Lecture Notes for
3/23/06
Title: Conveying Trust or “Doing crazy stuff with Web Browsers”
(Notes – Matthew DeSantis)

Overview:
Though many threats to WWW users stem from scams present in email or instant messaging, the web browser and its inherent “features” and “faults” are typically the vehicle that makes these threats possible.

In the beginning the attacks were relatively simple, simply because the web architecture (servers & browser architecture) was simple. Man in the middle attacks and traffic sniffing were commonplace and were ultimately solved by integrating SSL (a sockets layer based on a similar premise as ssh, etc.)

Visual Cues:
Visual cues to the user about whether communications were secured were initially locks & keys, presumably reinforcing the notion that something was locked down. Initially, these were displayed at the bottom corner of the browser but have recently become more prominent (in the URL bar with FireFox for example.)

Phishing attacks (trends)
As phishing attacks became more prevalent and successful, the browsers have become more prudent in their default settings, thereby minimizing the risks when a user in fact does get fooled into going to a bogus web site. But other extensions have been added to account for cases where the infrastructure or limitations of the protocols or standards can’t verify 100% that the site is legitimate, that is, not spoofed.

These take the form of toolbars, notification windows, indicators, community ratings, and heuristics.

**An interesting point: Why should users be trusted to make decisions about the validity of sites that ultimately affect the community?

Class discussion:
How do you determine if a site is legit?

Some answers
* (Matt) Usually if they make me go through a well defined process to do something, like, say double-opt-in emailing or a security process I know (that is commonplace), then I suspect it is probably legit.

* some people look for https
* some base legitimacy on whether communications by a bank are in accordance with an action of theirs. (phishing email falls out of sync with that) In other words, you know

phishing email when it asks you to do something to your account and you think to yourself “I know that account is up-to-date, and I didn’t do anything to cause such a change, so I will ignore this email”

- Examples of different toolbars follow –

Class formed groups and each downloaded a different toolbar to give a quick usability test.

At least one group reported that they couldn’t download the version (the software wasn’t managed correctly and was difficult to find and piece together and install.)

Our group used Trustwatch and we found that the indicators it used [Verified / Unverified / Warning] were visible enough to alert the user. The trouble is, millons of perfectly good sites report “unverified”

A site is rated by a combination of known blacklists, traffic analysis, and apparently site reports. But the site report functionality is so lean, that we doubted they used it much to create the ratings.

Major problem with Trustwatch is that it spawns a new window for each site you want to check the rating on. And it doesn’t put the domain name in that window, so you can’t keep track of what info windows go with what web site if you have enough of them open: major design flaw.

Class Question: “has anyone tried aggregating these tools?”
General answer was “no why would anyone want 7 toolbars on their screen.”

But I guess the real question is why hasn’t aggregated these tools into one bar, which used several dimensions of data analysis. The answer was something like “not enough economic motivation.”

Password Hashing:
Works to a certain degree, reencrypting your normal passwords on the fly each time. However, you can only do this from the machine that has the plugin installed.

Skins:
You associate a picture or shared secret between the window and login box.

Problem with this is – if you visit a fraudulent site first, then when you visit the legitimate site, you get a false negative.

Tokens:
Tokens are forms of 2 factor authentication, usually something you have with you and are usually cryptographic.

Phones:
People are using phones with Bluetooth as a form of 2 factor authentication.