CS 523: Social, Economic, and Legal Aspects of Security

Identity Theft
Why is there identity?

• A very ancient concept, introduced for multiple reasons including
  – Census
  – Taxation
  – Commerce
  – Contracts
  – Pricing (e.g., interest rate depends on borrower)

• Identity existed in a social/economic context
  – Job context?  Pub?  Kids’ soccer game?
Commonly used proofs of identity

- Social security number
- Date of birth
- A parent’s name or date of birth
- ...
- Major problem: All of the above are public or easily obtainable
- Criminals can use it to pretend they’re someone else (= “identity theft”)
Why is identity theft so easy?

• Same “credentials” are re-used over and over
  – Social sec. number (SSN), date of birth (DoB), …

• Re-use includes high-value transactions
  – E.g., social security benefits, tax refunds, …

• Re-use also includes low-value transactions
  – E.g., recreational fishing or hunting licence
  – For low-value, low security is used (“not worth it”)

• Attackers get data in “low”, use it in “high”
Identifiers

• An identifier distinguishes a distinct person, place or thing within a given context
  – Context (or namespace) for an identifier is the space in which the identifier is recognized
• An identity can have multiple identifiers, e.g.,
  – For a person: Social security number, student ID number, employee number, …
  – For a car: permanent VIN number, license plate
Personal identifiers

• Identifiers that are linked to exactly 1 person
• Based on attributes that are practically impossible (or very difficult) to alter
  – Date of birth, some biometrics (like DNA), ...
  – One can lie about these, but not change them
• Identification = accepting the claimed association of an identifier with a person
  – Always occurs within an implied namespace
You need to provide your SSN ...

• For a credit check so you can rent
• To open a bank account and obtain a safe deposit box
• To get a mortgage
• To get a car loan
• To get a job
• To buy insurance
• To get phone service (usually)
Example of identity theft scenario

- Thief learns the victim’s compromised info
  - Association between victim’s name, SSN, DoB
- Uses info to get credit card in victim’s name
- Uses that credit card to pay for his utilities
- Uses utility bills and phone number as proofs of residence, and gets a state driver’s licence
  - Driver’s license has the victim’s name on it, but the thief’s photo
Identity theft scenario (cont’d)

• Alternative (simpler) approach:
  – Thief goes to any of the (~ 30) driver licenses authorities known to have fraud, bribes his way into a driver’s license in the victim’s name but with his own photo on it
  – Corruption in the NJ authority was so endemic that all the line employees were fired and the name of the Bureau was changed
Why identities are stolen

- Theft of money
  - Shopping, restaurants, ...

- Theft of health care services, e.g.,
  - Thief has no health insurance and cannot afford to pay for the care (e.g., the $1M heart transplant for which the “identity” was bought for $75K)
  - Thief can pay but is wanted by the law, would go to jail if checked into hospital in own name

- Commission of crimes
  - For which the victim would be blamed
Typical consequences for victim

• About 2000 hours of time to clean up credit, clear name, obtain police papers affirming that identity thief committed the crimes
• Damaged credit loses them a job offer, the house or car they wanted to buy
• Thief-generated criminal record for victim can take a long time to clear
  – In the meantime: No passport, no job, no credit
Extreme consequences for victim

• Death
  – E.g., many alleged purchasers of child pornography were arrested in the UK, with credit card records as the only proof. Of those who were later found innocent of the crime (because the credit cards used were created through identity theft), two committed suicide after being found innocent.

• Health hazards
  – When “Alice” fraudulently get health care as, and the real Alice does not notice it, Alice’s medical info on record is inaccurate and can cause harm to Alice.
Mythical root cause

• Myth: Identity theft is mainly caused by careless victims who naively disclose their info.
• This is a problem, but not the main one. Theft is typically not the victim’s fault, e.g.,
  – Insiders at service or health providers sell info on potential victims (info is later used fraudulently)
  – Private info used in high-value fraud was learned by subverting low-value, low-security uses of same info
  – Private info was obtained legally by posing as a legitimate “merchant”
The real problem

• An inadequate legal and liability framework
  – Laws to punish thieves, let most costs fall on victims

• When Bob is victim of identity theft by Alice, inadvertently enabled by Carol and David, it is mainly Bob who bears the costs of the crime
  – Police usually show that they acted “in good faith”
  – Carol and David usually also show they acted “in good faith”, used standard industry practices (standard, yet flawed: under-authenticate, provide credit reports to anyone, mail unsolicited credit card offers, ...etc)
How to fix It

• The identity theft problem would vanish if liability and costs were placed on the entities most capable of mitigating the problem, e.g.,
  – Finance companies that give credit without proper authentication (based on knowledge of SSN/DoB)
  – Organizations that unnecessarily give their employees access to customers’ private info
  – Regulations and practices that force consumers to use the same “key” (SSN) in multiple contexts
Modest step: Opt-in as default

- Require opt-in (rather than the current opt-out) of the sharing of personal financial info
- If current opt-out is kept, at least make it last “until further notice” rather current 90 days
  - Would be strongly opposed by businesses, who make money out of sharing private personal data
- Not worth collecting Bob’s info if he opted out
  - Can get better privacy by permanently opting out
A less modest step: Liability

• Who? Whoever skimped on authentication:
  – The banks that let fraudsters open bank accounts or obtain credit cards (e.g., based only on their knowledge of someone’s SSN/DoB)
  – The banks that mass-mail unsolicited credit card offers, some of which ultimately result in fraud
  – The hospitals that provide health care without properly ascertaining patient identity
  – The credit bureaus with erroneous records
Liability (cont’d)

• How much? Much more than the current “dollar amount-of-fraudulent-charges”
  – Costs of cleaning up victim’s credit
  – Costs of correcting victim’s criminal records (expensive because no central location to do it)
  – Loss of job (or of job offer)
  – Denial of loan application
  – Reputational damage, psychological distress, …
Identity theft that results in arrest

- Currently, an innocent victim’s arrest because of identity theft is treated as an unfortunate side effect of due process
  - It is not, it is false arrest
  - Victims of false arrest can sue for damages
  - Liability would not be entirely the police’s, it would be shared with the source of the wrong info (the entity that mis-authenticated) and with other parties that propagated the wrong info
Current “advice” on self-protection

• Check your credit at least $k$ times a year
  – $k$ used to be 1, now it is 2 or 3 (likely to increase)
  – What about the months in between two checks?
• Check periodically your driver’s licence record
  – Current advice is twice a year
• Possible future advice
  – Check your criminal record at least $k$ times a year?
    (much more expensive than credit record check)
“Advice” on self-protection (cont’d)

• The “advice” is burdensome, and doesn’t work
  – It is like telling people they don’t really need a lock for the front door of their home when they leave for work, as long as they go back home at least k times a day to make sure that nothing is missing
  – In a good system, people’s reputation and records depend on their own actions (not on what others do)

• Current system is absurd
  – Yet those who benefit from it will fight to keep it