Identity Management

Authentication and Authorization

Anthony Cheng
OMIS675
Spring 2015

What is Identity?

A series of attributes that identify a person

Digital Identity

Like identities in the real world …

… multiple data points that identify a user digitally

Applications and Identity

Applications allow users to perform specific tasks …

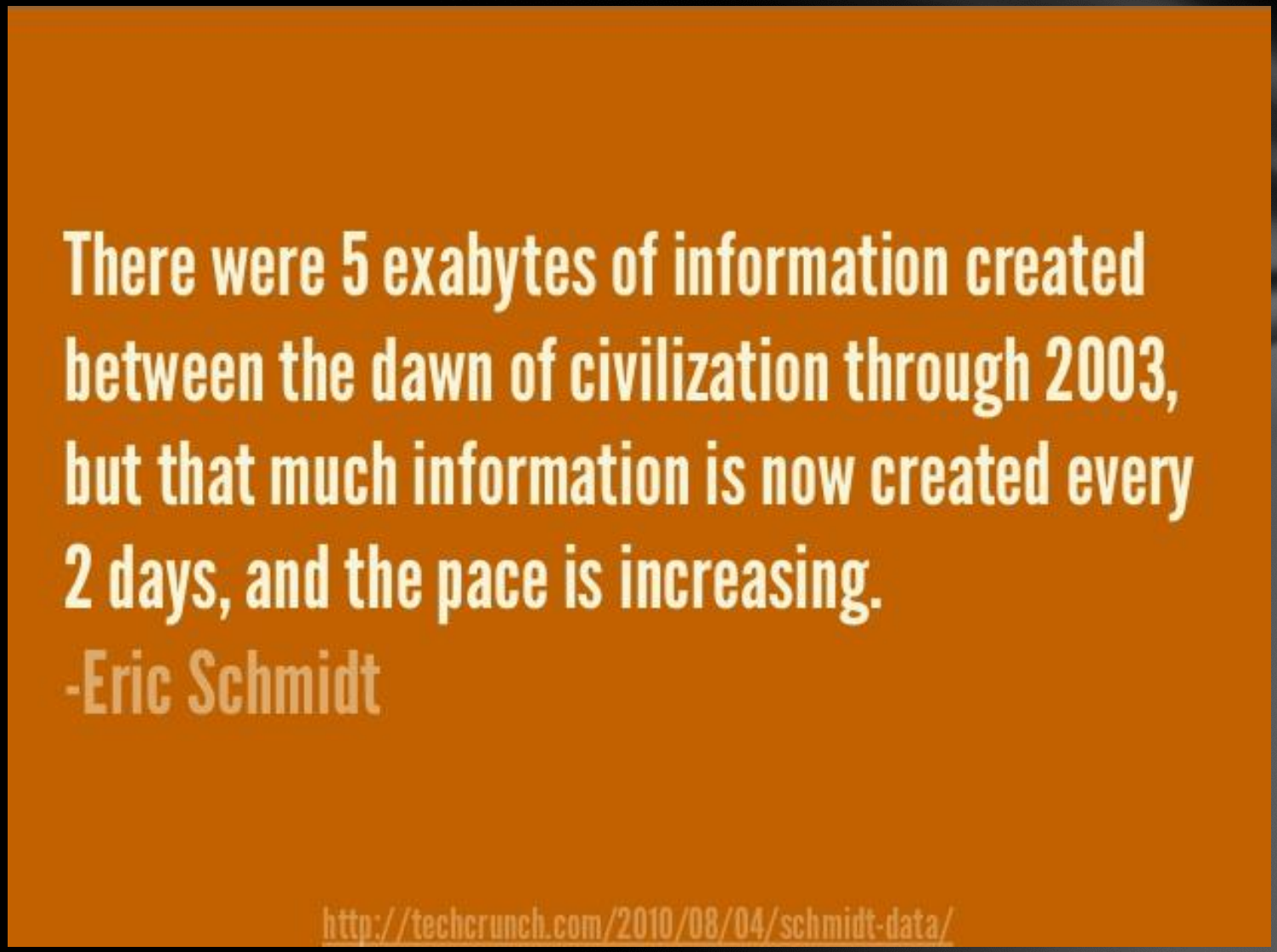
… but not all users perform the same specific tasks

Authentication and Authorization

- AuthN
  - Confirmation of an identity
  - Factors
    - Knowledge
      - "What you know"
    - Ownership
      - "What you have"
    - Inherence
      - "What you are"
- AuthZ
  - Access control policy
  - Authority to perform tasks
  - "Least Privilege"

Identity and Access Management (IAM) is the management of identities, their authentication and their authorization

Information Explosion



Application Ownership

Identify

Authenticate

Authorize

Logging

Compliance

Mitigate Risk

… PANIC!

Core Competency of an Application

Should it be the core competency of an application to manage identities …

OR

… provide the ability to for those identities to perform tasks?

Can it do both?

SHOULD IT?

Cloud

As more applications go to the "cloud" and outside of the management of one single entity, IAM becomes increasingly difficult.

WHY?

Cloud Deployments

Provider Types

Identity Provider

- Responsible for providing identities of users to a service provider
- Authenticates an identity
- Providing identity assurance to the service provider
- Provides additional data about the identity to he service provider
  - Age
  - Name
  - Favorite pizza topping

Service Provider

- Traditional applications that have been studied in class
- Authorizes an identity with the ability to perform functional tasks
- Aligns the incoming identity with the role (or roles) within the service provider

Works In Progress

Federated Single Sign-On (SSO)

- Federated identity
- Identity providers
- Reduces identity locations
- Identity clearing house
- Standards-based
  - Security Assertion Markup Language
  - OAuth

Identity Proofing

- Pulls from multiple sources
- Gradient scale of assurance
  - Low
    - User name and PIN
  - Medium
    - Personally Identifiable Information
  - High
    - One-time passwords (OTP)
    - Biometrics, e.g., voiceprints

External Authentication

Coding demonstration

```
using Microsoft.AspNet.Identity;
using Microsoft.AspNet.Identity.EntityFramework;
using Microsoft.Owin.Security;
using System.Web;
using System;
using OMIS675;

namespace OMIS675
{
    // You can add User data for the user by adding more properties to your User class, please visit http://go.microsoft.com/fwlink/?LinkID=317594 to learn more.
    public class ApplicationUser : IdentityUser
    {
    }

    public class ApplicationDbContext : IdentityDbContext<ApplicationUser>
    {
        public ApplicationDbContext()
  //        : base("DefaultConnection")            <-  The original value
            : base("z152400ConnectionString") //    <- The new value
        {
        }
    }

    Helpers
}
```