CPV @ DC25

Thu Jul 27, 2017

1:30pm - 3:30pm Village Setup (Volunteers and Organizers Only)

Calendar: CPV @ DC25
Created by: Chaim Cohen

3:30pm - 4:30pm Volunteer Huddle

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen

Fri Jul 28, 2017

10am - 10:30am Welcome

Calendar: CPV @ DC25
Created by: Chaim Cohen

10:30am - 11am Hacking on Multiparty Computation

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Name: Matt Cheung Abstract: Secure multiparty computation is about
jointly computing a function while keeping each parties inputs secret. This comes off as an esoteric area of cryptography, but the goal of this talk is to introduce you to the core concepts through a history of the topic. I will conclude by demoing an implementation of an example protocol I implemented. Bio: Matt Cheung started developing his interest in cryptography during an internship in 2011. He worked on implementation of a secure multi-party protocol by adding elliptic curve support to an existing secure text pattern matching protocol. From this experience he has given talks and workshops at the Boston Application Security Conference and the DEF CON Crypto and Privacy Village. Twitter handle of presenter(s): nullpsifer

11am - 12pm SHA-3 vs the world

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Name: David Wong (NCC Group) Abstract: Since Keccak has been
selectedas the winner of the SHA-3 competition in 2012, a myriad of differenthash functions have been trending. From BLAKE2 to KangarooTwelve we'llcover what hash functions are out there, what is being used, and whatyou should use. Extending hash functions, we’ll also discover STROBE, asymmetric protocol framework derived from SHA-3. Bio: David Wong is aSecurity Consultant at the Cryptography Services practice of NCC Group.He has been part of several publicly funded open source audits such as OpenSSL and Let's Encrypt. He has conducted research in many domains in cryptography, publishing whitepapers and sharing results at variousconferences including DEF CON and ToorCon as well as giving a recurrentcryptography course at Black Hat. He has contributed to standards likeTLS 1.3 and the Noise Protocol Framework. He has found vulnerabilitiesin many systems including CVE-2016-3959 in the Go programming languageand a bug in SHA-3's derived KangarooTwelve reference implementation.Prior to NCC Group, David graduated from the University of Bordeauxwith a Masters in Cryptography, and prior to this from the Universityof Lyon and McMaster University with a Bachelor in Mathematics. Twitterhandle of presenter (s): lyon01_david Website of presenter(s) orcontent: https://www.cryptologie.net

CPV @ DC25

11:30am - 12pm

WS: Mansion Apartment Shack House: How To Explain Crypto To Practically Anyone

Where: Caesars Palace, Florentine Ballroom 3
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Name: Tarah Wheeler (Psychoholics) Abstract: Ever stuttered when someone asked you "So, what *is* cryptography, anyway?" We're all ininfosec but explaining crypto easily and memorably to people withoutmaking it too complicated or insulting their intelligence isnontrivial. Keeping it simple is never stupid, and we all need moreconverts to understanding that crypto isn't magic, it's just a bit ofmath and trust. I've explained crypto to project managers,congressional aides, third graders, CEOs, and 7-11 clerks. I've createdseveral memorable analogies and visual aides to help people understandthe simple beauty of crypto. You learned everything you need tounderstand crypto in grade school. After watching this talk, you'll beable to easily explain simple ciphers, transforms, what really happensin a key exchange, a few brief historical facts, and why crypto is soimportant. And maybe I'll get to a few of those really dumb jokes welike telling at crypto parties. That one about 2xROT-13 hasn't gottenold yet. Unfortunately. Bio: Born in a log cabin on the prairie to a___ and an itinerant ___, Tarah Wheeler had a humble upbringing offighting the status quo, sticking it to the man, and shooting prairiedogs because they're good eatin'. An emeritus member of the Order ofthe Orange Badge, Tarah has founded or been in the first 10 employeesof many successful companies, mostly because she hates filling out jobapplications. Her life now consists mainly of sitting in airplanes,punctuated by writing books that smash the patriarchy and givingspeeches where she tells people to stop sucking so much at security. Noone can guarantee that the old proverb about "liquor in the front,poker in the rear" wasn't written about Tarah, as she's a midlevel limit Texas holdem pro with a fondness for highland Scotch and lowlandcompany. Twitter handle of presenter(s): @tarah Website of presenter(s)or content: tarah.org

12pm - 1pm Alice and Bob are Slightly Less Confused

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Name: David Huerta (Freedom of the Press Foundation) Abstract: Two years ago at DEF CON I discussed UX issues affecting every kind ofencryption tool. Since then, much has improved. We'll go over some ofthe better examples of usable privacy technology and, like last time,go over some new challenges that still need to be addressed to makecrypto usable in the real world. This talk is a sequel to this one: https://www.youtube.com/watch?v=pkh7gUm82QY. Bio: David Huerta is aDigital Security Fellow at the Freedom of the Press Foundation, wherehe's working on ways to train journalists to take advantage ofprivacy-enhancing technology to empower a free press. He's organizeddozens of trainings across the US from Brooklyn to Phoenix. Beforearriving in New York, he was one of the founding members for HeatSyncLabs, an Arizona hackerspace which brings makers, hackers, and theoccasional futurist together to build things and teach others how to dothe same. Twitter handle of presenter(s): huertanix

12pm - 1pm WS: Breaking the Uber Badge Ciphers

Where: Caesars Palace, Florentine Ballroom 3
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Name: Kevin Hulin Abstract: This talk will discuss the algorithms and tools that were developed to defeat the Running Key Ciphers that appeared on the DEFCon 20 and DEFCon 23 Uber badges. I will give a quick overview of the probability background and demonstrate the (open sourced) tool's use. Bio: A competitive crypto-hobbyist, Cryptok (Kevin Hulin) spends his spare time puzzling on cross words and developing language-model-based cryptanalysis tools for fun (and little profit). He's competed with Muppet Liberation Front [MLF] to win the DEFCon Badge challenge three years and hopes to make this year his fourth. Twitter handle of presenter(s): @0xf0unD Website of presenter(s) or content: https://cryptok.space/crypto/

1pm - 2pm

Protecting Users' Privacy in a Location-Critical Enterprise: The Challenges of 9-1-1 Location

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Trey Forgety Abstract: Precise location data can reveal the most sensitive details of a person's life. But, in an emergency, its the most important part of saving that life. This talk will detail how 9-1-1 systems acquire, use, and store sensitive location data today, and how that process will change as we transition to an all-IP Next Generation 9-1-1 world. Bio: Trey Forgety is Director of Government Affairs and Information Security Issues at NENA: The 9-1-1 Association. A physicist, lawyer, sailor, and inveterate tinkerer, Trey served two years as a Presidential Management Fellow with tours in DHS, the FCC, and NTIA, where he worked with the White House to develop policy for a nation-wide LTE network for public safety, known as FirstNet. By day, he handles legal, regulatory, and legislative issues affecting the 9-1-1 sector. By night, he handles the InfoSec issues, too. #SmallNonProfitLife Twitter handle of presenter(s): @cincvolflt

1pm - 2pm WS: FeatherDuster and Cryptanalib workshop

Where: Caesars Palace, Florentine Ballroom 3
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Daniel Crowley (NCC Group) Abstract: Want to get into cryptanalysis but don't have any experience? Want to exploit a cryptobug but don't have the chops or don't have the time? FeatherDuster andits core library Cryptanalib are designed to help you performcryptanalysis faster and easier. This workshop will help you learn touse FeatherDuster, to write Python scripts which take advantage of common crypto vulnerabilities with functions built into Cryptanalib,and how to turn those scripts into FeatherDuster module Bio: DanielCrowley is a Senior Security Engineer and Regional Research Directorfor NCC Group Austin, tasked with finding and exploiting flaws ineverything from Web applications and cryptosystems to ATMs, smarthomes, and industrial control systems. He denies all allegations ofunicorn smuggling and questions your character for even suggesting it.He has been working in information security since 2004. Daniel isTIME’s 2006 Person of the Year. He has developed and released variousfree security tools such as MCIR, a powerful Web applicationexploitation training and research platform, and FeatherDuster, an automated modular cryptanalysis tool. He does his own charcuterie andbrews his own beer. He is a frequent speaker at conferences includingBlack Hat, DEFCON, Shmoocon, Chaos Communications Camp, and SOURCE.Daniel can open a door lock with his computer but still can’t launchICBMs by whistling into a phone. He has been interviewed by variousprint and television media including Forbes, CNN, and the Wall StreetJournal. He holds the noble title of Baron in the micronation ofSealand. His work has been included in books and college courses.Twitter handle of presenter(s): @dan_crowley

2pm - 3pm Breaking TLS: A Year in Incremental Privacy Improvements

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Andrew Brandt (Symantec) Abstract: I run a lab in which I let a lot of computers, as well as networked "IoT" devices, phone home, and then I use enterprise-level tools to decrypt and capture that TLS/SSL network traffic. In the past year, I've been observing a steady increase in the number of devices and services which flat-out refuse to let me decrypt their communications - an unequivocally Good Thing for privacy and security. But I've also witnessed some disastrous problems, such as large corporations, who should know better, behaving badly, using self-signed or expired certificates for critical sites used to, for instance, deliver firmware updates. In this overview, I'll discuss the good, bad, and really, really ugly things I've learned about what, how, and to whom these devices communicate, and in some cases, the contents of those communications. I'll also provide an overview of the tools and techniques I've used to re-sign certificates and capture the decrypted data, including how (and why) you can (and probably should) do this yourself. Finally, I plan to offer my own manifesto to businesses large and small about how they should do a much better job at protecting the privacy of their customers. Bio: Andrew Brandt is the Director of Threat Research for Symantec, whose previous employer was acquired in the past year. In his role, he runs a malware research lab in which he infects all manner of devices with malware and permits the devices to phone home, in order to learn more about how, and to whom, malware communicates. Twitter handle of presenter(s): @threatresearch

3pm - 4pm

A New Political Era: Time to start wearing tin-foil hats following the 2016 elections?

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Joel Wallenstrom Robby Mook Abstract: The most trivial communications were weaponized and drastically changed the course ofthe 2016 elections right before our eyes. As a result, informationsecurity is now a number one priority for all political campaigns —domestic and international. Yet many in the political community,including France, the UK, and the US, are deploying the same old practices, tools, and user training for communicating highly-sensitiveinformation. In addition to continuing to hoard high-target data,political parties and candidates are reluctant to change behaviors andask for help. Admitting to being hacked has become increasinglystigmatized, preventing under-resourced campaigns and the policycommunity from understanding how to deal with persistent andwell-funded adversaries. What have we learned and how likely is it thatthis will happen to election campaigns again? This talk will provide afirst-hand context for understanding the exact political, media andsecurity environments in which multiple breaches were detected on thedemocratic side of the 2016 campaign and how they went unmitigated formonths. The talk will then trace how, in the aftermath, the affected parties have attempted, successfully or not, to recover and learn towork with the infosec community. We will also touch on what impactproduct decisions in the tech and security space have on ordinaryusers’ ability to do their work, including running national campaigns.Finally, the talk will touch on ephemerality becoming a number onebehavioral change the ‘victims’ of the election hacking seek as anantidote to information weaponization. Bio: Joel Wallenstrom is the CEOof Wickr, a secure communications company building peer-to-peerencrypted ephemeral messaging and collaboration platforms. Prior tojoining Wickr, Joel co-founded and led several top white-hat hackerteams including iSEC Partners and NCC Group, renowned for their cuttingedge independent security research and incident response inhigh-profile cases. Joel also served as Director for StrategicAlliances at @stake. Robby Mook is a former campaign manager for a $1billion start-up called HFACC, Inc., more commonly known as Hillary forAmerica. Robby successfully ran the Virginia gubernatorial campaign forTerry McAuliffe, served as an organizer for Barack Obama's 2008 team inNevada, Indiana, and Ohio while working for Hillary Clinton's firstcampaign and leading the Democratic Congressional Campaign Committee.Twitter handle of presenter(s): @RobbyMook @mywickr Website ofpresenter(s) or content: wickr.com

3pm - 3:30pm

WS: NoiseSocket: Extending Noise to Make Every TCP Connection Secure

Where: Caesars Palace, Florentine Ballroom 3
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:

Author: Dmitry Dain (Virgil Security, Inc.) Alexey Ermishkin (Virgil Security, Inc.) Abstract: NoiseSocket is an extension of the Noise Protocol Framework (developed by the authors of Signal and currently used by WhatsApp) that enables quick and seamless Transport Layer Security (TLS) between multiple parties with minimal code space overhead, small keys, and extremely fast speed. NoiseSocket is designed to overcome the shortcomings of existing TLS implementations and targets IoT devices, microservices, back-end applications such as datacenter-to-datacenter communications, and use cases where third-party certificate of authority infrastructure is not optimal. This talk will introduce users to NoiseSocket, showcase demos and benchmarks, and provide information about publicly available implementations of NoiseSocket. Bio: Dmitry Dain: Random is an old-school hacker who started at Lucent working on early Wi-Fi (before it was Wi-Fi), later worked on the DARPA XG program which revolutionized wireless networking by combining cognitive radios, distributed sensor networks, and mobile ad hoc networks to provide Dynamic Spectrum Access, and ran his own privacy and security oriented file sharing company. Random is all about building tools that scale globally across every possible platform and programming language and loves nothing better than seeing another product ship that is #SecuredByVirgil. Alexey Ermishkin: Scratch is a passionate cryptomaniac, software developer, and Russian paranoiac. Crypto is his beloved branch of science since school and now he is doing full time R&D at Virgil Security. His dream is to #EncryptEverything Twitter handle of presenter(s): @dmitrydain Website of presenter(s) or content: https://github.com/noisesocket/spec

4pm - 4:30pm Security Analysis of the Telegram IM

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:

Author: Tomas Susanka (CTU Prague) Abstract: Telegram is a popular instant messaging service, a self-described fast and secure solution.It introduces its own home-made cryptographic protocol MTProto insteadof using already known solutions, which was criticised by a significantpart of the cryptographic community. In this talk we will brieflyintroduce the protocol to provide context to the reader and thenpresent two major findings we discovered as part of our securityanalysis performed in late 2016. First, the undocumented obfuscationmethod Telegram uses, and second, a replay attack vulnerability wediscovered. The analysis was mainly focused on the MTProto protocol andthe Telegram's official client for Android. Bio: Tomáš Sušánka studiedand lives in Prague and occasionaly other universities and citiesbecause, according to him, why not. He wrote his Master's thesis onTelegram IM and amongst other things discovered an undocumentedobfuscation and a possible vulnerability, which he then reported to thepowers that be. Earlier this year he graduated from FIT CTU andcurrently would like to move into the world of infosec. He's joiningCloudflare's crypto team for a summer internship in 2017. When hewasn't roaming the world and studying abroad he worked on a number ofweb applications, APIs and a Q&A mobile game. He likes to eatgrapefruits before going to bed and playing chess, as unlikely acombination as it sounds.

4pm - 4:30pm Underhanded Crypto Announcement

Where: Caesars Palace, Florentine Ballroom 3
Calendar: CPV @ DC25
Created by: Chaim Cohen

4:30pm - 5:30pm Cryptanalysis in the Time of Ransomware

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:

Author: Mark Mager (Endgame) Abstract: Crypto has served an important role in securing sensitive data throughout the years, but ransomware has flipped this script on its head by leveraging crypto as a means to instead prevent users from accessing their own data. The crypto seen in ransomware covers a wide range of complexity of symmetric and asymmetric algorithms, but flaws in their implementation and key storage / transmission routines have left the door open for users to retrieve their data in certain cases. In this talk, I'll provide a glimpse into some of the more notable ransomware crypto implementations that have surfaced over the past few years and how their weaknesses were exploited by security researchers through reverse engineering and cryptanalysis. Bio: Mark is a Senior Malware Researcher for Endgame. Throughout his career in software engineering and computer security, he has served in prominent technical leadership roles in the research and development of advanced computer network operations tools and has provided malware analysis and reverse engineering subject matter expertise to a diverse range of government and commercial clients in the Washington, D.C. metropolitan area. Twitter handle of presenter(s): @magerbomb Website of presenter(s) or content: https //www.endgame.com/our-experts/mark-mager

5pm - 5:30pm WS: Supersingular Isogeny Diffie-Hellman

Where: Caesars Palace, Florentine Ballroom 3
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:

Author: Deirdre Connolly Abstract: Post-quantum cryptography is an active field of research in developing new cryptosystems that will be resistant to attack by future quantum computers. Recently a somewhat obscure area, isogeny-based cryptography, has been getting more attention, including impressive speed and compression optimizations and robust security analyses, bringing it into regular discussion alongside other post-quantum candidates. This talk will cover isogeny-based crypto, specifically these recents results regarding supersingular isogeny diffie-hellman, which is a possible replacement for the ephemeral key exchanges in use today. Bio: Deirdre is a senior software engineer at Brightcove, where she is trying to secure old and new web applications. Her interests include web application security, post-quantum cryptography, elliptic curves and their isogenies. Twitter handle of presenter(s): durumcrustulum

5:30pm - 6:30pm Unfairplay (NOT RECORDED)

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: [anonymous panel] Abstract: This panel includes developers and reverse engineers who cut their teeth building the most high-profile DRM system in history. They are now well-respected members of the security community and for the first time ever will be sharing their story. Bio: This panel includes developers and reverse engineers who formerly worked at a fruit company.

Sat Jul 29, 2017

10am - 10:30am Welcome

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen

10:30am - 11:30am The Surveillance Capitalism Will Continue Until Morale Improves

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: J0N J4RV1S Abstract: Surveillance Capitalism is a form of information monetization that aims to predict and modify human behavior as a means to produce revenue and control. It strives to be a pervasive background collector of our cyberspace and meatspace activities, attempting to both generate and profit from data collected about our wants and needs. It's what happens when Marketing decides to plagiarize from the NSA's playbook. The methods used by Surveillance Capitalism's practitioners are intentionally becoming harder to detect, trickier to thwart, and increasingly convoluted to opt-out from. Merchandisers, content producers, and advertising networks are actively seeking and developing new technologies to collect and correlate the identities, physical movements, purchasing preferences, and online activity of all of us, their desperately desired customers. This presentation will discuss existing data collection methods and review your options to avoid being profiled and tracked without your consent. Skip this session if you're already familiar with and are prepared to defend against: - Instant facial recognition & correlation at scale - Geofenced content delivery & user identification - Retailer & municipal Wi-Fi tracking - Unblockable browser fingerprinting - Cross-device tracking & ultrasound beaconing - Inescapable data brokers, IoT, and more.... Surveillance Capitalism is entrenched, it's profitable, and it's spreading. Ethical engineering, disposable personas, and extreme compartmentation may be the only chance for Privacy's survival. Bio: J0N J4RV1S has been plugged into the Internet since the early 90's and he wants to help make it a safer place for everyone. He is a proponent of data privacy, usable encryption, InfoSec diversity, digital security training, Utah's tech scene, and leaving things better than you found them. Twitter handle of presenter(s): @SecureUtah

11am - 12:30pm WS: Implementing An Elliptic Curve in Go

> **Where:** Caesars Palace, Florentine Ballroom 3
> **Calendar:** CPV @ DC25
> **Created by:** Chaim Cohen
> **Description:**
> Author: George Tankersley Abstract: Elliptic curve implementations - dark magic, right? We all copy the mysterious bit twiddles and havemechanically ported nacl everywhere. But what the hell are we actuallydoing? I recently implemented Ed25519 from scratch in both pure Go and(dramatically faster) amd64 assembly, spending a frankly pathologicalamount of time to be sure I understood what I was doing, for a change.Now I'd like to share that. I'll explain the code (mine, and byextension ref10, donna, and amd64-51-30k from SUPERCOP) and the underlying concepts / design decisions behind it all. Then I'll talkabout how I made the code fast - endianness tricks with Big.Ints, whyassembly doesn't always mean faster, how the inlining model of thecompiler works, and some tools you can use to make writing Plan9 asmless awful. Talk MAY use the “make it Go fast” joke but implementersSHOULD avoid the temptation. Bio: George Tankersley is a cryptography engineer at Cloudflare working on anonymous credentials, certificatetransparency, and crypto at scale. For fun he works on anonymity toolsand - very occasionally - even does some things that *don't* involveteaching eldritch geometry to thinking machines. Twitter handle ofpresenter(s): @gtank__ Website of presenter(s) or content:https://gtank.cc

11:30am - 12pm

> ### Privacy is Not An Add-On: Designing for Privacy from the Ground Up
>
> **Where:** Caesars Palace, Florentine Ballroom 4
> **Calendar:** CPV @ DC25
> **Created by:** Chaim Cohen
> **Description:**
> Author: Alisha Kloc Abstract: You want to design customer-focused, easy-to-use products that your customers will love - but you aren’tdoing your job if you wait until the last minute (or beyond!) to thinkabout privacy. Tacking on privacy features as an afterthought isn’tonly bad for your users, it’s also bad for your company. Privacy startswith your backend systems and carries forward through your productdevelopment cycle, your user testing, your product release, and all theway to your customer support. Learn how to build privacy into yourproducts from the ground up, and create an awesome privacy story forboth your company and your users. Bio: Alisha Kloc has worked in thesecurity and privacy industry for over eight years, at companiesranging from startups to global powerhouses. Her focus is on protecting users’ data and developing industry-leading security and privacyprograms. She is an advocate for user data protection, speaking atconferences across the US and Europe to highlight security & privacyissues and encourage people to choose security & privacy careers.Alisha is passionate about data security and user privacy, and believesin combining engineering, technology, policy, and culture to ensureusers’ protection. Twitter handle of presenter(s): @alishakloc

CPV @ DC25

12pm - 1pm Operational Security Lessons from the Dark Web

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Shea Nangle Abstract: The past 5 years have seen a number of arrests and a number of convictions of parties engaged in criminal activities on the Dark Web. From Dread Pirate Roberts to French Maid, Willy Clock to Shiny Flakes, and others, we will explore operational security failures made that led to their arrests, and in some cases, convictions. Why look at this? There are lessons to be learned from these cases even if you aren't in a position to be accused of running a multinational drug distribution ring. Whether you concerned with surveillance and/or reprisals from hostile nation-states or are simply wanting to better guard your privacy, we can all learn from these cases. Attendees will leave this session with concrete tactical recommendations for increasing the operational security of their online lives and protecting their privacy. Bio: Shea Nangle works in information security in the Washington DC area. His areas of interest include open source intelligence, operational security, and forensics. In his spare time, you can often find him homebrewing and attending heavy metal concerts. Twitter handle of presenter(s): @ultrashea

12:30pm - 1:30pm WS: Secrets Management in the Cloud

Where: Caesars Palace, Florentine Ballroom 3
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Evan Johnson Abstract: Secrets management in the cloud is a very hot topic. It's something every company must solve and is actually a fairly new problem with the meteoric growth of microservices and ephemeral services. Let's take a practical look at how Segment handles secrets on AWS. We will talk about different secrets management tools, when they are appropriate, and different models for protecting secrets. Bio: Evan Johnson is a Security Lead at Segment. He previously did security and engineering work at Cloudflare and LastPass. He enjoys long walks in San Francisco and copious amounts of diet pepsi.

1pm - 2pm The Symantec/Chrome SSL debacle - how to do this better...

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Jake Williams (Rendition Infosec) Abstract: When Google announced an intent to revoke trust from certificates issued bySymantec, this set off alarm bells all over the certificate authorityindustry. But that was March. What actually happened? Rendition Infosechas periodically tracked the SSL certificates on the Alexa top 1million sites. In this talk, we'll review that data set and examinewhat, if any, changes the Google announcement regarding Symantec certshad on certificate renewal/reissuance. We'll also offer realisticsuggestions for revoking trust in the future – had this been an actualfire drill, we'd have been burned alive. Bio: Jake Williams, thefounder of Rendition Infosec, has almost two decades of experience in secure network design, penetration testing, incident response,forensics and malware reverse engineering. Prior to founding RenditionInfosec, Williams worked with various government agencies ininformation security and CNO roles. He also works with SANS where heteaches and co-authors the Malware Reverse Engineering, MemoryForensics, Cyber Threat Intelligence, and Advanced Exploit Development.He is the two time victor of the annual DC3 Forensics Challenge. He hasspoken at Blackhat, Skytalks, Shmoocon, CEIC, RSA, EnFuse, DFIR Summitand DC3 Conference (and some we're forgetting here). His research areasinclude automating incident response throughout the enterprise, binaryanalysis, and malware C2. The primary focus of his work is increasingenterprise security by presenting complex topics in a way that anyonecan understand. Twitter handle of presenter(s): @malwarejake Website ofpresenter(s) or content: www.rsec.us

2pm - 3pm

Have you seen my naked selfies? Neither has my snoopy boyfriend. Privacy within a Relationship

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Lauren Rucker Abstract: Privacy is fairly cut and dry when it's US verses THEM, but what if it's ME verses YOU within US? What are YOURPrivacy Rights, in the context of OUR relationship? Am I yournon-trusting girlfriend? Am I your controlling boyfriend? Am I yoursnooping wife? Am I your abusive husband? How do YOU protect yourprivacy from ME? I will be providing tips, techniques, and resources toenable someone (anyone – even YOU) to protect their Privacy in arelationship, perhaps even one with ME. Highlights will include waysyou can be surveilled, at home techniques you can use to protectyourself when using your phone and computer, and individual privacyrights within a marriage. Presented by someone who may have needed theinformation, and had to discover this path themselves, and is zealous about assisting those in need of this talk. Even YOU. Bio: LaurenRucker is a threat intelligence analyst for NASA, with experience inthreat assessment, vulnerability analysis, risk assessment, informationgathering, correlating and reporting. Lauren is a former militaryintelligence officer that served at U.S. Cyber Command and U.S. Strategic Command. She is currently a graduate student earning hermaster's in cybersecurity and is passionate about making cybersecuritypractices relatable to the average internet user. Twitter handle ofpresenter(s): @laurenkrucker

2pm - 4pm WS: SECURE COMMUNICATIONS IN ANDROID WITH TLS/SSL

Where: Caesars Palace, Florentine Ballroom 3
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Miguel Guirao Abstract: Secure Communications in Android is an introductory talk into the amazing cryptographic technology of OpenSSL, that has helped us to achieve what the Internet is today, and the tasks we can perform on it. OpenSSL as become since many years ago, the defacto library/tool for implementing cryptographic protocols into our applications and secure them. Of course, this task is not that easy as it sounds, in order to achieve a secure communication in our applications, we not only have to choose the more secure library, but also, have the knowledge to implement it in a secure manner and more. This talk aims to teach you the basics of the world of criptography, then an introduction to the implementation of OpenSSL in Android, then three coding labs in Android in order to learn how to integrate the OpenSSL library and implement the cryptographic protocols into your own applications. You will learn to: What is Cryptography and it's basics What is OpenSSL and what it is used for The Android implementation of OpenSSL Coding Lab 1: Creating Secure Sockets (SSL/TLS sockets) Coding Lab 2: Working with Certificates Coding Lab 3: Working with Message Digest Coding Lab 4: Implementing a Client-Server Secure Communication Bio: Miguel Guirao (aka Chicolinux), as been in the information security industry for around ten years, he is a freelance consultant at Futura - Open Solutions, where he also has been training professionals about Linux Management, Information Security and Programming. He has been also a professor since 2009 for the Anahuac Mayab University where he teaches at the School of CS Engineering and at the School of Multimedia Design. He teaches Information Security in the Master of Information Technology Management. He holds a GCIH Certification from SANS. He is a SANS Mentor. This is the second time that Miguel participates at DEFCON, last year at DC24 he taught INTRO TO MEMORY FORENSICS WITH VOLATILITY workshop. Twitter handle of presenter(s): @miguelguirao

3pm - 3:30pm Yet another password hashing talk

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Evgeny Sidorov (Yandex) Abstract: Password hashing seems easy -just take a memory hard function, apply it to a password and you’redone. It might be so unless you have a high loaded web service withtight requirements for performance and response times and you need toachieve as maximum security as possible keeping in mind obviouscomputation DoS attacks (memory hard functions are hard not only forattackers, aren't they?). In this talk I'll give an overview of modernapproaches to password hashing. We’ll discuss some details about Argon2(d, i, id) and Yescrypt algorithms and different approaches to passwordhashing used in big Internet companies (what schemes are used, how toselect parameters for algorithms etc.). In addition, I'll present ouropen source library Argonishche* that contains implementations ofArgon2 and Blake2B optimized for SSE2, SSSE3, SSE4.1 and AVX2instruction sets and uses runtime CPU dispatching to achieve maximum performance on CPUs with different SIMD extensions supported. * inRussian suffix "-ищ" (-ishch) means something that is bigger thanordinary and that scares small children. In this case - something thatis bigger than Argon :) Bio: Evgeny Sidorov is a Security Engineer atYandex. Evgeny works in the Product Security Team and is responsiblefor developing and embedding various defense techniques in web and mobile applications. He finished his degree in applied mathematics atthe Institute of Cryptography, Telecommunications and Computer Scienceof Moscow.

3:30pm - 4pm Core Illumination: Traffic Analysis in Cyberspace

> **Where:** Caesars Palace, Florentine Ballroom 4
> **Calendar:** CPV @ DC25
> **Created by:** Chaim Cohen
> **Description:**
> Author: Kenneth Geers (Senior Research Scientist, Comodo) Abstract: Theinformation security discipline devotes immense resources to developingand protecting a core set of protocols that encode and encrypt Internetcommunications. However, since the dawn of human conflict, simpleTraffic Analysis (TA) has been used to circumvent innumerable securityschemes. TA leverages metadata and hard-to-conceal network flow datarelated to the source, destination, size, frequency, and direction ofinformation, from which eavesdroppers can often deduce a comprehensive intelligence analysis. TA is effective in both the hard and softsciences, and provides an edge in economic, political, intelligence,and military affairs. Today, modern information technology, includingthe ubiquity of computers, and the interconnected nature of cyberspace,has made TA a global and universally accessible discipline. Further,due to privacy issues, it is also a global concern. Digital metadata,affordable computer storage, and automated information processing nowrecord and analyse nearly all human activities, and the scrutiny isgrowing more acute by the day. Corporate, law enforcement, andintelligence agencies have access to strategic datasets from which theycan drill down to the tactical level at any moment. This paperdiscusses the nature of TA, how it has evolved in the Internet era, and demonstrates the power of high-level analysis based on a largecybersecurity dataset. Bio: Kenneth Geers (PhD, CISSP) is a ComodoSenior Research Scientist based in Toronto, Canada. Dr. Geers is also aNATO Cooperative Cyber Defence Centre of Excellence (CCD COE)Ambassador, a Non-Resident Senior Fellow at Atlantic Council, anAffiliate with the Digital Society Institute-Berlin, a member of theTransatlantic Cyber Forum, and a Visiting Professor at Taras ShevchenkoNational University of Kyiv in Ukraine. Kenneth spent 20 years in theU.S. Government, with time in the U.S. Army, at NSA, NCIS, and NATO,and was a Senior Global Threat Analyst at FireEye. He is the author“Strategic Cyber Security”, Editor of “Cyber War in Perspective:Russian Aggression against Ukraine”, Editor of “The VirtualBattlefield: Perspectives on Cyber Warfare”, Technical Expert to the“Tallinn Manual”, and author of many articles and chapters on cybersecurity. Twitter handle of presenter(s): @KennethGeers

4pm - 5pm rustls: modern, fast, safer TLS

> **Where:** Caesars Palace, Florentine Ballroom 4
> **Calendar:** CPV @ DC25
> **Created by:** Chaim Cohen
> **Description:**
> Author: Joseph Birr-Pixton (Electric Imp) Abstract: rustls is a new open-source TLS stack written in rust. This talk covers past TLS standard and implementation errors, and how those are avoided in rustls's design. Bio: I'm Joe, from Cambridge, England. I've been working in crypto, computer security and embedded development since 2005; building HSMs, mobile authentication, and securing IoT devices. Twitter handle of presenter(s): @jpixton Website of presenter(s) or content: https://jbp.io

5pm - 5:30pm Blue Team TLS Hugs

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Lee Brotherston Abstract: TLS, and it’s older forerunner SSL,are used to maintain the confidentiality and integrity of networkcommunications. This is a double edged sword for Information Securitydepartments as this allows private information to remain private, butcan also be used to hide malicious activity. Current defensive measuresfor dealing with network traffic encrypted using TLS typically takesone of two forms: - Attempting to detect malicious activities via othermeans which are outside of the encrypted session, such as endpointsecurity tools and IP address blacklists. - Break the TLS trust modelby effectively attacking all connections, including trustedconnections, via MiTM with a trusted certificate. (yes AV vendors, I'm looking at you) This talk discusses (ok maybe rants about) the problemswith the current "state of the art" and introduces other techniques,such as TLS Fingerprinting and TLS Handshake Mangling, which can beused to solve the same problems with less of the issues of currentsystems. Bio: Lee Brotherston is a Director of Security for a startupin the Toronto area. Having spent nearly 20 years in InformationSecurity, Lee has worked as an Internal Security resource across manyverticals including Finance, Telecommunications, Hospitality,Entertainment, and Government in roles ranging from Engineer to ITSecurity Manager. He's also old enough to have done computering on aCommodore 64. Twitter handle of presenter(s): @synackpse

5:30pm - 6pm

Automated Testing using Crypto Differential Fuzzing (DO NOT RECORD)

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Yolan Romailler (Kudelski Security) Abstract: I present a new approach to test crypto software we developed together with JP Aumasson: differential fuzzing and our newly released tool, CDF, implementing it along with many edge case tests for common algorithms such as ECDSA, DSA and RSA. CDF also features time leakage detection. CDF allowed the discovery of issues in high-profile, widely used crypto software components such as Go's crypto package, OpenSSL, and mbedTLS. It i easy to use CDF to test your own library and everything is performed in a black-box fashion, so you only need to provide CDF with an executable to test it. Bio: Yolan Romailler is a Security Researcher at Kudelski Seucrity, where he delves into (and dwells on) cryptography, crypto code, and other fun things. He graduated in mathematics at EPFL and later in information security at HES-SO, both in Switzerland. Twitter handle of presenter(s): anomalroil

Sun Jul 30, 2017

10:30am - 11am Welcome

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen

11am - 12pm WS: Reasoning about Consensus Algorithms

Where: Caesars Palace, Florentine Ballroom 3
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Zaki Manian Abstract: Consensus algorithms play an incredibly important role in many cryptographic systems from the Tor Directory authorities to cryptocurrencies to enterprise blockchains. Each of these systems use different processes to securely update the state of the system. After decades of minimal progress, a new consensus research seems to appear almost every day. This talk presents a framework for thinking about the diversity of approaches to consensus and evaluating the algorithm's security properties. Bio: Zaki is an activist, entrepreneur and researcher in the world of applied cryptography projects. He is a founder of a blockchain company called Skuchain and has contributed to projects from ZCash to Tendermint. Twitter handle of presenter(s): zmanian

11:30am - 12pm Cypherpunks History

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Ryan Lackey (ResetSecurity, Inc.) Abstract: We will go over the history of the 1990s cypherpunks and major topics discussed during that period -- including remailers, the first discussions of crypto currencies, and various forms of anonymous electronic markets. In addition, we will present a free archive of the mailing list and topics for future research. Bio: Ryan Lackey has been a cypherpunk for over 20 years. He founded the world's first offshore datahaven, HavenCo, on Sealand in 2000. He was involved with pre-cryptocurrency anonymous digital currencies backed with gold and other assets, and worked in Iraq, Afghanistan, and other conflict zones, bootstrapping a satellite and wireless communications company. Later, he founded a Y Combinator-backed startup, CryptoSeal, which he sold to Cloudflare in 2014. After working at Cloudflare for the following two years, he founded ResetSecurity, a travel security company, in 2016. Twitter handle of presenter(s): @octal

12pm - 12:30pm

The Key Management Facility of the Root Zone DNSSEC KSK

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Punky Duero (ICANN - PTI) Abstract: Take a rare peak on the facility that helps secure the Root DNSSEC Key Signing Key and learn its recent activities including the key rollover. Understand what happens during a typically behind closed door key ceremonies. Bio: Punky Duero, a Filipino dude who once set course to California in search for opportunities after receiving his Bachelor's degree in Computer Science from the Philippines. During his journey, he settled in Fukushima and Yokohama, Japan for almost a year to help tinker and test software for NEC mobile phones. Upon arriving in California, he helped commercial and government facilities deploy security systems to secure their assets from James Bond and Ethan Hunt. In 2014, he joined the folks that helps manage the address book of the Internet and settled for the time being. Twitter handle of presenter(s): punkyduero

12:30pm - 1:30pm The Policy & Business Case for Privacy By Design

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Zerina Curevac (Squire Patton Boggs) Abstract: See no personal data, hear no personal data, and speak no personal data. For someorganizations, requests for data by users and law enforcement are sofrequent that entire departments are dedicated to handling these typesof inquiries and providing information. To be able to respond to suchrequests, organizations need to invest in IT infrastructure, security,and legal advice just for starters. The status quo has been to respondto such requests despite the increase in demand, but is handing over “personal” data in the interest of the organization or the user?Privacy by design controls are able to reduce some or most of theburden associated with such requests by minimizing the “personal” dataheld by an organization. This presentation will introduce Privacy byDesign concepts, provide examples of successful implementations ofPrivacy by Design, and explain how Privacy by Design can improve consumer reputation and trust. Bio: Zerina Curevac focuses her practiceon data privacy and cybersecurity, as well as other corporatetechnology matters. She is a Certified Information Privacy Professionalin U.S. privacy law (CIPP/US) and has worked with clients in the U.S.,EU and Asia Pacific on a range of matters, such as HIPAA compliance,EU-US Privacy Shield certification and EU General Data Protection Regulation ("GDPR") preparation. Her approach to data protectionoptimizes business goals and strategy and supports technologyinvestments. Twitter handle of presenter (s): zericure Website ofpresenter(s) or content:http://www.squirepattonboggs.com/en/professionals/c/curevac-zerina

1:30pm - 2pm The Why and How for Secure Automatic Patch Management

Where: Caesars Palace, Florentine Ballroom 4
Calendar: CPV @ DC25
Created by: Chaim Cohen
Description:
Author: Scott Arciszewski (Paragon Initiative Enterprises, LLC) Abstract:
The life cycle of a software vulnerability begins when a developer makes a mistake. A lot of software security best practices aim for lessening the time until vulnerabilities are discovered, or the time between discovery and patch availability. Unfortunately, most software projects have zero control over security patch deployment. Bio: Scott (CDO, Paragon Initiative Enterprises) resides at the intersection of PHP, security, cryptography, and open source software. Twitter handle of presenter(s): @CiPHPerCoder Website of presenter(s) or content: https://paragonie.com

2pm - 3pm Closing

Calendar: CPV @ DC25
Created by: Chaim Cohen