Week 15
Cloud-Service Security Topics

Mastering Cloud Computing

Coleman Kane
(based on material by Paul Talaga)

UNIVERSITY OF Cincinnati

Cloud Model Introduces New Security Problems

New model encourages consumers to remotely-host data

Cross-user data now exposed to operations requested by non-data owners

Increasing reliance on service offerings you have little control over

“Frankenstein monster” applications

UNIVERSITY OF Cincinnati

Information (rather than Data) management

"Information Rights Management" - thinking in terms of information, not data or files

Conceive of new models for data access:

- Data owner (read, write, provision)
- Data store (write-only)
- Data reader (read-only)
- Data analyzer (Id blind, read-only)
- Data producer (Id blind, write-only)

UNIVERSITY OF Cincinnati

Facebook: Identity Manager

Example: “Facebook Login”
https://developers.facebook.com/docs/facebook-login/

Many established social media platforms now offer identity management services

Original (“core”) mission was social media, now 3rd parties relying upon them for authentication purposes

In some cases, even authorization (such as providing access to PII you manage)

Risky development, as if Facebook suffers compromise, your application is impacted (either insecure, or access restricted) and you’re reliant on Facebook’s timeline

News sites, Pokemon Go, Blogs, etc...

UNIVERSITY OF Cincinnati

Snapchat Private Data Exposure

Snapchat identifies you by phone number (numeric, globally unique Id)

You can “find friends” by uploading your entire address book and it will tell you what numbers it hits on (private data leakage)

Feature abused in 2014 to identify valid phone numbers through brute-force

UNIVERSITY OF Cincinnati

Snapchat Private Data Exposure

Snapchat identifies you by phone number (numeric, globally unique Id)

You can “find friends” by uploading your entire address book and it will tell you what numbers it hits on (private data leakage)

Feature abused in 2014 to identify valid phone numbers through brute-force

UNIVERSITY OF Cincinnati

“Snappening” Event

Later in 2014, a worse exposure: “Short-lived” photos had been saved by a third party client

Client had been popular, and used Snapchat API to interact with service, but behaved more like standard messaging client

Normal Snapchat users lacked ability to identify and/or opt-in if their “Friends” used the 3rd-party client

UNIVERSITY OF Cincinnati

iCloud Data Exposure - Backup

- Cloud backup becoming principle backup solution
- People treating cloud backup too much like “lockbox in storage”, while its more like “lockbox in shared storage”
- Ensure backup provider encrypts data *for you*
- Ensure service provider offers 2-factor authentication

UNIVERSITY OF Cincinnati

Office365 Accidental Exposure

- Microsoft, competing with GoogleDocs and similar, created a site called “docs.com”
- Integrated service with existing Office365, recommending users could publish to new service
- Similar concept to existing sharepoint.com service, but docs.com is different service with less controls
- Defaulted to “public view”

UNIVERSITY OF Cincinnati

Evernote Data Breach

- Online service Evernote had breach of identity information
- Encrypted (hashed) passwords, usernames, email
- Though no personal “notes” were ever taken, if users don’t reset their passwords, or use weak password schemes, future exposure possible
- Reuse of passwords across sites common

UNIVERSITY OF Cincinnati

Storefronts

- Think eBay, Amazon, PSN, Nintendo, BN.com, Target.com, etc…
- Common to upload credit card, personal address, email, phone number
- Online service usage increasing every year, each additional service increases risk of exposure
- Single-point of failure, in the retail industry

UNIVERSITY OF Cincinnati

Third-Party Applications

Centralization of public's data in the cloud facilitates emerging industry of third-party app providers

How to entrust data / not entrust data to third party providers

Revokable? If a stop trusting someone, can I take away historic data from them?

Data lifespan - If I shut down my Facebook account, can Facebook keep my information?

UNIVERSITY OF Cincinnati