Integrity Example

Simon Foley

February 2, 2016

A Document translation system I

The website `www.RurTranslate.com` hosts a Ruritanian to English language translation service. Registered users of the service may submit any URL to the translation service, for example,

```
https://www.RurTranslate.com/translate?URL=http://www.someURLaddress.com
```

The `translate` program retrieves the document at the user-specified URL (for example, the address `www.someURLaddress.com` above) and responds to the user with the document (with any embedded Ruritanian text translated to English).

A Document translation system II

Users sign up to use the service via the `https://www.RurTranslate.com/register` program where they can also purchase translation credits using their credit card.

A database table `Accounts` contains a record for each user that includes their name, encrypted credit card details and their current translation credits balance. Each time a user requests a document translation, the `translate` program decrements that user's current translation credits by one. If the user's translation credits balance is zero then the document is not translated.

A linux server currently hosts the website, `translate` and `register` applications, and the DBMS managing the `Accounts` table.

Biba Integrity Model (eg implemented on FreeBSD)

Integrity levels $doc < accounts < creditCard$.

The credit card services `ccServices` operate at (fixed) Integrity level $creditCard$. The accounts database has integrity level $accounts$. Documents have integrity level doc.

`Register` program runs at level $creditCard$, interacts (rw) with `ccServices`; creates/updates the customer details in accounts database (LWM mechanism).

`Translate` program runs at level documents, but needs to update accounts? Strategy: allow a security exception, or maybe translate starts at accounts, does the billing bit and then reads document (LWM),

Any other integrity problems? Who/what can edit billing?

CW Integrity Model

UDIs: documents?

CDIs: accounts database

TPs: `Register`, `Translate`

IVP: check CCs not stored anywhere else (not in document)

[Aside: URL problem: translate the URL $file : ///etc/passwd$]

CW model of security provided by Unix hosted webserver?

Enforcement Rules (provided by combination of Unix/webserver)

- □ E1 Customer/Users don't have usual login-accounts to the hosting server and so don't have direct access to CDIs.
- □ E2 Customer/users can only access CDIs via requests to the Register and Translate services. $(Customer, Register, Accounts)$ and $(Customer, Translate, Document)$
- □ E3 Need to authenticate web-requests from customers. For example, http-basic authentication?
- □ E4 authorizations may be changed only by root.

Certification Rules (on the application implementation)

- □ C1: what check for IVP?
- □ C2: Code inspection/check that `Register`, `Translate` operate properly, write to audit file (C4) and fail-safe/atomic (C5).
- □ C3: no separation of duty here?