

1 DEF CON 18 - Trip Report

- 2 - Edward Fok – Resource Center/Office of Technical Service
- 3 - Edward.fok@dot.gov : 415-744-0113
- 4 - Date submitted: September 7, 2010

5 This is a trip summary of the 18th meeting in Las Vegas of the hacker convention called DEFCON. This
6 meeting is attended by members of the hacker community as well as cybersecurity community members
7 from private/government/academia. (see DEF CON on Wikipedia) This meeting took place between July
8 30th and August 1st, 2010 at the Riviera Hotel.

9 Major Themes

- 10 1. Social Engineering continues to be the major vulnerability in all secure systems
- 11 2. Bluetooth travel time systems needs to be hardened to protect the back office
- 12 3. 2G and earlier GSM is now vulnerable to rogue client and access point attack
- 13 4. Implementation of IPv6 is now mandatory. New IPv4 assignment is projected to run out in late
- 14 2011

15 Social Engineering-

16 One of the hacking competition conducted at DEFCON (under the supervision of CERT) involved
17 the willful divulging of useful information (useful to penetrate network security) from personnel
18 working with secure systems via the use of Social Engineering. One of the competing team was
19 able to obtain information regarding corporate network structure, port restrictions, internal
20 software names and versions, identities of key network personnel, etc. All of which are useful
21 information for someone to penetrate a secure network. Additionally, the threat from insider
22 sabotage continues to be a major problem and no new solutions were presented at the
23 conference.

24 **Recommendation:** Beef up IT security training for all DOT personnel with access to network sensitive
25 information. This needs to be a recommendation to all agencies operating transportation management
26 centers.

27 Bluetooth security

28 An offensive attack using open Bluetooth was demonstrated at the conference. This attack is aimed
29 at mobile devices but can be converted to attack the hard drive of a connected computer platform. It
30 exploits the file transfer protocol and remote, static hardware are very vulnerable to this low data rate
31 attack. It is very important for use to remind agencies using Bluetooth reader to secure their sensors
32 by:

- 33 - Turn off "discoverable" mode, or verify that it has been turned off.
- 34 - Include an activity monitor system between the Bluetooth reader and rest of the network

35 **Recommendation:** Review network design and inventory profile states for integrated Bluetooth travel
36 time measurement systems.

37 GSM vulnerability

38 Agencies using GSM cellular needs to verify they are using encrypted 3G type communication
39 technologies. DEFCON demonstrated a rogue GSM base station can be created using about
40 \$2000 of COTS gears. The rogue GSM can be use as a "man-in-the-middle" agent between the
41 cellular device and the legitimate network to monitor all data and voice traffic. Encryption built
42 into 2G and earlier GSM services can be cracked with relatively little effort. However, encryption

FOR OFFICIAL USE ONLY.

USE OF INFORMATION IN THIS DOCUMENT IS RESTRICTED AND IS TO BE TREATED IN A CONFIDENTIAL MANNER.
When not in use, this document is to be stored in a safe area. This material is subject to the safeguards of the
Privacy Act of 1974, USC 552a, as amended. U.S. Department of Transportation, Federal Highway Administration.

43 used in 3G services remains secure. Due to the way GSM devices switches between 3G and 2G
44 services, an attacker can us a 3G jammer to force devices to switch over to 2G services where
45 the encryption can be cracked.

46 **Recommendation:** GSM used as part of the transportation network should utilize only 3G encrypted
47 services. This will likely reduce the number of sites that can benefit from cellular network communication
48 but will increase security.

49

50 IPv6 and IPv4 Shortage

51 IPv4 is the current generation of numbering system used by the internet to identify sites and other
52 resources. These numbers are managed and distributed by the 5 Regional Internet Registries in
53 the world. At the current rate of consumption (from new ISP's, individuals, corporations,
54 organizations, and governments) it is projected that all of the available IPv4 numbers will be used
55 up by late 2011, this factors in an aggressive number 'recycling' program to make sure all IPv4
56 numbers are being utilized. What this means is that in less than 2 years, the transition to IPv6
57 from IPv4 will begin and the transition period is expected to last approximately 10 years as old
58 equipment is retired with new IPv6 hardware. During this transition period, those using IPv6 can
59 continue to access IPv4 addressed resources on the internet, but IPv4 will be unable to access
60 IPv6 resources. This problem can best be illustrated in this example: Imagine a 4 digit telephone,
61 this will be IPv4. IPv6 will be a 6 digit telephone. The IPv6 phone, having more digit then the
62 IPv4 phone, can dial any IPv4 number in existence. But the IPv4 phone cannot dial all 6 digits of
63 an IPv6 phone, so it's impossible for it to communicate with the new equipment.

64 **Recommendation:** All network equipment specification should call for IPv6 compatibility and testing for
65 functionalities under IPv6 should be mandatory for all new deployments. Assessment of existing network
66 infrastructure for IPv6 compatibility should begin as soon as possible.

67 Emerging Problems and Solutions

- 68 1. Cloud computing was demonstrated as a viable platform to launch massive distributed denial of
69 service attack for relatively low cost.
- 70 2. Low cost security operation center design was proposed. The design substituted virtual
71 machines in lieu of actual hardware for security operations requiring dedicated machines. (i.e.
72 honey pot, virus sandbox, etc)
- 73 3. S2ERC, a cooperative research center backed by the National Science Foundation, has begun
74 the development of a software security and reliability metric. Additional information is available at
75 www.s2erc.net.

FOR OFFICIAL USE ONLY.

USE OF INFORMATION IN THIS DOCUMENT IS RESTRICTED AND IS TO BE TREATED IN A CONFIDENTIAL MANNER.
When not in use, this document is to be stored in a safe area. This material is subject to the safeguards of the
Privacy Act of 1974, USC 552a, as amended. U.S. Department of Transportation, Federal Highway Administration.