Pierre Pronchery

IT-Security Consultant

Gubener Straße 40, 10243 Berlin, Germany

Mobile: +49 (0)177 472 7481

pierre.pronchery@duekin.com

Background

Pierre Pronchery has been consulting as an IT-Security specialist for over five years now. Initially hired as a Senior Solutions Consultant at n.runs AG, he then set off to conduct projects as a freelance worker during the past three years, known as DUEKIN Consulting. He is also a co-founder and partner of loopb-ack GbR, a team of independent Security Consultants, which has allowed him to be part of larger and longer projects in spite of his status as a freelancer.

Before dedicating himself to Security, Pierre Pronchery was studying Computer Science in French and British universities and engineering schools, obtaining a Bachelor of Computer Science from Oxford Brookes University in 2003. Focusing on system programming, network architecture and systems administration, he keeps renewing and completing his skill set through his involvement in the Open Source community, and the development of his own Operating System.

Constantly following the state of the art of Operating System and networking design, Pierre Pronchery has always proven a key asset on any of his projects as a Security Consultant. This is the consequence of a broader culture and understanding of software and protocol architecture and designs, as well as the ability to develop relevant software on the spot. As a confirmed programmer, he was regularly able to identify the weaker aspects of his targets while planning respective audits, be it while assessing source code or reverse-engineering binary information.

His creative and communicative mindset has driven him to organize, deliver speeches or host workshops at a number of international conferences. Convinced that both sides are better improved well aware of the other, he was either detailing methodology as an attacker, or how to write better software in the first place. As much at ease orally or when writing, he praises reporting and presentation quality just as much as coding style.

Expertise

Security Consulting

- **Source code auditor**
  At ease reading thousands of lines of code per day, particularly during the analysis of C or PHP code bases; also able to concentrate on Assembly, C++ and Java, learning additional languages deeply is always a possibility.

- **Reverse-engineer**
  Typical scenarios, involving limited knowledge about the task and target, are a challenging and rewarding task; mostly encountering off-line firmware and protocol dumps so far, more elaborate forensics are not too far apart.

- **Penetration tester**
  Assessing and intruding live systems is perhaps the most known and envied aspect of this profession, yet best conducted with caution and methodology; understanding the relationships between the relevant parts of computer and networks architecture, as well as the mindset of developers and attackers alike, the ability to break into systems and rate their exposure is just a natural consequence.

Software engineer

- **System developer**
  Writing portable, networked, low-level system software, including some kernel-level tasks, although concentrating on UNIX platforms (Linux, *BSD, Solaris...)

- **Graphical interfaces**
  As a C/Gtk+ expert, native end-user applications are preferred, again with a strong bias for UNIX; either Web-based applications or the SDL/OpenGL framework are well-known and handled as well.

- **General guidance**
  Experience is gladly transferred through documentation, tutorials, workshops or seminars, during which Embedded Linux development was exposed a number of times already.

Experience

Freelance Security Consultant and Developer, DUEKIN Consulting
Co-founder and associate, loopb-ack GbR

Since October 2007 and February 2010, respectively

Performing Security audits regularly, together with occasional software projects and Research & Development consulting and activities. Most notably advocated the usage and development of Open Source hardware Europe-wide, together with Bearstech (French hosting company). This included the shipment of a Linux-based software distribution for the Openmoko Freerunner (hackable:1), along with the delivery of speeches and workshops at major conferences (CCC, GSMA, LinuxTag, CELF...).

Security audits are performed independently and as part of loopb-ack GbR alternatively. The latter was created together with another couple of independent consultants, allowing us to deliver longer-term projects and continuous service to customers, while also transferring practical knowledge and infrastructure costs.

Senior Solutions Consultant, n.runs AG

From February 2006 to May 2007

Conducted a number of Security projects internationally, usually working in pair together with another in-house consultant. The assignments were numerous and varied, ranging from network penetration-tests to reverse-engineering and source code audits. Environments included major hardware and software development companies, international banks, telecommunication providers, as well as some remote assignments.

Project selection

Building a security team at VZnet Networks, Ltd

Consulting independently for this company highlighted some key requirements in its organization, eventually leading to the creation of loopback GbR with another couple of consultants helping there. Its first assignment was to confirm and establish company-wide security processes, hiring and training an internal dedicated team in the process. This was performed successfully within three months.

Acknowledgments on http://www.meinvz.net/l/security/10/

DeforaOS, an Operating System project

Initially a derivative of the Debian GNU/Linux distribution, deeper changes and experiments have turned the DeforaOS project into a LFS-based (Linux From Scratch) and then fully self-hosted project. While currently relying on existing kernel technology (NetBSD and Linux), major parts of the system were completed already (libc, graphical desktop environment), with other components well in the works (distributed framework, compiler...). The aim is to provide a more secure alternative to the aging Operating Systems mostly used today, ultimately fulfilling the ever-growing mobile needs of modern users.

Found on http://www.defora.org/

### UWfirmforce, an offline reverse-engineering tool

First presented during the 0sec and 23C3 public conferences, this tool greatly assists auditors during the analysis of offline firmware images. Its principle is to identify well-known binary signatures for typical content of firmware images, along with a probability of the actual presence of relevant data. It is notably being used by the GPL Violations project.

Found on http://www.uberwall.org/

DeforaOS Phone, GSM telephony with security features

This application is meant to be used on actual phones, where it is handling the internal communication with the actual modem, managing phone calls, contacts and messages through a graphical interface based on Gtk+. It is best found as part of the embedded variant of the desktop environment developed within DeforaOS. It is completed with security features, including an encryption solution for SMS messages.
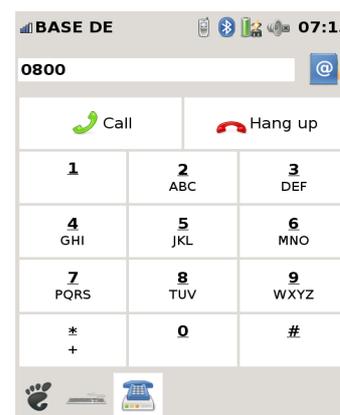
It was packaged and integrated for the Openmoko Freerunner phone in particular, which is one of the only Open Source hardware phones available today. It is currently being adapted for use with the OsmocomBB project, for a 100% Open Source, transparent yet user-friendly GSM telephony solution.

Also found on http://www.hackable1.org/