Section A

1. Alexander Tereshkin
3. alexander@coseinc.com
4. COSEINC
5. Alex Tereshkin is an experienced reverse engineer and an expert into UEFI security, Windows® kernel and hardware virtualization, specializing in rootkit technology and kernel exploitation. He has been involved in BIOS and SMM security research since 2008. He has done significant work in the field of virtualization based malware and Windows® kernel security. He is a co-author of a few courses taught at major security conferences. Alex holds the Russian equivalent of a Master's Degree in Applied Mathematics, and also the Russian equivalent of a PhD degree in Information Security from Southern Federal University.
6.

Section B

1. SMM Rootkits
2. This course is for people who want to find out more information about the most privileged and mysterious operating mode of x86 processors: System Management Mode. You will learn what it actually is, how to get there and what can be done by an attacker once his code is executed in SMM. Are there SMM rootkits in the wild? How feasible it is to create such rootkit? Can a kernel mode antivirus or a hypervisor protect against attacks from SMM? Can SMM rootkit be detected using memory forensics? Can you put an ultimate antivirus in SMM to fight SMM and kernel mode rootkits? We will cover these topics in much detail.

   There will be many lab exercises which will help you to better understand the ideas and techniques. By the end of the course you will have a good understanding of SMM security principles. You will also have a hands-on experience with implementing and detecting SMM rootkits.
3.
   a. Student prerequisite
      i. C system programming experience
      ii. Basic knowledge of x86 architecture
      iii. Experience with UEFI is an advantage
      iv. Understanding x86-64 assembly is an advantage
   b. Hardware prerequisite
      i. A laptop with Intel 64bit i3 CPU or higher. Hardware virtualization support (VMX) is required. Make sure it is enabled in BIOS.
      ii. At least 4GB RAM
      iii. 30GB free disk space
      iv. The ability to connect to a WiFi network
   c. Software prerequisite
      i. Either 64bit Ubuntu 16 or 64bit Windows installed
      ii. In case you choose Windows: VMware Workstation 12 or VMware Workstation Player 12 installed, with a valid license
      iii. Administrator / root access in your system
      iv. Free version of IDA
4.
   a. Day 1
      i. SMM overview
         1. Understanding SMM: environment, capabilities
         2. SMM security
         3. UEFI support for SMM
         4. Circumventing SMM security measures
   b. Day 2
      i. Understanding SMM code
         1. Setting up a development and testing environment for experimenting with SMM code
         2. SMM dispatcher interface and internals
         3. Gaining execution in SMM
         4. Reading and analyzing SMRAM
   c. Day 3
      i. Writing a prototype
         1. Hooking SMM dispatcher
         2. Gaining periodic execution
         3. Accessing OS memory
         4. Modifying S3 boot script
   d. Day 4
      i. Practical techniques
         1. Injecting code to OS
         2. Monitoring OS events
         3. SMM keylogger
         4. Network communication
      ii. SMM rootkit detection