

**BACKGROUND**

DEFCON 17 is the 17<sup>th</sup> meeting of the underground hacker community. This is an annual conference held in Las Vegas during the summer taking place immediately after the Blackhat conference. To draw contrast between the two conferences, Blackhat is designed to appeal to corporate security audience: Registration begins at \$1300 up to \$2000 and this does not including training courses. Blackhat is held at the Caesar Palace hotel. DEFCON registration is \$120 cash only, there are no training courses, but there are hacking villages, lockpick competition, and is held annually at the Rivera convention center.

This year's DEFCON was held from July 30<sup>th</sup> to August 2<sup>nd</sup>.

**SESSION SUMMARY****DoD prospective – Robert Lentz:**

Major take away is the focus is moving from network to Information security. This is a major recruitment pitch and explains a lot of the reasons behind odd 17 rules. Unfortunately none of which really applies to us.

**USMMA defense against NSA Red Team – Efstratios L. Gavas:**

This is a potential resource for us. the presenter is an instructor at the US Merchant Marine Academy. The talk is about how a five person team defended a network from cyber attacks coming from a NSA Red Team as part of the annual cyber challenge. The same year all of the team fielded by the major service academies all lost to the NSA Red Team. A list of open source tools were cited along with some very basis tantivities

- 1) If you don't understand it, you can't protect it.
- 2) Redundancy is nice, but it's useless if there is an unfixable weak link. (i.e. staffing)
- 3) Don't go nuts with group policies
- 4) Use pass phrases, not passwords.

**Bruce Schneier – Author and Security Expert**

Identity based security is obsolete. Key is intent based security. Two key take away:

- 1) Terrorism is simple engineering, why hasn't it happened more often? Failure is terminal. Yes it maybe simple to engineer, but each step has chances of failure. Failure in illegal activity generally results in prison on death. So there is little chance of learning from failure common to engineering
- 2) Identity based security is useless. Interest is in who is going to blow up the plane, not really who the terrorist one. In trusting in this type of security model ID theft does not have value

1 of 3

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.

**RFID – Chris Paget**

US Passport based RFID can be sensed up to 125' at an unknown data rate. Can be nuked remotely. Use metalized bag or Faraday caged wallet to protect.

**Smart Parking Meter Hack – Joe Grand/Jake Appelbaum:**

Basically a smartcard hack. Poor implementations and ignorant of DVR hack toolset which provided a platform to do this. This is a partial hack. They have not gotten into the firmware of the meter itself.

Social Engineering: They asked a detailed but slightly off question & the field tech provided critical information. This will be tricky to balance between "friendly" and no response.

**Cyber Warfare-1 – Jayson Street**

Who's ready by cyber warfare:

China: Red Hacker Alliance

Russia: 5th Division Cyber Army

2009 June DDOS: Unlikely to be NK since all sp routed to China. Source is TBD.

Scenario: Botnet in China, gets brined to run DOS attack on US. Who do you blame?

**Hardware Trojans – Janansky/Waite**

Interpreting 12 V noise to determine CPU activity by using compromised PSU.

1) How the hell do yore get the right pieces together?

2) This depends on a uncorrected PE supply. If connected this method may not work.

Check DEFCON 16 for additional H/W hacks. These are potential methods to infiltrate a secured and isolated TMC.

**Cyber Warfare-2 - Panal**

In terms of SCADA systems the vulnerabilities are in the communication over exposed wires and communication link. Yes, there is a threat to learning of control and command codes by monitoring the wiring. But existing OS are pretty much protected due to their specialized nature. However, this will change as more and more system moves into using mainstream OS'es.

Lot's of talk between coordinated cyber-kinetic strikes. Demonstrated in Georgia conflict.

**Social Engineering detection – Antonio Rucci**

2 of 3

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.

Nothing epic new here. Contact made with contractor at ORNL who specializes in this field. There is a two day training course on this subject area. Intent to follow up to get a better understanding of possible deliverables. Hope to develop sufficient understand for benefit/gap potential.

## **TOOLS**

**Metasploit** – automated attack tools designed to facilitate and automate multiple attacks to deliver multiple software payloads

**Direct EMP Injection** – Shows how to inject Electro Magnetic Pulse into a electrical network and how it can cause a solid state device to automatically reset or reboot.

## **REFERANCE**

### **“Dissecting the Hack”**

This is the prolog section of a fictional story about hackers. What is special about this is how the author explains the details of the hacking method used in the story...in extensive detail. This is a good entertaining eye opener on how IT system vulnerabilities are exploited.

3 of 3

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.