



Jet Propulsion Laboratory
California Institute of Technology

Cyber-Attack Methods, Why They Work On Us, and What To Do

DJ Byrne

JPL / California Institute of Technology

Mission Systems and Operations

AIAA-Space, 2015-09-01

Pasadena, CA

Cyber-Attack Methods, Why They Work On Us, and What To Do

DJ Byrne

JPL / California Institute of Technology

AIAA-Space, Aug 31 – Sept 3

Pasadena, CA

Cyber-Attack Methods

- Introduction
- Reconnaissance and Vulnerability scans
- Password Cracking
- Lessons Learned

Cyber-Attack Methods

- This paper only considers IPv4
 - IPv6 has a different set of capabilities and issues
- Cyber-attackers have decades of experience, tools, and techniques to draw on
- Defensive layers raise the attackers' costs to compromise you
- Do not be an inexpensive target!

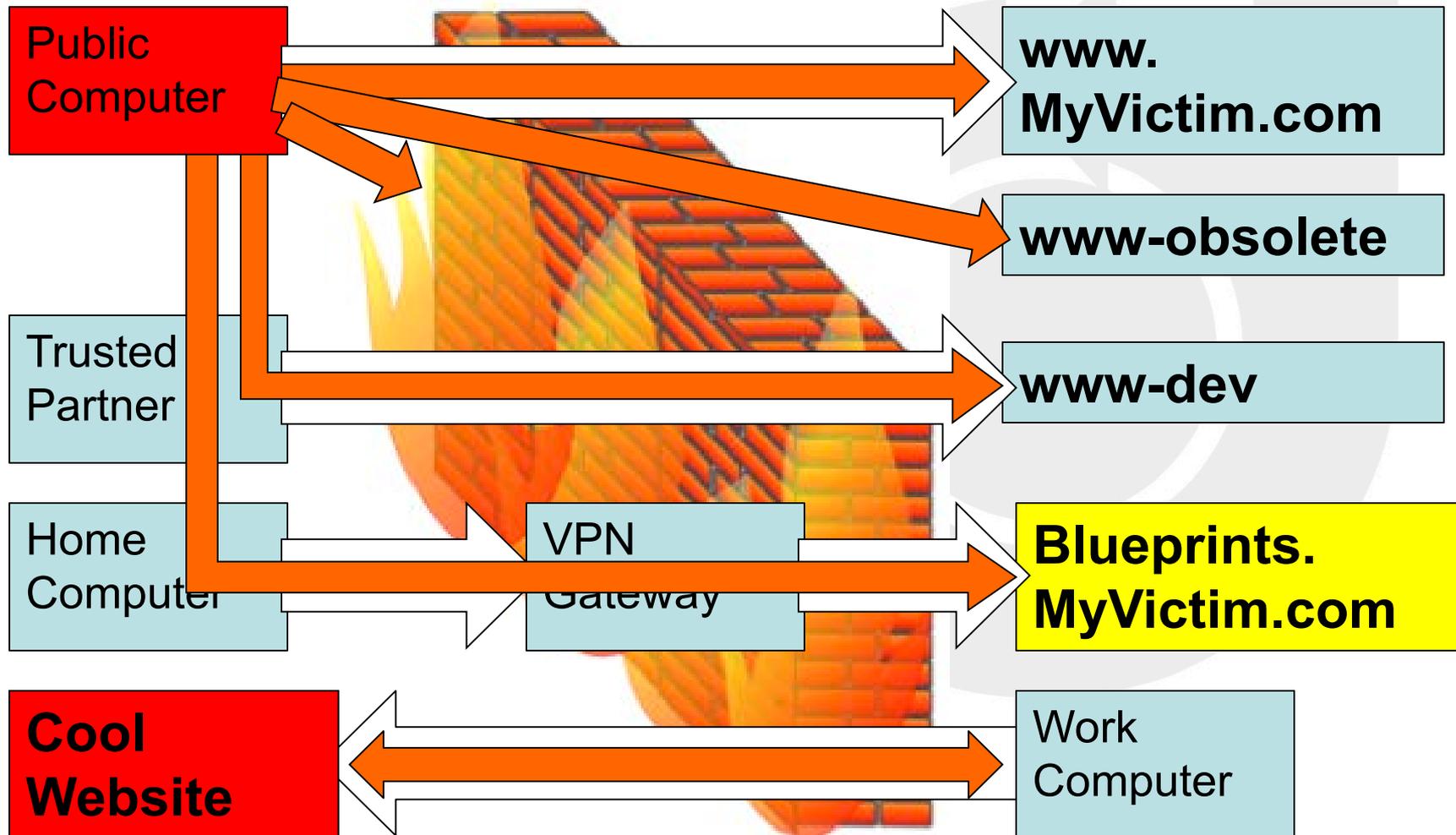
Cyber-Attack Methods

- Example:
 - Hostname: *blueprints*.MyVictim.com
 - IP address: 10.2.3.4
- Dangerous beliefs
 - "IP addresses without hostnames do not get attacked"
 - "Only descriptively named addresses get attacked"
 - "Only machines that respond to ICMP (Internet Control Message Protocol) pings get attacked."

Cyber-Attack Methods

- Common but Dangerous Beliefs
 - "We are behind a firewall, so no one can reach us."
 - "We use a private subnet, so our machines can only talk to each other."
 - "We use a VPN (Virtual Private Network), so we are only reachable through our authenticated gateway."
- Good, helpful layers. Not perfect

Cyber-Attack Methods



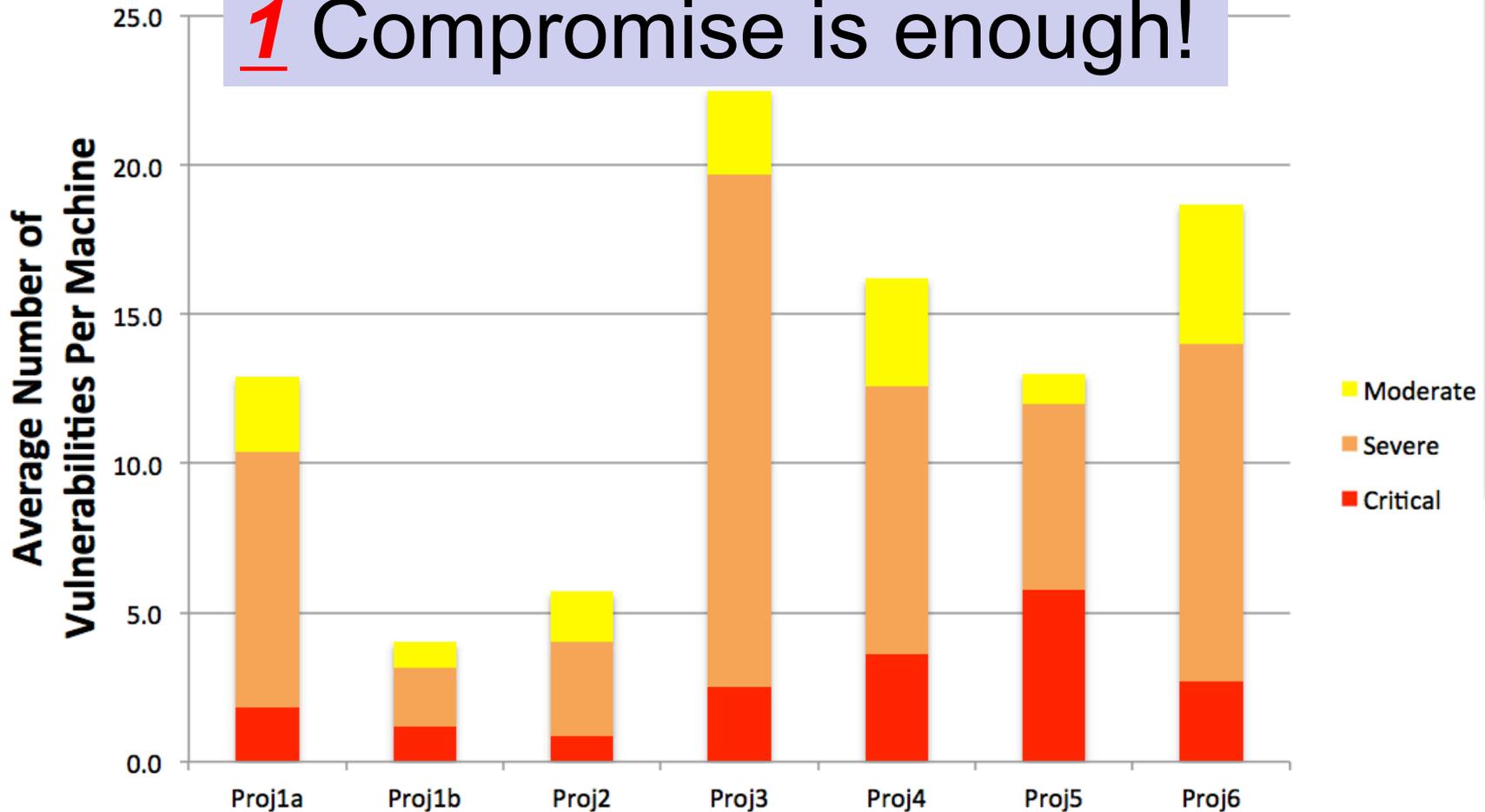
Cyber-Attack Methods

- What to do?
 - Endpoint security
 - Machines should not trust any network
 - Partition network into zones (a.k.a. subnet or VLAN)
 - Not just "inside" and "outside"
 - Limit traffic between zones
 - Do web / mail servers need to contact each other?
 - Deny ***outbound*** traffic by default
 - In addition to ***inbound***

Reconnaissance and Vulnerability scans: Scanning for Service Vulnerabilities

Cyber-Attack Methods

1 Compromise is enough!

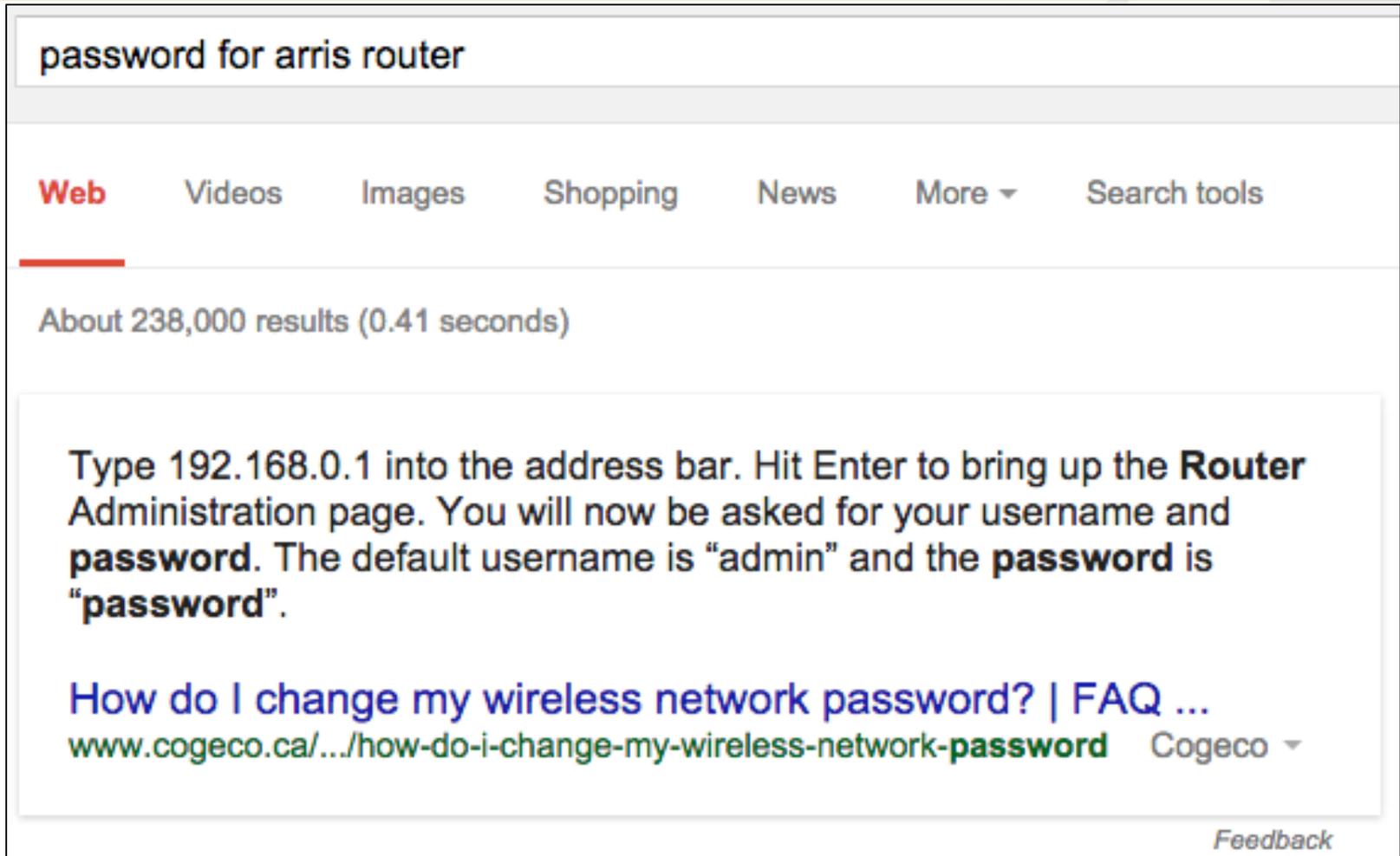


Cyber-Attack Methods

1 Compromise is enough!

Project	Number of Hashes (Cipher-text)	Number Cracked in Less Than 1 Hour	% Cracked in Less Than 1 Hour
<u>ProjA</u>	555	32	6
<u>ProjB</u>	165	8	5
<u>ProjC</u>	46	2	4

Cyber-Attack Methods



password for arris router

Web Videos Images Shopping News More ▾ Search tools

About 238,000 results (0.41 seconds)

Type 192.168.0.1 into the address bar. Hit Enter to bring up the **Router Administration** page. You will now be asked for your username and **password**. The default username is "admin" and the **password** is "password".

[How do I change my wireless network password? | FAQ ...](#)
www.cogeco.ca/.../how-do-i-change-my-wireless-network-password Cogeco ▾

Feedback

Cyber-Attack Methods

123456	baseball	abc123	michael
password	dragon	111111	superman
12345	football	mustang	696969
12345678	1234567	access	123123
qwerty	monkey	shadow	batman
1234567890	letmein	master	trustno1
1234			

Cyber-Attack Methods

- A wordlist is more than just dictionary words
 - ASCII as well as UTF-8 and other character sets
 - /usr/share/dict/words is 100,000 words
 - Oxford English Dictionary is 250,000 words
 - Our wordlist is ~95 million words
 - Pulled from various hacker tools, chiefly John-the-Ripper
- Wordlists are big business for the bad guys!
 - Billions of actual passwords have been cracked
 - ...and added to wordlists and rainbow tables

Cyber-Attack Methods

```
% echo "password" > simple_wordlist
```

```
% john --wordlist=simple_wordlist --stdout --rules
```

```
password      password3    psswrD      Password5    9password
Password     password7    drowssaP    Password7    5password
passwords    password9    Drowssap    Password4    6password
password1    password5    passworD    Password6    8password
Password1     password4    2password  Password8    Passwords
drowssap    password8    4password  Password.    passworded
1password   password6    Password2   Password?    passwording
PASSWORD     password0    Password!   Password0    Passworded
password2    password.    Password3   3password   Passwording
password!    password?    Password9   7password
```

Cyber-Attack Methods

- Patterns from cracked passwords go into "Brute force" algorithm heuristics
 - Rules of language
 - Character incidence probabilities
 - Like playing "hangman"
 - 'e' is more likely to occur than 'q'
- Markov chains
 - 'q' is more likely followed by 'u' or 'w' than by 'j'
- Capital letters are more likely as 1st character than 2nd

Password Cracking: Brute Force, Cracking Hashes Offline

Cyber-Attack Methods

Algorithm	Number of hashes per second on commodity laptop	Example
Clear-text	N/A	password
DES	10,000,000	xL f43jk6eLpF2
MD5	125,000	\$1\$ saltsalt \$qjXMvbEw8oaL.CzflDtaK/
SHA-256	1,500	\$5\$ saltsalt \$gOjOtoMpVhru2uyjeJSEc/JaLQWOXMNmlOnj6T4AtC.
SHA-512	1,500	\$6\$ saltsalt \$qFmFH.bQmmtXzyBY0s9v7Oicd2z4XSIecDzlB5KiA2/jctKu9YterLp8wwnSq.qc.eoxqOmSuNp2xS0ktL3nh/

Cyber-Attack Methods

- Necessary but not sufficient
 - Patch OS
 - Strong passwords that expire
 - Firewalls in layers
 - Investigate Anomalies
- Independent review
 - Test as the attackers fly
- If not used, turn it off!
 - Reduce the attack surface.

Cyber-Attack Methods

- **Defense in Depth – use layers**
 - Like spacecraft blankets: layers of mylar, aluminium, kevlar...
- **Periodically re-check your controls**
 - The only thing constant is change
 - Re-check what you believe you know