PacSec 2015 セキュリティカンファレンス

報道関係者各位 様

PacSec 2015 セキュリティカンファレンス、取材のご案内

来週11月11-12日に「PacSec2015 セキュリティカンファレンス」が東京で開催されます。世界の情報セキュリティトレンドを取材できるチャンスですので、ぜひおいでください。初日11日の17:00過ぎより、講演者が全員登場するプレス・ブリーフィングをカンファレンス会場にて行います。

これから取材事前申込みされる方は、こちらのアドレス secwest15@pacsec.jp まで "Subj:"を"Press Registration"とご記入してメールをお送りください。

PacSecカンファレンスには今年も発表応募が51本あり、質の高いものが多いためセレクションが難航しました。以下に概要リリースを付けておきますのご参照ください。また今年は参加費を試験的に昨年までの半額に下げることができたため、参加者数が大幅に増加すると思われます。

今年は日本からの発表申し込みが無かったため、発表は全員が来日講演者になります。HP, Yahoo!, Trend Micro, CloudFlare, Google, Cisco, Qihoo 360, Tencentなど、よく知られた企業の研究者が多数来日します。ブルートゥースとNFCの組み合わせでのスマートフォンの攻略、HTTP2プロトコルのセキュリティ、クラウドのハイパーバイザーのセキュリティ、ソフトウェア定義無線を使ったIoTへの攻撃、バーコードを使って任意のコマンドを実行する手法など、多数の興味深い講義が注目されます。タイムテーブルはこちらで参照できます https://pacsec.jp/agenda.html?language=ja

PacSecカンファレンスと同時に、注目のイベント「Mobile Pwn2Own」の開催がまた今年も予定されています。今回の日本でのPwn2Ownは、国際武器輸出規制のワッセナー合意の影響で開催できないという予測ニュースがありましたが、小規模ながら実現する予定です。脆弱性発見コンテストは普及してきましたが、Pwn2Ownそれらの中でも特別な脆弱性発見コンテストになっているので、最新の脆弱性発見の現場をリアルタイムで取材することができます。そのため毎回世界中のメディアが取材に来ます。

★ PacSec2015 概要

PacSec 2015 セキュリティカンファレンス、11月11-12日に東京で開催

会場: 青山ダイヤモンドホール(地下鉄 表参道駅 銀座線、半蔵門線、千代田線、B5出口)
日程: カンファレンス 11月11,12日 9:30amオープン予定、 レセプションディナー 11月11日夜
　http://pacsec.jp/　Twitter: @PacSecjp

★ PacSecは脆弱性発見コンテスト「Pwn2Own」で知られるCanSecWestセキュリティカンファレンスの日本版
★ 参加費を試験的に昨年までの半額に値下げ、早期登録は4万5千円+消費税、通常登録は5万円+消費税
★ 51本の発表応募から厳選された、最前線の攻撃手法と防御技術の講義

PacSecカンファレンスの情報: http://pacsec.jp/ , Twitter: @PacSecjp
総合問い合わせ先: email: secwest15@pacsec.jp , Fax: 020-4668-3367

PacSec 2015 セキュリティカンファレンス

★ グローバルな視点のセキュリティ最新研究の講義を直接聞ける、希少な日本開催のセキュリティカンファレンス
★ 最前線の攻撃手法と防御技術を学習し世界中の専門家と交流できる、11月11-12日の2日間の集中技術講義
★ セキュリティ専門家で構成された委員会にて選ばれた発表者による、宣伝を排除した中立性の高い講義内容
★ CanSecWest, Black Hat, DEFCON, HITBなど海外のセキュリティ会議での発表でも注目された講演者が来日予定
★ モバイルデバイス脆弱性発見コンテスト「Mobile Pwn2Own」を同時開催予定、世界のメディアが注目

「PacSec 2015 セキュリティカンファレンス」が、11月11, 12日の2日間にわたり表参道の青山ダイアモンドホールにて開催されます。カナダのdragostech.com inc.(ドラゴステック・ドットコム、本社: カナダ、エドモントン)が主催するPacSecは、海外で開催される最前線の情報セキュリティカンファレンスと同じレベルのイベントに、日本にいながら同時通訳付きで参加できるチャンスです。今年のPacSecは、参加費を試験的に昨年までの半額の5万円以下にしたことにより、大幅に参加しやすくなっています。

PacSecセキュリティカンファレンスで行われる講義は、世界中から応募してきた講演者の論文から審査の上選ばれています。今年13回目になるPacSecでは2日間に12本の講義が予定されています。51本の発表応募があった中から、世界各国のセキュリティ専門家で構成された委員会にて選ばれ絞り込まれました。

今年の注目される講義内容の一部をご紹介します。

"Attacking IoT with SDR (Software Defined Radio)" Jonathan Andersson
「SDR(ソフトウェア定義無線)を使ったIoTへの攻撃」 ジョナサン・アンダーソン, HP

"Attacking HTTP2 Implementations" Stuart Larsen + John Villamil
「HTTP2のインプリメントに対する攻撃」 スチュアート・ラーセン + ジョン・ヴィラミル, Yahoo!
使用が拡大しつつあるHTTP2プロトコルについてのセキュリティの観点からの考察

"Criminal Hideouts for Lease: Bulletproof Hosting Services" Maxim Goncharov
「犯罪の賃貸隠れ家: 防弾ホスティング・サービスについて」 マキシム・ゴンチャロフ, Trend Micro

"BlueToot / BlueProx - when Bluetooth met NFC" Adam Laurie
「BlueToot / BlueProx - ブルートゥースとNFCが出会う時」 アダム・ローリー, Aperture Labs
昨年のMobile Pwn2Ownでの優勝者の一人アダム・ローリーによる攻撃手法の解説。

"Windows 10, Elevator Action" James Forshaw
「Windows 10, エレベーターアクション」 ジェームズ・フォーショー, Google UK

"Warranty Void If Label Removed - Attacking MPLS Networks" Georgi Geshev
「ラベル剥がれの場合は保証無効 - MPLSネットワークへの攻撃」 ゲオルジ・ゲシェフ

PacSecカンファレンスの情報: http://pacsec.jp/ , Twitter: @PacSecjp
総合問い合わせ先: email: secwest15@pacsec.jp , Fax: 020-4668-3367

"The plain simple reality of entropy (Or how I learned to stop worrying and love urandom)" Filippo Valsorda
「まったくシンプルなエントロピーの現実(あるいは私はどのように心配をヤメてurandomを愛するようになったかについて)」 フィリッポ・ヴァルソルダ, CloudFlare

"High Performance Fuzzing" Richard Johnson
「ハイパフォーマンス・ファジング 」 リチャード・ジョンソン, Cisco Talos

"Universal Pwn n Play" Martin Zeiser + Aleksandar Nikolic
「ユニバーサル PnP(攻略と再生の意味で)」 マーティン・ザイサー + アレクサンダー・ニコリック, Cisco
広く普及しているUPnPプロトコルがどのように攻撃に利用されうるか

"Vulnerabilities mining technology of Cloud and Virtualization platform" Qinghao Tang, Qihoo 360
「クラウドと仮想化プラットフォームに対する脆弱性発見のマイニング技術」 キンハオ・タン, Qihoo 360
普及しているクラウド・プラットフォームで使われているハイパーバイザーとそのセキュリティの考察

"Exploiting Heap Corruption due to Integer Overflow in Android libcutils -- Escalate privilege by vulnerabilities in Android system services" Guang Gong
「Androidのlibcutilsに存在する整数オーバーフローによるヒープ汚染の攻略 -- Androidシステム・サービスの脆弱性を用いた権限昇格」 グァン・ゴン, Qihoo 360

"BadBarcode: Hacking with A PIECE of PAPER" Hyperchem Ma,
「バーコード: 一片の紙片で宇宙船をハックする方法」 ハイパーケム・マー, Tencent
バーコードを使ってターゲット・システムで任意のコマンドを実行する手法について

講演者は日本ビザ発給など様々な理由により変更になることがあります。講義内容の最新の詳細は http://pacsec.jp/speakers.html でアップデートをご覧ください。

また昨年に引き続き、脆弱性発見コンテスト「Pwn2Own」(ポゥン・トゥ・オゥンと発音)の一環として、モバイルデバイス脆弱性発見に特化した「Mobile Pwn2Own」の同時開催が予定されています。今回は小規模ですが日本で3回目の開催になる「Mobile Pwn2Own」は、複数のセキュリティ企業やモバイル機器企業が応援しています。Pwn2Ownには世界中の脆弱性ハンターが集まるため、毎回世界中の主要テクノロジーメディアが多数取材に来ています。

★ PacSecセキュリティカンファレンスについて
「PacSec 2015」セキュリティカンファレンスは、世界先端の情報セキュリティ専門家による最新の研究発表の講義と国際交流できる環境を兼ね備えた場を用意することにより、日本での先進的なセキュリティ人材育成への技術教育の場を提供することを目的として、CanSecWestとPWN2OWN脆弱性発見コンテストで知られるカナダのdragostech.com inc.が主催する国際セキュリティカンファレンス・シリーズ「SecWest」の一環として、2003年より日本で開催されて来ました。カナダのバンクーバーで開催される「CanSecWest」、イギリスのロンドンまたはオランダのアムステルダムで開

催される「EU-SecWest」、アルゼンチンのブエノスアイレスで開催される「BA-Con」と並び、SecWestにおいても東京は情報セキュリティにおける国際的に重要な都市として位置づけられています。

「PacSecセキュリティカンファレンス」は、NPO日本ネットワークセキュリティ協会、一般社団法人インターネット協会、社団法人日本インターネットプロバイダー協会、OWASP Japan, WASForum、CodeBlue、AVTokyoなどの後援団体の支援と、多数のスポンサーの協賛によって13年間にわたり東京で開催され続けてきました。「PacSec 2015」セキュリティカンファレンスでは、51本の発表応募から最先端の情報セキュリティに関する厳選された研究発表を集め、セキュリティに関する最新の技術トレンドと脆弱性の分析や実践的防衛策などの幅広い技術的話題を取り上げます。海外から来日するセキュリティ専門家と日本の専門家が集まり最新のセキュリティ技術に触れ合い話し合うことで、情報セキュリティに関する問題や有効な解決策などの情報交換とコミュニティ形成の場となることを目的としています。

スマートフォンやタブレット型デバイスの急激な普及によって、WiFiや3G、LTEなど無線環境からの常時接続されたインターネット環境が持ち歩かれる事が普通となり、私たちの仕事や生活も携帯デバイスによる移動環境のオンラインとクラウドサービスの一般利用に急速に移行しています。そして、ソーシャルネットワーク型の各種オンラインサービスが国境を越えて億単位のユーザー数を獲得し、企業の業務コミュニケーションやeコマースやオークション、またオンラインバンキングや株式やFXのオンライントレード他様々な金融サービスなどもインターネット上で拡大しています。

そのようなインターネット環境の激変の中で、政府機関や国家的基幹事業にたずさわる企業を狙う標的型攻撃やサイバースパイ活動が明らかになり、Stuxnetのようにインフラ構築に使われる組込コンピューターを狙った攻撃が登場し、またフィッシングやマルウェアによる個人情報の窃盗、ボットネットによるDDoS攻撃や脅迫などの犯罪、犯罪組織のマルウェア開発やボットネット運営への関与、さらには米NSAや英GCHQなどのスパイ機関が一般の通信の大規模サーベイランスを行って来た事が明らかになっています。

このように年を追って複雑で高度になるサイバー犯罪やサイバー攻撃やサイバースパイ活動に対応していくためには、最新の情報セキュリティ技術を常に学習し続けることが必要です。

主催: dragostech.com inc. (ドラゴステック・ドットコム) 10966 84th Avenue, Edmonton, Alberta T6G0V4, Canada