mobile business

Lecture 10

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Information & Communication Security (WS 16)

Computer System Security

Prof. Dr. Kai Rannenberg

Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe-University Frankfurt a. M.

Agenda

- Introduction
- Security Threats
- Operating System Security
- Mobile Malware
- Improving Security

Introduction

2008 landmark judgement by German Bundesverfassungsgericht (BVerfG):

Basic right to confidentiality and integrity of IT systems

"1. Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme."

Stealthy infiltration of IT systems is problematic:

„2. Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. (...)"

BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333), www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

mobile business

Agenda

- Introduction
- Security Threats
  - Malicious Logic
  - Buffer Overflow
- Operating System Security
- Mobile Malware
- Improving Security

mobile business

Agenda

- Introduction
- Security Threats
  - Malicious Logic
  - Buffer Overflow
- Operating System Security
- Mobile Malware
- Improving Security

Malicious Logic

Definitions

- Is a set of instructions that cause a site's security policy to be violated.

  [M. Bishop, Introduction to Computer Security]

- A program implemented in hardware, firmware, or software, and whose purpose is to perform some unauthorized or harmful action.

  [ISO/IEC 2382-8]

- Hardware, software, or firmware capable of performing an unauthorized function on an information system.

  [National Information Systems Security (INFOSEC) Glossary 2000]

Malicious logic is also known as malicious code or **malware** (**Mal**icious soft**ware**).

Types of malware

- Trojan Horses
  - Programs with a covert purpose, non-spreading
- Viruses
  - Self-spreading program – it replicate relying on user activity
- Worms
  - Propagate autonomously from system to system
- Logic Bombs
  - Hidden code, triggered by external event

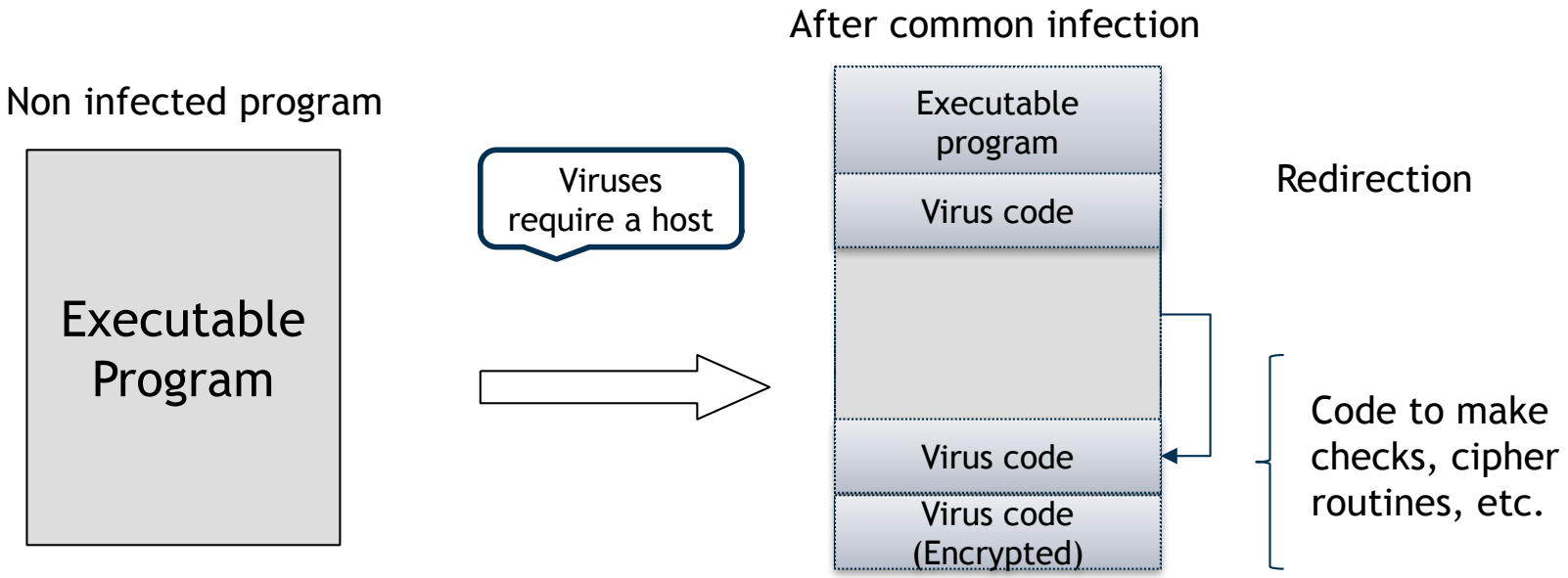
Trojan Horses

- Program with an *overt* purpose (known to user) and a *covert* purpose (unknown to user)
  - Often called a Trojan
  - Named by Dan Edwards in Anderson Report *[Anderson72]*
- Example: NetBus
  - Designed for Windows NT system
  - Victim uploads and installs it:
    - Usually disguised as a game program, or integrated within one
  - Acts as a server, accepting and executing commands for remote administrator
    - This includes intercepting keystrokes and mouse motions and sending them to attacker.
    - Also allows attacker to upload, download files

Viruses

Program that replicates itself, e.g. by inserting itself into one or more files, and that may perform some other action, too:

- *Insertion phase*: Virus is inserting itself into a file.
- *Execution phase*: Virus is performing some (possibly null) action.



Types of Viruses (1)

- Boot Sector Infector
  - Inserts itself into the boot sector of a disk
- Executable Infector
  - Infects executable programs, e.g. .EXE or .COM programs
  - May prepend itself (as shown) or put itself anywhere, fixing up binary so it is executed at some point
- Multipartite Virus
  - Can infect multiple platforms (e.g. either boot sectors or executables)
- TSR Virus (Terminate and Stay Resident)
  - Stays active in memory after the application is completed
- Stealth Virus
  - Conceals its presence on a system

Types of Viruses (2)

- Encrypted Virus
  - Is enciphered except for a small deciphering routine
- Polymorphic Virus
  - Changes its form each time it inserts itself into another program
- Macro Virus
  - Composed of a sequence of instructions that are interpreted rather than executed directly
  - Can infect either executables (Duff's shell virus) or data files (Highland's Lotus 1-2-3 spreadsheet virus)
  - Independent of machine architecture
- Retro Virus
  - Attacks anti-virus software present on the system

Worms

- A program that copies itself from one computer to another
- Origins: distributed computations
  - Animations, broadcast messages
- Segment
  - part of program copied onto workstation
  - processes data, communicates with worm's controller
  - Any activity on workstation causes segment to shut down.

Logic Bombs

- A program that performs an action that violates the site security policy when some external event occurs
- Example: program that deletes company's payroll records when one particular record is deleted
  - The "particular record" is usually that of the person writing the logic bomb.
  - If/when the person is fired and the payroll record deleted, the company loses *all* those records.

Example – Ransomware

It is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.

Example – ATM Attacks

- ATMs installed in non-branch areas with poor physical ATM security
- Low level of detection
- Malicious software physically install per ATM
- Approximately 2.5hrs

Source: [http://www.bankinfosecurity.com/]

Source: [SecurityIntelligence: ATM Malware: The Next Generation of ATM Attacks]

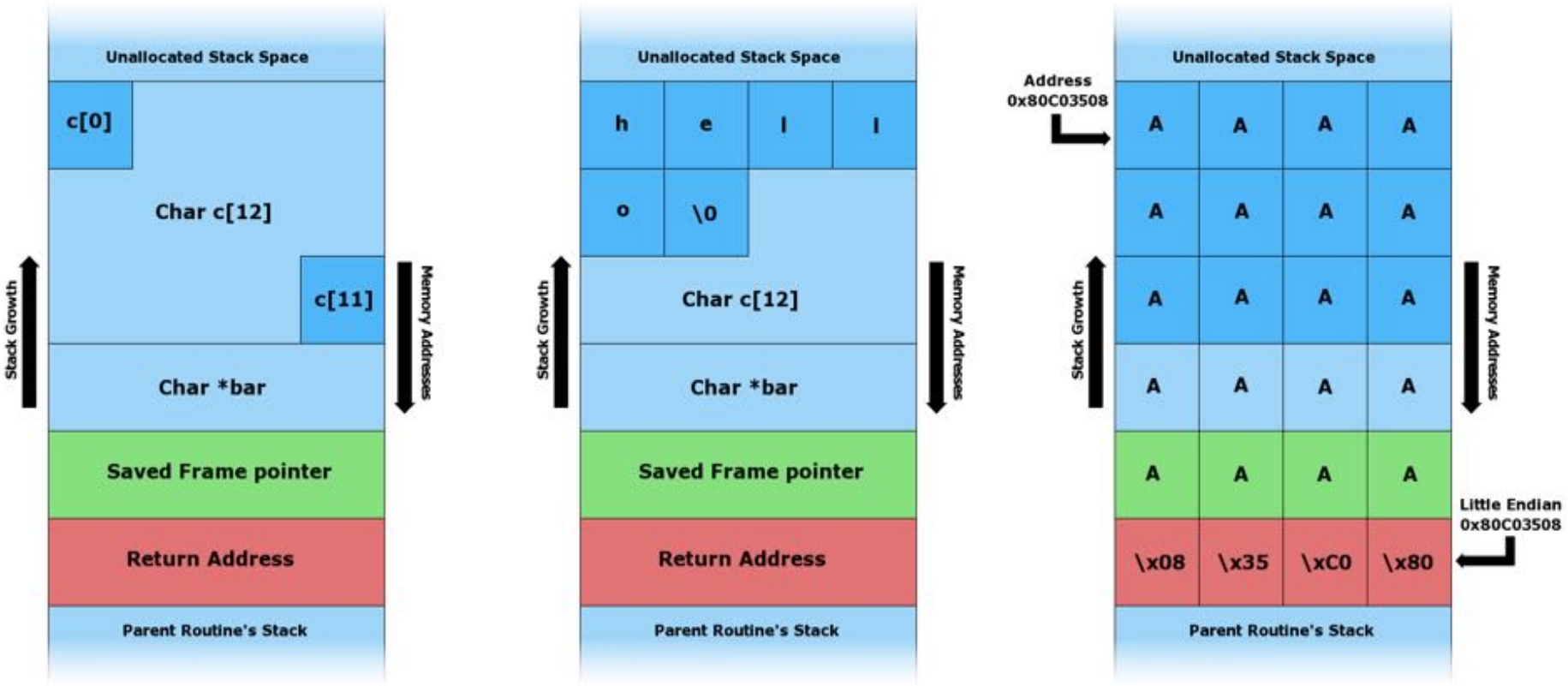
Agenda

- Introduction
- Security Threats
  - Malicious Logic
  - Buffer Overflow
- Operating System Security
- Mobile Malware
- Improving Security

Buffer Overflow (1)

- Buffer overflow software bug
  - data larger than the variable allocated for it
  - can overwrite a procedure return address in the procedure call stack in memory
- It offers attackers the ability to write arbitrary data to memory.
- Persisted for decades
  - Users do not bother to install patches supplied (free) by software vendors.
- Example of vulnerability that permits remote injection of hostile code, recruiting bot nets for later DDoS attacks

Buffer Overflow (2)



Before data is copied.

"hello" is copied.

"AAAAAAAAAAAAAAAAAA\x08\x35\xC0\x80" is copied.

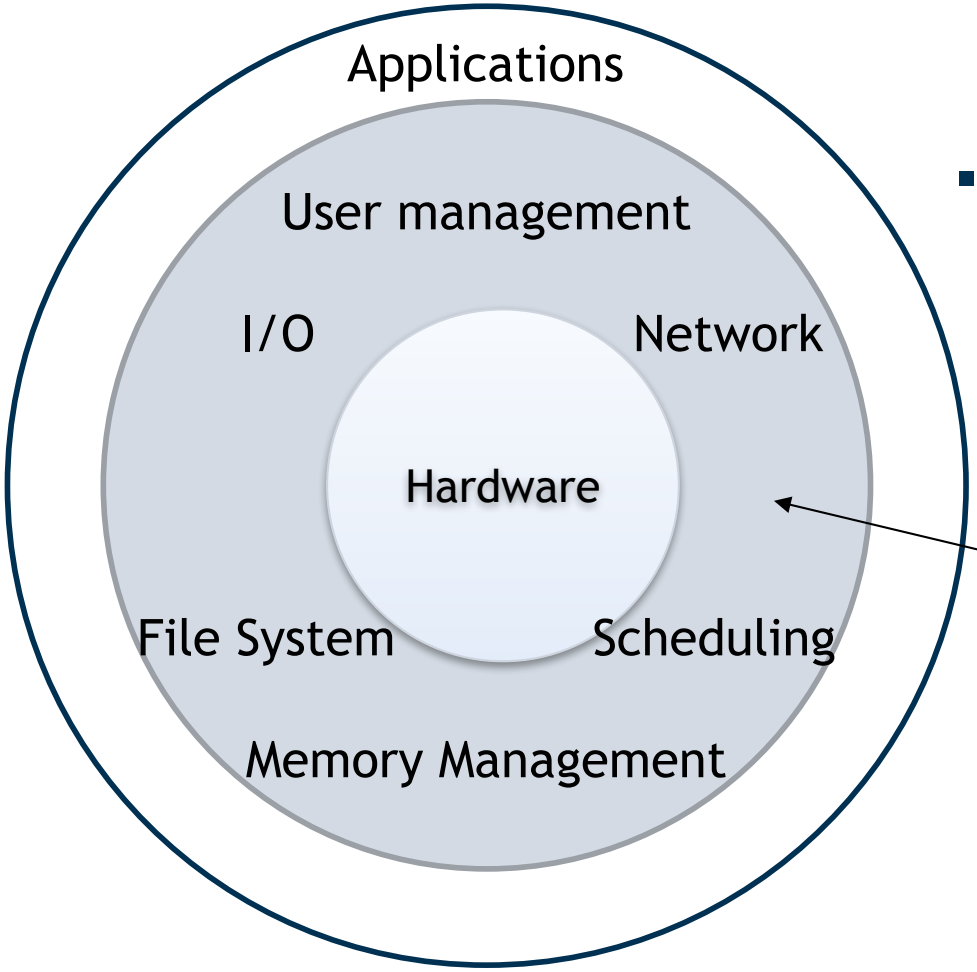
[Wikipedia]

mobile business

Agenda

- Introduction
- Security Threats
- Operating System Security
  - Unix
  - Windows
  - Mobile OSs
- Mobile Malware
- Improving Security

OS Security Considerations



- The whole code which is executed in the kernel is very security critical (supervisor mode!) .
- It is the target of a lot of attacks to gain root privileges by manipulating kernel functions.

OS Kernel

OS Security Control Mechanisms

- Identification
  - Recognition of human individuals
- Authentication
  - Secure confirmation of users' identifiers
- Access Control
  - Restricting usage of a service to authorized users
  - Sandboxing of apps
- Audit
  - Monitoring of system activities

mobile business

Agenda

- Introduction
- Security Threats
- Operating System Security
  - Unix
  - Windows
  - Mobile OSs
- Mobile Malware
- Improving Security

Unix Security Paradigm

- In the Unix operating system there are two parts:
  - Kernel
  - User space
- Any programming code in the kernel space has full access to the computer it is running on.
- Code running in the user space has access rights based on the User ID (UID) it is running under:
  - UID 0 is reserved for the super user or root and the kernel automatically gives this UID complete access.
- Note the difference between kernel and root access:
  - Kernel processes can access anything.
  - Root processes can order the kernel to access anything.

Unix Security Elements (1)

- IDs
  - User Identification number (UID)
  - Root/super user (UID 0)
  - Group Identification number (GID)
- Authentication
  - Password: /etc/passwd
    - User name (login name)
    - Password, encrypted
      - usually modified DES (or MD5, SHA…)
      - One way function, it is impossible to decrypt the password.
      - At login the entered password is encrypted and compared to file.
    - User id (number)
    - Login group id (number)
    - GCOS (Comment, usually real-life name)
    - Home directory
    - Program to be executed at login, usually shell

Unix Security Elements (2)

- Access Control
  - A file has owner and group id (sometimes several).
  - A process has owner and group id (sometimes several).
  - Kernel verifies permissions before executing system calls:
    - If owner uid=0 (root), everything is allowed
    - Otherwise the uid and gid of the process and object are compared in this order and permission for the operation is searched for based on owner, group and other (world) rights
- Auditing
  - Permanent Logging
  - Automatically recorded events
  - Manually set logging

mobile business

Agenda

- Introduction
- Security Threats
- Operating System Security
  - Unix
  - Windows
  - Mobile OSs
- Mobile Malware
- Improving Security

Windows Security Model

- Provides security controls access and auditing
- Implements the standard subject/object security model
  - Subject - process or thread running on behalf of the system or an authenticated user
  - Object – individually secured entity such as a file, pipe, or even a process. Access control may vary between different objects.
  - Kernel mode, User mode
- Controls applied to core OS elements like processes and sockets in addition to the more tradition file system elements (NTFS).
- Problems
  - Unexpected use of extensible elements like word macros or extensible DLL's
  - Unprotected file systems
  - Attempts at backwards compatibility with older version of Windows caused some security problems (NetBIOS and FAT).

Windows Security Elements (1)

- Identification
  - User Account
  - Security ID (SID) – A globally unique ID that refers to the subject (user or group)
- Authentication
  - Password, stored as hash value
  - Secure attention sequence CTRL+ALT+DEL
  - Security Accounts Manager

Windows Security Elements (2)

- Access Control
  - Object – Individually secured entity such as a file, pipe, or even a process
  - Rights – actions associated between object and subject (Read, write, execute, audit)
  - Access token – the runtime credentials of the subject
  - User Access Control (UAC) – administrative privileges not available by default at all times, but only after confirmation via UAC dialog box.
  - Access control list (ACL)
    - Associated with an object
    - Ordered list
    - Each access control entry (ACE) contains a subject and a right.
    - Evaluated by the security subsystem to determine access to protected objects
    - Discretionary ACLs control access
    - System ACLs control audit

Windows Security Elements (3)

- Auditing
  - Security Reference Monitor
  - Local Security Authority
  - Event Logger
  - If auditing applies and what is to be audited is determined by the Audit Policy

mobile business

Agenda

- Introduction
- Security Threats
- Operating System Security
  - Unix
  - Windows
  - Mobile OSs
    - Palm OS
    - PocketPC
    - Symbian
    - Linux
    - BlackBerry
    - Apple iOS
    - Android
    - Windows Phone 8
    - Firefox OS
- Mobile Malware
- Improving Security

mobile business

Once upon a time…

- Closed platforms
- No additional software could be installed.
- Limited functionality
- E.g., Java ME: restricted access

Mobile Devices Today

- Open platforms
- Lots of software can be installed:
  - For different purposes
  - From different vendors
- Communication with different protocols possible:
  - GSM/GPRS, UMTS
  - Bluetooth, Infrared, WLAN
- Private and confidential data can and will be stored on the mobile device.
- Camera is (in many cases) included.

Mobile Devices Today — Risks

- Risks of Malware
  - Viruses, Worms, Dialler, Trojan Horses, etc.
- Passwords can (and will most likely) be deactivated.
- External storage media enables potential attackers to steal private information.
- Different communication protocols can be used to attack device or steal data.
- Always connected
- Camera also introduces new risks:
  - Stealing paper based confidential information
  - Invasion of personal privacy

BlackBerry

- BlackBerry became a big problem in some countries:
  - United Arab Emirates: BlackBerrys are a "national security risk”.
  - India
  - Saudi Arabia
- (Reuters) - More than a million BlackBerry users may have key services in Saudi Arabia and the UAE cut off after authorities stepped up demands on smartphone maker Research In Motion for access to encrypted messages sent over the device.
- According to an internal note from the Indian communications ministry seen by the Economic Times in India, BlackBerry has the infrastructure for solutions that would allow agencies to track messages and monitor internet traffic, but had not provided "the architect of the solution as well as the communication path for the service" [http://www.security-technologynews.com/news/indias-blackberry-security-concerns.html].

- All of this does not address the security of the (proprietary) Blackberry Phone platform, e.g. its operating system.

mobile business

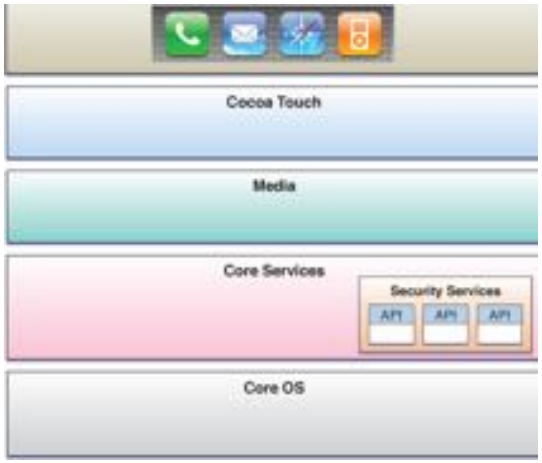
Apple iOS (1)

- The iOS security APIs are located in the Core Services layer.
- The iOS security implementation includes a daemon called the Security Server that implements several security protocols:
  - keychain items
  - root certificate trust management
- CFNetwork
  - High-level API that can be used by applications to create and maintain secure data streams and to add authentication information to a message.
- iOS provides process sandboxing:
  - An application running in iOS can see only its own keychain items and files.
- Digital signatures are required on all applications for iOS.
- Apple adds its own signature before distributing an iOS application.
- Each application is granted access permissions for certain system services when it's signed by Apple, Inc.

[http://developer.apple.com]

Apple iOS (2)

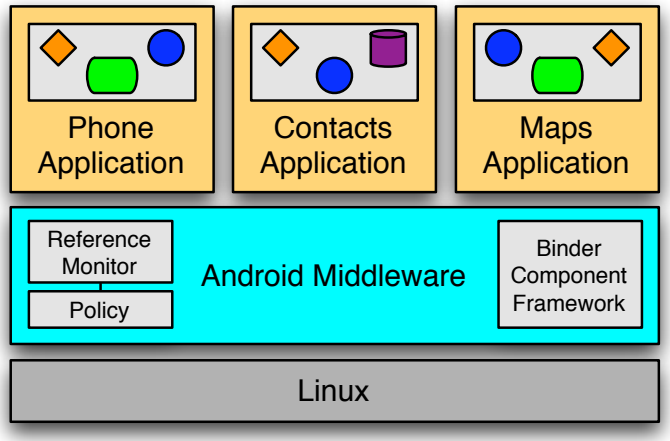
- System security
  - Secure boot chain
  - System Software authorization
- Encryption and data protection
  - Hardware security features
  - File data protection
- App security
  - App code signing
  - Runtime process security



- Network security
  - Industry standard networking protocols that provide secure authentication and encryption of data in transmission (SSL, TLS, VPN, Single Sign-on).
- Internet services
  - Apple's network-based infrastructure for messaging, synchronization and backup
- Device controls
  - Methods that prevent unauthorized use of device and enable it to be remotely wiped if lost or stolen
  - Passcode protection

Android

- A Linux platform programmed with Java and enhanced with its own security mechanisms tuned for a mobile environment
- Each application declares which permission it requires at install time.
- Android *permissions* are rights given to applications to allow them to do things like:
  - directly dialling calls (which may incur tolls),
  - disclosing the user's private data, or
  - destroying address books, email, etc.



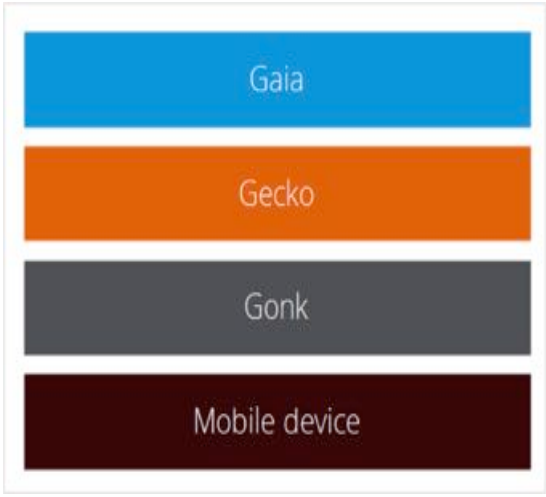
- When installed, applications are given a unique UID, and the application will always run as that UID on that particular device. The UID of an application is used to protect its data and developers need to be explicit about sharing data with other applications.
- Each process is running in its own address space (Dalvik virtual machine).
- The developer signs application .apk files, and the package manager verifies them.

Microsoft Windows Phone 8

- Data encryption
  - Support of several cryptographic algorithms, including AES, RSA, SHA1, SHA256,HMACSHA1, HMACSHA256, Rfc2898DeriveBytes
- Secure sockets layer (SSL) certificates
  - The Windows phone internet explorer shows a warning or error if the certificate is not valid or not issued by a trusted authority
- App management by Windows Phone app platform
  - Protect end user experience, especially
    - Avoid, that apps affect phone experience
    - Ensure, that a apps are easy to uninstall and that they uninstall completely
    - No access to the user's information without informing the user
    - No billable events without getting permission from the user
  - Application vetting
    - Apps required to go through the Windows Phone Store to be tested and digitally signed.
  - Application isolation
    - Developers use the Silverlight platform where the sandbox concept is used to provide an environment where applications have limited privileges.

Firefox OS (1)

- Firefox OS is an integrated technology stack consisting of four levels:
  - **Gaia**: the suite of web apps that makes up the user experience
  - **Gecko**: the application runtime layer that provides the framework for app execution
  - **Gonk**: the underlying Linux kernel, system libraries, firmware and device drivers that everything runs on top of
  - **The mobile device**: the mobile phone running the Firefox OS
- Security architecture
  - Multi-layered security model to mitigate exploitations risks at every level
  - Gecko as gatekeeper to enforce security policies designed to protect the mobile device from misuse



Based on [www.developer.mozilla.org]

mobile business

Firefox OS (2)

- Secure system deployment
  - Security measures are used throughout the technology stack.
  - File system privileges are enforced by Linux's access control lists (ACLs).
  - System apps are installed on a volume that is read-only (except during updates, when it is temporarily read-write).
- Secure system update
  - Update origin (verify the source location protocol:domain:port of the system update and manifest)
  - File integrity (SHA-256 hash check)
  - Code signature (certificate against a trusted root)
- App Security
  - Firefox OS limits and enforces the scope of resources that can be accessed or used by apps, while also supporting a wide range of apps with varying permission levels.

Based on [www. developer.mozilla.org]

mobile business

Agenda

- Introduction
- Security Threats
- Operating System Security
- Mobile Malware
- Improving Security
  - Security Enhancing Techniques
  - Security of kernels

Mobile Malware

- From traditional desktop to MOBILE
  - New mechanisms same purpose
    - Basic malware: very sucessful
    - Advanced: exploits, polymorphic code (=code mutates), botnets, crypto, …
  - Different goals
    - Fun
    - Fame???
    - $$$ Money $$$

Infection methods

- Social engineering: phishing
- Fake marketplace
- Repackaging an existing app and including the malware to generate a new infected version of the app
- Creating a legitimate app, and after a period of time when it has a huge number of downloads, the attacker release an update with the malware in it
- Executing a drive-by-download action, i.e., the app download their malicious payload after executing certain checks (e.g. is executed in a real device)
- Using malvertising to deceive users into clicking on a rogue advertisement that leads to an exploit

Example – Mobile Malware

- Eurograbber attack
  - 36 million euros were stolen
  - >30,000 victims
  - Netherlands, Spain and Germany
  - PC and mobile targeted
  - Hijack two-factor authentication (SMS-OTP)

mobile business

Agenda

- Introduction
- Security Threats
- Operating System Security
- Mobile Malware
- Improving Security
  - Security Enhancing Techniques
  - Security of kernels

mobile business

Agenda

- Introduction
- Security Threats
- Operating System Security
- Mobile Malware
- Improving Security
  - Security Enhancing Techniques
  - Security of kernels

Security Enhancing Techniques

- **Virus scanners** try to identify viruses according to a certain characteristic (virus signature) stored in a database.
- **Code Signing** helps to distinguish authorized code from other code.
- **A Trusted Operating Base** can then prohibit the execution of not authorized code e.g. viruses on a system.
- **Checksums and/or Encryption** make it possible to detect/avoid modifications done by a virus.
- **Intrusion Detection Systems (IDS)** monitor a system to detect processes which may be the result of a virus infection.
- **Heuristic virus scanners** try to identify a virus with a forecast about the runtime behaviour of code (sophisticated approach, but not really efficient).

mobile business

Agenda

- Introduction
- Security Threats
- Operating System Security
- Mobile Malware
- Improving Security
  - Security Enhancing Techniques
  - Security of kernels

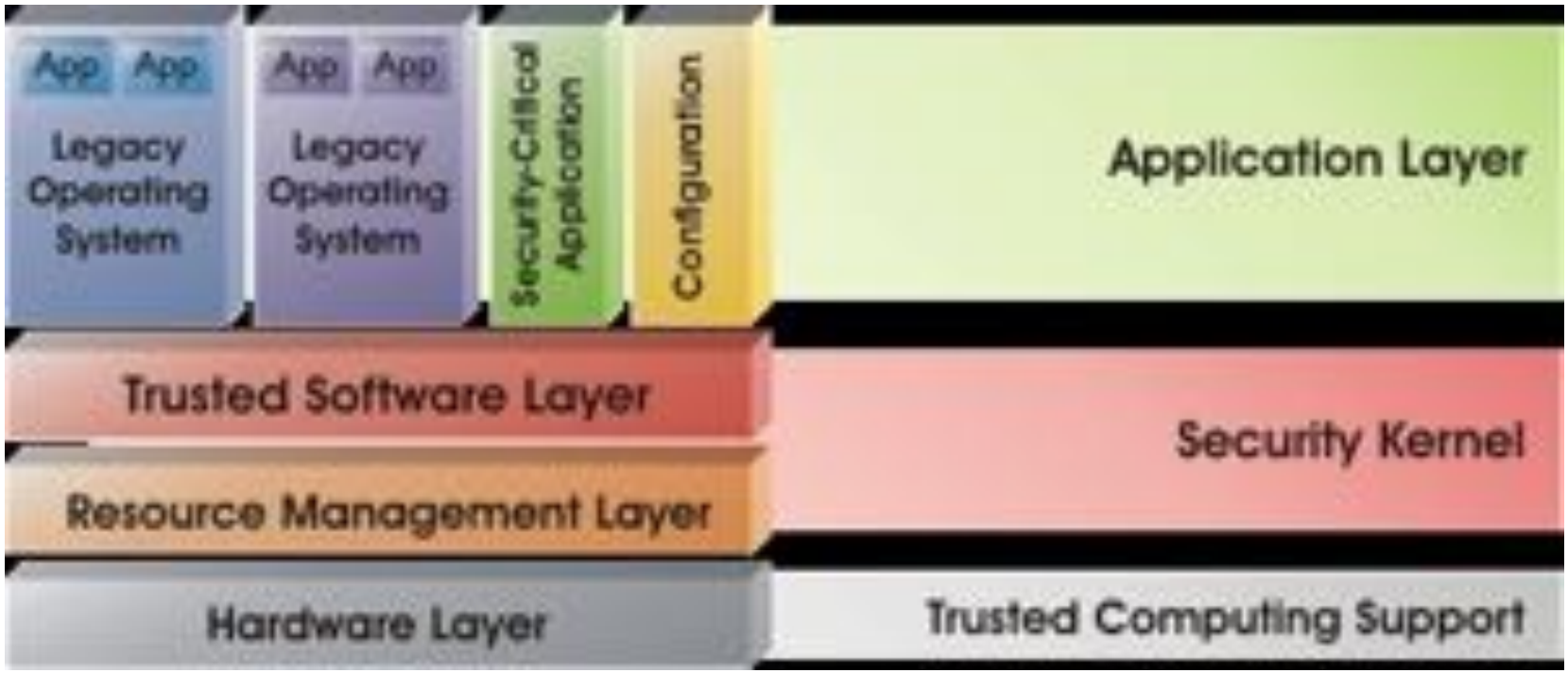
EMSCB

European Multilaterally Secure Computing Base (EMSCB)

- A trustworthy computing platform
- Employing open standards
- Solving many security problems of conventional platforms.
- Hardware functionalities provided by Trusted Computing
- Security kernel based on a microkernel
- Efficient migration of existing operating systems

[EMSCB]

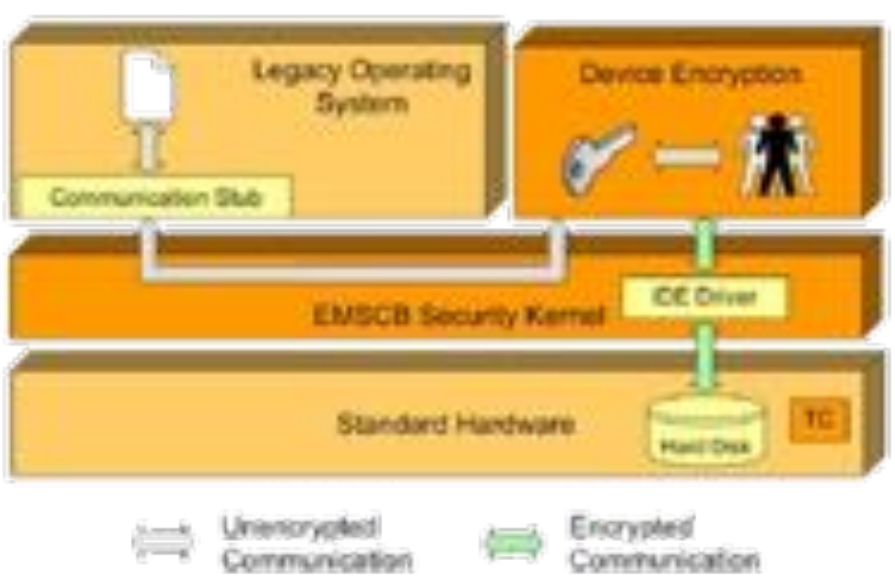
- Architectural Layers

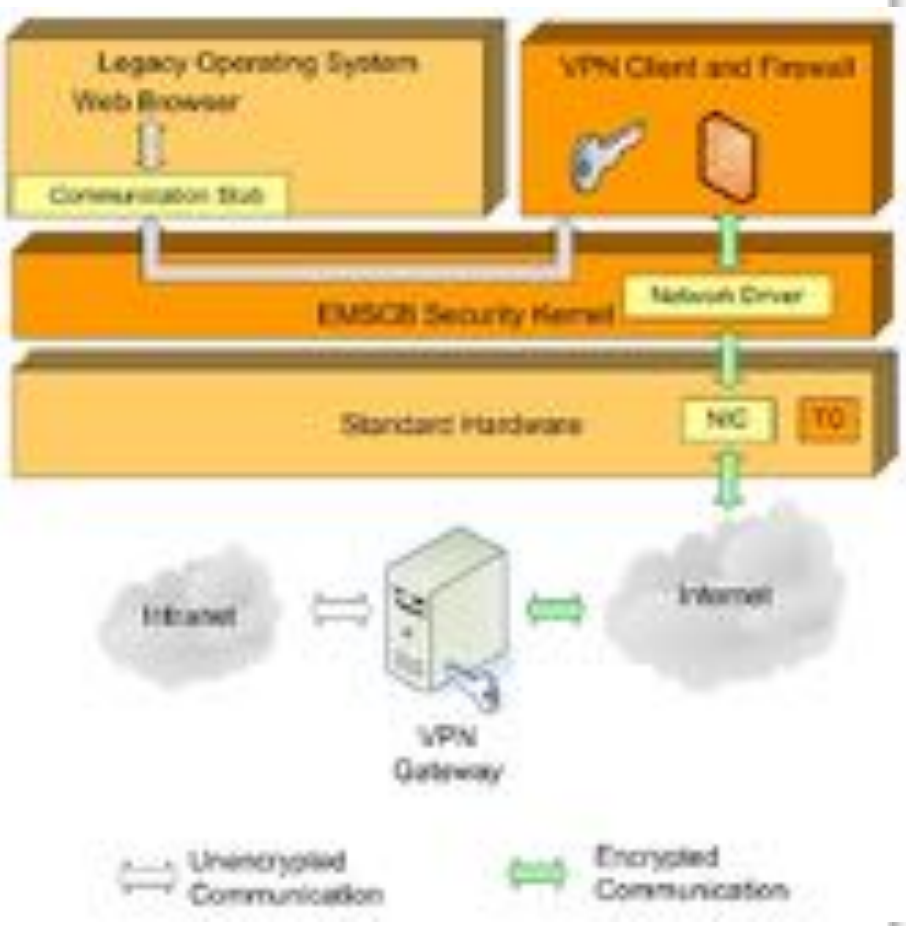


EMSCB: Turaya

- Implementation of EMSCB architecture
- Security and access policies
- Based on PERSEUS security framework
- L4 micro kernel
- Two prototypes as proof of concept (June 2006):
  - Turaya.Crypt: Device/drive encryption, transparent for user.
  - Turaya.VPN: Secure IPSec VPN-Client compatible with conventional VPN servers.

EMSCB: Turaya.Crypt Turaya.VPN





Example: BizzTrust

- BizzTrust is a secured plateform for smartphones and tablets.
- It has two workspaces: an open “personal” and a protected “business” workspace.
- Secure access to business resources via a secure VPN tunnel
- **TrustedObjects Manager (TOM):** a central place to remotely distribute firmware updates, security profiles, as well as the remote configuration of the devices.

[cybersecurity.rohde-schwarz.com]

References

- ***J.P. Anderson**: "Computer Security Technology Planning Study,"* ESD-TR-73-51, Vols I and II, NTIS AD758206, Hanscom Field, Bedford, MA (October 1972). http://csrc.nist.gov/publications/history/ande72.pdf
- **Matt Bishop:** *Introduction to Computer Security.* Boston: Addison Wesley, 2005. pp. 363-386.
- **Claudia Eckert:** *IT-Sicherheit*. München, Wien: Oldenbourg, 2006. pp. 37-45
- **Dieter Gollmann:** *Computer Security.* Chichester, New York, Weinheim, Brisbane, Singapore, Toronto: John Wiley & Sons, 1999. pp. 30-54
- EMSCB -Turaya www.emscb.de/content/pages/About-Turaya-de.htm
- **National Information Systems Security (INFOSEC) Glossary**, September 2000 http://handle.dtic.mil/100.2/ADA433929
- **Intel Trusted Execution Technology** www.intel.com/technology/security
- **ISO/IEC 2382-8, Information Technology - Vocabulary - Part 8: Security, 1998**
- **LAFKON: A movie about trusted computing; 2005; www.lafkon.net/tc**
- **LinuxDevices.com** www.linuxfordevices.com
- **Microsoft's Next-Generation Secure Computing Base** www.microsoft.com/resources/ngscb/default.mspx
- **Evgenia Pisko, Kai Rannenberg, Heiko Rossnagel:** Trusted Computing in Mobile Platforms – Players, Usage Scenarios, and Interests; Datenschutz und Datensicherheit (DuD); 29. Jg.; H. 9, September 2005; S. 526-530 www.m-chair.net/wps/wse/dl/det/rannenberg/5674/
- **Ravi Sandhu; Xinwen Zhang.** Peer-to-Peer Access Control Architecture Using Trusted Computing Technology, SACMAT05 , Stockholm, Sweden, June 1-3, 2005 http://portal.acm.org/citation.cfm?id=1064005
- Schreckxikon - Das A bis Z der Computer- und Datensicherheit www.sophos.de/sophos/docs/deu/papers/sophos-a-to-z-computer-and-data-security-threats.pdf
- iOS Security, February 2014 https://www.apple.com/au/iphone/business/docs/iOS_Security_EN_Feb14.pdf