Localization of Credential Information to Address Increasingly Inevitable Data Breaches

Mohammad Mannan and P.C. van Oorschot
mmannan@scs.carleton.ca

Carleton University, Canada
"...we do not have any evidence that the data ... has been improperly accessed or misused..."
Goals of our proposal

1. Goals:
   - limit misuse of breached ID numbers from relying parties
   - ameliorate huge data breaches (but not card theft or loss)
     – primary concern: identity theft

2. Non-goals:
   - prevent data breach
   - privacy
Overview of ID localization

1. Business name

2. Localized ID, Lookup data

3. Localized ID, Lookup data, Business name

4. yes/no

Locate user info and verify ID

address “compromise once, reuse multiple times”

design for damage control
Assumptions

1. Breaches will happen...there is no 100% prevention
2. Massive breaches usually involve relying party
3. ID issuers are targeted less often
4. Up-to-date user lookup data can be maintained
5. Online verification is possible
Overview of our proposal

1. ‘Localize’ ID numbers so that they are valid only for a particular relying party
   - valid for Internet/phone, physical world
   - not necessarily ‘one-time’ use IDs

2. Limit misuse, assuming breaches can’t be prevented

3. The problem domain is large: we propose several variants
ID localization: issue card

User

ID card

Fixed ID: custom length

128-bit secret

ID Issuer
ID localization: generate ‘localized’ ID

Generate localized ID

Fixed ID

Business name

Pseudo Random Function

Localized ID

User

Localized ID, Lookup data

Business name

Relying party
ID localization: verify ‘localized’ ID

Locate user info and verify ID

Lookup data

User info (database)

Fixed ID

Id Issuer

Relying party

Localized ID, Lookup data, Business name

Accept/Reject
Variants 1 & 2

1. Variant 1: Localized authorization code
   - PRF-output is used as authorization code (cf. CVV2)
   - fixed ID + auth. code is required for any valid use

2. Variant 2: Without chip-card or card-reader
   - shared ‘secret’ is printed on the card
   - localized ID (or auth. code) is generated through a personal device
Limitations

1. Data aggregation isn’t straight-forward

2. Several types of privacy-sensitive info remain unprotected

3. Requires online verification

4. Deployment would most-likely require:
   - increased liability
   - strong consumer lobbying
   - legislation/regulation

but now is the time for a change...
Open issues

1. Using static, reusable numbers invites repeated misuse
   ➤ but how can they be replaced?

2. Can we apply localization beyond data breaches?

Design for damage control
Backup slides
Current approaches that fall short

1. Data encryption
2. Intrusion detection/prevention systems
3. One-time use credit cards: Citibank MasterCard, DiscoverCard
4. Academic proposals: FC01, FC07, RIDE04, ESORICS08
5. Legal remedies, breach notification laws
Consequences for consumers: identity fraud

1. “Full identity” costs only $1-15
2. Time lost to resolve ID fraud
3. Denied financial services
4. Harassment by collection agencies
5. Criminal prosecution/arrest
Variants 3 & 4

1. Variant 3: Database poisoning
   - each relying party inserts fake user records in its database
   - breach is detected when fake records are used
   - card issuers may also use this technique

2. Variant 4: User-centric authorization
   - notify/seek user approval for e.g. issuing new card, transferring user info across domains, high-value trans.
   - deploy “physical presence” mechanisms for approval