(U) TCB Jamboree

TOP SECRET//SI//NOFORN
From WikiInfo-NF
Jump to: navigation, search

(S//NF) The **TCB Jamboree** is a conference hosted on an annual basis by the **Trusted Computing Base (TCB)** Program within **CIA's Emerging Technologies Branch** within IOC. TCB Jamboree brings together CIA analysts and all of the various contractors performing research for the CIA TCB program. In past years CIA has also invited NSA to participate through the NSA TCB Program (the counterpart to the CIA program).

(U//FOUO) The first Jamboree was held in 2006. Attendance is open only to US personnel.

Note: (2/6/12) As of this morning, clearances were verified for all registered attendees from NSA that we know of. - [redacted]

Contents

[hide]

- 1 TCB Jamboree 2012
- 2 (U) Invitation
- 3 (U) Registration
  - 3.1 (U) Clearance Passing
- 4 (U//FOUO) 2012 TCB Jamboree Presenters Deadlines
- 5 (U//FOUO) 2012 TCB Jamboree Agenda
  - 5.1 (U) Tuesday, February 7, 2012
    - 5.1.1 (U) Schedule
    - 5.1.2 (U) Abstracts
      - [redacted]
      - 5.1.2.2 (S//NF) Apple A4/A5 Application Processors Analysis
      - [redacted]
      - [redacted]
      - [redacted]
      - [redacted]
      - [redacted]

        - [redacted]
        - 5.1.2.9 (S//NF) Strawhorse: Attacking the MacOS and iOS Software Development Kit
        - [redacted]
    - 5.2 (U) Wednesday, February 8, 2012
        - 5.2.1 (U) Schedule
        - 5.2.2 (U) Abstracts
            - [redacted]
            - [redacted]
            - [redacted]
            - [redacted]
            - [redacted]
            - [redacted]
            - [redacted]
            - [redacted]
            - [redacted]
            - [redacted]
    - 5.3 (U) Thursday, February 9, 2012
        - 5.3.1 (U) Schedule
        - 5.3.2 (U) Abstracts
            - [redacted]
            - [redacted]
            - 5.3.2.3 (U) Advanced Debugging and RE Techniques on Embedded Platforms
            - [redacted]
- 6 Past Jamborees
- 7 Related

[edit] TCB Jamboree 2012

(S//NF) The Information Operations Center's Engineering Development Group (EDG) will hold its seventh annual Trusted Computing Base (TCB) Jamboree from February 7–9, 2012.

Visit the TCB Program WIKI.CIA page at:

https://[redacted]

[edit] (U) Invitation

(S//NF) The Information Operations Center's Engineering Development Group (EDG) would like to announce the seventh 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 Tuesday-Thursday, February 7–9, 2012 at the Lockheed Martin [redacted] Tuesday and Wednesday will run

from 9am to 5pm, Thursday will run from 9am to 12pm.

(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 February 1, 2012.

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

[edit] (U) Clearance Passing

[redacted]

[edit] (U) Thursday, February 9, 2012

[edit] (U) Schedule

Time	Presenter(s)	Talk Title
09:00-09:15	[redacted]	(U) Welcome, EDG/ETB Trusted Computing Base Program
09:15-9:45	[redacted]	[redacted]
9:45-10:15	[redacted]	[redacted]
10:15-10:30		(U) Break
10:30-11:00	(U//FOUO) [redacted] Northrop Grumman Xetron	(U) Advanced Debugging and RE Techniques on Embedded Platforms
11:00-11:30	[redacted]	[redacted]
11:30-11:50	[redacted]	(U) Jamboree Wrap-Up

[edit] (U) Abstracts

[edit] [redacted]

[redacted]

[redacted]

[edit] [redacted]

(U//FOUO) [redacted]

[redacted]

[redacted]

[edit] (U) Advanced Debugging and RE Techniques on Embedded Platforms

(U//FOUO) Presenter: [redacted] Northrop Grumman Xetron

(S//NF) Embedded platforms present many additional challenges to reverse engineering. Therefore, it is often advantageous to employ dynamic analysis in the form of hardware or software debuggers to speed up the process of reverse engineering and developing implants. Manufacturers often leave hardware debugging features such as JTAG enabled on their products. We will explore methods that NG Xetron uses to locate these hardware debugging features and how these features are utilized for reverse engineering.

(S//NF) Software based debugging facilities can also be very useful in performing initial reverse engineering and allowing the development team to scale rapidly without much additional equipment. We will look at common software debuggers that are used during development of embedded platforms including VxWorks shell, GDB and others. To facilitate rapid use of dynamic debugging and analysis capabilities on a wide range of embedded platforms, NG Xetron has developed a GDB server capability that can be added to existing firmware. This GDB server is very portable and reduces the dependence on the hardware and firmware of each platform of interest.

(U) These techniques have been applied to a wide range of target systems, and have proven to greatly reduce the amount of time spent either in static analysis or in working to create a custom one-off dynamic analysis technique on each system.

[edit] [redacted]

[redacted]

[redacted]

[edit] Past Jamborees

- TCB Jamboree 2011 Abstracts
- TCB Jamboree 2010 Abstracts
- TCB Jamboree 2009
- TCB Jamboree 2008
- TCB Jamboree 2007
- TCB Jamboree 2006

[edit] Related

[redacted]

[redacted]

[redacted]

TOP SECRET//SI//NOFORN
Derived From: SI Classification Guide, 02-01, **Dated:** 20060711
and NSA/CSSM 1-52, **Dated:** 20070108