

Phishing, Spoofing In-Flight Editing

Ken Birman

OK, we can build a PKI...

- Can we use it to create a secure banking platform?
 - Better hope the answer is yes!
 - After all: Most people are already using web banking systems at least to track their balance, and many pay their bills using them too
- Today
 - First look at the kinds of attacks that have been common
 - Then ask if the kinds of O/S mechanisms we've learned about can protect against them

2

Online banking

- Suppose you visit your bank's web site... is it really your bank?
- Common attacks
 - In the field of computer security, **phishing** is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
 - Typically involves email with incorrect hyperlinks



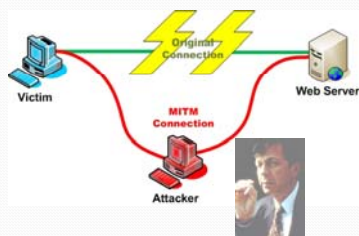
3

Spoofing

- **Website spoofing** is the act of creating a website, as a hoax, with the intention of misleading readers that the website has been created by a different person or organization. Normally, the website will adopt the design of the target website and sometimes has a similar URL.
- For example, a spoofer might try to become a man in the middle
 - Spoofer attempts to log into your bank
 - It passes you the bank's web page, and passes the bank what you type. But it actually sees everything

4

A man in the middle



5


A man in the middle



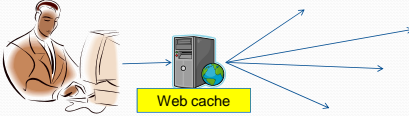
- What could he do?
 - He could "act on your behalf," relaying pages from the bank to you and keystrokes from you to the bank
 - He could modify pages in flight, adding or modifying URLs, tucking Javascript code in spots where you'll run it but won't realize it's running
 - He could just watch
- Clearly none of this is good!

6

Can this really happen?



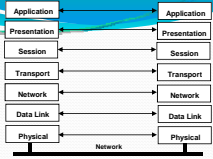
- Man in the middle could be a compromised web proxy (e.g. “pretty bad proxy”)
 - “Normal” proxy caches web pages, for performance
- If a web proxy goes bad, you would want the O/S to warn
 - DANGER: This mail isn't really from afcu.com!
 - CAUTION: This isn't really the afcu.com website!



- Question posed: How well can we do?

7

Layers of insecurity



- Recall that the Internet is
 - Layered: OSI standard...
 - Fiercely end-to-end: Issues like security are left for the end-points to resolve
- Our problem starts with these Internet features
 - If we exchange packets with afcu.org, do we really know we were talking to the right endpoint?

8

Physical insecurity

- At the lowest layer of the Internet are routers
 - When a router boots, a configuration file tells it what IP addresses it should handle directly
 - For example, perhaps this router handles traffic for Cornell.edu
 - Router talks to its neighbors using a protocol called BGP
 - Says “I can reach Cornell.edu”
 - They tell it what IP prefixes they can reach
 - Router blends, sifts, decides how to route packets to the rest of the Internet universe
- Problem?
 - All of this is very trusting! No obvious way to know if someone is lying or malfunctioning

9

Implication?

- In fact, when you talk to an IP address on the Internet, ***you have no way to be sure who you are talking to!***
 - All you know is that the router is sending traffic to some site (perhaps incorrectly)
 - It could even be duplicating the traffic and sending a copy to some other site entirely (basis of NSA covert program called “Eschalon”)
 - Widely reported by cnn, fox, others
 - NSA is apparently “trawling” for interesting web traffic, phone traffic, etc precisely this way
 - Legality not at all clear

10

So much for layers 1-3!

- This is also why spam is so hard to pin down
 - You know that the “From” field of an email can easily be forged – basically, it just contains text
 - But in fact the originating IP address can also be faked!
- Thought question
 - *Why can't we tell that a message has a fake “from” address in it, at the Internet level?*

11

Implication?

- Even something as simple as “afcu.org” poses challenges:
 - How can I know what it's true IP address is?
 - And even if I do know, how can I know I'm really talking to afcu.org and not a middleman?

12

Roll out the PKI!

- Last time we saw a plausible answer to this
 - I trust Microsoft
 - It trusts Verisign
 - Verisign says that such-and-such is a certificate for afcu.org
 - Certificate has a public key in it
- So if afcu.org is for real, I can establish a secure connection to it, right?

13

Trusted Password Window

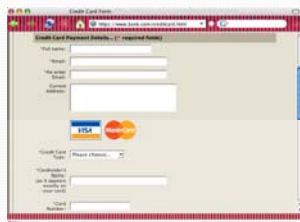


- Dedicated window
- Trusted path customization
- Random photo assigned or chosen
- Image stored in browser
- Image overlaid across window
 - User recognizes image first
 - then enters password
- Password not sent to server

Basis for what are called "Secure browser skins"

14

Browser Generated Images



- Browser chooses random number and generates image
- Can be used to modify border or web elements

15

Server Generated Images



- Server & browser independently generate same image
- Server can customize its own page

16

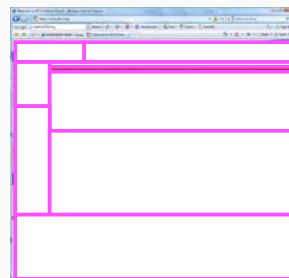
Objective

- With secure browser skins user is sure that
 - His browser is directly connected to afcu.org
 - Login connection isn't passing through a man-in-the-middle
- Key idea:
 - The image is actually split between the machine your browser runs on and the remote web site
 - Transmitted in a cryptographically secure form, combined in the browser itself
 - But user *must remember to check for the picture!*

17

A new issue: Web "frames"

- A web page is really a collection of frames



18

Frame is like a mini-web-page

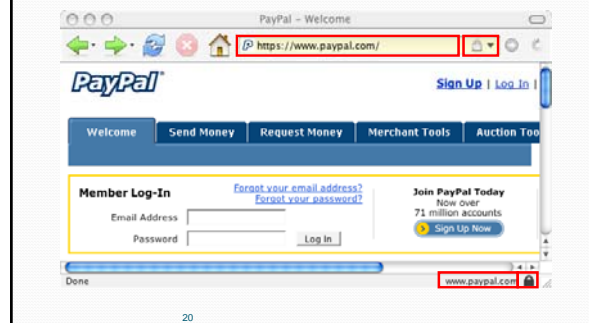
- Each frame has an associated “security context”
 - This is a binding to the web site the frame came from
 - Normally single page won't mix https (secure) and http (insecure) content; if it does, browser warns you
- But there are confusing cases that can be deceptive
 - For example, perfectly `Outer frame https://afcu.org` borders



- On almost all modern web browsers, the inner frame runs in the security context of the outer one! And no security warning occurs

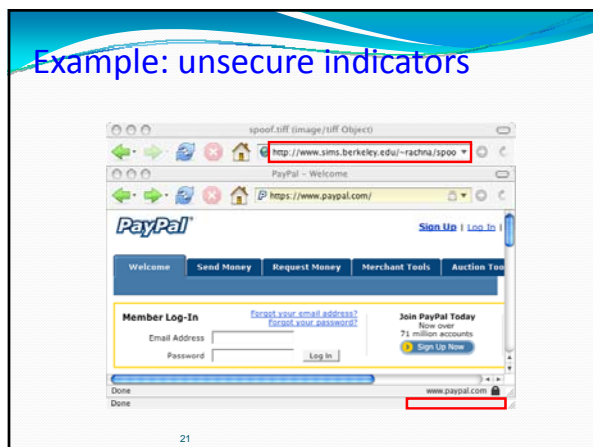
19

Firefox Browser - SSL indicators



20

Example: unsecure indicators



21

Http in Https?

- Web browser designers haven't managed to think of every possible combination of features
 - Afcu.org wanted to provide advertising on their web page for various products from the bank and its affiliates
 - Also wanted to use an external hosting service for some of the image content to speed up its web site
- Constant warnings are a nuisance; people ignore them
 - So... web browsers have ways to mix secure and insecure content without triggering warnings
 - Could be misused by a man-in-the-middle, for example “Pretty Bad Proxy”, a deliberately evil web proxy

22

Consequence?

- You could be logged into AFCU.org securely
 - Yet there could actually be an inner page that looks exactly like the AFCU.org page but is really being relayed via the man in the middle (an evil web proxy)
 - And it gets to see what you type (or fake your actions), selectively routing what it wants to send to AFCU.org or to spoof.com, or even could do both
- Secure browser skins would reveal this attack... but many browsers and sites don't use browser skins
- And this is just one of many such issues

23

Other issues

- Pretty bad proxy could be asked to connect to afcu.org, perhaps even securely over https
 - But it doesn't even try
 - Instead it returns an error code (“site unreachable”) and an error message (an arbitrary Javascript application)
 - The Javascript creates a nested insecure window and connects to afcu.org, showing the response as if it had made the original secure connection
- User sees an error message and yet the window looks right, because browser displays afcu.org welcome screen and it looks normal... so ignores error message
 - Tested... most browsers will malfunction this way

24

Other issues

- Pretty bad proxy can also steal cookies
 - Turns out that when using a proxy, browser sends cookies in the initial connection without waiting to see if the secure SSL handshake succeeds
 - So bad proxy doesn't need to even bother to connect to the remote site
 - Just reads the cookie off the TCP connection
- Now it can forward your cookies to any place it likes

25

Implication?

- Somehow, the mixture of the operating system, the Internet, the web browser, and the web site has left us with a hugely complex, insecure infrastructure
- Yes, we have PKIs and can make secure connections
 - But who made the connection? You, or the middleman?
 - Do we have any reason for confidence that there is a direct connection from you to the bank?

26

More contemporary issues

- Malware:
 - Keystroke loggers: they capture every action you take and relay a script to BadGuys.com
 - Famous example? FaceBook.com "Beacon" online ad placement system
 - Basically, installed an add-on (with your permission) that tracked every action you took, sending records to Facebook
 - Including actions in non-Facebook sites, like gmail
 - Then used this to optimize ad placement

27

More contemporary issues

- Virtual machines
 - We'll discuss in more detail soon
 - Basically, malware "virtualizes" your entire computer
- Applications think they are running on a normal Windows or Linux platform... everything works
 - Perhaps a tiny bit slower than usual for some operations
- But in fact the machine is being watched by the virtualization layer
 - It can, for example, record every bit displayed on screen, every network packet, every file on the disk
 - This defeats secure browser skins unless TPM hardware is used

28

More contemporary issues

- Google Voice... the best tool ever for managing your telephone communications..... It manages voice mail, gives free transcripts of calls... includes free voice conferencing, inexpensive overseas calls, and more. You'll also be able to record and store your calls online.
- *But all that information will be routed through Google. Google will know everyone who called you and when they called. They'll have records of your voice mail, and because they offer free transcription, it means they'll have not just the voice, but text of your calls as well.*

[Computerworld 3/12/2009]

29

GPS

- Most telephones and laptops have GPS location chips
 - We use them to get directions
- But this means that the location of the machine can be continuously tracked
- Google (and other companies) will know
 - Where you were. Who was with you. Who you phoned. What you talked about.

30

Opt-In

- We explicitly agree to let Facebook run Beacon or to let Google Voice play these roles!
 - When you think of implications you get outraged
 - But when the “user agreement” pops up you sign without even reading it
- Reasoning? Would Google really be spying on me?
 - Get real!
- But of course some people really *do* spy on others...

31

Major recent spying scandals

- Hackers apparently broke into computer used by Vice President Cheney during 2007
 - And more broadly into a number of military computers
- Corporate espionage increasingly common and serious
 - No need to plant bugs: just bug the guy's computer
 - By some estimates, 70% or more of all computers have at least some form of serious virus/malware on them, and this includes computers used in military and intelligence settings

32

Could we build a secure O/S?

- A major area for research
 - Like it or not, we're displacing medical records, financial systems, corporate activities onto computers
 - We need to be able to trust the solutions
 - Clearly we can't today
- How might a secure O/S work?

33

Start with the TPM

- TPM gives us a
 - Guaranteed “safe” place to store secret keys
 - Way to encrypt or sign data securely
 - Way to execute code that can't be virtualized or spoofed
- Sizer: Nexus kernel
 - A small, easily audited software module that exploits the TPM to offer various services
 - Goal is to know what software is really running on a machine and that you are really talking to that software, not some form of malware spoofing it

34

What makes this hard?

- One issue is the sheer size of modern systems
 - Systems like Windows Vista and Linux have tens of millions of lines of code
 - Internet adds tens of millions of lines more
 - Built by armies of developers, many revisions and patches for every module. Some are “evil developers”
- Effect of this?
 - In some sense, every computer is running a unique mixture of software
 - Even knowing what it runs won't give much confidence!

35

The Enemy?

- We've noticed that ad placement is a kind of economic enemy: creates incentives for companies to spy
- But there are other kinds of actors too
 - Nation-state competitors
 - Russian mafia
 - Corporate competitors
 - Disgruntled ex's
 - Counter terrorism organizations
 - Moms and Dads trying to monitor the sites their little bunny has been visiting...

36

Bugs

- Even with perfect, “clean-room” development
 - Most software remains buggy
 - New software? Perhaps 1 bug per 1000 lines
 - Mature? Perhaps 1 bug in 10,000 lines
- There are also configuration errors, features that can be misused or tricked, and user-approved malware
- So even with Nexus one has to wonder if the problem can actually be resolved

37

Summary

- Phishing and Spoofing are a serious problem
- This problem leads us down a path to a deeper and broader problem
- Only rational conclusion is that the problem just can't be solved today
- So anything we put on computers is at risk and will be at risk for the foreseeable future, like it or not.

38

Who cares?

- The issue is that for cost reasons, banking, medical records, business applications are moving to the web
 - These need to be secure, otherwise crooks will steal your money, sell your medical records to insurance companies and spy on your business transactions
 - Not even clear what things are legal and what aren't!
- Are we actually entitled to privacy on the web?
 - Many people think so... but nobody has yet asked the Supreme Court to weigh in on this
 - Google gathering all the data they can in the mean time


39

Lessig: East code vs West code

- Lawrence Lessig writes about web challenges
- He points out that there is a kind of arms race
 - East code: laws and other regulation
 - West code: technology
- Technology often outstrips the law
- Meanwhile many laws are basically meaningless because unenforceable.

40

West Code runs amok

- We probably all agree that dealing in child porn is disgusting, illegal and should be, too
 
- But suppose that Sheriff Smith seizes your computer on a tip and searches it. He finds offensive content.
 - Can he be sure you put it there?
 - What if your computer was “tricked” into downloading it, for example by a malicious Javascript application, or an evil web site, or a computer virus?
 - Can we hold you responsible if you didn't know you were doing it?

41

East Code Derails

- Congress passes a law
 - “No ISP should transport child pornography images”
- Images on the Internet are
 - Broken into packets: little chunks of data
 - When you see a packet how can you tell what image it came from?
 - Data is also often encrypted
- So: can we hold an ISP responsible for something it didn't know it was doing?



42

Bottom Line?

- Modern web is simultaneously simple... and complex
 - Simple in the sense that we get very sophisticated results from what are basically very simple actions that run fast and in parallel
 - Scale by massive "brute force"
- But on the other hand, it doesn't provide meaningful guarantees
 - We can't really know if things are working correctly
 - Not even a defined concept!
 - And certainly can't preserve privacy, security

43

Bottom Line?

- Yet the world is moving to rely more and more on this insecure, not private, not reliable infrastructure
- Laws can probably help... but beware unenforceable laws that just cause trouble!
- Technology could do better... but for 40 years trends have always favored features first, fancy properties later or never
 - Usually never...

44

Future of Privacy

- Scott McNealy (CEO of Sun Microsystems):
 - *You have zero privacy anyway. Get over it.* [1/26/1999]
- Brian Bershad (Lab Director, Google Seattle):
 - *Everything we do is legal. If you don't like the law, change the law.* [visit to Cornell, 2007]
- Lawrence Lessig (Professor of Law, Stanford)
 - *A free culture has been our past, but it will only be our future if we change the path we are on right now.*

45