

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

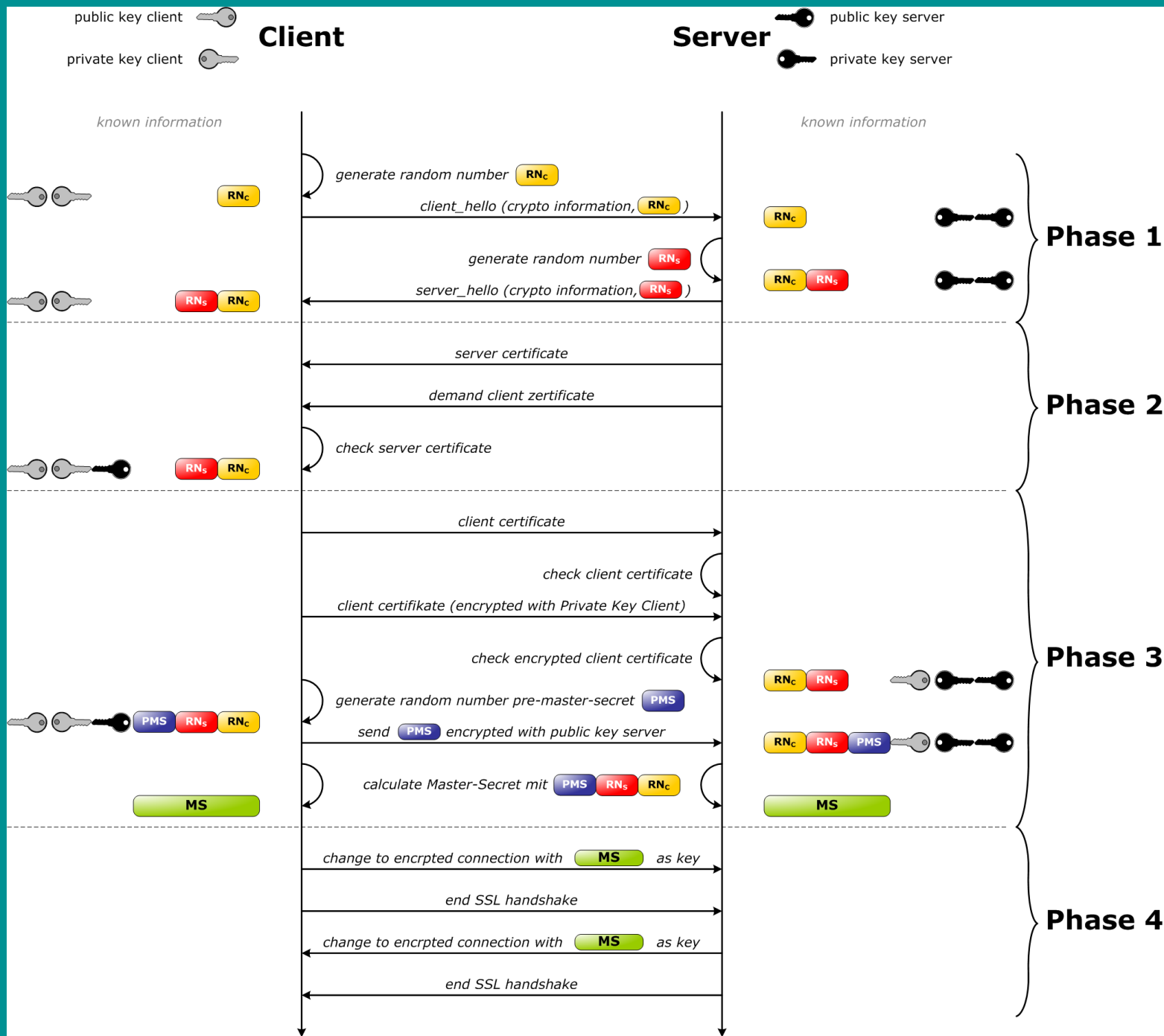
The image shows a screenshot of a web browser displaying the Halifax online banking login page. The browser's address bar shows the URL https://www.halifax-online.co.uk/_mem_bin/formslogin.asp. The page features the Halifax logo with the tagline "a little extra help" and navigation buttons for "Home" and "Help".

The main content area is divided into two primary sections:

- New to Online:** This section includes a "SECURITY GUARANTEE" icon and instructions to complete the registration process. It offers two stages: "Stage 1: Register my details" with a "Start registration" button, and "Stage 2: I've received my temporary password" with a "Complete registration" button. Below this, there is a link for "Employee Share Scheme Customers" to register for Employee Share Schemes.
- Sign In:** This section contains input fields for "Username" and "Password", followed by a "Continue" button. It also includes a "Remember my username*" checkbox (which is checked) and a note: "*Do not select if this computer is used by anyone else. [More information about storing usernames](#)".

At the bottom of the page, there is a "Useful info" section with links for "IMPORTANT INFORMATION: Email Scams & Pop-ups", "Online Banking Demo", and "Apply for a new account". To the right, a "Problem signing in?" section provides links for "Forgotten sign in details / access suspended?", "Why we're changing your sign-in process", and "Are your phone details up to date?".

A large orange banner at the bottom of the page reads: **NEW, EASIER TO USE ONLINE BANKING SERVICE**. A small thumbnail image of the account page is visible in the bottom right corner.

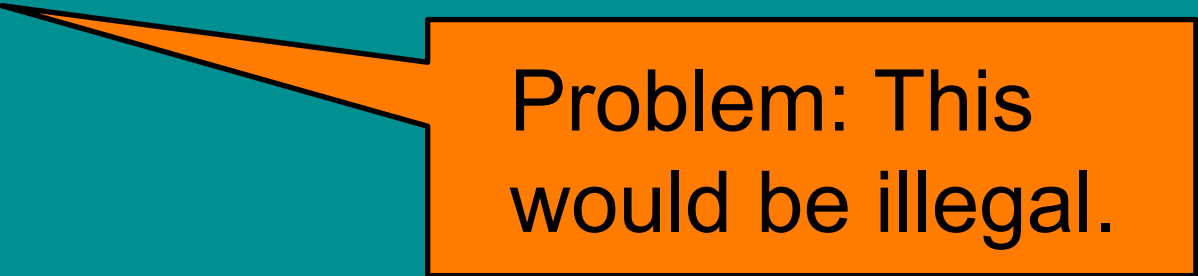


Cranor et al.'s Crying Wolf: An Empirical Study of SSL Warning Effectiveness.”

A scientific test of how users react to certificate warnings.

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

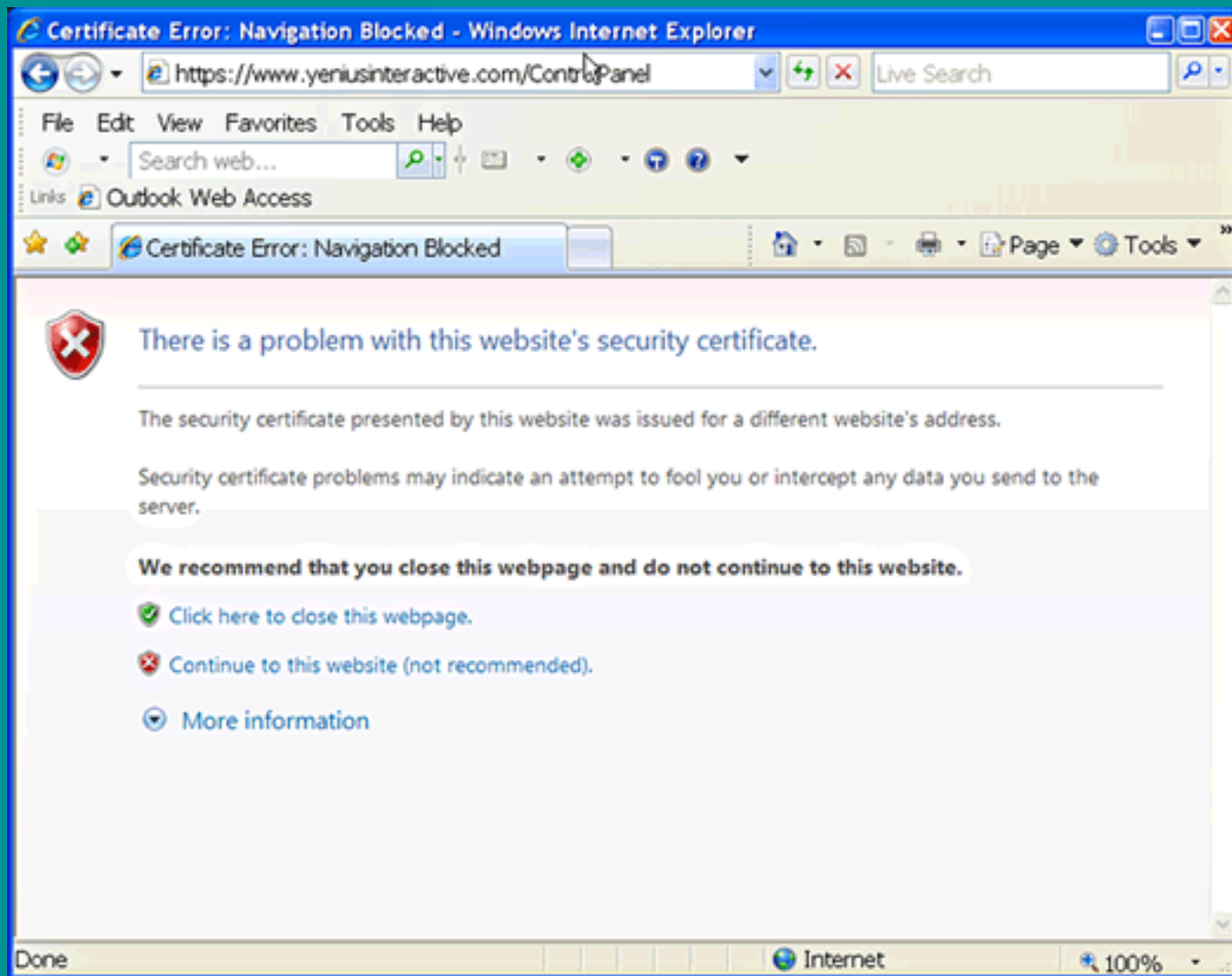
Use a web proxy to do a man in the middle attack.



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.



Security Error: Domain Name Mismatch

You have attempted to establish a connection with "www.whitehouse.gov". However, the security certificate presented belongs to "a248.e.akamai.net". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.

If you suspect the certificate shown does not belong to "www.whitehouse.gov", please cancel the connection and notify the site administrator.

View Certificate

Cancel

OK



This Connection is Untrusted

You have asked Firefox to connect securely to **webmin.nicola.textdrive.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

▼ Technical Details

webmin.nicola.textdrive.com uses an invalid security certificate.

The certificate is only valid for *.textdrive.com

(Error code: ssl_error_bad_cert_domain)

▼ I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...

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

Continue

You are seeing this warning because the response contained a [self-signed certificate](#).



High Risk of Security Compromise

Your connection to *cameo.library.cmu.edu* is either being intercepted by another party or someone is impersonating *cameo.library.cmu.edu*.

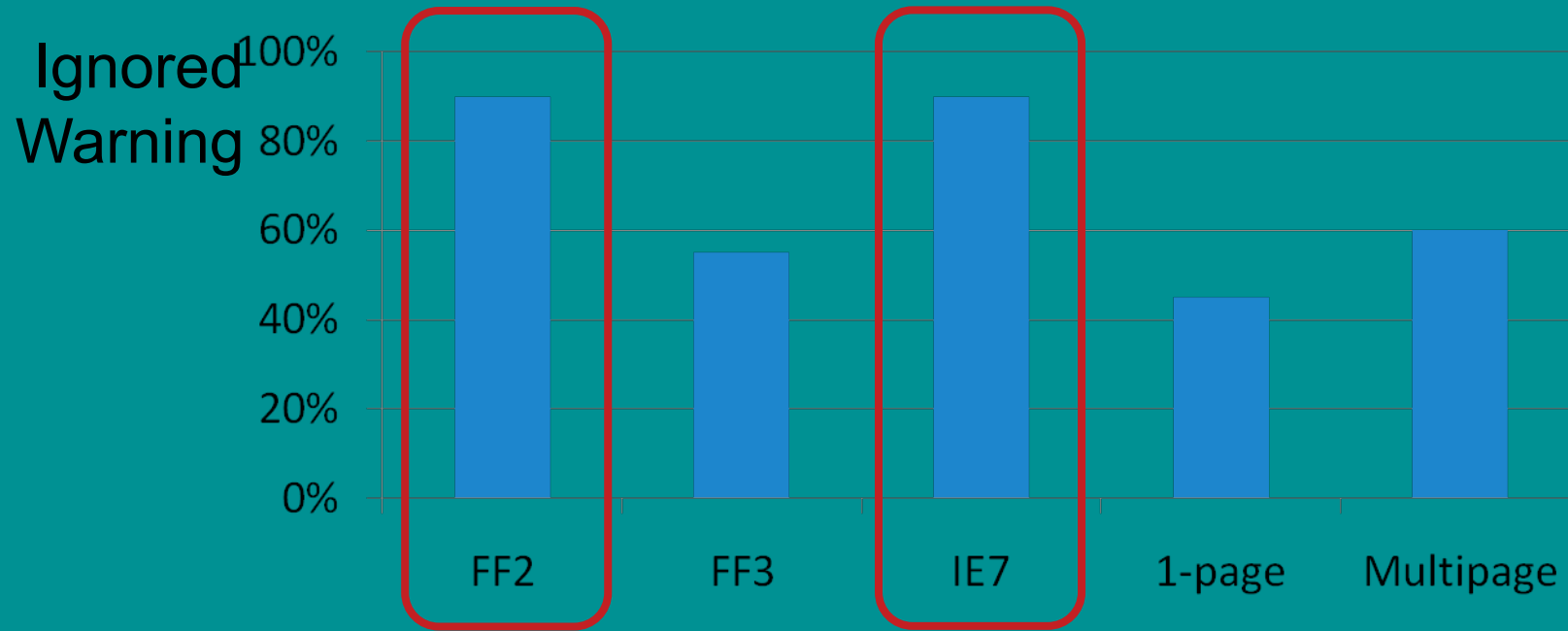
An attacker is attempting to steal information that you are sending to *cameo.library.cmu.edu*. We advise you to contact this company by telephone or using a different computer that does not yield this warning.

Get Me Out of Here!

Why was this site blocked?

[Ignore this warning](#)

Bank results



- In risky situation, significantly fewer people heeded IE7 and FF2 than other warnings

Library results



- In low risk situation, almost all users overrode warnings except in FF3 condition
- FF3 has 4-step process to override warnings



Image courtesy of Johnathan Nightingale

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=Xm4qjtrmGjM&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:

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


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

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


Example: Checking the URLs

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

Which of these URLs belongs to paypal?

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

www.palpay.com

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.