



# 2009

# ApriorIT

## Research & Development

Driver Development Team .....	2
Year Tech Summary .....	2
Main work directions: Virtualization is the whole show .....	2
Organizational issues: Learn and teach .....	2
Network Security Team .....	3
Year Tech Summary .....	3
Main work directions: Going wider and deeper .....	3
Organizational issues: Estimation before, during and after .....	3
Device Team .....	4
Year Tech Summary .....	4
Main work directions: Let them speak to each other .....	4
Organizational issues: Let us speak to each other .....	4

## Research & Testing

Driver Testing Team .....	5
Year Tech Summary .....	5
Main work directions: Taste of virtual reality .....	5
Organizational issues: Minimize time, maximize results .....	5
Network Testing Team .....	6
Year Tech Summary .....	6
Main work directions: Pushing the envelope .....	6
Organizational issues: From theory to practice .....	6

# Research & Development

## Driver Development Team

### Year Tech Summary

**Main Languages:** C++, ASM, Cocoa, Objective C, AutoIT, NSIS.

**Main Platforms:** Windows x64, x86; Linux, MacOS.

### Main Technologies:

- *libraries:* MFC, ATL, STL, Boost, LZMA, GoogleTest, Ogg, Vorbis, Mhook, QT, AppInit DLLs;
- *technologies:* Windows kernel mode drivers, Thin Client, Terminal services, VDI (Virtual Desktop Infrastructure), development on BIOS level, BootLoader development, TWAIN, COM, RPC, Code signing, Bochs;
- *tools:* VMware, Hyper-V, ActiveX CAB Packages, Audio Compression Manager (ACM), DirectShow, PREfast, Remote Desktop Addins, iSCSI, WMI, Windows CE.

### New knowledge & experience:

Thin Client, BootLoader, ActiveX, Boost, LZMA, TWAIN, Code signing; PREfast, ActiveX CAB Packages, Audio Compression Manager (ACM), GoogleTest, Windows Terminal Server (WTS), iSCSI, WMI, Hyper-V, Windows CE, monikers.

### Main work directions: Virtualization is the whole show

Dominating work direction in 2009 has been Virtualization solutions and Remote Access.

We had interesting tasks concerning multimedia in terminal sessions, improving user experience in working with remote devices: scanners, printers, etc. Significant research activities were performed in VDI (Virtual Desktop Infrastructure) and Hypervisor fields.

In 2009, the number of projects for Linux and MacOS increased. Our development activities embraced products for Mac and iPhone, thus we performed intensive research in Objective C and Cocoa.

Using Boot Loading technique team succeeded much in projects hardly connected with Windows system internals and advanced interaction with x86 architecture.

Being engaged into the projects with deep system integration, team specialists used and improved their skills of Reverse Engineering, including concentrated experience exchange with Reverse Engineers from other teams.

### Organizational issues: Learn and teach

Because of increased number of new projects and also junior specialists the new scheme of tutoring and project control was introduced and deployed. This system made it possible for senior developers to share their knowledge by directly taking part in the projects and lending support to juniors, or controlling their project process and results externally.

# Research & Development

## Network Security Team

### Year Tech Summary

**Main languages & dev tools:** C++, Visual Studio 2008; SQL: MySql, FirebirdSql, SQL; IncrediBuild.

**Main platforms:** Windows Vista, Windows 7, x64 support, UAC support.

**Main technologies & techniques:** work with Firebird API, Windows Crypto API; WiX, CryptoPP lib; RPC, Networking, Windows networking, Network collaboration; TDI and WSK filters; file system filter driver; devices blocking; AIM parsing support; dynamic disks; reverse engineering; development of extremely light-weight applications without CRT.

### New knowledge & experience:

MAPI monitoring, keyboard activity monitoring from the driver, work with dynamic disks, Windows USB architecture; data formats for monitoring purposes: Firefox, Skype 4, ICQ 6; WEB technologies: ASP.NET, jQuery, LINQ, .NET Framework 3.5, Javascript, CSS; custom physical device development.

### Main work directions: Going wider and deeper

As usual, main work direction for Network Security team is to monitor users' activity in the corporate networks of different architectures and provide maximal access to the data in the network for security purposes. These two points transform into a number of different tasks including those sliding at the technology cutting edge.

A number of new data formats were researched to provide effective monitoring of the corresponding information as well as some database structures including but not limited to Firebird, SQL. Interesting task was to implement distributed search in large networks by hash codes and other attributes.

Tasks of providing access included sparse & compressed file acquisition, remote access to the network disks and specific files, mounting and acquisition of dynamic disks. Besides the advanced development work, our specialists were also engaged into intensive research process with different reverse engineering techniques used.

To make corporate security tool really effective the accent was made on designing and developing scalable network systems, work in kernel mode, developing high-performance applications without CRT using boot agent technique.

### Organizational issues: Estimation before, during and after

As far as the proper estimation is one of the keys to the success of both huge long-term and small advanced projects, much attention was paid to this process in 2009.

Intensive technology modernization enforces appearance of increasing number of small and middle-size project tasks of high priority. It becomes vitally important to manage time for them properly. Managers of Network Security team improved their estimation skills and deployed some new tools and approaches to plan and control projects. One of them was Earned Value Analysis (EVA) now performed for all projects at all stages to control plan adherence, on-going performance and final estimation.

# Research & Development

## Device Team

### Year Tech Summary

**Main languages & dev tools:** C++, Java, WiX; autobuild system with parametric builds; advanced tools for IDA Pro.

**Main platforms:** a number of mobile platforms, Android, iPhone; Windows x32, x64.

**Main technologies:** QT, MFC, ATL/WTL; databases: MS SQL, Firebird, SQLite; Windows Installer; software protection: WinLicense, Dongle; pipes, sockets; custom serialization; FAT, USB, FreeRTOS driver patching; service development; reverse engineering and software research; test driven development.

### New knowledge & experience:

QT technology, GDI+, Java API for Android, Google Maps API; SyncML protocol; MMC 2.0 console; LPS; development of large distributed systems, Windows hooks methods; peripheral device detection methods; driver digital signing; software for embedded systems with AVR32, FreeRTOS; ELF data format.

### Main work directions: Let them speak to each other

In 2009, just as usual, tasks for Device Team mainly concerned computer-device interaction and acquiring and representing data from mobile devices.

Advanced tasks arose from both sides, computer and device. For example, the team got acquainted with different Windows hooks methods: windows messages, process hook, mouse and keyboard hooks; and also researched deeply the different methods of device detection, such as window and service messages, device enumerations, rapi notifications. Obtained experience in device detection transformed into the autonomous library that now is used in a number of projects. The practice of representing experience in the libraries and their further improvement lets the team work effectively and produce high-quality code in short terms.

We also faced with some interesting tasks from accompanying development area. Thus significant research of Windows Installer was performed to create advanced driver installations, simultaneous installations, performing correct installation for both x32 and x64 platforms. Much attention was paid to the software protection techniques.

### Organizational issues: Let us speak to each other

This year team specialists took part in several common projects with specialists from other teams. Such joint work enforced knowledge sharing and had a profound effect on team improvement.

Also the team provided lecturers for student courses of advanced software development and produced articles for external and internal portals with the results of research and experience representation. These activities are good for shaping experience we have and also for proper knowledge management.

Several improvements were made for the task distribution process and support & development work estimation. They let the team meet the terms more accurately and keep balance in different work types.

# Research & Testing

## Driver Testing Team

### Year Tech Summary

**Main platforms:** Windows w2k –w7 (x32/x64), Windows Server 2003/2008(x32/x64), MacOS, Linux.

**Main tools:** VMware; Windows Shell Scripts, AutoIT; Process explorer, TCPView, SmartSniff, KernRate, BWMeter, AdvancedPortScanner, Nmap, Everest, Perfmon, download managers (FlashGot), NetLimiter, FileZilla.

**Main technologies:** manual functional testing; automatic stress testing, automatic load testing; configuration testing; GUI testing incl. accordance to Microsoft standard.

### New knowledge & experience:

WAN emulation, RDP work research, Active Directory in Windows; IIS, Terminal Server, Load balancer, Session directory.

### Main work directions: Taste of virtual reality

In 2009, the team's main activity concerned creation and execution of test plans for virtualization products.

One of the most useful tools was VMware. Using virtual machines, our QA specialists managed to improve and enforce all testing processes and also engage them in some new activities such as two-display testing and extremely quick configuration testing.

Performing load testing our specialists got acquainted with a number of different utilities for measuring of traffic and OS load.

The important thing for client-server application testing was WAN emulation and so necessary experience was obtained. At the moment our testers can deploy emulated WAN in several ways: emulated WAN based on Linux, FreeBSD, by means of third-party applications (TMnetsim).

A lot of time was spent on the research tasks, mainly devoted to the OS features exploring, Windows and Linux administrating.

### Organizational issues: Minimize time, maximize results

QA specialists of Driver testing team permanently search the new ways to improve their knowledge and work. Thus the new methods were tried out, in particular to minimize test sets and make them maximally effective. We monitored and visited professional trainings to stay informed about all new approaches and requirements appeared in SQA field.

A number of interesting articles was written in our team for both internal and external publication. They helped knowledge formalization and sharing as well as were used in Intern teaching process.

# Research & Testing

## Network Testing Team

### Year Tech Summary

**Main platforms:** Windows, Linux, mobile platforms: WinCE 5.x-9.x, Symbian OS 6.x-9.x, Android 1.0.

**Main technologies:** manual & automatic (Test Complete) all-round testing, exploratory testing.

### New knowledge & experience:

Usability testing; testing with Exchange Server on both real and virtual machines; testing on the brand-new physical devices.

### Main work directions: Pushing the envelope

This year the usability training courses were conducted for our specialists. It made it possible to include this type of testing in our usual testing routine for all projects.

We started to use exploratory testing more intensively as far as this type of testing works good in situation of shortage of resources and time. Thus we managed to cover all our projects with acceptable testing volume.

Also Linux trainings were performed for the team, and after them we was able to effectively work with Linux applications, create and execute test plans for them. Such communication also gave us interesting and useful knowledge of different software and development features to help in every-day testing.

During 2009, we enforced communication between our testers and specialists of Device team. Thus we obtained necessary experience to work with brand-new physical devices (mobile phones, smartphones, palms) and perform testing with them.

### Organizational issues: From theory to practice

Another successful round of courses of software testing for students was conducted this year by specialists of our team. We changed the format of teaching from lecture style to the training style. Thus we gave students much more practical knowledge that could help them from their first days of the real tester work.