Cyber Security
The whole is as weak as its parts

Scott Bradner

2017-09-15

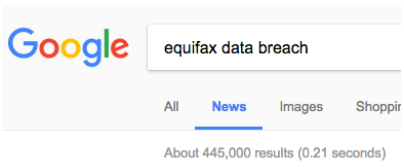
Poster Child

EQUIFAX®

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

Equifax had 'admin' as login and password in Argentina

Failure to patch two-month-old bug led to massive Equifax breach



Nearly 40 states probe Equifax's handling of massive data breach

Lawsuits against Equifax pile up after massive data breach

Lets Back Up

- What is information security?

  The protection of automated information from unauthorized access (accidental or intentional), modification, destruction, or disclosure.

  California State Administrative Manual

3

The "Other" CIA

- Information security is "CIA"
  - Confidentiality
  - Integrity
  - Availability

Confidentiality

- Control who sees what information

  Implied: only collect information you actually need & only retain while you have the actual need
- Does not mean no one can see the information, instead it means limit access to specific known individuals for specific purposes

  Prerequisite: you know who your users are

Integrity

- *Assurance that the data being accessed or read has neither been tampered with, nor been altered or damaged through a system error, since the time of the last authorized access*

  Businessdirectory.com
- Assumption: authorized users will not alter information improperly
- Requirement: limit unauthorized access

Availability

- *Availability, in the context of a computer system, refers to the ability of a user to access information or resources in a specified location and in the correct format.*

  Techopedia.com

- Requirements: patch systems and applications, filter network access

Failure to take care of the basics

- Underlying security problems have not changed that much over time

  According to virus incident reports as well as network users, weaknesses at host sites included (1) inadequate attention to security, such as poor password management, and (2) systems managers who are technically weak.

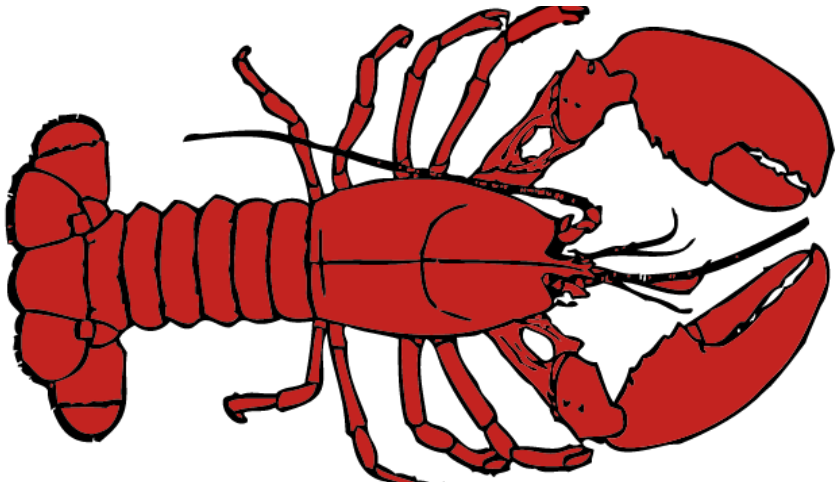
  – *Virus Highlights Need for Improved Internet Management*
  – US GAO **June 1989** (study in response to the Morris worm)

8

Other Security Issues

- People
  confused people, lazy people, evil people
- Buggy software
  Millions of lines of code – a bug every few thousand
- Flawed computer setup or configuration
  E.g., default passwords,
- Flawed network configurations
  E.g., servers without protection from Internet
- Pretending there is a safe "inside"

Crustacean Security



Other Security Issues, contd.

- Secrecy is not security
  - Surprisingly, many people think that secrecy creates security
  - Auguste Kerckhoffs (1883)
    - ***The design of a system should not require secrecy***
  - Bruce Schneier
    - ***every secret creates a potential failure point***
- i.e., security through obscurity (by itself) is very bad security
  - You should assume that the bad guys find out all your secrets (other than the key itself)

11

Who Are You?

- Core requirement for security is to know your users
- Two parts:
  - A/ Bind a person to an identifier
    - Including attributes (e.g. job title)
  - B/ Securely recognize the person when they return
    - Continuity of identity, "same Joe as last time"
- When done right it is called "IAM"
  - Identity and Access Management

Securely Recognize

- Traditional: a secret known "only" by the specific user – i.e. a password
  - Too easily shared or guessed
  - If you must use passwords use a password manager and long random passwords, one per service
- Current best practice: multi-factor (multi-step)
  - Something you know (password) + something you have (a smartphone with an app)

You are the Steward

- Every employee of the City of Boston shares in the responsibility to protect confidential information maintained by the City
- Everyone needs to understand the information security and sharing policies and internalize them
- Do not bypass security to make things "easier"
  - E.g., Sharing your password puts the information at risk
- IAM makes easier & safer at the same time