Wir leben IT-Security

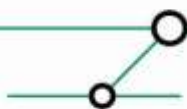# ERNW Newsletter 33 / September 2010

Dear Partners and Colleagues,

Welcome to the ERNW-Newsletters No. 33 covering the topic:

Using the iPad in Corporate Environments

Version 1.0 / 08. September 2010

by: Michael Thumann, mthumann@ernw.de & Rene Graf, rgraf@ernw.de

TABLE OF CONTENTS

1 INTRODUCTION

The mobile devices of Apple are one of most famous success stories. The recent gimmick, the Apple iPad, was made to change the way people think about mobile computing. It is smaller and lighter than every notebook, easy to use and also provides numerous applications. Lots of them can also be useful in corporate environments. For example, Pages, Numbers, and Keynote are the equivalents to Microsoft's Word, Excel, and PowerPoint.

Despite of the few experiences how to operate iPads in an efficient way; it has arrived in corporate environments. Because of the orientation as a lifestyle product, everybody wants to get an iPad. Therefore, also people on the management level use it, and, consequently, want to use it in the corporate environment. Due to this enforcement of the iPad use by managers, the IT department can literally do nothing to prohibit iPads in the corporate network.

This newsletter gives an overview of the relevant threats the iPad introduces into the corporate IT environment. It includes a risk assessment based on ERNW's Rapid Risk Assessment approach and makes recommendations for secure operation of Apple's recent gimmick.

Also there are some security relevant improvements described, that are introduced in iOS 4 for iPad (should be during the last quarter of 2010)

Because iPad and iPhone use the same operating system family, most of the things shown here apply to both of them.

2 THREATS

2.1 Physical Access

Two possible scenarios can lead to physical access by an unauthorized person. „Normal loss" of the device and theft (both caused by an opportunity or targeted). If an attacker gains physical access to the iPad, he can extract all data contained within the user partition, even without knowing the pass code.

The user partition contains all variable data of the device, such as:
❑ Saved and cached passwords (keychain)
❑ Certificates
❑ Pictures
❑ SMS messages
❑ Browser History
❑ Configurations (VPN, Mail, …)
❑ Caller Lists
❑ Contacts
❑ Emails
❑ Events
❑ Keyboard Cache
❑ Application data

Because the data can be extracted while the device is powered on, even the built in hardware encryption does not prevent this kind of access (decryption happens during device boot up).

The data can be extracted using special forensic tools, e.g. Lantern (Katana Forensics) or the Zdiarski Procedure. Forensic tools normally just extract the plain data. Using the Zdiarski Procedure, a complete image of the user and system partition is created. This can be useful when trying to recover deleted files.
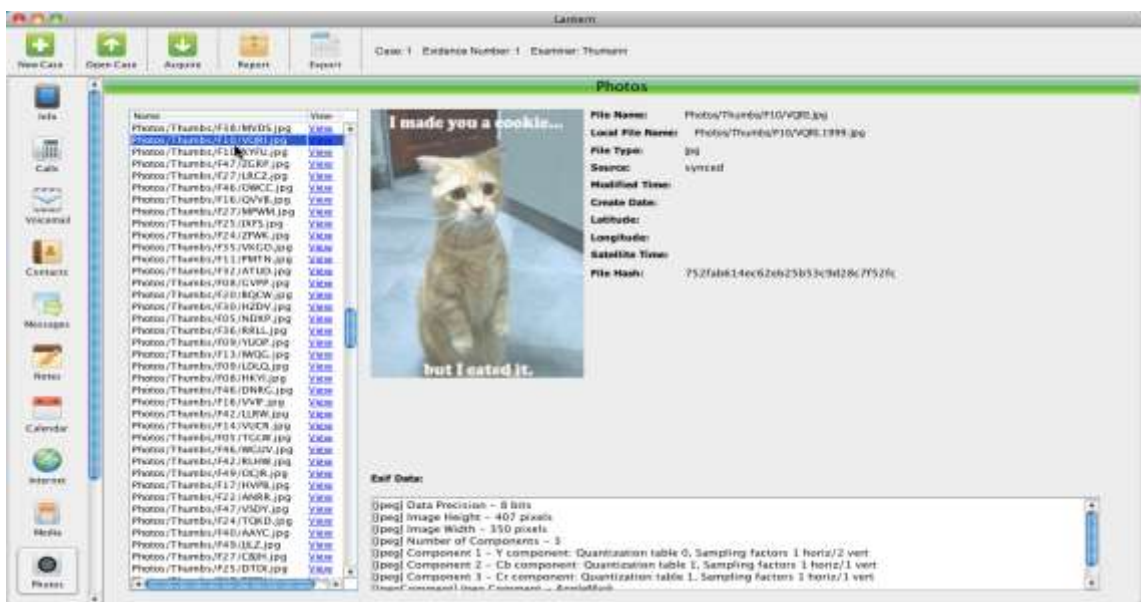
Figure 1: Lantern Photos
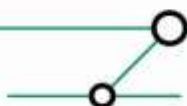
Using the Zdiarski Procedure also makes it possible to completely disable the pass code protection of the device.

Taking these facts into account, we must consider a device to be fully compromised when unauthorized physical access was possible.

2.2 Backup Access

ITunes performs device backups on a regular basis. Every time the device is synchronized with the user's iTunes library, a backup is created. These backups contain the same information that we already extracted from the device using the forensic tool.

By default, the iTunes device backup is stored unencrypted on the users workstation. Using available configuration options, the backup can also be stored encrypted. There are also tools available to browse stored backups (e.g. MobileSyncBrowser or JuicePhone)

Figure 2: MobileSyncBrowser & JuicePhone

The mentioned tools only work in case of an unencrypted backup. Elcomsoft, based in Russia, also (besides other password recovery tools) offers an iPad/iPhone password breaker software which can also use GPUs to speed up the recovery process.
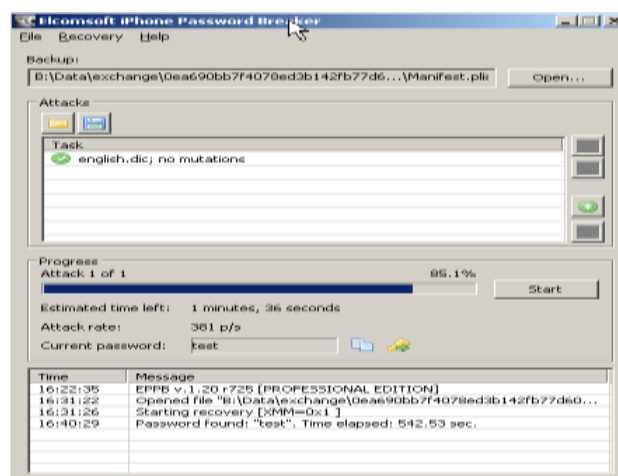
Figure 3: Elcomsoft iPhone Password Breaker
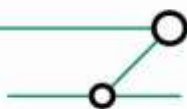
To prevent attackers from recovering the backup encryption key/password, it is necessary to ensure a proper password quality.

2.3 Malware access to confidential data

The iPad includes a mobile version of Apples browser application "Safari" which can be used to browse websites. This exposes the iPad to usual performed client attacks by malware.

To protect itself, the operating system runs threatened applications in so called sandboxes to isolate them. If an application gets compromised by malware, confidential data stored on the system cannot be accessed. Areas used by multiple applications however can be accessed (e.g. the keychain).

As a second protection mechanism, the operating system prevents unsigned code from being executed on the system. This does not affect e.g. JavaScript Code or code injected during exploiting.

2.4 Access to keyboard history

For the included auto complete feature to work, all keyboard input is cached in a text file. This file can be accessed with physical access to the device or by accessing an unencrypted backup (or an encrypted backup after the password was recovered).

It may contain confidential message contents or passwords. Since this file is a central component, it can be accessed by all applications (even sandboxed applications) and thus also malware could access the file.

At the moment, there is no known malware that uses this mechanism. Therefore, this is not considered to be a real threat.

Figure 4: Keyboard Cache

Figure 4 shows the access to such a file. Sometimes even passwords (if they were not recognized as such) are stored in this file.

2.5 Patchmanagement

Apple does not provide a dedicated update service for iPads/iPhones like it exists for e.g. Microsoft Windows or Mac OS X.

Known vulnerabilities on the iPad/iPhone are patched with upcoming firmware updates. This typically leads to very long periods during that the devices are operated in a vulnerable state. For example, the last version of the iOS3 family was released von 2nd Febr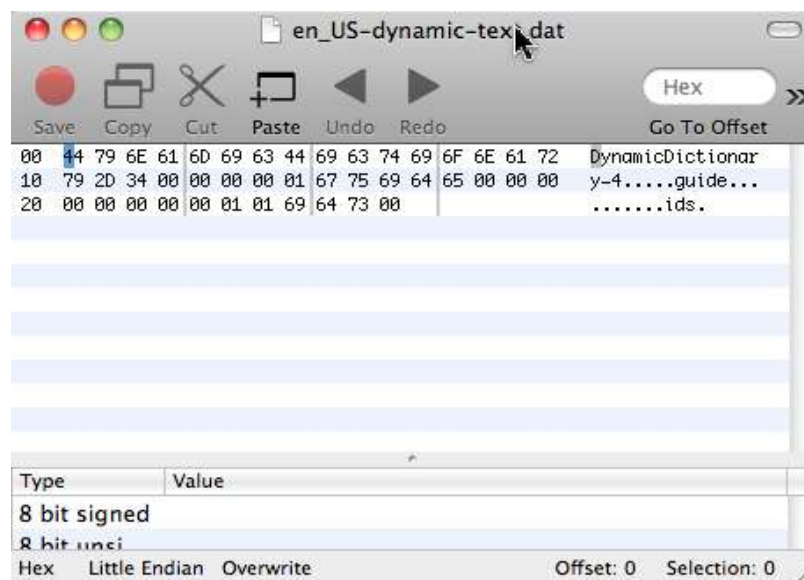uary 2010. The next update, including more than 60 security updates, was released on 21st June 2010. All vulnerabilities disclosed in the meantime (including critical ones; see CVE-2010-1775) were not patched until that date.

On the other hand, Apple has proved that they are also able to react very fast if it is (or they think it is) necessary to do so[1].

Since the only possibility to update an iPad is to replace the whole firmware and due to the fact, that firmware updates are only possible using iTunes, it is not trivial to implement a working patch management process.

2.6 Jailbreak

Apple requires all software developers to act upon Apples defines development rules if they want to distribute their software through the App Store. Per default, Apps can only be installed using this official way (exceptions exist for enterprise deployments).

To circumvent restrictions to only be able to install software from the App Store a so called Jailbreak is required. A Jailbreak is based upon a known vulnerability and usually disables security features such as "Sandboxing" and "Signed Code Only".

After a successful jailbreak, any application can be installed on the device.

After the market introduction of the iPad in summer 2010, a jailbreak for firmware version 3.2.1 was available almost immediately.

2.7 Performed Proof of Concepts (PoC)

The following table lists the performed proof of concepts with firmware version 3.2.1 along with the information if a PoC is possible on iOS version 4.

Performing a PoC usually means to practically execute an attack and see if it works.

The information provided by the table is based on state of the art technical possibilities.

Threat	PoC with iOS 3.2.1	PoC with iOS 3.2.1	PoC possible iOS 4
Physical access	YES	YES	NO
Backup access	YES	YES	YES
Malware accesses confidential data	NO	YES	NO
Keyboard cache access	YES	YES	NO
Patchmanagement	YES	YES	NO
Jailbreak	YES	YES	YES

More information on IOS4 and its new features can be found in chapter 5.4 and table 5.4.4. You will find some reasons there, why some attacks cannot be performed at the moment.

---

[1] Refer to http://www.heise.de/security/meldung/BSI-warnt-vor-Schwachstellen-in-iPhone-iPod-touch-und-iPad-1050706.html
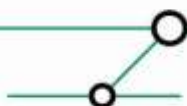
2.8 Summary

Some of the named threats depend on the occurrence of other threats. The keyboard cache for example can only by extracted if physical access to the device is also possible.

To define adequate mitigating controls and to be able to perform a realistic risk assessment, the threats are summarized as listed below:

❏ Physical Access
❏ Backup Access
❏ Malware accesses confidential data
❏ Patch Management
❏ Jailbreak

3 RAPID RISK ASSESSMENT

To determine to relevant risks, we used the ERNW Rapid Risk Assessment (RRA) approach. RRA differs from the traditional approach of performing risk assessments in some aspects. As other approaches, RRA also uses a Vulnerability, likelihood and consequences factor to calculate the resulting risk. It differs from the traditional approach in the number of considered threats. RRA uses a maximum of 10 threats. This enables the researcher to focus on the main threats and to find an answer to his questions in a short time.

The named factors for each threat are filled with numeric values between 1 and 5.

Factor	1	2	3	4	5
Likelihood	Lowest	Lower	Medium	Higher	Highest
Consequences	Lowest	Lower	Medium	Higher	Highest
Vulnerability	Lowest	Lower	Medium	Higher	Highest

To define a value for each of the three factors for each threat we use a methodology already known in the area of agile development. You just take the threat with the highest and lowest value, e.g. likelihood, and assign them to the values 1 and 5. All other threats are looked on in relation to the others. This procedure is repeated for each of the three factors.

By assigning the values related to other threats you prevent discussions about the definition of "high", "low", …

To calculate the resulting risk, the following formula is used:

Risk = Likelihood * Consequences * Vulnerability

After a Rapid Risk Assessment was performed, you are able to address the highest risks. You can also define some margins to define what risk value requires mitigating controls and which can be accepted.

Because some of the threats have different resulting risks when analyzed with different firmware versions, the risk assessment is performed for each firmware version.

3.1 iPad / iOS 3.2.1 or older

Threat	Likelihood	Vulnerability	Cons.	Risk
Physical Access	3	5	5	75
Backup Access	2	1	4	8
Malware accesses confidential data	1	3	3	9
Patchmanagement	4	4	2	32
Jailbreak	5	5	1	25
Average Risk				**29,8**

3.2 iPad / iOS 4.0 or newer

Threat	Likelihood	Vulnerability	Cons.	Risk
Physical Access	3	3	5	45
Backup Access	2	1	4	8
Malware accesses confidential data	1	3	3	9
Patchmanagement	4	2	2	16
Jailbreak	5	5	1	25
Average Risk				**20,6**

3.3 Risk assessment results

Based on the performed risk assessment the results can be summarized as follows:

The lowest risk results when operating the iPad with the announced firmware version IOS4.

The three highest resulting risks are:
1. Physical Access
2. Jailbreaks
3. Patchmanagement

4 MITIGATING CONTROLS

This chapter describes the mitigating controls recommended by ERNW for iPads in enterprise environments. The controls are selected based on the performed rapid risk assessment.

4.1 Technical minimal requirements

Based on the performed risk assessment, the following hardware requirements are defined:
❑ iPad WiFi+3G
❑ iOS4 or newer

Since it will increase the risk significantly, it is not recommended to operate devices with older firmware versions in an enterprise environment.

The WiFi only version of the iPad is also not recommended because the devices cannot be contacted on a regular base. Apple also currently recommends not to use the iPad with the current firmware version 3.2.2 in enterprise environments.

4.2 Provisioning/Configuration Profile

Provisioning means to rollout devices with an initial configuration so that it can be used. There are various possibilities to configure/provision the iPad/iPhone. The choice of the possibility depends mainly on the number of devices to be provisioned. Small amounts of devices (e.g. up to 20) can be configured and managed manually without problems. If you want to configure/provision a greater amount of devices, manual configuration is not practicable anymore.

Manual configuration takes place at the device itself using its built in configuration menu. This is the most simple way of configuring iPads but should not be used in a corporate environment. There is no way to ensure a consistent configuration of all devices. Also there is no possibility to prevent users from changing device settings and not all settings are available either (e.g. user restrictions, since they make only sense if they are enforced)

Using the "iPhone Configuration Utility", provided by Apple free of charge, one can create so called "Configuration Profiles", which are simple XML files containing either a complete device configuration or only a partial one. There can be one or more configuration profiles installed on one device. Configuration profiles also enable the use of settings not available for manual configuration on the device.

After creating configuration profiles, one must decide how to distribute them to the users. There are several ways to realize this. The simplest way is to install them on an iPad/iPhone directly connected to the computer running the iPhone Configuration utility. You can also export them, place them on a web server and direct your user to that website to klick on it (the link can be distributed via Email, SMS, MMS or on a piece of paper). Instead of placing them on a web server, you can also distribute them via Email directly (assuming that mail is already working on the iPad to receive the profile)

Mainly, these are the options directly supported by Apple (whereas "supported" means, that they can be used without the need to buy 3rd party software). A partly automated way to perform the initial configuration (called "enrollment" by apple) will be discussed in chapter 4.3.

It is recommended to sign the created configuration profiles to protect them from unauthorized changes. Encrypting them is also possible during the export procedure. Furthermore, the profile should be locked (meaning that the user is not able to remove it once installed)

The following screenshot shows the iPhone Configuration Utility:

Next we will discuss the configuration settings relevant for the overall security of the iPad. Every relevant setting is described with its possible and recommended values. At some points we will also already mention options which will become available with iOS version 4 (meaning they can currently only be used with the iPhone, not with the iPad). Especially regarding features required for proper centralized management, iOS 4 is coming up with some interesting things.

The section "general" is present in every configuration profile. The settings of all other sections are enclosed in so called payloads. A section with zero payloads does not change the device configuration in any way (regarding the section in question). Some sections can have only one payload some can have multiple. This allows the combination of multiple profiles to a well-organized configuration profile structure. E.g. it is possible to create different profiles for
❑ Corporate Root Certificates
❑ Location specific WLAN settings
❑ User specific settings

Detailed information regarding the multitude of configuration settings can be looked up in the official "iOS Enterprise Deployment Guide".

We recommend using SSL/TLS protected connections wherever possible, especially when the connection is routed through untrusted networks (e.g. the internet). If a specific connection is only established through an encrypted VPN connection and the corporate security policy allows unencrypted data transfers within the corporate network you can disclaim this. In all other cases: Encrypt all connections.
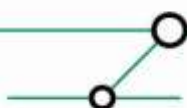
To use SSL/TLS connections in a secure manner, participating connection endpoints (including iPads) must be able to verify the authenticity of the used certificates. To enable this, all endpoints must know and trust the corporate root certificate (except you are using official certificates).

For the iPad/iPhone additional Certificates can be added in the section "Credentials" of a configuration profile. In this section, the corporate root certificate should be added.

We assume this as a prerequisite when configuring SSL/TLS connections in the following chapters.

The following outline is structured like the options/sections in the configuration profile

4.2.1 General

Global settings every profile must contain.

Option	Values	Recommended	Comment
Name	Preferably choose a significant name. This will be displayed to the User.		
Identifier	Unique Identifier for the profile. This is important when updating profiles. If an identifier of a profile pending installation is identical with the identifier of an already installed profile, it is replaced.		
Organization	Name of your Organization / Company		
Description	Significant Description		
Security	Always With Authorization Never	With Authorization	Controls whether an installed profile can be removed or not. "With Auth" means that a password is required to remove the profile. This is the recommended option, but the password must not be known by the user.
Authorization Password	Password to remove the profile from a device when the option "Security" is set to "With Auth".		

4.2.2 Passcode

This section controls the authentication procedure and the behavior on authentication failures.

The recommended values are based on common best practices. In general, the settings should be aligned with the corporate policy for mobile devices.

Option	Values	Recommended	Comment
Require passcode on device	Enabled Disabled	Enabled	Controls if a passcode is required at all

Allow simple value	Enabled Disabled	Disabled	Controls whether simple passcodes are allowed
Require alphanumeric value	Enabled Disabled	Enabled	At least one letter required
Minimum passcode length	0 – 16	8	Minimum passcode length
Minimum number of complex characters	0 – 4	1	Minimum number of special chars
Maximum passcode age	0 – 730	90	maximum age
Auto Lock	0 - 5	5	Idle time after which the device is locked
Passcode history	0 – 50	10	How many old password should be blocked for reuse
Grace period for device lock	None Immediately 1, 5, 15 Minutes 1, 4 hours	Immediately	Time between device lock and password required to unlock

4.2.3 Restrictions

This section controls user limitations. The recommended values are based on common best practices. The settings should be aligned with the corporate acceptable use policy for mobile devices.

Part: Device Functionality

Controls restrictions regarding the functionality of the device itself. Every option can either be enabled or disabled. Individual values cannot be specified,

Option	Comment
Allow installing Apps	Is the user allowed to install applications? Should be disabled. This makes it possible to control the applications in use (e.g. due to licensing issues) Users tend not to like such restrictions. If in doubt, make an individual risk assessment or think about having e.g. separate policies for VIPs and Non-VIPs ;-) Also take a look at you other mobile device policies!
Allow use of camera	Depends on the corporate security policy. Some companies in the production area have prohibited digital cameras (and phones) within

	their sites for confidentiality reasons.
Allow screen capture	Can be enabled without a risk increase.
Allow automatic sync while roaming	Depends on your contracts with mobile your mobile carrier. Maybe create different profiles for users with and users without special roaming rates.
Allow voice dialing	Can be enabled without a risk increase. Maybe think about teaching you users about how to use / not use mobile devices in public areas.
Allow In App Purchase	Can be enabled without a risk increase. Could depend on the acceptable use policy.
Force encrypted backups	Must be activated to protect the created backups from unauthorized access.

Part: Applications

Application restrictions

Option	Values	Comments
Allow use of YouTube	Enabled Disabled	Depends on the acceptable use policy.
Allow Use of iTunes Music Store	Enabled Disabled	Depends on the acceptable use policy.
Allow Use of Safari	Enabled Disabled	Depends on the acceptable use policy. Since the usability would decrease significantly, it is recommended to leave this option enabled. The following options are specific to safari.
Safari: Enable autofil	Enabled Disabled	Can be enabled without risk increase.
Safari: Force fraud warning	Enabled Disabled	Recommended: Enabled Enables fraud warning
Safari: Enable JavaScript	Enabled Disabled	Can be enabled without risk increase. Usability would decrease significantly when disabled.
Block Pop-ups	Enabled	No recommendation.

	Disabled	
Accept Cookies	Always Never From visited sites	Depends on the browser policy

Part: Ratings

Content Classification / Rating

Option	Values	Comments
Ratings region	Australia Canada France Germany Ireland Japan New Zealand United Kingdom United States	Depends on the geographical location
Movies	Dont allow Allow all Diverse Altersgrenzen	Align with the acceptable use Policy
TV Shows		
Apps		

4.2.4 Wi-Fi

This section contains configuration options for WLAN access profiles. One WLAN is configured with each WLAN configuration payload. The recommended values are based on common best practices. Therefore, settings must be evaluated to comply with the WLAN infrastructure in place. This newsletter does not cover WLAN security.

The iPad supports all common WLAN security standards (WEP, WPA, WPA2). Each in its "home" (shared secret) and "enterprise" (personalized) version.

The common best practices for WLAN in enterprises is to use WPA2 Enterprise with certificate based authentication. For authentication 802.1X based authentication takes place. The following EAP Methods are supported by the IOS:

❑ TLS
❑ TTLS
❑ LEAP
❑ PEAP
❑ EAP-FAST
❑ EAP-SIM

Besides the EAP Method, authentication settings and trust relationships must be configured.

The certificates used for authentication (if certificates are used; username password is also possible) can be deployed using methods described in section "credentials". Certificates for user authentication can also be obtained via SCEP.

Make sure to restrict the settings as much as possible (e.g. only allow the needed EAP Methods) and to specify all certificates.

It is recommended to disable the option "Allow Trust Exceptions". Users won't be asked what to do if a certificate cannot be validated.

4.2.5 VPN

This configuration sections describes the configuration of VPN access profiles. One VPN payload configures one VPN connection. The recommended values are based on common best practices.

The VPN configuration should be aligned with the corporate RAS policy and adjusted to work with the present infrastructure.

The iPad/iOS currently supports the following VPN Protocols:
❑ L2TP
❑ PPTP
❑ IPSec (Cisco)
❑ Cisco Anyconnect (iOS Version 4)
❑ Juniper SSL (iOS Version 4)

The only recommended protocol for iPads with iOS 3.x is "IPSec (Cisco)". The other supported protocols (L2TP, PPTP) are considered insecure and should not be used.

Machine and user (XAuth) authentication is supported

Machine Authentication

It is recommended to use certificates for machine authentication. The certificates should be clearly relatable to a device so they can be locked in case of device compromise. You should also keep CRLs in mind when implementing a PKI.

User Authentication

Additionally, users can be authenticated, too. It is recommended to implement an OTP based user authentication. In the iPad configuration, this can be enabled using the options "Account" and "Include User PIN".

It is also recommended to configure a proxy server for the VPN connection. This way, it can be ensured that the iPads use the corporate internet access infrastructure including AV and content filter.

If the VPN settings are configured using a configuration profile, the implicit option "Require Encrypted Backup" will be enabled to ensure that the VPN credentials are not stored in plain text.

4.2.6 Email

This section configures Email access profiles. One payload configures one email account. The recommended values are based on common best practices.

The iPad supports POP and IMAP based email accounts. To connect to a Microsoft exchange server, a separate configuration section exists.

It is recommended to use an encrypted SSL/TLS connection to the server. If the connection is only established through an encrypted VPN connection then this can be omitted.

4.2.7 Exchange Active Sync

This section configures exchange access profiles. One payload configures one exchange account. (IOS3 devices can only have one). The recommended values are based on common best practices.

Using Microsoft Exchange ActiveSync, the iPad can be synchronized with an Exchange account (Mail, Calendar, …).

Also, ActiveSync policies can be used to manage iPads/iPhones running IOS4 or greater. See chapter 4.3 for more information on this.

It is recommended to use an encrypted SSL/TLS connection to the server. If the connection is only established through an encrypted VPN connection then this can be omitted.

Certificate based client authentication can be used with Exchange ActiveSync. In comparison to nearly all other certificates, this certificate must be installed directly in the payload instead of the section "Credentials".

4.2.8 LDAP

This section configures access profiles for LDAP based directory services. One payload configures one LDAP server. The recommended values are based on common best practices.

Using LDAP, the iPad can be integrated with corporate directory services like address books.

It is recommended to use an encrypted SSL/TLS connection to the server. If the connection is only established through an encrypted VPN connection then this can be omitted.

4.2.9 CalDAV

This section configures access profiles for CalDAV based calendar services. One payload configures one CalDAV server.

CalDAV can be used to integrate with a corporate calendar system supporting the CalDAV standard.

It is recommended to use an encrypted SSL/TLS connection to the server. If the connection is only established through an encrypted VPN connection then this can be omitted.

4.2.10 CardDAV

This section configures configuration profiles for CardDAV address book services. One payload configures one CardDAV server.

Using CardDAV you can integrate iPads with your corporate address book services.

It is recommended to use an encrypted SSL/TLS connection to the server. If the connection is only established through an encrypted VPN connection then this can be omitted.

4.2.11 Subscribed Calendars

This section configures access profiles for iCal based public/read only calendars. One payload configures one calendar.

Using iCal, read only calendars can be included, which are published in the iCal format.
There are numerous public iCal calendars available, e.g. for football games or holidays.

For calendars containing confidential information, it is recommended to use an encrypted SSL/TLS connection to the server. If the connection is only established through an encrypted VPN connection, then this can be omitted.

4.2.12 Web Clips

These are kind of bookmarks that have their own icon on the home screen each. Not relevant for the overall security.

4.2.13 Credentials

This section is for integrating different certificates. Each payload includes one certificate. Either a root certificate, server certificate or user certificate.

To use SSL/TLS connections in a secure manner, participating connection endpoints (including iPads) must be able to verify the authenticity of the used certificates. To enable this, all endpoints must know and trust the corporate root certificate (except official certificates are used).

4.2.14 SCEP

This section configures the SCEP (Simple Certificate Enrollment Protocol) settings. Each payload configures one SCEP profile.
Using SCEP, user certificates can be obtained automatically from a certificate authority.

More information is included in chapter 4.3.

4.2.15 Mobile Device Management

This section configures the new IOS 4 features regarding Mobile Device Management. This topic is covered in more detail in chapter 4.3.

5 ADVANCED

This section configures advanced mobile carrier settings.

If no own APN is used, (some large organizations have one) then this is not relevant for the overall security and should be left alone.

5.1 Provisioning Systems/Mobile Device Management

Besides the manual iPad configuration using the built in configuration menu, it is possible to create configuration profiles as described in chapter 4.2 and distribute them via web or email.

Although one can handle more devices using configuration profiles than with manual configuration, this also has its limitations.

To operate iPads in a secure manner, it is necessary to have a central management or at least a possibility to configure these devices centrally. This paragraph gives a short overview of the possibilities.

To automatically configure or enroll devices, so called provisioning systems are used. Good provisioning systems also include extensive management features like hardware monitoring, inventory functionality or possibilities for reporting.

To enroll iOS devices automatically, the following components are required:
❑ Profile Distribution Service
❑ Certificate Authority (SCEP Support)
❑ Directory/Authentication Service (AD, LDAP, ...)

The profile distribution service is responsible for configuration profile delivery. A profile distribution service must either be developed in house or can be licensed from a 3rd party provider. Apple does not provide such software.

For a detailed description of the mode of operation see Apple's IOS enterprise deployment guide. The following paragraph gives a brief overview:

At the beginning of the enrollment process, the profile distribution service can request certain information from the device. This information can be used to check for minimum requirements like device type or firmware version. Furthermore, information like IMEI or MAC can be used to perform a kind of "device authentication" before installing configuration profiles (besides the user authentication using e.g. HTTP basic).

After triggering the iPad to contact the profile distribution service (HTTP request), the profile distribution service responds with a request for more information. After the user has accepted to install a configuration profile, the iPad sends (next http request) the requested information (signed with its preinstalled certificate) to the profile distribution service. The profile distribution service responds to that request with a configuration profile containing all information needed to create a certificate signing request and to request a certificate using SCEP.

The iPad will now try to request a certificate from the configured CA. After this has been successfully performed, the iPad contacts the profile distribution service again (next http request). Again, it sends the information the profile distribution service initially requested but this time data is signed by the freshly retrieved certificate. As a final response the iPad receives its final configuration profile(s).

Keep in mind to sign, encrypt and lock your profiles to protect them from unauthorized changes, sharing or removing.

To ensure that this process works in an automated way (besides entering the initial URL), the profile distribution service must be able to generate configuration profiles individually for every user and device. For authentication, it is recommended to integrate with existing infrastructure and use an AD or other LDAP directory.

Apple's enterprise deployment guide [8] describes the described process of operation in more detail.

Since the whole communication with the profile distribution service is based on HTTP, own implementations are not that hard to develop. A detailed example implementation including sample code can be found in [9].Alternatively, 3rd party products are available.

The described procedure provides an efficient enrollment/provisioning of iPads/iPhones.

Features like automatic profile updates, inventory, asset management, reporting or other administrative tasks cannot be realized like that. For example, Profile updates would require the user to trigger it by visiting a web site or installing from an email.

To prevent the installation of unwanted software (especially jailbreak software) and untrusted software, the management system should also provide the mentioned missing features. This is required to detect incompliances and initiate an adequate reaction.

5.1.1 Mobile Device Management (iOS 4)

This is a new feature introduced with iOS4. So currently it can only be used on iPhones. For iPads iOS4 is not released yet.

Using Mobile Device Management, the IT department has the ability to remotely enroll, configure, monitor, lock and wipe devices. This takes place by connecting the iPad/iPhone to a mobile device management server (Configured through "Mobile Device Management" payload in the configuration profile). When a management server wants to communicate with an iPad, it sends a notification through the Apple Push Notification Service (APNS) triggering it to check in with the server.

The device connects to the server and checks whether there are any pending tasks and performs the requested actions. This way, a management server can trigger policy updates, request device information, remove data or lock and wipe the device.

The technical features of the mobile device management method can be divided into four categories: enrollment, configuration, querying and management.

Enrollment:
To initially configure iPads/iPhones for management through a mobile device management server an enrollment process is required.

This can be performed in various ways as described in chapter 4.2 and at the beginning of this chapter with over-the-air enrollment. Basically a configuration profile containing a "mobile device management" payload and a certificate must be installed.

Using the over-the-air enrollment way, this would be performed by the following steps
- ❑ Contacting a Profile Distribution service (http), authenticating against it
- ❑ Providing requested information and receiving SCEP information (to receive cert)
- ❑ Obtaining a certificate using SCEP

❑ Reconnecting to the Profile Distribution Service and receiving the final configuration. In this case (we are only initializing for management through a management server) the configuration received basically contains a "mobile device management" payload with information for the device to connect to the management server.

The mobile device management section includes the following configuration options:
❑ Server URL (Mobile Device Management Server)
❑ Check In URL (Required for Installation)
❑ Topic (For Notification Service)
❑ Identity (Cert for Authentication)
❑ Access Rights (Configure according to the management system requirements)

Configuration:
After a device is enrolled and has a working "mobile device management" configuration, it can be configured using the management server. The management sends configuration profiles (see chapter 4.2) to the device, which are installed automatically.

Querying:
Using the mobile device management features, a device can be queried for information. Currently the following information can be obtained:
❑ Device information
  ▫ Unique Device Identifier (UDID)
  ▫ Device Name
  ▫ iOS and build version
  ▫ Model name and number
  ▫ Serial number
  ▫ Capacity and space available
  ▫ IMEI
  ▫ Modem firmware
❑ Network Information
  ▫ ICCID
  ▫ Bluetooth and Wi-Fi MAC addresses
  ▫ Current carrier network
  ▫ SIM carrier network
  ▫ Carrier settings version
  ▫ Phone number
  ▫ Data roaming setting (On/Off)
❑ Compliance and security information
  ▫ Configuration profiles installed
  ▫ Certificates installed with expiry dates
  ▫ List of all restrictions enforced
  ▫ Hardware encryption capability
  ▫ Passcode present
❑ Applications
  ▫ Applications installed (app ID, name, version, size and app data size)
  ▫ Provisioning profiles installed with expiry dates
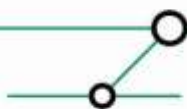
Management:

Furthermore using the new iOS4 management features, the following actions can be triggered remotely:

❑ Remote Wipe: one of the most essential features in mobile device management.
❑ Remote Lock: Trigger the device to require a passcode if currently unlocked
❑ Clear Passcode: Clears the passcode and requires the user the set a new one. Could be a useful helpdesk feature.

5.1.2 Mobile Device Management using Microsoft Exchange ActiveSync

Also available with IOS 4 is iPad/iPhone management using ActiveSync policies. There can be a lot of restrictions configured like password policies, etc. Also important features like remote wipe are available (even through user self service using OWA). However, configuration settings for the rest of the iPad configuration cannot be distributed.

For a detailed description see [10].

5.1.3 Evaluation Criteria

The following criteria should be considered when evaluating management systems:
❑ Device Type Detection (iPad WiFi / iPad WiFi+3G)
❑ Firmware Detection (> 4.0)
❑ Live hard-/software Inventory
❑ Support for all options of configuration profiles for the iPad
❑ Support for new iOS4 features

Using or extending existing systems should be preferred if possible.

5.1.4 3rd Party Products

Apple does currently not offer profile distribution service or mobile device management software, but in house development should not be that hard.

Furthermore there are numerous 3rd party products available. Some of them are specialized only on iPhones/iPads. Others are complete mobile device management solutions also supporting lots of other devices like blackberry, windows mobile, adroid, symbian or others.

In any case you should check if such a system might be already in place in your environment and possibly only needs to be updated to support iOS devices.

If you do not already have a solution in place and have to select one, also keep in mind to check the integration options (e.g. AD integration, …)

Here is a small list of the most popular 3rd party products:

Afaria:

Vendor: Sybase
Website: http://www.sybase.com/products/mobileenterprise/afaria
Devices: Apple, Windows Mobile, Symbian, PalmOS SyncML Devices

Feature	Description
Device Type Detection	Yes
Firmware Detection	Yes

Inventory	Yes
All iOS Options	Yes
iOS4 Features	Yes

TARMAC:

Vendor: Equinux
Website: http://www.equinux.com/us/products/tarmac/index.html
Devices: Apple only

Feature	Description
Device Type Detection	Only detects iPad, iPhone (2,3,3G,3GS), iPod, but not if iPad with 3G or not
Firmware Detection	Yes
Inventory	No, since only Provisioning system and no iOS4 features
All iOS Options	Yes. Configuration profiles are created using Apples iPhone configuration utility, exported and uploaded to the admin interface.
iOS4 Features	No, but provides log information about downloaded profiles (not a reliable information)

Airwatch:

Vendor: Airwatch
Website: http://www.air-watch.com/
Devices: Apple, Windows Mobile, Symbian, Blackberry, Android

Feature	Description
Device Type Detection	Yes
Firmware Detection	Yes
Inventory	No
All iOS Options	Yes, also iOS4 Options can be configured (e.g. new VPN types)
iOS4 Features	New features not used yet.

Ubitexx:

Vendor: Ubitexx
Website: http://www.ubitexx.como
Devices: Apple, Windows Mobile, Symbian

Feature	Description
Device Type Detection	Yes
Firmware Detection	Yes

Inventory	Yes
All iOS Options	Yes, also iOS4 options
iOS4 Features	Partially / planned

Good for Enterprise

Vendor: Good Technologies
Website: http;//ww.good.com
Devices: Apple, Windows Mobile, Symbian, PalmOS SyncML Devices

Feature	Description
Device Type Detection	Yes
Firmware Detection	Yes
Inventory	Yes
All iOS Options	Yes
iOS4 Features	Planned; advanced management features through dedicated app installed on the clients.

Mobileiron:

Vendor: Mobileiron
Website: http://www.mobileiron.com
Devices: Apple, Windows Mobile, Symbian, Palm webOS, Blackberry

Feature	Description
Device Type Detection	Yes
Firmware Detection	Yes
Inventory	Yes
All iOS Options	Yes
iOS4 Features	Yes

5.2   New Features in iOS 4

Besides numerous new features to fulfill user needs, like multitasking, there are also some important new security features, which are reducing some of the identified risks.

The following sections give an overview of the relevant new features.

5.2.1   Data Protection

With iOS 4, hardware encryption not only uses keys stored on the device, but also includes the user's passcode in the key generation process. Additionally, there can be per application keys (class keys) preventing other applications from reading an applications data.
The following picture shows this procedure (source: new iOS4 security features presentation)
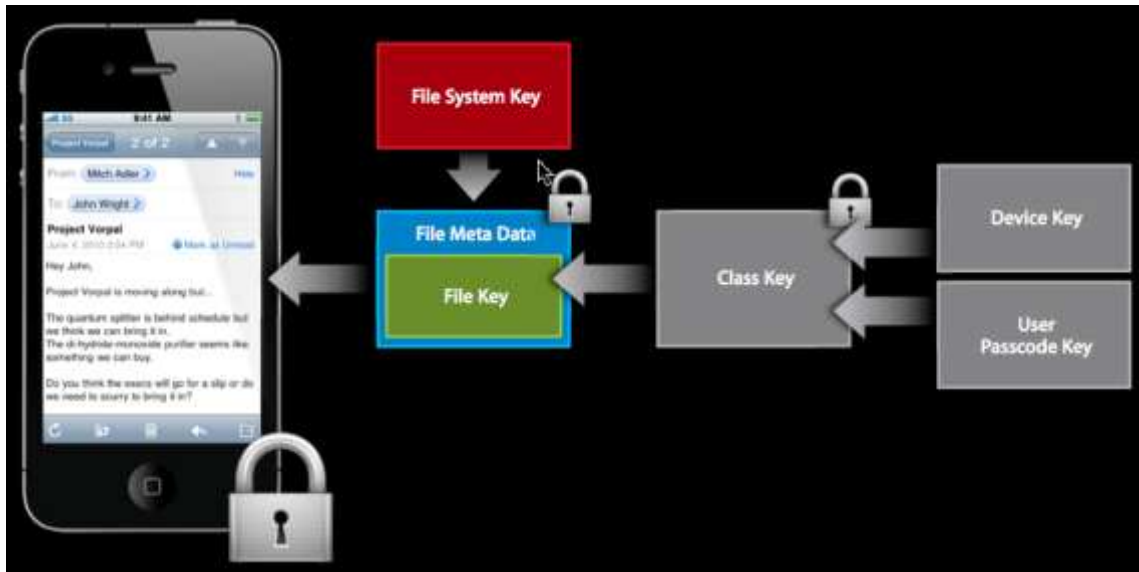
Figure 5: Data Protection

The implementation in own applications is done using new iOS4 APIs. This means application developers must use these features. So it is up to them to secure their applications. Some built in applications already support these features (like e.g. mail).

5.2.2 Backup

With iOS4, the backup process changes. IOS 3.2.x encrypts the keychain using the device key, making it impossible to recover the keychain on another device. Since iOS 4, this behavior changed. If an encrypted backup is created, the keychain data is stored in clear text. This makes it possible to recover the keychain on a different device. If an unencrypted backup is created, the old behavior is used.

The current version of Elcomsoft's iPhone Password Breaker is already aware of this change and includes a keychain explorer, which displays the contained data after successfully cracking the encryption password (mail accounts, WLAN, VPN, iTunes store, iPad passcode, SIM PIN, …).
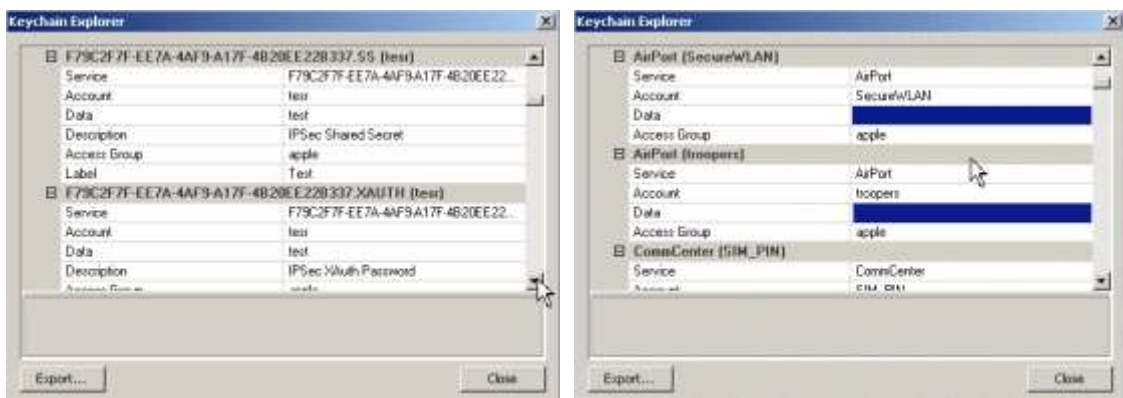
Figure 6: Keychain Explorer
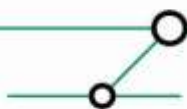
Prerequisite for the described scenario is the access to the encrypted backup and a successful password recovery attack. Strong passwords are recommended to mitigate this.
The following is an exemplary policy:

❑ Key space: Full Key space; letters, numbers, special chars
❑ no dictionary words or permutations of them
❑ Minimum length: 16 (regarding current performance test, Elcomsoft requires $2,7 * 10^{26}$ years to test all combinations)

5.2.3 VPN

IOS4 introduces SSL VPNs (Juniper, Cisco Anyconnect).

5.2.4 Mobile Device Management

IOS4 introduces (see 4.3) some new features, which enable a way to proper manage iOS devices. This also includes important features such as "remote wipe" to delete a device when it is lost. It is important to note that this is useless if the SIM card was removed. That would be very likelythe case for targeted thefts, because a thief wants to prevent localization or remote wipes.
For more information see 4.3.

5.2.5 Risk reduction with iOS4

The table shows the effect of iOS4 to the identified threats:

Threat	Improved by iOS4	Description
Physical Access	YES	Attack will be harder because of data protection features and patched vulnerabilities.
Backup Access	NO	Available password cracking tools already support iOS4.
Malware accesses confidential data	YES	The data protection feature to have application specific keys prevent (if used and implemented correct) unauthorized access by other applications.
Keyboard cache access	YES	Patching of known vulnerabilities and the introduced data protection features provide a better protection.
Patchmanagement	YES	The iOS4 update will probably fix known vulnerabilities.
Jailbreak	YES	There sure will be a Jailbreak for iPads running iOS4 but the new management features provide a way of detecting jailbreaked iPads.

5.3 Infrastructure Controls

Especially mobile devices are hard to protect from losing them (or being stolen). That means that the risk of unauthorized access to the device and potentially to the VPN access credentials increases.

This can be mitigated providing a dedicated network segment for mobile devices such as iPads. Devices like iPads most likely only have light requirements regarding access to enterprise resources (such as SAP systems) and can be much more restricted in their communication.

The allowed communication should be managed using filter rules (e.g. firewalls or ACLs).

5.4 Organizational Controls

There will always remain some risks, which can only be mitigated with high expense or even not at all. Therefore, there must also be some organizational controls supporting the technical controls.

In the case of an iPad, this mainly means there should be an acceptable use policy, which the users must agree upon. This policy should at least define the following:

❑ Duplicating the configuration (e.g. through backups) and replicating it to another device for VPN access is prohibited.
❑ iPads with firmware <4 are prohibited/must be updated
❑ No iPads without 3G
❑ Performing a jailbreak is prohibited
❑ Policy violation will lead to an account lock and exclusion from the iPad usage program ;-)

Add further requirements as needed.

5.5 Summarization

Finally, here are the most important controls to operate iPads in a secure manner:

❑ Hardware Requirement: iPad WiFi+3G with iOS4 or newer
❑ Configuration based on ERNW recommendations
❑ Usage of mobile device management system
❑ Network segmentation and filtering
❑ Acceptable Use policy

Kind regards,

Michael Thumann, Rene Graf

ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
www.ernw.de

6 ONLINE RESOURCES

[1] **Apple Business Resources**
http://www.apple.com/business/resources/
http://www.apple.com/de/business/resources/

[2] **IPad Enterprise Overview**
http://www.apple.com/support/ipad/enterprise/
http://www.apple.com/de/support/ipad/enterprise/

[3] **IPhone Enterprise Overview**
http://www.apple.com/support/iphone/enterprise/
http://www.apple.com/de/support/iphone/enterprise/

[4] **iPad Security Overview**
http://images.apple.com/ipad/business/pdf/iPad_Security_Overview.pdf
http://images.apple.com/de/ipad/business/pdf/iPad_Security_Overview.pdf

[5] **iPhone Security Overview**
http://images.apple.com/iphone/business/docs/iPhone_Security_Overview.pdf
http://images.apple.com/de/iphone/business/docs/iPhone_Security_Overview.pdf

[6] **IPhone Device Configuration Overview**
http://images.apple.com/iphone/business/docs/iPhone_Device_Configuration_Overview.pdf
http://images.apple.com/de/iphone/business/docs/iPhone_Device_Configuration_Overview.pdf

[7] **IOS Reference Library / Enterprise Deployment**
http://developer.apple.com/iphone/library/navigation/index.html#filter=Enterprise%20Deployment

[8] **IPhone OS - Enterprise Deployment Guide**
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf
http://manuals.info.apple.com/de_DE/Einsatz_in_Unternehmen.pdf
http://discussions.apple.com/category.jspa?categoryID=246

[9] **Over-the-air profile delivery and configuration**
http://developer.apple.com/iphone/library/documentation/NetworkingInternet/Conceptual/iPhoneOTAConfiguration/Introduction/Introduction.html

[10] **Exchange ActiveSync and iOS 4 Devices**
http://developer.apple.com/iphone/library/featuredarticles/FA_Exchange_ActiveSync_and_iOS4_Devices/Introduction/Introduction.html

[11] **Mobile Device Management**
http://images.apple.com/iphone/business/docs/iPhone_MDM.pdf

7 APPENDIX A: USEFUL APPS IN THE ENTERPRISE

Name	Description	iTunes Link
iBooks	Apple's eBook Reader	http://itunes.apple.com/de/app/ibooks/id364709193?mt=8
Pages	Apple's Word Processor	http://itunes.apple.com/de/app/pages/id361309726?mt=8
Numbers	Apple's Spreadsheet App	http://itunes.apple.com/de/app/numbers/id361304891?mt=8
Keynote	Apple's presentation software	http://itunes.apple.com/de/app/keynote/id361285480?mt=8
GoodReader	Document management and Reader (PDF, MS-Office)	http://itunes.apple.com/de/app/goodreader-for-ipad/id363448914?mt=8
iAnnotate PDF	PDF Editing	http://itunes.apple.com/de/app/iannotate-pdf-kommentar/id363998953?mt=8
CHMate Lite	CHM Reader	http://itunes.apple.com/de/app/id335157929?mt=8
iSaveWeb	Website Offline Browser	http://itunes.apple.com/de/app/isaveweb-website-download/id305594530?mt=8
Penultimate	Handwritten notes	http://itunes.apple.com/de/app/penultimate/id354098826?mt=8
Calculator	Calculator	http://itunes.apple.com/de/app/calculator-hd-for-ipad/id364905554?mt=8
World Clock	Worldtime	http://itunes.apple.com/de/app/the-world-clock/id368177365?mt=8
DevInfo	System Infos (running processes, network ports)	http://itunes.apple.com/de/app/devinfo/id294217490?mt=8
iSSH	SSH, Telnet and VNC Client (incl. X11 Support)	http://itunes.apple.com/de/app/issh-ssh-vnc-console/id287765826?mt=8