compare different design ideas based on the potential impact on security
- Facilitate structured conversations between stakeholders with different concerns related to usability and security

Future of UISA

- Evaluation of UISA process with participants with different backgrounds to improve instructions and handbook
- Case studies with different enterprise applications and designs, to evaluate handbook completeness and UISA outcomes
- Expansion with a security risk metric, to quantify the security risks of interface design decisions

UISA Guideline 5 Steps Process

Step1

Identify application workflows, to focus the assessment on particular tasks and screens of an application.

Step2

Elaborate all of the user interface elements that are part of those workflows. This includes elaboration of every element where users provide input, navigate or perform activities, including navigation links and tabs, menus, text entry, and checkboxes and buttons.

Step3

Identify all of the possible errors users could make interacting with each of those individual elements, as well as possible errors they make interacting with a combination of elements in workflow level actions.

Step4

Determine the security consequences of each error, and filter out those without security implications.

Step5

Identify the potential triggers for the errors based on usability and usable security guidelines.

