iAWACS 2009 - List of Accepted papers and talks

- Xavier Carcelle - Security overview and vulnerabilities of PLC technologies
- Philippe Langlois & Eugene Parkinson - Fully-Automated Wireless Security Audit Platform on Embedded Hardware
- Leonardo Nve Egea - Playing in a Satellite environment 1.2
- Erwan Abgrall - Oracle: A new hop
- Mahmoud Maqableh & Stefan Dantchev - Cryptanalysis of Chaos-Based Hash Function (CBHF)
- Robert Erra & Eric Filiol – Processor-dependent malware
- Benjamin Caillat - WiShMaster - Windows Shellcode MASTERy... reloaded (tutorial with technical practice)
- Robert Erra & Christophe Grenier - How to chose RSA keys? (Past, Present and Future)
- Cédric Tavernier & Thomas Roche – Side-channel Attacks based on Linear Approximations (MPLA)
- Anthony Desnos – Organizer of the PWN2RM Challenge

Abstracts

Security overview and vulnerabilities of PLC technologies

Power Line Communications had been widely used for Home Networking applications mainly though the DSL services from the different ISPs, though are these technologies completely secure from the MAC/PHY layers point of view? This article aims at giving an overview of the security of current PLC technologies with an emphasis on Home Plug. Thus the article gives the different potential vulnerabilities at the PHY and MAC layers using description of the possible attacks with respectively hardware equipments and software current tools (FAIFA at the layer2). Finally this article will explain the limits of the current attacks possible on PLC and will give security advices to increase the level of security for such technologies.

Fully-Automated Wireless Security Audit Platform on Embedded Hardware

Have you ever imagined what a recalcitrant access point would look like? Well… neither do we. So we're going to show you what REAL love is all about. HostileWRT tends to make love to your antennas thanks to the 802.11 protocol suite. Then, sharing the love is more than natural. No wonder then that HostileWRT, despite its very blackhat touch, is the most desirable item in one's sado-(techno)-masochist outfit. Computer and network security professionals are

confronted on a daily basis with the issues of testing the reality of perceived problems and suggesting fixes with high applicability potential. Such issues are particularly difficult in wireless environments since the measures are not of binary nature but depend on the capacity to detect effectively WiFi networks, access points and other radio equipments. There is always the chance of missing a radio equipment or not having good and accurate measurements. We propose in this paper to automate several critical parts of the wireless network security audit using pervasive and inexpensive platforms and thus to free more time to focus on the applicability of the fix, and even the verification of the application of the Fix. HostileWRT aims at automating scanning and cracking in wireless environment and improving results using different behaviours depending on the goal of the auditor. By using a hostile approach, we want to prove that it's not possible to fully audit a wireless environment without taking in account the several different kinds of vulnerabilities that affect both the infrastructure and the end-users.

Playing in a Satellite environment 1.2

This presentation is a warning call to those responsible for the companies that use or provide data connection (especially the Internet) via satellite, proving some of the attacks that are possible in this environment.

The presentation outline is:

- Insecurity in Satellite communications.
- Malicious Active Attacks
- Getting an anonymous connection
- Conclusions

The attendees will learn how insecure satellite connections are and why they need a more secure platform for this environment or how we must use secured protocols if we have this technology hired. Also, they will learn how these attacks can be made, including how to get an anonymous satellite connection. Previously satellite presentations exist, but these are focused only in feeds capturing and a bit in sniffing data, treating this as a passive vulnerability. I focused my presentation in the active attacks someone can make to the clients and ISP. This presentation is focused for a high technical attendees. Nowadays this presentation has not been previously presented.

Oracle : A new hop

Gaining access to a SQL back-end is often considered as the last move in a webapp pen-test. Nowadays SQL back-ends offers more functions than traditional data storage. Thanks to the web services hype, databases are no longer pushed in the back of the IT infrastructure in a locked up DMZ, but became a full interconnection node between IT services. Databases should no

longer be considered as the last point, but as a step-stone to go further inside networks.

We will see how an attacker, starting with a simple SQL injection can quickly turn an Oracle database into an Http proxy, and what can ease the process. From this, we will draw a picture of the potentials incoming threats and how prevent them.

Cryptanalysis of Chaos-Based Hash Function (CBHF)

Recently, M. Amin et al. suggested a new hash function based on chaos theory for cryptography applications. In this note, we will analysis security of the proposed chaos-based hash function CBHF. The analysis shows how to break both keyed and unkeyed versions of the CBHF.

Processor-dependent malware

Malware usually target computers according to their Operating system. Thus we have Windows malware, Linux malware… In this paper, we consider a different approach and show on a technical basis how easily malware can recognize target system according to the onboard processor chip. This technology is very easy to build since it does not rely on deep analysis of chip logical gates architecture. We give extended results for different families of processors: AMD, Intel, Sparc, Digital Alpha, Cell, Atom…

WiShMaster - Windows Shellcode MASTERy... reloaded (tutorial with technical practice)

Objectives of this tutorial:

- *To describe the concept of shellcode*
- *To explain the structure of a shellcode for Windows*
- *To present the new version of WiShMaster, a tool that generates shellcodes for Windows from C code*
- *Understand how to use WiShMaster by writing a few small projects*

Malicious codes often need to manipulate their own code in order to implement some viral techniques, like executable infections, memory-only execution or polymorphism. Such manipulations are considerably simplified if the program is a shellcode. There are a few solutions to obtain a shellcode: one is to write source code in assembly, but it quickly becomes a boring work. Another is to write source code in C language in a specific way, so that compiled code doesn't contain any hardcoded address. However, writing C code like this is very boring too, and it quickly becomes obvious that the use of an automatic tool that generates "specific" code from "normal" code is indispensable. WiShMaster is a tool that converts a set of C source files written almost "normally" (the compilation of those source files produces an executable) and generates a shellcode, that is a block of code without any hardcoded or external reference and that can run in any process at any address. If the execution is redirected to its first byte, the shellcode will accomplish exactly the same operation as the executable generated through normal sources compilation.

The aim of this tutorial is to describe the principle of this transformation – called "shellcodisation" and to show with a few practical examples how WiShMaster can be used to create some malicious codes.

Part 1: The use of shellcodisation in virology
Part 2: Definition of a shellcode; writing shellcode for Windows
Part 3: Description of the shellcodisation process
Part 4: Using WiShMaster to create a first shellcode: a reverse connect backdoor
Part 5: Developing applications with WiShMaster
Part 6: First malicious code: creating a Trojan with a reverse connect backdoor (encoding, executable infection)
Part 7: Second malicious code: writing a tool to spy the emails of an infected computer (code injection, API hooking)

A computer laboratory will be available for the tutorial. Anyway, if attendees wish to come with their own laptop (be careful: no Internet connection will be available during the tutorial), here are the configuration requirement.

Platform required for the manipulations:
- Windows XP SP2/SP3
- Python (http://www.python.org/download/)
- OllyDbg v1.10 (http://www.ollydbg.de/odbg110.zip)
- Nasm Win32 binaries (http://sourceforge.net/project/showfiles.php?group_id=6208)
- Netcat (http://joncraton.org/files/nc111nt.zip)
- Microsoft compiler: Visual C++ Express edition 2008 (http://msdn.microsoft.com/frfr/express/default.aspx)
- Latest Microsoft SDK (http://www.microsoft.com/downloads/details.aspx?FamilyId=A55B6B43-E24F-4EA3-A93E-40C0EC4F68E5&displaylang=en)

Warning= This tutorial is intended to give a background in computer security with respect to shellcode for a better understanding about this threat and a better proactive protection. A commitment of responsibility form will have to be signed by each attendee in order to ensure that no prohibited use will be done of the materials presented. The organizers reserve themselves the right to restrict the access to this tutorial at any moment.

How to chose RSA keys? (Past, Present and Future)

The RSA algorithm is without doubt the most famous asymmetric cryptosystem. It is used in a lot of commercial (military or not) and non commercial tools. But how does someone compute his RSA key? Generally, one simply "asks" to a software a RSA key by specifying (for example) the binary length. And you trust the results, of course. But, recently, Luciano Bello has proved that this can be dangerous. He has explained that, because of a single line of "miscommented" code, since September 2006 the RSA key generated by a Debian are not random but rather highly predictable.

So, when you compute RSA keys, how can you be sure that it is "secure" (whatever it means)? In fact you cannot be sure.
There are a lot of other examples that proves this statement. For example, an RSA can get older, i.e. unsafe, so, if you chose a RSA key of 1024 bits, this is a reasonable choice today but, will it be a good idea to have such a 1024 bits in 5 years?

We propose to present:

- *a review of some vulnerabilities and attacks;*
- *a brief description of the tools that one can use to attack a RSA key, from the user point of view.*

Side-channel Attacks based on Linear Approximations (MPLA)

Power analysis attacks against embedded secret key cryptosystems have widely studied since the seminal paper of Paul C. Kocher, Joshua Jaffe and Benjamin Jun in 1998 where has been introduced the powerful Differential Power Analysis. The strength of DPA is such that it became necessary to develop sound and efficient countermeasures. Nowadays embedded cryptographic primitives usually integrate one or several of these countermeasures (e.g. masking techniques, asynchronous designs, balanced dynamic dual-rail gates designs, noise adding, power consumption smoothing, etc. ...). This document presents new power analysis attacks based on linear approximations of the target cipher. This new type of attacks have several advantages compared to classical DPA-like attacks: first they can use multiple intermediate values by query (i.e. power trace) allowing to reduce data complexity to a minimum, secondly they can be applied on parts of the symmetric cipher that are practically unreachable by DPA-like attacks and finally they can be mounted on an unknown cipher implementation. Experiments on real power measurement traces from a DES hardware implementation prove the practical feasibility of the attack.

The PWN2RM Challenge

This challenge consists in removing and cancelling "on the fly" the protections deployed by a few antivirus software to protect the system and defend itself against the malware attacks. The target system will be Windows. The aim is to run a known malware (usually easily detected by the antivirus software) to prove that the removal is successful and hence the antivirus is no longer active.

This challenge intends to show on an operational basis how any antivirus can be inefficient at protecting itself and thus the host system. This is somehow an "on the fly" evaluation. The security target will that of Windows used with admin right – in other words more than 90 % of the user way of using Windows.

For that challenge, the computer (one per competitor) will configured as follows:

- *Windows XP*
- *Admin rights enabled (user with rights)*
- *Internet access active*

We have chosen to evaluate the main antivirus software which relentlessly claim

to be the best ones and protect your computer. They are also those you are certified with any five stars labels or other golden award and therefore trust all the first places of antivirus classification:

- *Norton from Symantec*
- *McAfee*
- *Kaspersky Antivirus*
- *Dr Web*
- *Nod 32*
- *GDATA*

Rules of the challenge:

- *You must register before the conference (send an email to iawacs2009_orga@esiea.fr)*
- *You will have a total time slot of 1 hour.*
- *The attack is successful as soon as the antivirus process is still present (active) AND the usually known malware can be run without triggering any AV alert (the ESIEA team will act as success verifier and consequently no member of ESIEA is allowed to take part to the challenge).*
- *No system reboot is allowed.*
- *Removing or deactivating the antivirus by any classical means is not allowed.*

The winner is who manage to bypass most antivirus in the shortest time. Price and wards will be published later. Technical reports will be sent to the AV vendors for feedback.

Bios

Xavier Carcelle.- Xavier Carcelle is senior telecommunication expert for PLC network applications. He is a member of the telecommunications standard group IEEE P1901. He is author of a previous book and several published papers on power line communications and has been a guest lecturer on the topic. He received his M.S. from Ecole Normale Supérieure in France and Texas A&M University.

Philippe Langlois.- Founder of P1 Security and Senior Security Consultant for Telecom Security Task Force. Philippe Langlois has proven expertise in network security. He founded and led technical teams in several security companies (Qualys, WaveSecurity, INTRINsec) as well as security research teams (Solsoft, TSTF). He founded Qualys and led the world-leading vulnerability assessment service. He founded a pioneering network security company Intrinsec in 1995 in France, as well as Worldnet, France's first public Internet service provider, in 1993. Philippe was also lead designer for Payline, one of the first e-commerce payment gateways. He has written and translated security books, including some of the earliest references in the field of computer security, and has been giving speeches on network security since 1995 (RSA, COMDEX, Interop, HITB Dubai, Hack.lu).

Eugene Parkinson (/tmp/lab).- Embedded developper, wireless pioneer and expert, toolchain master. Eugene combines talents and style in a very discreet yet powerful human being. Eugene has been notorious for his machine-like capabilities, pushing the limits of marathon coding and related activities to dimensions never envisionned before.

Leonardo Nve Egea.- Senior security auditor and trainer interested in computer security since 1996,working as consultant and auditor from 2000, 2002.

I managed several researches on various security technologies such as DOCSIS and Wireless, with various papers published in various Spanish specialized publications. Also I managed the UnderCON, the first Spanish underground security congress, where I presented the first full-ASCII Shellcode in 2000, other talks was about wifi and phone companies security.

Erwan Abgrall.- Erwan Abgrall is a Security engineer working at KEREVAL, an independent French software testing laboratory, composed of enthusiasts testing experts specialized in IT, embedded systems and security.

Mahmoud Maqableh.- Mahmoud Maqableh received the B.Sc. degree in Computer Science from the Al Al-Bayt University, Jordan, in 2004. He obtained his M.Sc. degree in Computer Science from University Sains Malaysia, Malaysia in 2006. Currently he is doing his Ph.D. in School of Engineering and Computing Sciences at Durham University – UK. His research interests in the field of Cryptanalysis, Cryptography, and E-Business Security.

Stefan Dantchev: Originally from Bulgaria. MSc in CS from Sofia University (Bulgaria) in 1994, PhD in CS from Aarhus University (Denmark) in 2002. Lecturer in CS at Durham since 2004. Interested in Theoretical Computer Science (Algorithms and Computational Complexity) in general and in Propositional Proof Complexity in particular.

Robert Erra.- Robert ERRA is Professor of Computer Science at ESIEA and the Head of the Specialized Masters "Network and Information Security". He is interested in computational number theory and cryptography.

Eric Filiol.- Eric Filiol is head of the Operational Cryptology and Virology Lab at ESIEA.

Benjamin Caillat.- Benjamin Caillat is a teacher in the specialized master in IT security of ESIEA, a French engineering school. He started a PhD in September 2008 on "the study of backdoors usage in targeted attacks of companies" in the IT security research laboratory of esiea.

Publications:

- SSTIC 2005 (French conference): Compromise the information system of companies through its employees

- Manager of the Challenge-SecuriTech in 2005 and 2006, a French security contest
- Article about developing advanced backdoors for Windows in MISC 2008, a French IT security magazine
- Member of the organization committee of SSTIC 2009
- Black Hat Europe 2009: WiShMaster, Windows Shellcode Mastery

Christophe Grenier.- Christophe GRENIER has finished his master in Computer Science at Université de Rennes and is doing a Phd in Computer Science.

Anthony Desnos.- Anthony Desnos is an ESIEA PhD student (SI&S team). He is an active contributor to many major security project like Eresi, Elfsh… He is a Python and Lua addict and speaks quite fluently Linux system.

Cédric Tavernier.- C. Tavernier has received his Phd thesis in 2004 from Ecole Polytechnique , France. He works actually for the company "Communication and Systems". His research topics are related to coding theory and its application to cryptography. For more information, refer to http://ced.tavernier.free.fr/

Thomas Roche.- Thomas Roche is a phd candidate shared between the "Informatics Laboratory of Grenoble" under the supervision of Roland Gillard and Jean-Louis Roch, and the company "Communication and Systems" under the supervision of Jean-Michel Tenkes. Thomas Roche received a master degree and engineer degree from the French engineer school of computer sciences and applied mathematics ENSIMAG, Grenoble en 2006.