ICS 132: Organizational Information Systems

Assignment #3: Security and E-Commerce

This assignment will be due at the lecture on 03/11/02.

Answer all three questions. Your answers for each question should be around half a single-spaced page.

1. One of the features that electronic commerce can provide is comparison shopping, either through side-by-side comparison between different vendors/products, or through sites, like www.cnet.com or www.cdw.com, that explicitly compare products or vendors. Take a look at cnet.com (or another comparison shopping site) to see the features they offer.

   How does this affect bargaining power and/or provide competitive advantage for (a) a shopper, (b) the vendor/manufacturer, and (c) the shopping site? (Note: try to come up with an answer for (b) that isn't just the inverse of your answer for (a)!)

2. Take a look at the attached article, which appeared in a ComputerWorld column in February 2002. Describe the problems that it reports in terms of the "three A's" – authentication, authorization, and accounting.

3. Some researchers are investigating the consequences of "crytographic abundance." Their theory is that much research in cryptography in the past has been based on the idea that cryptography (the ability to encrypt and decrypt) is hard to do, and therefore rare. Instead, they argue, trends in processor and network performance means that crypto is getting easy to do and will be everywhere. Give two examples of situations in which we assume that crypto is hard. What might be the consequences for these examples of living in a world of cryptographic abundance?

NICHOLAS PETRELEY

Lessons in CRM

(February 18, 2002) Customer relationship management and security are inseparable. That is, unless you're Pacific Bell or MCI. To illustrate, allow me to tell you a little story. It all started when I noticed that someone was using my MCI calling card to make calls to Germany. I canceled the calling card and, just to be on the safe side, switched my long-distance carrier to Sprint.

About a week or so after I received my Sprint materials, I got a call from MCI. I expected it to be a pitch to come back, but it wasn't. The MCI customer representative was checking to see if the recent calling card calls from Colorado to Germany were legitimate. The woman with the friend in Germany had apparently switched my long-distance carrier back to MCI.

I canceled the MCI account and then created a new one without the international plan and password- protected it. As an extra safety measure, I had my local phone company, Pacific Bell, put a Primary Interexchange Carrier (PIC) freeze on my phone number to stop anyone from changing long-distance carriers. I password-protected that account, too.

The next time I called Pacific Bell, I couldn't talk to customer service until I agreed to pay on my delinquent account. Delinquent? Well, come to think of it, I haven't received any statements in the past few months. I managed to get a human on the line and asked if there was a way I could pay off my bill via the Web. She said that if I created a Web account, I would stop receiving statements in the mail. Suddenly it became clear. Someone had already created a Web account for my number, which is why I wasn't receiving my statements.

Pacific Bell's system won't let me create a new Web account for the same phone number, which is the way it should work. The Pacific Bell representative couldn't change the Web user name or password or cancel the Web account, which isn't the way it should work. She asked another department to cancel the Web account and said a specialist would call me back.

Still Locked Out

As I write this, it's been well over a week since I made that call. The bogus Web account is still active. No calls from specialists. No responses to e-mails. I'm still locked out of the Web account.

This piqued my curiosity about how MCI handles Web accounts. MCI requires your account number or your calling card personal identification number (PIN) to create one. I hadn't received an MCI bill with my account number yet, so I entered my calling card PIN. It rejected the attempt. My MCI account had been compromised again.

I called MCI to get my account number. The representative gave it to me without asking for my account password. This fellow also offered to remove the PIC freeze. It's really easy, he said. All he has to do is call an 800 number. No wonder my account was so easily compromised. (MCI handled my next call properly, so it depends on the representative.)

I created an MCI Web account. (Unlike with Pacific Bell, you can create as many MCI Web accounts as you like for the same phone number.) I could see the calling card PINs on all five new calling cards. And although I could add new services, the Web software offered no options to remove the cards, the international calling plan or any other services.

So what have we learned?

Lesson 1: Integrate your CRM solutions. At the very least, synchronize the security data. Pacific Bell customer service uses your phone number to find your account. The corresponding Web account should therefore be based on the same phone number, not an arbitrary user name. Both should require the same password, too.

Lesson 2: Enforce security policies in software. The CRM software that customer service representatives use should prevent the representatives from making changes to a customer's account until they've asked for and entered the customer's password.

Lesson 3: Avoid blatant stupidity. If you haven't already created a Pacific Bell Internet account, anyone can create one for you—and lock you out of it—with little more than your phone number. MCI requires an account number, but if you want one, just glance at someone's unopened MCI bill. Their account number will be visible right through the address window on the envelope.