Views From The Underground

The Hackers View Of Cyber Threats

Brad “RenderMan” Haines
Hacker / Security Consultant
RenderLab.net, Churchofwifi.org, NMRC.org
render@renderlab.net

United States Military Academy,Westpoint
March 2010
http://www.renderlab.net/projects/presentations

Who Is This Guy?

- Hacker, independent security researcher and consultant
- Edmonton, Canada based, world sought
- Author of “RFID Security”, “Kismet Hacking” and upcoming “7 Deadliest Wireless Attacks” – Syngress
- White hat by trade, Black hat by fashion
- Speak and teach internationally on wireless security topics
- Member of several Hacker Thinktanks

My World

- My world is unlike anything many of you have seen, It’s a frightening place
- 11 Defcons, 5 Shmoocons, 6 HOPE's, 2 SecTor's, 3 Hackcon's, 1 SecVest , 1 CONfidence and a bunch of smaller corporate and regional events
- Been speaking regularly for ~6 years
- Hacking is a way of life for me, met my wife at a HOPE conference (2004)

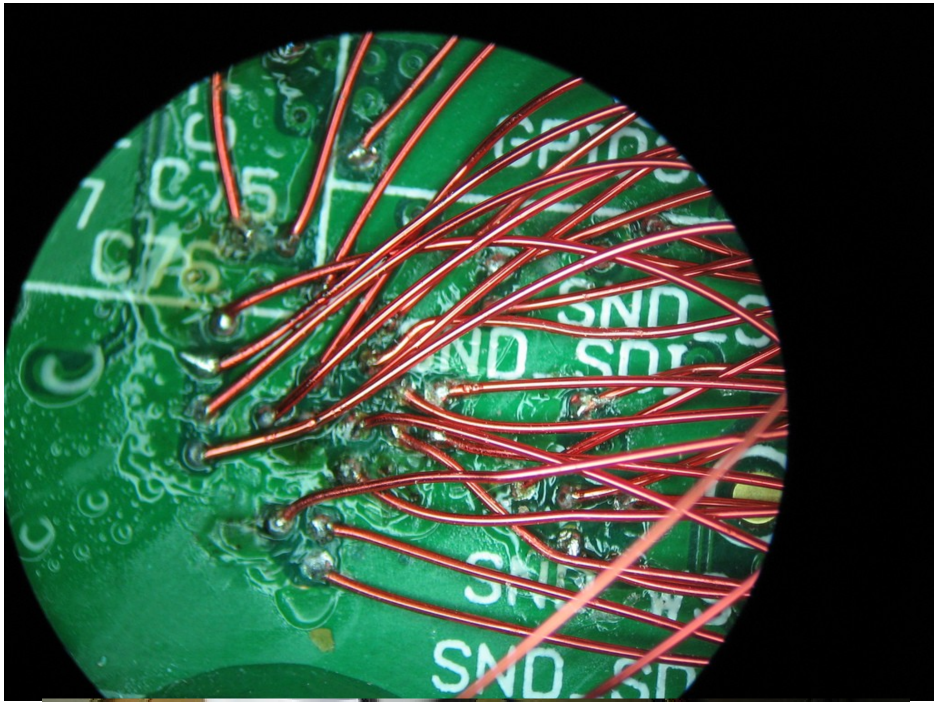
Thinking Security

- Books and classes are great, but have limits
- Defending against the last attack does little to defend against the next
- Thinking like a bad guy does not make you a bad guy, just an informed defender
- Anyone says that 'your secure' is lying, they just have'nt found the hole yet
- You are > 100ms away from every jerk in the world

Attackers

- No longer the 'Bored Teenager'
- Major financial incentives nowadays
- TJX / Albert Gonzalez
- China/Aurora
- Infinite time, Infinite resources, Infinite patience

What Is This



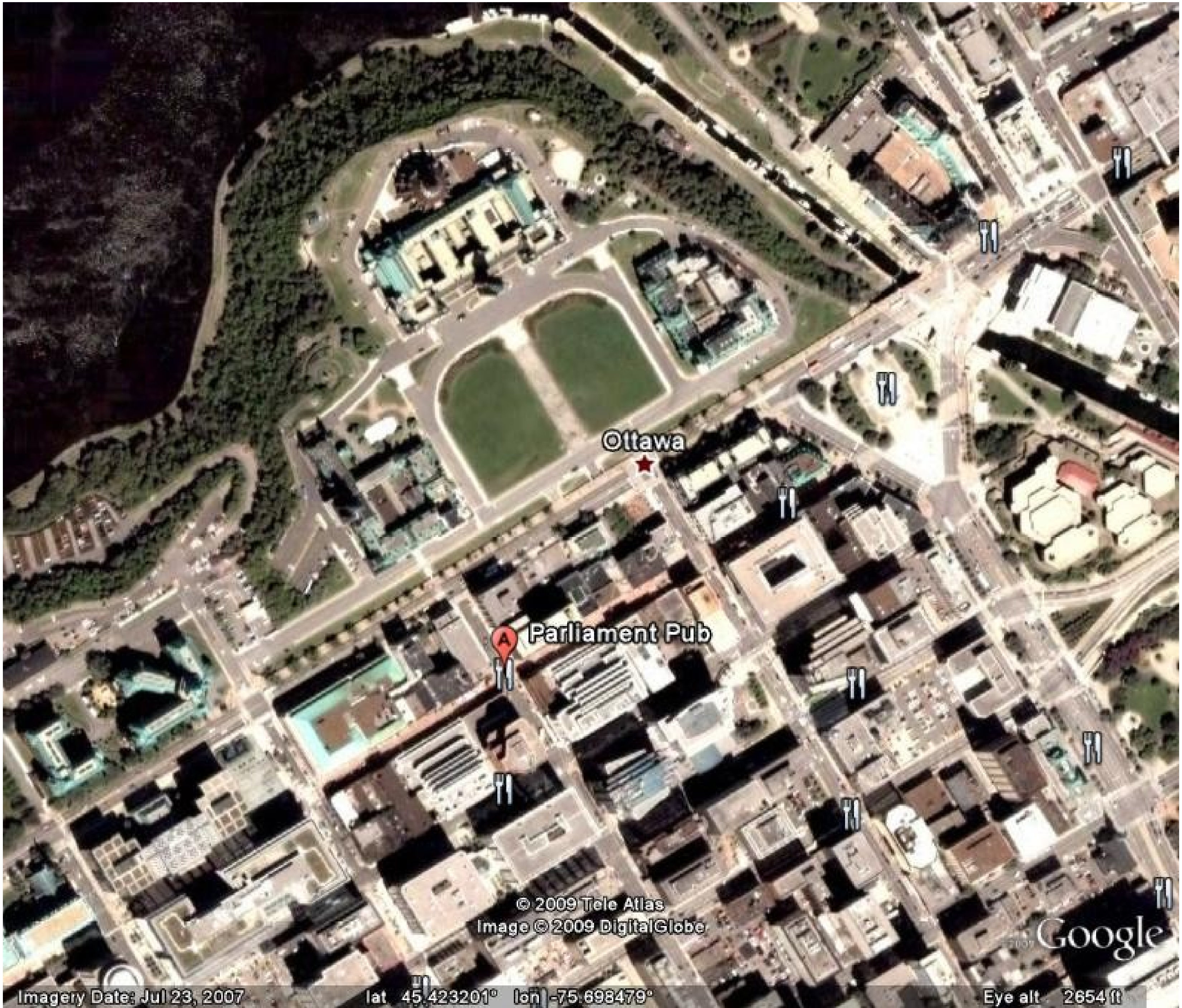
- 0.2mm wires
- Hand soldered to read RAM contents
- FPGA's and custom clock interface
- Any guess what it is?

Nintendo DSi

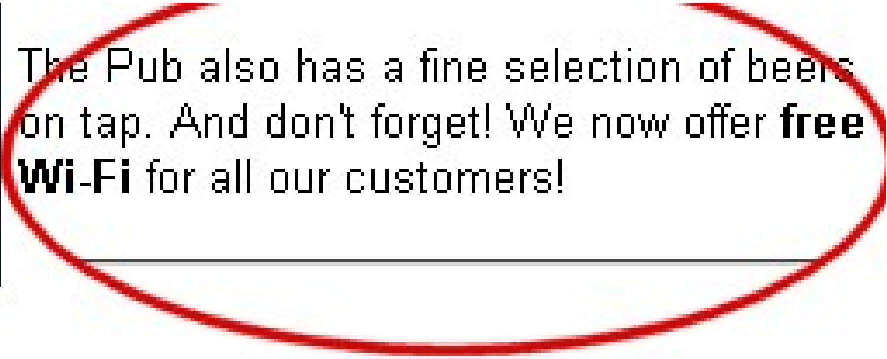
Someone Is Always Watching

- No mater how obscure you may be, someone is watching you and poking
- West Edmonton Mall Warwalk
  - Warwalk one of the worlds largest malls
  - Comparing 2007 to 2009 Xmas shopping
  - No one learned anything from TJX
- Canadian Parliament
  - In Ottawa for conference
  - Decided to have lunch, then take the tour....

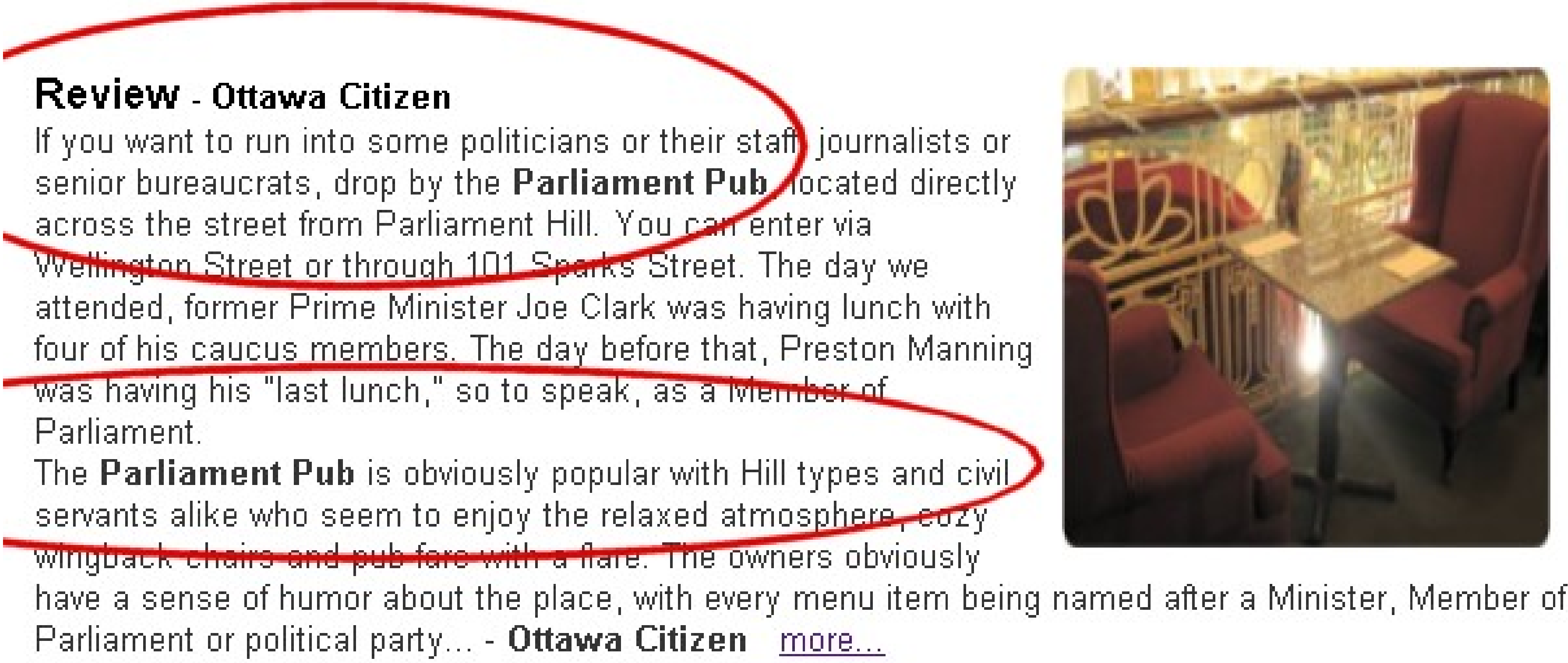
Parliament and the Parliament Pub


Ottawa
Parliament Pub
© 2009 Tele Atlas
Image © 2009 DigitalGlobe
Google
Imagery Date: Jul 23, 2007
lat 45.423201° lon -75.698479°
Eye alt 2654 ft

What's This?



The Pub also has a fine selection of beers on tap. And don't forget! We now offer **free Wi-Fi** for all our customers!



Review - **Ottawa Citizen**

If you want to run into some politicians or their staff, journalists or senior bureaucrats, drop by the **Parliament Pub**, located directly across the street from Parliament Hill. You can enter via Wellington Street or through 101 Sparks Street. The day we attended, former Prime Minister Joe Clark was having lunch with four of his caucus members. The day before that, Preston Manning was having his "last lunch," so to speak, as a Member of Parliament.

The **Parliament Pub** is obviously popular with Hill types and civil servants alike who seem to enjoy the relaxed atmosphere, cozy wingback chairs and pub fare with a flare. The owners obviously have a sense of humor about the place, with every menu item being named after a Minister, Member of Parliament or political party... - **Ottawa Citizen** more...

IT Can Always Get Worse...

- December 2008, 25C3
- MD5 broken for years
- 7 Guys, 200 PS3's create a trusted rogue CA certificate
- SSL could now be spoofed and phishing sites authenticated
- Imagine a well funded team?

All Your SSL Belong To Them

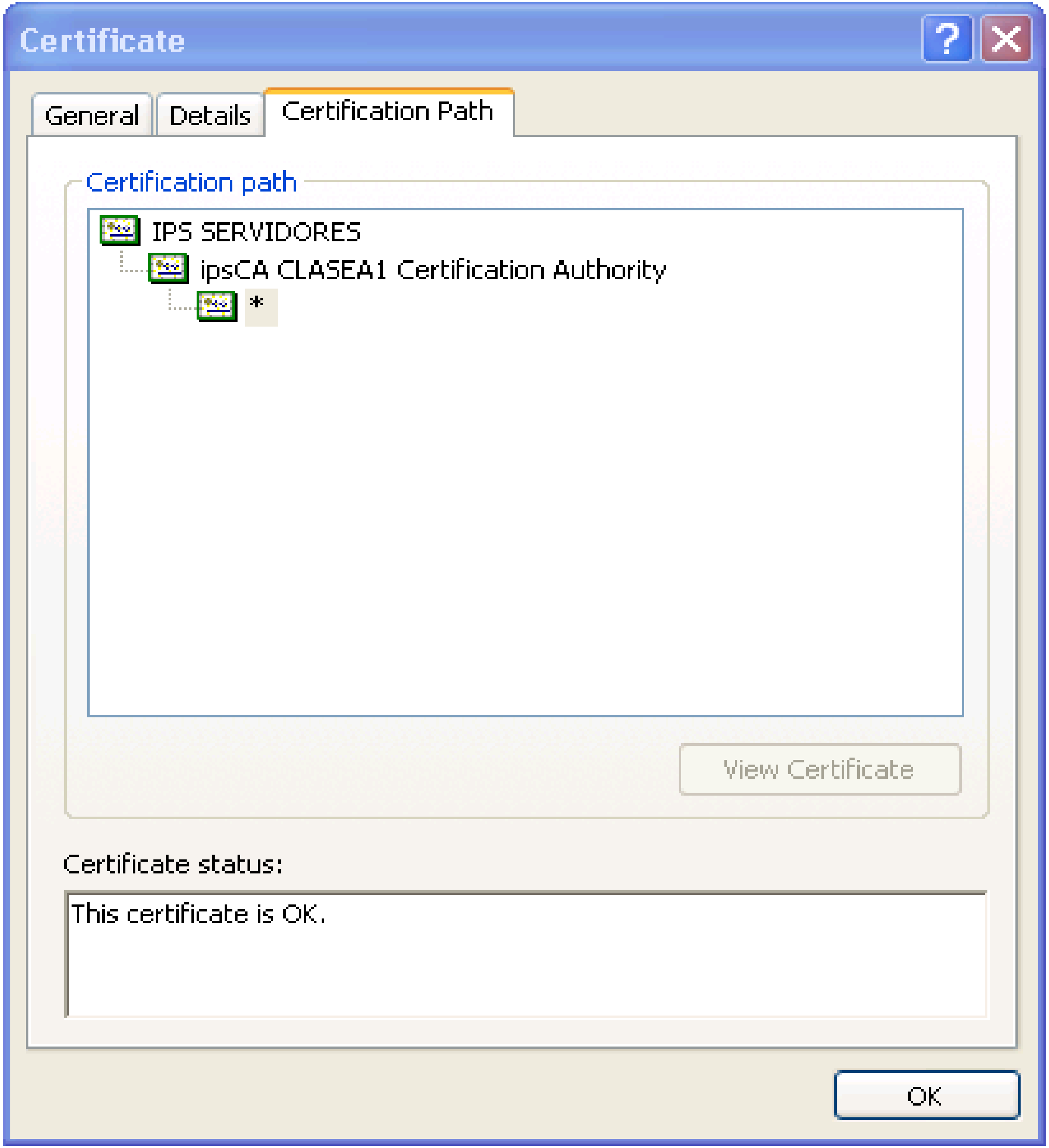
- Took several months of work but broke a fundamental trust needed for SSL to work
- Independent researchers who came forth and went public responsibly
- Imagine a well funded team from a small country with bad intentions...
- Demo cert was backdated to make it useless
- http://www.win.tue.nl/hashclash/rogue-ca/
- Still requires a fair bit of work and I'm lazy and want to do more

Marlinspike The Punch

- Moxie Marlinspike – Blackhat USA 2009
- Common name: **www.paypal.com\0.renderlab.net**
- Found that CSR's with null character only the root domain is examined and authenticated - renderlab.net
- SSL/TLS checks the part before the null - www.paypal.com
- This certificate would verify as www.paypal.com

All your SSL belong to him

- It gets better
- Wildcard (*) works too in some situations!
- *\0.renderlab.net is now EVERY site
- Signed, sealed, delivered by a trusted CA
- Have you updated your SSL apps lately?
- Yes this works, Yes it is being fixed, but is *everything* fixed yet?
- What about embedded systems?



IPS SERVIDORES
ipsCA CLASEA1 Certification Authority
*

Certificate status:

This certificate is OK.

All your SSL belong to them

- SSLSniff in a man-in-the-middle can fingerprint and custom target SSL sessions
- Force https to http, Generally breaks SSL
- What about CRL's, don't want our null cert revoked now do we
- SSLSniff intercepts, blocks and replies to OCSP requests with magic response that generates no errors and the browser just accepts the cert
- Anyone know the magic response?

3

We broke what?

- What has done here?
- SSL can be spoofed and silently provide false hope of security
- SSL authentication mechanisms can fail horribly
- Wireless makes this trivial
- Since we can control DNS, SSL, we control E-banking, commerce, secure mail, etc
- That little lock in the browser means bupkiss

Marlinspike The Punch To The Gut

- Moxie is at it again
- Next logical progression in WPA cracking
- Amazon EC2 'cloud computing' + WPA cracking software + $35 = Test WPA-PSK against 135 million words in ~40 minutes
- How good do you think your password is?
- Imagine a determined attacker with $100, $1000, $10,000 for cloud computing power?
- Supercomputing power available to the masses
- I bought Moxie a Reindeer Steak as Thank You

Hackers are people too

- Basement researchers are less likely to issue press releases
- They do it because they love it
- Not motivated by money, politics or duty
- The thrill of the hack, doing something deemed impossible
- “It's not what you know, it who you know!”
- Knowing who to talk to is half the battle
- We share info freely, (mostly) regardless of company affiliation, nationality or anything else

Conferences

- Conferences are a great place to make contacts
- Talks are good, but the best information isn't apparent
- Often good info is left out due to policies or politics
- Buy a speaker a beer (or 7) and get the digest version of a talk plus the really good stuff
- Random conversations can reveal work in progress and research of directions and what you need to worry about

Conferences

- A few random thoughts
  - “I drink, therefore I am” - The beer economy
  - Never volunteer for Kaminsky wrangling
  - Research speakers ahead of time, find them offstage
  - Ignorance is corrected, stupidity is punished
  - There is always someone smarter than you
  - Chaos breeds creativity, go with the flow
  - Do not use the network unless you know your #@$#
  - Patch everything and cover your ports
  - Always bring a soldering iron to the bar!

Threats

- The greatest threats are those you don't know
- Often vendors are the sole source of threat intelligence and mitigation
- Day to day mitigation is important, but accurate and timely intelligence or new threats is critical
- 'Open Source' Intelligence
- Best intelligence is from a bottle of beer
- Listen to the little people, give them a direct communication channel

My World

- I deal alot with medical facilities
- 1 Billion $ invested in electronic records systems
- Physicians hard to break from paper records
- WiFi + Tablet PC's = easy transition
- This terrifies me to no end
- It's hard to yell from the trenches to the top
- Feel free to scare the hell out of them

“Process Is No Substitute For Understanding”

- Security needs everyone to be involved
- Often security is top down - “Do this because we say so”
- Users can unravel the most complex system if it gets in the way, so get the users on your side
- Reward critical thinking about security, encourage coming forth with issues, don't punish
- Everyone is in this together, understanding “why” goes a long way

“If you can't afford to do it right, maybe you shouldn't do it”

- We can't get web banking right, why do we think we can do it with other stuff?
- “Because it's cool” isn't always an answer
- “Thou shalt be secure” edicts with no help
- There will be pushes for and against projects
- Careful consideration of risks goes beyond the latest whitepaper saying it’s secure
- Why do we run secure systems on hardware made in countries that don't have our best interests in mind?

“Two Things Are Infinite; The Universe And Human Stupidity”

- WEP is dead, the corpse is stinking, bury it!
- Why do I see brand new 802.11n gear installed with WEP (Sept, 09!)
- Who is verifying your security?
- Seek out the real experts, the ones doing the research
- “Security is a process, not a product”, it's constant re-evaluation and refinement
- If someone says you are secure, they are lying, they just haven't found the vulnerability yet
- Mistakes are another name for experience, share them!

Thoughts on what to do

- Hackerspaces – Community workspaces for high tech, high knowledge concentration
- If you have a problem, seek multiple answers including independent researchers
- Consider the implications of what you are trying to accomplish. Should you be trying that in the first place?
- Ask yourself; Do I know enough to do it right the first time?
- Consider that there is always someone looking at everything you do....

Questions? Discussion?

render@renderlab.net