*NSPW08 Presentation, Sept. 23, 2008*

# Localization of Credential Information to Address Increasingly Inevitable Data Breaches

Mohammad Mannan and P.C. van Oorschot

mmannan@scs.carleton.ca

Carleton University, Canada

**Bank customer data sold on eBay**

An investigation is under way into how a computer containing bank customers' personal data was sold on eBay.

The computer, bought by IT manager Andrew Chapman for £77, had the sensitive details on its hard drive

August 27th, 2008

Taiwan busts hacking ring, 50 million personal records compromised

TJX breach could top 94 million accounts

**Filings in case involving Visa cards alone as much as $83 million**

Data Leak in Britain Affects 25 Million

By ERIC PFANNER

**MoD admits loss of secret files**

More than 100 USB memory sticks, some containing secret information, have been lost or stolen from the Ministry of Defence since 2004, it has emerged.

Latest 'lost' laptop holds treasure-trove of unencrypted AT&T payroll data

**Every prisoner in UK victim of data breach**

Mark Mayne August 22, 2008

July 3, 2008 9:52 AM PDT

**Stolen: Google employees' personal data**

Bank's Lost Backup Tapes Contained IDs of 12 Million Clients

**IT pro admits stealing 8.4M consumer records**

**CIBC loses data file on 470,000 customers**

By: Joaquim P. Menezes - IT World Canada (19 Jan 2007)

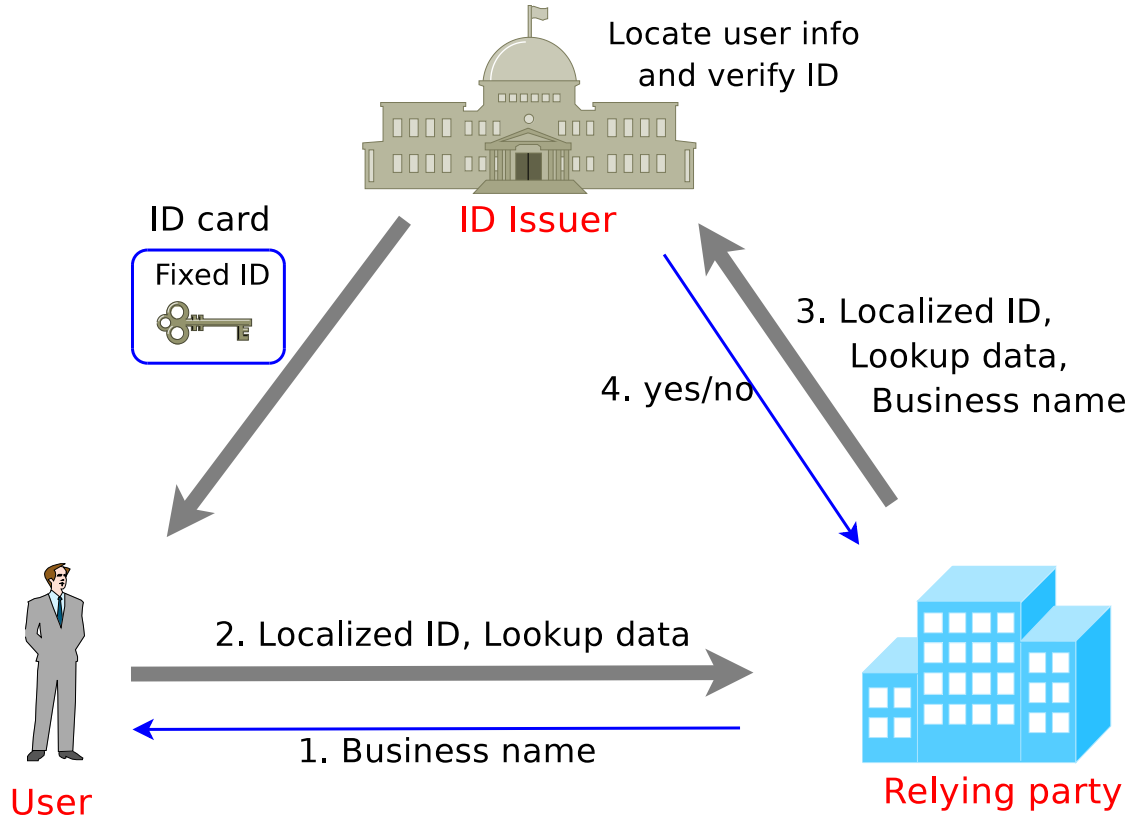
Hundreds of Laptops Missing at State Department, Audit Finds

"...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




address "compromise once, reuse multiple times"

design for damage control

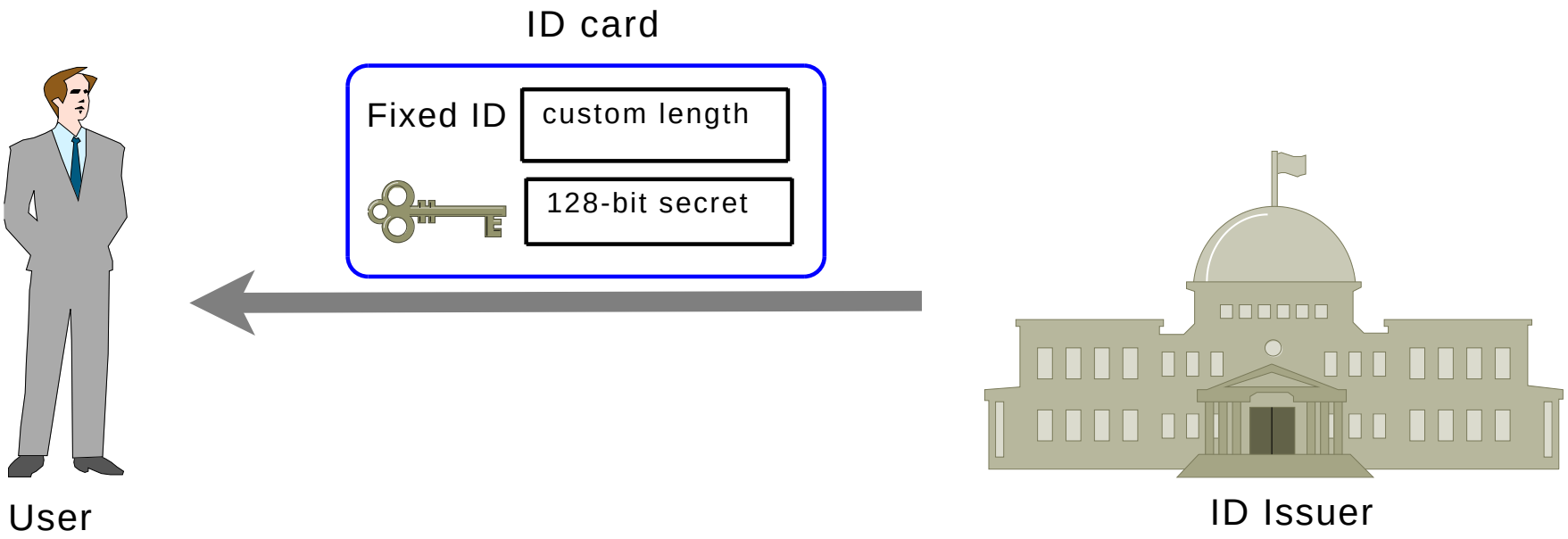
# Assumptions

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

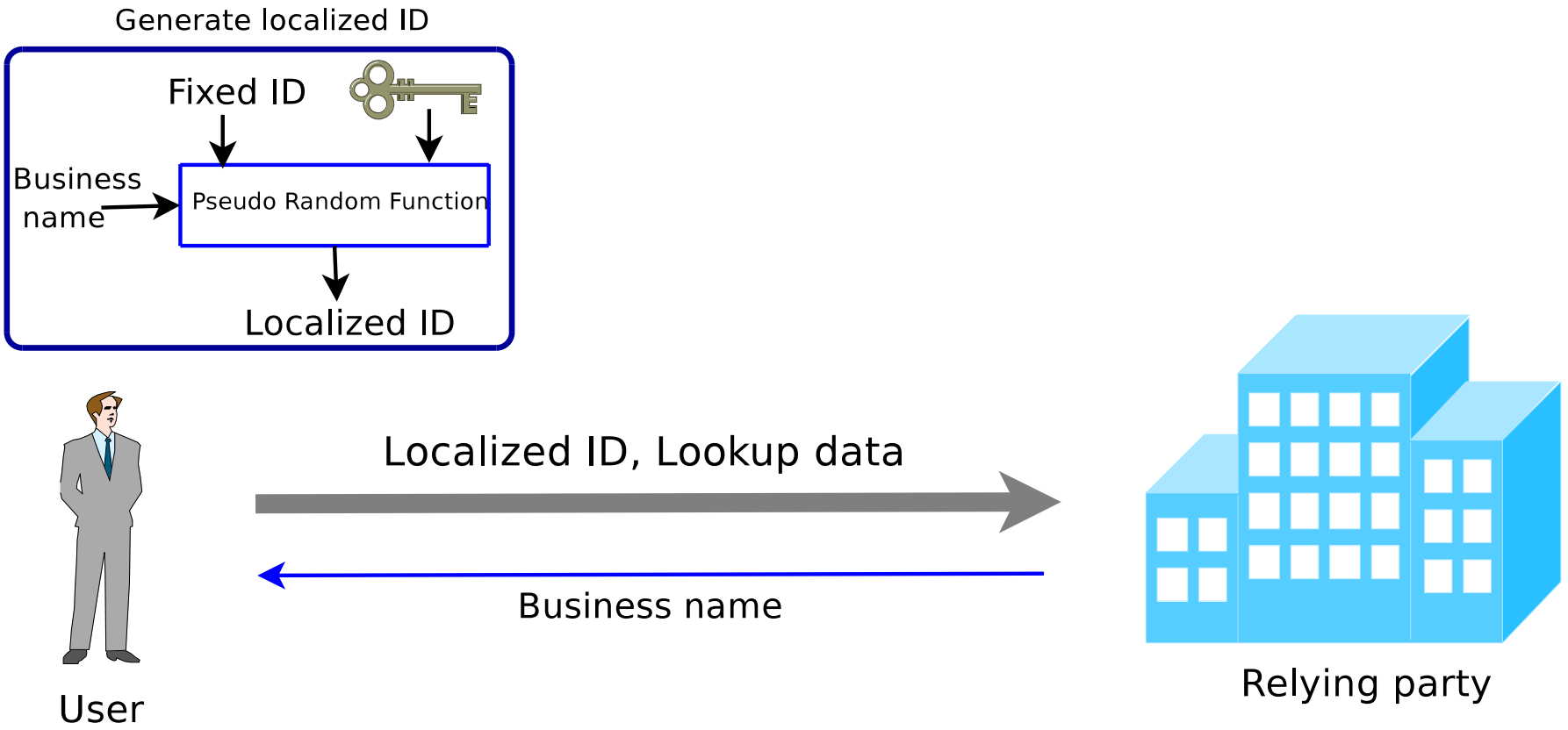
# Overview of our proposal

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

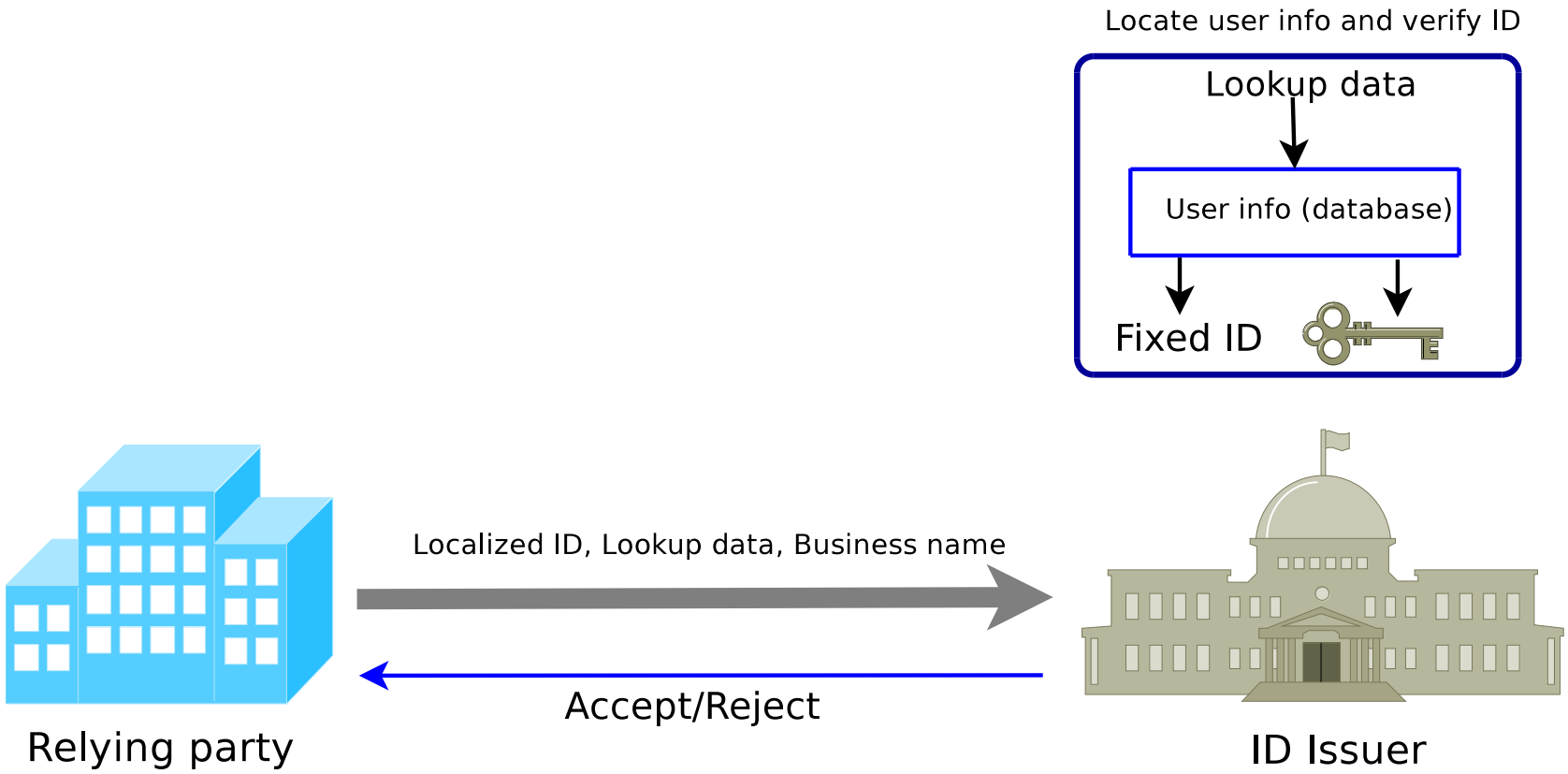
# ID localization: issue card



# ID localization: generate 'localized' ID



# ID localization: verify 'localized' ID



# 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