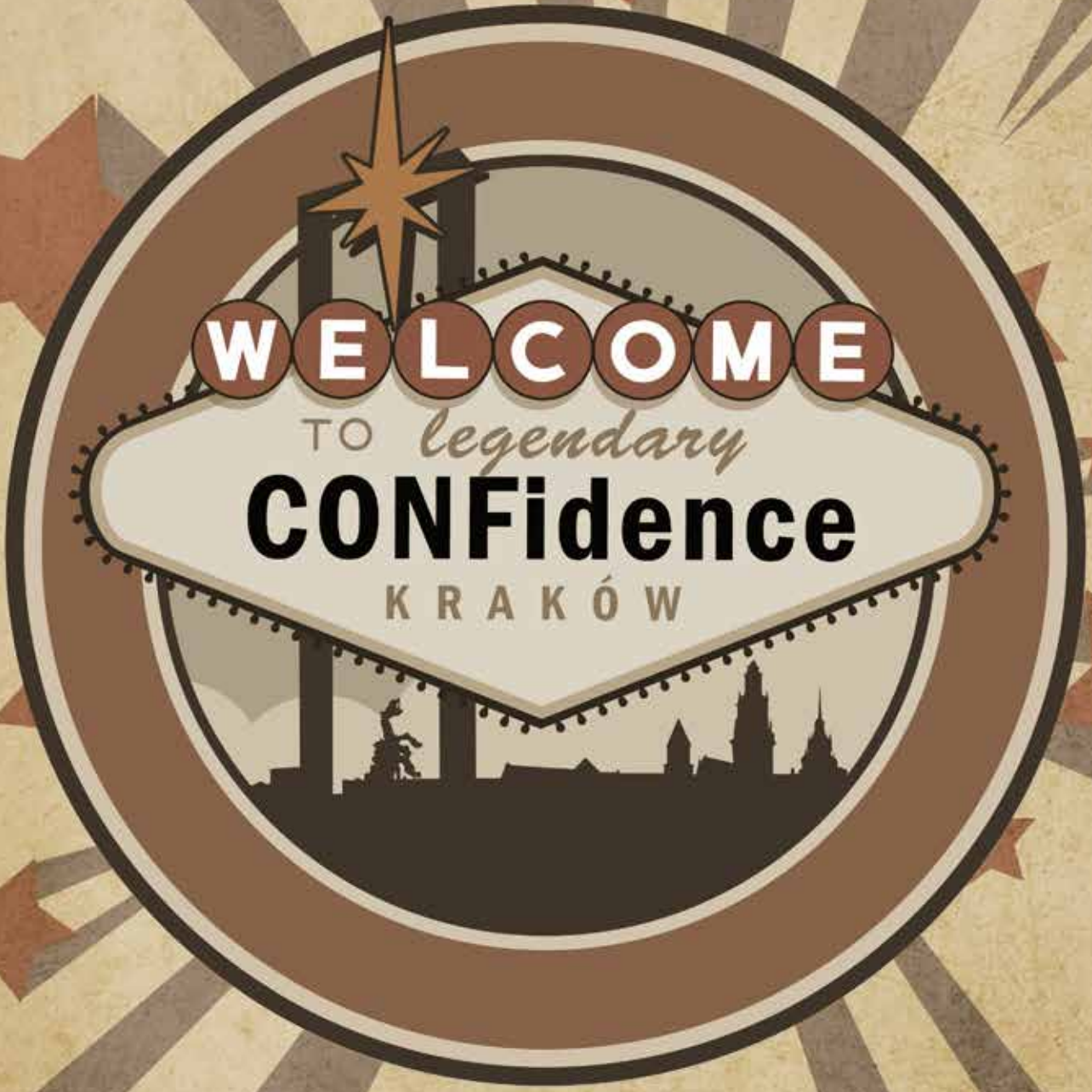
CONFIDENCE 2013



CONFIDENCE 2013

Cześć! Hi! Welcome!

Welcome to the 11th edition of the CONFidence conference, an international IT security event. We are extremely happy that you have managed to join us in magical Krakow for this year's edition.

In this guide you will find all the information you may need about the schedule, contests, leisure activities and the conference itself. If you have any questions, problems or suggestions, don't hesitate to talk to us. All members of the CONFidence staff are wearing red conference t-shirts, so it is easy to spot us in the crowd!

This year, apart from the technical part, together with whe Core Group, we will launch a second edition of the X-traction Point game, featuring live invasion on a bunker, with lock-picking, alarm disabling and assault on a bunker instalation preceded with additional onsite trainings on lockpicking, airsoft guns and more! Get ready!

With regards
CONFidence crew

CONFIDENCE 2013

SCHEDULE

The First Day, May 28th, 2013

09:00 – 09:50	Registration	
09:50 – 10:00	Opening Ceremony	
10:00 – 10:50	**Thomas Lim** - The Keynote	
11:00 – 11:50	**Mariusz Sawczuk, Jochen Belke** – Invisible attacks – visible in your network. How to see and follow the tracks?	
12:00 – 12:50	**Ilja van Sprudel** - Linux Desktop Insecurity	
13:00 – 13:50	Lunch Break	
13:50 - 14:40	**Nguyen Anh Quynh** - Opticode: machine code deobfuscation for malware analysts	
	Track 1	Track 2
14:50 – 15:40	**Yaniv Miron, MC** - Ph0k 0-days, We Will Pwn U with Hardware Mofos	**Nikita Tarakanov** - Exploiting Hardcore Pool Corruptions in Microsoft Windows Kernel
15:50 – 16:40	**Gynvael Coldwind, Mateusz "j00ru" Jurczyk** - Beyond MOV ADD XOR - the unusual and unexpected in x86	**Arseny Reutov** - PHP Object Injection revisted
16:50 – 17:40	**Robert Lipovsky** - The "Facebook PokerAgent"	**Julian Bangert, Sergey Bratus** - ELF Eccentricities
17:50 – 18:35	**Georgia Weidman** - Can You Hear Me Now: Leveraging Mobile Devices on Pentests	**Grzegorz Niemirowski** -Desktop applications vulnerabilities
21:00 – 01:00	CONFidence Afterparty	

The Second Day, May 29th, 2013

	Track 1T	Track 2
10:00 – 10:50	**Devesh Bhatt** - My Experiments with truth: a different route to bug hunting	**Michał Sajdak** - Embedded Devices Hacking
11:00 – 11:50	**Gaweł Mikołajczyk** - Networking Security Treasures	**Adam 'pi3' Zabrocki** – Crashdumps: hunt 0days and rootkits
12:00 – 12:50	**Rebecca Bx Shapiro, Julian Bangert, Sergey Bratus** – Any Input Is a Program: Weird Machines in ABI and architecture metadata	**Dmitriy Chastuchin, Evgeny Neyolov** - Breaking, Forensicating and Anti-Forensicating SAP Portal and J2EE Engine
13:00 – 13:50	**Felix "fx" Lindner, Gregor Kopf** - Cisco in the Sky with Diamonds	
13:50 – 14:50	Lunch Break	
15:00 – 15:50	**Fernando Gont** - Network Reconnaissance in IPv6 Networks	**Yury Chemerkin** – Insecurities in blackberry
16:00 – 16:50	**Jesse Burns** - Securing Data in Mobile Application Suites	**Marek Zmysłowski** - Penetration Testing - 7 Deadly Sins
17:00 – 17:50	**Meredith L. Patterson** - LANGSEC 2011-2016	
17:50 – 18:10	Closing Ceremony	

CONFIDENCE
2013

Second edition of the X-traction Point

Last year at CONFidence, attendees saw the birth of a new challenge game – an immersive and detailed contest that was both physically and technically demanding. Entitled X-traction Point, this game involved a two-person team-based assault on the secure bunker of ZłoCo in order to rescue a trapped hostage by agents who were simultaneously attempting to hack systems, disable alarms, and shoot at targets. This year's installment continues that same trend.

The story:

Last year's mission was a success. The Infiltration Agent was successful in erasing all of the files that ZłoCo had been collecting on citizens for years, including all records that they had compiled about the Underground Alliance… a group of cypherpunks dedicated to privacy and freedom of information. Because all records of the Underground Alliance were expunged, ZłoCo was unable to track them or retaliate. Furious at their inability to persue these digital rebels on the ground, the evil company is taking to the skies. ZłoCo has developed missile technology and is planning to fire upon a large communication sattelite that the Underground Alliance has hacked repurposed for secure cryptographic transmissions. Infiltrators and spies within the ZłoCo empire identified the remote facility which houses a missile silo and passed word along to the Underground Alliance.

After befriending and seducing one of the ZłoCo employees at this mountain site, the rebels hatched a plan to destroy the missile facility. By turning this ZłoCo technician into their own Sabatoge Agent and enlisting her help in initiating a launch of the rocket without proper procedure and with the silo still closed, they hope to obliterate ZłoCo's ability to make war in the heavens and to keep their crypto satellite safe.

Everything was going according to plan until someone else at the missile facility became suspicious. The Sabotage Agent was removed from her post and held in an interrogation room. Given enough time, it is likely that someone from ZłoCo will discover the commands that have been specially-prepared and entered into the missile system. It is up to you to help the Sabatoge Agent complete her mission! You will have to breach the bunker, free your fellow rebel, and escape to the waiting helicopter once she has completed her work.

CONFIDENCE
2013

The mission:

As before, two candidates form paired teams for every run of the x-Traction Point course. One candidate is a Support Agent: their job is to jack in to various communication lines and help with the monitoring of cameras, the hacking of alarms, and the providing of information to the Field Agent. However… this year the Support Agent will have to be up for some kinetic tasks, as well!

The Field Agent is responsible for the principal assault on the bunker. As the team approaches, the Field Agent will fire upon sentry equipment in order to disable guns and lights and allow access to the facility. However, once the team has advanced to a forward position, the Field Agent will turn over their submachine gun to the Support Agent, in case additional firepower is required outside. The Field Agent will proceed in armed only with a pistol, for subduing any guards encountered inside. The hope is that it doesn't come to that, however… as stealth will be rewarded above brute force. As the Support Agent gains access to networked cameras, they will be able to communicate and describe the scene within. Radio contact will have to be very subtle, but the Field Agent should then be able to proceed inside, picking locks and bypassing alarm circuts in order to reach the captured Sabotage Agent.

Dodge the guards, attack the systems, and attempt to unlock additional documents and equipment as you make your way to the interrogation room. If you can manage to free the captured rebel, get her back to the computer interface where she will initiate the missile destruction sequence. After that, it's up to everyone to get out of there as fast as possible, without setting off alarms, in order to reach the x-Traction Point for evac!

The training:

The above mission will take place on Day Two of CONFidence. Day One will be spent on training and qualification games for all participants.
There will be three training areas: lockpicking, wired systems, and shooting. Lessons and trainings will run throughout the first half of Day One.

Lockpicking – Basic intro to lockpicking will be taught and handcuff escapes will also be explained. Qualifing games will involve seeing how quickly contestants can open a series of locks and escape from restraints.

Wired Systems – From teleco jacking and some old phreaking tactics to modern alarm system tapping and code-sniffing, this will be the most detailed training and there will be either one or two mini-games which test your skills at deciphering alarm signals and making phone calls in unconventional ways.

Shooting – Like last year, a basic shooting range will be set up for everyone's enjoyment and then qualifying rounds will involve seeing how quickly people can fire successfully at a series of fixed targets.

Team preparation:

The two top-scoringcandidates in each of the mini-games will be allowed to pick a teammate and decide who will act as Field Agent and who will act as Support Agent when they run the x-Traction Point game course. No matter how well someone does in the mini-games, they may only be on a single team on Day Two… so 3rd or even 4th place qualifying people might still be part of an assault team.

Once teams are determined, the candidates will be given an Intelligence and Objectives Packet regarding the bunker (because secret details were leaked out by the ZłoCo employee who turned rogue) and the assault teams will determine how best to set up their gear and equipment on the next day.

All necessary equipment and rigging gear will be made available on Day Two and it is up to the Field Agent and Support Agent to determine exactly how they wish to prepare for their assault mission.

Assault:

As described above, the idea is to get in, collect intelligence, collect your teammate, and get out again… all without setting off alarms or running out of time. Assault missions will have 30 minutes to complete, and it may take every moment of that available time in order to accomplish all of the goals outlined in the Intelligence and Objectives Packet.

The Support Agent and the Field Agent should have reliable radio communications between each other the whole time, although extra points will be awarded if the Field Agent does not speak out loud once they have entered the bunker.
A guard will be present inside the ZłoCo facility, and they will make periodic and routine checks of the missile silo and the hostage room. By monitoring the camera feeds, the Support Agent should be able to inform the Field Agent of when it is safe to move or when it is best to hide.

Once you have freed the captured Sabotage Agent, things become more critical. If the guard notices that she is missing, alarms can go off. Once she has entered the destruct codes, the missile silo will begin arming. Get out of there and make it to the x-Traction Point so that you can all escape to safety!

AFTER PARTY

As usually after the first day of the CONFidence conference
we would like to invite you for a legendary after party where you can meet with other attendes, speakers and invited guests and have a relaxed conversation in a laid back atmosphere. We invite all CONFidence attendees to join the fun on the dance floor. There is also going to be a special game zone arena.

The party starts from 9pm at the BASE Club (Św. Anny 6 Street, Krakow) on the 28th of May. The official part of the party will end at 1am but that doesn't necessarily mean the end of fun.

A lot more pubs and clubs a wait you around the Main Sqare. We hope you join us and have a great time! Don't miss that!

You can check where the place is here:
http://goo.gl/maps/MaBDK

The entrance to the club will be possible only with red CONFidence badge. You can however invite your friends easily.

PARKING AT THE VENUE

There is plenty of parking space at the venue so feel free to come here by car.

CONFIDENCE 2013

Coach Bus Connections to and from the conference:

As the conference is held in venue far away from the city center, we will deploy a couch bus lines connecting the city center with the conference venue!

The connection will go on a route between parking in front of the Sheraton hotel (near Wawel castle) and the venue.

the map of the locations can be found here:
http://goo.gl/maps/CeUjF

Day 1 and 2 (May 28-29th, Tuesday, Wednesday):

Direction: Conference Venue
Departing from: Parking in front of Sheraton Hotel
From 8:00 till 11:00 – buses will be departing around:

- 8:00 (one bus)
- 8:30 (one bus)
- 9:00 (two buses)
- 9:30 (one bus)
- 10:00 (two buses)
- 10:30 (two buses)
- 11:00 (one bus)

Later during the day there will be a bus going in that direction at:

- 12:20
- 13:20
- 15:20
- 16:20
- 17:20

CONFIDENCE 2013

Direction: Parking in front of Sheraton Hotel
Departing from: Conference Venue parking

There is an option of going back to the city center during the CONFidence:

- 12:00
- 13:00
- 15:00
- 16:00
- 17:00

While closer to the **end of the 1st and 2nd day** two buses will be driving back to the Sheraton parking every 30 minutes:
From 17:30 till 19:00

On the second day, buses will start frequent departures **at 17:00**

CONFIDENCE 2013

Lectures

As always you will be able to meet and exchange ideas with the best and brightest minds in IT security today:

Adam Zabrocki
Crashdumps: hunt 0days and rootkits

Crashdumps are often underestimated source of very interesting information. It is a common belief that they are used only for application/system bugs/vulnerabilities analysis. In this presentation I would like to show a little bit different approach for this source of information. Microsoft Windows allows to change default configuration for WER/CER protocol in such a way, that all generated crashdumps will be stored in a custom storage. This is very useful in a large corporate networks, where we can find tens, hundreds or even thousands of machines, because more than a hundred crashdumps may be generated per day. In most of the cases administrators are afraid of a critical information leak (XBI, PII) via crashdumps, but could they gain some useful knowledge about the network status via this source? I will try to show what kind of benefits could be gained if we start analyzing crashdumps independently and in a little bit different perspective…

Arseny Reutov
PHP Object Injection revisted

The topic will cover new attack vectors regarding unserialiazation of user-supplied data due to vulnerabilities in PHP's builtin classes. Universal XSS, local file read, open_basedir bypass, examples of vulnerable web applications including demo attack on latest vBulletin, Smarty and others.

Devesh Bhatt
My Experiments with truth: a different route to bug hunting

The Best way to improve the security of your systems is to hire hackers. Unfortunately, companies can't hire all best hackers, so the companies has chosen another best way to improve their system security, "Bug Bounty Program".
Google, Facebook, Mozilla, PayPal, Etsy and many other companies pay a good amount to hackers for responsible disclosure and recently it is being started as a service in the form of "bugcrowd" Security Researchers have submitted bugs ranging from configuration issues to SQL injections.
This topic is not about what is a "Bug Bounty" program, who all is paying what amount

and the scope of testing. This paper is basically focused on the approach to finding simple and yet devastating vulnerabilities, earn hefty amounts and share space with the top researchers from around the globe.

This paper depicts easy but unique methods to look for bugs online.
I started on this journey roughly five months back and kind of formulated a procedure to attack the strongest of applications in a short span of time.

Dmitriy Chastuchin, Evgeny Neyolov
Breaking, Forensicating and Anti-Forensicating SAP Portal and J2EE Engine

One of the most critical SAP applications in terms of cyber attacks is SAP Portal, which is based on J2EE engine because it is usually available from the Internet and provides access and connections to other internal SAP and legacy systems. It is necessary to increase awareness in this area, especially after the Anonymous attack on Greece Government where an SAP 0-day vulnerability probably was used, but are you sure that your system has not been compromised? If we talk about SCADA attacks, they are mostly focused on sabotage, which is easy to recognize; attacks on financial systems like banking are focused on money stealing; but if we talk about SAP, the most critical attack is probably espionage, and it is hard to understand if there was espionage because there is no direct evidence of compromise except logs. In this talk, the security architecture of Portal itself and custom applications like iViews will be reviewed, and we will demonstrate how SAP Portal can be attacked. But the main area of the talk will be focused on forensics and finding attack patterns in logs traces and other places to understand if it is possible to completely reverse complex attack patterns. Finally, we will look at how an attacker can try to hide their attacks and how it is possible to deal with it.

There have been a lot of talks covering attacks, but now we will move to the understanding of how to deal with them in the cybercrime era.

Evgeny Neyolov, Dmitriy Chastuchin
Breaking, Forensicating and Anti-Forensicating SAP Portal and J2EE Engine

One of the most critical SAP applications in terms of cyber attacks is SAP Portal, which is based on J2EE engine because it is usually available from the Internet and provides access and connections to other internal SAP and legacy systems. It is necessary to increase awareness in this area, especially after the Anonymous attack on Greece Government where an SAP 0-day vulnerability probably was used, but are you sure that your system has not been compromised? If we talk about SCADA attacks, they

are mostly focused on sabotage, which is easy to recognize; attacks on financial systems like banking are focused on money stealing; but if we talk about SAP, the most critical attack is probably espionage, and it is hard to understand if there was espionage because there is no direct evidence of compromise except logs. In this talk, the security architecture of Portal itself and custom applications like iViews will be reviewed, and we will demonstrate how SAP Portal can be attacked. But the main area of the talk will be focused on forensics and finding attack patterns in logs traces and other places to understand if it is possible to completely reverse complex attack patterns. Finally, we will look at how an attacker can try to hide their attacks and how it is possible to deal with it.

There have been a lot of talks covering attacks, but now we will move to the understanding of how to deal with them in the cybercrime era.

Fernando Gont
Network Reconnaissance in IPv6 Networks

One of the traditional ways of doing network reconnaissance in the IPv4 world has been to perform IPv4 address scans of the target network prefixes. That is, given the IPv4 network prefix of a target network, every single IPv4 address in that prefix is probed in the hopes of finding "alive" nodes. This (somewhat) rudimentary approach to network reconnaissance has proved to be very effective in the IPv4 world, thanks to the reduced scale of the problem: since IPv4 networks are composed of a very reduced number of addresses, brute-forcing the entire search space is not only a feasible task, but is also generally a "good enough" approach.

The Internet Protocol version 6 (IPv6), and the emerging IPv6 deployments, somehow change the rules of the "network reconnaissance" game: with the typical 264 addresses per subnetwork, the traditional brute-force approach to address scanning from the IPv4 world becomes unfeasible. This has led to the widespread (and incorrect) assumption that "IPv6 address scanning attacks are unfeasible".

During the last few years, we have been working on the development of IPv6 network reconnaissance techniques, with two different (but somewhat related) goals in mind: enabling "traditional" penetration testing in the IPv6 world, and dismantling the myth that address scans are not possible in the IPv6 world (hence encouraging the mitigation of these attacks). The aforementioned work has led to the publication of an IETF Internet-Draft entitled "Network Reconnaissance in IPv6 Networks", that has already been adopted by the OPSEC (operations security) Working Group of the IETF (Internet Engineering Task Force).

Alongside our publication efforts at the IETF, we produced and released the SI6 Networks' IPv6 toolkit: a portable, free-software IPv6 toolkit for assessing and trouble-shooting IPv6 networks and implementations. The latest release (v1.3.1) of the toolkit ships with a full-fledged IPv6 address-scanning tool (scan6), that implements all the IPv6 address-scanning techniques discussed in our IETF Internet-Draft, and takes IPv6 address scanning to a new level.

New releases of the IPv6 toolkit are planned for the next few months, with a focus on network reconnaissance: essentially, we aim at producing an implementation of every single IPv6 network reconnaissance technique discussed in our IETF Internet-Draft "Network Reconnaissance in IPv6 Networks".

Following the release of the SI6 Networks' IPv6 toolkit v1.3.1, we embarked ourselves on related (and still ongoing) project: assessing public IPv6 Internet in the hopes of gaining further insights about IPv6 network reconnaissance. We believe that this project will not only serve as a basis to assess the effectiveness of the techniques that we have developed so far, but that the project will also result in a number of insights that will lead to new features in our IPv6 toolkit.

Fernando Gont will provide an overview of IPv6 network reconnaissance techniques, and wil explain how each of those techniques can be implemented in real networks with the SI6 IPv6 toolkit. Fernando will then describe our (currently) ongoing project of assessing the public IPv6 Internet (from a "network reconnaissance" perspective), and will discuss the insights learned as a result of that project.

Felix "FX" Lindner, Gregor Kopf

Cisco in the Sky with Diamonds

The majority of VMware Cloud deployments rely on Cisco virtual and physical switching and routing gear for the network layer. We will provide an introduction into the differences virtual networking makes, how to go about researching its components, as well as cover a number of issues, their exploitation path and some creative workarounds.

CONFIDENCE 2013

Georgia Weidman

Can You Hear Me Now: Leveraging Mobile Devices on Pentests

BYOD is not a new concept. From contractor laptops to an employee's game console in the break room, a compromised device in the corporate environment can lead to all sorts of bad things. In this talk we will look at the unique threats that BYOD for mobile devices brings to the table. The most security conscious corporations are deploying the latest devices and policies to stop attackers from breaching the perimeter and if they do to stop data exfiltration. We will discuss how mobile devices on a corporate network and/or handling company data undermines these efforts. We will look at multiple mobile platforms gathering sensitive information, attacking other devices such as other mobile devices, servers, and workstations, and using out of band communication to perform data exfiltration and communicate with internal devices. Multiple live demo scenarios will be shown and some useful code for pentesters will be released.

Attacking and Securing Mobile Devices

As smartphones take over the workplace, and customers begin deploying smartphone applications as frequently as traditional web applications, it falls to security professionals to integrate these new technologies into penetration testing. How will your organization fair when the smartphone apocalypse arrives? In this course we will study in-depth the techniques used by hackers to exploit mobile phone platforms and applications. We will look at smartphone jailbreaks/roots and real malicious code samples seen in the wild. We will look analyze smartphone apps, using open source tools and manual skills to detect potential attacks and vulnerabilities. Additionally, we will look at real world examples of smartphone apps with vulnerabilities exploitable by attackers. We will cover hands-on exercises exploiting real smartphone platforms and applications. After brushing up on the offensive side, we will switch gears and discuss available methods of defending smartphones in the workplace against the myriad attack vectors. We will look at using the same methods used by attackers for evil, for good to defend smartphone devices and the sensitive data they access. In this course we will use several open source tools for assessing smartphones such as the instructors own Smartphone Pentesting Framework.

Gregor Kopf, Felix "FX" Lindner
Cisco in the Sky with Diamonds

The majority of VMware Cloud deployments rely on Cisco virtual and physical switching and routing gear for the network layer. We will provide an introduction into the differences virtual networking makes, how to go about researching its components, as well as cover a number of issues, their exploitation path and some creative workarounds.

Grzegorz Niemirowski
Desktop applications vulnerabilities

The complexity of modern software in connection with low awareness of security issues among developers, often turns out to be a deadly combination. This applies to both desktop and web applications. The desktop programs, despite they often have web counterparts, are still popular and are an attractive target for cybercriminals. History of finding and exploiting their vulnerabilities is long, just like the list of security mechanisms used to protect them. The topic of desktop applications security is constantly evolving, and in the case of web browsers also touches the issue of security of Web solutions. For example when websites are attacked and infected in order to place malicious code inside visitors' browsers and execute it. A look at the most common attacks on desktop applications and used countermeasures gives an outlook on the most important issues of current situation of software security

Gynvael Coldwind, Mateusz "j00ru" Jurczyk
Beyond MOV ADD XOR – the unusual and unexpected in x86

Intel x86 and the derived AMD64 architecture families are by far the most widespread and commonly known ones, powering millions and millions of desktop PCs, server racks and even some mobile devices. Although understanding low-level X86 assembly code has been subject to extensive study by hobbyists, professional reverse engineers and exploit developers alike, the research typically covers only a small subset of both instruction set and features the architecture has to offer. In this presentation, we will address numerous interesting, often security-relevant tidbits, unpopular features and unusual behaviors that we have came across during our journey through the manuals, books and research papers, as well as our own experience. Basic knowledge of x86 assembly and its execution environment is highly recommended.

Nguyen Anh Quynh
Opticode: machine code deobfuscation for malware analysts

Modern malware use a lot of obfuscation techniques to make its code more difficult to understand for malware analysts, with the hope of preventing attempts to reverse engineer their codes. Unfortunately, malware analysts are still reversing such nasty codes manually since there are no reliable tools to help with this problem.

OptiCode is the answer to this headache. Our tool combines theorem prover and compiler techniques to automatically find and remove the obfuscated sections, then presents the cleaned code to the users. Available as a Web-based tool and IDA plugin, OptiCode is user-friendly, and supports both 32-bit and 64-bit Intel platforms.

In this talk, we will analyze some obfuscation techniques in use by malware, and introduce the design and implementation of OptiCode. Some cool demo will be presented, so the audience can see how OptiCode works in reality.

Ilja van Sprudel
Linux Desktop Insecurity

I used to use Linux and the bsd's. Then mostly switched to windows 6-7 years ago. I recently found some spare time and got reacquainted with the unices. Over the past weeks, I've spend some time assessing the local security of modern desktop unices. as it turns out, things are a total mess.
A short layout of the presentation:

- local security of modern desktop unices
- attack surfaces
- bugs found
- X client libs (attack surface, bugs, how to use them correctly and securely)
- shadow library issue
- a model for more secure suid binaries

Jesse Burns
Securing Data in Mobile Application Suites

Building sets of applications that work together, securely sharing data between them is a common challenge for developers at large companies. On mobile platforms like Android and IOS, this challenge has new dimensions. This talk will discuss how mobile security models need to be worked with in order to safely share data between

members in families of applications without also allowing attackers access. Android and IOS have very different ways of achieving similar security goals, and this talk will cover how to leverage the tools these platforms provide, as well as provide some advice for checking that your protections worked. The talk will also discuss user security expectations.

Jochen Belke
Invisible attacks – visible in your network. How to see and follow the tracks?

The nature of attacks have significantly changed recently. From broad and scattershot to very targeted attacks with persistent adversaries (often times nation-states). The attacks of today use advanced malware, zero-day and APT tactics to penetrate networks for the purpose of control, espionage and data theft. What is the most important, these attacks evade and obfuscate traditional security solutions (FW, IPS, Content Security, Antyvirus, etc.), trying to hide and to be invisible in a compromised network. During this session we will cover this problem. We will present modern technologies which discover and block stealth attacks, with an emphasis on the network layer solutions. We will also present case study of detecting data loss, network reconnaissance activity as well as detecting botnet command, control activity and tracking the spread of a malware infection throughout the network.

Julian Bangert
Any Input Is a Program: Weird Machines in ABI and architecture metadata

Complex enough input to a complex enough system can have effects indistinguishable from a native program for that system. A sufficiently complex input format may become "byte code" for a kind of a virtual machine within the software that handles it; in many classic exploit programming techniques, data is the program that runs on the code. We will show two examples of this that aren't exploits as such, but show Turing-complete programming by kinds of data that are hardly ever given a second glance: (1) ELF binary format headers with nothing but well-formed relocation and dynamic symbol entries (executed by the runtime linker-loader), and (2) x86 memory and interrupt descriptor tables (executed by the CPU page fault handling and context switching logic, without any instructions being successfully dispatched).

If these data formats can hide a Turing-complete computation, what about all others more complex "feature-rich" ones? What makes a format lend itself to being an equivalent of an instruction set? Can looking for "weird machines" help design trustworthy systems? Join us for the talk and discussion of this weird research direction!
ELF Eccentricities

.Bx has demonstrated how to build a Turing machine out of well-formed relocations and symbols of the ELF binary format. Other aspects of the format can be just as twisted. From a language-theoretic standpoint, the ELF format is very context-sensitive: much metadata is stored redundantly and interesting things can happen when metadata is inconsistent. Furthermore, we believe these dependencies are one of the reasons ELF binary manipulation tools are so hard get right and will present a work-in-progress framework in the style of ERESI's elfsh that takes care of metadata-consistency for modified binaries and parsing inconsistencies for untrusted binaries.

MC, Yaniv Miron
Ph0k 0-days, We Will Pwn U with Hardware Mofos

We gives you the ultimate hardware hacking kit.
Wanna pwn some banks? Wanna own big companies? You need some boost up. We will show you that your current set of tools is not enough. You need to have some help from hardware, like 007.

We have bundled a set of hardware hacking tools that will assist you.
For example we will show you how to bypass typical corporate Windows 7 machines with Bitlocker encryption enabled, dump and extract goodies from memory, long range RFID tricks to copy ur CEOs proxcard, using hardware screenloggers (not the old crappy keyloggers – cuz everybody knows them and it's lame) and more. You have to be there – cuz we rock.

Marek Zmysłowski
Penetration Testing – 7 Deadly Sins

Plenty of both small and large companies use penetration testing as tools for checking the security of various system components. Although, as any tool, it has to be used properly. Many mistakes made during planning of different test steps often lead to a conclusion that penetration tests were useless. In this presentation we will show 7 base reasons which lead to a penetration tests failure. Those are the mistakes not in the tests design but the fails of developers and project managers.

Mariusz Sawczuk
Invisible attacks – visible in your network. How to see and follow the tracks?

The nature of attacks have significantly changed recently. From broad and scattershot to very targeted attacks with persistent adversaries (often times nation-states). The attacks of today use advanced malware, zero-day and APT tactics to penetrate networks for the purpose of control, espionage and data theft. What is the most important, these attacks evade and obfuscate traditional security solutions (FW, IPS, Content Security, Antyvirus, etc.), trying to hide and to be invisible in a compromised network. During this session we will cover this problem. We will present modern technologies which discover and block stealth attacks, with an emphasis on the network layer solutions. We will also present case study of detecting data loss, network reconnaissance activity as well as detecting botnet command, control activity and tracking the spread of a malware infection throughout the network.

Mateusz "j00ru" Jurczyk, Gynvael Coldwind
Beyond MOV ADD XOR – the unusual and unexpected in x86.

Intel x86 and the derived AMD64 architecture families are by far the most widespread and commonly known ones, powering millions and millions of desktop PCs, server racks and even some mobile devices. Although understanding low-level X86 assembly code has been subject to extensive study by hobbyists, professional reverse engineers and exploit developers alike, the research typically covers only a small subset of both instruction set and features the architecture has to offer. In this presentation, we will address numerous interesting, often security-relevant tidbits, unpopular features and unusual behaviors that we have came across during our journey through the manuals, books and research papers, as well as our own experience. Basic knowledge of x86 assembly and its execution environment is highly recommended.

Meredith L. Patterson
LANGSEC 2011-2016

As our "voyage of the Beagle" continues, the language-theoretic security framework, initially proposed by Len Sassaman, Meredith L. Patterson, and Sergey Bratus, has developed not only as a descriptive framework for the classification of vulnerabilities, but a constructive framework for conceptualizing and reducing to practice both "weird machines" in the most unusual places and engineering principles for more attack-resistant, more performant software. In this talk, we'll highlight an important example of LANGSEC in practice before we even gave it that name, follow the growth in the field over the last two years, and give a look ahead at just some of the directions

in which the field is expanding.

Michał Sajdak

Embedded Devices Hacking

The presentation will cover a few simple but unusual methods of obtaining root shell on embedded devices. I will also present my latest research – backdoor in TP-Link devices which allows for unauthenticated remote root execution. The whole discovery features such problems as – path traversal, ftp chroot escape, http communication, tftp communication and configuration files overwriting.

Nikita Tarakanov

Exploiting Hardcore Pool Corruptions in Microsoft Windows Kernel

Each new version of Windows OS Microsoft enhances security by adding security mitigation mechanisms.
Kernel land vulnerabilities are getting more and more valuable these days. For example, the easy way to escape from a sandbox (Google Chrome sandbox for example) is by using kernel vulnerability.

That's why Microsoft struggles to enhance security of Windows kernel. Kernel Pool allocator plays significant role in security of whole kernel. Since Windows 7 Microsoft started to enhance security of kernel pool allocator.

Kernelpool aka Tarjei Mandt has done great job on analyzing internals of kernel pool allocator, which includes great attack techniques, mitigations bypasses etc. In windows 8 Microsoft has eliminated almost all reliable techniques of exploiting kernel pool corruptions. However, attack techniques by Tarjei need a lot of prerequisites to get success. There are a lot of types of pool corruptions where these techniques don't work, unfortunately.

What if there is no control over overflown data?
What if there is constant(zero bytes) and you have no chance to apply one of Tarjei's techniques?
What if there is uncontrolled continuous overflow and #PF and BSOD is unavoidable?
So what to do?
Commit suicide instantly?
NO!
Come and see this talk!
This talk presents technique of 100% reliable exploitation of kernel pool corruptions. This unique technique works since NT 4.0 to Windows 8 including.

Rebecca Shapiro, Sergey Bratus, Julian Bangret
Any Input Is a Program: Weird Machines in ABI and architecture metadata

Complex enough input to a complex enough system can have effects indistinguishable from a native program for that system. A sufficiently complex input format may become "byte code" for a kind of a virtual machine within the software that handles it; in many classic exploit programming techniques, data is the program that runs on the code. We will show two examples of this that aren't exploits as such, but show Turing-complete programming by kinds of data that are hardly ever given a second glance: (1) ELF binary format headers with nothing but well-formed relocation and dynamic symbol entries (executed by the runtime linker-loader), and (2) x86 memory and interrupt descriptor tables (executed by the CPU page fault handling and context switching logic, without any instructions being successfully dispatched).

If these data formats can hide a Turing-complete computation, what about all others more complex "feature-rich" ones? What makes a format lend itself to being an equivalent of an instruction set? Can looking for "weird machines" help design trustworthy systems? Join us for the talk and discussion of this weird research direction!

Robert Lipovsky
The "Facebook PokerAgent"

In March 2012 we have been tracking a botnet, which was used by the perpetrator to harvest Facebook log-on credentials. In addition to expanding the database of stolen Facebook user names and passwords, the bots were being instructed to ascertain the number of credit cards linked to the Facebook accounts and Zynga Poker player stats of the victimized users. The threat was mostly active in Israel.

With Facebook being such a hot topic, this would constitute an interesting phishing threat just due to the aforementioned characteristics, but the matter gained more seriousness when we discovered that the bot master had managed to acquire over 16000 Facebook credentials through his operation, as our botnet monitoring had revealed.

The presentation begins with an overview of the threat and the technical details of the used trojan horse. Afterwards, we will describe the process of monitoring the botnet and present the highlights of the following investigation.

CONFIDENCE 2013

Sergey Bratus, Julian Bangret, Rebecca Shapiro
Any Input Is a Program: Weird Machines in ABI and architecture metadata

Complex enough input to a complex enough system can have effects indistinguishable from a native program for that system. A sufficiently complex input format may become "byte code" for a kind of a virtual machine within the software that handles it; in many classic exploit programming techniques, data is the program that runs on the code. We will show two examples of this that aren't exploits as such, but show Turing-complete programming by kinds of data that are hardly ever given a second glance: (1) ELF binary format headers with nothing but well-formed relocation and dynamic symbol entries (executed by the runtime linker-loader), and (2) x86 memory and interrupt descriptor tables (executed by the CPU page fault handling and context switching logic, without any instructions being successfully dispatched).

If these data formats can hide a Turing-complete computation, what about all others more complex "feature-rich" ones? What makes a format lend itself to being an equivalent of an instruction set? Can looking for "weird machines" help design trustworthy systems? Join us for the talk and discussion of this weird research direction!

ELF Eccentricities

.Bx has demonstrated how to build a Turing machine out of well-formed relocations and symbols of the ELF binary format. Other aspects of the format can be just as twisted. From a language-theoretic standpoint, the ELF format is very context-sensitive: much metadata is stored redundantly and interesting things can happen when metadata is inconsistent. Furthermore, we believe these dependencies are one of the reasons ELF binary manipulation tools are so hard get right and will present a work-in-progress framework in the style of ERESI's elfsh that takes care of metadata-consistency for modified binaries and parsing inconsistencies for untrusted binaries.

Thomas Lim
The Keynote

Yaniv Miron, Marcel "MC" Carlsson
Ph0k 0-days, We Will Pwn U with Hardware Mofos

We gives you the ultimate hardware hacking kit.
Wanna pwn some banks? Wanna own big companies? You need some boost up. We will show you that your current set of tools is not enough. You need to have some help from hardware, like 007.

We have bundled a set of hardware hacking tools that will assist you.
For example we will show you how to bypass typical corporate Windows 7 machines with Bitlocker encryption enabled, dump and extract goodies from memory, long range RFID tricks to copy ur CEOs proxcard, using hardware screenloggers (not the old crappy keyloggers – cuz everybody knows them and it's lame) and more. You have to be there – cuz we rock.

Yury Chemerkin
Insecurities in blackberry

This paper proposes a new security research covers BlackBerry issues relating their own features relied on highest possible way of integration and aggregation with data, service and application that simplifies management. Such way integration shapes developer's outlook as well as malware writer's outlook led to the bypass security methods. Despite of that, BlackBerry is full of holes to the brim if consumer has a flexible IT Policy even because current security techniques implemented in BIS (BlackBerry Internet Service) or BES (BlackBerry Enterprise Server) are indecisive argument to be sure in security and privacy and do not provide enough control. As opposite to smartphone, the tablets (PlayBook) are quite new, QNX-based and have the most known technologies, such Adobe Air, HTML5, and Android Dalvik-Runtime, are implemented widely. However, they have a poor application environment and a little those feature known on non-QNX BlackBerry device. This makes security more difficult and unstable to reliably use it by end-users. Research shows that additional third party security solutions often ruin security while native environment allows intercepting, blocking, stealing, misleading, substitute data in real-time bypassing security controls that, finally, reveal sensitive information and turn security solutions to the malware agents. The non-malware applications may use rootkit techniques, e.g. firewall hooks API to watch any incoming or outgoing network traffic. The legitimizing effect of commercial "malware" software led away from user-mode towards the kernel-mode techniques at first glance. However, user-mode rootkits or

spyware are still effective to bypass security applications because they have simple APIs calling kernel methods. This research examines and highlights a range of issues referred to the incorrect approach to the security techniques development. It draws security management level of inefficiency outside isolated environment as well as old-attack techniques possibility of application for new BlackBerry device known as Playbook. The research presents pressing issues for fundamental and application BlackBerry security cases, exploitation of native applications built in OS. In additional, third-party security applications are going to be examined for security holes and misunderstanding BlackBerry security concepts.

Trainings:

Georgia Weidman
Attacking and Securing Mobile Devices

As smartphones take over the workplace, and customers begin deploying smartphone applications as frequently as traditional web applications, it falls to security professionals to integrate these new technologies into penetration testing. How will your organization fair when the smartphone apocalypse arrives? In this course we will study in-depth the techniques used by hackers to exploit mobile phone platforms and applications. We will look at smartphone jailbreaks/roots and real malicious code samples seen in the wild. We will look analyze smartphone apps, using open source tools and manual skills to detect potential attacks and vulnerabilities.

Additionally, we will look at real world examples of smartphone apps with vulnerabilities exploitable by attackers. We will cover hands-on exercises exploiting real smartphone platforms and applications. After brushing up on the offensive side, we will switch gears and discuss available methods of defending smartphones in the workplace against the myriad attack vectors. We will look at using the same methods used by attackers for evil, for good to defend smartphone devices and the sensitive data they access. In this course we will use several open source tools for assessing smartphones such as the instructors own Smartphone Pentesting Framework.

CONFIDENCE 2013

Fernando Gont

IPv6 Hacking Crash Course

The IPv6 protocol suite was designed to accommodate the present and future growth of the Internet, by providing a much larger address space than that of its IPv4 counterpart, and is expected to be the successor of the original IPv4 protocol suite. The imminent exhaustion of the IPv4 address space has resulted in the deployment of IPv6 in a number of production environments, with many other organizations planning to deploy IPv6 in the short or near term.
There are a number of factors that make the IPv6 protocol suite interesting from a security standpoint. Firstly, being a new technology, technical personnel has much less confidence with the IPv6 protocols than with their IPv4 counterpart, and thus it is more likely that the security implications of the protocols be overlooked when the protocols are deployed. Secondly, IPv6 implementations are much less mature than their IPv4 counterparts, and thus it is very likely that a number of vulnerabilities will be discovered in them before their robustness matches that of the existing IPv4 implementations. Thirdly, security products such as firewalls and NIDS's (Network Intrusion Detection Systems) usually have less support for the IPv6 protocols than for their IPv4 counterparts. Fourthly, the security implications of IPv6 transition/co-existence technologies on existing IPv4 networks are usually overlooked, potentially enabling attackers to leverage these technologies to circumvent IPv4 security measures in unexpected ways.

The imminent global deployment of IPv6 has created a global need for security professionals with expertise in the field of IPv6 security, such that the aforementioned security issues can be mitigated.

IPv6 Hacking Crash Course provides a full-day intense IPv6 hacking experience, focusing on hands-on IPv6 hacking exercises. The training is carried out by Fernando Gont, a world-renowned IPv6 security expert.

Contests

ESET Crackme

This time before the CONFidence conference, we have published on our website a special application prepared by the ESET team. By solving it before the conference you had a chance to win a ticket to the CONFidence 2013.
However if you still want to have a breake and solved a puzzle look for one of the news on the webpage to find that Crackme. Have fun!

Treasure Hunt

It's a task only for the most daring! We have prepared special tasks for teams of max. four people. Register your team at the information stand and get points in the Treasure Hunt! A great prize will be waiting for the team with the highest number of points.

The task is simple: we will prepare a list of collectable objects and crazy activities. Every item on the list will be assigned a certain number of points. The goal for the team is to get as many items and activities as they can and present them to the CONFidence crew. In case of activities, we will need a proof of performing the task. The list will be available at the registration area since the beginning of the conference.

WARNING! This contest involves crazy tasks so prepare yourself for the hardest competition you have ever seen!

CONFIDENCE 2013

Sponsors

Platinium Sponsor

Cisco Poland was established in 1995, with the opening of the Warsaw office. Over the past 17 years, Cisco has been actively contributing to building a knowledge-based economy and creating an ecosystem of more than 1,000 local partners. The Cisco Global Support Center in Krakow was opened in May 2012. The center complements existing locations to provide technical and business services to internal and external stakeholders, including channel partners and customers, across multiple functional groups such as Cisco Services, Finance, Operations and others. The Cisco Global Support Center in Krakow is part of a network of operations located around the globe and has a special focus on Europe, Middle East, Africa and Russia (EMEAR). Cisco's largest corporate social responsibility initiative, Cisco Networking Academy, has been active in Poland since 2000 and there are currently more than 400 academies with 20,000 students operating across the country. Since its launch in Poland, more than 80,000 local students have participated in the diverse IT and networking courses offered by the academy.

Sevenet S.A. is an IT sector company offering advanced ICT solutions for companies and institutions in Poland since 1997. Since June of 2011 shares of the company are noted on the OCT market of Newconnect.
Sevenet is a Cisco Gold Certified Partner, Microsoft Gold Communications Partner and Microsoft Gold Management & Virtualization. Our offer is constantly widened by partnerships with the following companies: EMC, McAfee, F5, Palo Alto, FireEye, Motorola, 2RING, NICE.

CONFIDENCE 2013

The main field of Sevenet S.A. activity is Borderless Network connected with designing, building, configuring and servicing wired and wireless communication networks solutions, based on the IP protocol. Another field of Sevenet activity are Unified Communication solutions exploited in innovative business communication in B2B and B2C relations: videoconferences, routers and switches and multimedia information kiosk. Sevenet S.A. also offers security solutions – systems which guarantee security for different areas of IT infrastructure.

In 2011 SeveNet commenced two significant projects by establishing SPV`s: Sevenpen Sp. z o.o. offers an innovative digital pen technology – Digital Pen & Paper which simplifies and streamlines business and administrative processes. Seventica Sp. z o.o. offers Non-verbal Communication System enabling non-distorted communication between an institution and the person with hearing disability.

Golden Sponsors

ESET, founded in 1992, is a global vendor of security software for corporate customers and households. ESET develops software solutions that deliver instant, comprehensive protection against evolving computer security threats. We pioneered and continue to lead the industry in proactive threat detection.

Flagship products are ESET NOD32 Antivirus and ESET Smart Security. Built on the award-winning ThreatSense® engine are highly integrated security solutions trusted by more than 100 milion of users to protect their computers against a host of Internet-borne malware, such as viruses, trojans, worms, adware, spyware, phishing, rootkits and other Internet threats.

CONFIDENCE 2013

Silver sponsor

SAFE COMPUTING

Safe Computing Sp. z o.o. – is provider of the newest technologies in information security and electronic transactions. The company provides data security solutions in the areas of consulting, design and development, implementation and maintenance. Safe Computing was establish in 1992 and from the beginning of its existence concentrated solely on supplying IT security solutions to large organizations in Poland (large banks and financial institutes). Company accommodated to the market's growing demands and customer's individual needs and extended the offer about for example – appliaction level security testing In Q2 of 2004 Safe Computing received a certificate of compliance of its quality management system with ISO 9001:2000 standard. The company is divided into departments, with full separation of duties: Sales, Technical, Finance and Administration. Safe Computing employs full time consultants and IT specialists, providing advice in choosing an optimal solutions, the best for customer's needs. We ensure the highest level of security and all of our solutions are based on industry standards.

UBS

UBS draws on its 150-year heritage to serve private, institutional and corporate clients worldwide, as well as retail clients in Switzerland. Headquartered in Zurich and Basel, Switzerland, UBS has offices in more than 50 countries, including all major financial centres, and employs approximately 62,800 people.

UBS Poland Service Centre (UBS PSC) was established in 2007 and plays an important role in achieving UBS's goal of being the world's leading financial services company.

CONFIDENCE
2013

UBS PSC provides majority of supporting functions which are crucial to the functioning of the client-facing business divisions, i.e. HR, IT, Finance, Operations.

Within the Technology stream we provide a full range of IT services, including: software development, quality assurance, L2/L3 support, systems analysis, risk assessment. We have developed a long track record of successful projects and initiatives, including the entire application life cycle process requiring all IT roles also using cutting edge technologies and applying the best industry standards and methodologies.

Our IT Risk & Security experts assess risks related to a wide range of IT systems and vendors and prepare recommendations which help the business in creation of action plans.
We're one of the largest financial IT Risk & Security hubs in Poland, offering interesting positions on each stage of career – starting from interns to senior security experts.

In addition to our internal IT teams, we work with strategic UBS partners. We develop and maintain applications for UBS, supporting Investment Banking business mainly, by providing in-house IT solutions and co-creating them with UBS offices around the globe.

To check the variety of our IT roles, please see: www.ubsc.com/polandcareers

CONFIDENCE 2013

Strategical Partners

Małopolska

Małopolska Region is the cradle of science and culture, the region opened to tourists (9 million tourists a year) and investors, with a high level of economic development.

Kraków – Quintessentially Polish, the country's former capital and the polish kings headquarter embodies everything tourists seek. Its attractions includes Wawel Castle, the Dragon, the oldest Polish university, festivals, countless cafes, and charming narrow streets. Małopolska – vibrant and rich in cultural and natural attractions, offers an opportunity for adventure while exploring Poland's history and heritage.

Małopolska Region boasts a constantly evolving innovation, which is associated with the presence of high-tech industries, research institutes, universities and innovative companies. Regional Government supports the economic development of the Region. Already 500 million zlotys paid businesses within 5 years of the Małopolska Regional Operational Program for the years 2007 – 2013, another 300 million will be gradually settled. Enterprise support, also in areas of smart specialization of Małopolska Region such as information and communication technologies (including multimedia), life science, sustainable energy, chemistry, is also one of the key growth areas in the Małopolska Region until 2020.

Throughout years, we have been achieving significant successes, changing the face of the Małopolska ICT sector – Małopolska takes 2nd place among the regions with the highest percentage of employment in the ICT sector – more than 4 000 employees. The value of investments in Małopolska amounted to EUR 7.6 million, creating 1,580 jobs. It is in Kraków that two out of the three most popular Polish web portals, i.e. Onet and Interia, were established. Kraków is also seat of ComArch – one of the most dynamic companies in the Polish ICT sector. Naturally, not only Polish entrepreneurs invest in Kraków, but also renowned international companies from the high-tech sector, such as Motorola, IBM, ABB and Delphi. There is no doubt that Małopolska is a dynamically developing region of solid foundations therefore join us and grow with us because Here, the future begins.

www.malopolskie.pl

CONFIDENCE
2013

Historia Wodociągów Krakowskich sięga końca XIX wieku. W 1889 roku, po ponad trzydziestu latach starań, rozpoczęto budowę nowoczesnego systemu wodociągowego. Było to jedno z największych i najkosztowniejszych przedsięwzięć, których podjął się ówczesny Kraków. Uroczyste uruchomienie pierwszego Zakładu Uzdatniania Wody na Bielanach w 1901r. rozpoczyna historię Miejskiego Przedsiębiorstwa Wodociągów i Kanalizacji S.A.
Na przestrzeni lat spółka podlegała wielu zmianom, tak jak zmieniało się otoczenie i oczekiwania mieszkańców.
Obecnie MPWiK S.A. to firma nowoczesna, jej produkt spełnia wszystkie obowiązujące normy, a dzięki podejmowaniu nowych wyzwań Krakowskie Wodociągi stały się synonimem jakości i bezpieczeństwa zaopatrzenia w wodę.

Realizację nadrzędnego celu MPWiK S.A., jakim jest zapewnienie mieszkańcom Krakowa usług najwyższej jakości, potwierdzają posiadane certyfikaty, m. in. Certyfikat ISO 9001-2000 i ISO 14001-2004, certyfikat Przedsiębiorstwa Fair Play. Najwyższą jakość świadczonych usług zapewnia między innymi stały monitoring Akredytowanego Laboratorium (akredytacja nr 776). Na podstawie analiz wykonywanych przez Centralne Labolatorium można śmiało stwierdzić, że woda w Krakowskich Wodociągach jest czysta i zdrowa, ponieważ spełnia wymagania zarówno krajowe jak i europejskie.

MPWiK S.A. to cztery zakłady uzdatniania wody, dwie oczyszczalnie centralne, sześć oczyszczalni lokalnych i blisko cztery tysiące kilometrów sieci wodociągowych i kanalizacyjnych zapewniających nieprzerwaną dostawę wody i odprowadzanie ścieków. Spółka działa na terenie Gminy Miejskiej Kraków oraz dodatkowo dostarcza wodę do dwunastu gmin ościennych, a odbiera i oczyszcza ścieki dostarczane siecią kanalizacyjną z sześciu gmin podkrakowskich.
W roku 2013 Wodociągi Krakowskie rozpoczęły kampanię zachęcającą do picia wody kranowej. Kampania przebiegająca pod hasłem „Dobra woda prosto z kranu", ma rozpowszechnić, potwierdzić i utrwalić przekonanie mieszkańców Krakowa, że

woda z kranu jest zdatna do bezpośredniego spożycia. Grupę docelową oprócz mieszkańców Krakowa stanowią także mieszkańcy gmin sąsiednich pracujący lub uczący się w Krakowie, jak również turyści odwiedzający Kraków. Celem kampanii jest m.in. podniesienie poziomu wiedzy mieszkańców Krakowa na temat wysokiej jakości wody z kranu, zachęcenie do picia wody z kranu bez uprzedniego przegotowania, a także zbudowanie wizerunku wody jako produktu bezpiecznego.

www.wodociagi.krakow.pl
www.prostozkranu.krakow.pl

Partners

http://www.ccie.pl/
http://www.hackersonaplane.info/
https://hacktivity.com/hu/
https://issa.org.pl/
http://www.nullcon.net/website/
http://niebezpiecznik.pl/
https://www.nethemba.com/
https://www.owasp.org/index.php/Main_Page
http://www.ph-neutral.org/
http://webhosting.pl/

MEDIA Sponsors

http://www.beyondsecurity.com/
http://www.computerworld.pl/
http://www.cybsecurity.org/
http://dsecrg.ru/
http://di.com.pl/
http://e-biznes.pl/
http://www.egospodarka.pl/
http://ethicalhacker.net/
http://www.globalsecuritymag.com/
http://hack.pl/
http://hacking.pl/
http://www.infoprof.pl/
http://locos.pl/
http://portalmedialny.pl/
http://mobiledeveloper.pl//
http://nfsec.pl/
http://pentestmag.com/
http://phdays.com/
https://www.securitysummit.it/
http://securityxploded.com/
http://www.sectechno.com/
http://www.bluekaizen.org/security-kaizen-magazine/
http://securitymag.pl/
http://www.siis.org.pl/
http://www.virusbtn.com/index
http://vulnerability-lab.com/
http://www.xakep.ru/

CONFIDENCE 2013

With great satisfaction we can conclude that our previous projects resulted in a huge success and became the motivation to create a new department, which carries out external conferences for commercial clients. We believe that nine years of experience backed by organising almost 50 Polish and international conferences attended by more than 15,000 participants, will provide the highest level services for you.

We offer comprehensive event organisation, web design, software development, graphic service, design and implementation of advertising gadgets, provision of conference venue, organisation of activities and evening after party, provision of conference staff, contact with speakers, sponsors, media partners and company representation at the events. Our current projects include:

PLNOG Polish Network Operators' Group

euronog european network operators group

ConFidEncE

bitspiration

ennovation more than experience

StartupWeekend Kraków

JDD

4DEVELOPERS

CISCO SECURE

PROIDEA Foundation always puts on high level of presentations, but also on professional and efficient organisation. Knowing the needs of the industry and having many years of experience, we encourage you to cooperate with us. We are confident that we can meet all of your expectations and meet the many challenging tasks!

CONFIDENCE 2013

Lunch

Because there is no restaurants anywhere around the venue, we decided to open a special BBQ section for all attendees. The lunch will start around the time specified in the conference schedule and will last until we run out of the food of the day.

Venue

CONFidence has always had a special, underground atmosphere and we believe that using the historic buildings of Water Pumping Station in Bielany as a venue perfectly fits the amazing wibe of the meeting. Here you can not only attend the technical lectures held in the amazing, industrial interiors, but also enjoy BBQ, play games and participate in various contests.

Venue address:

Księcia Józefa Street 299
Krakow, Poland
Google coordinates:
@50.042298,19.841225

Critical Contacts

Sławomir Jabs - Main ogranizer +48 506 689 591
Justyna Bień - Speakers +48 506 689 463
Marek Nowak - Berlin Trip Interviews Sponsors +48 506 689 503
Kuba Płaziński - Venue X-traction Point +48 506 804 470
Jakub Kozioł - Proidea Representative +48 504 172 327
Karolina Pachel - Proidea Representative +48 506 689 456

CONFIDENCE 2013

Twitter account

Our account is @CONFidence_news and the hash tag is # CONFidence_news
So use it frelly

Conference schedule for mobile application

The schedule is avaiable on Lanyrd so feel free to look it up at:
http://lanyrd.com/2013/confidence-news/schedule/
You can use the mobile Lanyrd application to access a mobile schedule of the conference.

Feedback!

We always welcome all comments and suggestions, so please don't hesitate to contact us! We are also reachable through Twitter at @CONFidence_news.

Thank you!