

Act for Affordable Data Care

Saikat Guha, Srikanth Kandula

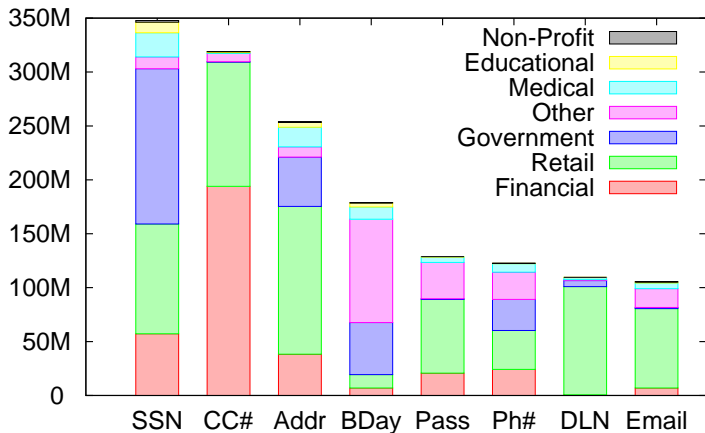
Microsoft Research

HotNets-XI

Data Breaches Today

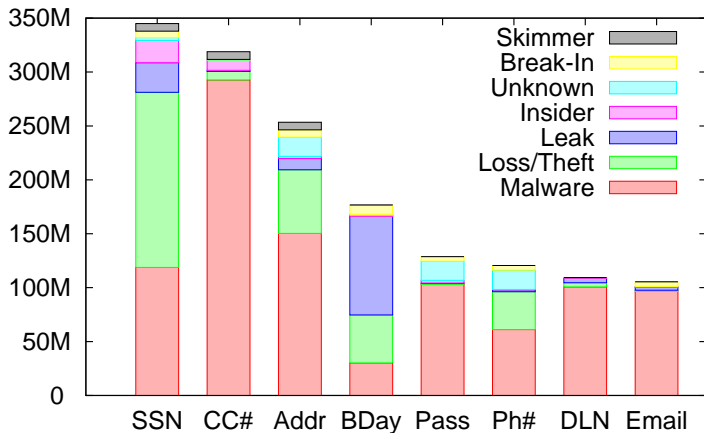
- ▶ July 2012: Yahoo! — 400K passwords
- ▶ June 2012: LinkedIn — 6M passwords
- ▶ May 2011: Sony — 100M+ passwords, CC#

Data Breaches Today



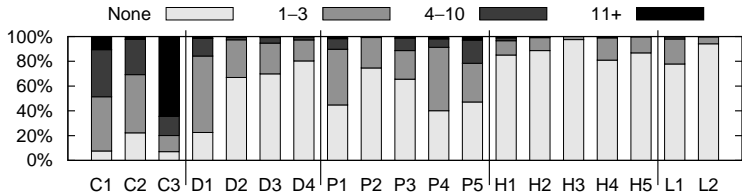
Data source: Privacy Rights Clearinghouse

Data Breaches Today



Data source: Privacy Rights Clearinghouse

User Behavior Today



Credit and Debit Cards

- C1 Online transactions (monthly)
- C2 Sites credit-card saved at
- C3 Monthly statements checked (yearly)

Data Protection

- D1 Sites persistently logged into
- D2 Public devices used (monthly)
- D3 Identity document emailed (last year)
- D4 Sensitive number emailed (last year)

Loss

- L1 Fraudulent transactions (last two years)
- L2 Transactions above resulting in money loss

Password Security

- P1 Bank passwords changed (last year)
- P2 Banks with same password
- P3 Non-bank sites with bank password
- P4 Email passwords changed (last year)
- P5 Non-email sites with email password

Physical Security

- H1 Device left unlocked and unattended (last year)
- H2 Phones lost or misplaced (last year)
- H3 Laptop/tablet lost or misplaced (last year)
- H4 Wallet/keys lost or misplaced (last year)
- H5 Items above that weren't recovered

Data Breaches Today

New technology is NOT the solution

- ▶ Cryptographic hashing: 30y+ old
- ▶ Salting hashes: 30y+ old
- ▶ Encrypted FS: commercialized 12y+ ago
- ▶ Single-use CC#: commercialized 12y+ ago
- ▶ Password managers: freeware 5y+ ago

New policies or regulation is NOT the solution

- ▶ Yahoo!, LinkedIn, Sony have good policies
- ▶ Past regulation ineffective (spam, cookies, . . .)

What are we Missing?

What are we Missing?

Money

Crazy Idea: Data-Breach Insurance

- ▶ **Underwrite damages** for a small premium
 - ▶ Users: fraudulent charges, ID-theft monitoring, ...
 - ▶ Enterprises: lawsuits, cleanup, ...
 - ▶ *Safety-net*. No changes needed.
- ▶ Create an **incentive to improve**
 - ▶ Lower premiums for good behavior
 - ▶ Data driven. *Individualized*.

Crazy Idea: Data-Breach Insurance

- ▶ **Underwrite damages** for a small premium
 - ▶ Users: fraudulent charges, ID-theft monitoring, ...
 - ▶ Enterprises: lawsuits, cleanup, ...
 - ▶ *Safety-net*. No changes needed.
- ▶ Create an **incentive to improve**
 - ▶ Lower premiums for good behavior
 - ▶ Data driven. *Individualized*.

Insurance 101

- ▶ **Scale:** Many prospective clients
- ▶ **Non-Catastrophic:** No hurricane Katrina
- ▶ **Loss:** Large enough to justify premium
- ▶ **Premium:** Low enough that clients pay
- ▶ **Incident:** Loss event can be identified
- ▶ **Accident:** Outside of client's control
- ▶ **Risk-Assess:** Loss probability and magnitude

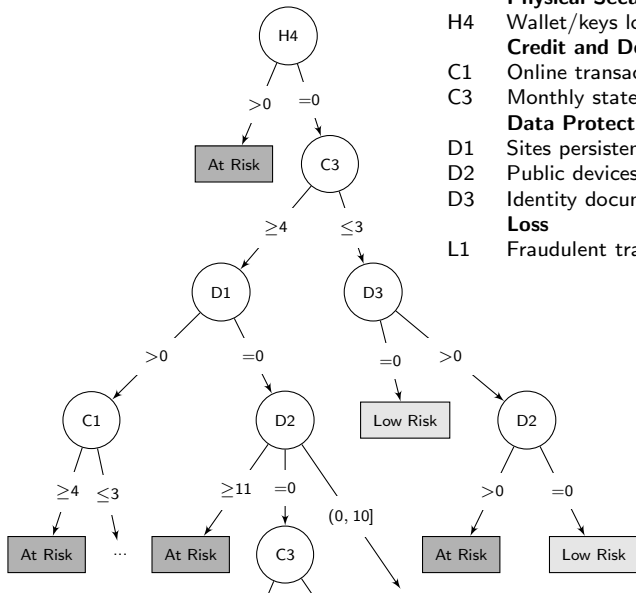
Insurance 101

- ▶ **Scale:** Many prospective clients
- ▶ **Non-Catastrophic:** No hurricane Katrina
- ▶ **Loss:** Large enough to justify premium
- ▶ **Premium:** Low enough that clients pay
- ▶ **Incident:** Loss event can be identified
- ▶ **Accident:** Outside of client's control
- ▶ **Risk-Assess:** Loss probability and magnitude

Correlating User Behavior with Loss

| Response | all | victims (Δ) |
|---|-----|----------------------|
| C1: Online transactions (monthly) ≥ 4 | 48% | 67% (+18%) |
| H4: Wallet/keys lost or misplaced (last year) > 0 | 18% | 31% (+12%) |
| C2: Sites credit-card saved at ≥ 4 | 30% | 42% (+12%) |
| D1: Sites persistently logged into > 0 | 75% | 87% (+11%) |
| D3: Identity document emailed (last year) > 0 | 29% | 40% (+11%) |
| H5: Items above that weren't recovered > 0 | 12% | 20% (+8%) |
| P5: Non-email sites with email password ≥ 4 | 21% | 28% (+7%) |
| C3: Monthly statements checked (yearly) ≥ 4 | 78% | 85% (+6%) |
| D4: Sensitive number emailed (last year) is 1-3 | 16% | 23% (+6%) |
| D2: Public devices used (monthly) > 0 | 32% | 37% (+5%) |
| P4: Email passwords changed (last year) is 1-3 | 50% | 55% (+5%) |
| P1: Bank passwords changed (last year) is 0 | 43% | 37% (-5%) |
| P2: Banks with same password > 0 | 24% | 30% (+5%) |

Correlating User Behavior with Loss



Physical Security

H4 Wallet/keys lost or misplaced (last year)

Credit and Debit Cards

C1 Online transactions (monthly)

C3 Monthly statements checked (yearly)

Data Protection

D1 Sites persistently logged into

D2 Public devices used (monthly)

D3 Identity document emailed (last year)

Loss

L1 Fraudulent transactions (last two years)

Discussion

- ▶ **Would users pay?** 77% say they would
- ▶ **How much?** \$20 per year (median)
- ▶ **Profitable for insurance company?** Likely
- ▶ **Behavior change?** 94% want to
- ▶ **Fraud, Moral hazard?** Existing mechanisms
- ▶ **Adverse selection?** Also, advantageous
- ▶ **Other mechanisms?** Complementary

Act for Affordable Data Care

- ▶ **Make users *act*** for data safety
 - ▶ Data safety linked directly to money
- ▶ One crazy idea: **Data Breach Insurance**
 - ▶ but is it crazy enough to work?
- ▶ Technology: **individualized risk-assessment**
 - ▶ Immediate feedback for bad behavior
 - ▶ Ongoing work

Putting Money Where Mouth Is

- ▶ **Monitor user behavior** privacy-preserving; in-browser
 - ▶ Track password re-use
 - ▶ Opening unknown attachments
 - ▶ Not locking computer
- ▶ Offer **different incentives** to change
 - ▶ Gentle nudge
 - ▶ Gamification
 - ▶ Social incentives
 - ▶ Financial
- ▶ **Real data** from few thousand users
 - ▶ A/B testing
 - ▶ Success metric: **change user behavior**