From: Eric Friedman ([redacted])
To: Srinivas Vedula ([redacted])
CC: GP Fasoli ([redacted]) Julien Lerouge ([redacted]) Ritwik Kumar ([redacted])
BCC:
Subject: Re: slides for review
Attachments: Usecases_flow_diagrams.key;
Sent: 01/25/2016 03:38:38 PM 0000 (GMT)

I can't do your Monday slot. Tuesday is no better. Wednesday is good at 1. But you don't need me to proceed.

Regarding your rogue app scenario: this is phishing. For it to work, the phisher would have to have compromised the APNS send key of the spoofed service. That seems unlikely.

Regarding review processes: please don't ever believe that they accomplish anything that would deter a sophisticated attacker. I consider them a wetware rate limiting service and nothing more. Yes, they sometimes catch things, but you should regard them as little more than the equivalent of the TSA at the airport. Their KPI is "how many apps can we get through the pipe" and not "what exotic exploits can we detect?"

Eric

> On Jan 24, 2016, at 12:39 AM, Srinivas Vedula wrote:
>
> All,
>
> I have added new flow diagrams and use cases. Please review.
>
> I booked a slot on Augustin's calendar to update him. I am thinking of moving it to Tuesday. Let me know if you would rather do it on Monday.
>
> Creating the use case for use on iOS brought up a question in today's iOS apps.
>
> How do we handle the possibility that a rogue app pretends to be a genuine app. Let's say a rogue app reversed all of e-trade's login flows and implemented it in their app. Essentially, it will be a proxy for e-trade. It will genuinely log you into e-trade but will just siphon the credentials while doing so. That should be pretty straightforward to do. If done properly a user can be tricked into downloading the app and giving it the login info.
>
> Do you know how we deal with it today? We haven't seen an instance like that till now. That is probably what the review process is supposed to look at but it will be nice if we have a technical solution for it. We kind circumvented the browser+HTTPs combination with binary apps.
>
> - Srinivas
>
>