DNS: The Internet’s Dirty Little Secret

Day-Con 2007

Angus Blitter

NOTICE

Everything you are about to see, hear, read and experience is for educational purposes only. No warranties or guarantees implied or otherwise are in effect. Use of these tools, techniques and technologies are at your own risk.

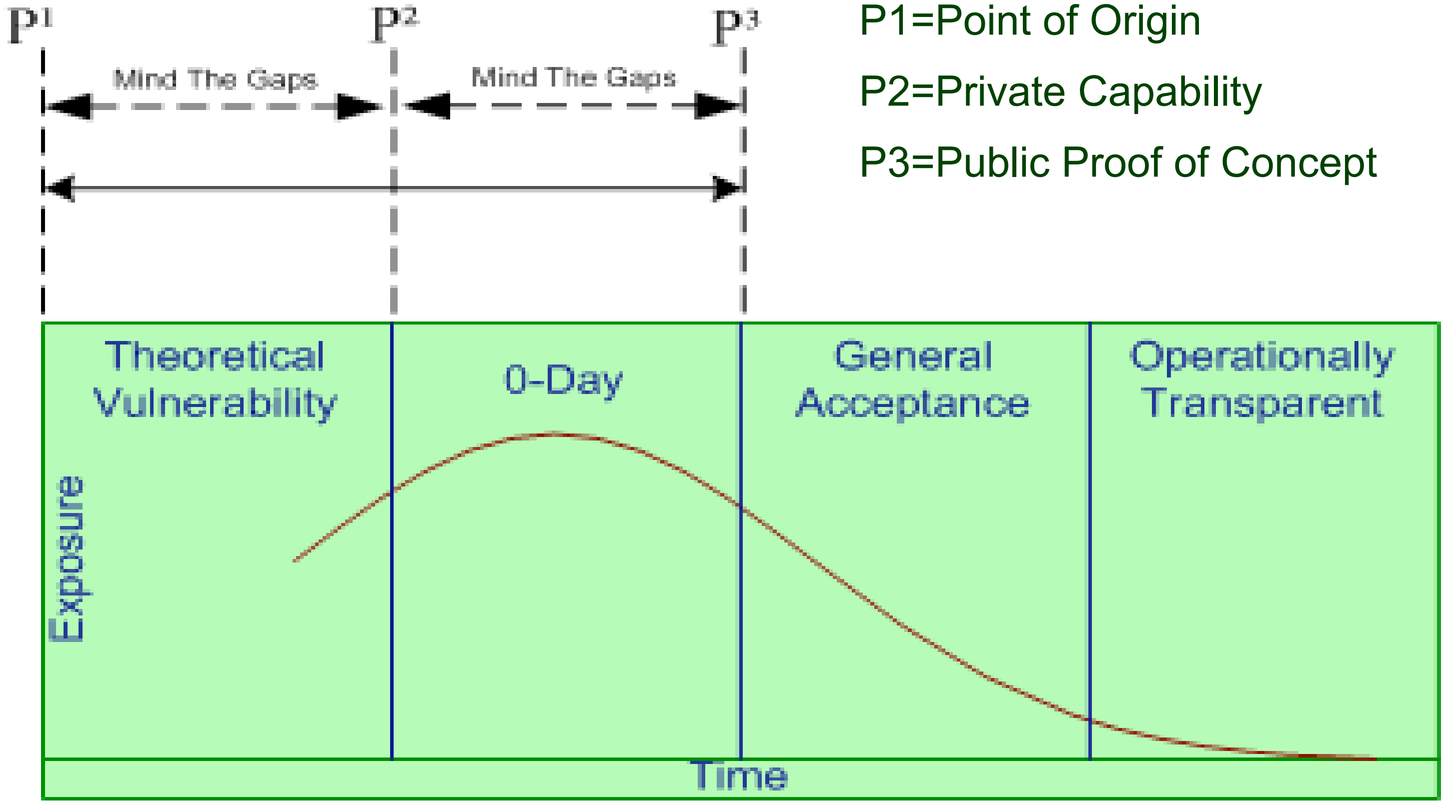
Who Am I?

- Angus Blitter
  - Global Security Architect
  - Veteran Information Security Practitioner, Researcher & Hacker
  - Founder of HACKSEC
  - Media Whore, Ego Maniac or Swell Guy;)

Agenda

- Mind The GAP
- DNS Defined
- Attack Surface
- Seen In The Wild
- Theoretical Vulnerabilities and The Future
- Open Discussion

“Mind The Gap” Series



P1=Point of Origin

P2=Private Capability

P3=Public Proof of Concept

Risk Management

- Risk = Threat * Vulnerability * Cost
- Practical Approach
  - Define Assets
  - Identify Asset Owners & Custodians
  - Assign Asset Value (high, medium & low)
  - Define <u>Relevant</u> Threats
  - Identify <u>Relevant</u> Vulnerabilities
  - Accept, Reject, Transfer or Mitigate

When To Worry?

If an adversary is motivated they will develop or obtain a capability to exploit a vulnerability.

Exposure Index = Motivation * Capability * Vulnerability

Dedication

- This presentation is dedicated to Dan Kaminsky

Yes Dan, DNS is VERY, VERY Interesting and VERY VERY Important!

DNS Defined

- An Acronym: Domain Name System
- Application
- Uses UDP (TCP for Zone Transfers)
  - Connectionless/Unreliable
  - Un-Authenticated (for the most part)
- Critical Infrastructure

DNS Defined

- Serves 4 Basic Functions
  - Lookup - Internet “Yellow Pages”
  - Reverse Lookup
  - Publish Preferred Servers (MX Records)
  - ENUM -mapping single ID to multiple Services (VOIP/SIP/Telephonic Convergence)

Defining The Attack Surface

- Read the RFC's (the theory)
- Identify the moving parts (OSI 1-7)
- Define dependencies
- Compare against reality (layers 8-10)
  - – people: ignorance, sloth and greed
  - – politics: strange bed fellows (agendas)
  - – religion: dogma (it is the way)

Application

- Bugs/Vulnerabilities
  - In the servers (open to the world)
  - In the client
- Stupid Human Tricks
  - Poor architecture (no segmentation)
  - Mis-configuration
  - No PTR records

Application

- Importance of Perspective:
  - on host
  - internal
  - external
- Covert Data Channels (Thanks Dan)
  - OzyManDNS
  - NSTX (IP-over-DNS)
  - DNStunnel.de

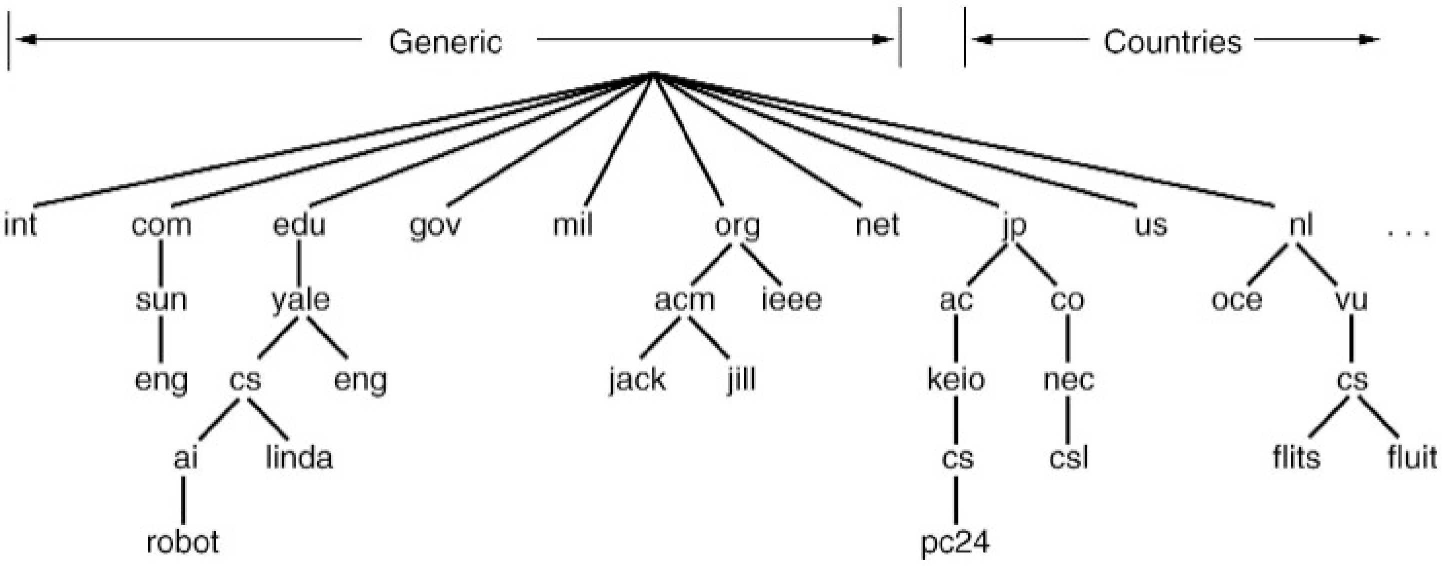
Application

- !!!Blatant Project Solicitation!!!
  - – Windows Executable
  - – Tunnels Any Protocol Through DNS Slack
  - – Transparent To Tunneled Application
  - – Other Features To Be Determined
  - – See me at the after party ;)

Availability & Dependencies

- According to root-servers.org:
  - 117 root servers exist worldwide
  - Operated by 12 different organizations
  - Geographically disproportionate
  - "Governed" by ICANN (Internet Corporation for Assigned Names and Numbers)
  - Top Level Domains (TLD's)

TLD's


Generic
Countries
int
com
edu
gov
mil
org
net
jp
us
nl
. . .
sun
yale
acm
ieee
ac
co
oce
vu
eng
cs
eng
jack
jill
keio
nec
cs
ai
linda
cs
csl
flits
fluit
robot
pc24

Brand Abuse

- Identity Asset
- G-Commerce
  - Phishing
  - Pharming
  - Fast Flux
- Spoofing

Brand Abuse

- Highjacking
- DNS Pinning (Dan’s Newest Obsession)
  - I don’t understand the practical implications but if Dan is interested it probably is important!
  - Involved TTL & browser caching

DNS Scanning

- Sony Root Kit (Way to go Dan)
  - Caching & TTL
- Trust Relationships
- (Business) Intelligence???

Critical Infrastructure

- Availability Dependencies
- DDoS
  - What if everyone thought your web server was google.com?
- "We don't know what it does but the last time we touched it everything broke. So don't touch it!"

Future Opportunities

- DNSSEC
- IPV6
  - Anycast
  - Dual-Stack Stuff (must support legacy)
- Secure & “Aware” DNS Services

Putting It All Together

- DNS is taken for granted but critical
- Very simple functions but many moving parts (complexity kills)
- A changing world (chaos) breeds opportunity!!!

Open Discussion

(Angus at Hacksec dot org)