
SecTheory
Internet Security

About Me

- Robert "RSnake" Hansen - CEO
- SecTheory LLC
  - Bespoke Boutique Internet Security
    - Web Application/Browser Security
    - Network/OS Security
    - Advisory capacity to VCs/start-ups
    - http://www.sectheory.com/
- Founded the web application security lab
  - http://ha.ckers.org/ - the lab
  - http://sla.ckers.org/ - the forum

Why?

- Because I use the Internet
- Because I'm a target
- Because most people don't know
- Because it's a fun conversation to have over drinks with security guys
- Maybe/hopefully you'll continue this conversation instead of just arguing!

Ground Rules

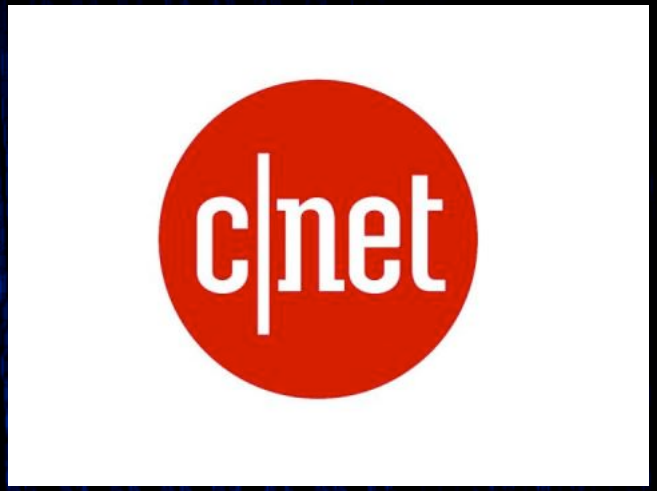
- Must be non-obvious and must be directly related to the Internet. Not:
  - … the President or any other government official
  - … or someone involved with SCADA Systems/Brick and mortar
- Must be in control of some infrastructure or software, etc…
- Must have the largest or widest negative impact possible for the least amount of work and least likelihood of being stopped
- No magic – must be real and dangerous
- They can't be "bad" people
- You can't take this list too seriously

How I Got Started

- Started thinking about core technologies that everything relies on.
- Made a big list
- Shopped it around to dozens of security experts
- Assigned an arbitrary, unscientific, hand-wavy, risk-rating system of my own design
- Ranked them in order of how scary they are to me personally

Let's Do This!

#10



- John Doe at C|Net
- Job: Network Engineer
- Why: Controls com.com
- Impact: Largest collection point of typo traffic both for web and email.
  - csuchico.com story…
  - I have attempted this sort of squatting before with .xn--g6w251d to no avail – very limited possibilities here
  - Doesn't require anything overt or even indefensible.

#9

- Giorgio Maone of NoScript
- Job: Consultant
- Why: Controls NoScript
- Impact: Nearly every security researcher on the planet – complete compromise. In general the most paranoid people on earth would be compromised.
  - Builds arbitrary whitelists (ebay.com)
  - Has changed functionality to subvert Adblock Plus

#8

- Eddy Nigg at StartCom Ltd…
  - or John Doe at SSL Cert Reseller
- Job: Developer/QA
- Why: Has access to create wildcard SSL certs for any domain
- Impact: Would allow an attacker to steal any information they were able to man in the middle.
  - Previously demonstrated bad security
  - Much smaller and therefore less controlled than Verisign or Thawt, etc…

#7

- John Doe at Authorize.net
- Job: Network admin/Server admin
- Why: Has the ability to see the vast majority of online transactions.
- Impact: Would allow an attacker to get PII and credit card information for the bulk of the US online shopping population and many international shoppers as well
  - Just a Merchant Bank
  - Regulated, but not like Visa/MC, etc…
  - Blackmail opportunities galore!

#6

- John Doe at Mozilla
- Job: Has check-in access
- Why: Has the ability to change functionality within the browser, including installing new SSL certs.
- Impact: Would allow the attacker to man in the middle and read all SSL traffic.
  - Almost no documentation
  - The verification process is very open and subject to tampering – meaning the update mechanism isn't probably much better.

#5

- Chirag and Floyd at Adwords
- Job: Whomever checks in code
- Why: Has access to millions of websites because it is XSS
- Impact: Can be leveraged for stealing cookies and hijacking web functionality
  - Is embedded in millions of web pages
  - Is already obfuscated heavily
  - Is seen daily by the bulk of the Internet population
  - Begs the question about CDNs in particular

#4

- John Doe at Google's Postini
- Job: Programmer/Server admin
- Why: Controls and can view the bulk of the world's email - including Gmail
- Impact: Would enable attacker to steal credentials, spoof conversations, tamper with data, introduce malware, etc…
  - More dangerous than Adwords because it's passive
  - Is the biggest in terms of amount of traffic it sees
  - Does tons of processing already and is delegated authority to reject email as it sees fit

#3

- John Doe at 1 Wilshire
- Job: NOC Monkey
- Why: One of the largest peering centers on the west code
- Impact: Can tamper with machines, install malware, inject malicious traffic, intercept communications etc…
  - Most amount of data links in one physical location
  - CIA has already demonstrated interest in choke points using Arbor like infrastructure in San Francisco as outed by Mark Klein

#2

Router	Location	Current Index	Response Time (ms)	Packet Loss (%)
anhm7204.exo.com	California (Anaheim)	84	151	0
mc-gateway.lansmart.com	California (Fresno)	97	28	0
dns-auth1.sys.gtei.net	California (Los Angeles)	99	9	0
rx0ar-technicare.ed.bigpipeinc.com	Canada (Edmonton)	92	78	0
gw02.wlfdle.phub.net.cable.rogers.com	Canada (Ontario)	0	0	100
anguhub14.net.ubc.ca	Canada (Vancouver)	0	0	100
loopback0.gw2.den4.alter.net	Colorado (Denver)	95	41	0
router.firstds.com	Georgia	0	0	100

- John Doe at gtei.net
- Job: Network Admin/Server Admin
- Why: Controls 4.2.2.2 and 4.2.2.3
- Impact: Can be used to subvert a huge chunk of Internet traffic by giving erroneous DNS answers.
  - Used by default in many devices
  - Used by tons of individuals and companies who are lazy
  - Can be used in very targeted attacks for a very short period of time

#1

- John Doe at iDefense
- Job: Security Engineer/Consultant
- Why: Consults for and is owned by Verisign, who owns Network Solutions, who controls authoritative DNS for ".com"
- Impact: Would allow the bulk of the Internet traffic to be modified
  - Heavily monitored and protected but still could lead to temporary and targeted compromise
  - More dangerous than 4.2.2.2 because it controls all of .com and not just a subset of users

Disappointed? Upset?

The List

1. John Doe at iDefense
2. John Doe at gtei.net
3. John Doe at 45 Freemont
4. John Doe at Google Postini
5. Chirag and Floyd at Google Adwords
6. John Doe at Mozilla
7. John Doe at Authorize.net
8. Eddy Nigg at StartCom Ltd
9. Giorgio Maone at NoScript
10. John Doe at C|Net

Questions/Comments?

- Robert Hansen
  - Robert _at_ sectheory d0t c0m
  - http://www.sectheory.com/
  - http://ha.ckers.org/
  - Detecting Malice
    - http://www.detectmalice.com/
  - XSS Book: XSS Exploits and Defense
    - ISBN: 1597491543