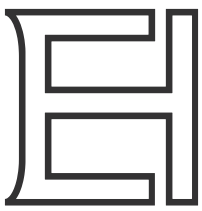
SECURI-TAY 2019

PROGRAMME

SECURI-TAY 2019

PRESENTED BY



Abertay Ethical Hacking Society

team@hacksoc.co.uk

@AbertayHackers

DESIGN BY

Cari Watterton

@cariwatterton

behance.net/cari-watterton

WELCOME

Hello and welcome to Securi-Tay 2019.

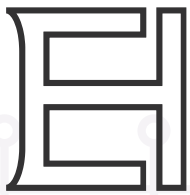
Securi-Tay is organised each year by the Ethical Hacking Society and we're pleased to announce that this is the 8th year the event has been run. Each year builds on the previous work by the Society to make Securi-Tay an enjoyable event. The conference takes a lot of time and patience to plan and all our members and the committee work throughout the year to make this event happen. We'd like to take the time at this point to thank all of our members for their support in helping to organise the conference as well as supporting our weekly meetings by creating quality content in the form of talks and workshops. We would also like to thank the staff of the Abertay Student Association as without them Securi-Tay would not be the event it is today.

We are excited to have over 20 fantastic talks this year as well as having a lockpicking village. Everything you need to know about the conference is located within this programme including a map to help find your way around. If you require any help please find one of our volunteers in yellow T-Shirts, or a committee member in bright pink.

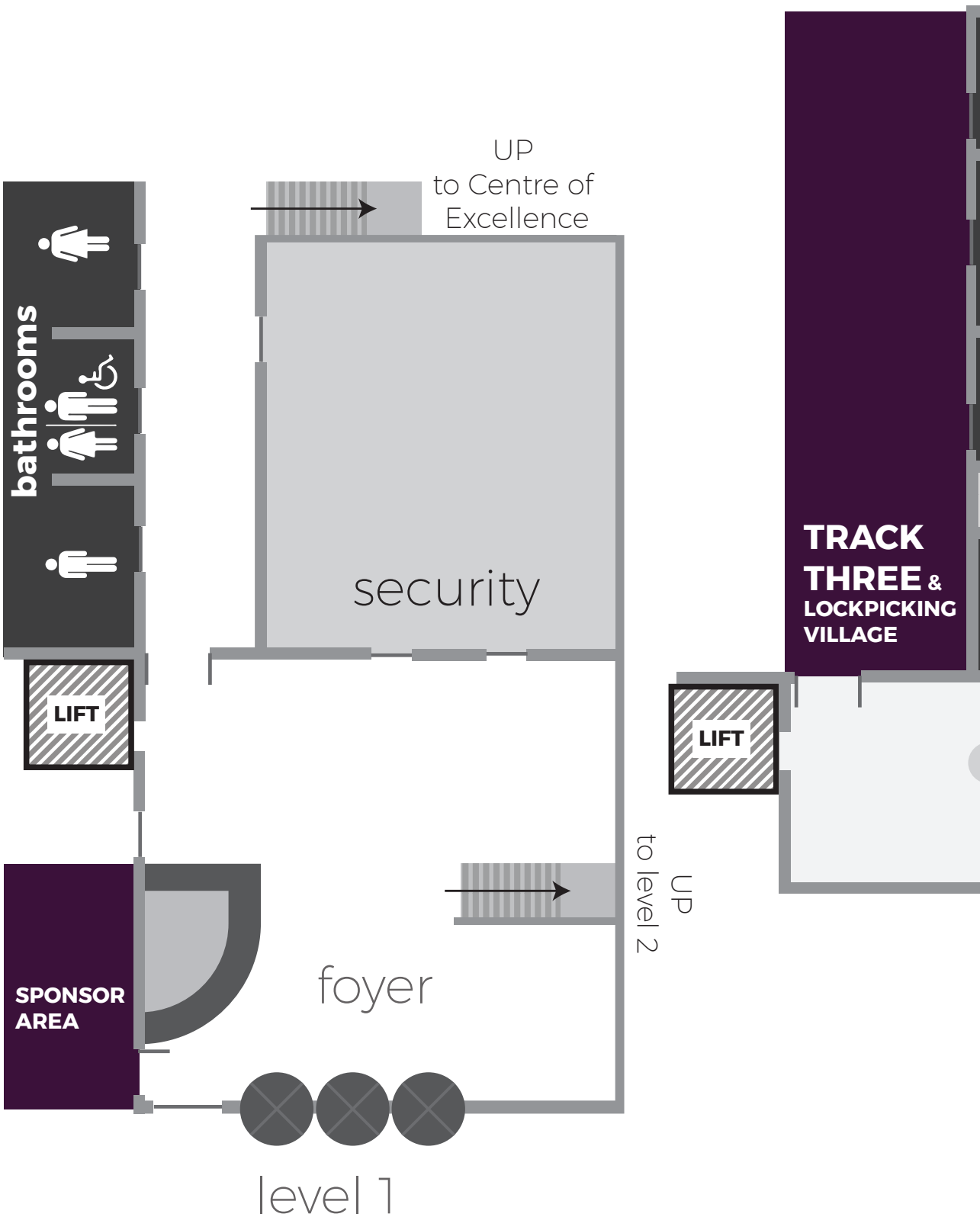
As we pride Securi-Tay on having good talks we would like to say a special thank you to all our speakers, as without them there would be no Securi-Tay. Finally, we would like to say a big thank you to our sponsors who provide invaluable support by funding the conference, please go see them in Room 1502 (The first left as you enter the university building).

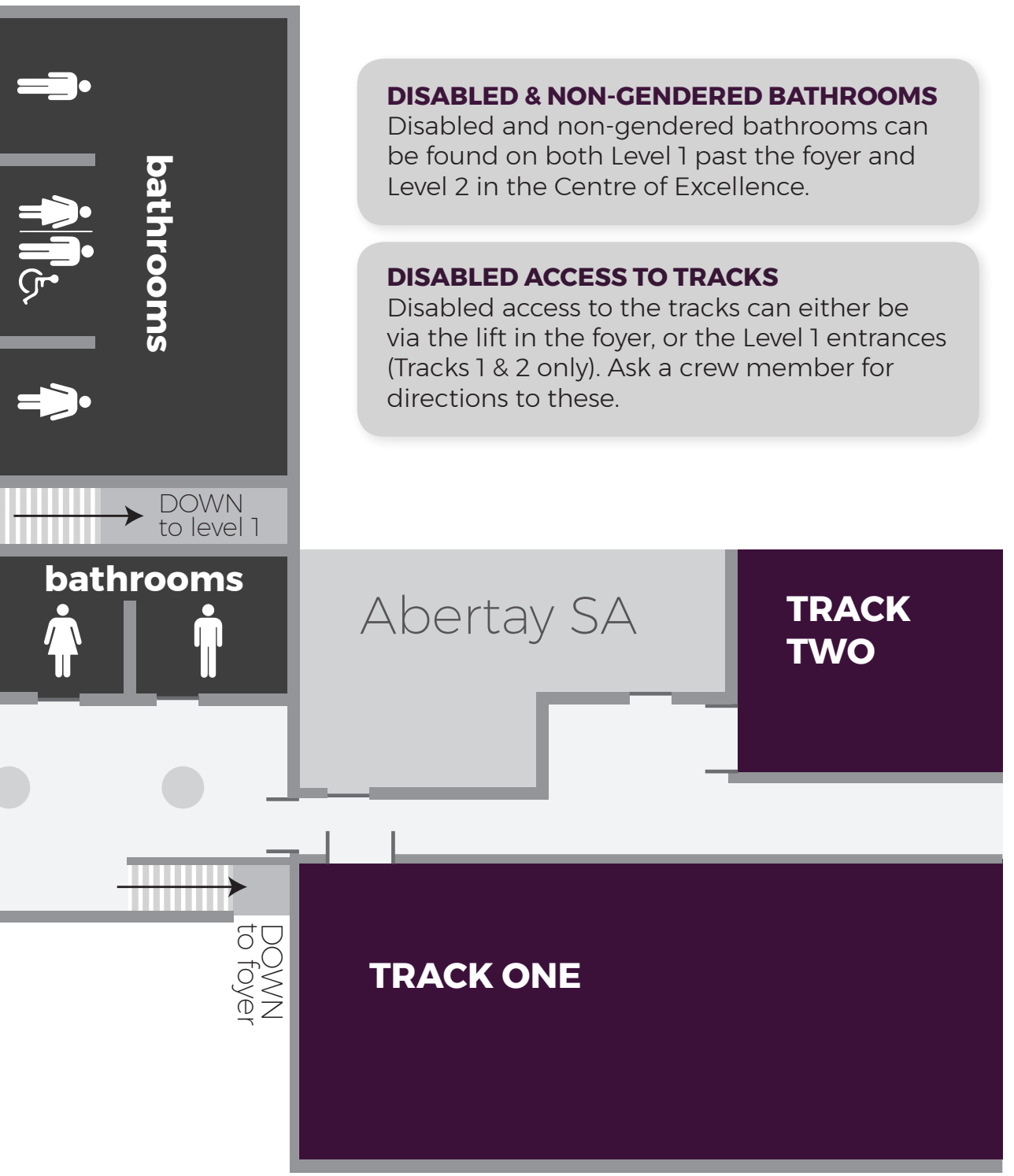
We hope you have a brilliant day.

Kind Regards,
The Committee



MAP


UP
to Centre of
Excellence
bathrooms
security
TRACK
THREE &
LOCKPICKING
VILLAGE
LIFT
LIFT
SPONSOR
AREA
foyer
UP
to level 2
level 1



DISABLED & NON-GENDERED BATHROOMS
Disabled and non-gendered bathrooms can be found on both Level 1 past the foyer and Level 2 in the Centre of Excellence.

DISABLED ACCESS TO TRACKS
Disabled access to the tracks can either be via the lift in the foyer, or the Level 1 entrances (Tracks 1 & 2 only). Ask a crew member for directions to these.

level 2

JOIN CYBER SECURITY AT CAPITAL ONE

We're one of the UK's top 10 credit card providers, so keeping our millions of customers safe is vital for our business. For a Cyber professional like you that means an opportunity to make a difference, learn and grow.

We're making finance simpler and more human. So our cutting-edge products need to work for our customers as well as being super secure.

Protecting our customers means bringing together the smartest people, new technologies (we're already in The Cloud), new products, new ideas and new ways of working. That's why we're after the brightest brains to join our team.

Current Vacancies

Cyber Security Consultant
Nottingham

Cyber Incident Response Specialist
Nottingham

Threat Modelling Engineer
London/Nottingham

Senior Cyber Security Consultant
Hybrid Environments
London/Nottingham

Senior Penetration Tester
London/Nottingham

Senior Cyber Engineer
London/Nottingham

Lead Cyber Engineer
London

Come and meet us:
www.meetup.com/London-Cyber-Capital-One

CAPITALONECAREERS.CO.UK

#LifeAtCapitalOne

THERE'S MORE TO CAPITAL ONE THAN CREDIT

25 days holiday + option to buy up to 5 more

On-site health and fitness facilities

Interest-free travel season ticket loans

Educational Assistance Programme

glassdoor
2018 BEST PLACES TO WORK
EMPLOYEES' CHOICE

QUICK REFER

	TRACK 1	TR
09:45		Introduction
11:00	We take your security seriously. Or do we?	Beyond Windov Micr
12:00	7 Hardware Hacks for 7GBP	RATs, Crypters Cons
12:30		
13:00		
14:00	Ridiculous Radios	Physical Securit Building CTF
15:00	Hardware Isn't Hard	Mobile Applicati Busine
15:30		
16:00	Where 2 Worlds Collide: Bringing Mimikatz et al to UNIX	Weap
16:30		
17:00		
17:15		Closing Keynote: IS
18:15		Closi
18:30		MWI

RENCE

RACK 2	TRACK 3
& Synopsys Keynote	
ws Forensics with Built-in rosoft Tooling	Student Lightning Talks
s & Zombies: A History of umer Malware	Profiling The Attacker - Using natural language processing to predict crime
	Using Natural Language Processing Techniques to Crack Passwords
LUNCH	
ty Games: Lessons Learnt Challenges for Hackers	Striking While The Iron's Hot - The do's and dont's for getting a job in infosec
ion Hardening: Protecting ess Critical Apps	From Breaking In to Breaking Through
	Intro to Machine Learning for Hackers
onising Layer-8	It might get loud! Exfiltrating data using audio interfaces
	Back to School: Bringing it Back to the Students
BREAK	
SIS Online: Junaid Hussain	
ing Remarks	
R Afterparty	

KEYNOTE

09:45 Software Security: Never Stop Evolving

From the early days of software bugs through to the modern day, software security practitioners have had to adapt to a cascade of paradigm shifts. As technology has increased in complexity, so have the attack vectors. Not only have we played cat and mouse with the attackers and their evolving attacks, but we've had to adapt to how software development has gone from Waterfall to Agile to DevOps.

As security finally appears to have won enough credibility to be given a voice in software development, there are opportunities and risks. In this talk, I will focus on software security specifically, some of its history, the current challenges, and how you as a security subject matter expert can help shape its future.

NICK MURISON

Nick is the head of software security services for Nordics and BeNeLux within Synopsys' Software Integrity Group. He's spent the last 14 years in the security industry, working within R&D, security assessment services, incident response, training, and strategic security initiative development. Combining his passion for software security and butchering multiple languages, Nick helps customers in FinTech, IoT, Embedded Systems and other industries build high quality secure software faster. Nick holds a MSc in Information Security from Royal Holloway, University of London.

TRACK 1

11:00 We take your security seriously. Or do we?

In this talk, we discuss the lengths some organisations go to, in order to protect personal data, as opposed to those that say they do, once the personal data they were responsible for has been flooded onto the Web.

It's a tale of breach after breach after breach, laced with some hope that certain firms are at least trying to do the right things. We all make mistakes, but we should at least give it our best shot at avoiding doing so.

MIKE THOMPSON, SEAN WRIGHT & ANDY GILL

"Mike Thompson, Sean Wright and Andy Gill, doing a Beer Farmers 'gig'.

Mike is a relative newcomer to the community, but has a passion and enthusiasm to help educate and improve the security of the citizens of the web. Mike was also invited to deliver his talk on web application firewall technology at 2018's Securi-Tay, however had to withdraw due to a dental fail.

Sean is a Lead Software Security Engineer and OWASP chapter leader, with a special interest in web based security as well as TLS security. He has presented at talks around the UK and is passionate about user security, education and awareness.

Andy is a hacker at heart, who's always been interested in taking things apart and sometimes even putting them together again(in-fact he spent a good few years in computer repair and data recovery). As his day job, Andy works as a senior penetration tester who is capable of delivering a wide spectrum of assessment types. He has delivered many talks around the UK and is well respected for his depth of knowledge, as well as irreverent presentation style

All members of The Beer Farmers; a parody project, who's aim in life is to help the InfoSec community take itself less seriously, bring some fun, while at the same time help us focus on the important things in what we do."

12:00 7 Hardware Hacks for 7GBP

We may live in a software world, but all that software runs on hardware at some point down the stack. Sure, you need some hardware to talk to hardware, but that shouldn't be a barrier to entry. The cost of a couple pints is enough to get a device to help you.

I'll demonstrate 7 different cases where you can use an FT232H-based board or cable to pull off a hardware hack, including:
- Getting a root shell over a UART
- Modifying I2C configuration of a device
- Sniffing a hardware bus as a Logic Analyzer
- Dumping flash off a device for offline analysis
- Backdooring firmware and flashing it to a device
- Jtag debugger
- Replaying custom crafted protocol packet

Hopefully you'll come away with the confidence and know-how to tackle a hardware attack of your own.

JOE FITZPATRICK

Joe FitzPatrick (@securelyfitz) is an Instructor and Researcher at SecuringHardware.com. Joe has spent over a decade working on low-level silicon debug, security validation, and penetration testing of CPUS, SOCs, and microcontroller. He has spent the past 5 years developing and leading hardware security-related training, instructing hundreds of security researchers, pen-testers, hardware validators worldwide. When not teaching classes on applied physical attacks, Joe is busy developing new course content or working on contributions to the NSA Playset and other misdirected hardware projects, which he regularly presents at all sorts of fun conferences.

14:00 Ridiculous Radios

There are many Software Defined Radios (SDRs) available, with a great deal of time and effort having gone in to their design. These are not those radios. I present four radios that we have designed using crude, novel, and sometimes ridiculous methods for transmitting and receiving signals.

The arrival of SDR allowed more hackers than ever to experiment with radio protocols, but we're still using hardware built by other people. In the time honored hacker tradition of rolling our own tools, we'll demonstrate four simple radios that can be home-built using commonly available parts for little to no cost.

DOMINIC SPILL

Tim Brown joined Cisco as part of their Dominic is a senior security researcher at Great Scott Gadgets, where he builds tools and investigates communications protocols.

15:00 Hardware Isn't Hard

With the advent of IoT connected everything - doorbells, dishwashers, ovens, alarms, and uh... more private items - you may be interested to try your hand at pwning some devices. Messing with web portals and network traffic is one thing, but what about the board itself? What do those components do? What is that chip doing? How do I not electrocute myself? All equally important questions. This talk covers the basic hardware knowledge you need to start picking apart boards, accessing debug functionality, dumping firmware, and finding juicy secrets.

GRAHAM SUTHERLAND

Graham works as a senior researcher at Nettitude, and prior to that spent many years tinkering with various bits of hardware. He has only given himself near-fatal electric shocks twice. His main areas of focus are hardware, cryptography, and Windows internals.

16:00 Where 2 Worlds Collide: Bringing Mimikatz et al to UNIX

Over the past fifteen years there's been an uptick in "interesting" UNIX infrastructures being integrated into customers' existing AD forests. Whilst the threat models enabled by this should be quite familiar to anyone securing a heterogeneous Windows network, they may not be as well understood by a typical UNIX admin who does not have a strong background in Windows and AD. Over the last few months I've spent some time looking a number of specific AD integration solutions (both open and closed source) for UNIX systems and documenting some of the tools, tactics and procedures that enable attacks on the forest to be staged from UNIX.

TIM WADHWA-BROWN

Tim Brown joined Cisco as part of their acquisition of Portcullis for whom he worked for almost 12 years. He is equally happy performing white box assessments with access to source code or where necessary diving into proprietary binaries and protocols using reverse engineering methodologies. Tim has contributed to a number of Cisco's bespoke methodologies covering subjects as diverse as secure development, host hardening, risk and compliance, ERP and SCADA. In 2016-2017, Tim looked at targets as varied as Active Directory, z/OS mainframes, power stations, cars, banking middleware and enterprise SAP Landscapes. Outside of the customer driven realm of information assurance, Tim is also a prolific researcher with papers on UNIX, KDE, Vista and web application security to his name. Tim is credited with almost 150 vulnerability advisories covering both kernel and userland, remote and local. Tim particularly like to bug hunt enterprise UNIX solutions.

TRACK 2

11:00 Beyond Windows Forensics with Built-in Microsoft Tooling

Microsoft has slowly been introducing tools to help organisations better manage and troubleshoot Windows performance and issues; these are now entirely integrated into Windows. To improve performance and troubleshooting capabilities, Microsoft introduced System Resource Usage Monitor (SRUM) in Windows 8 and beyond. PowerShell has become the default "command line" management tool for windows administrators. These tools provide both a wealth of information into what has happened and is present on the system.

For Forensics and even Incident Response, these tools are now a go to built-in option to bootstrap and drive the forensics process including opening access to artefacts that overzealous user or even a "smart" attacker has removed. SRUM for instance can provide data points ranging from network to process activitiy providing insight into what, who, when and how an attacker or malicious process introduced itself into the environment.

This talk will help the participant build the foundations to identify which built in tools can assist in the Windows Forensics process and the data points that are available as well as examine how services such as SRUM can be used to extract key data points to provide information for incident response or threat hunting activities.

THOMAS V. FISCHER

Thomas has over 30 years of experience in the IT industry ranging from software development to infrastructure & network operations and architecture to settle in information security. He has an extensive security background covering roles from incident responder to security architect

THOMAS V. FISCHER (CONT.)

at fortune 500 companies, vendors and consulting organisations. He is currently security advocate and threat researcher focused on advising companies on understanding their data protection activities against malicious parties not just for external threats but also compliance instigated.

12:00 RATs, Crypters & Zombies: A History of Consumer Malware

Malware has become one of the most prevalent threats to personal computer security: how did this happen? Does every threat actor make their own? Come with me on a journey into the internet's archives, exploring how enterprising malware developers created a new market with "remote administration tools" and how they lowered the barrier to running a malware campaign significantly.

This talk will help you become familiar with the role generic malware plays in the world of not-so-sophisticated threat actors, how it's built and what job it's designed to do. Expect a deep dive into the different sectors of the malware economy, a timeline of notable events and a technical analysis of some more interesting examples.

DAN NASH

I'm a software engineering student turned security engineer. I helped run ENUSEC for a while and now i'm helping to improve security with Sophos' Security Engineering team. Lifelong love of CTFs, programming and malware.

14:00 Physical Security Games: Lessons Learnt Building CTF Challenges for Hackers

In the past, I've built a number of challenges for a variety of events. I've always tended towards the more physical side of things. It's remarkably hard to second guess the skill level of potential players, and to build something that hits the fine balance between being achievable without being too easy, when given competitors of varying ability. Sometimes things go well, sometimes, almost comically less so. I'll give some examples of games I've built in the past, the approaches I took when designing them, and some lessons learnt actually getting people stress testing them in the real world...

STEVE WILSON

22+ year veteran of the security industry. Forgotten more than I remember. :-(Physical security nutjob, currently doing advanced red team work. Builder of games for the likes of Hack Fu and the Cyber Security Challenge. Long time friend of Abertay (ask Colin) and occasional Ladywell drunk. @a8n_pub

15:00 Mobile Application Hardening: Protecting Business Critical Apps*

Mobile application security isn't always super exciting or challenging but when it comes to application hardening things get more interesting. These days, it is not uncommon for particular types of application to go out of their way to defend themselves at runtime. Such application types would include but are not limited to:

- financial apps
- multiplayer games
- apps which feature DRM protected content
- apps with intellectual property

etc.

It's often the case that such applications attempt to protect themselves via internally developed controls, as well as leveraging commercial products.

During this talk we'll look at some of the typical controls that Android/iOS applications exhibit, how they work, how to spot them, and how to sidestep them. We'll be demonstrating analysis and techniques using free open source tooling such as Radare, Frida, and for some parts we'll also leverage IDA Pro.

Since automation is the buzzword of the year too we'll also be discussing how to automate some of these activities that typically take up most of the assessment window.

GRANT DOUGLAS & NIKOLA CUCAKOVIC

Both Grant & Nikola are Abertay Alumni and are now working in security consulting at Synopsys Software Integrity Group (SIG)

Grant Douglas is an associate principal consultant specialising in mobile security, having researched & worked in the space for over 7 years. Grant has published mobile tooling which has featured in books such as the mobile app hackers handbook as well as iOS Forensics. My particular areas of interest are in reverse engineering, application hardening, Runtime Application Self Protection (RASP), etc.

Nikola Cucakovic is a security consultant, specialising in mobile security with a particular focus on financial services. Nikola has worked in a number of mobile based roles including Android software engineer, security testing, and also security architecture. Nikola is particularly interested in Reverse Engineering, Application Hardening, and Biometrics.

***FILMING OF THIS TALK IS NOT PERMITTED**

16:00 Weaponising Layer-8

Do you think users are the weakest link in the security chain? Here is some duct tape to change that, and to raise the bar for social engineers and other attackers alike. Over the last few decades, sysadmins and people working in IT have called users names and generally rolled their eyes at the antics of those allegedly lazy, stupid and uneducated people.

From PEBKAC to ID-Ten-T we have been calling them names and didn't want them on our networks. This way of destructive thinking needs an overhaul, and here are some easy tricks how users can become the valuable asset in corporate security that indeed they should be. Finding creative solutions to existing problems has been a standard skill for red teamers, whereas those defending networks often rely on standards. Discover some creative solutions people have come up with to significantly raise their security - most of them are easy to implement - and how users can become a major asset of any security team.

STEFAN HAGER

Stefan works for the Internet Security Team at German company DATEV eG. Having started with computers and starting to be puzzled by reality in the 80s, he started out as a programmer in the early 90s. Since 2000 he has been securing networks and computers for various enterprises in Germany and Scotland.

His main focus nowadays is security research, raising security awareness, coming up with creative solutions to security problems and discussing new ideas concerning threat mitigation. When not trying to do any of the stuff mentioned above, he is either travelling, procrastinating or trying to beat some hacking challenge. Stefan also writes blog posts (in English and German) on his site https://cyberstuff.org.

TRACK 3

11:00 Abertay Student Lightning Talks

This slot will be split up into a number of short talks all presented by first-time conference speakers from our own Abertay Ethical Hacking Society!

12:00 Profiling The Attacker - Using natural language processing to predict crime

What does Minority Report, Black Mirror, and 1984 all have in common?.. Well, turn up to the talk to find out.

On a day to day basis we countlessly write notes, send messages and respond to emails. The question is, however, what does what we write actually show about us, and how can we use the meaning behind these pieces of text to predict crimes and attacks.

This talk delves into just this - how machine learning, and specifically natural language processing and sentiment analysis, can be used to predict crime and security attacks. This, of course, comes hand in hand with talking about predictive policing approaches, biases in predictive policing, and how natural language processing can be used to automate this whole process.

JAMES STEVENSON

My names James, and I've entered the industry in a very typical way: I went to university to study computer security, I interned at a SOC and now I work as a Software Engineer at BT Security.

I've spoken at a few other conferences and I love to do research into why we do the things we do - from sentiment analysis and natural language processing to profiling malicious actors.

I'm also on twitter @_JamesStevenson

12:30 Using Natural Language Processing to Crack Passwords

A custom dictionary that exploits the shared social experience of a userbase can be interactively built by making multiple cracking passes through a hash dump, and on each pass adding other similar words to the dictionary. We might crack one user's password that is based on a local football team and another based on an anime character but if we can add all the other regional football teams and other anime characters to the dictionary for the next cracking pass, we are likely to discover that other users share similar interests. Here we explore the use of Natural Language Processing models for automatically discovering candidate words for a custom password cracking dictionary.

ROBIN VICKERY

Robin is a senior cybersecurity penetration test consultant and has worked across a number of disciplines including offensive and defensive security. This has included offensive security in protecting ultra-high net worth individual's online reputation and assets as well as more traditional commercial engagements. Prior to that Robin spent time as a developer.

14:00 Striking While The Iron's Hot: The do's and dont's of getting a job in infosec

What's a job in infosec really like? In fact how do you even get one in the first place?

Based off experiences from their first few years in industry the team break down some of their favorite do's and don'ts with getting your first job in infosec.

JAMES STEVENSON, CHLÖE UNGAR, BRETT CALDERBANK, DANIEL NASH & JACK WILSON

A team with a mix of backgrounds from entering the industry through university to working in internships and apprenticeships. We now all work, in one form or another, in computer security companies from small startups to large global organisations.

15:00 From Breaking In to Breaking Through

What isn't there to love about talking your way into places you're not allowed, free stuff, or any number of other things that leave you with epic stories? We glorify and revel in impressive and amusing social engineering hijinks, which is great until the point where we need to get our colleagues to be better about security behaviours and the first "soft skills" that we think of using in the context of security are about deception and manipulation. Social engineering can be powerful for getting people to do things for you, but helping people to be better with security practices requires a different approach to be effective. This talk will cover some basics tips from teaching and behaviour change interventions, which skills developed in the context of social engineering have some crossover, and pitfalls with using social engineering tactics on your coworkers.

ROSE REGINA LAWRENCE

Rose Regina Lawrence is the digital security coordinator at Tactical Tech in Berlin. She has supported activists, human rights defenders, and journalists in heightened risk settings both in the US and internationally for over a decade. Her graduate level training in Public Health/ Community Health Education with a focus on communicating for behaviour change on individual and collective risk has deeply shaped her approach to digital security education. In addition to digital security workshops and interventions for activists and their attorneys, she has developed materials and presented on digital security and sexuality, including the specific needs of sex workers, people who have experienced domestic and intimate partner violence, and the queer community.

15:30 Intro to Machine Learning for Hackers

As cyber security students & professionals, do we really need to care about Machine Learning? In this talk we will go over what machine learning is, what it can do, and how it can (and can't) help the cyber security profession. After taking a deep dive into a particular algorithm, where we will learn a bit of maths and logic behind how ML works, will focus on: examining how the industry is currently utilising it (ML for phishing detection, ML for NIDS and ML for SIEM), how adversaries could use it to our disadvantage and how Machine Learning is vulnerable to attack itself.

HELENA LUCAS

I am a Cyber Security and Forensics student currently on placement, which is where I first came into contact with Machine Learning. At Uni I was on the committee of ENUSEC and organised a TEDx conference. Oh and if you see me around, ask me to do a card trick!

16:00 It might get loud! Exfiltrating data using audio interfaces

Data exfiltrating is often the final and most important phases of an attack as this is when the target data is actively stolen and transmitted across network boundaries. However, on restricted and isolated environments, this stage becomes more challenging as avenues for data to be transferred are drastically reduced, and it is quite common for removable storage devices to be disabled.

How about using devices that are usually permitted such as sound cards to exfiltrate the data? Turning files into analogue signals is not a novel idea, modems did this many years ago... but how about using a USB soundcard to transfer files from a computer to another device? When classical methods fail, jazz it up and rock it out! (This can involve very low or high frequency sounds).

MIGUEL MARQUES

Miguel is a senior cybersecurity penetration test consultant and brings many years of experience across a range of disciplines. Prior to joining Commissum, Miguel led successful engagements across complex systems including banking platforms and biometric based authentication systems. He specialises in web application testing, infrastructure testing and mobile application security assessments.

16:30 Back to School: Bringing it Back to the Students

This talk will discuss tools, tricks and stories from students on how to advance yourself and get a foothold in the infosec industry. Whether for a current student, a newbie or a hacking veteran, hopefully this talk brings some inspiration and knowledge to you.

CALLAN GARRATLEY

4th year student & part time consultant. I love learning, talking and hacking things

CLOSING KEYNOTE

17:15 ISIS Online: Junaid Hussain*

This talk examines the online tactics of Junaid Hussain (Aka TriCk) as a hacktavist and later as a member of ISIS.

The talk will cover:

- Hussains hacking abilities
- The hacks he and his crew perpetrated
- How Hussain transferred his knowledge to propagandising for ISIS
- Hussains role in ISIS' propaganda and recruitment efforts

The main aim of the talk is to discuss how Hussain utilised his hacking skills and their effectiveness in relation to ISIS' objectives.

MICHAEL JACK

Former @AbertayHackers Vice Gaffer. Purveyor of macOS security & tequila.

***FILMING OF THIS TALK IS NOT PERMITTED**

MWR

Proud sponsors of the official Securi-Tay Afterparty 2019!

Head on over to the Student Union across the road from 6.30pm where the drinks are on us! Relax and chat with other con-goers and be sure to look out for that all-important swag. No tickets needed – so see you there.

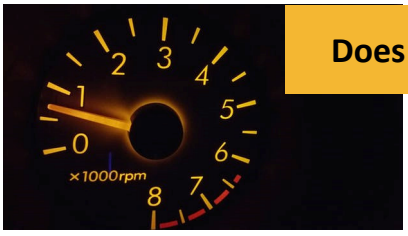
Student Union
6.30pm

mwrinfosecurity.com

linkedin.com/company/mwr-infosecurity/

@mwrinfosecurity
@mwrlabs

Practical solutions to protect your information



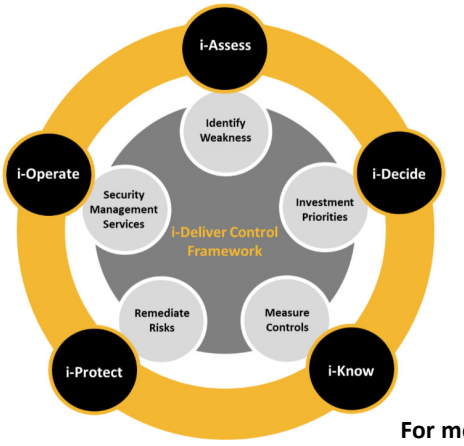
Does your cyber risk management need to step up a gear?

A skilled team

Innovative solutions

Direct experience

Business insight



i-confidential provides trusted leadership on information security for some of the UK's largest firms, blending best practice and common sense.

Our approach views every organisation end to end, focusing on people, process, and technology. We target outcomes that exceed expectations.

Our proprietary **i-Deliver** Control Framework enables us to:

- Carry out security assessments and detailed control measurement
- Remediate risks and advise on strategic investment planning
- Offer tailored security management services

For more information about how we can help your business, please contact us

i-confidential
Cyber Security & Information Risk Specialists®

0131 445 1458
info@i-confidential.com

LOOKING TO START A CAREER IN CYBER SECURITY?

Our internships and trainee consultant programmes might be just the right place for you to get started.

Context is an independently operated cyber security consultancy. We specialise in security penetration testing, incident response and technical security research.

We are rapidly expanding our teams across the globe. If you are interested in joining us, please get in touch.

context

recruitment@contextis.com
+44 (0)20 7537 7515
ctx.is/talent

ecs security

Formed and run by ex-security leaders, ECS Security is proud to sit among the largest independent security services companies in the UK, counting almost 30 of FTSE 100 companies as clients.

We support our customers in all aspects of cyber threat management from landscape awareness and threat analysis through to monitoring & detection and control improvement. We've developed a trusted reputation around building and optimising large-scale Security Operations Centres (SOCs), designing complex IAM solutions, implementing large SIEM deployments and supporting large scale transformation programmes.

We are always looking for talented and enthusiastic people who share our values and over the last 3 years, ECS Security has employed 100+ graduates.

careers@ecssecurity.co.uk
enquiries@ecssecurity.co.uk

ECS Security Ltd

@ECS_Cybersec

NOTES

NOTES

Thank you

We'd like to say a huge thank you to the Abertay Students Association. Without their hard work and effort, Securi-Tay wouldn't be the success that it is.

ABERTAY SA

FEEDBACK
SECURI-TAY 2019

Scan here to let us know what you thought of the conference and how we can improve!

Incident Line

+44 7479 277343

Please SMS or Call

if during the event you have a serious issue

(e.g. Code of Conduct violation)


Abertay Ethical Hacking Society