CISS Hot Summer

Generated by CISSRT

19.05.2011

CISS Hot Summer

Уже прошла первая половина июня месяца, через каких-то 10-15 дней у всех студентов закончится сессия и они будут отданы сами себе на 2 месяца, которые они будут проводить, как они захотят. Это время можно провести с толком для себя.

Как показывает практика компании Google Inc. проведение образовательных, практических мероприятий в летнее время очень результативно.

Вот с 2005 года Google Inc. проводит в летнее время Google Summer of Code. В данной программе можно получить опыт работать в Open Source проектах, программировать, работать в команде.

Идея летнего взаимодействия со студентами очень интересная и полезная. И в этом году CISSRT с 1 июля запускает проект CISS Hot Summer. По своей сути это Русский Google Summer of Code, только проводит его CISSRT.

Так же основное отличие данного проекта в том, что он целиком и полностью будет посвящен информационной безопасности.

Хотелось отметить, что для информационной безопасности на территории России уделяется очень мало внимание.

Если смотреть по пропорции то в Западных компаниях на организацию безопасности в ИТ проектах тратится от 40-60% от сумы данного проекта.

В проектах, которые реализовываются Русскими компаниями это максимум 30%. Это говорит о том, что нужно поднимать уровень ИБ и его финансирование.

А так же не маловажно подготовка молодых кадров и формировании не коммерческих организации, целью которых будет обмен опыта.

Что из себя будет представлять CISS Hot Summer?

Это проект, который будет с 1 июля до 1(10) сентября.

До 1 июля нужно написать на CISSHOTSUMMER@gmail.com про желание участвовать в нем.

В период проведения проекта будут сформулированы задания для каждого участника. Так же будут назначены кураторы для каждого участника, которые будет отвечать на вопросы участников по задания, помогать правильно выбрать алгоритмы решения, и всячески способствовать результативной работе участника.

Так же во время CISS Hot Summer будут проходить online конференции и мастер-классы, основные цели которых повышение уровня, как теоретических, так и практических знаний участников.

Многие студенты, которые будут проходить университетскую практику в CISSRT, тоже будут участвовать в CISS Hot Summer.

Задания будут даваться участникам индивидуально в процессе обсуждения их интересов.

Участник сам будет выбирать, над каким именно задание он хочет работать.

Аспектов данной программы - исследование и разработка:

1) Динамический анализ

1. Pin plugins - трассировка, автоматизация детектора уязвимостей (улучшение RedFlag например и т.д.) и т.д.

2. BitBlaze - работа с Temu, написание плагинов, исследование тентирования.

2) Статический анализ

1.IDA plugins:

a. differs: turbodiff, patchdiff, DarunGrim - merge с findAlloc, findmemcpy и т.д.

b. визуализаторы - прорисовка трасс от различных трассирощиков(Pin, temu и т.д.), оптимальные пути от точек и т.д.

c. связывание Vine'a с IDA - IDAOCaml

3) Исследование Solvers - STP,Z3,SMT и т.д.

4) Исследование отладчиков:

1. плагины к Windbg,
2. плагины gdb (актуально для Mac OS X, iOS)
3. плагины Immunity Debugger

5) Поиск уязвимостей, исследование новых векторов атаки:

1. Ядра OS по направлениям LPE (вектор повышение привилегий):

a. Windows - GUI(win32k.sys,atmfd.dll и т.д.), kernel(ntoskrnl.exe), drivers(standart and additional)

b. Windows 3rd party drivers - ioctl, syscall hooks fuzzing - аверы, крипто и прочие вендоры

c. MacOS X

d. Apple iOS - пересекается с MacOS X(специфичный xnu), ARM архитектура

e. Linux

f. *BSD - немного пересекается с MacOS X(/bsd source dir - форк FreeBSD 5.0)

g. Solaris,QNX - редкие никсы, хотя соляра не такая редкая имхо.

h. Android - немного пересекается с Linux, ARM архитектура

j. cisco IOS.

2. Ядра OS по направлениям RCE (удалённое выполнение кода):

a. TCP/IP, IPv6 fuzzing - все OS

b. GSM, 3G, 4G, Bluetooth, Wifi fuzzing - Apple iOS, Android

c. SMB(Samba) - Windows/Linux.

3. Приложений.

a. Браузеры: Windows Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera

b. Flash: Adobe, Gnash, swfdec.

c. PDF: Abode, Foxit.

Все желающие поучаствовать, или просто задать интересующий вас вопрос, пишите на CISSHOTSUMMER@gmail.com или

mail: virvdova@gmail.com

Skype: abazhanyk_cv

twitter: @ABazhanyuk