Segurança em iOS

Protegendo os dados de seus aplicativos

Trilha iOS

Guilherme Andrade

@gui_aandrade

Introdução

Tudo são dados do usuário

Tudo são dados do usuário

- Documentos
  - Textos
  - Fotos
- Credenciais
- Preferencias

Os dados dos usuários estão em todas as partes

- No dispositivo
- Em trânsito
  - dados de rede (3G, WiFi)
- Fora do dispositivo
  - Servidor
  - iCloud
  - Backup

O que irei demonstrar

- Mecanismos de segurança do sistema iOS
- Técnicas de proteção de dados
- Análise de aplicativos conhecidos da App Store

O que não irei demonstrar

- Segurança em aparelhos com Jailbreak
- Proteção de dados em trânsito

Mecanismos de segurança do iOS

Sandboxing

Sandboxing

- Aplicativos iOS são instalados em diretórios exclusivos para cada app
- Cada aplicativo possui uma "casa" própria, onde são incluídos os dados e suas preferências
- Os dados não podem ser compartilhados entre aplicativos
- Importante: O propósito de um sandbox é limitar os danos que um aplicativo comprometido pode causar em outros aplicativos ou em outras partes do sistema.

Kik Message

.app | Documents | Library | tmp

Camera+

.app | Documents | Library | tmp

LogoQuiz

.app | Documents | Library | tmp

Code Signing

- Todos os aplicativos iOS devem ser assinados com um certificado
  - Apps fornecidas com o aparelho são assinados pela Apple
  - Apps de terceiros são assinados com um certificado emitido pela Apple
- Não é possível instalar aplicativos de fontes desconhecidas

Code Signing

- Após o boot do kernel, o sistema controla todos os processos de usuário e aplicativos
  - Todos os apps de fonte conhecida e aprovada
  - Aplicativo não foi modificado desde que foi instalado ou atualizado

Address Space Layout Randomisation

- É um método de segurança que envolve randomizar os endereços de memória dos aplicativos em execução
- Foi introduzido no iOS 4.3
- Dificulta os ataque de "corrupção de memória"
- É ativo através da flag de compilação -fPIE

Compilação sem -fPIE

Main Executable	Heap	Stack	Libraries	Linker
0x2e88	0x15ea70	0x2fdff2c0	0x35e3edd1	0x2fe00000
0x2e88	0x11cc60	0x2fdff2c0	0x35e3edd1	0x2fe00000
0x2e88	0x14e190	0x2fdff2c0	0x35e3edd1	0x2fe00000
0x2e88	0x145860	0x2fdff2c0	0x35e3edd1	0x2fe00000
Main Executable	**Heap**	**Stack**	**Libraries**	**Linker**
0x2e88	0x174980	0x2fdff2c0	0x35e3edd1	0x2fe00000
0x2e88	0x13ca60	0x2fdff2c0	0x35e3edd1	0x2fe00000
0x2e88	0x163540	0x2fdff2c0	0x35e3edd1	0x2fe00000
0x2e88	0x136970	0x2fdff2c0	0x35e3edd1	0x2fe00000

Compilação com -fPIE

Main Executable	Heap	Stack	Libraries	Linker
0xd2e48	0x1cd76660	0x2fecf2a8	0x35e3edd1	0x2fed0000
0xaae48	0x1ed68950	0x2fea72a8	0x35e3edd1	0x2fea8000
0xbbe48	0x1cd09370	0x2feb82a8	0x35e3edd1	0x2feb9000
0x46e48	0x1fd36b80	0x2fe432a8	0x35e3edd1	0x2fe44000

Main Executable	Heap	Stack	Libraries	Linker
0x14e48	0x1dd26640	0x2fe112a8	0x35e3edd1	0x2fe12000
0x62e48	0x1dd49240	0x2fe112a8	0x35e3edd1	0x2fe60000
0x9ee48	0x1d577490	0x2fe9b2a8	0x35e3edd1	0x2fe9c000
0xa0e48	0x1e506130	0x2fe9d2a8	0x35e3edd1	0x2fe9e000

Ferramentas

iExplorer

iExplorer

- Permite explorar arquivos e pastas existentes no aparelho
- Não necessita de Jailbreak
- 100% freeware
- Compatível com Mac e Windows
- http://www.macroplant.com/iexplorer/

Demo

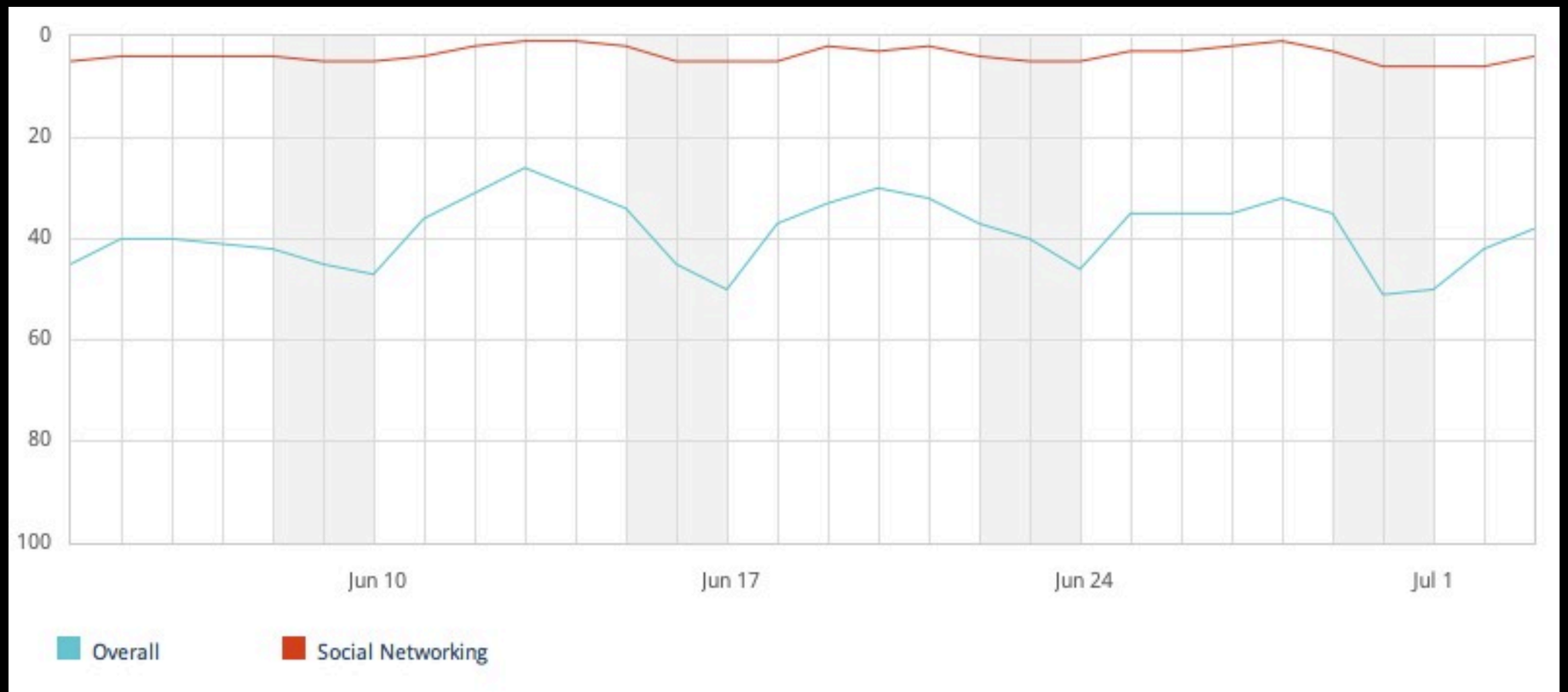
Técnicas de proteção de dados

Proteção de dados sensíveis do usuário

Proteção de dados sensíveis do usuário

- Os usuários estão confiando seus dados para o aplicativo
- Os dados podem ser sensíveis
- Assuma que é e proteja!

Case: Kik Messenger



Proteção de dados sensíveis do usuário

- Perigos reais
  - Aparelhos perdidos
- Credenciais são valiosas

Implementação segura

- Nunca guarde dados sensíveis com o NSUserDefaults
- Utilize sempre o Keychain
- SSKeychain é simples de usar!
  - https://github.com/samsoffes/sskeychain

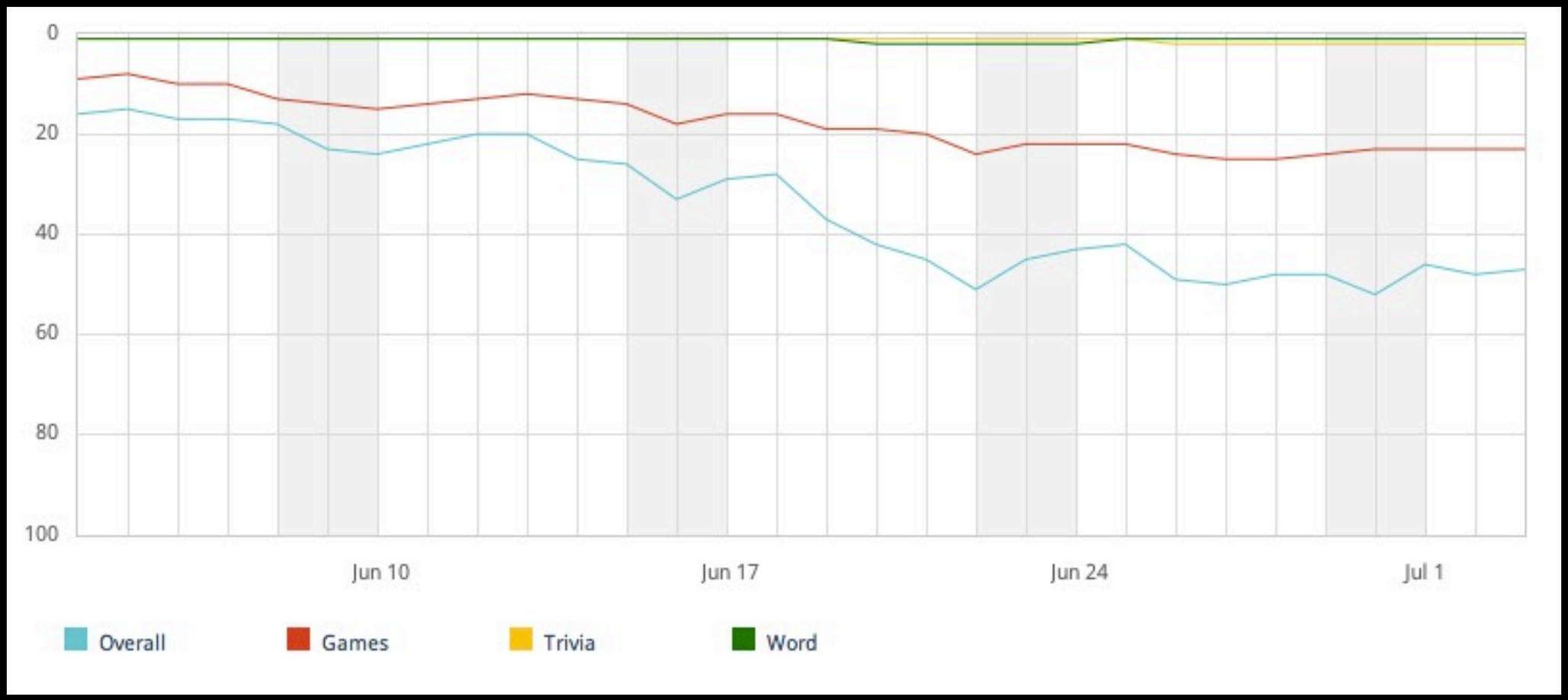
Demo

Proteção de dados sensíveis do aplicativo

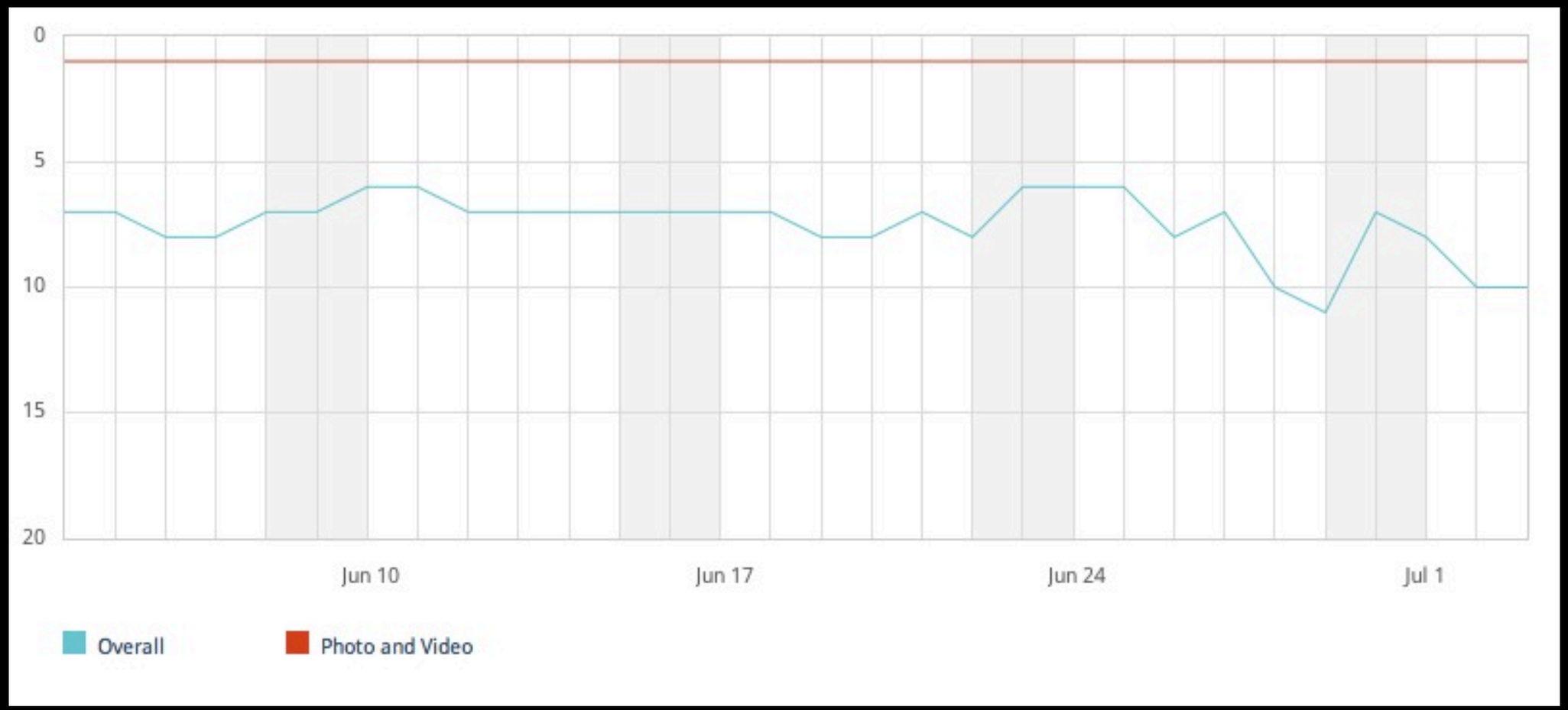
Proteção de dados sensíveis do aplicativo

- Os aplicativos também possuem dados sensíveis
- Muitas vezes os dados estão diretamente ligados ao negócio do aplicativo

Logo Quiz


0
20
40
60
80
100
Jun 10
Jun 17
Jun 24
Jul 1
Overall
Games
Trivia
Word

Camera +



Implementação segura

- Utilize o SQLCipher para criptografia do banco de dados
- Dados menores podem ser salvos no Keychain

Proteção de dados no dispositivo

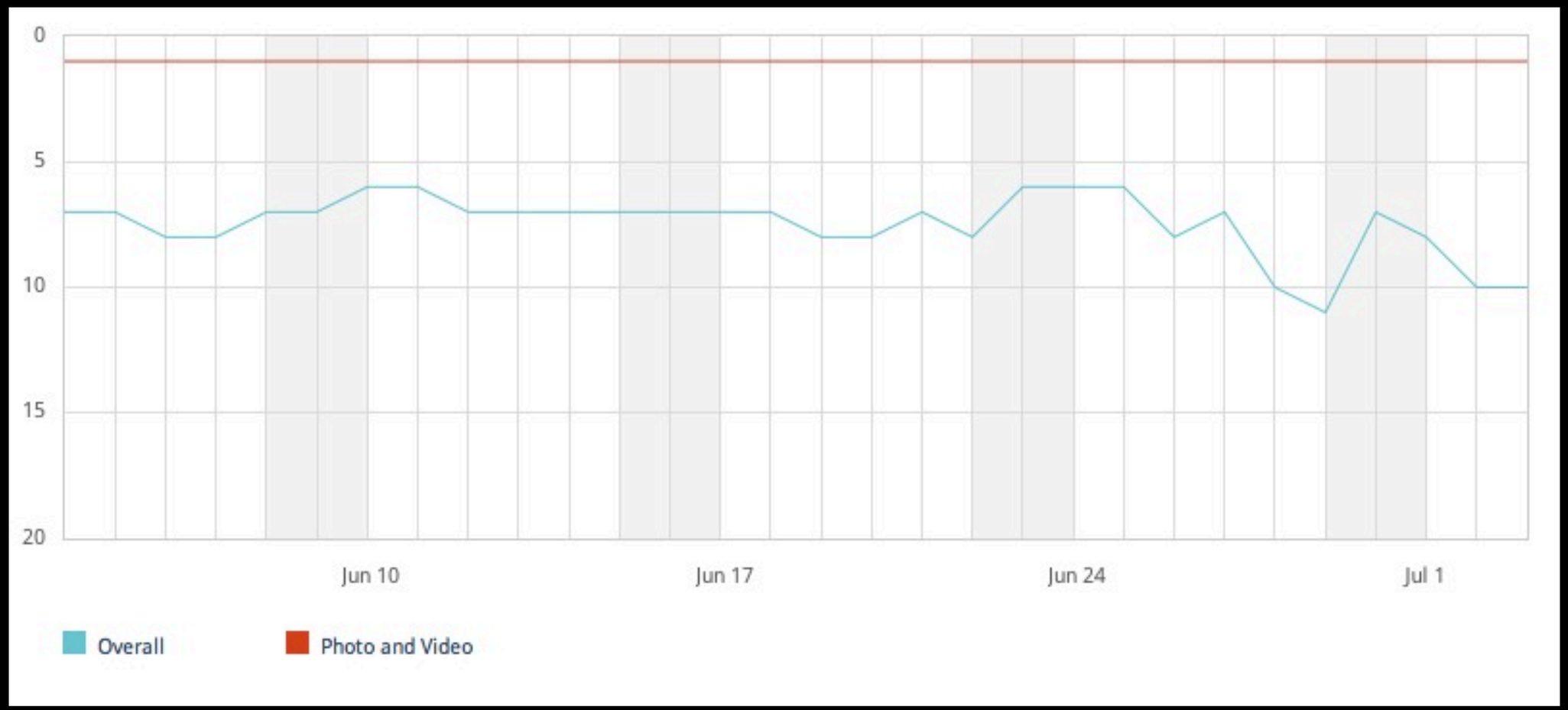
Proteção de dados no dispositivo

- Todos os dados devem ser armazenados de forma segura no aparelho
- Desbloqueio e ferramentas forenses permitem o acesso ao sistema de arquivos
- A proteção é necessária no caso de um dispositivo perdido ou roubado

iOS Data Protection

- Mecanismo de segurança existente no iOS
- Os dados são amarrados a senha do usuário
- A segurança é implementada no padrão “File based”

Camera +



Demo

Conclusão

- Tenha sempre em mente o nível de segurança que deseja adotar
- Lembre-se que o usuário está confiando todos os seus dados para o aplicativo
- Valide a segurança implementado análises na app gerada

Dúvidas?

Guilherme Andrade

gui.aandrade@gmail.com

@gui_aandrade