(U) TCB Jamboree/TCB Jamboree 2011

TOP SECRET//NOFORN
From WikiInfo-NF
< TCB Jamboree
Jump to: navigation, search

(S//NF) The Information Operations Center's Engineering Development Group (EDG) held its sixth annual Trusted Computing Base (TCB) Jamboree on March 15 – 16, 2011.

Visit the TCB Program WIKI.CIA page at:

https:/ [redacted]

Contents

[hide]

- 1 (U) Invitation
- 2 (U) Registration
  - 2.1 (U) Clearance Passing
- 3 (U//FOUO) 2011 TCB Jamboree Agenda
- 4 Presentation Abstracts – Tuesday, 15 March
  - [redacted]
  - [redacted]
  - 4.3 (S//NF) Driver Signing Footprint
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- 5 Presentation Abstracts – Wednesday, 16 March
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

[edit] (U) Invitation

(S//NF) The Information Operations Center's Engineering Development Group (EDG) would like to announce the sixth Trusted Computing Jamboree. The Jamboree is organized and sponsored by the Security Portfolio of EDG's Emerging Technologies Branch (ETB). As in past years, the Jamboree will be an informal and interactive conference with an emphasis on presentations that provide important information to developers trying to circumvent or exploit new security capabilities.

(U) The Jamboree will be held on Tuesday and Wednesday, March 15-16th, 2011 at the Lockheed Martin [redacted].

(S//NF) The TCB Program continues to explore architectures that will have a significant impact on future Information Operations. Technologies such as the Trusted Platform Module (TPM) pose both threats and opportunities for the Intelligence Community.

(S//NF) The main purpose of the Jamboree will be to discuss how the results of the Security Portfolio research can be applied today. Rather than an overview of all the activities within the Program, we will present notable results that will provide developers insight into how to meet the threats of the TCG architectures and embedded architectures and how they can exploit new avenues of attack.

[edit] (U) Registration

(U) Pre-registration for this event is required; registration closes on March 11, 2011.

(C) Please send an email (CWE Note or ICEmail) to [redacted] and [redacted] that includes your full name, SSN and contact number.

[edit] (U) Clearance Passing

[redacted]

(U) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[edit] (U//FOUO) 2011 TCB Jamboree Agenda

Schedule (U) Each day will run from 9am to 5pm. In order to facilitate planning, the topics presented on each day are highlighted below. The abstracts for each topic are on the following pages.

Tuesday March 15th, 2011

Presenters	Talk Title
[redacted] (Sandia National Laboratory)	(S//NF) Differential Power Analysis on the Apple A4 Processor
[redacted] (Sandia National Laboratory)	(S//NF) Secure key extraction by physical de-processing of Apple's A4 processor
[redacted] (Xetron)	(S//NF) Driver Signing Footprint
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[edit] Presentation Abstracts – Tuesday, 15 March

[edit] (S//NF) Differential Power Analysis on the Apple A4 Processor

(U) Presenters [redacted] (U) The Apple A4 processor contains an on-board, AES cryptographic key called the Global ID (GID) that is believed to be shared across all current "iDevices". This GID key is used to un-wrap the keys that decrypt the corresponding boot firmware code stored in system non-volatile memory. Currently, the only way to examine unencrypted boot code is to gain execution through an exploitable software security flaw. However, Apple is quick to address these flaws with

[edit] (S//NF) Driver Signing Footprint

(U) Presenter: [redacted] (S//NF) Driver signing requirements on the 64bit versions of Windows 7 and Vista are a challenge when trying to load kernel level drivers and implants. The aim of this study is to understand the observability and traceability of signature credentials used to sign kernel-level drivers. The eventual goal of the research is to: 1. Render improbable the detection of the signature credentials used to sign a kernel-driver 2. Where not impossible to remove credential artifacts, quantify the remnants and associated risk

(U) This talk will discuss: (S//NF) The forensic data quantifying the residual footprint of the signature authority for drivers that have been installed and removed from 64-bit versions of Windows 7 and Vista. (S//NF) The analysis of the forensic results, providing insights as to the operational risk to Sponsor activities if this technique is used.

[edit] [redacted]

[redacted]

[edit] (S//NF) [redacted]