Insecure & Unintuitive: How We Need to Fix the UX of Security

Jared M. Spool
@jmspool

Our design’s first experience: **SUX**.
Most common dialog box in the world.
Most expensive dialog box in the world.
Most expensive dialog box in the world.

Costs an Australian bank $75,000,000 a year for password resets.

Most expensive dialog box in the world.

Costs a major retailer $300,000,000 a year in lost sales.
Most expensive dialog box in the world.

Costs an organization $????,???,???,??? a year in lost productivity.

Most complicated dialog box in the world.
Password Guidelines

Follow these guidelines when creating a password:

- The password must be 8-32 characters long.
- The password must contain a mix of letters, numbers, and/or special characters. Passwords containing only letters or only numbers are not accepted.
- The password is case-sensitive.
- The password must contain a mix of letters, numbers, and/or special characters. Passwords containing only letters or only numbers are not accepted.
- Single quotes, double quotes, ampersands (`, `), and spaces are not allowed.
- Successive passwords should not follow a pattern.
- The password cannot be the same as your Merchant Login name and should not contain any part of your company name or user name.
- Do not post or share your password or send your password to others by email.
Insecure & Unintuitive: How We Need to Fix the UX of Security
Most judgmental dialog box in the world.
Creating an account is often the **first** thing users do with our design.

Logging in is the **first** action of each session.
Security UX (**SUX**) is our users’ first experience.
SUX is the last holdout of intentionally designed user experiences.

The real threats from poor security.
We need to protect the user and the system.

Protecting data
Data breaches and records exposed

Sources: Insurance Information Institute, Identity Theft Resource Center

Cybercrime Complaints

Sources: Insurance Information Institute, Internet Crime Complaint Center

We need to protect the user and the system.

Protecting data

Protecting personal information
Fraud Victims

<table>
<thead>
<tr>
<th>Year</th>
<th>Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>11.6</td>
</tr>
<tr>
<td>2012</td>
<td>12.6</td>
</tr>
<tr>
<td>2013</td>
<td>13.1</td>
</tr>
<tr>
<td>2014</td>
<td>12.7</td>
</tr>
<tr>
<td>2015</td>
<td>13.1</td>
</tr>
<tr>
<td>2016</td>
<td>15.4</td>
</tr>
</tbody>
</table>

Sources: Javelin

Fraud Losses

<table>
<thead>
<tr>
<th>Year</th>
<th>Losses (in billions of dollars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>$18.8</td>
</tr>
<tr>
<td>2012</td>
<td>$21.8</td>
</tr>
<tr>
<td>2013</td>
<td>$19.1</td>
</tr>
<tr>
<td>2014</td>
<td>$16.2</td>
</tr>
<tr>
<td>2015</td>
<td>$18.3</td>
</tr>
<tr>
<td>2016</td>
<td>$16.0</td>
</tr>
</tbody>
</table>

Sources: Javelin

We need to protect the user and the system.

Protecting data

Protecting personal information

Protecting financial instruments
We need to protect the user and the system.

Protecting data

Protecting personal information

Protecting financial instruments

Protecting access to other systems
Somebody sitting on their bed that weighs 400 lbs?

The Internet thinks Hackers are men wearing hoodies working in rooms with binary wallpaper.
Celebrity identity theft victims

- 50Cent
- Jessica Alba
- Carmelo Anthony
- Katie Cassidy
- Eric Clapton
- Kaley Cuoco
- Miley Cyrus
- Kirsten Dunst
- Hugh Grant
- Christina Hendricks
- Paris Hilton
- Julianne Hough
- Vanessa Hudgens
- Mick Jagger
- Scarlett Johansson
- Leslie Jones
- Kim Kardashian
- Mila Kunis
- Jude Law
- Jennifer Lawrence
- Blake Lively
- Sienna Miller
- Olivia Munn
- Rihanna
- Amanda Seyfried
- Steven Spielberg
- Analeigh Tipton
- Kate Upton
- Sofia Vergara
- Emma Watson
- Oprah Winfrey
- Mary Elizabeth Winstead
- Tiger Woods

---

**THE HUFFINGTON POST**

NYC  05/29/2011 03:04 pm ET | Updated Jul 29, 2011

**Anthony Weiner Says He Was #Hacked, After Briefs Shot Tweeted From His Account**

AP/The Huffington Post

NEW YORK — A *lewd photograph* of a crotch sent from the Twitter account of U.S. Rep. Anthony Weiner is just “a distraction” perpetrated by a hacker, his spokesman said Sunday.

Dave Arnold told The Associated Press in an email that the tweet, directed at a woman, was “a distraction” from the married New York Democrat’s “important work representing his constituents.”

“Anthony’s accounts were obviously hacked,” Arnold said. “He doesn’t know the person named by the hacker, and we will be consulting on what steps to take next.”

The photo showed a man’s bulging underpants.

It first was reported Saturday by BigGovernment.com, a website run by conservative commentator Andrew Breitbart. The site said the photo was tweeted to a Seattle woman.
Electronic Research Administration Procedure

National Institutes of Health

SUBJECT: Password Policy for Publicly Available eRA Applications
(Latest Revision: March 2009)
Policy

- **Password Complexity:**
  - Passwords must be at least eight (8) non-blank characters in length
  - Passwords must contain a combination of at least three of the following types of characters:
    - capital letters
    - lower case letters
    - numeric characters
    - special characters
      - ! # $ % - _ = + < >*
  - Passwords cannot contain username
  - First and last characters cannot be numbers

- **Changing Passwords:** Passwords must be changed at least every 90 days and the password cannot be reused within one year. Users must change their newly assigned passwords the first time they log on.

- **Account Lock-out:** Systems will lockout a user account after 6 consecutive failed login attempts.

- **User Session Inactivity:** System will disconnect user sessions that are idle longer than 45 minutes.

- **Caching Passwords:** Users are prohibited from caching (auto-saving) passwords on the local system. Users must enter the password at each login. Storing passwords in files on the user’s system is prohibited.

- **Sharing Passwords:** Users are prohibited from sharing passwords with each other and each user must have a separate and unique password. Users should not allow others to access resources under their credentials by logging on and then letting others use the computer.

- **Password Distribution and Storage:** Passwords must be stored, transmitted, and distributed in a secure manner. Passwords must not be displayed on the screen when entered. Electronically storing or transmitting passwords in plain text is prohibited.

- **Audit:** Accounts and their adherence to the password policy will be audited periodically.

- **Compromised Passwords:** Compromised passwords must be reported to the eRA Help Desk. Please see contact information below.
Compliance Budget: Managing Security Behaviour in Organisations

Angela Sasse
University College London
Department of Computer Science
Malet Place, London, WC1E 6BT
a.sasse@cs.ucl.ac.uk

The Compliance Budget: How individuals trade off the burden costs against the benefits to the organization.

1. Introduction

It is widely acknowledged in security research and practice that many security measures are enabled by human rather than technical factors (e.g., Merrett 2005). Researchers exploring the issue draw from a range of research perspectives, including psychology, sociology, and organisational behaviour. Although these fields have contributed to our understanding of how security measures are enabled by human factors, they have not yet fully addressed the issue of the trade-off between the burden costs and the benefits of security measures.

Categories and Subject Descriptors

© Copyright 2017, User Interface Engineering. All Rights Reserved.
Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?

Ross Koppel^{1,}, Sean Smith^{b}, Jim Blythe^{c}, and Vijay Kothari^{b}

^{a} University of Pennsylvania
^{b} Dartmouth College
^{c} University of Southern California

Abstract. Workarounds to computer access in healthcare are sufficiently common that they often go unnoticed. Clinicians focus on patient care, not cybersecurity. We argue and demonstrate that understanding workarounds to healthcare workers’ computer access requires not only analyses of computer rules, but also interviews for example, passwords were so commonly written on sticky notes and placed on terminals that they formed "stalactites," and in some hospitals, all workers shared a single password, which was written on a piece of tape stuck to the device -- to solve this, one vendor offers stickers "to write your username and password and post on your computer monitor."
Health workers were also skilled at defeating the proximity sensors that logged them out of their terminals when they got up from their workstations (these automated logouts are vital to ensuring that clinicians check that the record they’re looking at is for the patient they’re treating, preventing potentially fatal mixups): for example, by styrofoam cups over the sensors or assigning the most junior staffer to press the spacebar at timed intervals.

These workarounds were driven by clinicians’ need to get their jobs done and by IT’s failure to understand what that entailed. For example, IT’s imposition of password rotation schedules meant that no one knew what their passwords were from moment to moment, forcing them to write them down and share them (in some cases, IT might have had this policy set by vendors or regulators/insurers). Aggressive timeouts on terminals meant that clinicians spent an undue amount of time logging in, making it impossible to get their work done.
When poorly-designed SUX prevents people from doing their job, they work extra hard to bypass it.

The First Law of SUX:

If it’s not usable, it’s not secure.
Crafting a designer’s palette of great SUX.
Common security states

- Not Logged In
- Logged In
Sign in to your account

Email or username

Password

Sign In

Forgot your password?

Amazon’s security states

Not Logged In

Logged In
Amazon’s security states

- Not Logged In
- Identified & Not Logged In
- Logged In

Insecure & Unintuitive: How We Need to Fix the UX of Security

© Copyright 2017, User Interface Engineering. All Rights Reserved.
Amazon’s security states

- Not Logged In
- Identified & Not Logged In
- 1-Click Enabled
- Logged In

Sign in to your account

- Email or username
- Password

Identification

Authorization

Forgot your password?
Check your email

An e-mail was sent to dtrump@trump.com. In order to complete the e-mail verification process, you must click on the link in the e-mail we sent you.

Be sure to check your spam filters if you can't find the e-mail in your in-box. You may also contact customer service for help.

Identify: Who are you?

Authorize: Do you have permission?

Authenticate: Are you who you say you are?
Amazon’s checks for authenticating new accounts

Authorizing the purchase with merchant

Checking shipping address against problem list

Matching business address to credit card database

Checking IP address against known problem list

Design:
The Rendering of Intent
We can thoughtfully split up Identification, Authorization, and Authentication to reduce friction in our SUX experience.
Identification, Authorization, and Authentication

Are we asking for only what we need to deliver a great experience?

Your Account > Manage Default Address and 1-Click Settings

Click here to add a new address Enter a new address

Need to change an address on an open order? Visit Your Orders
To manage your addresses visit Manage Address Book

**Default Address and 1-Click Settings** (what this means)

**Jared M. Spool**
User Interface Engineering
510 Turnpike St Ste 102
North Andover, MA 01845-5812
United States
Phone: 978 327 5561

**Default 1-click settings and payment method preferences**

**Shipping method:** Standard Shipping (3-5 business days)
**Include in 1-Click dropdown:** Yes
**How address appears in dropdown:** Jared (Work/Amex)

**Payment method:** American Express ***

[Edit] 1-Click settings for this address.
[Edit] payment method for this address.
Insecure & Unintuitive: How We Need to Fix the UX of Security

![Gift Cards Image]

- **Gift Cards**
  - **eGift**
  - **Print-at-Home**
  - **Mail**

![Amazon Checkout Image]

- **Digital delivery:** See details in “shipping options” section below.
- **Payment method:** American Express ending in 4321
- **Review items and shipping**
  - **Estimated delivery within 5 minutes**

Digital delivery: Your gift cards will typically arrive within 5 minutes of the successful completion of your order, or on the scheduled delivery date.

Order total: $50.00

© Copyright 2017, User Interface Engineering. All Rights Reserved.
We can mitigate risk for most users by employing sophisticated threat models.

**SUX Designer’s Palette**

<table>
<thead>
<tr>
<th>Identification, Authorization, and Authentication</th>
<th>Threat Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are we asking for only what we need to deliver a great experience?</td>
<td>Have we matched our designs to the specific user and system risks?</td>
</tr>
</tbody>
</table>

© Copyright 2017, User Interface Engineering. All Rights Reserved.
Volvo Safety Features

- Laminated windscreen
- Three-point seat belts
- Padded instrument panel
- Twin-circuit triangular braking system
- Crumple zones
- Three-point seat belts in rear
- Three-point inertia-reel seat belts

- Child-proof door locks
- Energy-absorbing steering column
- Energy-absorbing bumpers
- Gas tanks located forward for enhanced safety
- Anti-locking brakes
- Brake lights placed at eye level
- Three-point seat belt in the middle rear seat

When we’re building a **security system**, we’re really building a **safety system**.
Seat belts put the burden on the user.
Airbags embed the burden in the system.

iMessage

Hey, you know what sucks?

Hey, you know what sucks in a metaphorical sense?

Hey, you know what just isn’t cool?

I hate you...

Not really, now that I think about it.
Safety is a Burden

Burden placed on the user
- Creates frustration
- Prone to accidents

Burden placed in the system
- Higher development costs
- Requires innovation

When the burden is on
the user, any mistake is
their fault.

When the burden is in
the system, any mistake is
our fault.
User Error is the opposite of Empathy.

We’ve temporarily locked your account after too many failed attempts to login. Please try again later.
Empathy means designing for our users’ safety without assigning them any burden.

**SUX Designer’s Palette**

<table>
<thead>
<tr>
<th>Identification, Authorization, and Authentication</th>
<th>Threat Models</th>
<th>User Burden Reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are we asking for only what we need to deliver a great experience?</td>
<td>Have we matched our designs to the specific user and system risks?</td>
<td>Have we created designs to embed the risk into the system?</td>
</tr>
</tbody>
</table>
Security Perimeters

Insecure & Unintuitive: How We Need to Fix the UX of Security
Smart security perimeters postpone UX friction to the last possible moment.
### Identification, Authorization, and Authentication

Are we asking for only what we need to deliver a great experience?

### Threat Models

Have we matched our designs to the specific user and system risks?

### User Burden Reduction

Have we created designs to embed the risk into the system?

### Security Perimeters

Have we created the right levels of security throughout our designs?

---

We now have sophisticated control over **SUX**.

There’s no better time to start improving it than now.
4 Building a toolkit for great SUX.

The top reasons we continue to ignore SUX:

“This is what we’ve always done.”

&

“This is how everyone else does it.”
“The most dangerous phrase in the language is:

We’ve always done it this way.”

— Admiral Grace Hopper
Password Policy

Password must not be a dictionary word.
Password must not contain or match first name.
Password must not match or contain last name.
Password must not be longer than 12 characters.
Password must contain at least 2 alphabetic character(s).
Password must be at least 8 character(s) long.
Password must contain at least 1 lowercase letter(s).
Password must contain at least 1 numeric character(s).
Password must contain at least 1 special character(s).
Password must contain at least 1 uppercase letter(s).
Password must not match or contain user ID.

Password Policy

Password must not be a dictionary word.
Password must not contain or match first name.
Password must not match or contain last name.
Password must not be longer than 12 character(s).
Password must contain at least 2 alphabetic character(s).
Password must be at least 8 character(s) long.
Password must contain at least 1 lowercase letter(s).
Password must contain at least 1 numeric character(s).
Password must contain at least 1 special character(s).
Password must contain at least 1 uppercase letter(s).
Password must not be one of 6 previous passwords.
Password must not match or contain user ID.

GSV Steen
@mediapathic

Your password must contain at least two female characters who talk about something other than a man

RETWEETS 1,455
LIKES 3,222

8:57 PM - 26 Dec 2016
Insecure & Unintuitive: How We Need to Fix the UX of Security

© Copyright 2017, User Interface Engineering. All Rights Reserved.
Password strength doesn’t matter when the user willingly tells it to the criminal.
Are all of these legitimate?
Time cost of a brute force dictionary attack: 3-4 days

Time cost of a phishing attack: 1 minute
Two-Factor Authentication

1. Something You Know (password)
2. Something You Have (device, key)
3. Something You Are (biometrics)
Insecure & Unintuitive: How We Need to Fix the UX of Security

© Copyright 2017, User Interface Engineering. All Rights Reserved.
MileagePlus account security enhancements

In order to enhance the security of your MileagePlus account, we need you to make a few account updates. You will no longer be able to use a PIN to access your account online, although your PIN will still be required for certain phone transactions.

Please select security questions and answers from the dropdown menus.

Question 1 of 5
What is your favorite pizza topping?

Question 2 of 5
What is your favorite warm weather activity?

Question 3 of 5
What was your most favorite fruit or vegetable?

Question 4 of 5
What was your least favorite subject in school?

Question 5 of 5
What is your favorite flavor of ice cream?

Save my security questions
The First Law of **SUX**: If it’s not *usable*, it’s not *secure*.
Assume passwords will never make your system secure.
Most common agile user story in the world.

As a user, I want to log in.

Customer Journey

When does our user log in?

What’s their experience when it doesn’t go well?
Multiple SUX Customer Journeys

- When user recalls username & password correctly.
- When user returns to session before the session expires.
- When user returns after session has expired.
- When user remembers correct username, but can’t recall password.
- When user locks their account because they tried a little too hard.
- When user can’t recall either username or password.

David Marcus
Paypal CEO – 2012-2014
“That which gets measured, gets done.”

— Tom Peters

“That which gets measured, gets done.”

— Peter Drucker
“That which gets measured, gets done.”

— W. Edwards Demming

“That which gets measured, gets done.”

— Lord Kelvin
A Starter Kit for key SUX metrics

- How may SUX-related error messages are you issuing?
  - Username / Password doesn’t match
  - Locked accounts
  - Session timeouts

- How many requests for password resets are you receiving?
- How many legitimate resets are being fulfilled?
- How much business/productivity is lost due to security problems?

We don’t have to keep doing what we’ve always done.
Fixing the UX of Security

- If it’s not usable, it’s not secure.
- We can embed the SUX burden in the system by being intentional about when we identify, authorize, and authenticate users.
- Sophisticated threat models help us ensure the SUX experience is appropriately matched to the risk.
- Thoughtful security perimeters reduce the friction from user burden.
- We can’t let we’ve always done it this way be the reason we continue to ignore SUX.

Find me at:

- uie.com
- jspool@uie.com
- @jmspool

Don’t forget to connect to me on the LinkedIn.

Go ahead! Follow me on the Twitters.
2-year school for industry-ready UX Designers.

Looking for new students.

Looking for projects for students to design.

www.CenterCentre.com