

Subject code: P.6(1)	Subject name: Mobile Operating Systems		
Study load: 2 ECTS	Load of contact hours: 40	Study semester: Autumn	Assessment: Credit / no credit
Objectives:	The goal of this course is to create a profound knowledge of mobile operating systems: their architectures, services and a life-cycle, as well as skills to implement mobile solutions on a particular hardware platform.		
Course outline:	<p>Topics covered:</p> <ol style="list-style-type: none"> 1. Mobile and embedded hardware platforms architectures. 2. Mobile OS architectures and life-cycle. 3. Android general architecture. File systems and partitions. OTA and A/B system updates. Project Treble. 4. HIDL and binder IPC. 5. Modular System Components. Device tree overlays. VNDK. 6. ART and Dalvik. Android code management. 7. Application security: sandbox and signing. 8. System security. Authentication. SELinux. Google cloud-based security services. 9. Security features. Verified Boot. File-based and disk-based encryption. Hardware-backed Keystore. Trusty TEE. 10. Soong and Make build systems. Flashing devices. Flash tools. Building Linux kernel. 11. Student's presentation on a given topic. <p>Contact lessons will be divided into two parts: lectures and labs.</p>		
Learning Outcomes:	<p>The following knowledge, skills, and attitudes are to be achieved by the end of the course:</p> <ol style="list-style-type: none"> 1. Critically evaluate modern mobile OS architectures, inter-process communications; understand and implement OS life-cycle, OS boot process. 2. Be able to build and flush custom kernels and ROM, and perform custom boot. 3. Be able to customize OS security features, and implement application security. 		
Assessment Methods:	Assessment is split into two parts: tests and individual tasks, including 1 mandatory presentation		
Teacher(s):	Andrey Savinkov		
Prerequisite subject(s):	None		

Compulsory Literature:	Meier, Lake Professional Android, 4-ed, Wrox, 2018, 929p				
Replacement Literature:	Google LLC, Android Open Source Project, https://source.android.com Tyler J., XDA Developers' Android Hacker's Toolkit: The Complete Guide to Rooting, ROMs and Theming, Wiley, 2012, 192p.				
Participation requirements:	Lower limit of lectures attendance is 80%, each test and individual project must be presented by end of the course.				
Independent work:	<ol style="list-style-type: none"> 1. Flash virtual device using Android SDK. 2. Build and flash custom Linux kernel (before critically evaluate mainline and factory kernels). 3. Design and implement custom SELinux policy (before, critically evaluate factory policy). 4. Develop a module for Magisk. 				
Grading criteria scale or the minimal level necessary for passing the subject:	<table border="1" style="margin-left: 20px;"> <tr> <td>Failed</td> <td>< 50 points</td> </tr> <tr> <td>Passed</td> <td>>= 50 points</td> </tr> </table> <p>Points distribution:</p> <p>Test on lectures: 30 points Individual Tasks: 15 points Presentations : 10 points</p>	Failed	< 50 points	Passed	>= 50 points
Failed	< 50 points				
Passed	>= 50 points				
Information about the course:	Room ____, on ____ at ____				
Date 1	Mobile and embedded hardware platforms architectures.				
Date 2	Mobile OS architectures and life-cycle.				
Date 3	Android general architecture. File systems and partitions. OTA and A/B system updates. Project Treble.				
Date 4	HIDL and binder IPC.				
Date 5	Modular System Components. Device tree overlays. VNDK.				
Date 6	ART and Dalvik. Android code management.				
Date 7	Application security: sandbox and signing.				
Date 8	System security. Authentication. SELinux. Google cloud-based security services.				
Date 9	Security features. Verified Boot. File-based and disk-based encryption. Hardware-backed Keystore. Trusty TEE.				
Date 10	Soong and Make build systems. Flashing devices. Flash tools. Building Linux kernel.				
Date 11	Student's presentation on a given topic.				