ecommerce_scenario

Scenario: Packaging Resources for E-Commerce Vendors (Accepted)

Submitted by: Eve Maler

This scenario focuses on the typical set of information that we hand over to online vendors repeatedly, and the desire to avoid sharing the data "by value", instead focusing on how to share it "by reference" (pointers).

Problem scenario

Let's look at how an online buying scenario might look today.

1. Bricks and mortar

   Maya recently became extra-concerned about identity theft and fraud because a friend had his bank account stolen from, and she has decided to buy a shredder so she can dispose of old bills, credit-card offer junk mail, and outdated backup CDROMs. She visits her local Staplers store, prepared to buy a shredder that day (with cash! hey, it's anonymous), but can't find a shredder in stock that handles CD shredding.
2. Comparison shopping

   She goes to Google and a couple of specialized comparison-shopping sites and plugs in search terms like paper shredder cdrom, but can't easily figure out which ones have the features she wants, but the prices at Staplers.com, the site for the local store she was just in, look good and she decides to just go ahead and shop there.
3. Clicks and mortar

   Once Maya is at Staplers.com, she finds a suitable shredder and adds it to her shopping cart (which is, so far, "anonymous" with respect to everything but some sort of device identification, possibly based on a cookie, associated with her browser session).
4. Checkout

   When she goes to check out, Maya is asked for consent and personal data for various purposes. First, she must choose a username and password, on the theory that this will make her future purchases at the site easier. She also has to provide her home address and phone number (though this isn't so onerous because her browser auto-fills the data) so Staplers can transfer the shredder to its outsourced shipping company for delivery, and her credit card number, its security code, its expiration date, and her real name (the name the card was issued to) so Staplers can be paid for the purchase. She might be given the opportunity to provide some third-party store loyalty program information, to get "extra points" from transactions here. Finally, she is asked to click "I Agree" certifying that she agrees to Stapler's site terms of use and has seen its privacy policy.

Desired improvements

Following are some key questions we can ask, identified by whether they capture an identity management (IdM) issue, a vendor relationship management (VRM) issue, or a social networking issue. (Note that some of these questions highlight scenarios and use cases that the calendar scenario has already captured. Some of these might want to get turned into unique use cases for this scenario.)

- Can we imagine better ways for Maya to set up a data-sharing relationship with Staplers.com? (IdM, VRM)
  - She's planning to move in a couple of months, and that means the address information Staplers has saved will go stale.
  - Same for her credit card: it will expire next year. When these items change, she has to go fix them at dozens of sites.
  - She's not crazy about having to supply things like credit card information to every vendor on the web.
  - She thought the site terms and privacy policy were just "okay", but accepted them because she effectively has no choice – and OfficeArmory.com is probably the same anyway.
- Is it possible for Maya to have a "one-night stand" with Staplers.com rather than a long-running relationship? (IdM, VRM)
  - ...if she doesn't really want Staplers to track her purchases, browsing habits, or anything else over time.
  - ...if she wants to share only the minimum personal information Staplers really needs to do its job this once, and then only temporarily.
- Can we imagine betters ways for Maya to engage in the shopping-around process, possibly involving her sharing **more** data about herself? (VRM – particularly volunteered personal information!)
  - What if she could "issue a personal RFP" indicating the price and features she's interested in, and entertain vendor site "bids", such that not only Staplers.com and OfficeArmory.com could bid, but also Ann, who has a used shredder she'd like to sell?
  - What if she could let Staplers know her customer-support phone line preferences, such as wait time and ad-playing tolerance?
- What would it look like for Maya to get a unified understanding of **all** of her data-sharing relationships? (VRM)
  - She sure would like to get a handle on her own "personal data analytics" – "who knows what" about her.
  - If Staplers behaves badly (gives out her data against her rules or allows a data breach to occur), she wants to have better options for recourse.
  - ...and she wants to be able to cut off their future access to information about her.

Solution Scenario

Maya shares the information about herself that Staplers.com needs at the beginning of her e-commerce relationship with them, but instead of having to share it "by value", she shares it as some form of *pointer* to a package of resource pointers that Staplers can dereference and refresh as they needs to over time. She can change the underlying information whenever she wants to without worrying about paying special attention to Staplers (or any of the other hundred e-commerce sites with which she has registered.

Actors:

- Maya (User)
- Authorization manager (AM)

- Personal datastore (Host) in which authoritative versions of resources to be shared reside (that colocation of AM and Host is not a requirement, but for this scenario the individual resources are assumed to live on a single Host)
- Staplers.com (Requester)

Distinctive aspects:

- User can package and reuse pointers to resources commonly needed for e-commerce into a rolled-up resource that is available for access by multiple requesters (assume for this scenario that all the individual resources and the rolled-up resource are available from the same host in the "personal datastore" model).
- The data involved is "self-asserted" to a first approximation. (The credit card data we often share today is "asserted" solely by us, but then the vendor validates it out of band.)
- Requester can handle receiving and dereferencing both a pointer to a package resource and pointers to individual resources.
- AM can manage the offering and meeting of terms for resource-sharing for the whole package and can take advantage of efficiencies where the terms for individual resources are identical (possibly similar to the Distributed Services scenario).
- Requester will often represent a requesting party who is *the same human being* as the authorizing user, and can take advantage of efficiencies in any real-time requester/AM/user connection for obtaining user consent in that moment.
- Requester, host, and AM are likely to be willing to deal with each other solely on the basis of the user's say-so (unlike in the personal loan scenario).

Use Case: Online Purchase with Setup of a Long-Running Account Relationship (Accepted)

Submitted by: Eve Maler

Preconditions: Maya has already stored, and packaged together, pointers to the set of relevant resources frequently needed for online purchases:

- Her desired credit card number, expiration month and year, security code, name on card, and billing address
- Her shipping address and phone number

So...

1. She goes to Staplers.com and puts her desired shredder in her shopping cart.
2. When she goes to check out, she's presented with a requirement to register for an account. The form has fields for the data listed above, but also has a new field for "Personal data feed".
3. In a separate browser window, Maya visits her Relationship Manager and generates a unique URL representing the disclosure package she wants to offer Staplers (CC number etc.) and the policies she expects it to adhere to in accepting her information (they can't sell her data etc.).
4. She goes back to Staplers and pastes the URL she just generated, and presses a button that says "Share personal data".
5. The Staplers web application follows the link, discovers it has to agree to a set of policies before getting through to the info it needs, decides to agree, and gets through.
6. Staplers retrieves data items with content-types that indicate they contain CC numbers, addresses, etc., and then displays the values retrieved in the regular registration form fields, possibly with some graphical indication that Maya can override any one of them.
7. (later) Maya can use her RM to view the activity related to Staplers' retrieval of her information, check what she's told them (and others), and also check the conditions under which she released information.

Issues

- How can we ensure that the sensitive data is secured in motion (while being conveyed to Staplers)? (generic across all scenarios)
- What is the right UX paradigm for letting Maya override information? Ideally, any info that's changed should be updated in the RM, not on the Staplers site. But if she wants to override a value just once, with values to be updated in future pulls of the feed, the right place to change it is on the Staplers site itself. Does this latter situation sound likely?
- What about interfaces where the credit card information is provided at a separate point in the process? How should that be accounted for? Perhaps, except for subscription-type payments (ongoing over time), this information is not part of the registration bundle and is provided (by reference or by value) only at purchase time.

Use Case: Engaging in a Purchase "One-Night Stand" (Accepted)

Submitted by: Eve Maler

This is the same as the first use case outlined above, except that Maya provides her resource package not as part of a request to register a new account, but as part of a one-time purchase. (Some websites today allow for purchases without registering, and are prepared not to give you a browser cookie or retain your information beyond necessary for the purchase and its aftermath.)

The policies Maya chooses in this case are likelier to be more stringent about not retaining personally identifiable information (PII) for any significant length of time, and may ask the vendor to generate "positive" assurance messages about policy adherence (not just silent adherence).

(The protected-inbox scenario might play an especially important role if Maya is engaging in a one-night stand purchase, since it enables the vendor to report product recalls and such to Maya without her having to expose other more compromisable communications endpoints such as persistent email addresses or phone numbers.)