Departamento Estudos e Investigação em Tecnologias de Informação e Sociedade

kriativ.tech

Edição Nº 7 – 28 de Agosto de 2018
ISSN Print: 1646-9976 | ISSN Online: 2184-223X |
DOI: https://doi.org/10.31112/kriativ-tech-2018-01-20
http://www.kriativ-tech.com http://www.kriativ-tech.pt

# Um estudo sobre o sistema operativo iOS da Apple

Isabel Alvarez
Professora Coordenadora no ISTEC
*ISTEC – Departamento de Estudos e Investigação em Tecnologias de Informação e Sociedade*

**Resumo**: O aparecimento do *smartphone* como uma tecnologia altamente complexa veio acompanhado por sistemas operativos móveis (OS), largas comunidades de desenvolvedores, fornecedores de conteúdos e redes complexas, formando em conjunto infraestruturas digitais. Estes *smartphones* tornaram-se poderosos dispositivos sendo basicamente versões em miniatura de computadores pessoais. Múltiplos factores tem tido um efeito significativo na evolução destas plataformas incluindo as *interfaces* gráficas de utilizador, plataformas de desenvolvimento, modelos de negócio e princípios de extração de valor. Contudo, a crescente popularidade e sofisticação dos *smartphones* também aumentou a preocupação sobre a privacidade dos utilizadores que usam estes dispositivos.

**Palavras-chave:** *sistemas operativos móveis, smartphones, iOS, aplicações móveis, segurança de dados*

**Abstract:** *The emergence of the smartphone as a highly complex technology was accompanied by mobile operating systems (OS), large developer communities, content providers and complex networks, forming together digital infrastructures. These smartphones have become powerful devices being basically miniature versions of personal computers. Multiple factors have had a significant effect on the evolution of these platforms including graphical user interfaces, development platforms, business models and value extraction principles. However, the growing popularity and sophistication of smartphones has also heightened concern about the privacy of users using these devices.*

***Keywords:*** *mobile operating systems, smartphones, iOS, mobile applications, data security.*

## I. Introdução

Os telefones móveis têm sido transformados de simples telefones a poderosos dispositivos multimédia de banda larga de acesso à internet. Embora os dispositivos móveis sempre tiveram sistemas operativos (OS) desde os anos 80, a sua função tornou-se muito mais importante nos últimos anos. Prevê-se mesmo que os dispositivos móveis em breve ultrapassem os computadores pessoais como as unidades de acesso mais comum à Web [5]. Consequentemente, os sistemas operativos móveis tornaram-se as plataformas fundamentais para criar novos serviços de cada vez maiores proporções e apoio à população mundial. Pode-se assim argumentar de pleno direito que a computação móvel se tornou uma das mais importantes infraestruturas de informação – complementando e ampliando os seus homólogos fixos.

As infraestruturas móveis digitais também formam uma nova fase da evolução das tecnologias de informação, refletindo o facto que estas se tornaram profundamente integradas socialmente [2]. A evolução das tecnologias de informação é coordenada através de diversos

mundos sócio-técnicos frequentemente com a ajuda de numerosas normas.
Há, contudo, que considerar a segurança das aplicações e acautelar as suas implicações na privacidade [18] devido a potenciais fugas, manipulação ou perdas de informação bem como o potencial valor da informação dos utilizadores para terceiros.

## II. Perspectiva Teórica

Considera-se a computação móvel como o último passo numa sucessão de sistemas tecnológicos intensamente escaláveis e infraestruturas relacionadas [7]. Estas infraestruturas de modernidade transformaram fundamentalmente a forma como o trabalho é feito, como se vive e como a sociedade é organizada. As infraestruturas tecnológicas anteriores incluem as estradas, canais, fornecimento de água e esgotos, caminhos de ferro, telégrafo, rádio, televisão, telefone, computação, e a internet bem como as comunicações móveis. Os telefones móveis evoluíram rapidamente ao longo dos últimos anos. As últimas gerações de *smartphones* são basicamente versões em miniatura de computadores pessoais; oferecem não só a possibilidade de fazer chamadas telefónicas e enviar mensagens, mas são também uma plataforma de comunicação e entretenimento para os utilizadores poderem navegar na web, enviar emails e jogar jogos [11]. Os telefones móveis são também omnipresentes permitindo acesso à informação de qualquer local e em qualquer altura.
Enquanto todas estas infraestruturas se manifestam em artefactos físicos e tecnológicos, o seu crescimento e evolução salientam a natureza essencialmente sociotécnica da sua evolução [15, 17]. Tal como infraestruturas técnicas anteriores, a computação móvel é profundamente integrada socialmente. A sua evolução é coordenada através de diversos mundos socio-técnicos, tais como normas, mercados, *designers* de *chips*, desenvolvedores de software aplicacional e fornecedores de conteúdo [16]. Além disto, numerosas normas são necessárias para coordenar a ação através destes mundos sociais e são aplicadas e, por sua vez, influenciadas, pela computação móvel incluindo, por exemplo, protocolos, plataformas de sistemas operativos móveis e práticas empresariais. Em termos simples, a evolução de grandes infraestruturas tecnológicas é tanto um fenómeno social como técnico [8]. Consequentemente, a computação móvel como uma infraestrutura tecnológica necessita ser estudada analisando-se os processos em curso da sua integração em práticas individuais, organizacionais, institucionais e de mercado, de forma a permitir e conduzir a novos comportamentos sociais.

## III. Sistema Operativo Móvel – O iOS da Apple

O iOS é o sistema operativo para vários dispositivos da Apple, sendo um dos mais importantes o *smartphone*[19] o qual, logo no seu lançamento, incluía um ecrã táctil grande e, já nessa altura, especificações de *hardware* impressionantes [21].
A estratégia inicial da Apple em 2007-2008 para as aplicações para o iPhone, era que os programadores criassem aplicações para a web que pudessem ser acedidas através do *Browser Safari* integrado no iPhone. Esta abordagem desenvolvida na Web 2.0 existente e tecnologias AJAX, necessitava adaptação ao pequeno ecrã do dispositivo bem como a outras características.
Na segunda fase (2008-2009) a Apple introduziu um novo conjunto de desenvolvimento de *software* (*Software Development Kit* - SDK) que permitia aos programadores desenvolver aplicações nativas com base em muitos APIs do iPhone – expandindo assim fortemente o potencial da sua infraestrutura digital emergente. O aumento da flexibilidade da plataforma do iPhone desencadeou uma nova oportunidade para as empresas de desenvolvimento aplicacional. A Apple adicionou à sua infraestrutura existente a *App Store* como o único canal de distribuição oficial para desenvolvedores terceiros.

Em 2009-2010, foi lançada uma terceira versão do sistema operativo e do SDK com mais de 100 novas características e 1,000 novos APIs [14]. Algumas das alterações introduzidas foram em resposta a preocupações apresentadas pelas empresas / programadores de desenvolvimento.
Numa quarta fase foi adicionado outro fator à sua plataforma móvel com o lançamento do iPad no início de 2010 em versões com e sem ligação celular sem fios. O sistema operativo do iPhone (renomeado iOS) e o SDK foram melhorados para suportar todos os três tipos de dispositivos, e no caso do iPhone e do iPod, várias gerações de hardware. Uma quarta versão do sistema operativo (OS) e do SDK ofereciam mais de 100 novas funcionalidades e mais de 1500 novas APIs.
As aplicações para o iOS são escritas em *Objective-C* usando a biblioteca *Cocoa Touch*. *Objective-C* é uma extensão da linguagem C, enquanto que o *Cocoa Touch* é um conjunto de classes [22]. Enquanto que o C# e Java (usados no desenvolvimento para *Android* e *Windows Phone*) são bastante similares em sintaxe, a biblioteca do *Objective-C* providencia uma alternativa diferente. O *Objective-C*, tal como o nome indica, suporta programação orientada a objectos.

## IV. Privacidade dos utilizadores

Contudo, a crescente popularidade e sofisticação dos *smartphones* também aumentou a preocupação sobre a privacidade dos utilizadores que operam estes dispositivos [11]. Estas questões têm sido exacerbadas pelo facto de ser cada vez mais fácil para os utilizadores instalar e executar aplicações. Para proteger os seus utilizadores de aplicações maliciosas, a Aple introduziu um processo de verificação (*vetting process*) o qual assegura que todas as aplicações seguem as regras de privacidade da Apple antes de poderem ser disponibilizadas através do *App Store*. Lamentavelmente, este processo de verificação não está bem documentado, e tem havido casos em que aplicações maliciosas têm de ser removidas do *App Store* após reclamações dos utilizadores [11].
*Egele et al* (2011) investigaram as ameaças de privacidade que as aplicações escritas para o iOS da Apple colocavam aos utilizadores. Apresentam uma nova abordagem e uma ferramenta, iPOS, que permite analisar os programas para possíveis fugas de informação sensível a partir de uma unidade móvel para terceiras partes. O PiOS usa análise estática para detectar fluxos de dados em *Mach-Obinaries*, compilado a partir do código de *Objective-C*. As experiências mostraram que, com a exceção de alguns casos, a maior parte das aplicações respeitam a informação identificável nos dispositivos dos utilizadores.
Considerando a vasta gama de aplicações para telefones móveis e a sua popularidade, não é de surpreender que os *smartphones* armazenem uma quantidade crescente de informação sigilosa sobre os seus utilizadores. Por exemplo, o livro de endereços contém informação sobre as pessoas com quem cada utlizador interage. O receptor de GPS revela a localização exata do dispositivo; fotografias, emails e o historial de navegação podem conter informação privada. Além disto, por exemplo, as aplicações móveis de saúde (*mHealth*) que visam providenciar acesso constante a tecnologia especialmente concebida para apoio ao sector da saúde com o objectivo potencial de facilitar o apoio aos cidadãos [18], confrontam-se com o risco da segurança e privacidade da informação dado que os utilizadores revelam informação médica sensível e privada.
Desde a introdução dos sistemas operativos iOS da Apple e o Android, as vendas dos *smartphones* aumentaram significativamente. Adicionalmente, a introdução de locais de mercado para as aplicações (tais como o *AppStore*) providenciou uma forte força motora económica, tendo sido desenvolvidas milhares de aplicações para o iOS. Assim sendo, verifica-se a necessidade de serem criados mecanismos para proteger os dados sensíveis contra as aplicações maliciosas.
Com o iOS da Apple, os utilizadores são protegidos pelo acordo de licenciamento de desenvolvimento da Apple [12]. Este documento

define os termos de aceitação para acesso a dados sensíveis. Uma regra importante é que uma aplicação é proibida de transmitir quaisquer dados a menos que o utilizador dê o seu consentimento explícito. Além do mais, uma aplicação pode pedir autorização só quando os dados forem diretamente requeridos para implementar uma determinada funcionalidade da aplicação. Para reforçar as restrições estipuladas no acordo de licenciamento, a Apple introduziu um processo de verificação (*vetting process*) já referido atrás.

Durante este processo de verificação, a Apple escrutina todas as aplicações submetidas pelos desenvolvedores externos. Se uma aplicação é considerada estar de acordo com o contrato de licenciamento, é aceite, assinada digitalmente e disponibilizada através do *iTunes App Store*. É importante observar que acedendo ao *App Store* é a única forma para que os utilizadores de dispositivos iOS não modificados, possam instalar aplicações. Isto assegura que só os programas aprovados pela Apple podem correr nos iPhones (ou outros produtos da Apple). Para se poder instalar e executar outras aplicações, é necessário desbloquear o dispositivo e desativar a verificação que assegura que só programas aprovados pela Apple podem correr.

Lamentavelmente, os detalhes exactos do processo de verificação (*vetting process*) não são conhecidos publicamente. Este facto dificulta a confiança plena das aplicações desenvolvidas por terceiras partes, e levanta dúvidas sobre a proteção adequada aos dados dos utilizadores. Por outro lado, há ocorrências conhecidas [20] em que uma aplicação maliciosa passou o processo de verificação, tendo sido mais tarde retirada do *App Store* quando a Apple tomou conhecimento do seu comportamento nocivo.

Para analisar as aplicações em iOS, *Egele et al* desenvolveram em 2011 o PiOS, uma ferramenta automática que pode identificar possíveis quebras de privacidade nas aplicações do iOS. O PiOS usa análise estática para verificar as aplicações procurando a presença de caminhos de código onde uma aplicação aceda primeiro a informação sensível e subsequentemente transmita esta informação através da rede. Dado que não existe código fonte disponível, o PiOS tem de executar a sua análise diretamente sobre os binários. Embora estática, a análise binária é já por si complicada, sendo o trabalho mais dificultado pelo facto de que muitas aplicações em iOS são desenvolvidas em *Objective-C*, que é um superconjunto da linguagem de programação C com características orientadas a objectos.

Assim sendo, o objectivo do PiOS é detectar quebras de privacidade nas aplicações escritas para iOS. Como quebra de privacidade, pode-se definir qualquer evento em que uma aplicação para iOS leia dados sensíveis do dispositivo e envie esses dados para uma terceira parte, sem o consentimento do utilizador. Para pedir o consentimento do utilizador, a aplicação deverá mostrar uma mensagem (através da interface de utilizador) que especifica os itens de dados a ser acedidos. Além disto, ao utilizador é dada a escolha de autorizar ou negar este acesso. Quando uma aplicação não pede a autorização do utilizador, está em violação direta do acordo de licenciamento para desenvolvimento de programação para o iPhone [12], que estipula que não podem ser transmitidos dados sensíveis a menos que o utilizador expresse explicitamente o seu consentimento.

O acordo de licenciamento também estipula que uma aplicação possa pedir autorização de acesso só quando o adequado funcionamento da aplicação dependa da disponibilidade dos dados. Lamentavelmente, este requisito torna necessário perceber-se a semântica da aplicação e o seu uso previsto.

## VII. Conclusão

A crescente popularidade e sofisticação dos *smartphones,* tais como o *iPhone,* também trouxeram crescentes preocupações sobre a privacidade dos seus utilizadores. Para abordar estas questões, os desenvolvedores dos sistemas operativos para *smartphones* têm usado diferentes modelos de segurança para proteger a segurança e privacidade dos utilizadores. A Apple decidiu aliviar a carga dos seus utilizadores de iPhone e determinar, em seu nome, se uma aplicação está conforme com as

regras predefinidas sobre privacidade. Infelizmente, tal como referido acima, o processo de verificação da Apple não é público, tendo havido casos no passado [20] em que se descobriu que aplicações previamente verificadas violavam, contudo, as regras de privacidade definidas pela Apple.

De forma a estimular a aceitação e confiança do utilizador [18], verifica-se a necessidade de desenvolvimento e utilização de medidas e processos adequados de segurança de forma que os utilizadores possam beneficiar de aplicações perfeitas e acessíveis, sem se exporem a repercussões sérias de violações de segurança e privacidade.

## XIV. Referências


[1] Y. Yoo, "Computing in Everyday Life: A Call for Research on Experiential Computing," MIS Quarterly, vol. 34, pp. 213-231, 2010.

[2] D. Tilson, K. Lyytinen, and C. Sørensen, "Digital Infrastructures: The Missing IS Research Agenda," Information Systems Research, vol. 21, pp. 748-759, December 2010.

[3] M. Needham and N. Rich, "Psion the Organiser," Accountancy, vol. 100, pp. 137-138, 1987.

[4] J. E. Vascellaro and A. Sharma, "Google's Android Has Phone Debut via T-Mobile," Wall Street Journal - Eastern Edition, vol. 252, p. B3, 2008.

[5] Gartner, "Gartner Highlights Key Predictions for IT Organizations and Users in 2010 and Beyond," 2010.

[6] K. Lyytinen and Y. Yoo, "Research Commentary: The Next Wave of Nomadic Computing," Information Systems Research, vol. 13, pp. 377-388, 2002.

[7] D. Tilson, C. Sorensen and K. Lyytinen, “Change and Control Paradoxes in Mobile Infrastructure Innovation – The Android and iOS Mobile Operating Systems Cases”, 45th Hawaii International Conference on System Sciences, 2012

[8] O. Hanseth and K. Lyytinen, "Design theory for dynamic complexity in information infrastructures: the case of building internet," Journal of Information Technology vol. 25, pp. 1-19, 2010.

[9] Y. Yoo, O. Henfridsson, and K. Lyytinen, "The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research," Information Systems Research, vol. 21, pp. 724-735, 2010.

[10] A. Tiwana, B. Konsynsky, and A. A. Bush, "Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics," Information Systems Research, vol. 21, pp. 675-687, 2010.

[11] Manuel Egele, Cristopher Kruegel, EnginKirda and Giovanni Vigna, “PiOS: Detecting Privacy Leaks in iOS Applications”, NDSS Symposium 2011

[12] iPhone Developer Program License Agreement. http://www.eff.org/files/20100302 iphone dev agr.pdf.

[13] Gartner Newsroom. Competitive Landscape: Mobile Devices, Worldwide, 2Q10. http://www.gartner.com/ it/page.jsp?id=1421013, 2010.

[14] A. Ghazawneh and O. Henfridsson, "Governing ThirdParty Development Through Plaform Boundary Resources," in ICIS, 2010, p. Paper 48.

[15] T. P. Hughes, Networks of power: electrification in Western society, 1880-1930. Baltimore, Maryland: John Hopkins University Press, 1983.

[16] D. Tilson, "The interrelationships between technical standards and industry structures: Actor-network based case studies of the mobile wireless and television industries in the US and the UK ": Ph.D Thesis, Case Western Reserve University, 2008.

[17] P. N. Edwards, S. J. Jackson, G. C. Bowker, and C. P. Knobel, "Understanding Infrastructure: Dynamics, Tensions, and Design," 2007, p. Report of a Workshop on "History & Theory of Infrastructure: Lessons for New Scientific Cyberinfrastructures".

[18] Tobias Dehling, Fangjian Gao, Stefan Schneider and Ali Sunayev, “Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android”, JMIR mHealth and uHealth, 2015

[19] http://www.apple.com/pr/library/2007/01/09Apple-Reinvents-thePhone-with-iPhone.html [Accessed: 13 November 2013]

[20] Wired. Apple Approves, Pulls Flashlight App with Hidden Tethering Mode. http: //www.wired.com/gadgetlab/2010/07/ apple-approves-pulls-flashlight% 2dapp-with-hidden-tethering-mode/.

[21] https://developer.apple.com/ [Accessed: 13 November 2013]

[22] J. Conway and A. Hillegass, iPhone Programming: The Big Nerd Ranch Guide (Big Nerd Ranch Guides), Addison-Wesley, 2010.