Reducing the Impact of Data Breaches

George Yee

Computer Research Lab, Aptusinnova Inc.

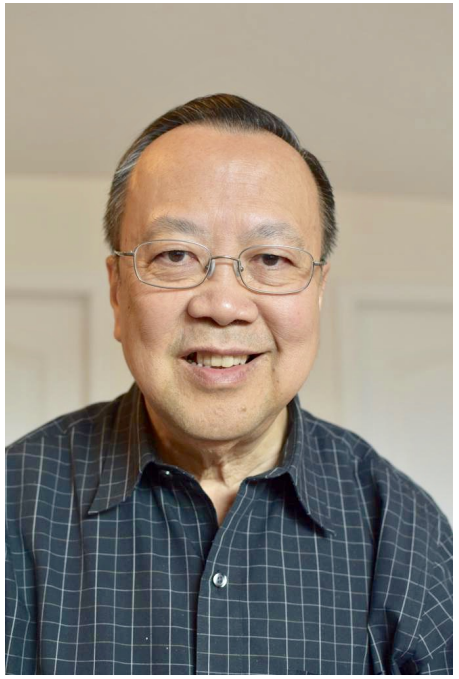
Dept. of Systems and Computer Engineering, Carleton University

Ottawa, Canada

gmyee@sce.carleton.ca | george@aptusinnova.com

SECURWARE 2020

George Yee



George Yee is a research scientist with Aptusinnova Inc. (his own company), doing research in Information Security and Privacy. He is also an Adjunct Research Professor in the Dept. of Systems and Computer Engineering at Carleton University, Canada. Previously, he worked as an IT Research Analyst with the Office of the Privacy Commissioner of Canada, as a Senior Research Officer at the National Research Council Canada, and as a research engineer at Bell-Northern Research and Nortel Networks. George received his Ph.D. (Electrical Engineering) from Carleton University. Dr. Yee is an IARIA fellow, a Life Senior Member of IEEE, and a member of ACM and has over 100 refereed scientific publications. His current research interests include security and privacy for software, and improving security through computational intelligence.

Content

- Introduction
- B2C Data
    - Purposes of Data Collection
    - Data Types
- Approach
- Example
- Conclusions and Future Work

Introduction

- Data breaches of personal information held by companies happening more often
- Companies respond by installing security controls to secure vulnerabilities
- Security controls are not fool proof, e.g., cannot identify all vulnerabilities
- **IDEA – store most of the company's collected private information on users' devices**
  - Reduces impact of a data breach since a smaller quantity of private information remains on company's system
  - Need to show that company can still carry out its purposes for collecting the private information
  - Apply idea to B2C e-commerce companies, which collect large amounts of private information and appear to suffer the most data breaches

B2C Data

- Types of B2C companies and their products

Company type	Products
Sellers of goods and services (e.g., Amazon.com)	Physical items such as pots, clothing, and electronics; services such as selling your items for you
Hotels (e.g., Mariott.com)	Rooms
Travel Agencies (e.g., Expedia.ca)	Travel bookings
Financial services (e.g., CIBC.com)	Fee-based banking accounts

B2C Data

- A B2C company collects private information for the following purposes:
  - transaction uses (e.g., shipping address),
  - communication with buyer,
  - use in securing other data (e.g., voice print to access highly sensitive data),
  - establishing loyalty,
  - targeted advertising,
  - market research,
  - sharing or selling.

B2C Data

- A B2C company's order consists of the following **data types**:
  - **Customer personal data (CPD)**, e.g., postal address, data of birth
  - **Product selection**, i.e., which products do the customer wish to buy
  - **Amount paid**, i.e., what price did the customer pay for the product(s)
  - **Ancillary data**, e.g., type of payment, date ordered, date shipped
- The instantiation of these data types may be different for different B2C companies, e.g., product selection for Amazon different from product selection for Mariott
- This data would normally be stored on the company's computer system

Approach

- GOAL: Reduce storage of personal data on the company's computer system by storing most of it on customer devices, while allowing for the purposes of collecting the data to be carried out.
- 5 parts
  1. Identify data to be stored on customers' devices (e.g., smartphone, laptop)
  2. Design for linking customer stored data to company stored data
  3. Design for the company's communication purpose
  4. Design for retention of the customer stored data in case the customer changes devices
  5. Design for security

Approach

1. Identify data to be stored on customers' devices: **CPD**
2. Linking customer stored data to company stored data: use

   Unique Customer Identifier (UCI)

   UCI = hash (userid, password)

   (e.g., SHA-3)
3. Communication purpose: use "Contact information" record (Figure 1). Contact information = email address + telephone no.

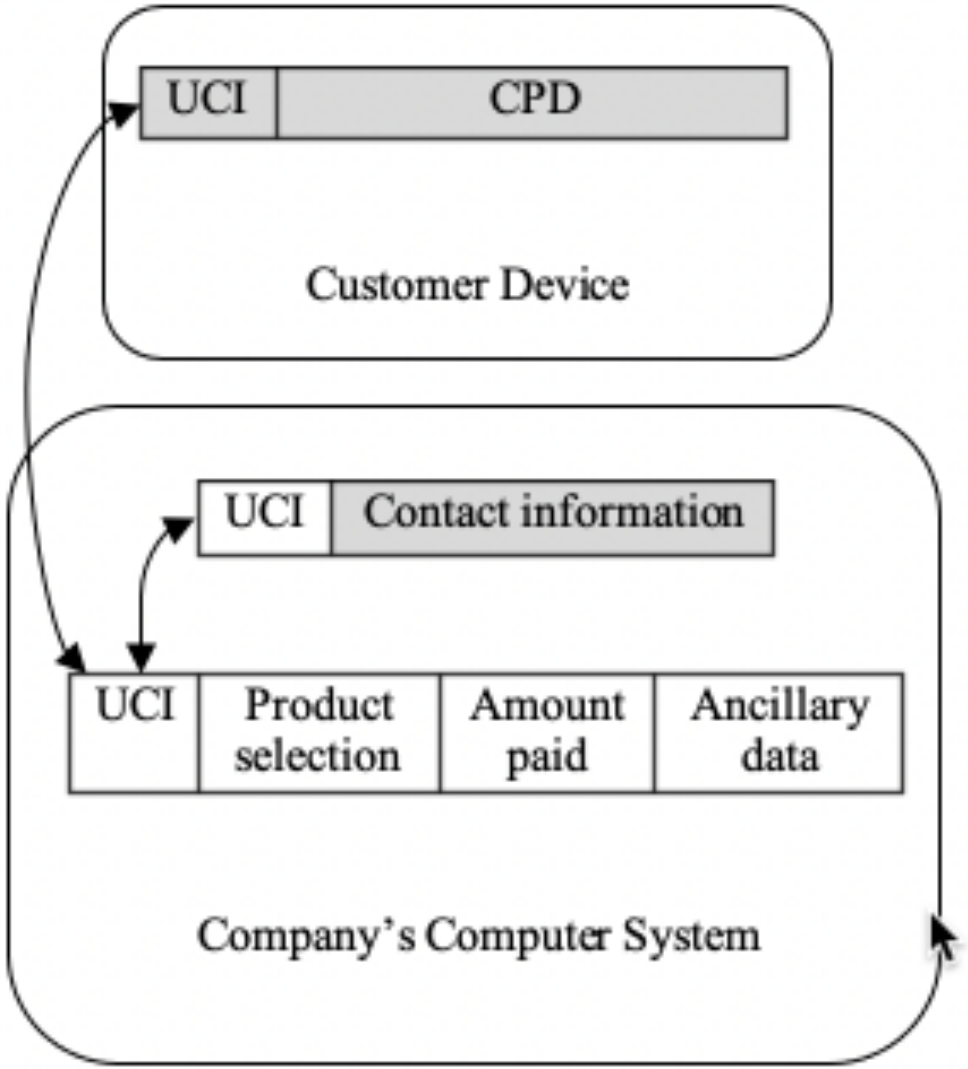


Figure 1. How the UCI links data records together.

Approach

4. Design for retention of the customer stored data in case the customer changes devices: a) uses new device after using other devices, b) loses device used (e.g., accident, theft) – see paper
5. Design for security: use **authenticated symmetric encryption** (e.g., AES-GCM) to encrypt the shaded parts in Figure 1.

Normal Use Case: Customer logs into company website. If first use of website, customer enters personal data, company creates UCI, CPD, Contact information, and stores CPD record on customer device. Company stores Contact information and product purchase record on its system. If used website before, company uploads CPD record from customer device (customer does not re-enter personal data).

Approach

- Other use cases, security analysis, implementation notes, verification of purposes – see paper.
- Strengths:
  - Straightforward – easier to sell to management
  - Efficient – attackers would have to breach many devices to gain a similar quantity of data prior to this approach
  - Makes company less attractive to attackers
  - Should please customers who want more control over their private data
- Weaknesses:
  - Storage/retrieval of CPD may attract more attacks on secure channel – no significant extra risks
  - Additional overhead for encryption/decryption - insignificant
  - Vulnerable to insider attacks – common – use specific measures against

Example

- Instantiate data types “CPD”, “Product selection”, “Amount paid”, “Ancillary data” for a hotel.

CPD	Product selection	Amount paid	Ancillary data
Name	Room - double	$200 / night	Date of reservation
Billing address			Arrival date
Home address			Departure date
Email address			Payment method
Phone number			Airport shuttle y/n
Credit card data			Daily laundry y/n
Loyalty ID number			Daily cleaning y/n
Country of origin			Wake-up call y/n
Passport country			Stay extended y/n
Passport number			
Room preferences			
Floor preference			

Conclusions and Future Work

- Presented straightforward approach for B2C companies to reduce the impact of a data breach by storing most of the customer's private data on his/her own device.
- Verified that the approach allows the company to carry out its purposes for collecting the private data (see paper).
- Nothing wrong with a straightforward (even simple) approach if it gets the job done.
- Future work includes a) looking at other types of organizations to which the approach may be applied and b) implementing it for fine tuning, measuring implementation effort, and checking performance.

Thank you for your attention.