



WiFi and Network Infrastructure

**MacTech InDepth:
Mobile Device Management
2012**

**Alyssa Robinson
Senior Systems Security
Analyst, The Broad Institute**



Wi-Fi: Guest versus Internal Questions



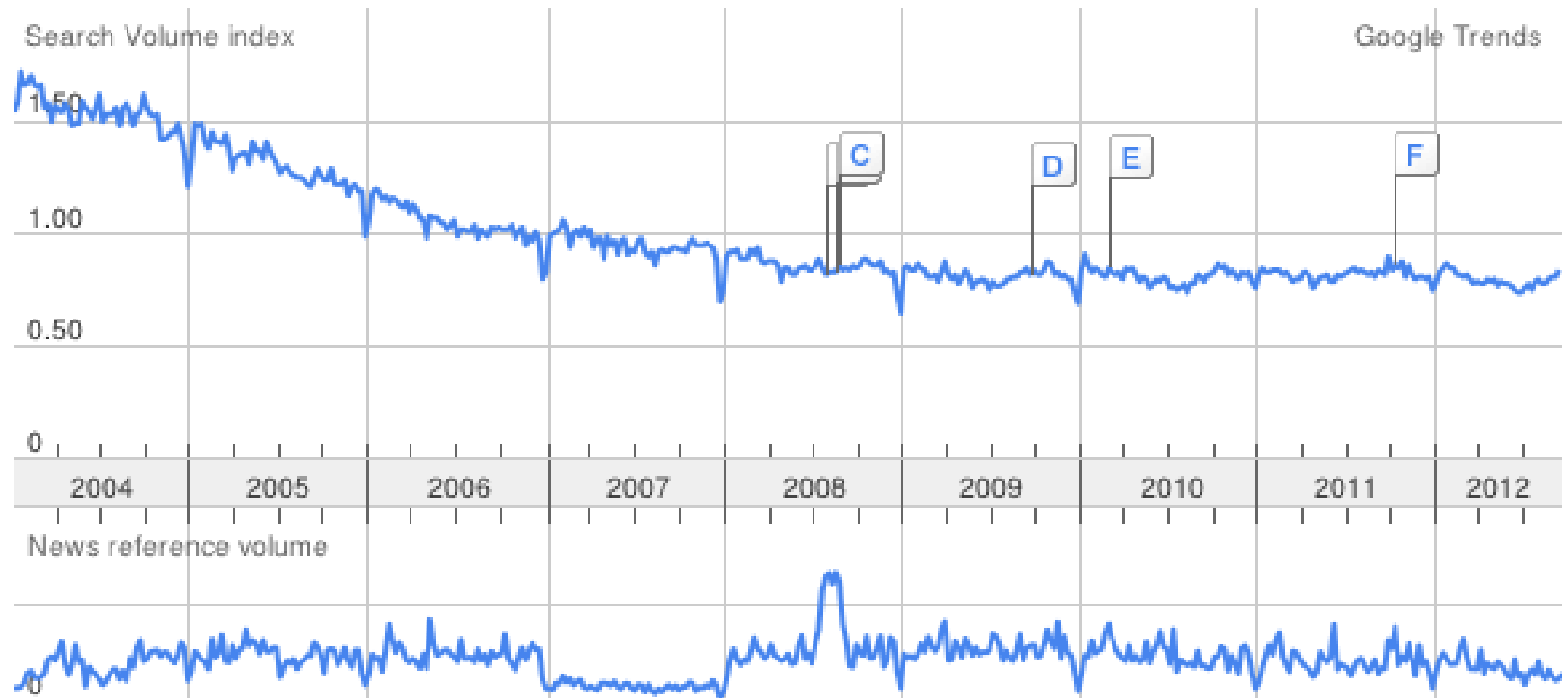
Guest Wireless

- What are the dangers?
- Wide Open, Captive Portal or Pre-Shared Key?
- Services: http/s or more?
- Applications to block
- Logs to keep

Internal Wireless

- WPA2 Enterprise/802.1x
- Full access to Internal network?
- VPN?
- BYOD?
- NAC?





VPN Risks and Counter-measures



- Endpoint security and malware
- Mobile devices
- Data Loss Prevention
- Bandwidth Usage
- Zoning and access lists
- Rogue wireless access points
- Endpoint posture assessment and remediation
- Always-on tunnels or data download prevention
- Next-gen firewall/traffic shaping
- User/group based access control
- IPSec

Bandwidth Managment



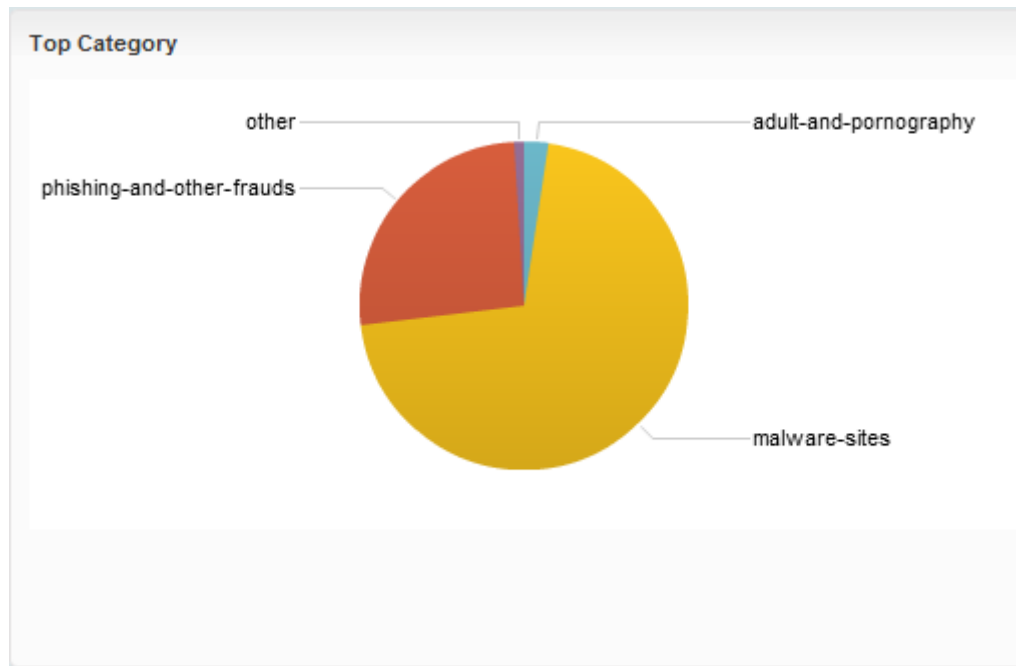
| | Application Name | Bytes ▼ | Sessions |
|----|------------------|---|---|
| 1 | ftp | 253.5 G  | 15.9 K  |
| 2 | ssl | 181.8 G  | 2.3 M  |
| 3 | web-browsing | 88.9 G  | 611.6 K  |
| 4 | ssh | 74.2 G  | 12.0 K  |
| 5 | crashplan | 42.1 G  | 3.5 K  |
| 6 | ciscovpn | 22.3 G  | 1.8 K  |
| 7 | apple-update | 14.5 G  | 7.7 K  |
| 8 | smtp | 12.8 G  | 76.3 K  |
| 9 | gmail-base | 11.3 G  | 39.4 K  |
| 10 | youtube-base | 6.5 G  | 1.4 K  |
| 11 | dropbox | 6.0 G  | 23.5 K  |
| 12 | web-crawler | 5.7 G  | 80.6 K  |
| 13 | dns | 3.4 G  | 2.1 M  |
| 14 | skype | 2.6 G  | 4.6 K  |
| 15 | snmp-base | 2.3 G  | 205.5 K  |
| 16 | flash | 1.7 G  | 4.3 K  |
| 17 | facebook-base | 1.2 G  | 73.1 K  |
| 18 | pandora | 1.2 G  | 5.0 K  |
| 19 | unknown-tcp | 1.1 G  | 1.4 K  |
| 20 | itunes-base | 1.1 G  | 1.5 K  |
| 21 | google-docs-base | 770.0 M  | 16.4 K  |
| 22 | ntp | 586.1 M  | 180.0 K  |

Bandwidth Shaping Choices



- Increase Bandwidth
- Routers
- Next-gen firewalls
- Dedicated traffic shapers

The Web Unfiltered



Web Filtering Technologies



- Endpoint protection suites
- Cloud services
- Content filtering software and appliances
- IPS
- Next-gen firewall/UTM
- Internet Service Providers
- Search Engines

Control 3G, Control Costs

- Amtel TEM/MDM

AMTELnet



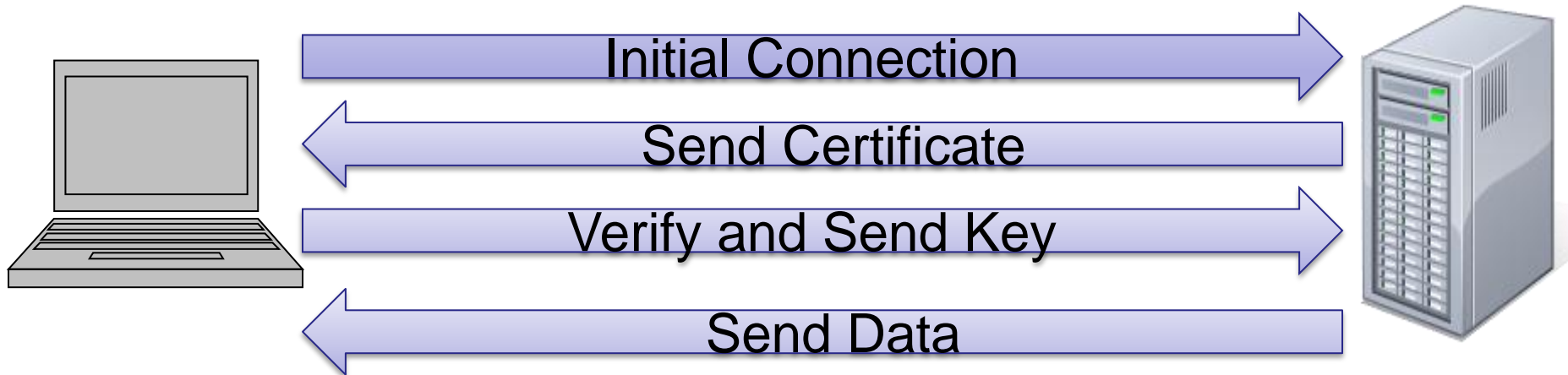
Web Security: Protecting Your Server from the Big, Bad Internet



- Follow established benchmarks:
<http://benchmarks.cisecurity.org/>
- Have good change management procedures
- Log to a dedicated syslog server
- Turn off unused modules (CGI, anyone?)
- Update webserver software and all modules regularly (bonus points for a test environment)
- Vulnerability Scans/Application Security Testing
- Place public-facing servers in a DMZ

SSL Certificates

- Verify Identity and encrypt connection
- Internal webserver, VPN, web mail, IDS or DLP system, e-commerce or any private customer data
- Sign code for download



How do we get one?



- Self-signed, domain validated, fully authenticated, extended validation
1. Generate CSR
 - myhost.mydomain.com
 - *.mydomain.com
 2. Send CSR to your chosen certificate authority (e.g. Digicert, Entrust, Symantec)
 3. Get validated by CA
 4. Install certificate

In Summary



- Lots of new innovations in all areas of networking and security to support BYOD
- So many options, you have to know what you're trying to protect against
- If you don't like it, it will probably be different in a year