Early Report: How to Improve Programmers' Expertise at App Security?

Charles Weir
Security Lancaster
Lancaster University
c.weir1@lancaster.ac.uk

Awais Rashid
Security Lancaster
Lancaster University
a.rashid@lancaster.ac.uk

James Noble
Victoria University
Wellington, NZ
kjx@ecs.vuw.ac.nz

Abstract

Apps present a significant security risk. Developer inexperience of security is a major contributor to this risk. Based on interviews with a dozen app security experts we identify that most app programmers simply do not care about security. Only by working on the factors influencing programmers' motivation, and afterwards developing their whole system security skills, shall we shall we begin to see the kind of secure apps that industry needs.

The western world relies heavily on apps. Apps run on mobile phones, on PC browsers, as PC native apps, or as the software running on sensors and controllers in the Internet of Things, but all share a number of common features. Typically they communicate with one or at most a few services on the internet; they are not advertised on the Internet in the way that services must be; and in many cases they may contain data, have access to data, or control services that could embarrass or harm an individual or organisation if they are compromised.

So securing apps that run on such services is becoming increasingly important. There are two questions that address this, both worthwhile: (1) how can we improve the systems and compilers that host and produce such apps; and (2) how can we improve the security skills of the developers who produce them? Most existing work, such as [EOMC11], has studied the kinds of mistakes programmers make, but there has been little exploration of underlying causes, though a recent survey of US organisations [Pone15] found that 73% of respondents saw developer lack of skills as a major cause of app security issues. This paper, therefore, is an early report of an ongoing research project to explore the second question.

In: D. Aspinall, L. Cavallaro, M. N. Seghir, M. Volkamer (eds.): Proceedings of the Workshop on Innovations in Mobile Privacy and Security IMPS at ESSoS'16, London, UK, 06-April-2016, published at http://ceur-ws.org

1. Research Approach

For this research we interviewed a dozen experts in mobile app security: developers, architects and team leaders. We chose our interviewees opportunistically through contacts and referrals; they average some 30 years of industry experience, are typically quite senior in their professions, and work in organisations ranging from start-ups to global software giants. Since the purpose was to find positive approaches to app security, the interview questions derived from Appreciative Inquiry [Reed06], and focussed on success stories and aspirations. To analyse the results, we used Grounded Theory [GlSt73], transcribing and coding the interviews to draw out the participants' concerns as themes and correlations between interviews. This report is based on overview results of all twelve interviews plus detailed analysis of the first four, and includes quotations.

The results surprised us. We'd hoped the experts would tell us of learning resources and successful security training methods. The participants, even those who'd been active in creating resources for programmers to learn, didn't feel that such resources had solved the problems. Instead they highlighted two main issues:

1.1 Lack of interest in security

Programmers simply aren't motivated to get security right. The youth and inexperience of many programmers means they don't have a feeling for the possible impact of a security problem: "It's not that [programmers] have passed judgement on it, and that it is unimportant – they just don't realise that it is important".

Also, few of the stakeholders in apps are interested in security at all – most non-experts, if they think of it at all, expect security to happen automatically; security is seen as an additional cost, and not one justified by industry experience of apps so far: "You can see that from the Apps World [exhibition] where there's no mention of security at all. It's not on people's radar."

1.2 Need for whole system security

Much of the literature and research has focussed on small-scale aspects of security, such as correct use of APIs, and approaches for securing data. But in practice

a main source of security issues is wider, typically related to the problem domain or the way systems interconnect: “The things that are the most challenging around security really are trying to understand the threat landscape and trying to understand how threats are realised”.

To address these requires developers who can analyse security threats, and who can explain security issues to stakeholders in ways that allow them to make decisions.

2. Tackling these issues

Most of the interviewees had significant experience of a variety of projects involving software security, and they offered a variety of practical solutions to these problems. We’ll look at each in turn.

2.1 Tackling programmers’ lack of interest in security

Different interviewees suggested different ways to address this. Most common was an approach we’d sum up as ‘corporate interest’. Here the organisation itself drives programmer interest: company targets, product specifications, project processes and team organisation all focus on app security, including whole system security. The result is that every team member takes an interest; it becomes an exciting part of their normal day’s work.

Where this corporate interest is lacking, some suggested enforcing it as part of professional discipline: app security and motivation to be included in university courses and as a necessity for professional qualifications. Others prefer to wait for app-based security breaches that will change industry ways of thinking.

One interviewee, who uses developers in an external company that hadn’t been security-aware, finds it very effective to have a long discussion with each new developer on his projects, getting to know a bit about their life and relating their experiences to the security requirements of his project.

2.2 Tackling Whole System Security

Our interviewees highlighted a variety of successful techniques they use to achieve app security, including:

Analysis: They use ideation sessions working with stakeholders and penetration testing experts of different possible attacks on the system; they analyse reasons for attacks and profiles of possible attackers; and they do formal and informal risk assessments combining the likelihood of each attack with its potential impact.

Effective communication: They find good ways of communicating security decisions in ways their stakeholders can understand: “this data may be visible to an attacker. Do you mind?”

Development techniques: They use processes to avoid the kinds of defect in software that can lead to a security breach. Examples are pair programming, code reviews, using code analysis tools and security-aware choices of libraries and environments.

Continuous feedback: They ensure they receive security status information from released products; they analyse emergent security issues and plan fixes into the development stream for the future.

Continuous enhancement: They emphasise the continuous nature of security: the need for regular upgrades of the live software. They also use development contracts and system architectures that allow for this rather than the more traditional ‘fire and forget’ approach.

3. Summary and next steps

So a major threat to app security is that few app programmers are motivated to do anything about it. And for those that are, the major wins will be in addressing skills in whole system security.

This paper represents early findings; further work will expand the taxonomy of solutions in section 2. This will provide insights into the issues underpinning app programmers’ security behaviour, and into mitigation measures that work in practice.

4. References

[EOMC11] ENCK, WILLIAM ; OCTEAU, DAMIEN ; MCDANIEL, PATRICK ; CHAUDHURI, SWARAT: A Study of Android *Application* Security. In: *USENIX security symposium* (2011), Nr. August

[GlSt73] GLASER, BARNEY G ; STRAUSS, ANSELM L: *The Discovery of Grounded Theory : Strategies for Qualitative Research*, *Observations*. Chicago : Aldine Transaction, 1973 — ISBN 9780202302607

[Pone15] PONEMON INSTITUTE: *The State of Mobile Application Insecurity*, 2015

[Reed06] REED, JAN: *Appreciative inquiry: Research for change* : Sage, 2006 — ISBN 1452279020