



# SWISS CYBER STORM 3

**Join Swiss Cyber Storm 3  
4-day Security Conference**

12-15 May 2011 Rapperswil  
[www.swisscyberstorm.com](http://www.swisscyberstorm.com)

# CYBER STORM BRIEFINGS THURSDAY / FRIDAY



www.swisscyberstorm.com

„Triple Track Series“ – We are proud to announce the lecturing talks of Swiss Cyber Storm 3. We have received a great number of CFPs (Call for Paper) submissions from local and international speakers. Check out the speaker list below.

Cyber Crime	Exploit & Defense	OWASP Web Security
+ <b>Dr. Bruce Nikkel (CH)</b> CORPORATE IT FORENSIC READINESS	+ <b>Jeremy Brown (USA)</b> SCADA HACKING	+ <b>Antonio Fontes (CH)</b> OWASP SUMMIT & OUTCOMES
+ <b>Marc Henauer (CH)</b> CYBER WAR IN EUROPE	+ <b>Srdjan Capcun (CH)</b> CRACKING KEYLESS CAR SYSTEM	+ <b>Stefano Di Paola (ITA)</b> DOMXSS ANALYSIS - EXPLOITATION
+ <b>Christiaan Beek (NL)</b> INVESTIGATION NIGHT DRAGON	+ <b>Daniel L. Creus (ES)</b> MAN IN THE MOBILE	+ <b>Marco Balduzzi (ITA)</b> PARAMETER POLLUTION
+ <b>Mauro Vignati (CH)</b> BANKING GANGSTER - CYBER CRIME	+ <b>Pascal Junod (CH)</b> CRYPTO ATTACKS - LIVE SHOW	+ <b>Christian Folini (CH)</b> WEB DDOS PREVENTION
+ <b>Raoul Chiesa (ITA)</b> HACKER PROFILING PROJECT	+ <b>Celil Ünüver (Turkey)</b> BUG HUNTING IN WINDOWS MOBILE	+ <b>Yiannis Pavlosoglou (UK)</b> WEB PORT KNOCKING
+ <b>Daniel Weng (China)</b> CHINA PROFESSIONAL INVESTIGATION AND SURVEILLANCE ALLIANCE	+ <b>Alaa Al-Din Al-Radhi (JO)</b> IPV6 SECURITY TESTING TOOLS	+ <b>Sylvain Maret (CH)</b> STRONG AUTHENTICATION IN WEB APPLICATION
+ <b>Stefan Frei (CH)</b> CTO SECUNIA, FAILURE OF CLIENT SIDE SECURITY	+ <b>Julien Bachmann (CH)</b> APPLE IOS REVERSE ENGINEERING	+ <b>Peter Greko (USA)</b> + <b>Fabian Rothschild (USA)</b> ANTI BOTNET DEVELOPMENT
+ <b>David Rosenthal (CH)</b> EUROPEAN VIEW TO DATA LEAKAGE	+ <b>Jeremiah Talamantes (USA)</b> PLUG-BOT BACKDOOR	+ <b>Jörg Ewald (CH)</b> APPLICATION SECURITY AS A TEAM EFFORT
+ <b>Darren Turnbull (UK)</b> TURNING SECURITY LATENCY INTO COMPETITIVE ADVANTAGE	+ <b>Lee Ling Chuan (Malaysia)</b> MALWARE HUNTING EMULATOR & DISASSEMBLER	+ <b>Rosario Valotta (ITA)</b> COOKIE JACKING - UI REDRESSING
+ <b>Roger Blum (CH)</b> TREND: HACKING GSM NETWORKS	+ <b>Dave Wollmann (GER)</b> ADVANCED SOCIAL ENGINEERING	+ <b>Thomas Röthlisberger (CH)</b> HTML5 (IN)SECURITY
+ <b>Reto Inversini (CH)</b> CCERT - HOW TO ADDRESS ADVANCED PERSISTENT THREATS	+ <b>Mathias Payer (Li)</b> BYPASS SOFTWARE ISOLATION AND VIRTUALIZATION	+ <b>Brian Mariani (CH)</b> ACTIVE-X EXPLOITATION

## LEARN FROM THE EXPERTS - SORT BY TRACK

02

### Cyber Crime Track



Target Audience: CIO, CTO, CISO, IT Risk Management

- \* Swiss Intelligence Service - Cyber Crime in Europe
- \* Investigation report: ‚Criminal Networks‘ - Banking Fraud
- \* Investigation report: ‚Night Dragon‘ attacks from China
- \* Who are the attackers? Social background? Statistics
- \* Cloud-based Shared Mental Model for Cyber warfare prediction
- \* The fundamental failures of endpoint security - rule the future
- \* European data loss prevention - the delay of policy makers
- \* Trend: Hackers invest into GSM/Telco hacking. Where is the trust?

### Exploit & Defense Track



Target Audience: Pentester, Security Researcher

- \* SCADA Hacking, Exploit Writing, Reverse Engineering
- \* GSM Hacking
- \* Hacking keyless car systems - latest research from the ETH
- \* Plug-Bot Hardware Pentesting Tool
- \* Man in the Mobile & Hacking Windows Mobile
- \* IPv6 Security Testing
- \* Apple IOS Reverse Engineering
- \* Reverse Engineering & Disassembler - Malware Hunting
- \* Advanced SE attacks - new approach to bypass human trust
- \* Bypassing software isolation and virtualization solutions
- \* Showcase: How to break crypto systems - from a cryptographer!

### OWASP & Web Security



Target Audience: Web Security Experts, Web Pentester, Auditors

- \* OWASP initiatives - learn and participate in the OWASP future
- \* SpiderMonkey JavaScript Engine Hack - find new DomXSS vulns
- \* Latest http parameter pollution tricks and IDS evasion
- \* Defeating DDOS web attacks after Wikileaks storm
- \* New approach for admin interfaces - web port knocking
- \* Study: Identify users without authentication - Facebook correlation
- \* Crazy approach of botnet resistant web development
- \* Bypassing Same Origin Policy: UI Redressing
- \* HTML5 (In)Security
- \* ActiveX Exploitation

### Professional Moderation



Regula Späni - Former SF Switzerland TV moderator - Switzerland

Regula Späni is our Cyber Crime talk master and moderator. She will guide through the agenda and lead the podium discussions at the end of the day.

www.swisscyberstorm.com

03

## KEYNOTE - PETER GLOOR, MIT USA



**Dr. Peter A. Gloor** - Research Scientist, MIT Center for Collective Intelligence, Chief Creative Officer, galaxyadvisors AG, USA

How to forecast the future! In this talk we introduce a wide range of methods for predictive analytics based on social network analysis and the emerging science of collaboration. Our methods are based on analysis of large corpora of digital traces of human activity, in particular the Web, Blogs, online forums, social networking sites, e-mail archives, phone logs, and face-to-face interaction through using sociometric badges. Learn more about this kind of correlation was used by the CIA to forecast the election of the president in Iran.

## THURSDAY NIGHT - VIP CRUISE (MAY 12, 2011)

SCS3 invites you to the social event on the VIP cruise on the Lake of Zurich. A perfect opportunity for networking and in-depth discussions while enjoying a cozy ambiance. Enjoy the talks, the food and the view.



## THURSDAY SCHEDULE (MAY 12, 2011)

Latest version of the schedule: <http://www.swisscyberstorm.com/program/>

07:30-09:15	Registration Cyber Storm Briefings		
09:15-09:30	Welcome and Opening Remarks		
09:30-10:15	Keynote - Collective Intelligence - Prof. A. Gloor, MIT USA		
10:15-10:40	Coffee Break		
	Cyber Crime Track	Exploits & Defense Track	OWASP Track (Web Security)
10:40-11:25	Is Switzerland and Europe under Attack? Marc Henauer	Cracking Keyless Car Systems Srdjan Capkun	OWASP Initiatives and Strategy Antonio Fontes
11:30-12:15	How to beat a dragon with a shark Christiaan Beek	I Control Your Code - Attack Vectors Through the Eyes of Software-based Fault Isolation Mathias Payer	HTTP Parameter Pollution Marco Balduzzi
12:15-13:15	Lunch		
13:15-14:00	Hacker Profiling Project Raoul Chiesa	threats on your smartphone Celil Ünüver	Become fully aware of the potential dangers of ActiveX attacks Brian Mariani
14:05-14:50	Turning Security Latency into Competitive Advantage Darren Turnbull	Live Demo: Crypto Attacks Pascal Junod	Application Security as a Team Effort Jörg Ewald
14:50-15:20	Afternoon Tea		
15:20-16:05	Today's Criminal Groups in Cyberspace Mauro Vignati	Obfuscated Malcode Hunting with Emulator+Disassembler Lee Ling Chuan	HTML5 (In)Security Thomas Röthlisberger
16:10-17:00	Podium Discussion	Podium Discussion Cyber Crime Room	Podium Discussion Cyber Crime Room
18:30-23:00	VIP Cruise / Lake of Zurich Sponsored by Weingut Höcklistein (Schmidheiny)		

## FRIDAY SCHEDULE (MAY 13, 2011)

Latest version of the schedule: <http://www.swisscyberstorm.com/program/>

07:30-09:15	Registration Cyber Storm Briefings		
09:15-09:30	Welcome and Opening Remarks		
09:30-10:15	Keynote		
10:15-10:40	Coffee Break		
	Cyber Crime Track	Exploits & Defense Track	OWASP Track (Web Security)
10:40-11:25	Corporate IT Forensic Readiness Dr. Bruce Nikkel, UBS	PlugBot: Emergence of the Hardware Botnet Jeremiah Talamantes	Hunting Slowloris and Friends Christian Folini
11:30-12:15	Failure to Endpoint Security Stefan Frei, Secunia	IPv6 Security Testing & Tools Alaa Al-Din Al-Radhi	DomXSS identification and exploitation Stefano Di Paola
12:15-13:15	Lunch		
13:15-14:00	Cyber Warfare Prediction Daniel Ching Wa Ng - Hong Kong	Zeus MitMo: a real case of banking fraud through mobile phones Daniel L. Creus	Botnet Resistant Coding Peter Greko & Fabian Rothschild
14:05-14:50	Threats to eGov - APT Reto Inversini	Backtrack Germany - SE Advanced Dave Wollmann	Cookie Jacking - UI Redressing Rosario Valotta
14:50-15:20	Afternoon Tea		
15:20-16:05	European directives approaching data loss David Rosenthal	Exploiting SCADA Systems Jeremy Brown	Web Port Knocking Yiannis Pavlosoglou
16:10-16:55	Mobile Phone (In)Security Roger Blum & Marco Di Filippo	iPhone iOS Reverse Engineering Julien Bachmann	Strong Authentication in Web Application Sylvain Maret
17:00-17:15	Closing Ceremony Cyber Storm Briefings		

## CYBER CRIME SPEAKERS



**Christiaan Beek** - Principal Consultant - IR, Forensics, and Assessment McAfee Strategic Security at Foundstone Services EMEA, **Netherlands**

Chinese hackers stole sensitive intellectual property from energy companies for as long as four years using relatively unsophisticated intrusion methods in an operation dubbed „Night Dragon,“. Criminals aiming at companies and governments using customized malware to infiltrate, hide traffic and steal the information. How do they do that, how can you discover this kind of unwanted traffic on your network? Learn more about these true stories from Christiaan Beek - he will show up with insider investigator knowledge, samples and demo.



**Marc Henauer** - Fedpol/MELANI, **Switzerland**

Marc Henauer is the head of the section MELANI at the Swiss Federal Intelligence Service (NDB), in the department of defence, civil protection and sport (VBS). Before that, he worked as an analyst for economic and internet crime as well as being the department head at MELANI/KOBIK in the service for analysis and prevention (DAP). He studied economic science at the University of Zurich and moreover media and communication management at the University of St. Gallen. Marc achieved his MA in Foreign Service and National Security Studies at Georgetown University in Washington D.C.



**Dr. Bruce Nikkel** - Head of IT Investigation & Forensics at UBS AG, **Switzerland**

Corporate IT Forensic Readiness; This talk covers an introduction to IT forensic readiness in organizations, including demands and challenges faced, and strategies for implementing forensic readiness.

## CYBER CRIME SPEAKERS



**Raoul Chiesa** - (OPST, OPST, ISECOM Trainer) @ Mediaservice.net, Founder, Strategic Alliances, **Italy**

Auditing the Hacker's Mind : wrong myths, real facts and the Hackers Profiling Project (HPP): Since years we hear about hackers described as asocial, young criminals, while reading reports written by infrastructures commonly linked to Law Enforcement Agencies or mass-media. In the last 4 years the project analyzed more than 1.200 questionnaires, being able to build a profiling approach to the underground IT world. Learn more from the HPP leader about the social background of the so-called cyber criminals.



**Mauro Vignati** - Senior advisor at MELANI and PhD candidate in criminology, **Switzerland**

Modern Criminal Networks: Infrastructure and Tasks Segmentation of Today's Criminal Groups in Cyberspace. The speech will focus on the structure of modern cyberspace criminal groups, analysing the tasks distribution, the different steps in the chain of the criminal activity and pointing out similarities to and differences from the same kind of groups in the real world.



**Roger Blum** - Principal Consultant - Penetration Tester and Security Analyst for Compass Security AG, **Switzerland**

Hackers are adding telephone hacking into the arsenal of cyber crime methods. Rogers talk is about his research in the field of mobile phone network attacks, including fake GSM cells and trust we have into mobile phone technologies.

## CYBER CRIME SPEAKERS



**Darren Turnbull** - Vice President of Strategic Solutions at Fortinet, **UK**

Turning Security Latency into Competitive Advantage. Security is now the biggest cause of electronic trading latency. In his presentation, Darren Turnbull, Vice President of Strategic Solutions at Fortinet, will explain how security latency issues affect the trading community and go through the most important firewall requirements IT decision-makers should consider to radically reduce the security impact; increasing trading system performance and profitability. The presentation will feature real-world examples and is aimed at IT professionals at financial trading firms and investment banks.



**NG, CHING WA (Daniel)** - Daniel is a committee member HTCIA Asia Pacific, Chairperson of Professional Internet Security Professional (HK/China), Founder C-PISA, Director of ISACA China, and Expert Advisor to HKSAR Legco Councillor Samson Tam, ISC2 CSSLP evangelist and authorized trainer - **Hong Kong, PRC China**

This presentation introduces new models in knowledge management, like Cynefin framework, to identify new directions adopted by cyber criminal. He will introduce „Cloud-based Shared Mental Model for Cyber information warfare prediction“, with new focus on emerging electronics health records (eHR).



**Reto Inversini** - Federal Office of Information Technology, Systems and Telecommunication of the Swiss government as a Security Architect, **Switzerland**

Governmental organizations are exposed to various risks: some are well known and are affecting enterprises as well, some are specific to a government. The talk is going to highlight various aspects of these risks and appropriate technical and organizational countermeasures. Learn how to address Advanced Persistent Threats.

## CYBER CRIME SPEAKERS



**Stefan Frei** - Research Analyst Director @ Secunia **Danemark**

This talk is about „Fixing the fundamental failures of endpoint security: managing vulnerabilities when the perimeter protection failed“. As Research Analyst Director at Secunia Stefan currently studies the security ecosystem, investigate cybercrime operations, and analyze the data generated by Secunia Vulnerability Intelligence and Secunia Personal Software Inspector (PSI)



**David Rosenthal** - lic. iur. David Rosenthal for Homburger AG, **Switzerland**

Data breaches can hit every organization. When they happen, however, many businesses are struggling on how to react appropriately. David Rosenthal talks about what in particular data protection law requires businesses to do in such situations, what consequences they may face and which steps they can take before and after a data breach has occurred to put them in a better position. He will also address the data breach notification obligations that are now being introduced in various European laws.



**How to Rule the World** - Cyber Warfare

Train your Brain - Cyber Risks are a challenge for you and your business. Think about the future and how we rule the world. Take your time to get latest research results from our international speakers! A great opportunity for risk managers, security officers, security engineers and researchers!

## EXPLOIT & DEFENSE SPEAKERS



**Jeremy Brown** - SCADA Exploitation. **USA**

This presentation has something for security professionals, security researchers, ICS engineers, or anyone concerned about security issues affecting not just this nation, but electronic infrastructure around the world. I will be discussing different vulnerabilities in SCADA software, a real vendor response, other possible ones, as well as a live demo.



**Srdjan Capkun** - Srdjan Capkun is an Assistant Professor in the Department of Computer Science, ETH Zurich, **Switzerland**

He will demonstrate relay attacks on Passive Keyless Entry and Start (PKES) systems used in modern cars. We build two efficient and inexpensive attack realizations, wired and wireless physical-layer relays, that allow the attacker to enter and start a car by relaying messages between the car and the smart key.



**Celil Ünüver** - Security researcher at SignalSEC Inc., **Turkey**

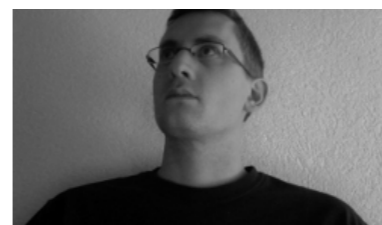
Bug hunting in windows mobile. My talk shows how to write shellcodes for windows mobile systems and the binary analysis of first windows mobile double free vulnerability. This vulnerability was discovered by me and published as a 0-day. At the conference I will demonstrate a 0-day attack to Windows Mobile system which can cause to freeze the device with a MMS. Additionally, my talk will cover the analysis of Zeus in The Mobile (symbian) and Terdial (wince) malwares.

## EXPLOIT & DEFENSE SPEAKERS



**Matthias Payer** - PhD student at the Swiss Federal Institute of Technology (ETH) Zurich, **Liechtenstein**

I Control Your Code - Attack Vectors Through the Eyes of Software-based Fault Isolation. This talk presents libdetox, an approach to the safe execution of applications based on software-based fault isolation and policy-based system call authorization. The talk briefly highlights the concepts of different attack vectors (stack-based/heap-based buffer overflows, return oriented programming, format string attacks, and other code-based attacks) and discusses how the virtualization system is able to detect and prevent a possible exploit.



**Pascal Junod** - professor of information security at HEIG-VD in Yverdon-les-Bains, **Switzerland**

In this talk, I will explain and demonstrate how to break cryptography-secured solutions in practice, even if they rely on seemingly strong algorithms and protocols. Several examples in real-life open-source products/protocols will be discussed. This talk will show active crypto attacks with live demonstrations.



**Lee Ling Chuan** - Senior Malware Analyst at Malware Research Center in Malaysia Computer Emergency Response Team, **Malaysia**

Obfuscated Malcode Hunting with Emulator and Disassembler. The emulator engine will first read the Entry Point (EP) of the virus code in identified binary file and located the decryptor – partial of the byte code decrypts the obfuscated virus body, determine the file type, length of the instruction with disassembler and lastly executed the result within emulator. Learn more from a Reverse Engineer!

## EXPLOIT & DEFENSE SPEAKERS



**Jeremiah Talamantes** - Managing Partner and Security Researcher for RedTeam Security Corporation, USA

Emergence of the Hardware Botnet. This talk will demonstrate the PlugBot interface and infrastructure and compare it with „traditional“ software botnets. We will explore what new threats the proliferation of hardware botnets present. Finally, I will provide suggestions and techniques for detecting and defeating hardware botnets.



**Alaa Al-Din Al-Radhi** - Ala'a Al-Din J. Kadhem Al-Radhi has a Bachelor degree in Electrical Engineering from the University of Baghdad and a Masters in Computer Information Network Security from DePaul University, Chicago. He has worked and trained in several countries and is currently based in Amman, Jordan

IPv6 has built-in IP security specifications which enable all traffic to be encrypted without the need for special hardware & hence IPv6 enables the creation of large-scale encrypted networks which are very resilient to cyber-attacks.



**Daniel L. Creus** - Daniel joined S21sec in 2008 as e-crime analyst, mainly involved in digital forensics and e-fraud research Security researcher at SignalS-EC Inc., Spain

ZeuS MitMo (Man in the Mobile). A real case of banking fraud through mobile phones! One of the techniques they use is the so-called MitMo attack, by means of which a malicious application is installed on the mobile phone to redirect communications and perform actions without the user's notice.

## EXPLOIT & DEFENSE SPEAKERS



**Dave Wollmann** - In 2008 I've become a moderator on the official Backtrack forums, 2009 I started the work as the community manager for the German Backtrack community and organized the Backtrack Day community events 2009 and 2010, Germany

Social Engineering is probably one of the most dangerous and neglected attack vectors in IT security. The talk will explain why Social Engineering is so dangerous, how it is working and how one can defend against it. In the past couple month the topic became more popular at least in the United States. But it is also a topic not only system administrators and pentesters should pay attention to but also every single person.



**Julien Bachmann** - Security Engineer @ SCRT Switzerland

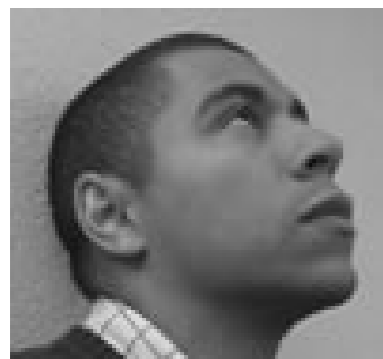
Reverse engineering iOS binaries . This presentation will introduce the iPhone architecture and the methods to reverse engineer iOS applications.



**Compass Security AG**  
Swiss Ethical Hacking & Penetration Testing Company  
Organizer of Swiss Cyber Storm 3 & Hacking-Lab

www.csnc.ch  
www.hacking-lab.com  
www.swisscyberstorm.com

## OWASP & WEB SECURITY SPEAKERS



**Antonio Fontes** - He leads the Geneva chapter and contributes in several reference projects such as the „CWE Top 25 most dangerous programming errors Switzerland

Do you OWASP? During this session, we will navigate through the most notable projects hosted by the OWASP, describe how organisations can benefit from them, and discuss about the ongoing initiatives that OWASP Switzerland has already established with both local companies and educational institutions



**Marco Balduzzi** - `embyte` Balduzzi, IT Security Specialist (freelancer) and PhD Researcher at EURECOM International Secure Systems Lab , Italy

HTTP Parameter Pollution Vulnerabilities in Web Applications. While input validation vulnerabilities such as XSS and SQL injection have been intensively studied, a new class of injection vulnerabilities called HTTP Parameter Pollution (HPP) has not received as much attention. HPP attacks consist of injecting encoded query string delimiters into other existing parameters. Learn more about HPP!



**Brian Mariani** - Senior Security Engineer at HIGH TECH BRIDGE based in Geneva World Trade Center, Switzerland

Exploiting ActiveX components vulnerabilities in Windows has become a favoured method of attackers aiming to compromise specific computers. Such targeted attacks have increasingly become a threat to companies and government agencies. This talk will explain this kind of attack and show how this flaw could be discovered while going through exploitation.

## OWASP & WEB SECURITY SPEAKERS



**Jörg Ewald** - Head of Product Management, Web Application Security at Ergon Informatik AG, Switzerland

There is very little interaction between individual web protection solutions. In this talk, we will investigate a more holistic approach, where applications, Web Application Firewalls and other components form a tightly coupled system, to markedly increase the overall security level.



**Thomas Röthlisberger** - Principal Consultant - Penetration Tester and Security Analyst for Compass Security AG, Switzerland

HTML5 introduces several new vulnerabilities. While in HTML 4.01 the attacks mainly focus the web servers, with HTML5 this boundary has moved towards the client. New HTML5 features enable possibilities for directly attacking the web browser and not all can be circumvented by secure implementation on the server side because some HTML5 features are the vulnerabilities itself.



**Dr. Christian Folini** - Contractor / Technical Consultant at netnea.com, Switzerland

Hunting Slowloris and Friends. On Practical Defense Against Application Layer DDoS Attacks that use Request Delaying Techniques. Network DDoS attacks are well known and widespread. Application level DDoS is a newer concept and it is more difficult to defend against. This talk gives some input on what happened when Swiss Post came under attack in December 2010 after closing the account of Wikileaks' Julian Assange.

## OWASP & WEB SECURITY SPEAKERS



**Peter Greko and Fabian Rothschild** - Fabian Rothschild is a Miami college student leading malware research for HackMiami and has presented his research on ZeuS for South Florida OWASP. He is a consultant for small and medium businesses providing best security practices for application development. He enjoys programming in Python and running Linux, **USA**

A guideline to mitigate and reduce the exposure of sensitive information from compromised clients through Zeus. Using a standard LAMP stack and web programming techniques, a guideline was developed to mitigate and reduce the exposure of sensitive information from compromised clients.



**Rosario Valotta** - Rosario Valotta is an IT professional with over 10 years experience. He has been actively finding vulnerabilities and exploits since 2007 and has released a bunch of advisories, **Italy**

Clickjacking attacks have been widely adopted by attackers worldwide on popular websites (eg Facebook) in order to perform some drive to download attacks, click forging, message sending and so on. He will show a new attack leveraging a UI redressing approach and allows an attacker to steal session cookies of from whatever site a victim is visiting. This new approach really moves UI redressing attacks a step further.



**Yiannis Pavlosoglou** - Member of the Application Security Advisory Board of (ISC)<sup>2</sup>. PhD in information security and is CISSP certified, **UK**

Single Packet Authorization (SPA) aims to provide an additional layer of security for services such as the Secure Shell. This presentation targets the applicability, as well as the hurdles crossed for implementing SPA on the authentication model of web applications. As a result, a new solution to hiding „admin“ type URLs, or only allowing for the existence of a user name and password field for a limited amount of time, will be discussed.

## OWASP & WEB SECURITY SPEAKERS



**Stefano Di Paola** - CTO and a cofounder of Minded Security, Research & Development Director of OWASP Italian Chapter, **Italy**

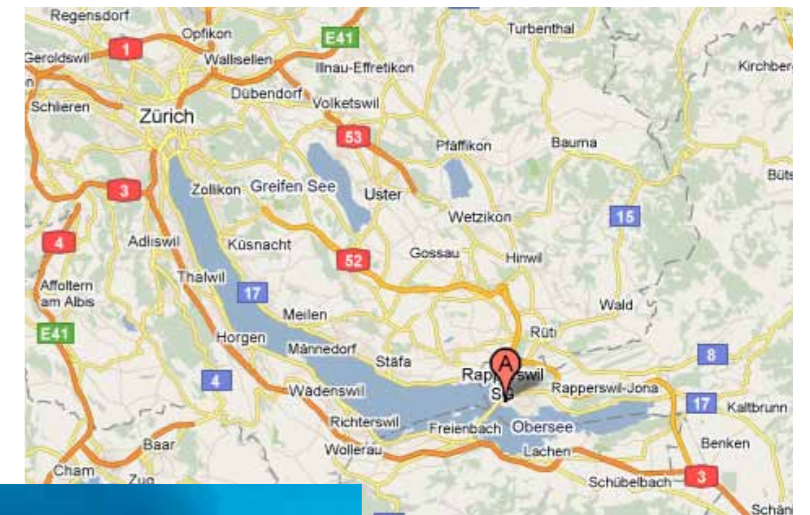
DOM based Cross Site Scripting. This is becoming more and more interesting in the application security field. The difference between vanilla Xss and the latter is hard to find among thousands of JavaScript lines of code. This talk will try to fill the emptiness of awareness about DOM Xss by showing new attacks, new analysis techniques and a new tool that is going to ease the pain of finding DOM based Cross Site Scripting issues.

## VENUE: UNIVERSITY OF APPLIED SCIENCE RAPPERSWIL 30 MINUTES FROM ZURICH (A)

**Rapperswil** - The conference will be held at the University of Applied Sciences in Rapperswil lakeside of Lake Zurich.

Take the S5 or S15 from Zürich mainstation to get to Rapperswil in 30 minutes.

<http://www.rapperswil-jona.ch>  
<http://www.hsr.ch>



## SPONSORS



### Fortinet

Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and a market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Visit: [www.fortinet.com](http://www.fortinet.com)



### Amag Retail Jona

Amag Jona is our CarGame Sponsor! The biggest car company in Switzerland, AMAG IMPORT is official Importer for Volkswagen, Audi, SEAT, Skoda, and VW commercials. AMAG RETAIL is with about 80 retail offices the biggest car dealer in Switzerland, selling the brands from the Volkswagen Group and Porsche.



### Winery Höcklistein

Enjoy the great local wine from the Höcklistein winery on the Lake of Zurich. We will be able to taste the great wine on our social tour!



### McAfee Security

Securing Your - Digital World™  
Industry-leading products, solutions, and technologies protect systems and networks around the globe. Visit: [www.mcafee.com](http://www.mcafee.com)



### High-Tech Bridge SA

High-Tech Bridge SA is a Geneva company exclusively dedicated to Ethical Hacking. Vendor independent approach and proprietary Security Research lab assure the highest quality of service. Visit: [www.htbridge.ch](http://www.htbridge.ch)



### University of Applied Sciences and Arts

Get your Master of Applied Science in Information Security. Educate yourself in a CAS or MAS. Visit: [www.hslu.ch](http://www.hslu.ch)

## SPONSORS



### Anti-Virus Security Solutions

100 Millionen clients world-wide trust in AVIRA security solutions. Our great team of security researchers is taking care of professional security and anti-virus update services day and night. We cover both local and global clients to support against the advanced persistent threats. Visit: [www.avira.com](http://www.avira.com)



### Ergon

Ergon stands for highly qualified IT specialists with a very clear focus on customer benefit. The company leads the field when it comes to developing custom applications, and it is an established manufacturer of software products. Solutions from Ergon give customers a real competitive edge. Visit: [www.ergon.ch](http://www.ergon.ch)



### ISACA Switzerland

As an independent, nonprofit, global association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. Visit: [www.isaca.ch](http://www.isaca.ch) / [www.itacs.ch](http://www.itacs.ch)



### TEMET

TEMET AG provides independent IT Security consultancy and is based in Zurich, Switzerland. Swiss financial institutions and federal authorities rely on our highly skilled and experienced consultants in the areas of IT Security architecture, IT Security management, and IT Security project delivery. For more information, visit our homepage on [www.temet.ch](http://www.temet.ch).



### DIGICOMP

With more than 650 course topics and eight central training locations, Digicomp is the leading IT education provider in Switzerland. In the security field Digicomp offers basic, advanced and preparation courses/workshops for international certifications like: CISSP, CISA, CISM, CEH, CHFI, ECSA. Visit: [www.digicomp.ch](http://www.digicomp.ch)

## CYBER STORM WARGAMES SATURDAY / SUNDAY



www.swisscyberstorm.com

20

„Wargame Disciplines“ – Do you feel like practising? Join one of the available hands-on sessions at Swiss Cyber Storm 3. If you have solved 3 out of 5 qualifying wargames (since November 2010), you can play for the VW Golf Blue Motion! If you missed the qualifying games and you are motivated to compare with others in a contest style challenge, go for the Defcon Challenge where you can win a Defcon 2011 ticket.

If you are a beginner or if you don't like contest games, join the Hack & Learn discipline. Educate yourself with the individual wargame challenges provided by Hacking-Lab.



## Available Challenges @ SCS3

CarGame Challenge	Defcon Challenge	Hack & Learn
+ WIN A NEW CAR!	+ WIN A TICKET TO DEFCON	+ Train your Brain
+ VW BLUE MOTION SPONSORED BY AMAG JONA	+ TRAVEL, HOTEL AND ENTRY SPONSORED BY MC AFEE	+ SMALL PRIZES TO WIN SPONSORED BY AVIRA
+ TEAMING ALLOWED	+ TEAMING ALLOWED	+ WARGAME CHALLENGES
+ QUALIFICATION REQUIRED	+ WITHOUT QUALIFICATION	+ LOCK PICKING
+ MAIN PRIZE OF SCS3	+ OPEN FOR EVERYONE	+ EDUCATE YOURSELF
+ GAME STYLE: CONTEST!	+ GAME STYLE: CONTEST	+ OPEN FOR EVERYONE

## CarGame Challenge WIN A NEW \$30'000 CAR !



**CarGame Challenge** – This is the most awarded and awesome discipline at SCS3. Players must have solved 3 out of 5 qualifying wargames since November 2010 until May 2011 to be allowed to play for the car when they are on-site. We have a large number of international participants who have played the qualifying online Hacking-Lab wargames in advance. During the week-end of SCS3, these guys will battle in the final and you as a visitor can profit from their knowledge because the winner team of a challenge must present its solution to the audience. This is part of the game!



### Meet the Geek

Do you want to meet best IT security experts? Join SCS3 and learn from their expertise. There will be time for socializing and networking, join the famous HackNight party to get in touch with the best talents in the IT security field!

www.swisscyberstorm.com

21

## Defcon Challenge



**Defcon Challenge** – Everybody is invited to play without prior qualification in advance as in the CarGame challenge. Form your team and play for a Defcon ticket to Las Vegas, sponsored by McAfee! Test your IT security skills and win the prize. This game is in contest style - has a team leader and team members. One person is only allowed to be in one team. Take the chance and test your skills.



## Hack&Learn Challenge

**Hack & Learn** – If you don't like „contest style“ wargames but you are still interested with hands-on labs in the field of IT security - join the Hack & Learn discipline. You can train your brain and you can solve different wargames and get support and help from our staff members. This discipline is ideal for beginners or students but also for intermediate and advanced geeks. But still, even this is not a classic contest, you can win an official 5-day CEH (Certified Ethical Hacker) training sponsored by Digicomp Switzerland! You can choose from a large variety of available wargames provided by Hacking-Lab.

- \* web hacking
- \* windows hacking
- \* vlan hacking
- \* pentesting
- \* reverse engineering
- \* cryptography
- \* unix security
- \* mobile devices

## HackNight Party - Saturday Night

After a long day with security puzzles, challenges and wargames, you can sit back and relax at the famous HackNight party in the centre of Rapperswil. The Ponte Lumi bar is hosting our party and the location is within walking distance from the University campus.



Let's party! Enjoy yourself and socialize with other participants. Additionally, make sure you gain some extra valuable information for the next day, including a CarGame advantage.

### Ticket 4-Day Pass

Normal	1190 CHF
Members	950 CHF
Cyber Tycoons	800 CHF
Students	750 CHF

<https://www.swisscyberstorm.com/register>

### Group Tickets (Reduction)

1-2 Participants*	Full Price
3-4 Participants*	10%
5-10 Participants*	15%
> 10 Participants*	20%

\* from the same company, institution, university

### Ticket 2-Day Pass (SAT/SUN)

Normal	150 CHF
Members	120 CHF
Cyber Tycoons	100 CHF
Students	95 CHF

<https://www.swisscyberstorm.com/register>



SCS3 Voting Device ( hardware hacking challenge ?! )



# Swiss Cyber Storm 3

---

Since the RSA breach and also before, I am convinced we live in a time where attackers are planting their warfare frameworks at random and well chosen targets world-wide. This is named as APT, advanced persistent threat.

There will never be a time like this, where getting access into foreign network is as easy as today. After years of new waves of gadgets, innovations and fully connectivity in the cloud, we have to step forward and zone our core assets into disconnected areas. We have to think about our assets, their sensitivity and impact in case of disclosure.

Its time to share and exchange our knowledge - it's time for Europe to take its responsibility. Let's meet at Swiss Cyber Storm 3!

Regards,

Ivan Bütler  
CEO Compass Security AG  
ivan.buetler@csnc.ch



Compass Security AG  
Werkstrasse 20  
P.O. Box 2038  
CH-8645 Jona - Switzerland

<http://www.csnc.ch>  
<http://www.swisscyberstorm.com>  
<http://www.hacking-lab.com>  
<http://www.cyber-tycoons.com>