Northeastern University

Practical Network Security: Basic Tools & Techniques

Guevara Noubir

Northeastern University

noubir@ccs.neu.edu

Lesson Outcomes: you need to be able to

- Describe and discuss the various security threats to computer networks
  - Recon & Info gathering, Probes & Scans, Network Vulnerabilities, Applications/OS Vulnerabilities
- Describe well known and commonly used techniques for each of the threats
- Describe and discuss defenses
- Practice the tools within laboratory assignments

Reading

- Too many books, forums, websites!

- **Counter Hack Reloaded,** Ed Skoudis, 2006, Prentice-Hall
    - Old but the approach & principles remain the same
    - Many of the techniques or variants still work against many systems specially older technologies recently bridged to the Internet

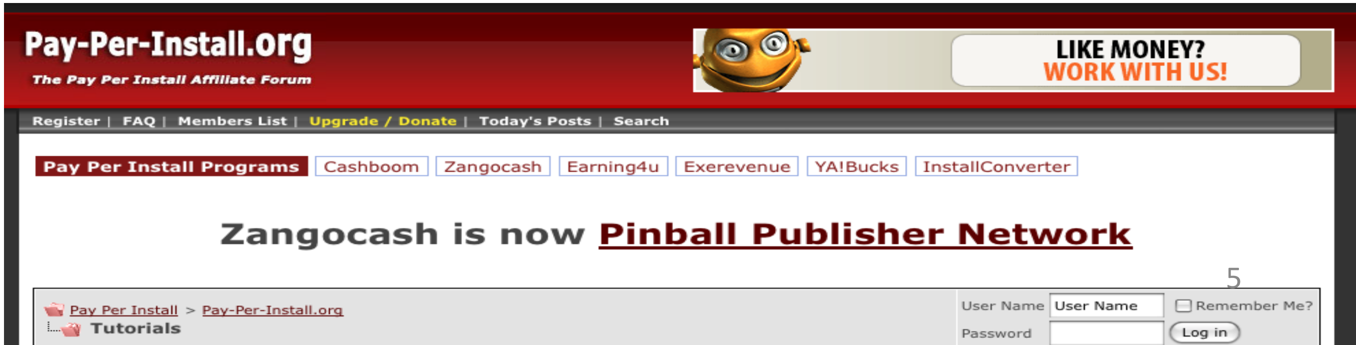
Discussion Points

- Threats: Basic Network Recon and Info Gathering
- Threats: More Intrusive Probes and Scans
- Threats: Network Vulnerabilities
  - Network Architecture Vulnerabilities
  - Denial of Service (DoS)
- Threats: Application/OS Vulnerabilities
  - Remote to Local (R2L) Attacks
  - User to Root (U2R) aka Privilege Escalation
  - Attacker Access Maintenance (root kits, etc)
- Defenses Reviewed
  - Firewalls, Intrusion Detection, etc.

Threats to Communication Networks

- Security was an add-on to many network protocols
- Wired and wireless networks still have major vulnerabilities
  - Motivation evolved from pursuit of fame to financial and political
  - BGP hijacking (e.g., 2005 google hijacking by cogent, 2008 youtube hijacking to Pakistan, 2008 US Universities to Indonesia, 2010 China Telecom, 2014 22 x 30 seconds x 19 ISPs to steal Bitcoins)
  - Viruses, worms and bots are more stealthy today
    - 2008-20015 conficker infected 2-15 million windows servers
    - Stuxnet, Flame targeted worms; Red October
  - Malware led to an underground economy

    “MPack is sold as commercial software (costing $500 to $1,000 US), and is provided by its developers with technical support and regular updates of the software vulnerabilities it exploits.”
  - Ransomeware (CryptoLocker) innovate using Bitcoin and Tor hidden services
  - Embedded systems: Access Points, Target Point of Sale, Cars



Zangocash is now Pinball Publisher Network

Recon & Info Gathering

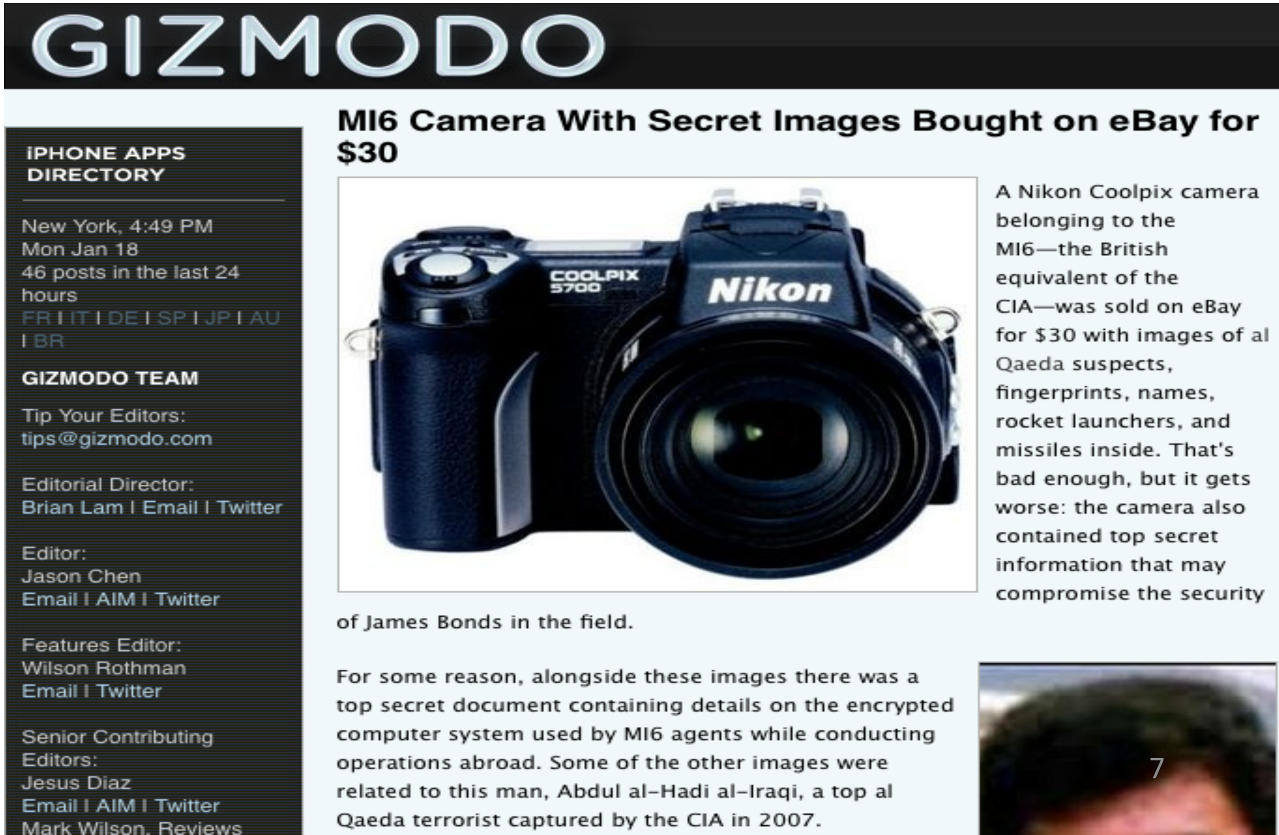
- Social Engineering: “the weakest link”,
  - Physical or automated (e.g., phishing)
  - Defenses: user awareness

  http://www.darkreading.com/security/news/208803583/banking-on-security.html
- Physical Security
  - Physical access, theft, dumpster diving
  - Defenses: locks, policies (access, screen savers, etc.), encrypted file systems, paper shredders

  http://gizmodo.com/5056749/mi6-camera-with-secret-images-bought-on-ebay-for-30
- Web Searching and Online Recon
  - Check company website, get contact names, look for comments in html, etc.
  - Use Search Engines: Google!, forums to discover technologies in use, employee names, etc.
  - Defenses: “Security Through Obscurity”, Policies

Recon & Info Gathering

- Physical security and policies are still a major concern



GIZMODO

iPHONE APPS DIRECTORY

New York, 4:49 PM
Mon Jan 18
46 posts in the last 24 hours
FR I IT I DE I SP I JP I AU I BR

GIZMODO TEAM

Tip Your Editors:
tips@gizmodo.com

Editorial Director:
Brian Lam I Email I Twitter

Editor:
Jason Chen
Email I AIM I Twitter

Features Editor:
Wilson Rothman
Email I Twitter

Senior Contributing Editors:
Jesus Diaz
Email I AIM I Twitter
Mark Wilson, Reviews

MI6 Camera With Secret Images Bought on eBay for $30

A Nikon Coolpix camera belonging to the MI6—the British equivalent of the CIA—was sold on eBay for $30 with images of al Qaeda suspects, fingerprints, names, rocket launchers, and missiles inside. That's bad enough, but it gets worse: the camera also contained top secret information that may compromise the security of James Bonds in the field.

For some reason, alongside these images there was a top secret document containing details on the encrypted computer system used by MI6 agents while conducting operations abroad. Some of the other images were related to this man, Abdul al-Hadi al-Iraqi, a top al Qaeda terrorist captured by the CIA in 2007.

Recon & Info Gathering

- `whois` database via Internic (.com, .net, .org)
  - Publicly-available starting place for determining contacts, name servers, etc.
  - Query listed registrar for detailed who is entries including contacts, postal address, name servers, emails (and formats of email)
  - E.g., use Internic, Network Solutions
  - Also: Use ARIN to find IP blocks for organizations! How about mobile?

    http://www.arin.net/index.shtml
  - Whois tool under UNIX
- `whois` info is necessary but should be limited to required minimum

Recon & Info Gathering

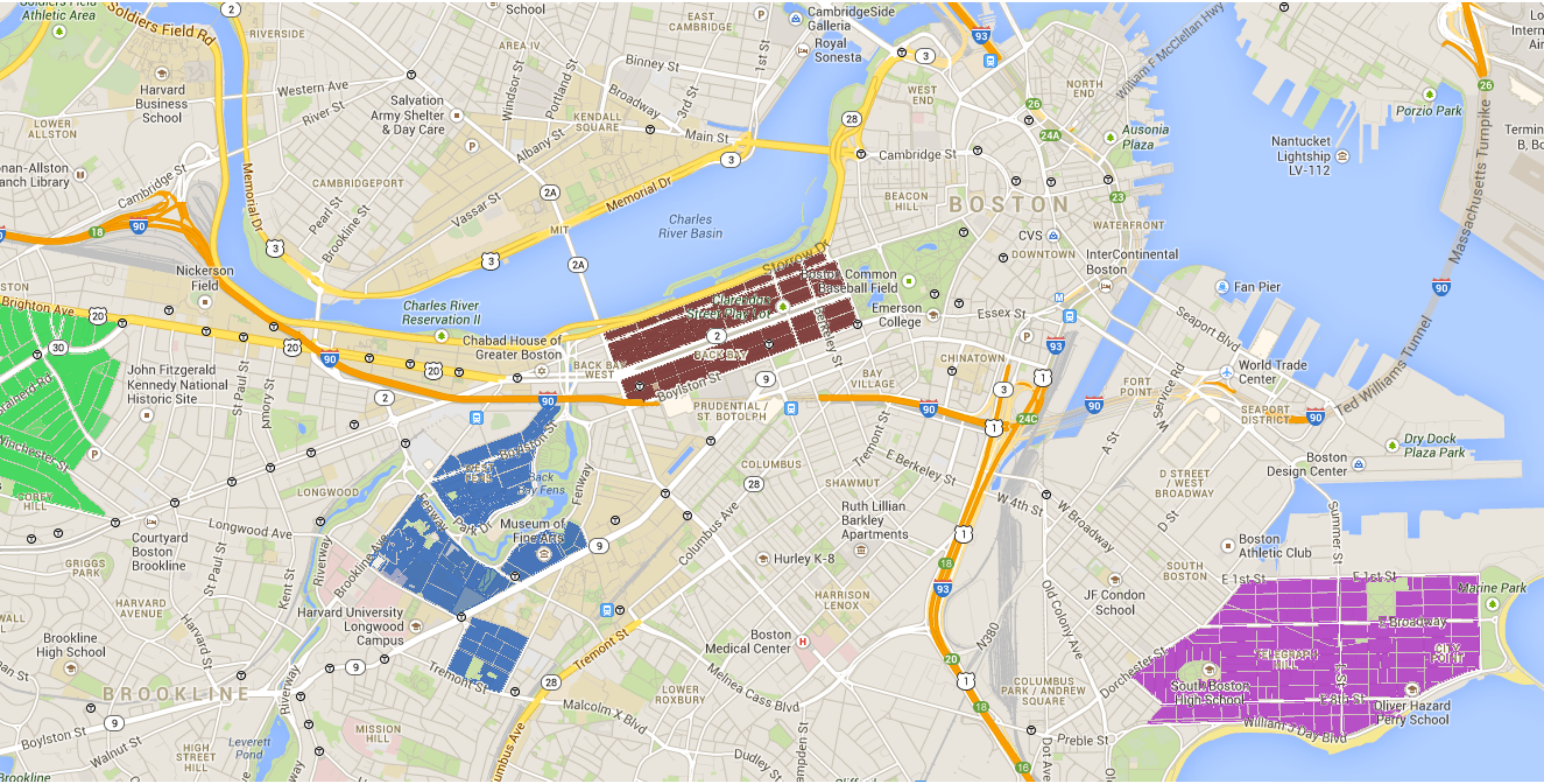
- DNS Interrogation
  - Tools: nslookup, dig, host, axfr
  - Using the name server, do a zone transfer (type=any) to list all public hosts in a domain and more (ls -d x.com.)
  - Defenses: Don’t leak unnecessary info
    - Don’t use HINFO, TXT records at all, limit host names
    - Restrict zone transfers! Limit to only some local machines and/or secondary DNS servers that need it (allow-transfer directive in BIND)
    - Configure firewall to block TCP 53 except to these hosts (UDP used for lookups, TCP for zone transfers)
    - Transaction Signatures (TSIG security) for trusted hosts
    - Split DNS to discriminate between internal and external hosts
      - External nodes only need to be able to resolve a subset of names

Intrusive Scans and Probes

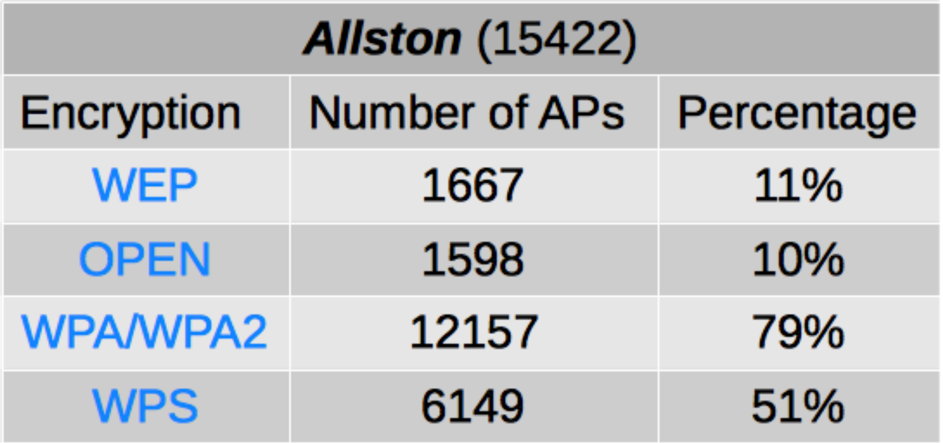
- From Insecure Modems to Insecure Access Points
  - Past: War Dialers (ToneLoc, THC-Scan), Demon Dialers, Rogue RAS
  - Today: War Driving - Rogue and insecure Wireless Access Points [detect RF signal 2Km away using high-gain antennas, NetStumbler, Wellenreiter, kismet, ESSID-Jack tools]
    - Scan of Internet Uncovers Thousands of Vulnerable Embedded Devices
    - https://www.infosecisland.com/articleview/1567-Scan-of-Internet-Uncovers-Thousands-of-Vulnerable-Embedded-Devices.html
  - Defenses: Conduct periodic sweeps/checks, create policies, crypto WPA2/802.1x, VPN, explicitly prohibiting behavior (WEP, TKIP are broken)
- Determine if a Networked Host is Alive
  - ICMP (Ping, Echo Request/Reply) Sweeps
  - TCP/UDP Packet Sweeps ("TCP Ping")
  - Defenses: Configure firewalls, border routers to limit ICMP, UDP traffic to specific systems. Monitor with IDS
  - Problems with these proposed defenses?

Wireless Spreading of Infections

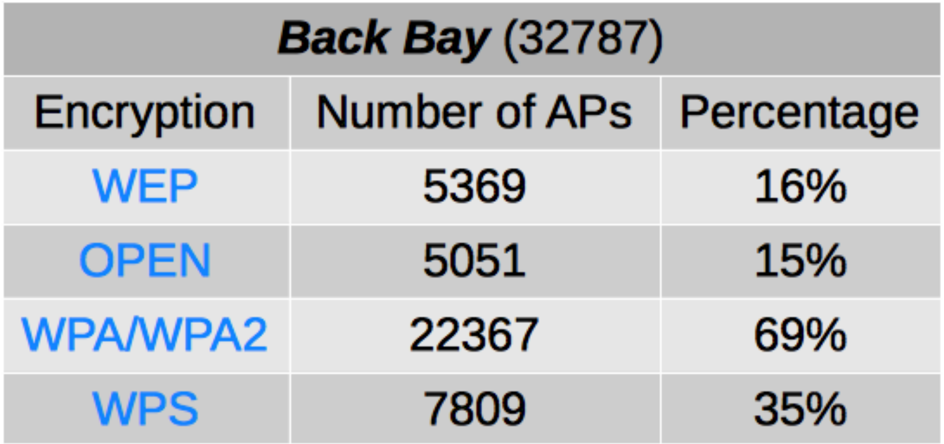
- Wi-Fi Protected Setup (WPS) Flaw



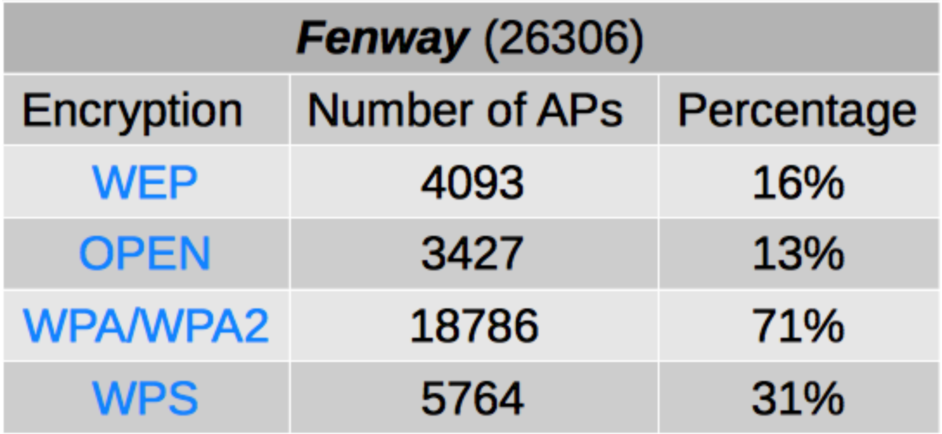
Vulnerability Assessment a Wardriving Experiment



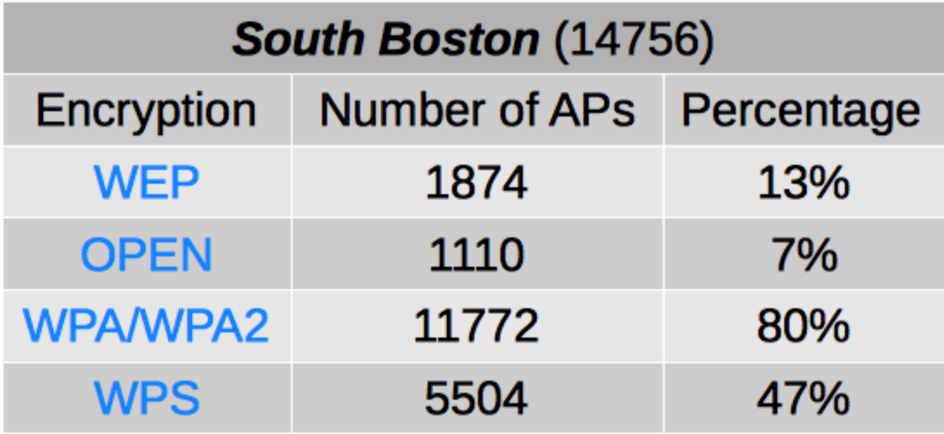
Allston (15422)		
Encryption	Number of APs	Percentage
WEP	1667	11%
OPEN	1598	10%
WPA/WPA2	12157	79%
WPS	6149	51%



Back Bay (32787)		
Encryption	Number of APs	Percentage
WEP	5369	16%
OPEN	5051	15%
WPA/WPA2	22367	69%
WPS	7809	35%

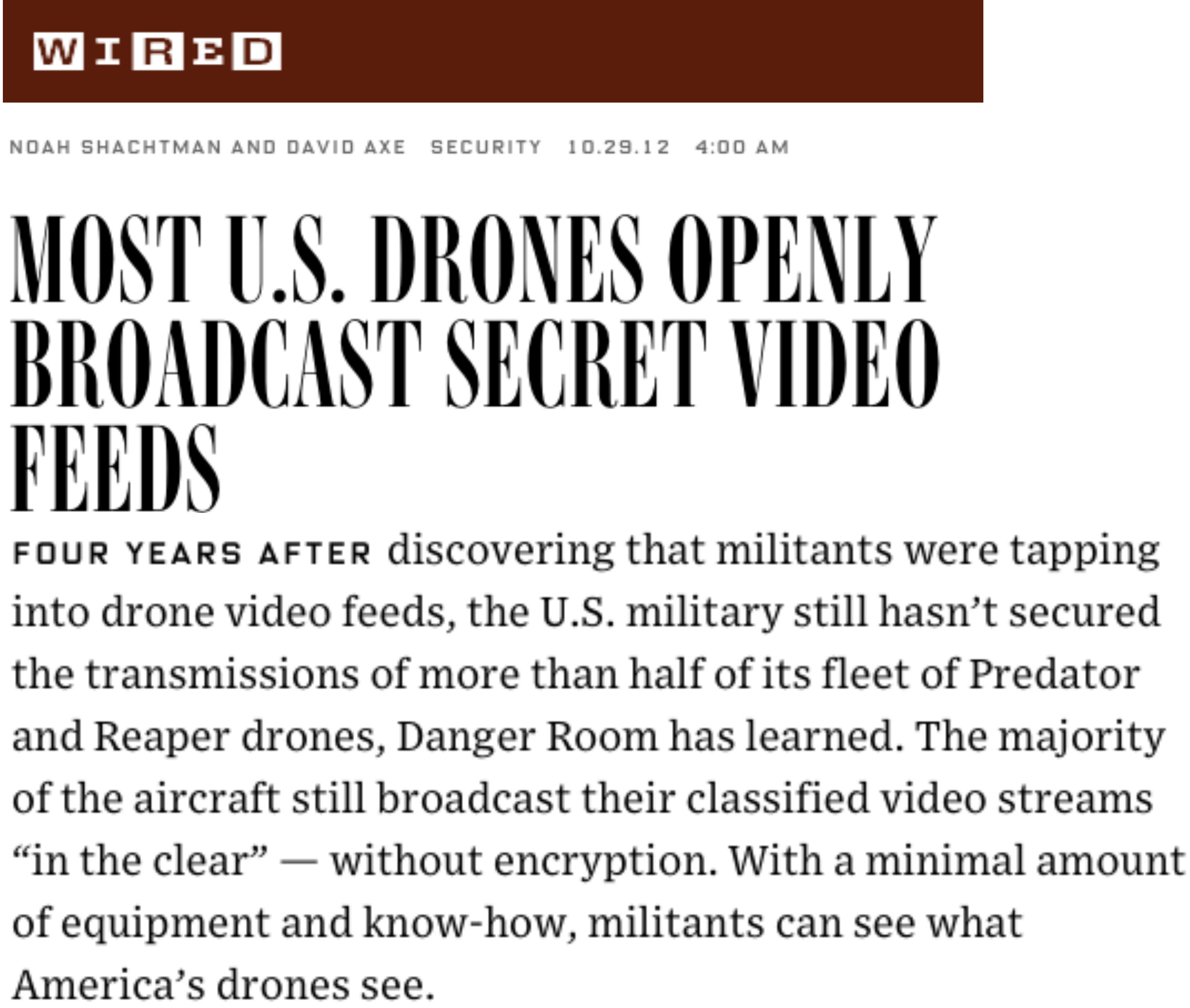


Fenway (26306)		
Encryption	Number of APs	Percentage
WEP	4093	16%
OPEN	3427	13%
WPA/WPA2	18786	71%
WPS	5764	31%



South Boston (14756)		
Encryption	Number of APs	Percentage
WEP	1874	13%
OPEN	1110	7%
WPA/WPA2	11772	80%
WPS	5504	47%

WPS + WEP APs gives a wirelessly connected graph!



WIRED

NOAH SHACHTMAN AND DAVID AXE SECURITY 10.29.12 4:00 AM

MOST U.S. DRONES OPENLY BROADCAST SECRET VIDEO FEEDS

FOUR YEARS AFTER discovering that militants were tapping into drone video feeds, the U.S. military still hasn't secured the transmissions of more than half of its fleet of Predator and Reaper drones, Danger Room has learned. The majority of the aircraft still broadcast their classified video streams "in the clear" — without encryption. With a minimal amount of equipment and know-how, militants can see what America's drones see.

Intrusive Scans & Probes

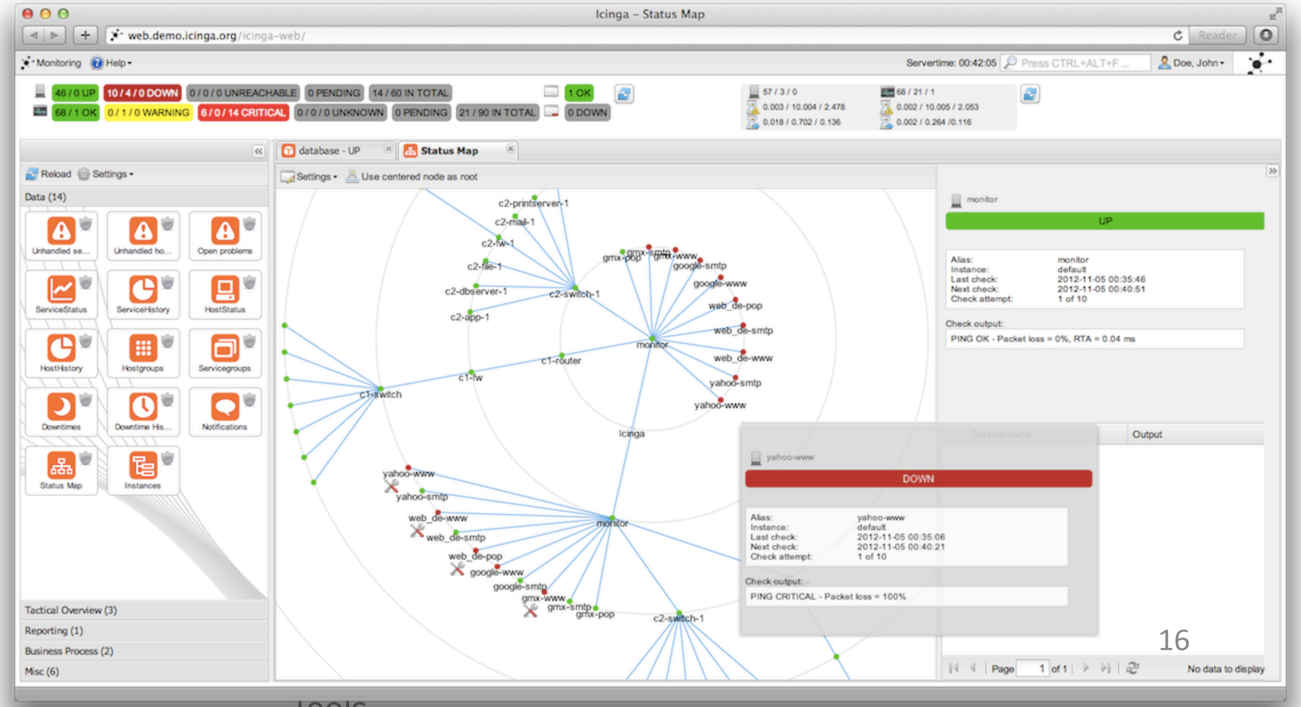
- Port Scanning using `nmap`TCP Connect, TCP SYN Scans
  - TCP ACK, UDP Scanning
  - TCP FIN, Xmas Tree, Null Scans (Protocol Violations)
  - Some sneakier than others
  - Ex: TCP SYN doesn't complete handshake so connect isn't logged by many apps (if open we get SYN-ACK response, if closed we get a RESET or ICMP unreachable or no response)
  - Ex: ACK scan can trick some packet filters. If we get a RESET, packet got through filtering device == "unfiltered". If no response or ICMP unreachable, port is possibly "filtered"
  - Set source port so it looks more "normal" e.g. TCP port 20
  - Use decoys to confuse, idle scanning, Timing Options, Basic Fragmentation

Intrusive Scans & Probes

- Nmap (continued)
  - Combinations of these scans allow NMAP to also perform Active OS Fingerprinting/Identification
    - Based on a database of OS characteristics
    - Also measures ISN predictability (IP spoof attacks)
  - Defenses: tweak logging and monitoring
    - Firewalls/routers should log things like this (e.g. SYN scans) and IDS should note patterns of behavior
    - Use of stateful firewalls for packet filtering?
    - Scan your own systems before attackers do
    - Close ports and remove unnecessary applications: netstat –nao
- All-Purpose Vulnerability Scanners
  - Automate the process of connecting and checking for current vulnerabilities e.g., OpenVAS, Nesssus

Intrusive Scans & Probes

- Rudimentary Network Mapping
  - Use traceroute to determine an access path diagram
    - Different packets may take different routes through different interfaces with different ACLs
    - UDP (UNIX) vs. ICMP Time Exceeded (Windows)
  - Cheops, VisualRoute, NeoTrace, Cacti, Nagios, Icinga
  - Defenses: Limit ping (e.g., webserver but not mailserver or hosts?), filter ICMP TTL exceeded, etc.



Alias: monitor
Instance: default
Last check: 2012-11-05 00:35:46
Next check: 2012-11-05 00:40:51
Check attempt: 1 of 10

Check output:
PING OK - Packet loss = 0%, RTA = 0.04 ms

Alias: yahoo-www
Instance: default
Last check: 2012-11-05 00:35:06
Next check: 2012-11-05 00:40:21
Check attempt: 1 of 10

Check output:
PING CRITICAL - Packet loss = 100%

Network Attacks: Traffic Sniffing

- Sniffing
  - Still lots of unencrypted protocols in common use
    - E.g., predator drones / skygrabber: http://online.wsj.com/article/SB126102247889095011.html
  - Sniffers like TcpDump, wireshark, cain & abel
  - Defenses: Use encrypted protocol replacements
    - E.g. IPSEC, SSH, HTTPS, SFTP, PGP for mail, etc
  - Targeted Sniffers like Dsniff understand specific protocols and can pick out certain types of traffic
    - Passwords in FTP, Telnet sessions, etc
- Sniffing on Switched Networks
  - MAC Flooding results in some switches forwarding packets to all links after its memory is exhausted
  - Spoof ARPs from legitimate hosts to receive their packets, construct a Man-In-The-Middle scenario
  - Dsniff tools with arpspoof, dnsspoof, webmitm, sshmitm
  - Ettercap tool: port stealing

Network Attacks

- Sniffing on Switched Networks (cont'd)
  - Defenses: no hubs, static ARP tables where necessary (difficult to manage), arp poisoning detection, e.g., DMZs, ArpON, DHCP snooping, arpwatch
- DNS Spoofing
  - Multiple purposes: blackholing and set-up for mitm attacks or site redirects to attacker replica
- Do SSH/HTTPS Prevent these attacks?
  - Not necessarily; built on trust relationships
    - Users must be careful to use only HTTPS sites with valid certificates
    - Must watch out for SSH warning messages if keys don't match previously recorded keys
  - These problems allow for man-in-the-middle scenarios

Network Attacks: Remote IP Sniffing

- IP Address Spoofing
  - Simple spoofing: just change the packet's IP address
  - More dangerous: undermining UNIX r-commands (rsh, rhosts), exploiting trust relationships
    - Must be able to predict sequence numbers since attacker never sees SYN-ACK (different LANs)
    - DoS the legitimate host so it can't send RESET
  - Defenses: Make sure sequence numbers are not predictable (vendor patches, etc) don't use r-commands, don't use IP addresses for "authentication"
  - Also: ingress/egress filtering, deny source-routed packets

R2L, U2R Attacks

- Remote 2 Local Attacks: Mostly Buffer Overflows in OS and networked applications
  - Processor and OS-specific
  - Overflow stack, inject shell code to do something
    - Also heap, array, integer overflows, etc.
  - R2L = remote to local;
    - Exploit flaw on remote listening application to obtain local user privileges
  - U2R = user to root;
    - Exploit flaw on system (ex: setuid) for privilege escalation
  - Often, backdoors created via Netcat, TFTP, Inetd
- In-depth discussion out of scope for this presentation, unfortunately but do the labs!

Web-based Attacks

- Web-based flaws important to be wary of
  - Ex: IIS unicode flaws allow attacker to escape web root directory and run a command as IUSR to upload a copy of netcat and send back a shell… (vendor R2L)
- Account harvesting (different messages for incorrect username/password), session tracking (tools: Achiles, Paros),
- SQL Injection
  - Inject unexpected mishandled data into web apps, expanded inside the query for surprising results
  - Example: Poorly constructed SQL queries allow attacker to “piggyback” a query modifier in a POST, I.e. listmyinfo.asp?ID=0;delete from users
- Cross-Site Scripting (XSS)
  - Insert scripted data into web apps, which process and return content containing the scripting (send cookies to a malicious third party, etc.)
  - Persistent (e.g., saved on server and served to users) vs. non-persistent XSS attacks (e.g., script embedded in url sent through phishing, not sanitized by server, executed on browser client)

Example SQL Injection

- C# code to form sql query

```
string query = "SELECT * FROM items WHERE user = ”’"
             + userName + ”’ AND itemname = ‘"
             + ItemName.Text + ”’";

sda = new SqlDataAdapter(query, conn);
```

- If user Tom enters

```
    "name' OR ‘1’=’1"
```

- Query expands to

```
SELECT * FROM items
WHERE user = ’Tom’
AND itemname = ‘name’ OR ‘1’=‘1’;
```

R2L/U2R and Web App Vulnerabilties

- Defenses: Be aware of standard solutions to these problems, rely on "what has come before"
- Defenses: Patch, patch, patch, patch, and detect too
  - Practice responsible coding for security awareness
    - Beware strcpy!
- Defenses: Practice responsible ("safe") coding for security awareness
  - Buffer Overflows: (Example) beware strcpy, monitor mailing lists (e.g., bugtraq), use nonexecutable stack

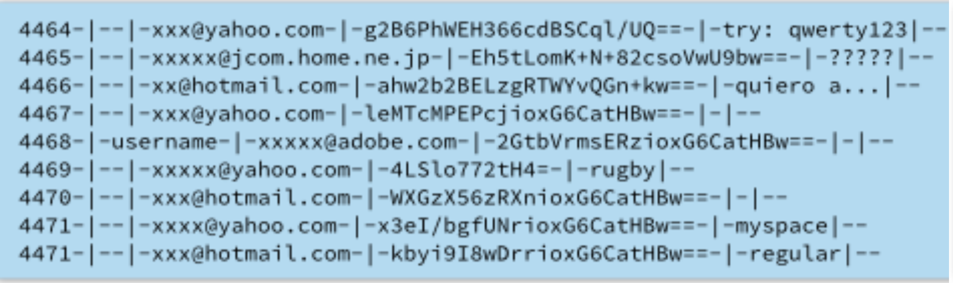
```
dmesg | grep '[NX|DX]*protection'
sysctl -w kernel.randomize_va_space=1
```

  - Web Applications: (Example) Don't rely on hidden fields for data security, used stored procedures with input validation (e.g., quotes escaping)
- Where do attackers go from here?
  - Use this information to get to "the next step"
  - Once rooted, installation of root kits, log cleaners, etc.

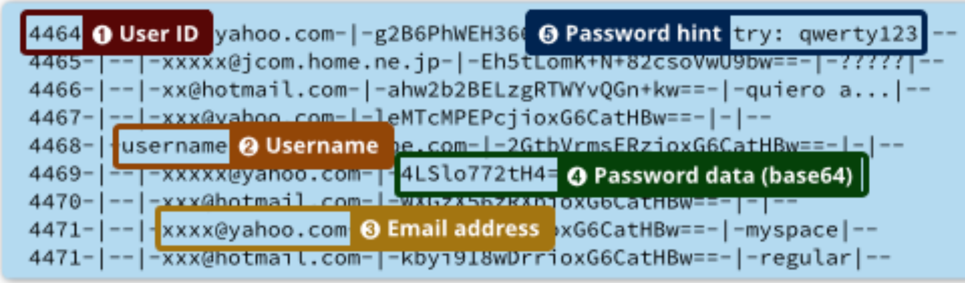
Password Cracking

- Guessing Passwords via Login Scripting
- Better: Obtain Windows SAM or UNIX /etc/password (/etc/shadow, /etc/secure)
  - Crackers: John the Ripper (UNIX), Cain & Abel
- Dictionary vs Brute-Force vs Hybrid methods
- Defenses:
  - Strong password policy, password-filtering sw
  - Conduct your own audits
  - Use authentication tools instead if possible
  - Protect encrypted files (shadowing, get rid of MS LM reps, etc.)

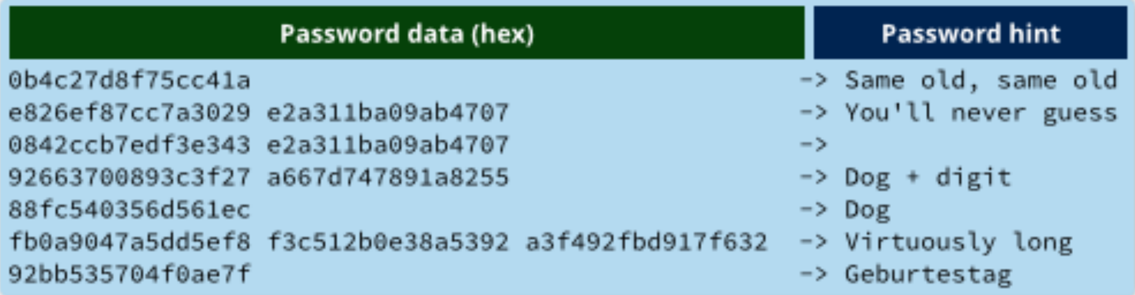
Adobe Breach (October 2013)



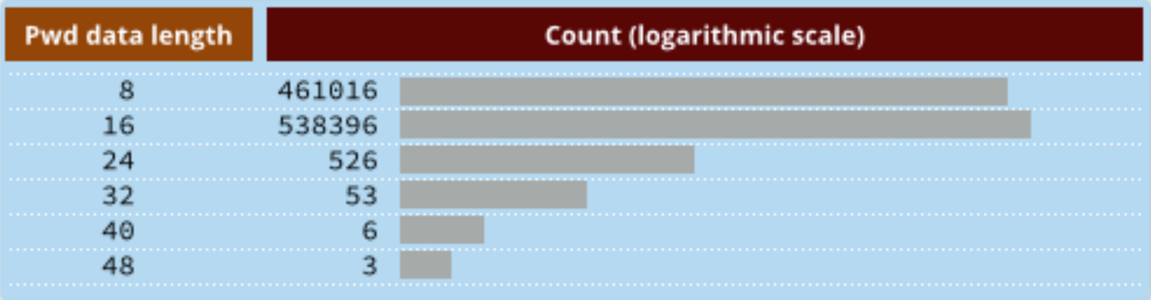
```
4464-|--|-xxx@yahoo.com-|-g2B6PhWEH366cdBSCql/UQ==-|-try: qwerty123|--
4465-|--|-xxxxx@jcom.home.ne.jp-|-Eh5tLomK+N+82csoVwU9bw==-|-?????|--
4466-|--|-xx@hotmail.com-|-ahw2b2BELzgRTWYvQGn+kw==-|-quiero a...|--
4467-|--|-xxx@yahoo.com-|-leMTcMPEPcjioxG6CatHBw==-|-|--
4468-|-username-|-xxxxx@adobe.com-|-2GtbVrmsERzioxG6CatHBw==-|-|--
4469-|--|-xxxxx@yahoo.com-|-4LSlo772tH4=-|-rugby|--
4470-|--|-xxx@hotmail.com-|-WXGzX56zRXnioxG6CatHBw==-|-|--
4471-|--|-xxxx@yahoo.com-|-x3eI/bgfUNrioxG6CatHBw==-|-myspace|--
4471-|--|-xxx@hotmail.com-|-kbyi9I8wDrrioxG6CatHBw==-|-regular|--
```


4464 ❶ User ID
❺ Password hint try: qwerty123
username ❷ Username
4LSlo772tH4= ❹ Password data (base64)
xxxx@yahoo.com ❸ Email address

- Passwords encrypted with 64 bits 3DES in ECB
  - Not hashed, not salted, not in CBC, not AES



Password data (hex)		Password hint
0b4c27d8f75cc41a	->	Same old, same old
e826ef87cc7a3029 e2a311ba09ab4707	->	You'll never guess
0842ccb7edf3e343 e2a311ba09ab4707	->	
92663700893c3f27 a667d747891a8255	->	Dog + digit
88fc540356d561ec	->	Dog
fb0a9047a5dd5ef8 f3c512b0e38a5392 a3f492fbd917f632	->	Virtuously long
92bb535704f0ae7f	->	Geburtestag

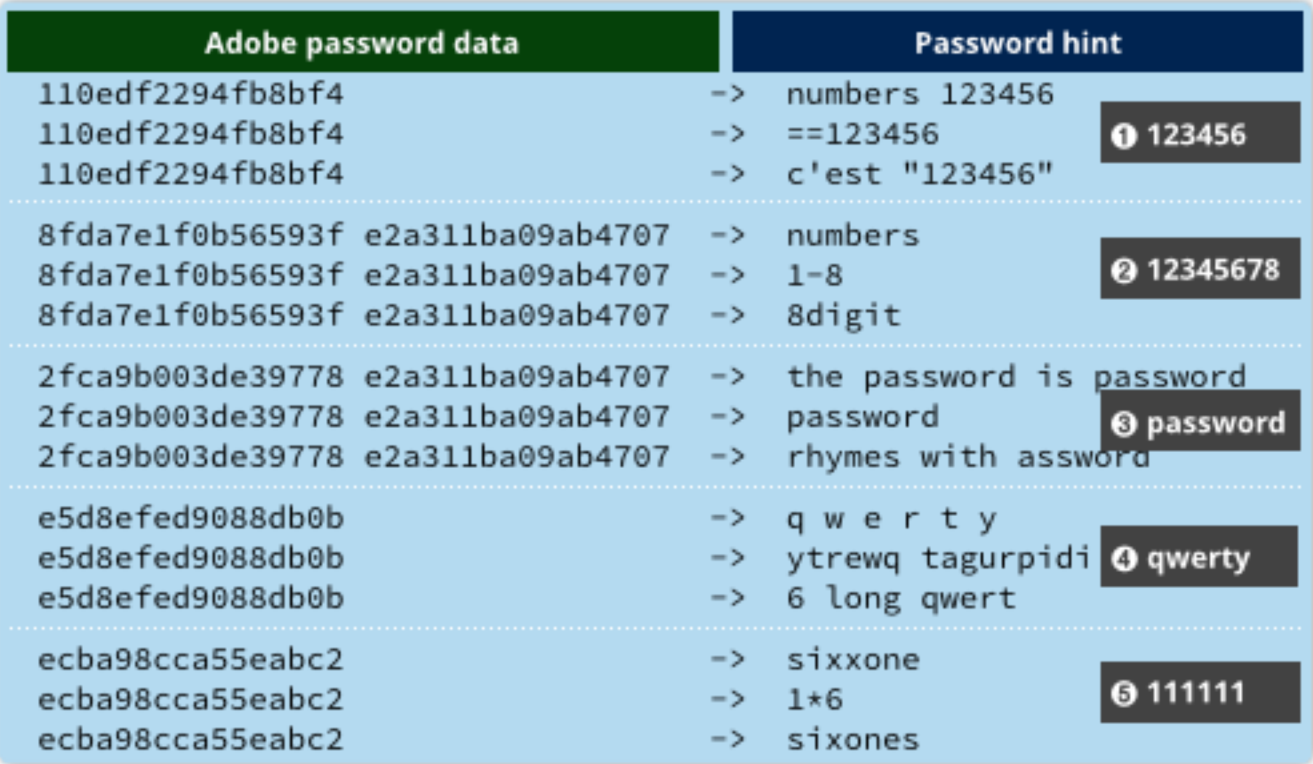


Pwd data length	Count (logarithmic scale)
8	461016
16	538396
24	526
32	53
40	6
48	3

Source: Naked Security

Adobe Breach (October 2013)

- ECB, no salting
- same password results in the same hash
- combining the hints makes he guesses easy



Adobe password data		Password hint	
110edf2294fb8bf4	->	numbers 123456	
110edf2294fb8bf4	->	==123456	❶ 123456
110edf2294fb8bf4	->	c'est "123456"	
8fda7e1f0b56593f e2a311ba09ab4707	->	numbers	
8fda7e1f0b56593f e2a311ba09ab4707	->	1-8	❷ 12345678
8fda7e1f0b56593f e2a311ba09ab4707	->	8digit	
2fca9b003de39778 e2a311ba09ab4707	->	the password is password	
2fca9b003de39778 e2a311ba09ab4707	->	password	❸ password
2fca9b003de39778 e2a311ba09ab4707	->	rhymes with assword	
e5d8efed9088db0b	->	q w e r t y	
e5d8efed9088db0b	->	ytrewq tagurpidi	❹ qwerty
e5d8efed9088db0b	->	6 long qwert	
ecba98cca55eabc2	->	sixxone	
ecba98cca55eabc2	->	1*6	❺ 111111
ecba98cca55eabc2	->	sixones	

Denial of Service

- Remotely stopping service
  - land (uses same ip src and dst), jolt2 (ip fragment badly structured no 0 offset), teardrop (overlapping fragments), etc.
  - Mostly older exploits, prey on flaws in TCP stack
  - Defenses: patch everything, keep up to date
- Remotely exhausting resources
  - Synflood: send lots of SYNs
  - Smurf: directed broadcast attack
  - Defenses:
    - Adequate bandwidth, redundant paths, failover strategies
    - Increase size of connection queue if necessary
    - Traffic shaping can help
    - Ingress/Egress filtering at firewall, border routers
    - SYN cookies eliminate connection queue

Distributed Denial of Service

- Botnets DDoS (but also adware, scareware, spam, spyware, ransomware)
  - Takes advantage of distributed nature of the ‘Net, use amplifiers and bouncers
  - Bots live on numerous hosts, remotely controlled through public IRC channels, DGA, fastflux, twitter, etc.
    - Examples: conficker, mariposa, TDL4
    - Bandwidth capability of hundreds of gbps (2014 NTP reflection attack, 2015 wireless routers)
  - Newer threats feature encrypted client-server communication (sometimes stealthy via ICMP, etc.), decoy capabilities, built-in updaters, and a variety of attack types
    - Harder and harder to trace sources: subverting privacy infrastructure -> OnionBot
  - Defenses: Consider all previous advice. Also, do your part to keep zombies off systems
    - Detect and Remove
  - Best defense is rapid detection; work with your ISP to help eliminate flood with upstream filters

Denial of Service

- DoS (all forms) sometimes used as diversions to hide “real” attacks
  - Flooding behavior can help to conceal something much more serious e.g., DNS poisoning
  - Be alert!

Defenses

- It’s an arms race and there is no bullet proof solution today

- Defense in depth
  - A best practice strategy devised by the NSA
  - A multi-layered defense approach
  - People, Technology, Operation
  - https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

All-Purpose Defenses 1

- Stay up to date with OS service patches and security-list mailings [most important!]
- Follow principle of least privilege with user accounts
- Harden your systems
  - Close all unused ports, don't run services you don't need
  - Do you really need a C compiler on your webserver?
- Find your vulnerabilities before attackers do and check regularly
  - Probing Tools, Vulnerability Scanners, etc.
- Centrally log all relevant information and monitor as appropriate
  - Network monitoring packages, Intrusion Detection including file integrity checks for system executables
  - E.g. snort, AIDE, tripwire

All-Purpose Defenses 2

- Use of Encryption where possible for communication
  - Non-snakeoil certificates for production systems
- Good Solid Policies, Recovery Plans
  - Scripted post-mortems important so no on-the-spot-decisions
- Of course… Regular Backups of crucial data!
  - Be able to recover critical systems with little notice, think about data mirroring and redundancy

Defenses: Firewalls 1

- Stateful Packet Filters
  - Remember earlier packets
  - Allow new packets originating from outside in only if they are associated with earlier packets
- Proxy-Based Firewalls
  - Operates at the application level, so it “knows when a session is present”
  - “Safer” but operate differently; lower performance and you may need features of packet filter

Defenses: Firewalls 2

- Audit your Firewall with adequate tools
  - Determine which packets are allowed through a firewall or router
  - Utilizes TTL field of IP header, given two IP addresses
  - Response from “one hop beyond” indicates port is open
  - Use this information to harden your firewall, configure it for a minimal set of rules!
  - Is it worth filtering ICMP time exceeded messages? Would cripple attacker’s but may present administrative problems

Defenses: Intrusion Detection

- Deploy an IDS to “watch” for suspicious traffic on your network
  - Equivalent of a network watchguard, “heads up”
  - Must keep it up to date
  - NIDS vs. HIDS
- Problems: Information Correlation
  - How to correlate to provide “scenario views”?
  - Must carefully tune to find relevant information, limit false positives and wasted time

Defenses: Intrusion Detection 2

- Problems: IDS Evasion
  - Attackers mess with the appearance of traffic so it doesn't match a signature
    - Fragmentation
      - Some can't handle it at all, others can quickly become exhausted with a flood of fragments -- fail open or closed?
      - Tiny Fragment Attack (IDS looks for port number to make filtering decisions, first packet is so small it doesn't have it)
      - Fragment Overlap Attack (second fragment overlaps and writes over "okay" port number with "sneaky" one)
      - FragRouter Tool
    - Minor modifications to popular attacks (ex: overflow strings)
      - Whisker and Nikto CGI scanner tools provides: URL encoding (unicode), directory insertion, fake parameter, session splicing, many more at application level (ex: HTTP)

More on…

- Session Hijacking Mechanisms
- Netcat usage, other common tools
  - ngrep, LSOF, Log Analyzers, Monitoring Tools
- Much more in the way of R2L, U2R methods and defenses
  - Buffer Overflows, Privilege Escalation, XSS
- Wireless Security
- Backdoors/Rootkits/Trojans
  - Vulnerability Maintenance, log cleaners

Some Tools

- John The Ripper, L0phtCrack (LC4/5), Cain & Abel
- Ethereal, wireshark, tcpdump, snoop
- Ettercap, hunt, arpwatch
- IPFW, IPTables, IPF, firewalk, nmap, etc.
- Dsniff
- FragRouter
- Snort, ACID,
- AIDE, Tripwire
- OpenVAS, Nessus, Whisker
- Netcat, Nagios, Cacti

Web Links

- www.securityfocus.com (inc. BugTraq)
- cve.mitre.org
- icat.nist.gov
- www.cert.org
- www.packetstormsecurity.org
- www.packetfactory.net
- www.phrack.org
- www.honeynet.org
- www.owasp.org