ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

FAKULTA PROVOZNĚ EKONOMICKÁ

INFORMATIKA

KATEDRA INFORMAČNÍCH TECHNOLOGIÍ

DIPLOMOVÁ PRÁCE

Operační systém Symbian

Autor diplomové práce: Bc. Václav Hykeš

Vedoucí diplomové práce: Ing. Jiří Vaněk, Ph.D.

Praha 2010

Prohlášení

Prohlašuji, že tato diplomová práce je mým původním autorským dílem, které jsem vypracoval samostatně. Všechny zdroje, prameny a literaturu, které jsem při vypracování používal nebo z nich čerpal, v práci řádně cituji s uvedením úplného odkazu na příslušný zdroj.

V Praze dne 8. dubna 2010

……

Václav Hykeš

Poděkování

Děkuji vedoucímu diplomové práce Ing. Jiřímu Vaňkovi Ph.D. za jeho odbornou pomoc, vstřícnost, konzultace a cenné rady.

Operační systém Symbian

Operating system Symbian

Souhrn

Diplomová práce navazuje na bakalářskou práci z roku 2007 nesoucí název „Smartphones a Symbian OS“, která se věnuje problematice chytrých mobilních zařízení, charakteristikám operačního systému Symbian a porovnáním systému s konkurenční platformou.

Cílem práce je komplexní analýza bezpečnosti, definování slabých míst systému a vytvoření vlastní modifikace.

Kapitoly jsou rozvrženy, aby komplexně shrnuly bezpečnostní prvky systému, a následně zmapovaly formy modifikací.

Práce se zabývá také kategorizací modifikací s ohledem na bezpečnostní koncept Platform Security. Jsou zde nastíněny různé druhy modifikací a jejich přínos pro uživatele mobilního zařízení se Symbian OS.

V práci se podařilo shrnout hlavní bezpečnostní mechanizmy včetně jejich slabin a způsoby jako tyto slabiny prakticky využít pro modifikování systému Symbian. Autorem vytvořená modifikace byla vyzkoušena a názorně demonstrován způsob jejího fungování.

Klíčová slova

Symbian OS, S60, mobilní zařízení, Platform Security, Data Caging, oprávnění, certifikace, modifikace, patch

Summary

Diploma thesis builds on the bachelor thesis in 2007 entitled "Smartphones and Symbian OS, which deals with the issue of smart mobile devices, the characteristics of the Symbian OS and comparing the system with a competitive platform.

The aim of this work is a comprehensive safety analysis, the definition of vulnerabilities and create their own modifications.

Chapters are divided as to fully bring together elements of the security system and then mapped the form modifications.

Work deals with the categorization of modifications with respect to the safety concept of Platform Security. Outlined here are different kinds of modifications and their contribution to the user's mobile device with Symbian .

The work managed to summarize the main security mechanisms, including their weaknesses and how these weaknesses as a practical use for modifying the system Symbian. The author has created modification and graphically demonstrated how it works.

Key words

Symbian OS, S60, mobile device, Platform Security, Data Caging, trust, certification, modification, patch

OBSAH

1 Úvod

Diplomová práce navazuje na bakalářskou práci, v níž se autor věnuje obecným charakteristikám operačního systému Symbian.

Operační systém Symbian je celosvětově nejrozšířenější systém pro mobilní zařízení typu smartphone. Nejvíce je uplatňován v zařízeních firmy Nokia. Nokia se počátkem roku 2010 stala dlouho plánovaným majoritním vlastníkem Symbian Ltd.

Po odkoupení zbylých podílů od firem Samsung, Siemens a Sony Ericsson podnikla Nokia zásadní kroky, jenž ovlivní další vývoj Symbian OS a jeho platforem. V únoru roku 2010 Nokia uvolnila zdrojový kód Symbianu, který poskytla vývojářům na svých stránkách.

Svým způsobem si tímto krokem Nokia podmanila část vývojářské základny ve smyslu podílení se na vývoji Symbian OS a jeho součástech. Nokia, uvolněním zdrojových kódů, přenáší vývoj určitých prvků směrem k vývojářům, a tudíž může své aktivity přesunout jiným směrem.

Sofistikovaná mobilní zařízení nesou stále více personálních a firemních dat a zároveň poskytují bohaté prostředky pro komunikaci. Hlavní výhodou operačních systémů pro mobilní zařízení je jejich otevřenost. Uživatel není limitován aplikační škálou danou výrobcem, ale je schopen si jednoduše rozšířit spektrum aplikací v mobilním zařízení. Funkcionalita, kterou je možné mobilní zařízení rozšířit, v sobě má velký potenciál.

S rostoucími uživatelskými nároky na funkcionalitu, jde ruku v ruce i bezpečnostní faktor. Uživatel v mobilním zařízení obvykle uchovává osobní informace nejrůznějšího charakteru a tuto skutečnost je třeba zohlednit při zabezpečení systému.

Existuje primární ochrana ve formě PINu, a pokud tento kód uživatel zadá, může se systémem pracovat. Neexistuje zde žádný koncept logování apod.

Z tohoto důvodu jsou kladeny větší nároky na bezpečnost operačního systému vzhledem k jeho fungování a ovládání.

Bezpečnostní mechanismus Symbian OS se souhrnně nazývá Platform Security. Je tvořen třemi koncepty, které dohromady zajišťují integritu a bezpečné fungování operačního systému.

Neustále probíhají pokusy o narušení bezpečnosti Symbian OS, tzv. „závody ve zbrojení“, ze strany uživatelů a vývojářů a následné kroky Nokie zabraňující zmíněnému narušování.

Postupem času se ukázalo, že bezpečnostní mechanizmy Platform Security nejsou stoprocentní. Některá narušení pramení přímo z chyb v Symbian OS, další zase z podstaty fungování operačního systému jako takového. Nejrůznější modifikace, které jsou schopny obcházet bezpečnostní mechanizmy, poskytují uživateli další možnosti, jak si systém přizpůsobit dle svých požadavků.
Problematika narušování je natolik komplexní, že autor čerpá informace majoritně z odborných internetových fór.

2 Cíl práce a metodika

Hlavním cílem práce je zmapovat bezpečnostní mechanismy Symbian OS a definovat různé přístupy k modifikacím operačního systému. Autor se zaměří na vybrané modifikace s použitím patche a zároveň uvede praktický příklad vytvoření vlastní modifikace.

Dalším cílem je analýza a kategorizace druhů modifikací s ohledem na možnosti uplatnění v praxi. Druhotným cílem je rovněž vysvětlení principu fungování vybraných modifikací a slabiny systému, jenž tyto modifikace umožňují.

Nejprve je provedena strukturovaná analýza dokumentů pojednávajících o bezpečnostních mechanizmech. Dále pak návrh vlastního řešení v podobě modifikačního patche, ke kterému je využito odborných článků zabývajících se problematikou modifikací (např. SymbianFreak.com). Při vlastní analýze je použita např. studie společnosti Sec Consult, která se orientuje na poradenství v oblasti informačních systémů.

První a druhá kapitola se zabývá úvodem do dané problematiky, seznámení se s cíly a metodikou práce.

Kapitola třetí nejdříve pojednává o operačním Systému Symbian, následně pak kategorizuje mobilní zařízení dle jejich vlastností. Poté je charakterizován předchůdce Symbianu Epoc OS, jeho vývojové fáze a parametry vybraných zařízení.

Dále je definován samotný systém Symbian OS. Jsou zde zkoumány jeho prvky, struktura a systémový model. Následně jsou uvedeny jednotlivé verze Symbianu a obecné vlastnosti uživatelského rozhraní.

Čtvrtá kapitola Hodnotí platformu Symbian z ekonomických hledisek a zároveň mapuje bezpečnostní prvky Platform Security. Rovněž jsou zde uvedeny možnosti modifikací systému.

Kapitola pátá, s názvem Výsledky a diskuze, se zabývá modifikačními aplikacemi a konkrétní formou těchto modifikací. Je zde také vysvětlen princip tvorby patche včetně praktického příkladu.

Šestá, závěrečná kapitola, pojednává o kladech modifikací a také záporech, které modifikovaný systém determinuje.

3 Operační systém Symbian

Symbian OS je otevřený operační systém firmy Nokia (dříve Symbian Ltd.), který umožňuje přístroj (se základní výbavou) rozšířit o mnoho dalších funkcí k libovolnému účelu. Vychází z operačního systému EPOC32 vytvořen firmou Psion.

Nejrozšířenější platformou Symbian OS je Series 60. Symbian je majoritně uplatňován v mobilních zařízeních Nokia (modely N73, 5800, N95 atd.).

Existují však i další výrobci, kteří implementují Symbian ve svých zařízeních (Sony Ericsson, Samsung, Motorola). Systém, za svou dobu působení, prošel značným vývojem a to jak z hlediska ovládání, tak funkcionality.

3.1 Mobilní zařízení se systémem Symbian

Zařízení se systémem Symbian jsou momentálně založena na následujících uživatelských rozhraních (platformách) otevřených pro programátory v jazycích C++ a Java:

Series 60 (Nokia 7610,5800,6620, N-Gage, Siemens SX1, Panasonic X700 atd.);
Series 80 (Nokia 9200/9500 - Communicator);
Series 90 (Nokia 7700);
UIQ (Sony Ericsson P800, P900, Motorola A950 atd.);
FOMA (p720i, d720i, atd.).

Podrobnější zkoumání platforem je uvedeno v kapitole 3.3.2 – Verze Symbian OS.

Zpravidla se rozlišují tři druhy mobilních telefonů z hlediska uskupení funkčních tlačítek a druhů displejů. [6]

3.1.1 Mobilní telefony s numerickou klávesnicí

Zařízení s numerickou klávesnicí jsou určena pro použití v jedné ruce a vyžadují flexibilní uživatelské rozhraní, které lze ovládat pomocí joysticku, dočasných tlačítek, tlačítka JogDial nebo jiné kombinace. Příklady těchto zařízení vychází z platformy Series 60. Telefon Nokia N95 je na obrázku č. 1.

Obr. č. 1, Nokia N95 [3]

3.1.2 Mobilní telefony s vertikálně umístěnými dotykovými displeji

Tato mobilní zařízení mají větší displeje, než se standardně využívají u předchozí kategorie zařízení. Rozměrnější displej se lépe hodí na prohlížení obsahu nebo práci.

Je zde také možnost interakce pomocí pera, která poskytuje uživatelům a vývojářům nové možnosti. Je možné zmínit např. Nokia 5800, která je na následujícím obrázku.

Obr. č. 2, Nokia 5800 [3]

3.1.3 Mobilní telefony s horizontálně umístěnými displeji

Zařízení s horizontálním umístěním mají obvykle největší displeje ze všech telefonů se systémem Symbian. Zařízení mohou mít kompletní klávesnici, ale i dotykový displej. Konkrétním příkladem je platforma Series 80. Toto rozhraní je základem řady Nokia 9200 Communicator, 9210i a 9290. [6]
S platformou Series 90 je model Nokia 7700 příkladem mobilního telefonu s dotykovým displejem bez klávesnice, který je ideální na častější použití multimédií. Zařízení Nokia E75 je na obrázku 3.

Obr. č. 3, Nokia E75 [3]

3.2 Epoc OS

Než systém Symbian nabyl dnešních podob, prošel dlouhým vývojem. U jeho zrodu stál Dr. David Potter, který v roce 1963 vystudoval univerzitu v Cambridgi na studijním oboru přírodní vědy, později dosáhl i doktorátu z matematické fyziky. Řadu let na této univerzitě učil jako profesor, později se však rozhodl založit vlastní firmu. [6]

Obr. č. 4, Dr. David Potter [5]

Trvalo řadu let, než sehnal potřebné finanční prostředky k realizaci firmy. Vše se po čase podařilo a Dr. Potter roku 1980 zakládá firmu Psion. Původně název Psion znamenal: Potter's Scientific Instruments. „ON" nakonec bylo prý přidáno, aby se název nepletl s fyzikální jednotkou. Hlavní náplní práce v této době bylo vyvíjet software pro tehdy rozšířený Sinclair ZX81. Vyvíjení softwaru stále pokračovalo, ale Dr. Potter se nechtěl smířit s velkou energetickou závislostí tehdejších počítačů a s tím související omezenou přenositelností a velikostí. Roku 1984 byl vyvinut první model mobilního organizéru, označovaného jako Organiser I. [6]

Obr. č. 5, Organiser I [6]

Cena tohoto zařízení nebyla nijak vysoká. Pří poměrně kompaktních rozměrech (14x9 cm), se přístroj vešel skoro kamkoliv. Zařízení obsahovalo paměť 2kB RAM a 4kB ROM, což na tu dobu byla nadstandardní velikost. Roku 1989 Psion vytvořil opravdu revoluční přístroj. Jmenoval se Psion MC 400. Dá se říci, že tento přístroj opravdu předběhl svou dobu. Obsahoval totiž vlastní operační systém EPOC, vyvinut Psionem. Systém měl plně multitaskingové jádro a grafické uživatelské rozhraní (GUI). Velkým kladem bylo to, že zařízení se ovládalo přes touchpad (dotykově). Operační paměť o velikosti 256 kB byla na svou dobu dostačující a LCD panel dělal z přístroje opravdový klenot. Samozřejmě s přihlédnutím na dobu. [6]

Obr. č. 6, MC 400 [6]

Zcela zásadním byl pro PSION rok 1998, kdy Dr. David Potter rozdělil společnost na několik odvětví: Psion Computers, Psion Enterprise a Psion Software. Poslední odvětví se spojilo s týmy firem Nokia a Ericsson, a tak vznikl základní kámen projektu Symbian. Symbian se stal majitelem práv na operační systém EPOC32. Tyto firmy získaly 30% podíl v Symbianu, k nimž se postupem času připojila americká společnost Motorola, která se později stala také podílníkem.

Symbian v té době zasadil pomyslnou ránu do týla společnosti Microsoft, která měla svůj organizér se systémem Windows CE. Firmy jako Sony a Siemens nejdříve chtěly ve svých zařízeních realizovat jmenovaný Windows CE, ale s příchodem Symbianu měli možnost volby. [6]

Prvoplánový záměr vytvořit mnohostranný operační systém, který lze nasadit, jak na mobilní telefony, tak i na organizátory a komunikátory se povedlo uskutečnit.

3.3 Symbian OS

Tato kapitola pojednává o samotném systému Symbian, jeho prvcích, principech a dalších aplikačních komponentách. Důležitá je rovněž část zabývající se základními vlastnostmi uživatelského rozhraní.

3.3.1 Design a struktura

Symbian OS byl navržen tak, aby byl realizován na „zařízeních do ruky“ s omezenými zdroji. Symbian používá specifické programovací techniky (deskriptory, haldy). Nabízí některé bloky pro systémy obsluhy událostí známé jako aktivní objekty.

Použití těchto technik pomáhá prodloužit životnost baterií. Nezastupitelnou roli zde hraje samozřejmě paměť. Paměťové jednotky jsou označeny podobně jako u PC. Přesnější význam souborových jednotek je uveden v kapitole 4. Při zapnutí bootuje Symbian z paměti ROM (spouští *.exe soubory a načítá dynamické knihovny).

Systém je složen z mnoha programů a procesů, které běží na pozadí. V základním správci souborů uživatel nemá přístup k systémovým souborům na jednotce Z:\. Všem běžným uživatelům zůstávají tedy systémové soubory skryty. V případě, že majitel investuje do pokročilejšího softwaru, může procházet a kopírovat jednotlivé soubory a složky, ale zápis není povolen vůbec. Tohoto kroku lze dosáhnout až při zákroku pomocí datového kabelu a příslušného patche (kapitola 5). [6]

Symbian má ve svých funkcích zahrnutou plnou podporu multitaskingu, tudíž je potřeba, v těle zařízení, vymezit místo pro paměť typu RAM. Operační systém pracuje s pamětí, kam lze ukládat data. (C:\). Paměť typu RAM
je v Symbianu reprezentována jednotkou D:\. Paměť je možné editovat, ale po restartu se data mažou.

Jednotka E:\ je vyhrazena pro paměťovou kartu a Z:\ je ROM, kde je uložen firmware.

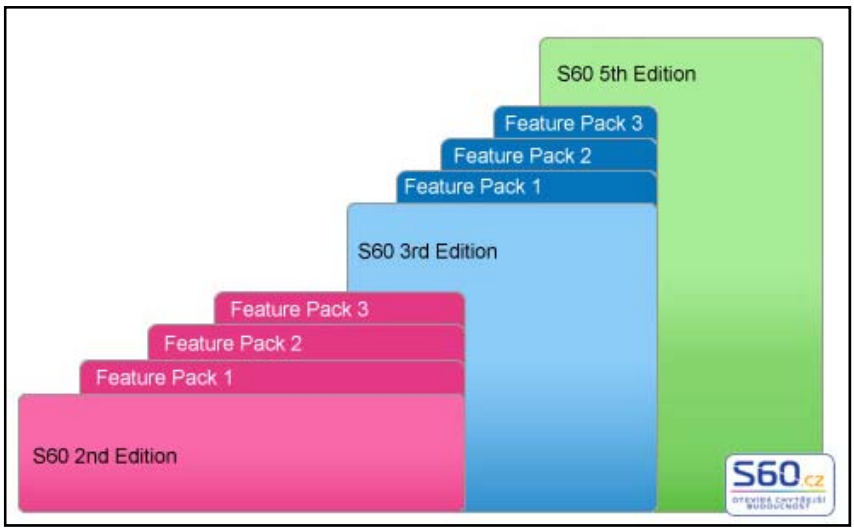
3.3.2 Verze Symbian OS

Zde jsou uvedeny hlavní verze systému. Autor záměrně neuvádí předešlé verze, tehdy ještě s názvem EPOC (např. Release 4).

Series 60

Nejrozšířenější platforma Symbia OS.

- 1st Edition - verze 6.1(Nokia 7650, 3650, N-Gage, N-Gage QD, Siemens SX1...);
- 2nd Edition - verze 7.0 - 8.1(Nokia 3230, 6260, 6600, 7610, 6670, 6630. 6680, 6681, n70, n72, n90, Panasonic X700, Panasonic X800...);
- 3rd Edition - verze 9.1(Nokia 3250, 5500, E50, E60, E61, E70, N71, N73, N80, N91, N92, N93..);
- 3rd Edition - verze 9.2 (9.1 + Feature pack 1) - (Nokia N95, E90, N82, N75, N76, Nokia 6120 Classic, E90, Nokia 5700, Nokia N81, Nokia E51..);
- 3rd Edition - verze 9.3 (9.1 + Feature pack 2)Nokia N96, N78, 6220 Classic, 6210 Navigator);
- 5th Edition - verze 9.5;



Obr. č. 7, Verze Series 60 [11]

Series 80

Velmi vybavené komunikátory s plnohodnotnou klávesnicí (9300(i), 9500)

- Verze 6.0 (Nokia 9210, 9210i)
- Verze 7.0 (Nokia 9300, 9300i, 9500)

Series 90

V současné době pouze v Nokii 7710, jejím hlavním specifikem je velký dotykový displej.

- Verze 7.0 (Nokia 7710)

UIQ

Pro tato zařízení je charakteristický velký dotykový displej. Počátkem roku 2010 se zatavil veškerý vývoj platformy UIQ.

- Verze 2.1 (Sony Ericsson P910i, P900, Motorola A1000, BenQ P30)
- Verze 3.0 (Sony Ericsson M600i, W950i, P990i)
- Verze 3.2

FOMA

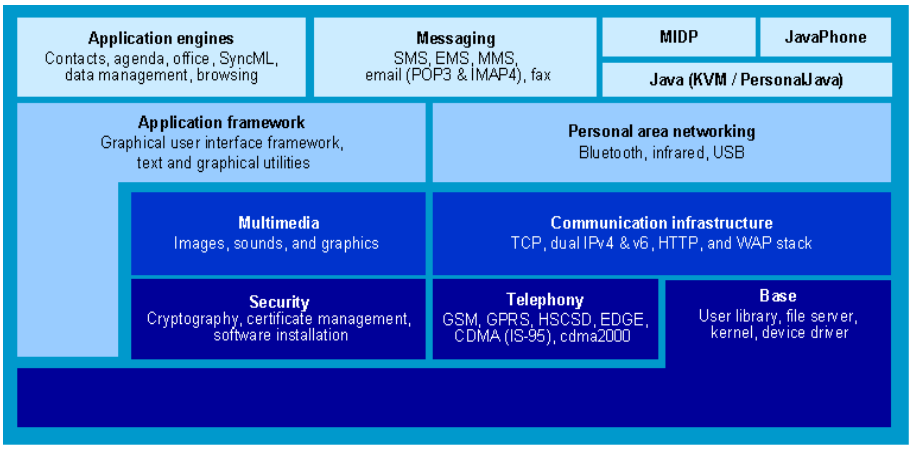
FOMA (MOAP) je označení pro zcela novou platformu, fungující na Symbianu verze 8.1. Je to prostředí vyvinuté přímo u NTT DoCoMo ve spolupráci s Fujitsu tak, aby vyhovovalo požadavkům japonského operátora. [6]

Systémový model Symbianu

Systémový model reprezentuje vyšší vrstvy architektury Symbian, znázorňující zobrazení komponent systému Symbian ve vrstvách.

Symbian tvoří pět vrstev:

- systém uživatelského rozhraní;
- aplikační služby;
- služby OS;
- základní služby;
- služby jádra a rozhraní hardwaru;



Obr. č. 8, Architektura Symbian OS verze 7.0 [7]

3.3.3 Základy systému symbian

Uživatelské rozhraní

Series 60 je nejrozšířenější platforma operačního systému Symbian s volně přístupnými SDK (Software Developer Kit).

Obě tato rozhraní jsou vrstvou nad jádrem operačního systému, které se skládají nejen z grafické části, ale i z množiny programů (e-mailový klient, databáze kontaktů, webový prohlížeč, multimediální aplikace). [6]

Platforma Symbian 60, kterou vytvořila společnost Nokia, je v současné době nejrozšířenější a nejrychleji se rozvíjející implementací operačního systému Symbian. Tento systém existuje v několika variantách. Starší verze 1.0, 1.1, 1.2, nazývané souhrnně Series 60 Platform 1.x, jsou založené na operačním systému Symbian verze 6.1. Novější modifikace nese název Series 60 Platform 2.0 a je založená na operačním systému Symbian v 7.0s.

Rozdíly mezi uvedenými verzemi v oblasti grafického rozhraní jsou minimální. Asi největší změnou, mající dopad na vzhled programů, kterou přináší platforma 2.0, je podpora témat, tj. vrstvy obrázků, které jsou uloženy ve speciálním formátu, zobrazitelné přes ovládací prvky, ikony a pozadí obrazovky. Tato vlastnost umožňuje měnit vzhled uživatelského rozhraní telefonu, podle vkusu a aktuálních potřeb uživatele.

Všechna zařízení Series 60 lze ovládat tlačítkem, nebo malým pákovým ovladačem, umožňujícím pohyb a stisk potvrzující volbu. Rozložení tlačítek je zvoleno tak, aby uživatel mohl své zařízení ovládat pouze jednou rukou. Pro vkládání textu, je telefon vybaven standardní dvanácti - tlačítkovou číselnou klávesnicí a možností použití prediktivního vkládání slov (slovník T9).

Platformu UIQ vyvinula dceřiná firma UIQ Technology AB společnosti Symbian Ltd. První verze nazývaná UIQ 1.0 byla uvolněna v prosinci roku 2000 a od té doby bylo vytvořeno několik dalších verzí.

Tyto telefony jsou vybaveny velkou dotykovou obrazovkou (rozměr 6 x 8 nebo 4 x 6 cm). Hlavním ovládacím prvkem je přiložený stylus (dotykové pero).

Obdobně jako telefony Series 60 byly všechny vyráběné modely UIQ vybaveny různě velkým počtem tlačítek. Rozdíly ve způsobu ovládání zařízení a velikosti obrazovky ovlivňují přímo škálu a možnosti programů dostupných na obou typech telefonů. Jak již bylo řečeno výše, platforma UIQ se již nevyrábí. [6]

Společné vlastnosti

Nejmenším společným jmenovatelem platforem Series 60 a UIQ, je vrstva nazvaná Uikon. Skládá se z množství tříd a rozhraní a definuje řadu vlastních ovládacích prvků a dialogů. Nad ní obě popisované platformy vystavěli dvě rozdílné vrstvy: Avkon (Series 60) a Quikon (UIQ).

Aplikace

Na mobilním zařízení s operačním systémem Symbian je aktivní vždy pouze jedna aplikace. Běh ostatních programů však nemusí být nutně ukončen. Program je přepnut na pozadí a uživatel může mezi nimi prostřednictvím grafického rozhraní libovolně přepínat. Mezi podporované formáty patří např.: Java: MIDP2.0, CLDC 1.1 a C++ a Java SDK.

Obrazovka

Operační systém Symbian není svázán žádnou hardwarovou architekturou a obě nejrozšířenější implementace Symbian 60, je možné instalovat na množství odlišných zařízení.

Jednou z důležitých vlastností operačního systému, hojně využívaná a oceňovaná výrobci mobilních zařízení, je možnost velice snadné změny celkového vzhledu grafického rozhraní a odlišení výrobků od produktů konkurence. Změna zahrnuje volbu palety barev, fontů, textů, vzhled ikon a všech viditelných grafických prvků obrazovky.

Series 60

Obrazovka těchto zařízení s rozhraním Symbian 60 je rozdělena do tří logických celků nazvané jako stavový řádek, hlavní panel a panel ovládacích prvků (dočasná tlačítka). Viz obr. č. 9.

Obr. č. 9, Obrazovka mobilního telefonu Series 60 [8]

Stavový řádek

Zabírá úzký pruh v horní části obrazovky. Zobrazuje dva typy informací: název a ikonu aplikace běžící v popředí a údaje o stavu mobilního zařízení. Panel složený z šesti částí obsahuje následující:

- údaj o síle signálu sítě GSM operátora spolu s ikonou udávající stav, typ paketového přenosu dat (GPRS, WCDMA) apod. Tato ikona však nerozlišuje typ přenosu a zobrazuje pouze symbol 2G nebo 3G;
- kontextový panel (context panel) s ikonou aplikace běžící v popředí;
- název aplikace běžící v popředí;
- navigační panel;
- informace o zdroji napájení a nabíjení;
- malý panel s různými ukazateli (stav připojení a přenosu dat přes infračervené rozhraní, Bluetooth, kabel USB, informace o příchozí SMS, apod.);

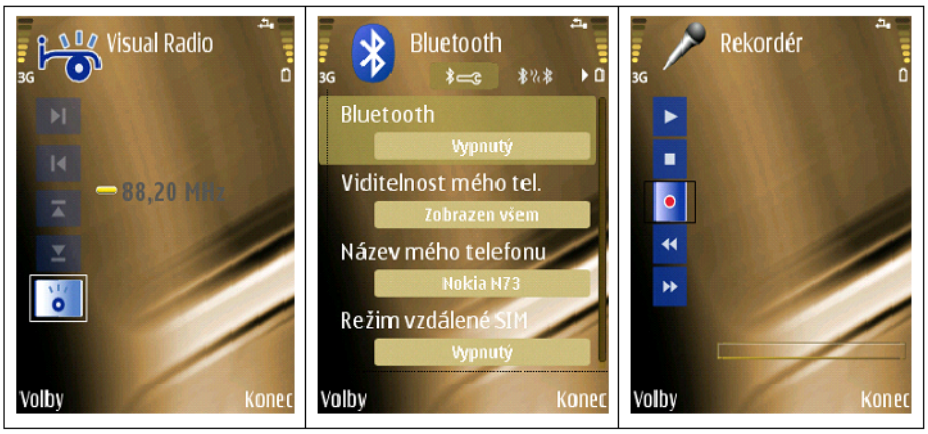
Panel ovládacích prvků

Na panelu ovládacích prvků jsou, kromě ikony se dvěma šipkami, která na platformě Series 60 nahrazuje vertikální posuvnou lištu, po obou stranách zobrazené dva krátké textové řetězce. Tato tlačítka nejsou implicitně spojena s žádnou konkrétní akcí, význam jim přiřazuje aplikace. Proto se tato tlačítka označují jako dočasná (softkeys). Stisk levého tlačítka označovaného textem volby (options), bývá ve většině případů spojen se zobrazením roletového menu. Často také slouží k provádění akce.

Hlavní panel aplikace

Největší část obrazovky mezi dvěma panely je možno bez jakýchkoliv omezení použít k zobrazení uživatelských dat aplikace.

Na následujících obrázcích jsou hlavní panely aplikací: Visual Radio (poslech rádia), Bluetooth klient a Recorder (nahrávání zvuků – diktafon). [6]



Obr. č. 10, Symbian aplikace (3rd edition) [8]

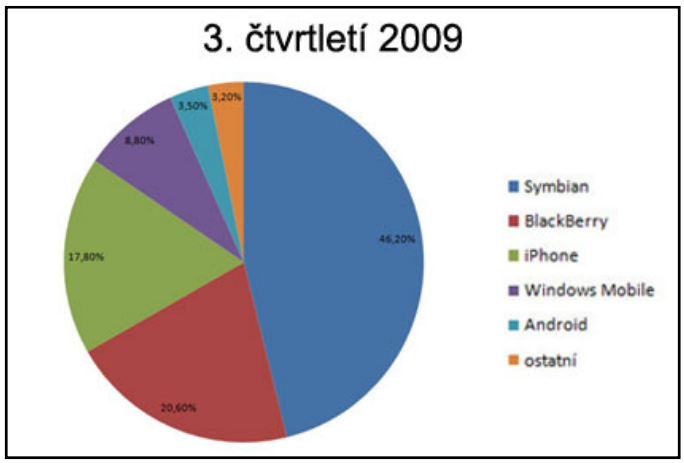
4 Hodnocení plaformy

Následující kapitoly mapují platformu z ekonomických a manažersko-podnikatelských hledisek.

4.1 Postavení na trhu

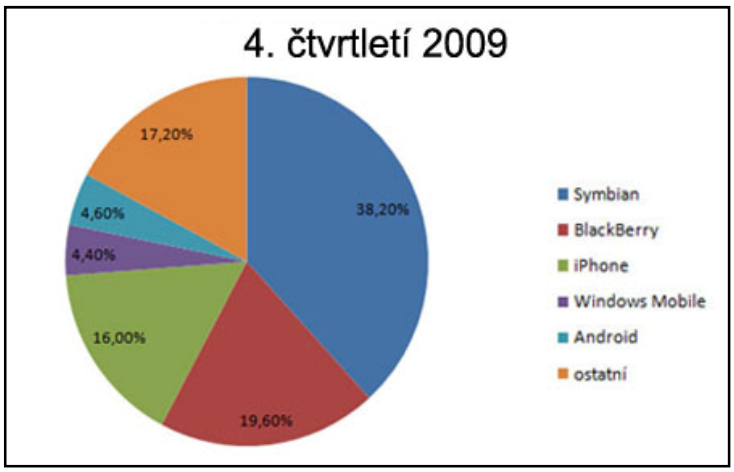
Operační systém Symbian je celosvětově nejrozšířenější mobilní operační systém v oblasti tzv. „chytrých telefonů“. Hlavním „tahounem“ Symbian OS je firma Nokia, která je nejvýznamnějším implementátorem Symbianu. V nedávné době však proběhlo spojení obou firem. Více v kapitole s názvem: Akvizice.

Ve 3. čtvrtletí roku 2009 bylo podle analytiků společnosti Canalys celosvětově prodáno 41,39 milionů kusů mobilních zařízení s operačním systémem. Proběhlo zde navýšení oproti stejnému čtvrtletí roku 2008 o 3,9 %. Na následujícím grafu je uveden podíl jednotlivých výrobců operačních systémů pro mobilní zařízení.



Obr. č. 11, Podíly na trhu ve 3. čtvrtletím 2009 [9]

Navzdory finanční krizi byl ve 4. čtvrtletí roku 2009 prodán rekordní počet smartphonů. Podle průzkumu společnosti IDC se prodalo 54,5 milionů mobilních zařízení s operačním systémem. Dle IDC je zde nárůst o 39 % oproti 4. Čtvrtletí roku 2008. [16]



Obr. č. 12, Podíly na trhu ve 4. čtvrtletí 2009 [9]

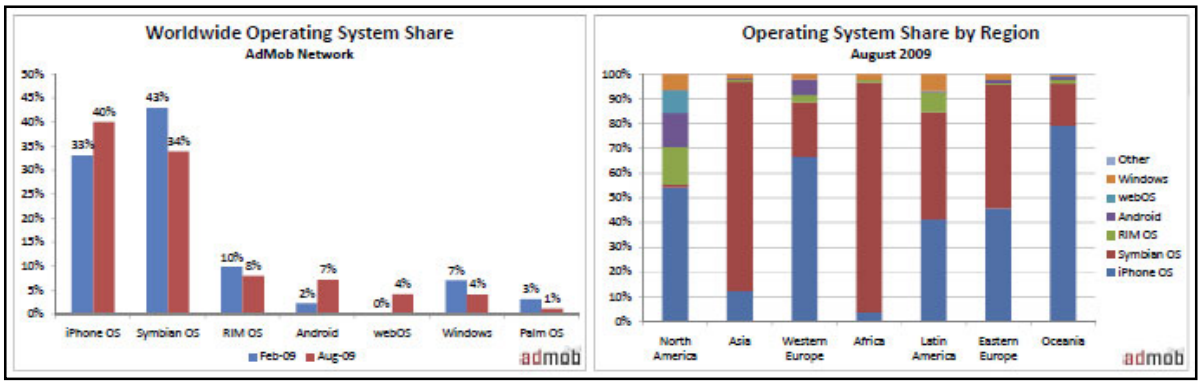
Z grafů je patrná klesající tendence podílu Symbianu na světovém trhu na úkor ostatních OS.

Existují různé studie s různými výsledky. V největší míře závisí na metodice, která je použita při analýzách. Jako příklad je možné uvést studii společnosti Admob, která uvádí nejsilnějším hráčem 4. čtvrtletí roku 2009 společnost Apple a jejich iPhone OS.

Následující grafy uvádějí vývoj trhu s mobilními operačními systémy od ledna do srpna 2009 v celosvětovém i regionálním měřítku. Je třeba si všimnout zejména rozdílu v srpnovém podílu iPhone OS (43 %), kdy oproti předešlým analýzám nastal rapidní nárůst o 13 % , jak uvádí studie analytiků společnosti Canalys. [7]

Dle názoru autora bude podíl na trhu Symbian OS mírně ovlivněn konkurenční platformou iPhone, která má mino Evropu velké podíly. Postavení Symbianu bude ovlivňovat také to, jakým způsobem se vyrovná s alternativními operačnímy systémy.

Je třeba reflektovat, že Symbian bude pravděpodobně stále více uplatňován v levnějších zařízeních. Pokročilejší zařízení budou postaveny na platformě Maemo, která nabízí větší možnosti využití.



Obr. č. 13, Podíly na trhu v roce 2009 [2]

4.2 Ovi (Nokia) maps

Koncem ledna 2010 Nokia podnikla zásadní krok, jenž zahýbal trhem navigačních GPS přístrojů. Nabídla navigaci Ovi Maps (Nokia Maps) zcela zdarma s veškerou funkcionalitou.

Nokia Ovi Maps patří mezi off - board navigační aplikace. Veškerá data se stahují prostřednictvím mobilních datových přenosů a to má své výhody. Nokia se chlubí detailními mapovými podklady pro 180 zemí a v 74 z nich lze využít automobilovou navigaci. Uživatel si může mapy průběžně aktualizovat, za což neplatí žádné poplatky. Důležitým předpokladem jak plnohodnotně provozovat Ovi maps je kvalitní datová služba.

Pro uživatele to znamená disponovat přijatelnou rychlostí připojení a v nejlepším případě datově neomezeným tarifem. Bez přijatelné rychlosti se aktualizace stahují poměrně dlouhou dobu a „sankce“ za překročený datový limit, v podobě snížení rychlosti, jsou pro české operátory samozřejmostí. Aplikace Nokia Ovi Maps doposud fungovala zdarma jen bez navigačních funkcí. Pokud byla vyžadována navigace s hlasovými instrukcemi, nebo navigace pro pěší, požadovala Nokia zaplacení ročního paušálního poplatku. To již neplatí. Veškeré funkce jsou nyní pro všechny uživatele zařízení Nokia zdarma. Uvolnění navigační aplikace s veškerou funkcionalitou je celé v režii Nokie. Z tohoto důvodu není možné zdarma provozovat aplikaci na konkurenčních Symbian zařízeních (např. Samsung i8910 HD). Tento krok Nokie lze hodnotit pozitivně. Ze dne na den získaly miliony uživatelů plnohodnotnou navigaci v mobilním zařízení. Důsledkem toho se zájem o klasické automobilové navigace snižuje. Například akcie TomTomu obchodované na burze v Amsterdamu již zaznamenaly propad
o 13 %. Lze předpokládat, že i cena akcií Garmin a ostatních výrobců navigačních systémů bude klesat. [8]
Ukázky z Nokia Ovi Maps je možné vidět na následujícím obrázku.

Obr. č. 14, Ovi Maps [3]

Akvizice

Nokia v minulosti již zaplatila desítky milionů dolarů za licenční poplatky Symbianu. Firma se racionálně rozhodla raději investovat dalších 410 milionů do koupě celé společnosti než dále pokračovat tímto způsobem.

Proces přechodu Symbianu začal v létě roku 2008, kdy byl kompletně odkoupen společností Nokia, a byla založena organizace s názvem Symbian Foundation, jež má rozvoj Symbian OS na starost. Jedním z důvodů akvizice mohla být zvyšující se konkurence na trhu, hlavně ze strany platformy Android od společnosti Google.

Android je analytiky v současnosti považován za hlavního vyzyvatele pro Symbian. Někteří komentátoři spolu s otevřením kódu Symbianu ovšem varují před možnou fragmentací a nekompatibilitou takto vzniklých verzí.

Zdrojový kód Symbianu je od února 2010 k dispozici z vývojářských stránek Symbianu. Předešlé verze Symbianu jsou využívány po celém světě a stále si udržují dobrou pozici na trhu, kterou však útoky nových platforem mohou v budoucnu ohrozit. Jedním z možných důvodů může být např. určitá zastaralost Symbianu, což by se v průběhu příštích dvou let mělo změnit s uvedením nových verzí s přepracovaným rozhraním. Nokia informovala o přípravě nového Symbian^3, který by se v smartphonech měl objevit na začátku roku 2011.

CEO firmy Nokia Olli-Pekka Kallasvuo k Symbianu^3 řekl:

„Rozhraní nového Symbianu potřebuje ještě další zlepšení a je nyní na jeho firmě a na komunitě kolem tohoto mobilního operačního systému, aby se této úlohy zhostila. Do konce roku by mělo být již bez chyb a být připraveno pro oficiální nasazení do prvních smartphonů.“ [17]

Dle názoru autora je zde důležité slovní spojení „komunita kolem mobilního operačního systému“. Firma Nokia si s otevřením platformy do jisté míry zjednodušuje práci ve smyslu rozdělení vývojářského portfolia. Pravděpodobně přesune vývoj určitých prvků směrem ke komunitě a bude se soustředit na jiné (možná důležitější) cíle.

4.3 Symbian a bezpečnost – Platform security

Bezpečnostní mechanizmus jako celek se nazývá Platform Security. Existují 3 koncepty, které jsou základem pro Symbian OS Platform Security. Následující kapitola mapuje první z nich, tedy stupně oprávnění (Tiers of Trust).

4.3.1 Stupně oprávnění

Mobilní telefon je primárně určen k osobnímu použití. U chytrých telefonů (smartphonů) je tento požadavek zvláště důležitý, protože zařízení obsahuje soukromé informace nejrůznějšího charakteru (kalendář, emaily, kontakty).

Design Symbianu např. umožňuje pouze jeden telefonní seznam. Není zde seznam pro dalšího uživatele. Příčiny této skutečnosti jsou jasné. Symbian je jedno-uživatelský operační systém a není zde žádný koncept logování (jméno uživatele, heslo). Je samozřejmě možné používat PIN kód, ale po zadání správného kóduje lze zařízení plně ovládat. Omezení na jednoho uživatele do jisté míry zjednodušuje bezpečnostní model. Proto lze bezpečnostní model Symbianu z pohledu architektury označit jako lehký model (lightweight security model). Bezpečnostní systém se nemusí zabývat, zda je uživatel důvěryhodnou osobou. Pokud je osoba schopna ovládat zařízení, je k ovládání implicitně oprávněna. [2]

Bezpečnost se však musí zabývat důvěryhodností procesů, které jsou v zařízení spuštěny jménem uživatele. Tyto procesy mohou být vyvolány různými programy a tím pádem mohou provádět např. operace, které ovlivňují fungování telefonu nebo sítě.

Architektura Symbian Os Platform Security byla navržena pro kontrolu toho, co proces může dělat. Proces je pouze schopen vykonávat činnosti, pro které má příslušná oprávnění. Jak jsou oprávnění přidělována, bude vysvětleno později.

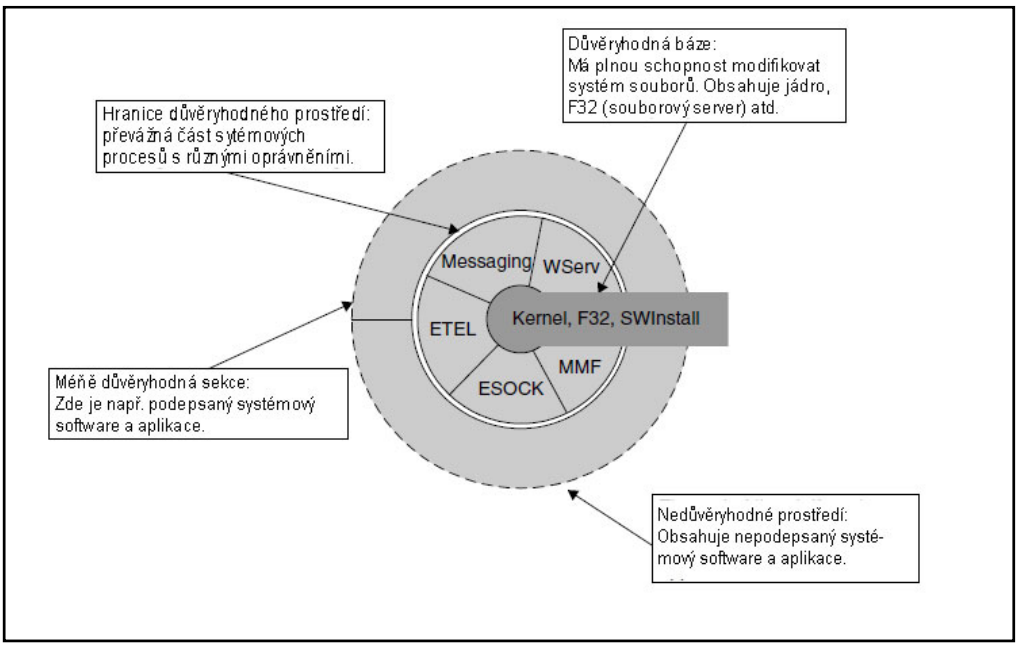
Důležité je, že bez zvláštního povolení Symbian nedovolí procesu provést požadované služby, neboť není považován operačním systémem za dostatečně důvěryhodný. [3]

Základním prvkem systému je proces. OS vymezuje hranici jeho chování, kontroluje oprávnění a přiděluje zdroje. Díky MMU (memory management unit) je zabezpečeno, že žádný proces nemůže přistupovat do adresového prostoru jiného procesu. Jsou zde také mechanizmy na sdílení dat mezi procesy a inter-procesní komunikaci. Výše zmíněné operace jsou řízeny jádrem operačního systému. [13]

Platform security obsahuje 4 hlavní moduly (vrstvy):

- Důvěryhodná báze (Trusted code base - TCB)
- Důvěryhodné prostředí (Trusted code environment - TCE)
- Data Caging
- Capabilities - oprávnění

Stupeň důvěryhodnosti se tedy pohybuje od zcela důvěryhodný, po zcela nedůvěryhodný. Podrobnější vysvětlení je uvedeno na následujícím obrázku:



Obr. č. 15, Stupně důvěryhodnosti [8]

TCB je nejdůvěryhodnější částí systému, která ovládá bezpečnostní mechanismy a má odpovědnost za zachování integrity systému. Tato část obsahuje jádro operačního systému a spravuje údaje o jednotlivých procesech včetně jejich oprávnění. V bázi je rovněž implementován file server (F32), který je používán k načtení kódu procesu. Informace o privilegiích pro jednotlivé procesy spravuje jádro.

Některá zařízení s operačním systémem Symbian mohou být „zavřená“. To znamená, že nepodporují instalace softwaru výrobce. Po „otevření“
je software installer (SWInstall) částí nejdůvěryhodnější skupiny.

Software installer je spuštěn při každé instalaci Software Install Skriptu (SIS). Tento program extrahuje data z SIS balíku a zároveň ověřuje privilegia požadovaná pro aplikaci.

Jádro, file server procesy a Software installer musí být kontrolovány, aby se zajistilo jejich správné chování.

Je třeba zmínit i hardwarové opatření v podobě MMU (Memory Management Unit) a dalších prvků souvisejících s bezpečností. [4]

Aplikace mající TCB oprávnění (plný přístup do systému) jsou většinou vestavěné. Jedná se například o antivirový software, ale i třeba modifikující utilita hellocarbide.

Důvěryhodné prostředí (TCE)

TCE obsahuje další důvěryhodný software od společnosti Symbian Ltd., výrobce telefonu, nebo poskytovatele uživatelského rozhraní. Software je označen jako důvěryhodný, ale nepotřebuje nejvyšší systém privilegií. Důvěryhodnost je určována dle systému priorit.

TCE vrstva obvykle implementuje systémové síťové procesy. Selhání těchto procesů by nemělo ohrozit integritu operačního systému jako takového. Jádro může restartovat síťové služby a udržet tak integritu systému.

Mezi takto podepsaný software se řadí skoro všechny doplňky umožňující úpravu částí TCB nebo TCE. Musí být však podepsány důvěryhodnou autoritou. Oprávnění jsou poskytována prostřednictvím TCE vrstvy a v případě, že je software podepsán důvěryhodnou autoritou, mu vrstva práva přidělí. [13]

Podepsaný software

Je možné instalovat software, který modifikuje komponenty v TCB a TCE, ale pouze v případě, že software je podepsán důvěryhodnou autoritou a je-li autorita oprávněna udělit potřebná privilegia. Většina doplňujícího software je mimo TCE. I když takový software není součástí TCE, může potřebovat určitá privilegia za účelem využití služeb poskytovaných TCE.

Symbian Signed

Podepsáním aplikace se rozumí proces, během kterého je do aplikace zakódován digitální certifikát.

Certifikát garantuje původ aplikace a umožňuje přístup k množině oprávnění chráněných aplikačních rozhraní, jež jsou definována při kompilaci aplikace. Podepsání je zárukou, že aplikace, kterou instaluje uživatel, je shodná s aplikací od vývojářů softwaru. Jedná se o poměrně důležitou součást Platform Security, jelikož výrobci a operátoři umožňují do zařízení instalovat pouze podepsané aplikace.

Cetifikace - podepsání

Od února roku 2008 nelze vytvářet certifikáty prostřednictvím Symbian Signed. Přes tyto stránky funguje pouze certifikace jednotlivých aplikací Open Signed Online, nebo při použití Publisher ID. Tento krok byl ze strany Symbianu velmi riskantní a způsobil nevoli velkého počtu vývojářů. Došlo tak k určitému omezení otevřenosti platformy.

Proces podepsání aplikací společně s testováním je zajištěna určitá úroveň spolehlivosti aplikací. U takto podepsané aplikace není uživatel vystaven žádným varováním a lze tedy předpokládat, že aplikace, která prošla testováním, nebude jeho zařízení s nejvyšší pravděpodobností neohroženo ani nepoškozeno.

Symbian Signed v současné době poskytuje pro vývojáře tři možnosti podepsání:

- Open Signed – umožňuje podepsat aplikaci pro zařízení s jedním konkrétním IMEI.
- Express Signed – pro tento program je nutné vlastnit Publisher ID.

- Certified Signed – dovoluje použití všech oprávnění kromě AllFiles, DRM a TCB. Vyžaduje nezávislé testování u některého z akreditovaných partnerů Symbian Signed.
- OPDA certifikace – Na čínských stránkách http://cer.opda.cn je možné po registraci vytvořit tzv. OPDA certifikát. S pomocí tohoto certifikátu lze legálně podepisovat aplikace pro Symbian OS, které se vážou na konkrétní IMEI. Aplikace podepsaná tímto certifikátem nepůjde na zařízení s jiným IMEI.

Obr. č. 16, Logo Symbian Signed [10]

Nepodepsaný software

Je-li software označen jako nepodepsaný, (není podepsán některým z důvěryhodných orgánů) systém ho klasifikuje jako nedůvěryhodný. To však neznamená, že je software škodlivý. Existuje celá řada aplikací, které nepotřebují oprávnění (kalkulačka).

4.3.2 Model oprávnění - Capability model

Druhý koncept se vyznačuje tím, že jednotlivé procesy mohou mít současně víc práv. Tato technika se nazývá Capability. Koncept definuje 20 druhů práv (obr. č. 17).

Práva procesu se během jeho existence nemění. Největší váhu má oprávnění TCB. Má-li proces oprávnění TCB, může jakémukoliv jinému libovolnému procesu přiřadit jiné oprávnění.

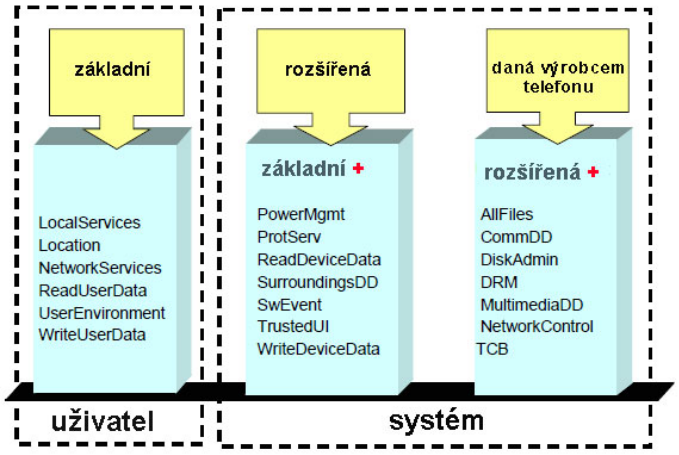
Některá oprávnění lze získat podepsáním aplikace přes Symbian Signed.

Model oprávnění úzce souvisí s certifikací (podepsáním). Ve složce \sys\bin je vždy *.exe soubor, který musí mít nějaké oprávnění (capabilities, zkráceně caps). Podle tohoto oprávnění systém kontroluje na co má dotyčný soubor nárok a na co nikoliv.

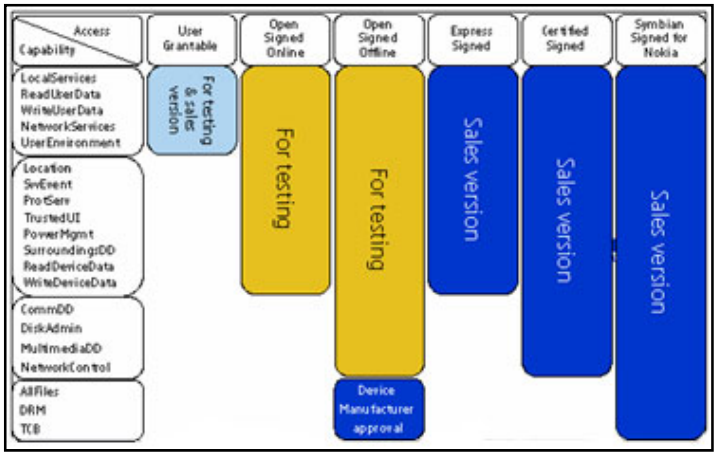
Tato kontrola je zapsána v několika souborech v Z:\sys\bin (efile.exe, checkintegrity.exe a chckintegritysrv.exe). [2]

Dále se jedná o přidružený soubor swipolicy.ini z:\resource, který je volán při instalaci samotnou aplikací instalátoru (installserver.exe).

Všechna oprávnění aplikace (*exe a *dll souborů) se musí ztvrdit certifikátem. To znamená, že certifikát vlastně musí garantovat to, na co si aplikace "dělá nárok". Certifikáty ze Symbian Signed garantovaly 13 oprávnění (viz obr. níže). Nejvyšší oprávnění TCB není schopen garantovat žádný z volně dostupných certifikátů. Toto je jeden z hlavních důvodů pro „modifikaci“ systému Symbian. Oprávnění lze rozdělit na uživatelská a systémová. [3]



Obr. č. 17, Práva systému [8]



Obr. č. 18, Práva systému – rozdělená [10]

Uživatelská oprávnění (práva přidělitelná uživatelem)

Oprávnění tohoto typu jsou definována tak, aby korespondovala s činnostmi vyžadující interakci s uživatelem. Oprávnění jsou důležitá například, když aplikace bude chtít přistupovat k privátním datům uživatele. Uživatel bude jednoduše dotázán, zda tento přístup povolí, či nikoliv. Struktura uživatelských oprávnění je uvedena níže.

oprávnění	funkce
LocalServices	Přístup k připojením s "krátkým" dosahem, jako jsou bluetooth nebo IR.
Location	Přístup k informacím o pozici telefonu.
NetworkServices	Přístup ke službám poskytovaným přes WiFi, GSM, CDMA a IP transportní protokoly.
ReadUserData	Přístup pro čtení k osobním uživatelským datům (zvuky,fotky, atp.). Toto právo má chránit soukromí uživatele.
WriteUserData	Zápis osobních uživatelských dat.

Obr. č. 19, Uživatelská práva [8]

Systémová oprávnění (rozšířená a daná výrobcem)

Největší skupinou oprávnění, jsou oprávnění systémová. Udělení systémového oprávnění dovoluje procesu přistupovat k citlivým operacím. Systémová oprávnění chrání systémové služby, nastavení zařízení a přístup k hardwaru.[9]

Systémová oprávnění lze dále rozdělit následovně:

- Práva zaručená podpisem **bez ověření identity vývojáře** – práva, která je možné udělit konkrétní aplikaci tím, že jí vývojář podepíše na http://www.symbiansigned.com. Práva takto přidělená obsahují samozřejmě i práva přidělená uživatelem (Obr. č. 19). Je-li aplikace takto podepsaná, nemusí se na uživatelská práva ptát, neboť již je získal automaticky. V následující tabulce jsou práva spadající do této skupiny označena oranžovou barvou.

Práva vázána na **ověření identity vývojáře**. Jedná se o výslovná schválení konkrétní aplikace a smluvního závazku s výrobcem. V tabulce označeno modrou barvou. [9]

oprávnění	funkce
UserEnvironment	Přístup k zařízením jako je fotoaparát, mikrofon, nahrávání videa atp.
PowerMgmt	Právo ukončit proces, odpojit nepoužívané periferie, přepnout telefon do stand-by, zapnout telefon nebo jej vypnout.
ProtServ	Toto právo umožňuje procesu se zaregistrovat jako chráněný proces (jeho jméno začíná !). Ten není možno ukončit, je hlídán watchdogem a není impersonalizován.
ReadDeviceData	Přístup k informacím o operátorovi, výrobci telefonu a některým nastavením telefonu. Zejména takovým, která ovlivňují jeho chování.
SurroundingsDD	Přístup k zařízením jako GPS nebo biometrickým zařízením připojeným k telefonu.
SwEvent	Schopnost simulovat stisky kláves zařízení a odchytávat tyto události z jakékoli aplikace a zpracovávat je.
TrustedUI	Schopnost vytvořit tzv. trusted UI dialogy, což jsou zvláště chráněné dialogy například pro zadávání hesel, PINu atp. U nich je zaručeno že nikdo neodchytí vstup do nich i když má SwEvent právo.
WriteDeviceData	Právo zapisovat data jenž mění chování zažízení (budík, zámky kláves, čas, hodiny, časové pásmo atp.).
AllFiles	Právo pro přístup pro čtení do celého filesystému a pro zápis do private adresářů aplikací.
ComDD	Právo přímého přístupu k hardwarovým komunikačním prostředkům telefonu bez použití API. Například Wifi.
DRM	Právo pro přístup k surovým datům chráněným DRM. Toto právo lze udělit pouze tehdy, je-li poskytovatel práva přesvědšen, že budou respektovány práva nastavená DRM. DRM je smluvně vázáno.
MultimediaDD	Právo přímého přístupu k multimediálním prostředkům telefonu bez použití API. Například fotoaparátu.
NetworkControl	Právo modifikovat, nastavovat a přistupovat k síťovým protokolům telefonu.
TCB	Pokud existuje toto právo lze zasahovat do dat, jenž ovlivňují integritu systému. Například zápis do adresáře sys\bin. Toto právo je třetím stranám udělováno pouze zcela vyjímečně (například pro antivirový sofware renomovaných společností smluvně vázaných s Nokií).

Obr. č. 20, Systémová práva [8]

Zápis oprávnění v certifikátu

Oprávnění je v certifikátu zapsáno v šestnáctkové soustavě. Údaje o tom, zda aplikace je podepsaná, či nikoliv se ukládají do *.exe souboru v c:\sys\HASH.

Do stejného souboru, který má vždy 20 bitů, se uloží v HEX znacích údaje o IMEI oprávněních a také kontrolní algoritmus, který systém kontroluje při spuštění aplikace. Výše popsaná metoda upravuje stávající certifikát ve formátu *p7b, kde by údaje o oprávněních měly vypadat např. takto:

13 caps:002D8FF0

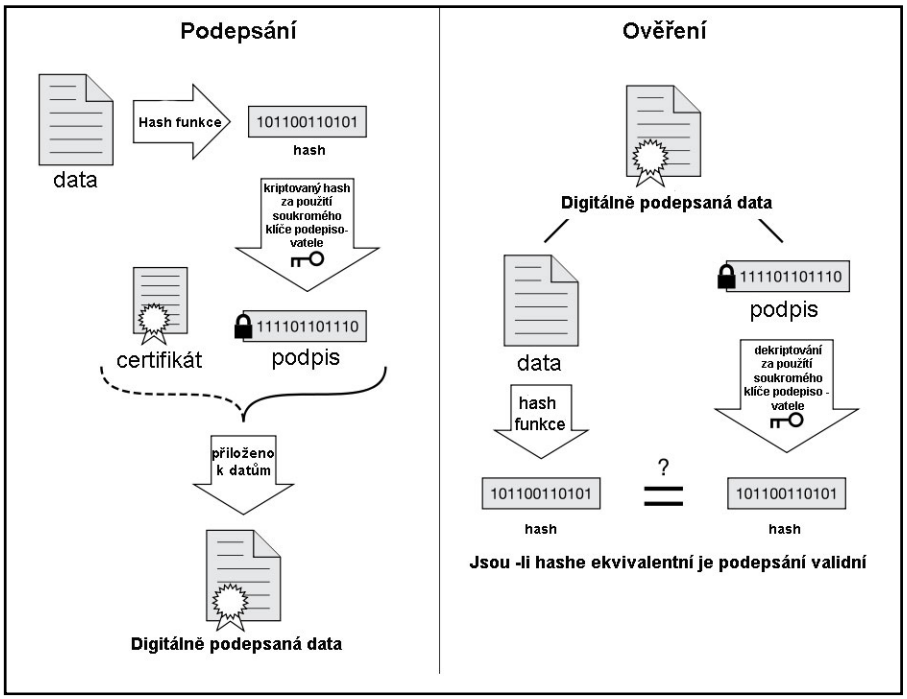
17 caps:007DEFF0

20 caps:00FFFFF0

První číslo značí oprávnění, z čehož vyplývá, že první jich má 13. V tomto případě se jedná o certifikát z dob volně přístupného Symbian Signed.

Certifikát se 17 oprávněními je tzv. OPDA certifikát, neboli certifikát vyrobený přes Symbian Signed prostřednictvím Publisher ID. OPDA certifikát umožňuje vytvořit certifikát až na 1000 IMEI. [3]

Nakonec certifikát s 20 oprávněními, který garantuje přímý přístup do systému, ale spolupracuje pouze s Symbian Public Key, jehož získání je poměrně složité. Nabízí se možnost modifikace změnou IMEI v imei listu daného certifikátu, ale tato změna se uloží při podepsání do instalačního souboru \HASH a nebude souhlasit s algoritmem v *key, ani kontrolou systému. Zařízení si uchovává algoritmy ze všech *key souborů, se kterými je již obeznámen. Pro lepší pochopení slouží následující obrázek. Je zde zobrazen samotný proces podepisování a následné ověřování (verifikace).



Obr. č. 21, Certifikace a verifikace [14]

Identifikátory

V zabezpečeném prostředí server musí vědět, které programy mají oprávnění přístupu k aplikačnímu rozhraní. Server buď sám udržuje seznamy těchto programů, nebo využívá oprávnění v rámci Platform Security modelu. Tento způsob odstraňuje potřebu konkrétní identifikace programů, neboť server může řídit přístup ke svému aplikačnímu rozhraní, aniž by znal, kdo daný proces zavolal.

Někdy je však potřeba program jednoznačně identifikovat. Například jsou li data vázána na konkrétní program. Pro identifikaci jsou definovány následující identifikátory:

UID (unikátní identifikátor)

V Symbian OS je UID reprezentováno 32 – bitovým číslem v rozsahu 0x00000000 až 0xFFFFFFFF. Jednotlivé hodnoty v tomto rozsahu mohou být rezervované pro různé objekty k různým účelům. Pro jednoznačnou identifikaci binárního souboru (*.exe,*.dll) v systému, stejně jako k rozlišení mezi procesy, se používá unikátní identifikátor (UID3), který je zapsán v *.mmp souboru aplikace za použití klíčového slova „SecureID“.

Symbian umožňuje snadný a rychlý způsob jak automaticky získat unikátní identifikátor. Tímto je možné určit vlastníka podepsané aplikace podle jeho UID. Zmíněný postup zabraňuje náhodnému nebo záměrnému použití cizího identifikátoru a ručí za spolehlivost údajů, popřípadě zajišťuje proti úniku dat.
UID hodnoty menší nebo rovné 0x7FFFFFFF jsou chráněny. Jsou určeny pouze pro použití v podepsaných nebo v ROM předinstalovaných aplikacích. Instalátor neumožňuje instalaci nepodepsané aplikace, je-li zahrnuta v oblasti chráněných UID hodnot. [4]

Z důvodu omezení prostoru hodnoty UID Symbian OS 9.x lze použít chráněné UID a to jak pro certifikátem podepsané, tak pro nepodepsané aplikace. To zahrnuje UID pro binární soubory a jim příslušející balíky *.pkg (takzvané SISUID).

Jestli pro Symbian aplikace starších verzí než 9. x bude použito UID z nechráněné oblasti, utilita Makesis.exe oznámí zprávu o chybě a samotná aplikace se po nainstalování a spuštění může zhroutit. [10]

SID (Secure Identifier)

Od Symbianu verze 9. x musí každý spustitelný program obsahovat tento identifikátor. SID je unikátní a přiřazuje se každému spustitelnému EXE souboru. Identifikátor SID, který používají novější verze (např. 9.1) je modernější a dovoluje Platform Security následující:

- chránit uživatelské rozhraní;
- omezit přístup některým aplikacím do uživatelského rozhraní;
- chránit přístup k systému souborů;

Hodnoty identifikátoru jsou opět specifikovány v *mmp souboru aplikace za použití klíčového slova „SecureID“. Zde je zajištěno, aby majitel SID mohl být autorizován v rámci programu Symbian Signed.

Identifikátory UID jsou rozděleny na dvě části:

- **Chráněná část:** Je-li aplikace podepsaná (Symbian Signed) bude UID získáno z chráněné oblasti. Přidělování UID je kontrolováno a při podepisování je ověřeno, zda je identifikátor unikátní. Ověření unikátnosti UID pro aplikaci probíhá na celosvětové úrovni.

- Software Installer zajišťuje, že nepodepsané aplikace nemohou mít UID z chráněné oblasti a že není žádné UID asociováno na více než jeden spustitelný soubor.
- **Nechráněná část:** Poskytuje přidělování UID pro nepodepsané aplikace, ale bez záruky globální jedinečnost.

VID (Vendor Identifier)

Spustitelné soubory může také identifikovat tzv. VID (nepovinný), který rozlišuje původ programu. Pokud aplikace používá VID, musí být podepsána. U nepodepsaných aplikací je VID tvořen z nul (defaultní hodnota). [10]

4.3.3 Data Caging

Třetím konceptem architektury Platform Security je model přístupu k souborům. Data Caging se využívá k ochraně důležitých souborů. Vychází z myšlenky uložení souboru společně s aplikací v jejím privátním adresáři. Hlavním cílem je vytvořit pro každou aplikaci část souborového systému, která bude chráněna před ostatními procesy. Integrita systémových souborů je důležitou součástí celkového pohledu na bezpečnost operačního systému Symbian.

Mnoho systémových souborů má zásadní vliv na funkcionalitu systému, která v tomto pojetí znamená ochranu integrity těchto souborů. Uživatelské soubory musí být také chráněny. Systém musí chránit program a zamezit případným přístupům k systémovým nebo důvěrným údajům.

Všechny soubory nemusí být nutně chráněny. Data Caging je aplikován v případě potřeby. Soubory lze „uzamknout“ do soukromé oblasti, a tím zabezpečit integritu.

Souborový systém Symbianu s příslušnými oprávněními je v následující tabulce. [9]

	funkce	oprávnění nutné pro čtení	oprávnění nutné pro zápis
\sys	Je přístupný pro zápis programů s TCB. Ke čtení je nutné právo AllFiles.	AllFiles	TCB
\sys\bin	Zde jsou umístěny všechny spustitelné soubory. Pokud je soubor v jiném umístění, systém ho odmítne spustit.	AllFiles	TCB
\sys\hash	Umístění pro hashe spouštěcích souborů nacházejících se na výměnitelných médiích.	AllFiles	TCB
\private\<otherSID>	Obsahuje soukromá data a programy uloženy v adresáři /private/otherSID.	AllFiles	AllFiles
\private\<ownSID>	Obsahuje soukromá data a programy uloženy v adresáři /private/ownSID.	žádné	žádné
\resource	Obsahuje veřejná data. Programy bez TCB mohou pouze číst.	žádné	TCB
\<other>	Obsahuje veřejná data. Programy bez TCB mohou pouze číst.	žádné	žádné

Obr. č. 22, Souborový systém [8]

4.4 Modifikace systému

Důvody modifikace

- Plný přístup do systému - nastane - li problém se systémem, tak možnost nápravy bez formátu zařízení je větší u modifikovaného zařízení.
- Možnost „patchování“ Symbianu - vše co Symbian od základu nabízí, nemusí být nutně korektní, nebo uživatelsky žádoucí.
- Instalace necertifikovaných (unsigned) aplikací. Zde odpadají jakékoliv problémy s podepsáním aplikací.

Následující kapitola mapuje možnosti modifikace operačního systému Symbian. Jedna z modifikací využívá chyby systému a obchází aktivní Platform Security. Druhá modifikace je schopna plnohodnotně deaktivovat Platform Security. Novinkou je modifikace, která si je schopna podmanit celý firmware mobilního zařízení.

Způsoby lze obecně rozlišit:

- modifikace při aktivním Platform Security;
- modifikace při deaktivovaném Platform Security;
- flashování již modifikovaného Firmware;

4.4.1 Modifikace při aktivním Platform Security

Modifikace prvního typu není tedy prolomení Platform Security jako celku, ale pouze odemknutí systémových složek (sys, resource, private). Zjednodušeně řečeno si systém myslí, že tyto systémové složky jsou naprosto normální. Platform Security je ale stále aktivní. Nevyužívá se žádného python skriptu apod. Princip spočívá v „chybě“ Symbianu, kdy systém zná pouze jednotky C, D, E a Z.

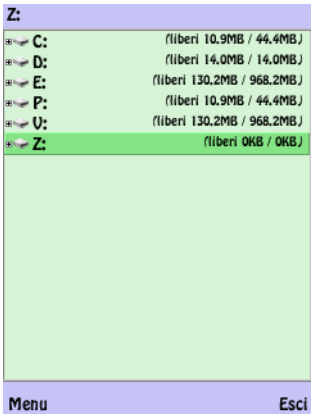
Význam diskových jednotek v Symbian OS je následující:
C:\ - je paměť telefonu kam se ukládají data;
D:\ - je paměť RAM - jedná se o RAM disk - je možné editovat, ale po restartu se data mažou;
E:\ - pamětová karta;
Z:\ - pamět kde je OS (ROM) – nelze editovat (zde je uložen firmware);

Po aplikaci modifikace využívající např. aplikaci Hellocarbide, Symbian zobrazuje navíc jednotku Y:\. Disk Y:\ je sektor RAM.

Na Y:\ se vytvoří složka sys\bin a v ní patchovaný installserver. Konkrétní installserver po restartu načte z disku Y:\ místo načítání z disku Z:\, odkud by se za normálních okolností načítat měl. V této situaci stačí přemapovat jednotky.

K změnám disků slouží aplikace Mapdrives, která emuluje disk Y:\ na zařízeních, kde se běžně nezobrazuje.

Na následujícím obrázku jsou přemapované (virtuální) diskové oddíly zobrazeny pomocí aplikace X-plore.



Obr. č. 23, Přemapované jednotky [10]

Symbian OS není schopen poznat, že se nejedná o jeho disk a načítá všechny *exe a *dll soubory z „falešného“ disku Y:\.

V souboru efile.exe je nadefinováno, že složky private, sys a resource mají být uzamčené. Po vyhledání řetězce v efile.exe je možné zjistit, co se „patchuje“. Posloupnost v HEX zápisu souboru efile.exe je uvedena níže.

SnR:sys\bin\efile.exe:5C005200DFFFDFFF450053004F0055005200430045005C00DFFF00005C0050
0052004900:2000520020FF20FF200053004F0055005200430045005C00DFFF00005C00200022002900

Podrobnější vysvětlení řetězců je uvedeno v kapitole 5.2.

4.4.2 Modifikace při deaktivovaném Platform Security

Druhou možností je plné odstavení Platform Security. Na prolomení tímto způsobem se používá např. aplikace Hellocarbide. Hellocarbide je v principu python skript implementován do *sis aplikace podepsaný OPDA certifikátem garantující TCB oprávnění. Python skript je součástí všech aplikací jako jsou např. Rompatcher a SecMan. Více o skriptech níže.

Aplikace při bootování zařízení patchuje proces Superpage a tím deaktivuje Platform Security. Modifikace tohoto typu se projeví např. tím, že při spuštění libovolného správce úloh všechny aplikace mají plný přístup do systému.

U starších firmware je možné modifikovat za použití tzv. Quick Hack Kitu. Modifikace formou Quick Hack kitu funguje na vybraných modelech s operačním systémem verze 9.1 a 9.2. Záleží také na verzi firmwaru v zařízení. Quick Hack Kit je balík, jenž obsahuje instalační soubory:

- BiNPDA Security manager (SecMan) – s pomocí tohoto programu lze instalovat většinu aplikací. Zároveň umožňuje aktivaci/deaktivaci Platform Security. Pomocí něj je zároveň dokončeno kopírování InstallServeru do C:/sys/bin. Aplikace umožňuje vytvoření tzv. root certifikátu.
- InstallServer 9.x - verze InstallServeru závisí na konkrétním zařízení, v případě nekorektnosti nepůjde instalovat ani odinstalovat žádná aplikace.
- CapsOff Driver 9.x - Python Ovládá aplikace CapsOFF a CapsON

Po instalaci všech aplikací a vytvoření root certifikátu je v C:/resource vytvořen SwiCertstore/dat/0000001, který umožňuje instalaci nepodepsaných aplikací. Opětovná aktivace Platform Security je možná opět přes SecMana.

Tohoto lze dosáhnout více postupy. Jeden z nich je pomocí CapsOFF + CapsON. Aplikace CapsON/OFF zpracovává skript napsaný v jazyce Python.

Jazyk Python je objektový jazyk, ve kterém lze psát aplikace pro Symbian OS. Takové aplikace lze vytvářet a spouštět přímo v zařízení. Zároveň lze v zařízení spouštět pythonské skripty, které jsou jádrem každé aplikace, ale mohou fungovat i samostatně. Skripty je možné vykonávat v konzoli PythonScriptShell. [3]

Python, o kterém je řeč, je interpretátor programovacího jazyka Python pro Symbian S60 3rd. Je možné ho přirovnat k Java emulátoru, který je v současných telefonech součástí standardního firmware.

Pro správnou funkčnost Python aplikace obvykle potřebuje importovat moduly - ty jsou různé podle toho, jaké funkce má aplikace vykonávat. Nejběžněji používané moduly jsou obsažené v sbornících modulů - jsou to tzv. ModulePacky nebo RightPacky. Aplikacím obvykle nestačí základní moduly Pythonu a je nutné potřebné moduly samostatně doinstalovat.

4.4.3 Komunikace mezi mobilním zařízením a PC

Propojením mobilního zařízení a PC lze rozšířit možnosti použití a dále do značné míry zjednodušit a zefektivnit práci. Synchronizační aplikace obvykle umožňují přístup k internetu, synchronizaci kontaktů, správu SMS a emailu. Možností, jak připojit zařízení, je několik.

Přímé propojení kabelem

V minulosti se jednalo o jediný efektivní způsob, jak zařízení propojit k PC. V dnešní době se stále používá, neboť často je jedinou dostupnou možností (v případě, že PC nemá wifi, bluetooth ani IrDa).

Komunikace je v tomto případě analogová a kabel je omezen délkou. Nevýhodou je fakt, že každé zařízení má obvykle své vlastní komunikační rozhraní, a proto je kabel nepřenosný (pro komunikaci mobilu a PC se musí využít jiný kabel než pro komunikaci mobilu a PDA).

Infračervený přenos

Princip přenosu informací pomocí infračerveného záření, byl poprvé otestován v roce 1993. Jde o technicky jednoduché a levné zařízení s překvapivě dobrými komunikačními výsledky. Dnes se používá spíše okrajově z důvodu rychlosti. [11]

Bluetooth

Komunikace probíhá na veřejné frekvenci v pásmu 2,4 GHz, není nutná přímá viditelnost komunikujících zařízení (některá jsou dokonce schopna komunikovat i přes několik zdí). Přenosová rychlost je okolo 1 Mb/s, ale norma Bluetooth 2 umožňuje dokonce až 12 Mb/s. Dosah signálu obvykle bývá 10-20 metrů, ale může být i větší. Výhodou je, že většina současných mobilních zařízení (ať už mobilů, PDA, MDA či notebooků) je vybavena Bluetooth rozhraním.

Paměťové karty

V mobilních telefonech se nejčastěji setkáváme s kartami SD / MMC a MemoryStick – méně pak s CompactFlash či MicroDrive od IBM. U smartphonů, MDA, PDA a MP3 přehrávačů je využití paměťových karet převážně pro uchovávání dat (aplikací, textů, hudby, apod.). U Nokia N-Gage je využití zejména pro uchovávání her.

WiFi

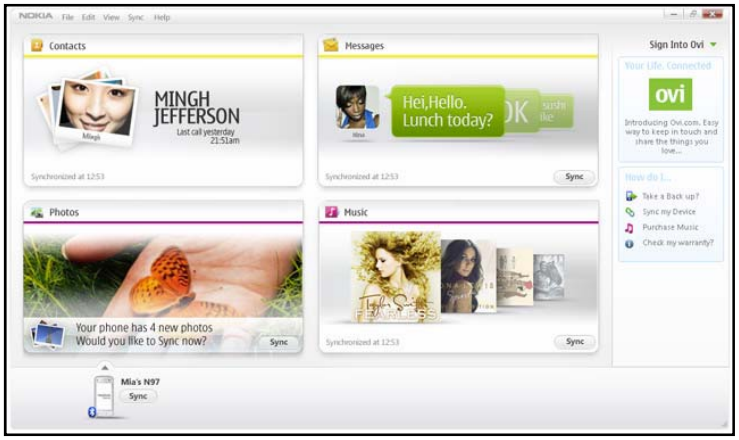
Funkčnost je podobná jako u Bluetooth – tedy obě technologie pracují na stejné frekvenci 2,4 GHz. Ostatní parametry jsou odlišné. Například dosah je až 100 metrů a komunikační rychlost je více jak desetinásobně vyšší než u Bluetooth. Největším nedostatkem je značná energetická náročnost, která u stávajících akumulátorů obvykle způsobuje rychlý úbytek energie. [11]

Všechny zmíněné způsoby připojení jsou hlavním kamenem synchronizačních procesů a transformací dat. Existuje několik programů, které využívají připojení prostřednictvím výše zmíněných metod a umožňují tak správu obsahu mobilního zařízení. Jedním z nich je software od společnosti Nokia s názvem PC Suite a novější verze Ovi Suite.

Nokia PC Suite – Ovi Suite

Většinou všechny modely nabízí synchronizaci dat s počítačem prostřednictvím některého z komunikačních rozhraní. Pro tyto účely vyvinula společnost Nokia program PC Suite, jež komunikaci mezi telefonem a počítačem zajišťuje. Během roku 2009 byl PC Suite nahrazen Ovi Suite (přejmenováno). Ovi Suite je funkcemi totožný s PC Suite, jen je upraveno uživatelské rozhraní.
Aplikace zajišťuje automatický přenos dat mezi telefonem a PC. S její pomocí lze připojit zařízení bezdrátově či pomocí kabelu. Rovněž umožňuje připojení k internetu.

V Nokia Ovi Suite je možná správa hudby, zpráv, kontaktů a obrázků. Software také poskytuje důležitou funkci v podobě zálohování obsahu mobilního zařízení. Ovi Suite je bezpodmínečně nutný pro korektní fungování aplikace Nokia Maps. Pro běžného uživatele je Ovi Suite velkým zjednodušením, ale erudovanější uživatel přejde pravděpodobně k jinému způsobu synchronizace.



Obr. č. 24, Ovi Suite [4]

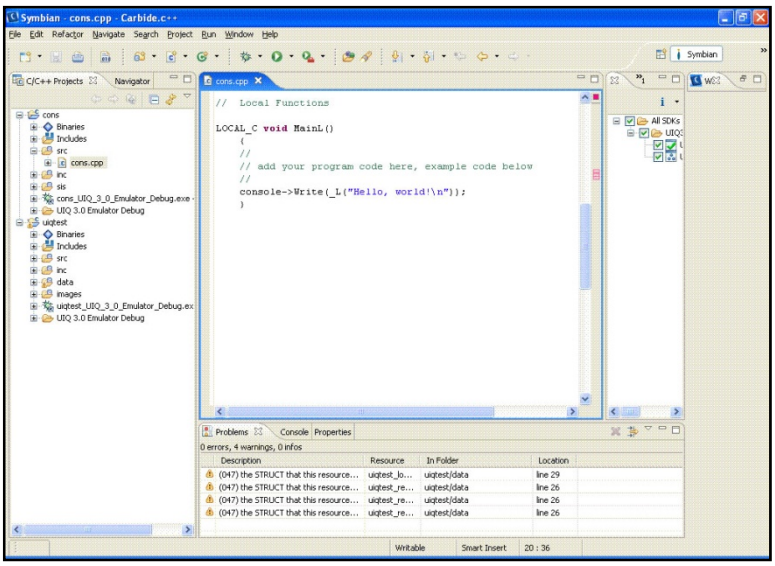
Obr. č. 25, PC Suite [4]

Prostředí

Oficiální vývojové prostředí pro Symbian OS se nazývá Carbide C++. V tomto prostředí je možné psát kód v syntaxi jazyka C++ obohacený o konstrukty specifické pro objektové programování (např. haldy). Kód zde napsaný, je možné spouštět, testovat a odlaďovat (debuggovat) pomocí aplikačních nástrojů, které jsou implementovány v Carbide C++.

Součástí je také debugger - aplikace AppTrk, jenž je možné spouštět přímo v zařízení. AppTrk je *sis aplikace vyvinutá stejně jako Carbide C++ firmou Nokia. Umožňuje nahlížení do registrů programů, paměti telefonu, procesů a také změnu dat.

Pro korektní práci s AppTrk je nutné mít zařízení propojené s PC. Propojení je možné realizovat kabelem nebo přenosem Bluetooth. Je žádoucí také správně nastavit komunikační port. Pokud spojení funguje, je aplikace AppTrk schopna komunikovat přímo s prostředím Carbide C++ (není nutná synchronizace prostřednictvím Nokia PC suite atd.) Prostředí Carbide C++ je na následujícím obrázku. [14]



Obr. č. 26, Prostředí Carbide C++ [9]

5 Výsledky a diskuse

Následující kapitola shrnuje výsledky z praktické analýzy modifikací. Zároveň je uvedena demonstrace vytvoření modifikace pro program ROMpatcher.

5.1 Modifikační aplikace

CapsON + CapsOFF

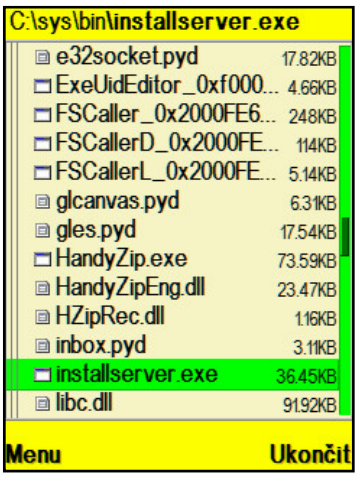
Jádro tvoří pythonský skript a aplikace, která ho spouští. Součástí je také knihovna CProfDriver_SISX.dll, jež je umístěna v C:/sys/bin. Tato metoda sama o sobě neumožňuje instalaci nepodepsaných aplikací. Funguje jako správce pythonského skriptu.

CapsON/OFF „pouze“ umožní přidělit aplikaci neomezená oprávnění. Po restartu zařízení, je bezpečnostní mechanismus opět aktivován, a proto není nutné CapsON/OFF vypínat ani nijak odstraňovat.

Je pochopitelné, že Nokia usilovně pracuje na znemožnění modifikací podobného typu. Dnešní zařízení obsahují firmware, na kterých je však zatím nemožné modifikovat OS. Během existence OS Symbian vznikla poměrně velká základna uživatelů, kteří mu rozumí a budou schopni dříve nebo později najít způsob opětovné modifikace. Zařízení obsahující novější verze Symbianu (např. verzi 9.3 a výš) lze modifikovat metodou pomocí aplikace HelloOX2. Pro použití této metody je nutné vlastnit OPDA certifikát.

Výše zmíněnou aplikaci HelloOX2 je nutné podepsat OPDA certifikátem. Po instalaci a spuštění aplikace se mapují jednotky, do zařízení se nahraje root certifikát, Rompatcher atd. Výsledkem je zpřístupnění a možnost modifikace systémových složek Symbian OS.

Zpřístupnění C:\sys\bin je znázorněno na následujícím obrázku. [27]



Obr. č. 27, Zpřístupnění C:\sys\bin [9]

ROMpatcher

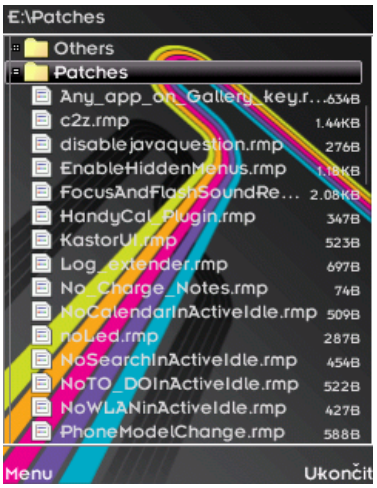
ROMPatcher je aplikace, která jednoduše a bezpečně umožní patchovat ROM telefonu. Aplikace rovněž využívá python skriptu. V zásadě pomocí ROMpatcheru lze vytvářet patche na téměř cokoliv. Aplikace namapuje ROM do paměti RAM a poté ji upraví. Nejedná se o zásahy přímo do firmware. Veškeré úpravy tedy nejsou trvalé a restart telefonu jej vrátí opět do původního stavu. ROMPatcher dokáže nahradit aplikaci CapsOFF / ON, protože dokáže také vypínat ochranu systému.

5.2 Praktické využití modifikací

V následující kapitole se autor věnuje praktickým využitím modifikací. Jelikož společným jmenovatelem modifikací při deaktivovaném Platform Security je python skript, je autorem použita aplikace ROMpatcher. ROMpatcher má veškeré náležitosti pro pachování Symbian OS, a tudíž je ideální pro praktickou demonstraci.

Aplikace ROMpatcher pracuje s patchy, které jsou uloženy v E:\Patches.

Patche je možné prostřednictvím ROMpatcheru aktivovat nebo deaktivovat. Samotný patch je soubor s příponou *.rmp (např. EnableHiddenMenus.rmp). Veškeré změny v systému při použití zmíněné metody jsou většinou do restartu mobilního zařízení. Existují však patche, které se spouští automaticky během bootování zařízení. Neexistuje zde pravděpodobně možnost trvalého poškození přístroje. Vybrané patche je možné vidět na následujícím obrázku.



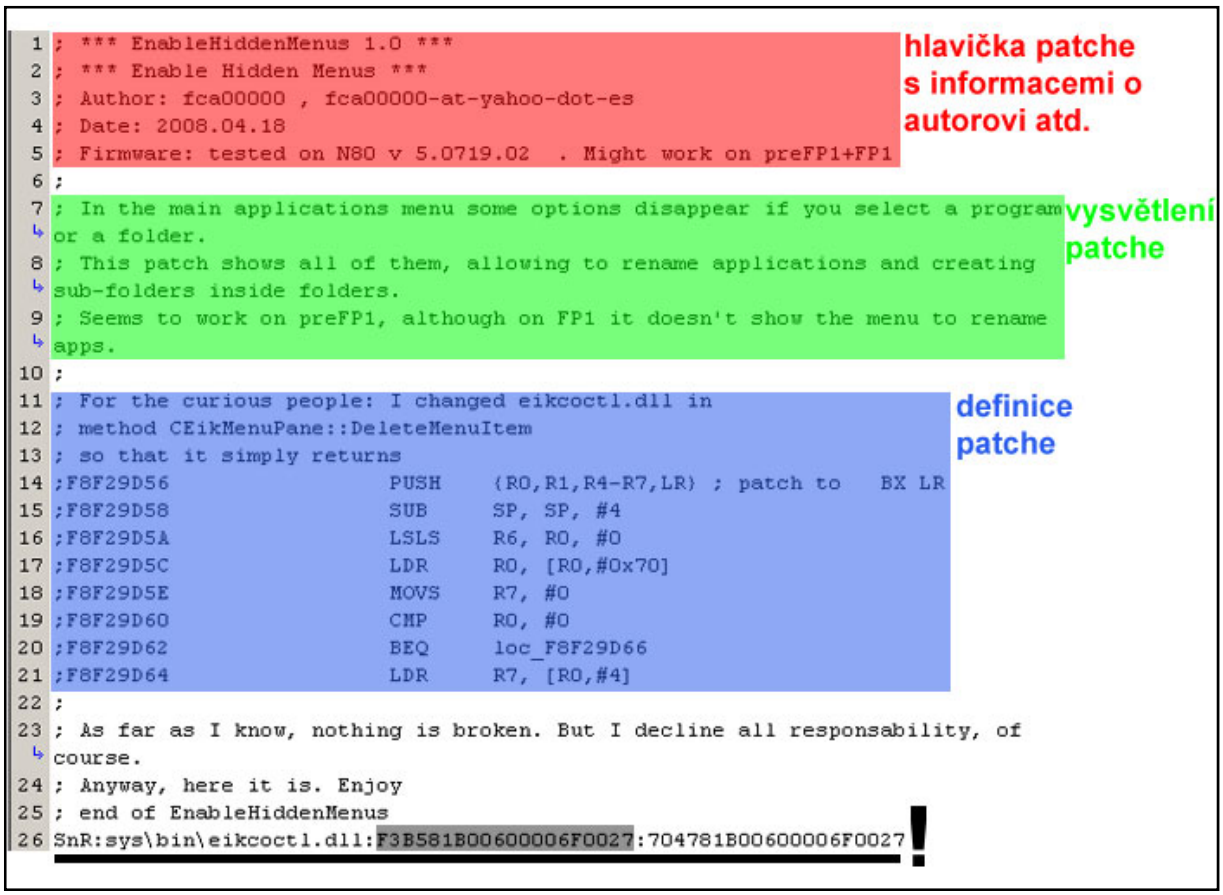
Obr. č. 28, Patche v E:\patches [9]

Patche mohou mít nejrůznější použití. Zde jsou uvedeny vybrané patche a jejich výhody, které přináší. Všechny níže zmíněné patche autor testoval a garantuje jejich funkčnost.

5.2.1 EnableHiddenMenus (zobrazení skrytého menu)

Patch zobrazí všechny volby jednotlivých ikon. V hlavním menu se nabídka u ikon mění podle toho, zda se jedná o aplikaci, nebo složku. Tento patch je schopen např. přejmenovávat aplikace, nebo vytvářet podsložky ve složkách. Autor testoval na zařízení s Feature Pack 1, je tedy možná diferenciace chování u jiných firmware (FP2).

Na následujícím obrázku je obsah EnableHiddenMenus.rmp a vysvětlení kódu.




```
1  ; *** EnableHiddenMenus 1.0 ***
2  ; *** Enable Hidden Menus ***
3  ; Author: fca00000 , fca00000-at-yahoo-dot-es
4  ; Date: 2008.04.18
5  ; Firmware: tested on N80 v 5.0719.02  . Might work on preFP1+FP1
6  ;
7  ; In the main applications menu some options disappear if you select a program
   ↳ or a folder.
8  ; This patch shows all of them, allowing to rename applications and creating
   ↳ sub-folders inside folders.
9  ; Seems to work on preFP1, although on FP1 it doesn't show the menu to rename
   ↳ apps.
10 ;
11 ; For the curious people: I changed eikcoctl.dll in
12 ; method CEikMenuPane::DeleteMenuItem
13 ; so that it simply returns
14 ;F8F29D56                PUSH    {R0,R1,R4-R7,LR} ; patch to   BX LR
15 ;F8F29D58                SUB     SP, SP, #4
16 ;F8F29D5A                LSLS    R6, R0, #0
17 ;F8F29D5C                LDR     R0, [R0,#0x70]
18 ;F8F29D5E                MOVS    R7, #0
19 ;F8F29D60                CMP     R0, #0
20 ;F8F29D62                BEQ     loc_F8F29D66
21 ;F8F29D64                LDR     R7, [R0,#4]
22 ;
23 ; As far as I know, nothing is broken. But I decline all responsability, of
   ↳ course.
24 ; Anyway, here it is. Enjoy
25 ; end of EnableHiddenMenus
26 SnR:sys\bin\eikcoctl.dll:F3B581B00600006F0027:704781B00600006F0027!
```

Obr. č. 29, Kód EnableHiddenMenus.rmp [10]

Důležitou částí kódu je poslední řádek s vykřičníkem. Zde je uvedeno nahrazení řetězce F3B581B00600006F0027 řetězcem 704781B00600006F0027 v knihovně eikcoctl.dll.

Podrobnější vysvětlení bude uvedeno v kapitole 5.2.3.

5.2.2 Open4All (přístup do systémových složek)

Je jeden z nejpraktičtějších patchů na Symbian OS S60. Patch funguje na způsob CapsOFF. Dokáže přidělit správcům souborů (např.X-Plore) práva přístupu do systémových složek. Princip fungování Open 4All je uveden na obrázku níže.

```
; *** Patch: Open4All ***
; Author: wadowice
; Date: 29-Jan-09
;
; This patch open branch c:\sys\bin for all file navigators.
; Must hack your handy by use of DeltaFoX mehod.
; Must install ROMpatcher and then copy this patch-file at e:\patches\Open4All.
↳rmp
; Runs ROMpatcher and Apply
; MODO not useful now.
; Thank-you to WiTch3d, DeltaFoX, Zorn, FCA00000
SnR:sys\bin\efile.exe:5C005200DFFFDFFF450053004F00 55005200430045005C00DFFF00005
↳C00500052004900:20005 20020FF20FF200053004F005500520043004500 5C00DFFF000
↳05C00200022002900
```

Obr. č. 30, Kód Open4All.rmp [10]

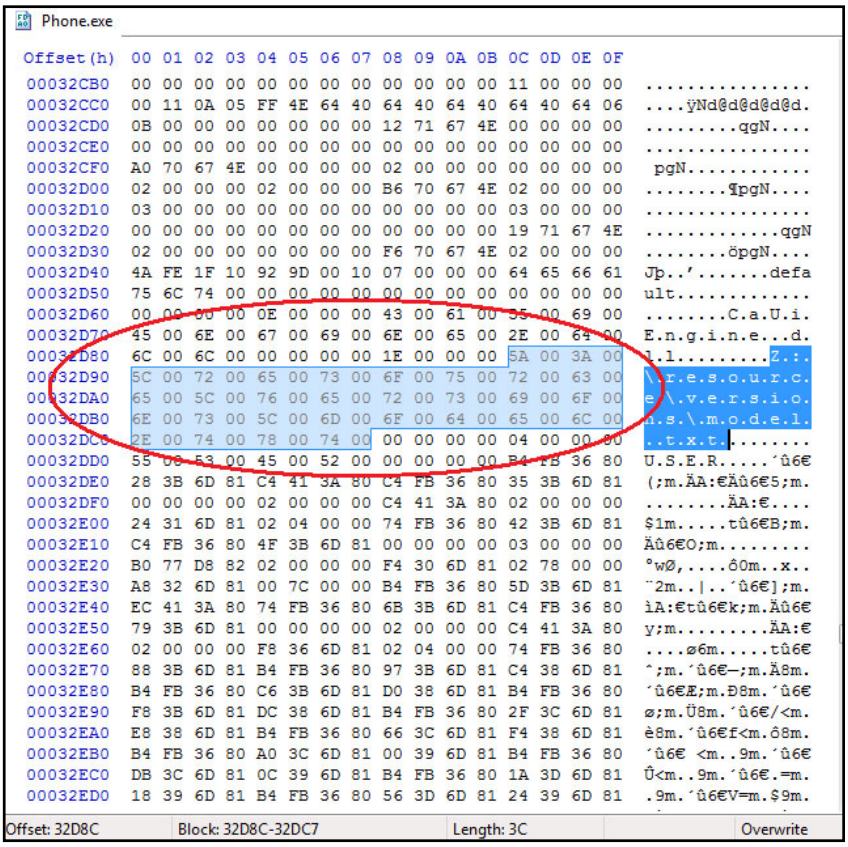
Opět se nahrazuje řetězec. Tentokrát však v souboru efile.exe.

5.2.3 Vytváření vlastních patchů

Na základě předešlých informací, orientaci v souborech a jejich významu, je možné vytvořit jakýkoliv patch. Je zde nutný předpoklad toho, co má patch přesně vykonávat a s jakými daty. Autor si dal za cíl změnit název (model) mobilního zařízení. Respektive po zadání *#0000# na úvodní obrazovce vypíše např. „Nokia N95“. Po aplikaci patche bude změněn model telefonu na libovolný řetězec omezený na 20 znaků. V tomto případě bude změněn na „Nokia N99“.

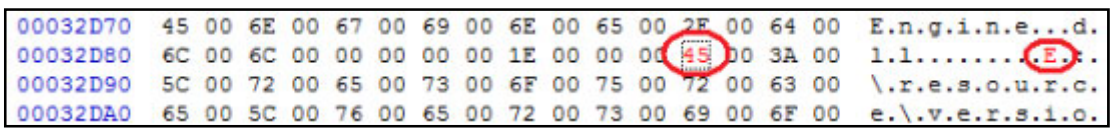
Ke korektnímu čtení phone.exe umístěného v Z: \sys\bin, je potřeba libovolný HEX editor. Je možné využít např. PsPad.

Samotný model mobilního zařízení je uložen v Z:\resource\versions\model.txt. Na tento soubor odkazuje řetězec v phone.exe.



Obr. č. 31, Nalezení řetězce [10]

Na předchozím obrázku je uvedeno nalezení řetězce Z:\resource\versions\model.txt a kód jemu příslušející. Při změně Z:\resource\versions\model.txt na E:\resource\versions\model.txt (nyní je soubor umístěn na paměťové kartě) se upraví HEX kód z 5A na 45 (Obr. č. 32).

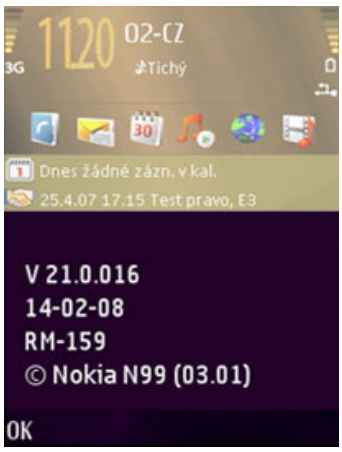


Obr. č. 32, Modifikace [10]

Patch může tedy vypadat následovně:

;ZmenaModeluTelefonu
;patch zmeni nazev (model) mobilniho zarizeni
;vytvořil vhyk 2010
; SnR:sys\bin\Phone.exe:5A003A005C007200650073006F007500720063006
5005C0076006500720073006900 6F006E0073005C006D006F00640065006
C002E00740078007400:45003A005C007200650073006F007500720063006
5005C0076006500720073006900 6F006E0073005C006D006F00640065006
C002E00740078007400

Patch začíná předponou SnR (Search and Replace - najdi a nahraď). Původní kód se nahradí modifikovaným a Symbian OS po zadání *#0000# spustí soubor phone.exe, v němž je změněno umístění souboru model.txt (nyní je umístěn v E:\resource\versions\model.txt). Výsledek může vypadat takto:



Obr. č. 33, Výsledek modifikace [9]

Modifikace za použití debuggingu

V Symbian OS existuje DProcess::DoHasCapability(TCapability , char const). Je umístěn v paměti například na F80478BC a říká: F8047968 BL log_missing_capabilities (F80458D8).

obsah F80458D8:

…

F8045930 LDR R0, =pSuperPage

F8045934 LDR R0, [R0]

F8045938 LDR R0, [R0,#0x148]

F804593C TST R0, #2

F8045940 BEQ loc_F804597C

F8045944 ADR R1, aError

F8045948 MOV R0, R1

…

Jedná o data na pSuperPage +0x148 a kontroly druhého bitu. Pokud je druhý bit nastaven, oprávnění vyvolá chybu. Když není, vytvoří se log s chybovou zprávou, ale kontrola bude úspěšná. Je potřeba tedy změnit tuto hodnotu.

Na zařízení má pSuperPage hodnotu např. 0x60000000. Přes různé programy na odlaďování aplikací (debugging) lze zjistit, že na adrese 0x60000148 je uložena hodnota 0x1E.

Po výpisu z paměti 0x60000000, nalezení hodnoty 0x0000001E ve výpisu a změnou příznaku (flagu) např. na 0x00000010, má aplikace potřebná oprávnění. Tato metoda je schopna plnohodnotně deaktivovat Platform Security.

Je-li program podepsán a nainstalován, oprávnění jsou uložena do interního adresáře. Když je program spuštěn a zkouší získat přístup ke službám, jsou oprávnění zkontrolována.

V případě, že oprávnění nesouhlasí, služba nebude spuštěna a vyvolá chybu. V podstatě se tedy přepisuje, aby chybějící oprávnění nevyvolalo chybu, ale pouze warning (log). [13]

6 Závěr

Při korektním a cíleném použití modifikací, je uživatel schopen rozvinout možnosti mobilního zařízení. Hlavním motivem pro modifikaci obvykle bývá možnost instalace nepodepsaných aplikací. Instalace nepodepsaných aplikací je však pouze zlomek potenciálu, jenž modifikace přinášejí.

S možností patche Symbianu se zařízení dostává plně pod kontrolou uživatele. Patch je schopen opravovat chyby v Symbianu a zároveň přinášet odlišné pohledy na použití systému.

Uživatel je schopen ovlivňovat funkcionalitu a zároveň ji rozšiřovat. Jako praktický příklad byl vytvořen patch na změnu modelu mobilního zařízení. Byl uveden pro demonstraci toho, jakých podob modifikace může nabývat. Jedná se o modifikaci, jejíž princip je totožný i pro pokročilejší modifikace typu Mapdrive (přemapuje diskové jednotky).

Primární cíl práce, tedy analýza bezpečnostních mechanizmů a způsoby jejich narušení, byl splněn. Byly zmapovány kritické oblasti systému a modifikace, které jsou těmito slabinami umožněny. Další cíl v podobě vytvoření vlastní modifikace byl uplatněn v praxi a odzkoušen na konkrétním zařízení (Nokia N73). Výsledkem vlastní modifikace byl patch, který změnil označení mobilního zařízení.

Zajímavé bude sledovat, jakým způsobem bude Nokia dále ovlivňovat použitelnost modifikací prostřednictvím vydávání nových (zatím) nemodifikovatelných firmware. Je možné, že s uvolněním Symbianu jako opensource, se investice do znemožnění modifikací omezí.

Stále důležitým faktorem je však bezpečnost systému. Může se například stát, že uživatel má plný přístup do systémových složek (má oprávnění) a je infikován virem, který automaticky posílá zprávy na vysoce zpoplatněná telefonní čísla.

Uživatel tedy sám musí zvážit, jaké má modifikace klady i zápory, a podle toho se rozhodnout.

Modifikace ve velké míře nejsou určeny pro běžné uživatele, kteří používají mobilní zařízení primárně k telefonování a ani netuší, že v jejich zařízení je implementován operační systém.

Erudovaný uživatel, si však rychle osvojí aplikaci modifikací a bezesporu využije přínosů při dalším používání mobilního zařízení.

7 Seznam literatury

7.1 Seznam zdrojů

[1] HARRISON, R. Programujeme aplikace pro Symbian OS v jazyce C++. Brno: Computer Press, 2006. ISBN 80-251-1243-8

[2] HEALTH, C. Symbian OS Platform Security. Wiley. 2008. ISBN: 339-586643824

[3] STICHBURY, J. Symbian OS Explained: Effective C++ Programming for Smartphones. John Wiley & Sons Ltd, 2005. ISBN: 978-0254021775.

[4] MORRIS, B. The Symbian OS Architecture Sourcebook. John Wiley & Sons Ltd, 2007. ISBN: 978-0473688560.

[5] POHL, O. Využijte svůj mobil naplno! Computer Press. květen 2006. ISBN 80-251-0887-2

[6] HYKEŠ,V. Symbian OS - Bakalářská práce, katedra informačních technologií, ČZU, 2007.

[7] AdMob. Q4 2009 Mobile Metrics August 2009 [on-line] Zveřejněno: 2.3.2010. (cit. 2010-03-21) Dostupné z WWW:< http://metrics.admob.com/wp-content/uploads/2009/09/AdMob-Mobile-Metrics-Aug-092.pdf />.

[8] KURUC, J. Nokia Ovi Maps, [on-line] Zveřejněno: 21.1.2010. (cit. 2010-03-21) Dostupné z WWW:<http://navigovat.mobilmania.cz/Clanky/AR.asp?ARI=114450>.

[9] Symbian a opensource, [on-line] (cit. 2010-01-14) Dostupné z WWW: <http://computerworld.cz/softwarel>.

[10] Platform Security, [on-line] (cit. 2010-01-14) Dostupné z <WWW: http://developer.symbian.com>.

[11] MÜLLER, B. From 0 to 0 day on Symbian, [on-line] Zveřejněno: 11.1.2010. (cit. 2010-03-21) Dostupné z WWW:<https://www.secconsult.com/files/SEC_Consult_Vulnerability_Lab_Pwning_Symbian_V1.03_PUBLIC.pdf>.

[12] Forum N73, [on-line] Zveřejněno: 8.7.2008. (cit. 2010-03-21) Dostupné z WWW:< http://forum.n73.eu>.

[13] Symbian Portal [on-line] Zveřejněno: 24.7.2009. (cit. 2010-12-1) Dostupné z WWW:<http://www.symbianportal.cz>.

[14] Imserba – The mobile forum [on-line] Zveřejněno: 16.5.2007. (cit. 2009-2-25) Dostupné z WWW:< http://www.imserba.com/forum/showthread.php?t=111351>.

[15] Symbian Freak [on-line] Zveřejněno: 28.6.2009. (cit. 2010-2-16) Dostupné z WWW:<http://www.symbian-freak.com>.

[16] Mobile 2 Day. 2009: Rekord bei Smartphone-Verkäufen [on-line] Zveřejněno: 5.2.2010. (cit. 2010-2-16) Dostupné z WWW:< http://www.mobile2day.de/news/news_details.html?nd_ref=44011&cid=nl>.

[17] NOSKA, Martin. Nová verze Symbianu chce konkurovat Androidu i iPhonu. [on-line] Computerworld, 2010 [cit. 17.1.2010] URL: <http://computerworld.cz/software/nova-verze-symbianu-chce-konkurovat-androidu-i-iphonu-5493>.

7.2 Seznam zdrojů obrázků

[1] http://galaxie.name/clanky/708.php

[2] http://metrics.admob.com

[3] http://www.mobilmania.cz

[4] http://www.stahuj.centrum.cz

[5] http://www.brunel.ac.uk

[6] http://palmare.idnes.cz

[7] http://www.symbian.com/developer

[8] vytvořeno autorem;

[9] zdroj autora (PC + datový kabel);

[10] http://forum.n73.eu

[11] http://www.mynokia.cz

[12] http://faizlive.com/ - přeloženo a upraveno;

[13] http://www.wmhelp.cz