

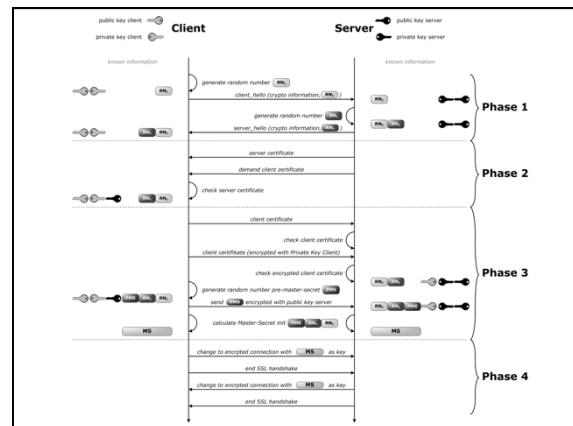
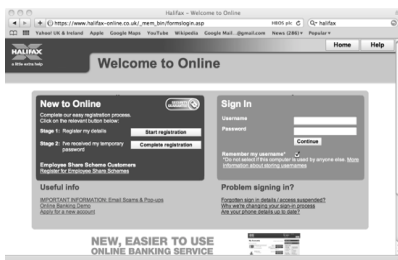
Usability & Security

Tom Chothia
Computer Security

Today's Lecture

- Usability & Security
 - Often the most over looked factor.
 - Social Engineering
- Cost benefit analysis for security advice

Breaking SSL



Cranor et al.'s Crying Wolf: An Empirical Study of SSL Warning Effectiveness."

A scientific test of how users react to certificate warnings.

Their first idea: make them think their online bank account is being attacked:

Use a web proxy to do a man in the middle attack.

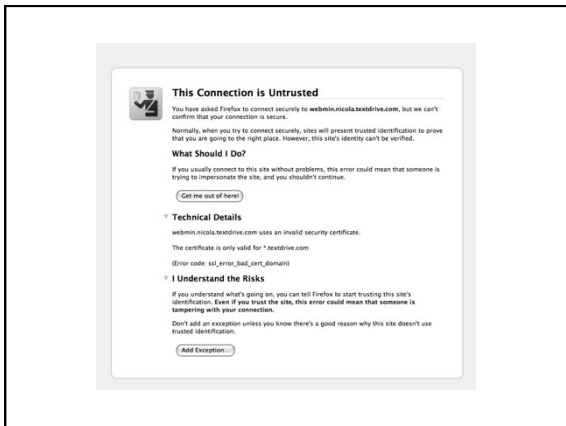
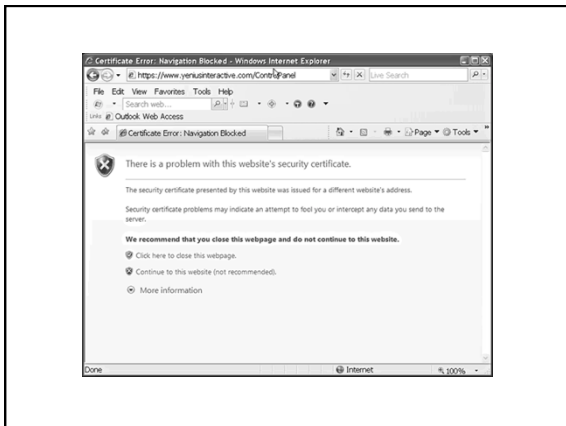
Problem: This would be illegal.

Second Idea

• Remove the root certificate from browser so that web site certificates can't be verified.

• Therefore the browser gives the same warning as a faked certificate.

• See how users react.



Laboratory Study

- 100 participants
- 5 Randomly-assigned conditions
 - FF2
 - FF3
 - IE7
 - Single-page custom warning
 - multi-page custom warning
- 4 tasks, warning triggered twice
 - Bank
 - Library catalog

Secure Connection Failed

The website responding to your request failed to provide verifiable identification.

What type of website are you trying to reach?

Bank or other financial institution

Online store or other e-commerce website

Other

I don't know

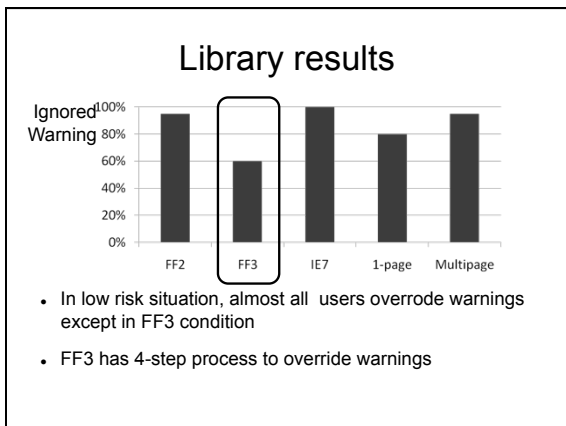
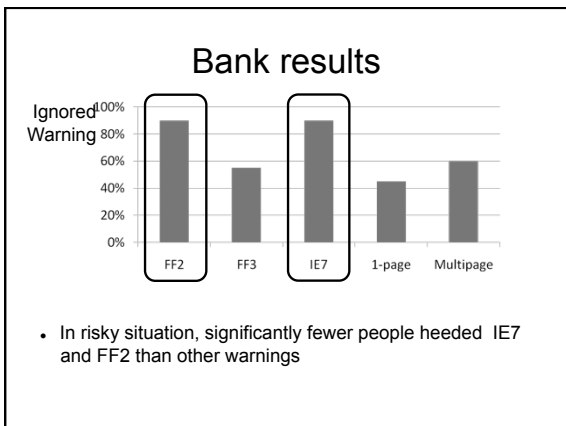
You are being warned because the certificate's name does not match the name of the website.

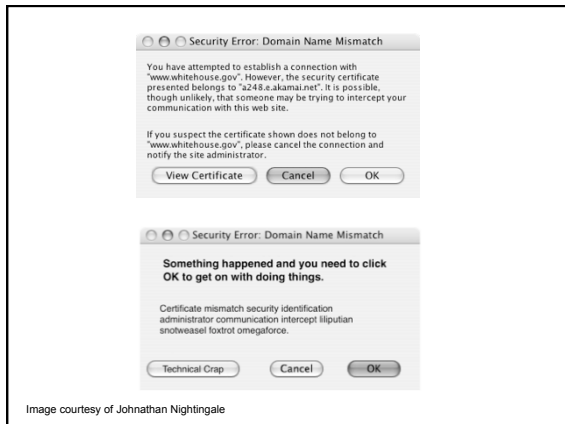
High Risk of Security Compromise

This connection to [cannoli.library.cornell.edu](#) is being intercepted by another party or someone is impersonating [cannoli.library.cornell.edu](#).

An attacker is attempting to steal information that you are sending to [cannoli.library.cornell.edu](#). We advise you to contact the company by telephone or using a different computer that does not use this warning.

Source: Firefox





Other “Social” Attacks

- There are many ways information can leak out of a system.
- Computer security experts often overlook the non-technical attacks.

For example

- A Defcon talk by Johnny Long at
 - <http://www.youtube.com/watch?v=5CWrzVJYLWw>
- Particularly 34:00 - 39:00.
- Imagine you are in charge of security for a company, how could you stop these kinds of data leaks?

Other Ways to Get Information

- “Shoulder surfing”
 - reading data from someone’s laptop screen,
 - and from paper documents
- Dumpster driving:
 - Picking documents out of the trash

Social Engineering

In general people want to be helpful.

- Why not just phone them up and ask for: Passwords, Credit card numbers, etc. etc.
- Attackers might say they are from the phone company and walk into your server room.

For example

- Kevin Mitnick at “HOPE” on stealing source code by just asking for it:
 - <http://www.youtube.com/watch?v=puNKT5h6ams>
 - <http://www.youtube.com/watch?v=Xm4qjrmGjM&NR>
 - 5:26 to 1:00

Kevin spent 5 years in jail for this and other crimes. I’m showing you this so you can think about how to stop this kind of attack.

Danger:

This often leads to people thinking:

“Users are stupid: they are the problem”

NO! Users are doing what they need to do to get the job done. Bad security design is often the problem.

When is a New Security Measure Good?

When it saves more than it costs:

$$\sum \Delta \text{Costs} < \sum \Delta \text{Benefits} \quad \checkmark$$

Benefits can be very hard to calculate, however we know a security measure is bad when:

$$\sum \Delta \text{Costs} > \text{Total Losses} \quad \times$$

Example: Checking the URLs

Phishing sites often use fake URLs to trick people, into giving away their password.

www.paypal.com
www.paypa1.com
www.paypal.com
www.paypal.org
66.211.169.2
active-www.paypal.com
www.paypal.org.host.com
www.paypalobjects.com
<u>www.palpay.com</u>

Which of these URLs belongs to paypal?

Losses Due To Phishing

Using US figures from 2008:

Total losses due to phishing attacks: \$60 million
Number of Internet users: 180 million
Phishing cost per person: 33 cents / a year

Cost Benefit Analysis

Valuing people's time at twice minimum wage: \$7.25.

It doesn't make sense for the average user to spend more than 2.6 mins per year, looking at URLs.

Maybe the users aren't so stupid after all.

Back to Certificates

What is the point of certificates in SSL?

- There is no evidence of large scale, active MITM.
- Phishing sites don't use fake certificates

Fake Certificates

There is no record of major financial lost due to fake certificates.

- Almost all certificate alerts are false positives.

Cost of checking a certificates: 10mins, once every 2 years, for 180 million people, at twice min. wage = \$108.7 mil

Some Warnings:

- I'm not saying don't look for a correct certificates. I'm saying this is a design mistake in SSL.
- Does 10 minutes really cost \$1.21?
- Costs calculated like this are very rough, and may totally change over night.

Some Warnings:

- Some groups of people are much more likely to be targeted e.g.
 - people with financial or government information
 - last spring, Syria used fake certificates to access dissidents Facebook accounts.

Recommended Paper:

“So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users”

By Cormac Herley

Conclusions

- The easiest way into any system is usually to exploit human factors.
- A good security policy can help, but a bad policy can makes thing worse.
 - Users want to get their work done, and will find a way around a policy if it stops them.
 - Users are sometimes “right” to ignore security advice.