Authentication on Mobile Devices for Business Application

Martina Müller (MM)[*], Fabian Zoller (FZ)[†], Ingo Pansa (IP)[‡], Ansgar Gerlicher (AG)[§]

martina.mueller@ic-consult.at
fabian.zoller@ic-consult.de
ingo.pansa@ic-consult.de
gerlicher@hdm-stuttgart.de

Abstract: Identity management faces new challenges of protecting resources that are aces from different and maybe unknown devices. This is caused by the fact that employees bring their own mobile devices to their offices and work with them [Gar12]. Consequently users, programmer and companies have to face challenges that arise from mobile authentication: the need for accessing business application is based on the employees user identity. This paper describes a methodical analysis and evaluation of the current state of the art authentication methods. The resulting evaluation is the basis for a prototypical implementation of the best evaluated authentication methods on mobile devices. To test and confirm the theoretical architectures implemented on mobile devices a usability test has been made. A conclusion sums up the lessons learned and recommendations are made.

1 Introduction

Authentication in Business Environments is a vital part in securing business data and business processes. Different approaches have been utilized in the past decades; various efforts in implementing externalized authentication and authorization systems have been made. However, these approaches are all based on the assumption that the device that requests access to business application is controlled by the IT department of the companies. With the success of mobile devices, employees start to bring their own devices to the enterprise networks to access protected resources. Thus, new challenges in integrating these devices arise.

Mobile Authentication is an environmental part of working with private devices in a company and accessing resources that are protected. This creates new challenges for the security department. How to verify that a user is actually the one he or she claims to be? Additionally, access via mobile devices emerges the mobility problem to the ubiquitous used authentication methods that have been discussed [AZEH09, BM02, DYB11, Rae11].

[*] MM, iC Consult Austria / Kernstockgasse 8 / 2700 Wiener Neustadt
[†] FZ, iC Consult GmbH / Keltenring 14 / 82041 Oberhaching
[‡] IP, iC Consult GmbH / Keltenring 14 / 82041 Oberhaching
[§] AG, Hochschule der Medien / Nobelstraße 10 / 70565 Stuttgart

This article analyzes and evaluates those methods against the background of mobility focusing the interest on three stakeholders that are involved in IAM: users, company and programmers.

The analysis used the requirements usability and functionality, security, accuracy, expenditure and implementation effort. Furthermore, a rating matrix that adds the results together of the analysis generates a ranking. Authentication methods are evaluated by using distinctive criteria. Based on that the best rated authentication methods have been used to create prototypical implementations. Four functional prototypes on two operating systems (iOS and Android) were developed. Following this, the prototypes that included seven showrooms were tested by a group of 26 testers in a usability test. The conclusive evaluation of the test was necessary to verify or reject the initial analysis of the authentication methods.

1.1 Distinction

This paper focuses on the process of mobile authentication. Several prerequisites have been created. The focus for the authentication is set on strong authentication (involving two factors). The prototypes are fully functional, including front end and back end. The data distribution is considered to be secure and is not part of that paper.

2 Foundation for Mobile Authentication

For the analysis of the requirements for mobile authentication current authentication methods were used and taken into account. Biometrics are used to identify an individual by using certain unique physiological (face, finger, iris, retina, hand) or behavioral (voice, signature, keystroke) characteristics [vT05]. Knowledge based authentication requests the knowledge of the user (secret question, username, specified knowledge). The input can be textual, graphical or made by a gesture. The basis is the challenge-response model. Property based authentication is not intrinsically linked to an individual but describes the possession of e.g. a token or an NFC chip that needs to be verified. Location based authentication methods use the physical aspect of location (latitude, longitude and altitude) that are used by Location Based Services like GPS or WLAN. An additional option to exchange data for authentication in a secure way is the use of digital certificates, signatures and keys, respectively a public key infrastructure (PKI) that can include encryption. Mobile authentication can use several different factors to protect a resource. But which do have a good usability? The specific constraints of mobile devices need to be taken into consideration when comparing mobile authentication methods, in order to find a balance between security and usability.

3 Comparison of Mobile Authentication Methods

The selection of requirements is based on the assumption that there are three stakeholders with different interests that disperse from each other: user (usability, functionality and accuracy), programmer (implementation effort, accuracy, security) and the company (expenditure, accuracy and security).

To make those requirements understandable and reasonable they are subdivided into characteristics as it is presented in table 1.

$\mathbf{R_n}$	**Requirement**	**Characteristic 1**	**Characteristic 2**
R1	Usability and Functionality	Access Time	Acceptability
R2	Security	Distinctiveness	Resistance to Attacks
R3	Accuracy	False Accept Rate	False Rejection Rate
R4	Expenditure	Purchase	Administration
R5	Implementation Effort	Software	Hardware

Table 1: Requirements and Characteristics

Access Time describes the time that elapses from opening the application until the process of authentication has been executed.

Acceptability indicates to what extent people are willing to accept an authentication system. Attention should be paid to intrusiveness, intuitive handling, overview and performance.

Distinctiveness describes the level of uniqueness and the level of differentiation of authentication input.

Resistance to Attacks describes the level of robustness against attacks like fraud, man in the middle or impersonation.

False Acceptance Rate (FAR) and False Rejection Rate (FRR) categorized by Moulton into error types I (FRR) that classify authorized users as imposters and error type II (FAR) that classify imposters as authorized users [Mou83].

Purchase describes the level of expenditures that must be calculated for acquisition only; including hardware like fingerprint scanner, smart cards sensors etc.

Administration describes the amount of work that needs to be calculated for creating a running authentication system with the purchased objects. Reference points are: capturing of data, creation of IDs, managing IDs, maintain the database and solving occurring problems.

Implementation Effort Software describes the amount of work units for learning the required skills like programming language, coding, testing, using frameworks and libraries.

Implementation Effort Hardware describes the amount of work units that are required for implementing hardware (if necessary) like sensors, server and infrastructure to the existing infrastructure.

Every characteristic is subdivided into fragmentations. They are rated upon literature. The ratings are divided into the following essential level: minimal (1), low (2), medium (3) and high (4). Each level refers to the corresponding mathematical value.

Characteristics are using the mathematical equivalent for generating the appropriate requirement. Following Gartner the combination of characteristics is structured in table 2.

Level of Second Characteristic (C2)	Level of First Characteristic (C1)				
	High	High	Medium	Low	Minimal
	High	High	Medium	Low	Low
	Medium	Medium	Medium	Low	Minimal
	Low	Low	Low	Low	Minimal
	Minimal	Low	Minimal	Minimal	Minimal

Table 2: Combination of Characteristics

That means that the output is the geometric mean of the two input values. The output is the square root of the product of the two characteristics.

$$\sqrt{C_1 * C_2}$$

For example: combining level medium (3) with level low (2), the output is 2,44 and therefore low. The mathematical equivalent is:

$$R = Requirement = \sqrt{C_1 * C_2} = \sqrt{3 * 2} = 2,44 \approx 2$$

The mathematical results are converted into the connected values. Requirement one, two and three have a positive scaling, while requirement four and five have a negative scaling. For that reason a meta scale, shown in table 3, was introduced.

Scaling	Level			
Positive Scaling (R1, R2, R3)	high	medium	low	minimal
Meta Scaling	highly advisable (4)	advisable (3)	satisfactory (2)	inadvisable (1)
Negative Scaling (R4, R5)	minimal	low	medium	high

Table 3: Scaling System

3.1 Selection of Methods for further Investigation

Rated by the five requirements (R1-R5), and after the transformation of the values the mathematical results vary from 2,4 to 3,6.

Methods that reach more than three have been taken into consideration for the prototypical implementation. Certificates, tokens, signatures, and key exchange form a set and therefore can be seen as one method. Results are shown in table 4.

Text Based Authentication and Credentials (3,2) are the most widely authentication technique being used [CDW04]. Due to their ease of implementation, cost and accessibility to multiple platforms they reach a high level. Graphical Password authentication has a high acceptance and security level. This authentication method was rated with 3,2.

Method	Authentication	Usability/Functionality	Security	Accuracy	Expenditure	Implementation Effort	Result
Biometrics							
Physiological	Face Recognition	satisfactory	satisfactory	advisable	satisfactory	highly advisable	2,6
	Finger Recognition	advisable	advisable	satisfactory	advisable	highly advisable	3,0
	Iris Recognition	advisable	advisable	highly advisable	inadvisable	highly advisable	3,0
	Retina Recognition	satisfactory	satisfactory	inadvisable	satisfactory	inadvisable	2,0
	Hand Geometry Recognition	advisable	advisable	advisable	satisfactory	highly advisable	3,0
Behavioral	Voice Recognition	highly advisable	highly advisable	advisable	highly advisable	highly advisable	2,4
Knowledge							
	Text Based Authentication	highly advisable	inadvisable	highly advisable	highly advisable	advisable	3,2
	Graphical Password Authentication	advisable	advisable	advisable	highly advisable	advisable	3,2
	Gesture Based Authentication	satisfactory	satisfactory	highly advisable	advisable	advisable	3,0
Property							
	Hardwaretoken	highly advisable	highly advisable	highly advisable	inadvisable	highly advisable	3,0
	Softwaretoken	highly advisable	highly advisable	highly advisable	satisfactory	highly advisable	3,4
	NFC	highly advisable	highly advisable	highly advisable	advisable	highly advisable	3,6
Location							
	GPS	satisfactory	advisable	highly advisable	advisable	advisable	3,0
	WLAN	advisable	highly advisable	highly advisable	highly advisable	advisable	3,6
Other							
	Certificates	highly advisable	advisable	highly advisable	advisable	advisable	3,4
	Signatures	highly advisable	advisable	highly advisable	advisable	advisable	3,4
	Key Authentication	highly advisable	advisable	highly advisable	advisable	highly advisable	3,6

Table 4: Evaluated Rating Matrix

Software Tokens (3,4) are eminently suitable for adding a second channel to the process of authentication can be created without user interaction. The support of security aspects is also given. Location based services like WLAN (3,6) and NFC (3,6) reach a high level due to the fact that they do not require pre-established user-agreement, key, distribution or communication overhead [Bao08]. Additional acceptability and access time had a high score. Digital Certificates (3,4), Signatures (3,4) and Key Exchange (3,6) protect confidentiality, authenticity and integrity by using the public key. The exchange of keys (data) by using certificates and signatures between entities is organized by a PKI. Once installed, the usability and functionality, security and functionality are high.

4 Prototypical Implementation

4.1 Security in Mobile Operating Systems

This chapter discusses the two major mobile operating systems [The11].

Android and iOS. Both of them have strong application layer security models. Android and iOS are generating unique numbers[1] for an application during the installation process. These identifier remain the same until the application is deleted.

Android uses an application UID to enforce the permission for the application. For example accessing the camera. The granted permissions are only set during installation and cannot be changed later.

iOS handles the access to certain resources by using the Mandatory Access Control (MAC). The user can decide at runtime whether an application has access to a certain resource or not [Wat12].

Besides the mentioned application layer security, Android and iOS are also isolating applications from direct hardware access which is called sandboxing [Goo]. Android uses a service layer called Hardware Abstraction Layer (HAL) [Tan09] and in comparison to iOS using a system based on the TrustedBSD project [WFMV03].

4.2 System Components

The components of the system, as shown in figure 1, are divided into three parts, Authentication Back End (ABE), Information Storage (IS) and AuthApp. The ABE comprises a web server, application server and an authentication agent (AuthAgent). It furthermore contains the main business logic for the authentication process. The business data are located in the IS. In this case a basic directory services are used. The client application, AuthApp, is the main part where the user interacts with the system. It handles the communication to the ABE and presents different authentication methods to the user.

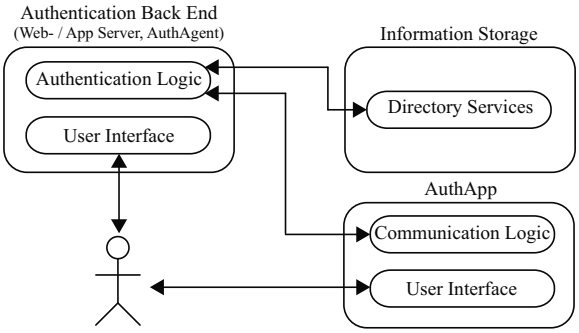

Figure 1: Complete Prototype Ecosystem

[1] Android: Unique Identifier (UID); iOS: Globally Unique Identifier (GUID)

4.3 Mobile Key

The Mobile Key showroom combines Near Field Communication (NFC) and credentials for the user authentication. AuthApp recognizes the NFC tag and reads the data on it. In case of the NFC authentication, a simple number is used as identification attribute. This number is stored on the NFC tag and in the users object in the IS. Once the data is read from the NFC tag, AuthApp requests the validation of the number. It sends an HTTP request to the ABE and processes the response. On the next step, the user enters his credentials and AuthApp performs an HTTP request to validate the credentials. Is the result also positive, the user is now properly authenticated.

4.4 Location Based

The Location Based showroom uses the BSSID from the connected wireless access point to authenticate the user in the first place. AuthApp gathers the BSSID and constructs a validation request. This request is send to the back end and is verified. The back end extracts the BSSID and checks if the BSSID is in the white list. Based on that result the back end returns âtrueâ or âfalseâ. After a successful BSSID authentication, an OTP generator is shown which requires a personal PIN to generate a code. This code is used to log in to a web service.

4.5 Mobile Desk

The Mobile Desk showroom uses certificates and graphical passwords to authenticate the user. In a previous step a suited device certificate is loaded on the mobile device. AuthApp uses the certificate and consults the back end service to validate the certificate. The next step is to enter a graphical password. AuthApp consults the back end server to validate the entered graphical password. When a positive match is found, AuthApp grants the access.

4.6 Quick Response Code and Credentials via Two Channels

This showroom uses the ability to separate username and password. The user has to use two physically independent systems. In this case, a desktop computer and a mobile device with camera.

On the desktop computer, the user types in his name in the Front End and generates a QR code. Then, he has to scan this QR code with the mobile device. The QR code is used to encode a URL. This URL is loaded in the mobile browser and the user can enter his password. If the correct password is entered, the desktop front end recognizes the successful login and grants access.

4.7 Front End Implementation

The Front End is where the user gets in touch with the system. It is browser based and uses the framework jQuery Mobile for the presentation. No device detection was used to distinguish between a mobile or desktop browser. For that reason, all devices (browsers) which access the front end will receive the same user interface. The interface is optimized for touch devices. Desktop user are still able to use the interface as normal due to the fact that a bigger button can still be clicked by a mouse pointer.

4.8 Back End Implementation

The Back End part of the system uses PHP as server side scripting language. The functionality, such as an authentication agent or communication to the directory services, are implemented in PHP.

There are several definitions about when a user is authenticated. One definition being when the credentials of the users returning an positive BIND to the directory service.

Another definition is comparing values, which are gathered as user input, with values from the directory. For example the showroom Mobile Desk uses a hash value which is generated in AuthApp by entering a graphical password. This hash is used to send a request to the Back End, validate the hash and response with a result.

4.9 AuthApp Prototype

AuthApp was developed based on previous analysis of the sufficient authentication methods on mobile devices. It is the central part of the mobile authentication system from a user perspective.

AuthApp has several authentication entry points gathering data from the user. The data is used to create an HTTP request which is send to the authentication back end. After receiving an HTTP response from the back end, AuthApp reacts by either continuing in the work flow or displaying an error message to the user.

4.10 Conclusion of Prototypical Implementation

This chapter discusses the implementation of different showrooms on iOS and Android. Each showroom differs from another, due to the combination of authentication methods. Thus, the Front End and Back End were basically the same. The Front End implementation was realized with jQuery Mobile while the Back End implementation uses PHP. A universal prototype that works with HTTP requests has been developed to combine the different demands of operating systems and showrooms.

All authentication methods used by the showrooms are available today. Some of them are more accepted than other. For example credentials are used by users for decades. On the other hand public-key authentication is far less common.

Additionally, a systems interface is used by users not by programmers! Due to this fact, it is vital to think about the users who are operating the system. Therefore, a detailed analysis of usability and testing is indispensable.

5 Evaluating the Usability of Mobile Authentication

The requirement Usability and Functionality has been selected to be verified by an usability test.

McLaughlin and Skinner have defined possible components of usability that have been used: confidence, ease of use, speed and understanding [MS10]. An additional component is the aspect of required background. Those components have been transformed into the following interrogations.

1. Is there a significant difference between the arithmetic average authentication time?
2. Is there a significant difference between the authentication time within the showrooms?
3. Is there a significant difference between the different operating systems focusing on the success quotient?

5.1 Used Methods

To obtain those aspired usability results different methods have been used. In order to receive a distinctive comparison, the testers filled in a personal questionnaire that also inquired their skills. A second method was observation, executed by the interviewer and the assistant. Problems and needed support were noted. Confidence and ease of use was verified by the standardized questionnaire AttrakDiff. To evaluate the understanding and the speed needed for a successful authentication time was measured by using a stopwatch. The tasks were explained in detail and an illustration was given as help. The task was considered as completed, when the tester has authenticated himself successfully. The group of participants amounted to 26 being divided into two groups, the target user group employees (14) and target user group students (12).

Considering Nielsen that the number of participants is 20 at the minimum the usability test produced reliable, replicable and applicable results [Nie94].

The testers have been mixed differently. The age ranged from 20 to 51, the tester group was male dominated and there was a majority of iPhone users present. Twelve of them were students while 14 of them were employees.

That corresponds with the described showrooms and therefore the results can be seen as reliable. Those are the consolidated results of the usability test. The results are subdivided into arithmetic average authentication time, authentication time showrooms and success quotient.

5.2 Arithmetic Average Time for Authentication

On average the fastest authentication could be done within 30 seconds using the iPhone and the showroom QR code. The second fastest authentication could be done with the Android (iPhone has no NFC) using the showroom Mobile Key (37 seconds). The showrooms Location Based enabled both iOS and Android users to authenticate within 39 seconds. The showroom Mobile Desk could be used to authenticate within 41 seconds, while using the showroom Mobile Desk (iPhone) the users needed 46 seconds to authenticate and 49 seconds to authenticate with the showroom QR code (Android). A reason for that difference may be the different frameworks the operating systems use for QR code recognition. This is displayed in figure 2.

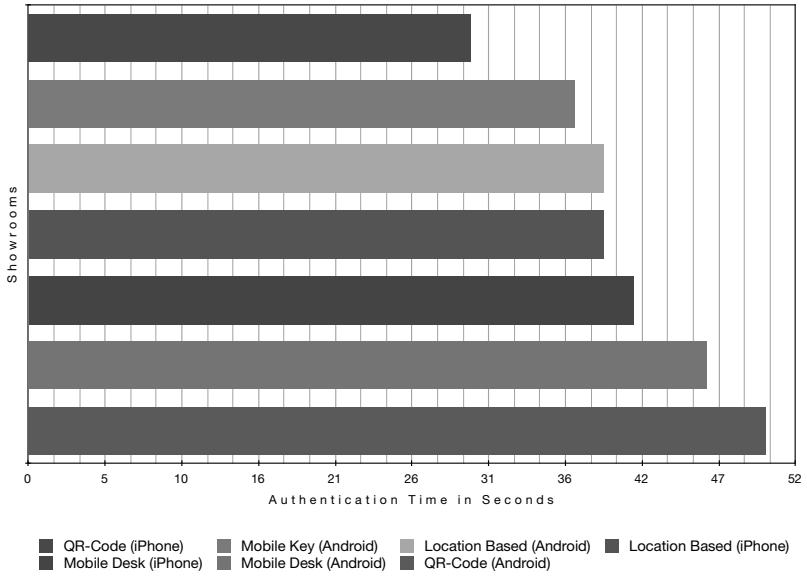

Figure 2: Arithmetic Average Time for Authentication of all Showrooms

5.3 Authentication Time Showrooms

The average authentication time shown in figure 3 is independent from the operating system and lists each showroom separately. The fastest showroom was Mobile Key (37 seconds), followed by Location Based (39 seconds) and QR code (40 seconds). The slowest authentication was achieved with the showroom Mobile Desk (44 seconds). It can be assumed that authentication with Mobile Key was possible in 37 seconds, because the user interaction (place the NFC Card on the mobile device) is minimal. Location Based and QR code are similar. The time of 44 seconds for the showroom Mobile Desk may be a result of the unknown graphical password that determined incorrect inputs that let to reentering the password and a corresponding time.

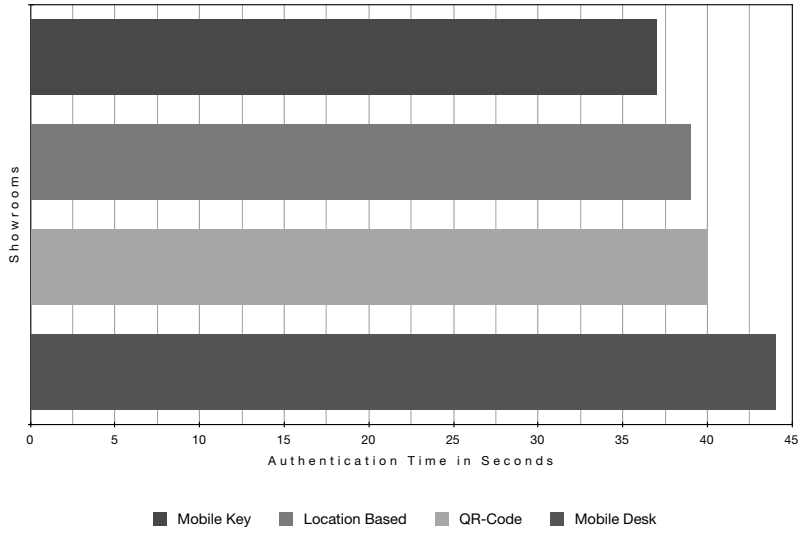

Figure 3: Authentication Time Operating Systems

5.4 Success Quotient

Success quotient describes the number of testers, that were able to authenticate themselves in less than four minutes; retry was possible. The highest success quotient of the showrooms (on average and independent from the operating system) was achieved with QR code, 93 percent.

That may be caused to the fact that QR codes are ubiquitous and the use of NFC techniques is quite new to consumers.

Ignoring the individual showrooms the success quotient of the Android was 86 percent, while the success quotient of the iPhone was 91 percent. The fact that 70 percent of the testers had prior knowledge of using the iPhone should be consulted here.

6 Conclusion

With the assistance of the usability test the results generated by the rating matrix could be specified within the requirements usability and functionality. The following showrooms are advisable (with certain reservations) for a successful mobile authentication with business application: QR code, Mobile Desk and Mobile Key. Those showrooms include the following highly recommended authentication methods: credentials, graphical password, second channel, QR code , certificates and NFC.

With regards to stakeholder interests the showrooms must be looked at in particular; arrangements may be combined differently. The basis for that redefinition is directly interconnected with the standards of usability and functionality, security, accuracy, expenditure and implementation effort are set by each company itself. The rating matrix that was developed can be used for that redefinition by rating the significance of each requirement. In the case of accuracy is being considered as key performance, the results can be multiplied by two. A less important requirement can be multiplied with the factor 0,5. For this reason the developed rating matrix is a useful instrument to find the appropriate authentication methods that match with specific needs to face the challenges of mobile authentication.

References

[AZEH09] Fadi Aloul, Syed Zahidi, and Wassim El-Hajj. Multi Factor Authentication Using Mobile Phones. *International Journal of Mathematics and Computer Science, 4 (2009), no.2, 65-80*, 2009.

[Bao08] Lichun Bao. Location Authentication Methods for Wireless Network Access Control. 2008.

[BM02] Nicky Boertien and Eric Middelkoop. Authentication in mobile applications. 2002.

[CDW04] Art Conklin, Glenn Dietrich, and Diane Walz. Password-Based Authentication: A System Perspective. *Proceedings of the 37th Hawaii International Conference on System Sciences*, 2004.

[DYB11] Mohammad Omar Derawi, Bian Yang, and Christoph Busch. Fingerprint Recognition with Embedded Cameras on Mobile Phones. March 2011.

[Gar12] Gartner. Gartner Authentication Method Evaluation Scorecards, 2011: Assurance and Accountability. 2012.

[Goo] Google Inc. Android Security Overview. visited 23.05.2012.

[Mou83] R. T. Moulton. *Network Security*. Datamation, 1983.

[MS10] Janice McLaughlin and David Skinner. *Developing Usability and Utility: A Comparative Study of the Users of New IT*. 2010.

[Nie94] Jakob Nielsen. *Usability Engineering*. Morgan Kaufman, 1994.

[Rae11] Jussi Raemaenen. Perceived security in mobile authentication. Master's thesis, Aalto University, School of Electrical Engeineering, August 2011.

[Sch04] Jean Scholtz. Usability Evaluation. *National Institute of Standards and Technology*, 2004.

[Tan09] Andrew S. Tanenbaum. *Modern operating systems*. Pearson Prentice-Hall, Upper Saddle River, NJ, 3. ed., pearson international ed. edition, 2009.

[The11] The Nielsen Company. Generation App: 62November 2011.

[vT05] Henk C.A. van Tillborg. *Encyclopedie of Cryptography and Security*. Springer, 2005.

[Wat12] Robert N. M. Watson. New approaches to operating system security extensibility. Technical Report UCAM-CL-TR-818, University of Cambridge, Computer Laboratory, April 2012.

[WFMV03] Robert Watson, Brian Feldman, Adam Migus, and Chris Vance. Design and Implementation of the TrustedBSD MAC Framework. April 2003.