**Association of Voice Interaction Designers – Workshop 2013**

**Topic: Authentication**

**ATTENDING:**

Jenni McKienzie (Travelocity), Susan Hura (Speech Usability), Yves Normandin (Nu Echo), Mark Smolensky (AT&T), Crispin Reedy (Versay), Robert Costa (eLoyalty)

**SUMMARY:**

There was a lively and wide-ranging discussion around the topic. The attendees eventually focused around three areas:

1. There could be a flowchart depicting the business process that a designer and business might use to help them decide on an appropriate identification and authentication process. For example, what are the criteria by which identifiers and authenticators are chosen? Where should this be done in the login process? And so on.
2. The possible future state of identification and authorization: For example, voiceprints, other biometrics, multi-factor authentication, etc.
3. The concept of setting your own security level for your account. Some users may have additional security concerns and are interested in such things as second sign-on, secondary PIN, etc.

The following notes loosely document the discussion which the group had. Our ultimate goal was to regroup and write white papers fleshing out these subjects in more detail. Until such time as the attendees have a chance to do so, these minutes have been revised to be a bit more organized around the discussed topics.

**INTRODUCTION:**

The group discussed the difference between Identification and Authentication. Identification means who you are and what are you calling about (which account?). Authentication means the next level, beyond which you might allow the caller to do a transaction or make a change to their account.

**TOPIC 1: FLOWCHART / BUSINESS PROCESS AROUND IDENTIFICATION AND AUTHENTICATION**

* + **IDENTIFIERS**
    - First question: What personal information does the business have available to use? And what quality is it?
    - Of that personal information, what is the caller most likely to remember?
    - And/or readily locate?
    - How “hackable” is it?
    - How easy is it to recognize over the phone with speech input i.e. digits vs. alphanumeric?
    - How high quality is it (challenge questions, etc.)?
    - There is always a balance of risk and convenience. (to both the company and the caller). What is the right balance? Ultimately this is a business question.
* **DATA**
  + How important is the data we are making available to the caller?
  + What kinds of changes are we allowing the caller to make, and how critical are they?
* **TYPE OF ATTACK**
  + What type of attack are we protecting against? Is it generic or personal, i.e. are we protecting against a generic hack or the crazy ex?
* **OTHER CONSIDERATIONS:**
  + Where to do it in the call flow?
  + How to do it i.e. allow speech input only?
  + There have to be multiple ways to identify and validate, depending on how vulnerable the information is, and what information and technologies have available to you.
* **LIST OF IDENTIFIERS AND DISCUSSION AROUND THEM**
  + ANI / DNIS
    - Passive collection
    - ANI: changes less, but not reliable as to where the caller is from. Also, is easily spoofed. And, there are issues about having multiple phone numbers, and having multiple people in the same household.
    - How much can you give out based on ANI? It's fairly low quality, so should probably only be used for fairly low-risk situation.
    - Potential to do ANI capture and then ask them, are you calling about XXX-XXX-XXXX? and then if you don't know it, ask them to give us the phone number that they are calling about.
    - What if they have multiple phone numbers on the account? then ask them for a different phone number.
    - Current data shows that 1/3 of the population has cellphone only.
    - ANI / Phone number as input are essentially the same.
      * Inputting phone number covers the scenario where ANI doesn't match (calling from work, thing doesn't get passed)
  + Account number
    - Could be easy or difficult to collect, depending on whether or not it is numeric or alphanumeric
  + Transactional-based identifiers
    - Not something about you, something about the transaction. For example: Trip ID, Tracking number, Order number
    - These are pretty low-risk scenarios usually - the information you play back is more generic - for something like this, typically they just put it in and there is no alternate method. Perhaps payment information, if there is a payment associated
    - Personal and/or account identifier vs. transactional
    - (One to many, many to one regarding personal / account)
    - Note: A phone number could be either personal / transactional.
  + Location
    - GPS - have to make the phone call from the app, not the phone.
    - Could use for this information and then say, for example, I need to get another identifier if I see you are not where you usually are.
  + Last four of SSN
  + DOB
    - DOB comes up as something publicly viewable on background check sites.
  + Zip
  + Mother's Maiden Name
    - Note: Definitely less secure than it used to be due to Facebook, technology
  + PIN
    - Seems a bit old fashioned, but you have control over it; you can reset it and change it, which is not true of other items of personal information. For example, what if your account Is compromised? You can change it; you can’t change your birthdate. People tend to use the ones that are all the same everywhere. People tend to use one that is hackable, i.e. the birthday of your kids, your house number. They're hard to remember. If it's more than four, it becomes even more confusing. If you set it and you don't use it, it will be even harder to remember.
  + Password
    - Has similar issues to PIN.
  + Cross-channel
    - Cross-channels - becomes an even more difficult issue because websites are good for things like strong password, but IVR is good for numeric.
    - Some companies have you do input on the keypad - just type it in. But it assumes alphanumeric, no special characters.
    - Platform, of course, have to maintain this across web and IVR.
    - Also assumes that you can remember those across this platform. It is very easy to not remember them, or they ask questions that are not applicable to you or you can't remember the answer. Or you can't remember which one you put in.
  + Challenge Questions / Choose your own security questions
    - Typical security questions such as your hometown questions about school etc. - feel very insecure if you still live there, especially if it a small town.
    - Challenge question is a different problem than a traditional speech recognition problem in that you're collecting something you already know. You're just trying to figure out whether or not the person knows the right answer. Doing the recognition and then doing a sort of comparison, a distance calculation. So I might accept a result where the correct result is not even in the nBest list if it is within the comparison. There is a known false accept rate, but you can adjust for it. So they do constrain the grammar (at least for something like names). Generate the impostors based on the corpus and then calibrate the system.
  + Credit card
    - The security code is the only thing that a company can't retain. Otherwise, if you do transactions, you can save off the credit card number and work off that.

**TOPIC 2: WHAT IS THE WAVE OF THE FUTURE?**

* Biometrics?
  + Voiceprint login systems are being taken out - they are not necessarily a success story - but the passive systems can be more accurate as they are sampling over time and over multiple calls. Even a 2 minute conversation is a lot of data - but it is text independent. What's the role of the agent versus the IVR? In this particular case, the biometric is being done in the call center, so depending on where the software is deployed, they might have to transfer out to someone to do it.
  + Will there be a central repository of voice print associated with ANI?
    - It's very frustrating when you're the legitimate user and you can't get in to your own account
  + FIDO alliance - voice print information
  + The fraud is happening in the call center. You can do passive biometrics while the caller is talking to the agent to actually tell the agent whether or not this is the same caller that has called before.
* Multifactor?
  + Something you know, something you have, and something about you.
  + Something you have - your phone, your keyfob to login to a VPN network
* Single factor / multi-factor is key - financial institutions will lead the way.
* The point of security is that your barriers could always potentially be worked around, but are they strong enough to encourage people to go elsewhere? This goes back to random fraud vs. malicious insider hacking.
* Nothing is foolproof.
* Sliding scale - what do we want to protect, how much do we want to spend on building protections, and how hard do you want to make it for your legitimate customers to get into the account?

**TOPIC 3: PERSONALIZED SECURITY PREFERENCES**

* Can I set my own security preference? i.e. I'm a person and I want to have my security for my bank up high or down low. Or you have the option of making your own account more secure, using more identifiers, and / or adding a PIN to your account. For certain customers, you would want an extra layer. Or like email - adding the second-sign on to your account.
* Enough security so that the users feel secure. If you have all passive identification, for example, the users don't feel secure; they will say something like, How did you know it was me?
* Company sets minimum limit and users can add more authentication on there if they want it.