DeepSec GmbH
✉Weyringergasse 30A/Top 10
✉1040 Wien - Austria
✉deepsec@deepsec.net
✆+43.676.5626390 ✆+43.664.4145905 ✆+43.720.3493872

1 DeepINTEL 2017 Preliminary Schedule

This is the preliminary schedule of DeepINTEL 2017. All speakers have confirmed their availability and the content of their presentation. Some speakers are pending, i.e. they have confirmed their availability, but they have not provided an abstract of their talk.
The schedule is subject to change. The current schedule can be found at:
https://deepintel.net/DeepINTEL_2017_Schedule.pdf

1.1 Introduction: The Physics of Cyber/Digital Incident and Response

Computer science features a lot of acronyms hiding complexity and analogies from other fields of observation. We are all used to work with windows, workbenches, trash cans, files, folders, mouse, and many other tools that are pure abstractions. On top of these layers we have all the modern infrastructure consisting of networks, operating systems, mobile devices, cloud applications, and more. Information security often enters the end of these chains, especially when it comes to analysing incidents, assessing defences, and being ready for the next attack.

Leaving computer science aside and turning to physics, there are similar fields where the world the theoretical models have to describe are quite complex. Reducing matter to a set of atomic particles and focussing on the interaction between them allows for a clearer picture. These concepts can be applied to information security. No adversary can attack a system without interacting with potentially vulnerably components. In turn proofing your infrastructure against future attacks has a lot in common with California's building code in anticipation of the next big earthquake. Geology can't yet predict when it will happen, but statistics and geological evidence tells us that it will happen. Sounds familiar when you compare large scale digital destruction by malicious software with an earthquake.

The introduction tries to give you a new set of analogies and to develop a kind of Standard Model of Digital Defence.

René Pfeiffer works as a self-employed systems administrator and lecturer at the University of Applied Sciences (UAS) Technikum Wien and UAS Burgenland. He has more than 20 years of experience in the professional IT business and over 30 years of using computers for coding and other purposes. His main focus lies in the area of systems administration, architecture of IT security infrastructure, secure communication technologies, wireless security, technical documentation, supervision of research projects, and auditing of software and information processing systems.

Mr Pfeiffer lectures since 2000, and conducts workshops for companies, business partners, educational organisations, and the Free Software community.

1.2 Beyond Real-Time – Emergent Threat Analytics by IBM X-Force

Reacting to threats in real-time is no longer enough to stay on top of the security game. Being able to (reliably) predict emerging threats and provide protection before they become active is a better way forward. IBM X-Force, the R&D department of IBM Security, has been shifting away rapidly from traditional methods of gathering and processing threat intelligence towards analytics-based, predictive approaches. In this talk we will look at the current threat landscape, as IBM X-Force sees it, as well as the new techniques used to arrive at these insights. Together we will discover how to protect against tomorrow's threats - today.

Matthias Seul is a Development Manager in IBM Security, heading the IBM Protector product development team. Matthias regularly represents X-Force, the R&D department of IBM Security, on conferences and in client engagements across the globe. Coming from a career in software development and with over 14 years of experience in the security domain Matthias can offer insights on both strategic as well as tactical & technical level. He has also contributed to numerous security innovations, earning him the coveted „Master Inventor" title.

1.3 The great compliance distraction . . . – What happens when you spend your security budget, securing someone else's data?

Is data security a distraction delivered due to compliance? Or can compliance create controls that create a security culture?

Andrew will discuss the issues with **data** security being the primary objective of many security programs, often being driven by compliance frameworks and how that can often be a distraction to protecting the things applications do for our organisations. Taking a look at some what if scenarios he'll consider the different outcomes that may have occurred in some high profile breaches if criminals got less value from the data.

Andrew Barratt is a trusted Cyber security advisor with cross sector experience in IT audit, across Europe, with international experience spanning the United States, Middle East and Africa. Andrew manages a global team of consultants delivering complex security and compliance engagements.

With extensive experience in the payment industry, Andrew's team perform detailed application certification assessments to PA-DSS, EPCS as well as independent technology validation whitepapers. Andrew is also an expert advisor to one of the largest cyber insurance syndicates in the world and works with their underwriters to help manage policy with cover of up to $500m.
Andrew's background in IT infrastructure, software development and service management allows him to offer technical advice valued by those responsible for managing technology whilst engaging with executive stakeholders on the business impact of cyber risk.
As a regular speaker at security conferences on topics such as breach disclosure, cloud security and cyber risk management Andrew has also been invited to speak to private audiences at Lloyds of London, ISACA and at the UK Payments Association. He has also appeared on the BBC's Moneybox show, and in SC Magazine, Infosec magazine and numerous other information security publications.

1.4 ProcDOT – Behavioral Analysis on Steroids

When it comes to malware analysis, behavioral analysis is still the most promising and hence most important approach if your goal is to find out as much as possible in a minimum amount of time. To accomplish this, one will typically use one of the classic monitoring tools like Sysinternals' Process Monitor (procmon) as well as PCAP-generating network sniffers (i.e. Wireshark, Windump, tcpdump, etc).

However, there is one „handicap" which all of these tools have in common: The presentation of the merely unmanageable amount of data and information being produced.

That's where ProcDOT enters the stage. It processes all of this data and information eventually presenting you with an easy to grasp interactively investigable graph actually considering the chronological aspects.

In this terms, regardless if you are already an expert in malware analysis or a beginner scratching on the latter's surface, ProcDOT enables you to

- get an overall guts feeling for an entire situation within a glance,
- spot relevant parts and understand the correlation between them in minutes.

Sounds like a jack of all trades tool? You'll be surprised!

Christian Wojner is one of the core team members of the national and governmental computer emergency response team of Austria (CERT.at). In this respect he is responsible for

malware analysis, reverse engineering and forensical investigations on Microsoft Windows boxes. Furthermore Christian is author of various articles, technical papers, software tools, and frequently gives talks specifically focusing on malware analysis.

1.5 Social Engineering Manipulating Human Behaviour

Social Engineering is an accepted APT and is going to stay. Most of the high-value hacking attacks feature components of social engineering. Understanding of the methods and approaches used behind the scene of Social Engineering will help you to make the world a safer place. Or make your attack plans more successful! Social Engineering is a topic that does not really fit into technical hacking and is also underestimated by security professionals. My presentation is based on a book I recently wrote about Social Engineering. As a bonus to my talk I will present the participants with ebook-versions (PDF, epub, mobi) of my book for further study.

1. Social Engineering is an APT to be taken seriously. Most attacks feature Social Engineering.
2. Social Engineering attack execution and prevention needs training and skills. Don't be fooled, there are no tools you can solely rely on to prevent Social Engineering attacks.
3. Social Engineering has progressed and professionalized more than you think. It is deadly effective.
4. With the help of Social Engineering you can deliver exploits effective and efficient.

As a successful participant of the Social Engineering Capture the Flag (SECTF) competition at the Defcon 22 conference in Las Vegas I do know very well why Social Engineering still works brilliantly and what risk it presents to the corporate world. Social Engineering is another very important puzzle piece in everyones security posture. As the developer of the open source based freely available Social Engineering Engagement Framework (SEEF) I want to share how Social Engineering works today and why this understanding ultimately helps you to better protect yourself and your company.

The content I am going to share is brand-new and has been developed over the past years based on experience as an international consultant (Big 4, KPMG, Deloitte, Australia, China, Switzerland, Singapore, Malaysia etc.) by myself and my colleague and has not been presented anywhere else.

At DeepIntel I will share our work results for the first time publicly and exclusively. Just recently we decided to open source our knowledge with sharing the content of our Social Engineering Engagement Framework (SEEF), which looks at Social Engineering from a brand new point of view: Most Social Engineering frameworks are based on technical tools but rarely focus on the business and risk side of Social Engineering. But, on a corporate level, there is no methodology making Social Engineering engagements planable and secure and the achieved results comparable as well as repeatable. Most Social Engineering definitions are technically focused. We take a different point of view by defininig Social Enigineering simply as "The elicitation of information from systems, networks or human beings through methods and tools". For the presentation I will select elements from the framework in order to show the audience how to successfully plan, document and execute a professional Social Engineering (attack).

Dominique C. Brack is a recognized expert in information security, including identity theft, social media exposure, data breach, cyber security, human manipulation and online reputation management. He is a highly qualified, top-performing professional with outstanding experience and achievements within key IT security, risk and project management roles, confirming expertise in delivering innovative, customer-responsive projects and services in highly sensitive environments on an international scale. Mr. Brack is accessible, real, professional, and provides topical, timely and cutting edge information. Dominique's direct and to-the-point tone of voice can be counted on to capture attention, and – most importantly - inspire and empower action.

- SEEF
- LinkedIn Profile
- Xing profile

1.6 Manipulating Human Memory for Fun and Profit

The human memory is very volatile and not really trustworthy. Judges, interrogators and scientists know that humans often mix up or straight up create new false memories. In this talk I will show what we know about how the human memory works, which factors lead to a loss of quality of stored memories and how they can be altered or manipulated for social engineering attacks. Since this is an ethically very controversial topic, I will also speak about the ethics behind this. And be advised that I will not talk about NLP (Neuro Linguistic Programming), as this stuff is unsubstantiated, unscientific esoteric charlatanry.

Stefan Schumacher is the president of the Magdeburg Institute for Security Research and editor of the Magdeburg Journal for Security Research in Magdeburg/Germany. He started his hacking career before the fall of the Berlin Wall on an East German small computer with 1.75 MHz and a Datasette drive.
Ever since he liked to explore technical and social systems with a focus on security and how to exploit them. He was a NetBSD developer for some time and involved in several other Open Source projects and events. He studied Educational Science and Psychology and does a lot of unique research about the Psychology of Security with a focus on Social Engineering, User Training and Didactics of Security/Cryptography. He is currently leading the research project Psychology of Security, where fundamental qualitative and quantitative research about the perception and construction of security is done.
He works as an IT security consultant for several companies and government bodies since 2006 and helps organisations to establish a security culture.
He presents his research results regularly at international conferences like AusCert Australia, Chaos Communication Congress, Chaos Communciation Camp, DeepSec Vienna, DeepIntel Salzburg, Positive Hack Days Moscow or LinuxDays Luxembourg and in security related journals and books.

1.7 Hybrid Warfare – the Russian – Ucrainian cyber war and the role of propaganda

In this talk Volker Kozok gives an insight into Russian cyber warfare strategy and some examples of Russian and Ucrainain hacking activities, with the main focus on the well known hacker group „Cyber Berkut“. Volker gives examples of patriotic cyber crime activities, hacktivism and state sponsored attacks. The second part of the talk is about narratives and Russian propaganda, mainly about the one disseminated in Germany, and the role of trolls and Social Bots.

Lieutenant Colonel Volker Kozok is Assistant Branch Chief in the Legal Division of the German Ministry of Defense. Volker Kozok started his career as an Armored Infantry Officer in 1980. For the last 20 years he worked in the area of Cyber Security and is a trained Computer Forensic Expert, Ethical Hacker and Cyber Security Expert. He planned and built-up the Computer Emergency Response Team of the Federal Armed Forces and was the IT-Security Staff Officer for the Joint Service as well as the head of delegation of the yearly US-Studytour, where 18 Cyber Security Experts from German Armed Forces and German Industry visited different Cyber Organizations in the US. He also worked as Director of the Director of the “International Bulletproofhosting & Botnet” Conference and of the national „Social meets Media” Conference.

1.8 The Power Grid is vulnerable – and it's really hard to fix this

The power grid is a critical infrastructure, and it is under attack: The recent blackouts in the Ukraine demonstrate that the power grid is not off-limits to attackers. The Ukraine attacks achieved a high impact but are rather simple IT-based attacks. The attackers did not utilize the underlying physics of the power grid: Utility companies designed their systems for operational safety and availability, but did not consider It security. The failure models are designed to alleviate the impact of single failures, but not the effects of a coordinated attack on different elements of the power grid.

The talk will introduce the physics of the power grid and failure modes. Today's attacks on control systems incorporate only basic knowledge about the power grid. I will list the vulnerabilities of the power grid and show how physics can be used to amplify the impact of any attack. What's more: Renewable power plants, IoT devices and electric vehicles provide additional attack vectors on the demand side of the power grid that are not under control of the power utilities – and therefore very hard to protect against attackers.

Mathias Dalheimer is a researcher in computer science. His background is in distributed systems engineering (Grid/Cloud Computing). For the last 10 years he has been working at the intersection of IT and power grid control systems, ranging from smart meters, photovoltaik power generation, smart home integration to battery storage systems. He is an active member of the Chaos Computer Club and advocates a decentralized and cellular power grid.

1.9 Reconstruction of Social Networks: Breaking past API

Open source intelligence tools have become increasingly dependent on the use of API's to gather information. These channels are heavily restricted and are sometimes closed off to many who do not follow the guidelines. Gathering information from social media without authentication is possible but produces many challenges; retrieving relevant information, understanding connections between people and developing a system which can withstand the dynamism of social media. This vast amount of data can not only let us understand what people say in networks, but also how they interact online, what patterns occur from gathering this data and how information is passed effectively within a social network online.

Jack Link is a UK based security researcher who has a big passion for information security. Jack has been relentlessly researching in reverse engineering, web application security and open source intelligence to further his ability and knowledge. He has found bug bounties in

companies such as Microsoft, Netflix, AT&T and eBay and has contributed this year in tightening Wordpress security, by responsibly disclosing a cryptographic flaw in the platform. His malware analysis blog posts have contributed torward threat intelligence and yara rules that have helped protect networks. After recently finishing his degree, he is furthering his knowledge by exploring more abstract aspects of security such as threats within social media.
Jack has a blog at `https://itsjack.cc` and his Twitter is @linkcabin

1.10 Industrial DIY – Attacking SCADA Infrastructure

A few months ago a client asked us to assess the security of the ICS/SCADA of a brand new datacenter. As we were no industrial guys we discovered a whole new world and we tried and failed many times before owning the system. „Industrial DIY“ (title will probably change) tries to show how a small team of pentesters managed to assess the security of industrial systems (ICS/SCADA/BMC) and how to protect these critical infrastructures against a few major threats.

Founder of RandoriSec a security focused IT firm, Davy Douhine is working in the itsec field since almost fifteen years. He has mainly worked for financial, banks and defense key accounts doing pentests and trainings to help them to improve their security. He enjoys climbing rocks in Fontainebleau or in the Bourgogne vineyards and practices Brazilian jiu-jitsu.

1.11 Risk Communication – “To be informed, or not to be informed: that is the question”

Making correct and effective decisions requires complete, meaningful and tailored data. This is nothing new and what sounds like an easy challenge is nowadays still surprisingly difficult and not well (enough) implemented.

Although large enterprises and SMEs differ in many ways, they have at least one thing in common: immature risk communication. This leads to a lack of awareness and insight regarding a company’s security posture and risk profile. This problem is exacerbated by the fact that most companies are lacking adequate, complete, meaningful and tailored data that are an indispensable prerequisite for an informed and effective security steering function.

A fundamental problem is that security metric projects – if at all existent – are often implemented without proper planning and consequently are highly prone to scope creep and neglect. This leads to various well-known effects such as a lack

in top management awareness, "buy in" and support, risks not being adequately addressed, risks being accepted too hastily, a false sense of security, ineffective resource usage, defending against the "wrong" threats or buying tools that are not utilized effectively.

Without proper alignment with business needs and impacts, information security is often seen as a cost sink and a business disrupter – in combination this creates an explosive mixture that threatens business continuity.

Let us together have a look on common pitfalls in risk communication and some "KISS possibilities" – keeping it simple and smart.

Stefan Jakoubi is head of professional services at SBA Research delivering consultancy to partners and customers. For over 10 years his personal focus lies on organizational aspects of information security accompanying companies to institutionalize and improve their information security posture and capabilities. SBA Research is Austrian's largest research institution focusing exclusively on information security.

1.12 The enemy 'within'? Motivations, intent and profiling of malicious insiders

Malicious insider threat is not only a security- or technical-oriented issue, mainly it's a behavioural one. Insiders are so-called 'trusted' or privileged employees with broad legitimate access to the organization's systems and as such they are hard to catch. Furthermore, it is difficult to find appropriate factors for prediction as well as measures for prevention and detection. In fact, based on new technical developments and opportunities, data theft has become much easier nowadays: Mobile trends like BYOD,for example, the increased ability to work from home and access to the organization's systems from on the road, cloud services with related security vulnerabilities, as well as more and more malware opportunities have increased the potential of related attacks.

Other main security obstacles and triggering factors inside and outside an organization may be a bad market development and fear of job loss, internal (security-related) budget constraints, and the complexity of the internal (IT) environment, competing priorities, a lack of top-level direction and leadership, as well as a lack of awareness training, etc. Anyway, current studies in the field show that malicious insider threat is an increasing crucial issue for companies and governmental institutions. Beside the mentioned dependence on ICT, new attack forms and collaborations with third parties (for example social engineers and/or hackers) are on the rise.

DeepSec GmbH
✉Weyringergasse 30A/Top 10
✉1040 Wien - Austria
✍deepsec@deepsec.net
✆+43.676.5626390 ✆+43.664.4145905 ✆+43.720.3493872

This talk will focus on the current state of insider threat, on motivational and behavioural aspects as well as on current profiles of malicious insiders based on the newest available data. The emphasis on characteristics of malicious insiders is crucial, but also the fact that boundaries of insiders and outsiders are becoming more and more blurred in many cases of attacks. The talk will close with some starting points for organizational insider threat prevention management.

Professor Ulrike Hugl is senior scientist and lecturer at the University of Innsbruck (School of Management), Department of Accounting, Auditing and Taxation. She is member of various scientific committees of international conferences and reviewer of several journals. Her research mainly focuses on new technologies with impacts on information security and data protection of organizations, as well as on occupational/corporate crime (especially insider threat) and industrial espionage issues.