Eww You're Leaking:

A Formal Introduction to Information Leakage

Mireya Jurado
@mireya_anita
July 17, 2021
The Diana Initiative

1

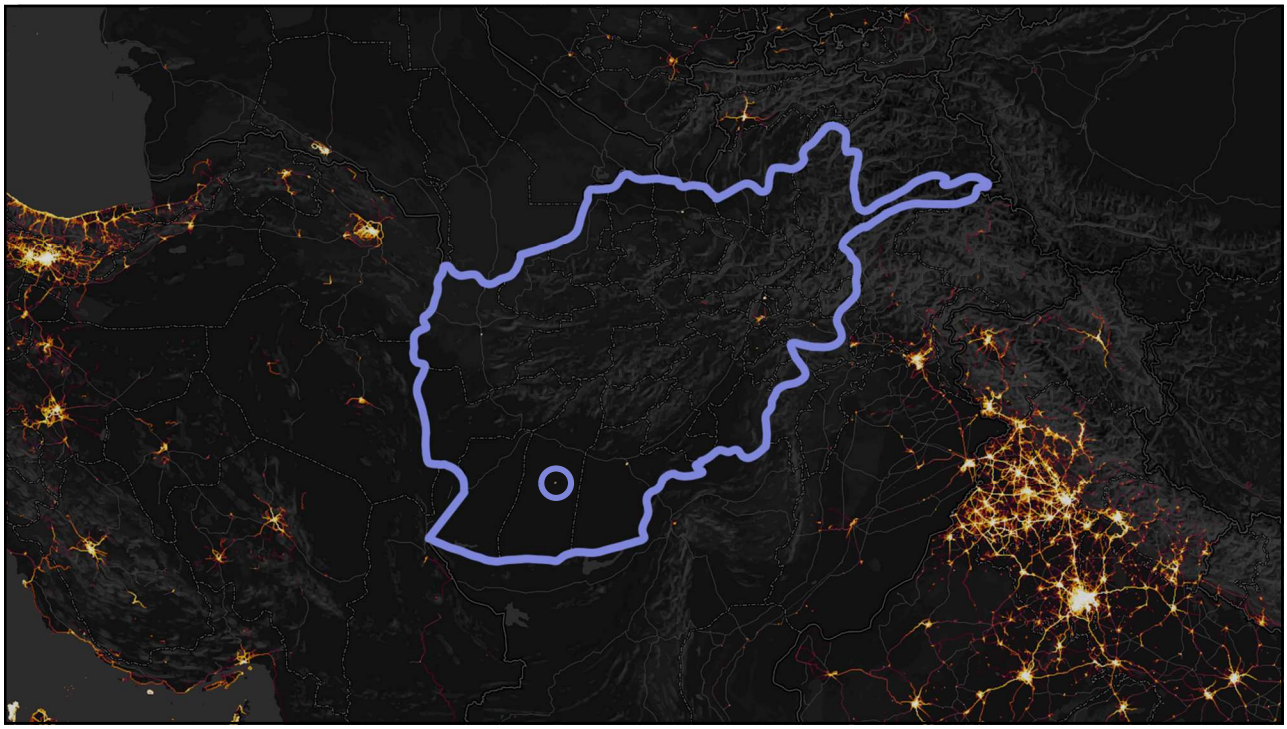
U.S. soldiers are revealing sensitive and dangerous information by jogging

Strava Fitness App Can Reveal Military Sites, Analysts Say

The Strava Heat Map and the End of Secrets

Fitness app Strava lights up staff at military bases

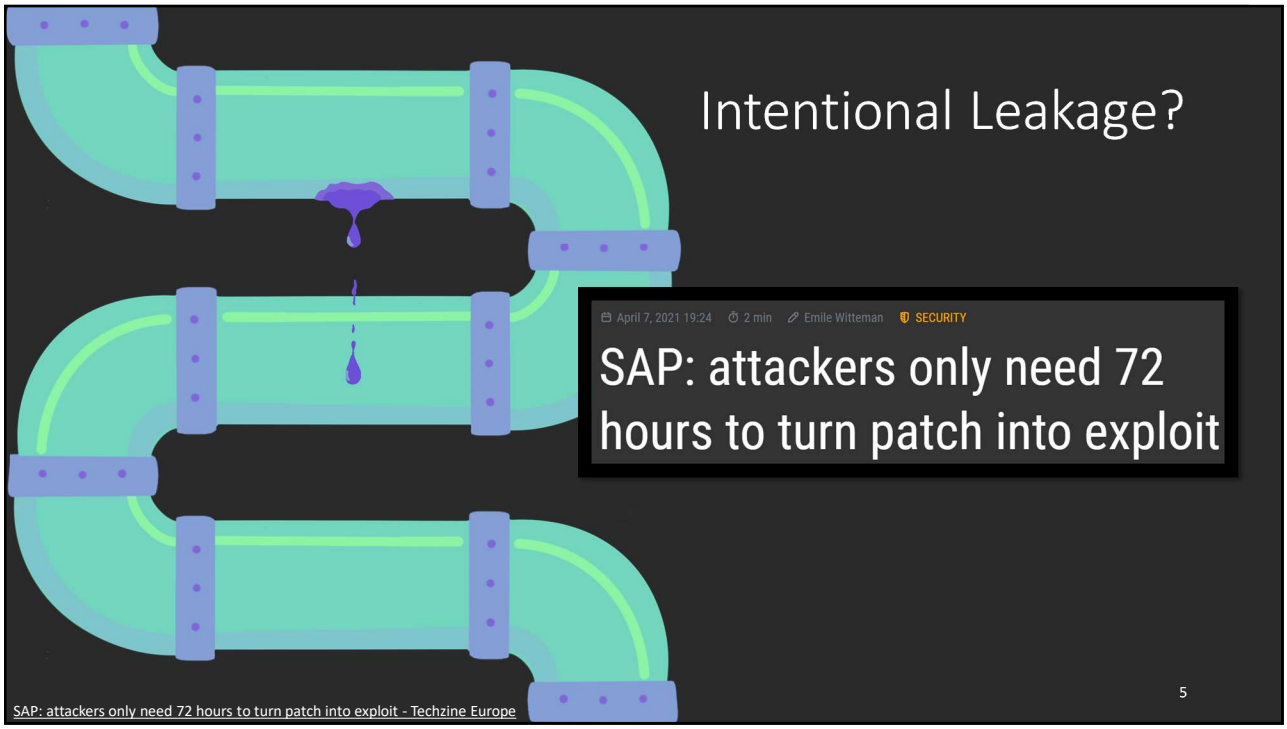
2



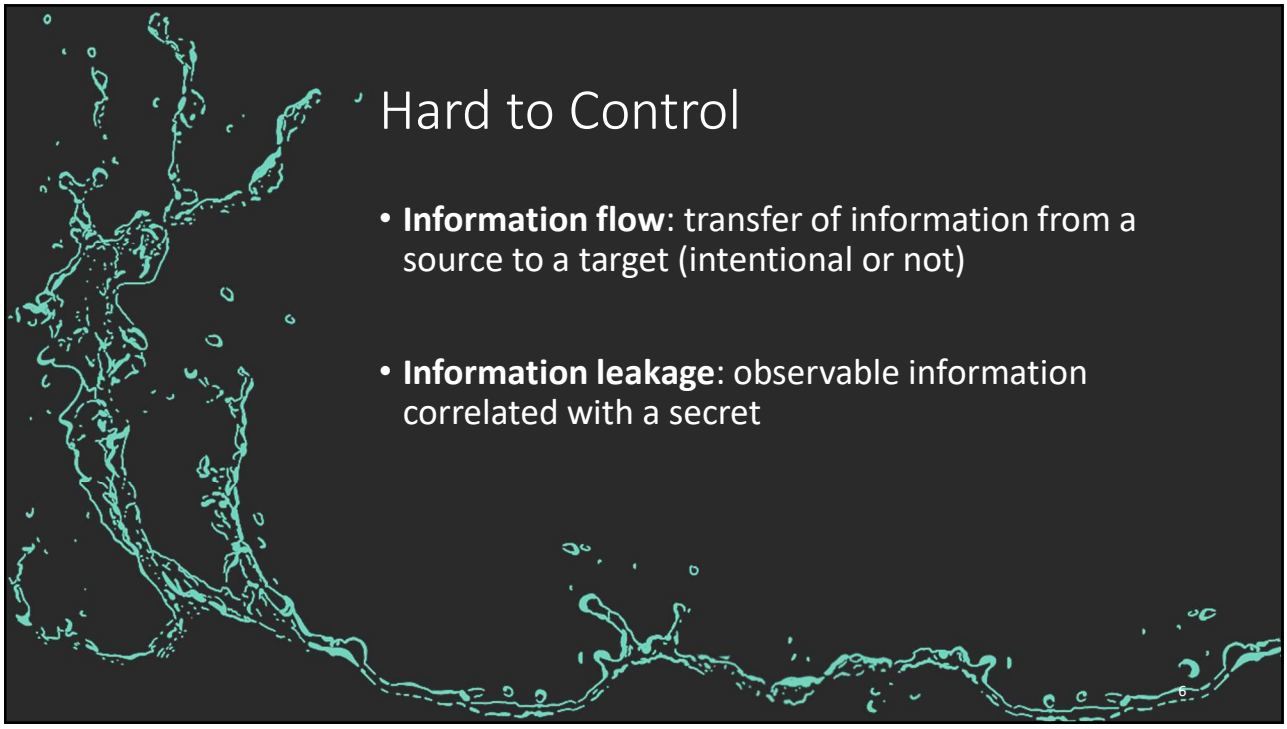
3


STRAVA
Mobile
Features
Subscription
Blog
Sign Up
Log In
Strava
Nathan Ruser @Nrg800
Strava Data Heat Maps Expose Military Base Locations Around the World | WIRED
4

4


Intentional Leakage?
April 7, 2021 19:24
2 min
Emile Witteman
SECURITY
SAP: attackers only need 72 hours to turn patch into exploit
SAP: attackers only need 72 hours to turn patch into exploit - Techzine Europe
5

5


Hard to Control
• **Information flow**: transfer of information from a source to a target (intentional or not)
• **Information leakage**: observable information correlated with a secret
6

6

The Point

- You have a framework for information leakage
- You have the tools to calculate leakage
- You can apply this framework to compare systems & to reduce your attack surface

7

7

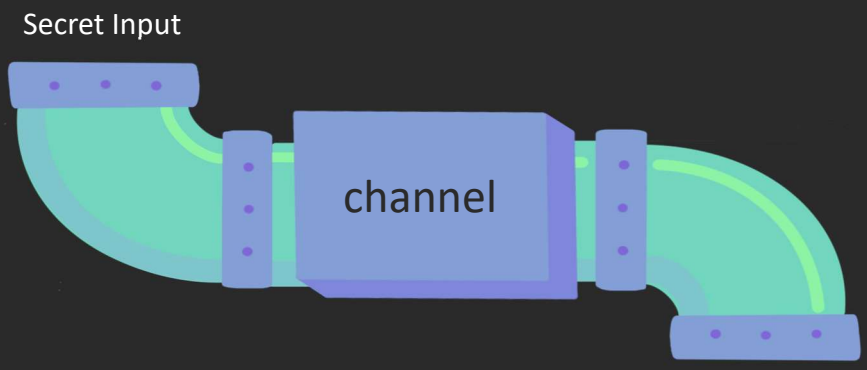
A (very) Brief Academic Timeline

Does it flow?	1973 Bell & LaPadula: Write Up, Read Down
	1982 Goguen & Meseguer: Noninterference: public output shouldn't tell you anything about secret input
How much does it flow?	1991 Grey: Use Mutual Information, Shannon entropy
What's the value of the flow?	2009 Smith: Use min-entropy
	2020 Alvim, Chatzikokolakis, McIver, Morgan, Palamidessi, & Smith: The Science of Quantitative Information Flow

8

8

Quantitative Information Flow (QIF)



9

9

Model the Adversary

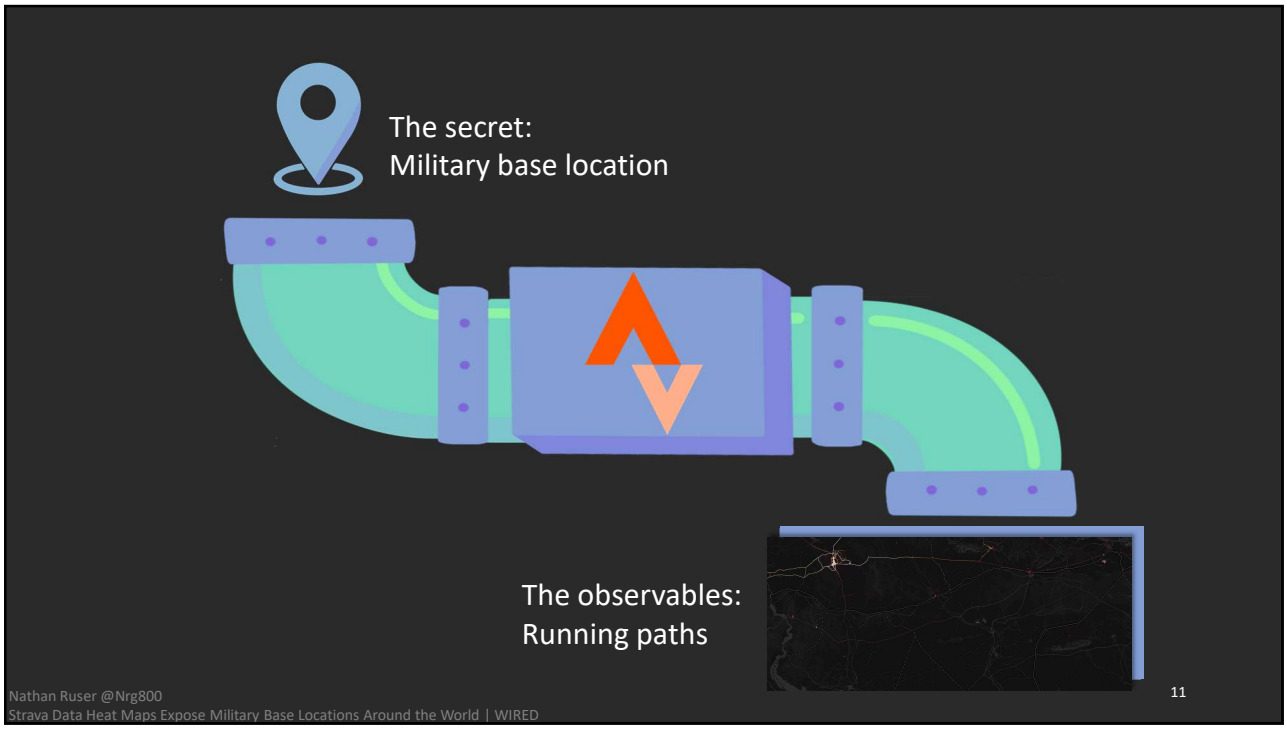
Goal: Exact or approximate?

Abilities: Multiple chances? Constraints?

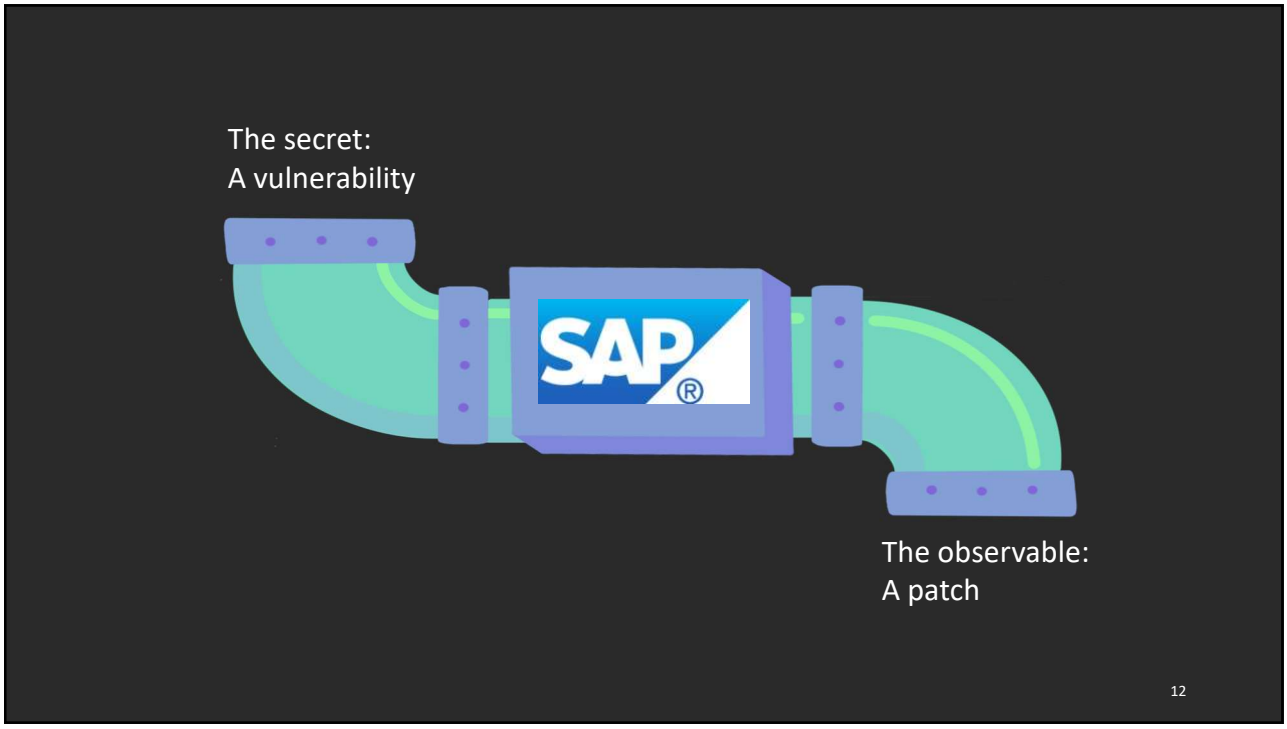
Cost: Consequences & rewards

10

10


The secret:
Military base location
The observables:
Running paths
Nathan Ruser @Nrg800
Strava Data Heat Maps Expose Military Base Locations Around the World | WIRED
11

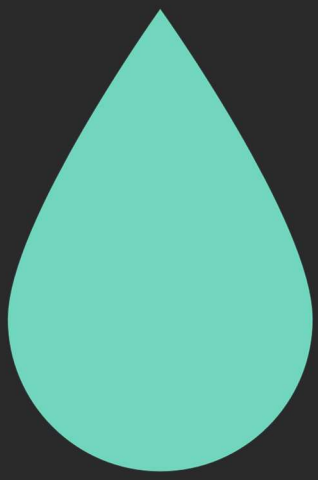
11


The secret:
A vulnerability
SAP
The observable:
A patch
12

12

Measuring Leakage

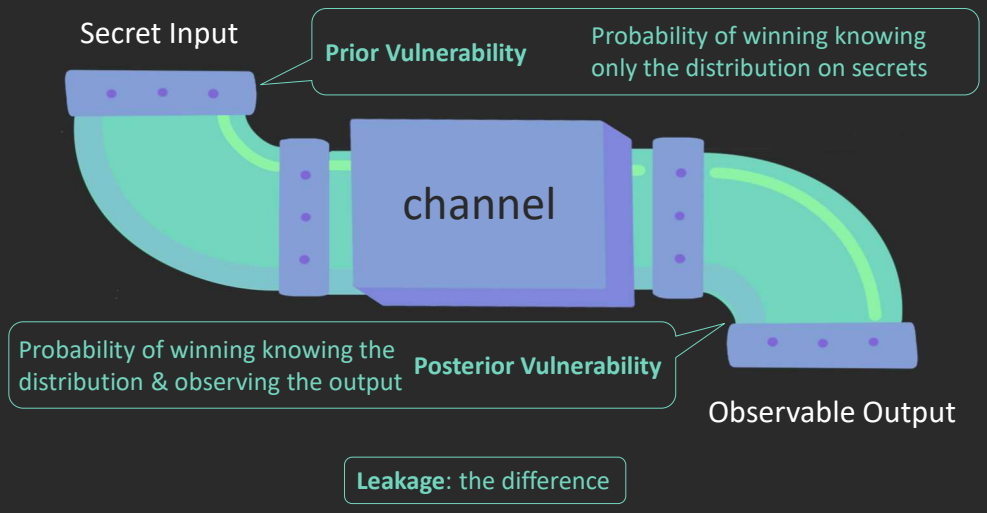
How to isolate the effect of a system



13

13

How to Measure Leakage



14

14

Calculating Leakage: Button vs Touchscreen

15

15

Setting Up

- Secret: 4-digit code
- Adversary: Bayes
  - Goal: guess entire secret exactly
  - Abilities: 1 try
  - Cost: All or nothing!

16

16

The Bayes Leakage Algorithm

1. Find distribution on secrets
2. Pick most likely secret ← prior vulnerability
3. For all outputs:
   1. Isolate secrets that could produce the output
   2. Sum secrets' probabilities ← prob. of output (PO)
   3. Normalize probabilities
   4. Pick most likely secret ← prob. of success (PS)
4. Σ(PO x PS) for all outputs ← posterior vulnerability
5. Leakage: prior vs. posterior (+/x)

17

17

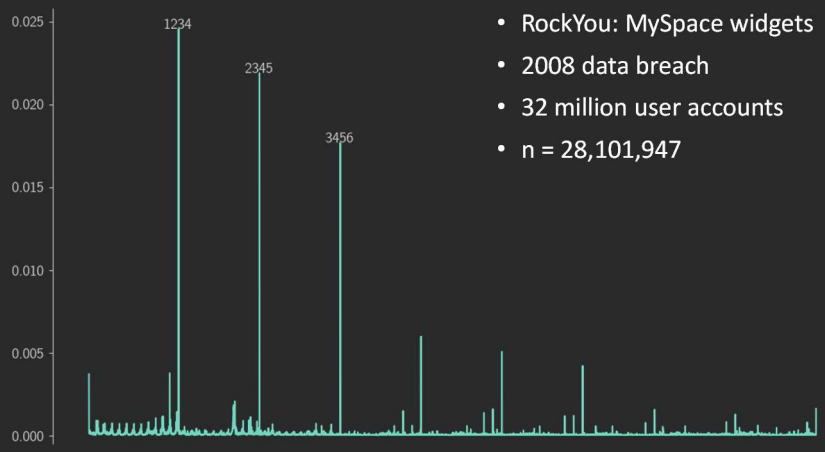
Bayes Leakage Algorithm

1. Find distribution on secrets
2. Pick most likely secret ← prior vulnerability
3. For all outputs:
   1. Isolate secrets that could produce the output
   2. Sum secrets' probabilities ← prob. of output (PO)
   3. Normalize probabilities
   4. Pick most likely secret ← prob. of success (PS)
4. Σ(PO x PS) for all outputs ← posterior vulnerability
5. Leakage: prior vs. posterior (+/x)

18

18

1. Find Distribution on Secrets



- RockYou: MySpace widgets
- 2008 data breach
- 32 million user accounts
- n = 28,101,947

https://github.com/sr-lab/pin-bank/blob/master/frequency/descending/4digit.txt

19

19

Bayes Leakage Algorithm

1. Find distribution on secrets
2. Pick most likely secret ← prior vulnerability
3. For all outputs:
   1. Isolate secrets that could produce the output
   2. Sum secrets' probabilities ← prob. of output (PO)
   3. Normalize probabilities
   4. Pick most likely secret ← prob. of success (PS)
4. Σ(PO x PS) for all outputs ← posterior vulnerability
5. Leakage: prior vs. posterior (+/x)

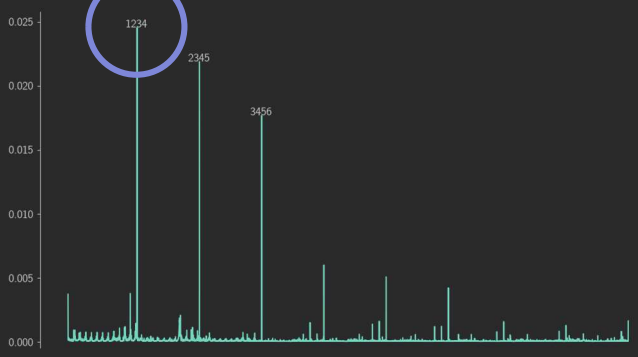
20

20

2. Prior Vulnerability

- Adversary will choose secret with the highest probability
- Pick the most likely code, 1234
- Prior Bayes vulnerability = 0.02455

Distribution on all 10,000 passcodes from the RockYou data breach



https://github.com/sr-lab/pin-bank/blob/master/frequency/descending/4digit.txt

21

21

Bayes Leakage Algorithm

1. Find distribution on secrets
2. Pick most likely secret ← prior vulnerability
3. For all outputs:
   1. Isolate secrets that could produce the output
   2. Sum secrets' probabilities ← prob. of output (PO)
   3. Normalize probabilities
   4. Pick most likely secret ← prob. of success (PS)
4. Σ(PO x PS) for all outputs ← posterior vulnerability
5. Leakage: prior vs. posterior (+/x)

22

22

Observable Outputs

Observables: numbers are worn

385 observable outputs

3 ... 2 5 ... 4 6 7 ... 1 6 8 9

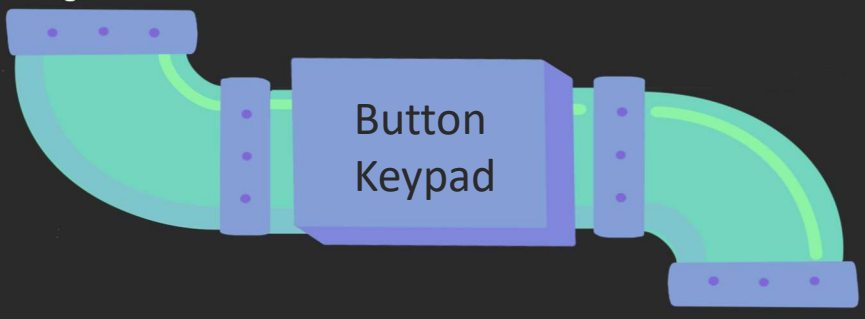
1 code | 14 codes | 36 codes | 24 codes

https://www.schneier.com/blog/archives/2009/07/information_lea_1.html

23

23

The secret:
4-digit code



The observables:
Worn numbers

24

24

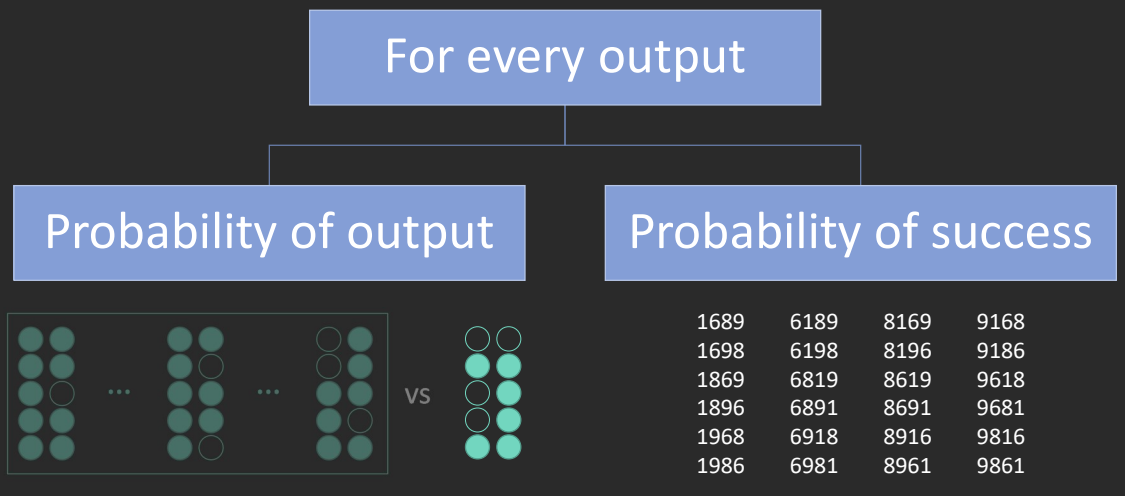
Bayes Leakage Algorithm

1. Find distribution on secrets
2. Pick most likely secret ← prior vulnerability
3. For all outputs:
   1. Isolate secrets that could produce the output
   2. Sum secrets' probabilities ← prob. of output (PO)
   3. Normalize probabilities
   4. Pick most likely secret ← prob. of success (PS)
4. Σ(PO x PS) for all outputs ← posterior vulnerability
5. Leakage: prior vs. posterior (+/x)

25

25

Observable Outputs



26

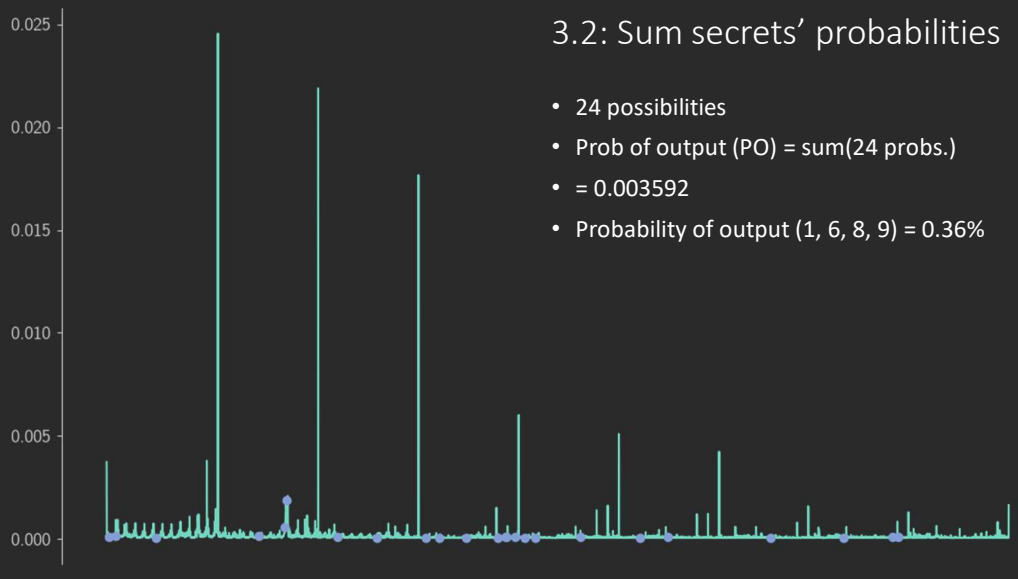
26

3.1: Isolate Secrets

1689	6189	8169	9168
1698	6198	8196	9186
1869	6819	8619	9618
1896	6891	8691	9681
1968	6918	8916	9816
1986	6981	8961	9861

27

27



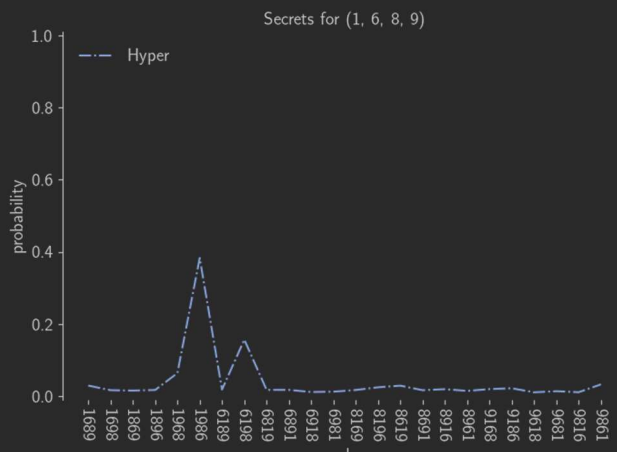
3.2: Sum secrets' probabilities

- 24 possibilities
- Prob of output (PO) = sum(24 probs.)
- = 0.003592
- Probability of output (1, 6, 8, 9) = 0.36%

28

28

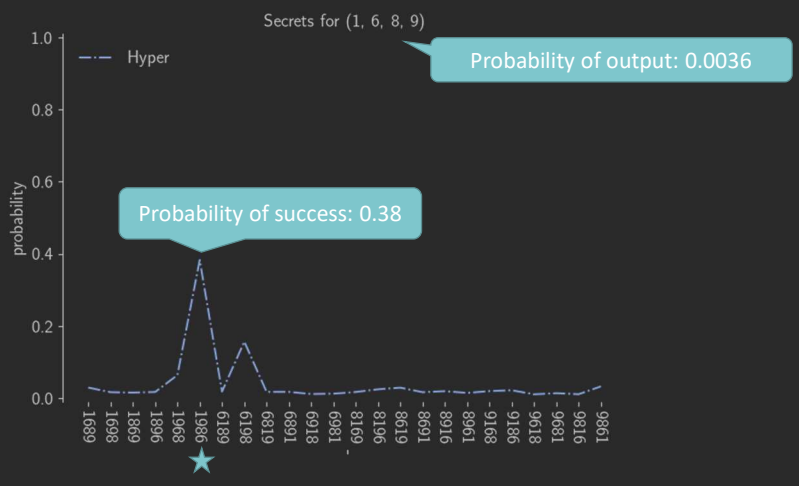
3.3: Normalize



29

29

3.4: Pick the Most Likely Secret



30

30

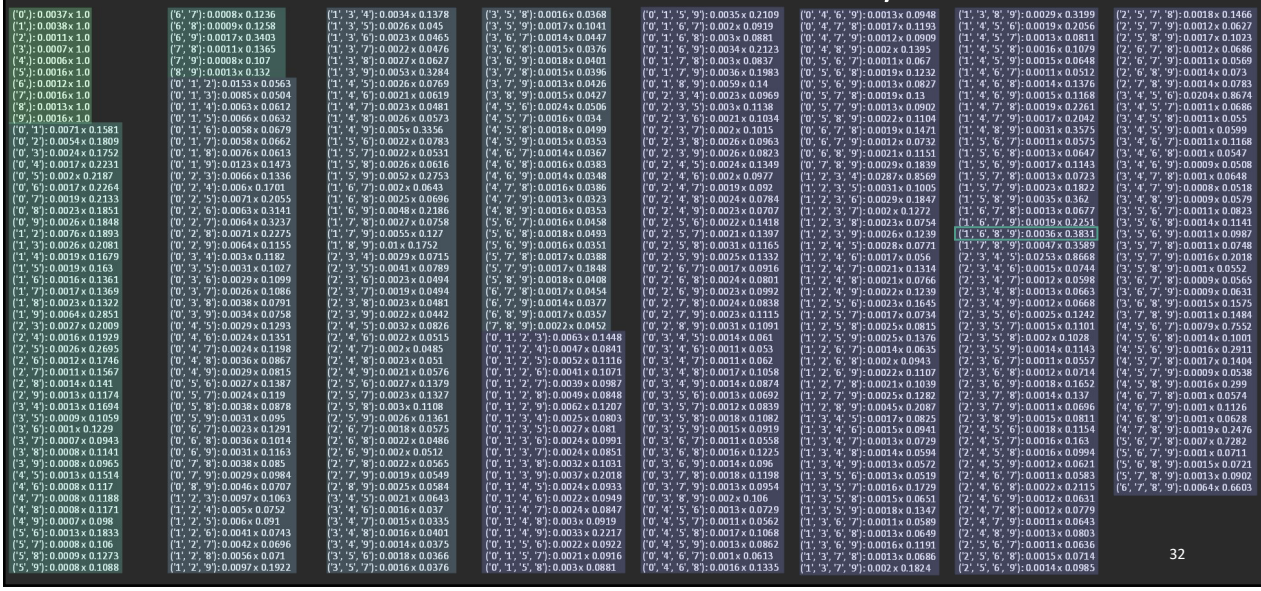
Bayes Leakage Algorithm

1. Find distribution on secrets
2. Pick most likely secret ← prior vulnerability
3. For all outputs:
   1. Isolate secrets that could produce the output
   2. Sum secrets' probabilities ← prob. of output (PO)
   3. Normalize probabilities
   4. Pick most likely secret ← prob. of success (PS)
4. Σ(PO x PS) for all outputs ← posterior vulnerability
5. Leakage: prior vs. posterior (+/x)

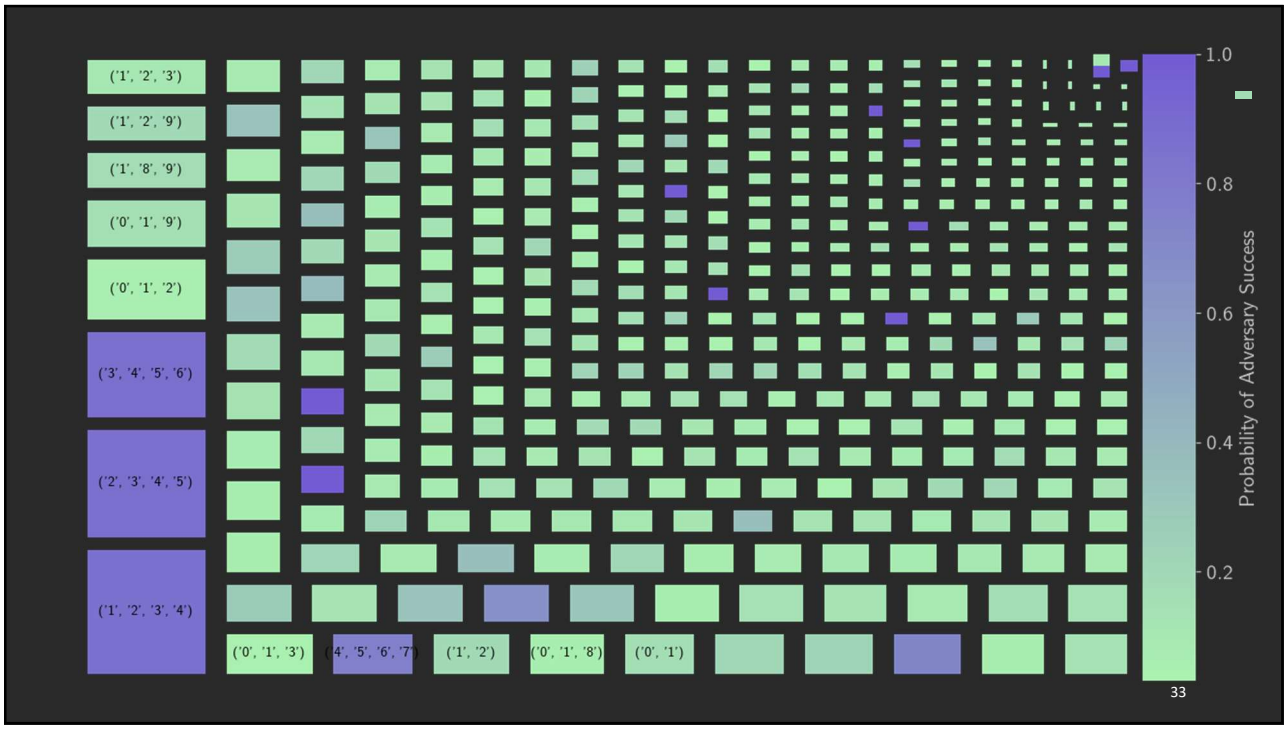
31

31

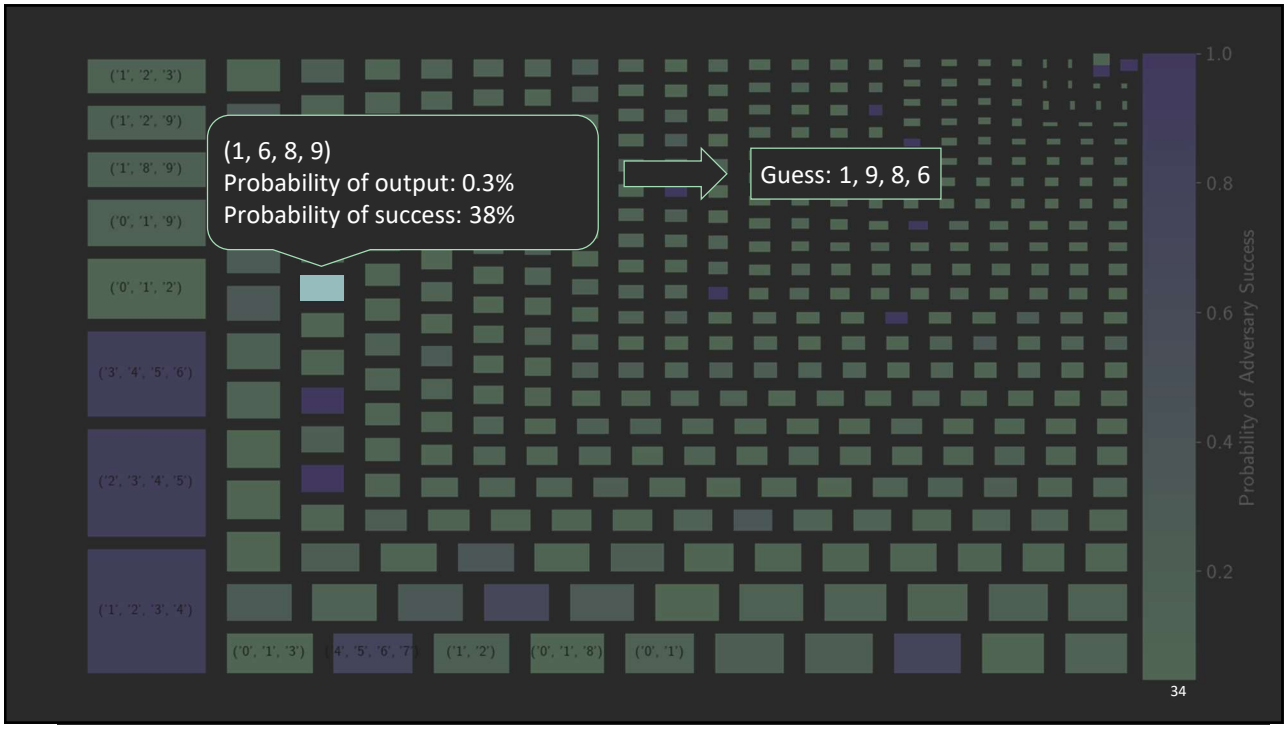
Posterior Vulnerability



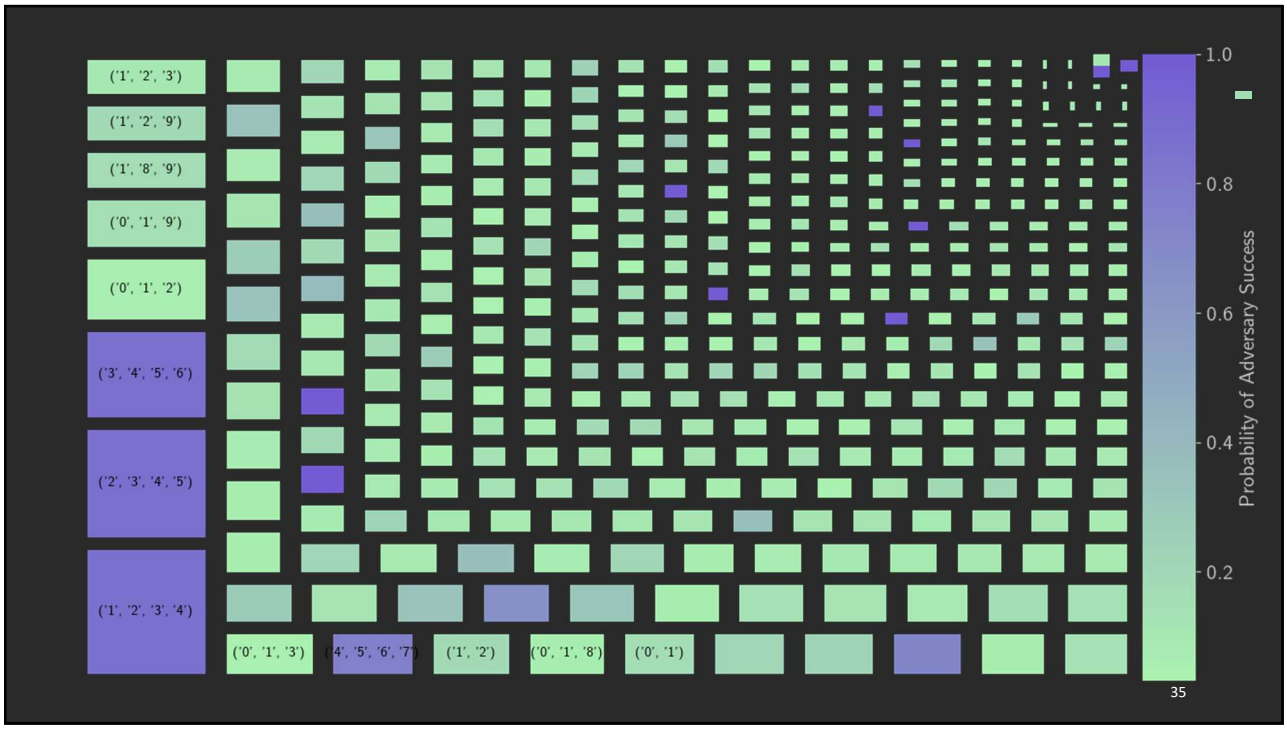
32


('1', '2', '3')
('1', '2', '9')
('1', '8', '9')
('0', '1', '9')
('0', '1', '2')
('3', '4', '5', '6')
('2', '3', '4', '5')
('1', '2', '3', '4')
('0', '1', '3')
('4', '5', '6', '7')
('1', '2')
('0', '1', '8')
('0', '1')
1.0
0.8
0.6
0.4
0.2
Probability of Adversary Success
33

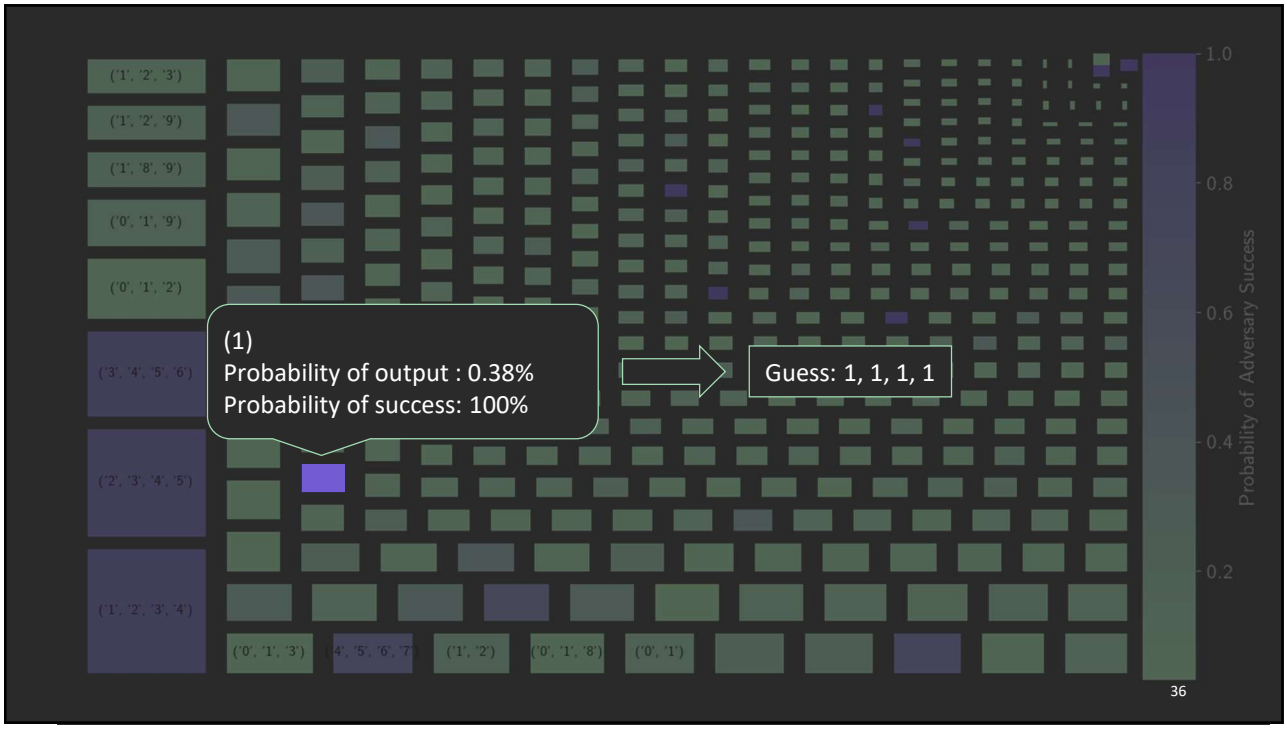
33


('1', '2', '3')
('1', '2', '9')
('1', '8', '9')
('0', '1', '9')
('0', '1', '2')
('3', '4', '5', '6')
('2', '3', '4', '5')
('1', '2', '3', '4')
('0', '1', '3')
('4', '5', '6', '7')
('1', '2')
('0', '1', '8')
('0', '1')
(1, 6, 8, 9)
Probability of output: 0.3%
Probability of success: 38%
Guess: 1, 9, 8, 6
1.0
0.8
0.6
0.4
0.2
Probability of Adversary Success
34

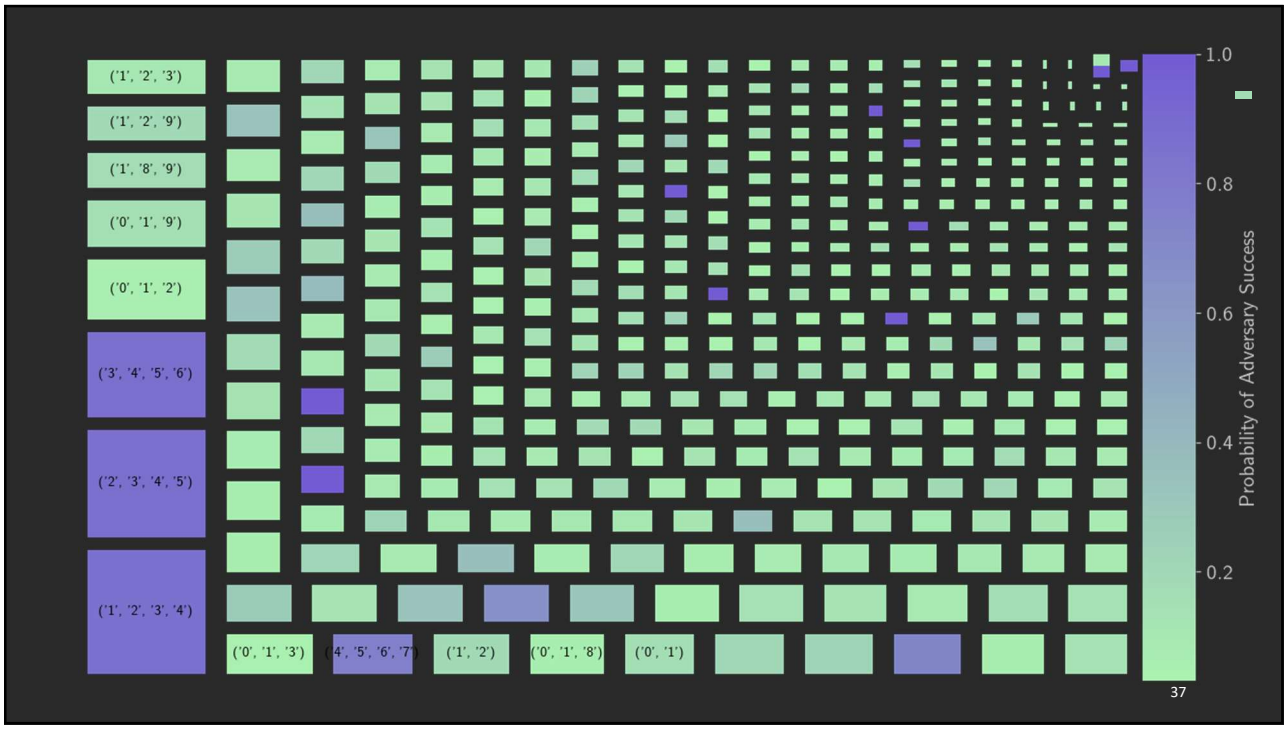
34


('1', '2', '3')
('1', '2', '9')
('1', '8', '9')
('0', '1', '9')
('0', '1', '2')
('3', '4', '5', '6')
('2', '3', '4', '5')
('1', '2', '3', '4')
('0', '1', '3')
('4', '5', '6', '7')
('1', '2')
('0', '1', '8')
('0', '1')
1.0
0.8
0.6
0.4
0.2
Probability of Adversary Success
35

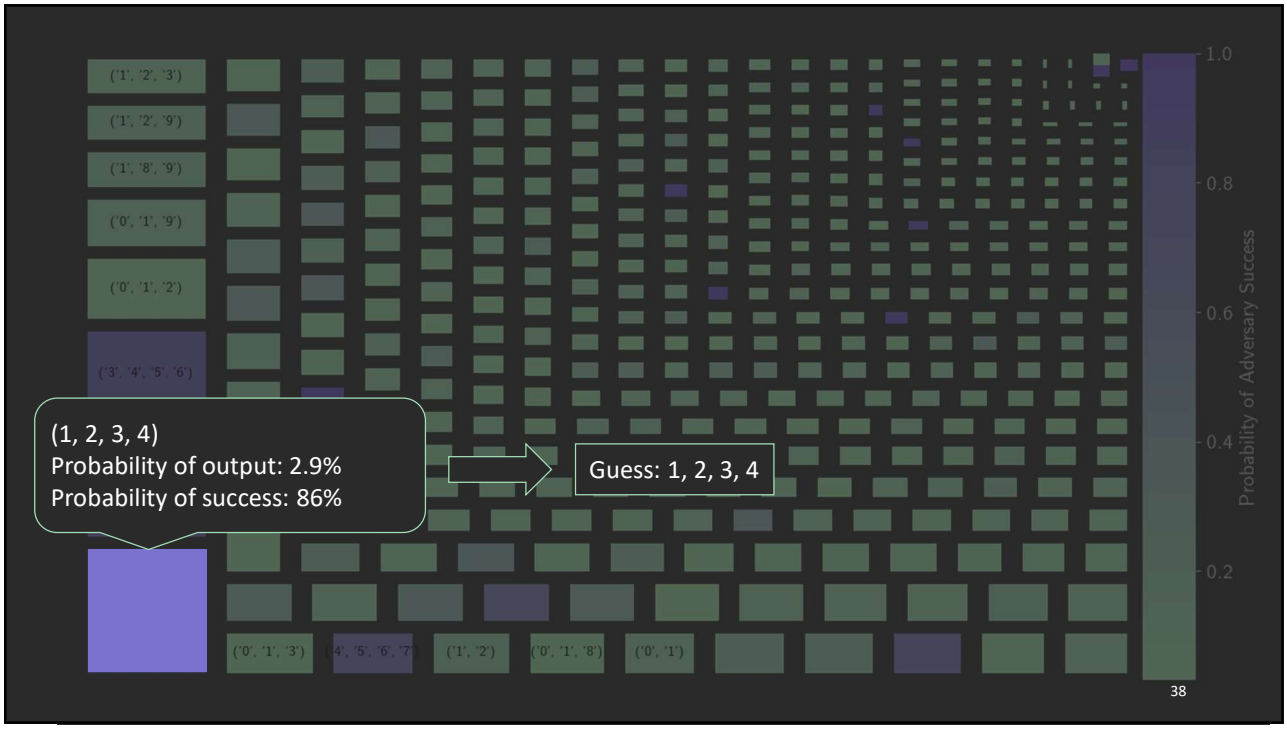
35


('1', '2', '3')
('1', '2', '9')
('1', '8', '9')
('0', '1', '9')
('0', '1', '2')
('3', '4', '5', '6')
('2', '3', '4', '5')
('1', '2', '3', '4')
('0', '1', '3')
('4', '5', '6', '7')
('1', '2')
('0', '1', '8')
('0', '1')
(1)
Probability of output : 0.38%
Probability of success: 100%
Guess: 1, 1, 1, 1
1.0
0.8
0.6
0.4
0.2
Probability of Adversary Success
36

36


('1', '2', '3')
('1', '2', '9')
('1', '8', '9')
('0', '1', '9')
('0', '1', '2')
('3', '4', '5', '6')
('2', '3', '4', '5')
('1', '2', '3', '4')
('0', '1', '3')
('4', '5', '6', '7')
('1', '2')
('0', '1', '8')
('0', '1')
1.0
0.8
0.6
0.4
0.2
Probability of Adversary Success
37

37


('1', '2', '3')
('1', '2', '9')
('1', '8', '9')
('0', '1', '9')
('0', '1', '2')
('3', '4', '5', '6')
(1, 2, 3, 4)
Probability of output: 2.9%
Probability of success: 86%
Guess: 1, 2, 3, 4
('0', '1', '3')
('4', '5', '6', '7')
('1', '2')
('0', '1', '8')
('0', '1')
1.0
0.8
0.6
0.4
0.2
Probability of Adversary Success
38

38

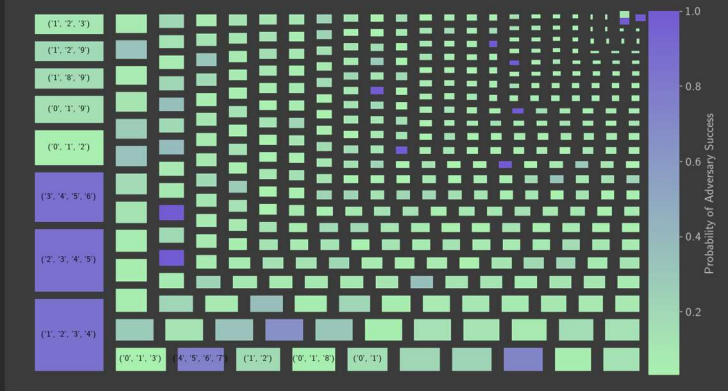
Bayes Leakage Algorithm

1. Find distribution on secrets
2. Pick most likely secret ← prior vulnerability
3. For all outputs:
   1. Isolate secrets that could produce the output
   2. Sum secrets' probabilities ← prob. of output (PO)
   3. Normalize probabilities
   4. Pick most likely secret ← prob. of success (PS)
4. Σ(PO x PS) for all outputs ← posterior vulnerability
5. Leakage: prior vs. posterior (+/x)

39

39

Posterior Bayes Vulnerability



- sum(prob. output x prob. success)
- Posterior Bayes vulnerability ≈ 0.2047

40

40

Posterior Vulnerability

('0',): 0.0037 x 1.0
('1',): 0.0038 x 1.0
('2',): 0.0011 x 1.0
('3',): 0.0007 x 1.0
('4',): 0.0006 x 1.0
('5',): 0.0016 x 1.0
('6',): 0.0012 x 1.0
('7',): 0.0016 x 1.0
('8',): 0.0013 x 1.0
('9',): 0.0016 x 1.0
('0', '1'): 0.0071 x 0.1581
('0', '2'): 0.0054 x 0.1809
('0', '3'): 0.0024 x 0.1752
('0', '4'): 0.0017 x 0.2231
('0', '5'): 0.002 x 0.2187
('0', '6'): 0.0017 x 0.2264
('0', '7'): 0.0019 x 0.2133
('0', '8'): 0.0023 x 0.1851
('0', '9'): 0.0026 x 0.1848
('1', '2'): 0.0076 x 0.1893
('1', '3'): 0.0026 x 0.2081
('1', '4'): 0.0019 x 0.1679
('1', '5'): 0.0019 x 0.163
('1', '6'): 0.0016 x 0.1361
('1', '7'): 0.0017 x 0.1369
('1', '8'): 0.0023 x 0.1322
('1', '9'): 0.0064 x 0.2851
('2', '3'): 0.0027 x 0.2009
('2', '4'): 0.0016 x 0.1929
('2', '5'): 0.0026 x 0.2695
('2', '6'): 0.0012 x 0.1746
('2', '7'): 0.0011 x 0.1567
('2', '8'): 0.0014 x 0.141
('2', '9'): 0.0013 x 0.1174
('3', '4'): 0.0013 x 0.1694
('3', '5'): 0.0009 x 0.1059
('3', '6'): 0.001 x 0.1229
('3', '7'): 0.0007 x 0.0943
('3', '8'): 0.0008 x 0.1141
('3', '9'): 0.0008 x 0.0965
('4', '5'): 0.0013 x 0.1514
('4', '6'): 0.0008 x 0.117
('4', '7'): 0.0008 x 0.1188
('4', '8'): 0.0008 x 0.1171
('4', '9'): 0.0007 x 0.098
('5', '6'): 0.0013 x 0.1833
('5', '7'): 0.0008 x 0.106
('5', '8'): 0.0009 x 0.1273
('5', '9'): 0.0008 x 0.1088

('6', '7'): 0.0008 x 0.1236
('6', '8'): 0.0009 x 0.1258
('6', '9'): 0.0017 x 0.3403
('7', '8'): 0.0011 x 0.1365
('7', '9'): 0.0008 x 0.107
('8', '9'): 0.0013 x 0.132
('0', '1', '2'): 0.0153 x 0.0563
('0', '1', '3'): 0.0085 x 0.0504
('0', '1', '4'): 0.0063 x 0.0612
('0', '1', '5'): 0.0066 x 0.0632
('0', '1', '6'): 0.0058 x 0.0679
('0', '1', '7'): 0.0058 x 0.0662
('0', '1', '8'): 0.0076 x 0.0613
('0', '1', '9'): 0.0123 x 0.1473
('0', '2', '3'): 0.0066 x 0.1336
('0', '2', '4'): 0.006 x 0.1701
('0', '2', '5'): 0.0071 x 0.2055
('0', '2', '6'): 0.0063 x 0.3141
('0', '2', '7'): 0.0064 x 0.3237
('0', '2', '8'): 0.0071 x 0.2275
('0', '2', '9'): 0.0064 x 0.1155
('0', '3', '4'): 0.003 x 0.1182
('0', '3', '5'): 0.0031 x 0.1027
('0', '3', '6'): 0.0029 x 0.1099
('0', '3', '7'): 0.0026 x 0.1086
('0', '3', '8'): 0.0038 x 0.0791
('0', '3', '9'): 0.0034 x 0.0758
('0', '4', '5'): 0.0029 x 0.1293
('0', '4', '6'): 0.0024 x 0.1351
('0', '4', '7'): 0.0024 x 0.1198
('0', '4', '8'): 0.0036 x 0.0867
('0', '4', '9'): 0.0029 x 0.0815
('0', '5', '6'): 0.0027 x 0.1387
('0', '5', '7'): 0.0024 x 0.119
('0', '5', '8'): 0.0038 x 0.0878
('0', '5', '9'): 0.0031 x 0.095
('0', '6', '7'): 0.0023 x 0.1291
('0', '6', '8'): 0.0036 x 0.1014
('0', '6', '9'): 0.0031 x 0.1163
('0', '7', '8'): 0.0038 x 0.085
('0', '7', '9'): 0.0029 x 0.0984
('0', '8', '9'): 0.0046 x 0.0707
('1', '2', '3'): 0.0097 x 0.1063
('1', '2', '4'): 0.005 x 0.0752
('1', '2', '5'): 0.006 x 0.091
('1', '2', '6'): 0.0041 x 0.0743
('1', '2', '7'): 0.0042 x 0.0696
('1', '2', '8'): 0.0056 x 0.071
('1', '2', '9'): 0.0097 x 0.1922

('1', '3', '4'): 0.0034 x 0.1378
('1', '3', '5'): 0.0026 x 0.045
('1', '3', '6'): 0.0023 x 0.0465
('1', '3', '7'): 0.0022 x 0.0476
('1', '3', '8'): 0.0027 x 0.0627
('1', '3', '9'): 0.0053 x 0.3284
('1', '4', '5'): 0.0026 x 0.0769
('1', '4', '6'): 0.0021 x 0.0619
('1', '4', '7'): 0.0023 x 0.0481
('1', '4', '8'): 0.0026 x 0.0573
('1', '4', '9'): 0.005 x 0.3356
('1', '5', '6'): 0.0022 x 0.0783
('1', '5', '7'): 0.0022 x 0.0531
('1', '5', '8'): 0.0026 x 0.0616
('1', '5', '9'): 0.0052 x 0.2753
('1', '6', '7'): 0.002 x 0.0643
('1', '6', '8'): 0.0025 x 0.0696
('1', '6', '9'): 0.0048 x 0.2186
('1', '7', '8'): 0.0027 x 0.0758
('1', '7', '9'): 0.0055 x 0.127
('1', '8', '9'): 0.01 x 0.1752
('2', '3', '4'): 0.0029 x 0.0715
('2', '3', '5'): 0.0041 x 0.0789
('2', '3', '6'): 0.0023 x 0.0494
('2', '3', '7'): 0.0019 x 0.0494
('2', '3', '8'): 0.0023 x 0.0481
('2', '3', '9'): 0.0022 x 0.0442
('2', '4', '5'): 0.0032 x 0.0826
('2', '4', '6'): 0.0022 x 0.0515
('2', '4', '7'): 0.002 x 0.0485
('2', '4', '8'): 0.0023 x 0.051
('2', '4', '9'): 0.0021 x 0.0576
('2', '5', '6'): 0.0027 x 0.1379
('2', '5', '7'): 0.0023 x 0.1327
('2', '5', '8'): 0.003 x 0.1108
('2', '5', '9'): 0.0026 x 0.1361
('2', '6', '7'): 0.0018 x 0.0575
('2', '6', '8'): 0.0022 x 0.0486
('2', '6', '9'): 0.002 x 0.0512
('2', '7', '8'): 0.0022 x 0.0565
('2', '7', '9'): 0.0019 x 0.0549
('2', '8', '9'): 0.0025 x 0.0584
('3', '4', '5'): 0.0021 x 0.0643
('3', '4', '6'): 0.0016 x 0.037
('3', '4', '7'): 0.0015 x 0.0335
('3', '4', '8'): 0.0016 x 0.0401
('3', '4', '9'): 0.0014 x 0.0375
('3', '5', '6'): 0.0018 x 0.0366
('3', '5', '7'): 0.0016 x 0.0376

('3', '5', '8'): 0.0016 x 0.0368
('3', '5', '9'): 0.0017 x 0.1041
('3', '6', '7'): 0.0014 x 0.0447
('3', '6', '8'): 0.0015 x 0.0376
('3', '6', '9'): 0.0018 x 0.0401
('3', '7', '8'): 0.0015 x 0.0396
('3', '7', '9'): 0.0013 x 0.0426
('3', '8', '9'): 0.0015 x 0.0427
('4', '5', '6'): 0.0024 x 0.0506
('4', '5', '7'): 0.0016 x 0.034
('4', '5', '8'): 0.0018 x 0.0499
('4', '5', '9'): 0.0015 x 0.0353
('4', '6', '7'): 0.0014 x 0.0367
('4', '6', '8'): 0.0016 x 0.0383
('4', '6', '9'): 0.0014 x 0.0348
('4', '7', '8'): 0.0016 x 0.0386
('4', '7', '9'): 0.0013 x 0.0323
('4', '8', '9'): 0.0016 x 0.0353
('5', '6', '7'): 0.0016 x 0.0458
('5', '6', '8'): 0.0018 x 0.0493
('5', '6', '9'): 0.0016 x 0.0351
('5', '7', '8'): 0.0017 x 0.0388
('5', '7', '9'): 0.0017 x 0.1848
('5', '8', '9'): 0.0018 x 0.0408
('6', '7', '8'): 0.0017 x 0.0454
('6', '7', '9'): 0.0014 x 0.0377
('6', '8', '9'): 0.0017 x 0.0357
('7', '8', '9'): 0.0022 x 0.0452
('0', '1', '2', '3'): 0.0063 x 0.1448
('0', '1', '2', '4'): 0.0047 x 0.0841
('0', '1', '2', '5'): 0.0052 x 0.1116
('0', '1', '2', '6'): 0.0041 x 0.1071
('0', '1', '2', '7'): 0.0039 x 0.0987
('0', '1', '2', '8'): 0.0049 x 0.0848
('0', '1', '2', '9'): 0.0062 x 0.1207
('0', '1', '3', '4'): 0.0025 x 0.0803
('0', '1', '3', '5'): 0.0027 x 0.081
('0', '1', '3', '6'): 0.0024 x 0.0991
('0', '1', '3', '7'): 0.0024 x 0.0851
('0', '1', '3', '8'): 0.0032 x 0.1031
('0', '1', '3', '9'): 0.0037 x 0.2018
('0', '1', '4', '5'): 0.0024 x 0.0933
('0', '1', '4', '6'): 0.0022 x 0.0949
('0', '1', '4', '7'): 0.0024 x 0.0847
('0', '1', '4', '8'): 0.003 x 0.0919
('0', '1', '4', '9'): 0.0033 x 0.2217
('0', '1', '5', '6'): 0.0022 x 0.0922
('0', '1', '5', '7'): 0.0021 x 0.0916
('0', '1', '5', '8'): 0.003 x 0.0881

('0', '1', '5', '9'): 0.0035 x 0.2109
('0', '1', '6', '7'): 0.002 x 0.0919
('0', '1', '6', '8'): 0.003 x 0.0881
('0', '1', '6', '9'): 0.0034 x 0.2123
('0', '1', '7', '8'): 0.003 x 0.0837
('0', '1', '7', '9'): 0.0036 x 0.1983
('0', '1', '8', '9'): 0.0059 x 0.14
('0', '2', '3', '4'): 0.0023 x 0.0969
('0', '2', '3', '5'): 0.003 x 0.1138
('0', '2', '3', '6'): 0.0021 x 0.1034
('0', '2', '3', '7'): 0.002 x 0.1015
('0', '2', '3', '8'): 0.0026 x 0.0963
('0', '2', '3', '9'): 0.0026 x 0.0823
('0', '2', '4', '5'): 0.0024 x 0.1349
('0', '2', '4', '6'): 0.002 x 0.0977
('0', '2', '4', '7'): 0.0019 x 0.092
('0', '2', '4', '8'): 0.0024 x 0.0784
('0', '2', '4', '9'): 0.0023 x 0.0707
('0', '2', '5', '6'): 0.0022 x 0.1418
('0', '2', '5', '7'): 0.0021 x 0.1397
('0', '2', '5', '8'): 0.0031 x 0.1165
('0', '2', '5', '9'): 0.0025 x 0.1332
('0', '2', '6', '7'): 0.0017 x 0.0916
('0', '2', '6', '8'): 0.0024 x 0.0801
('0', '2', '6', '9'): 0.0023 x 0.0992
('0', '2', '7', '8'): 0.0024 x 0.0838
('0', '2', '7', '9'): 0.0023 x 0.1115
('0', '2', '8', '9'): 0.0031 x 0.1091
('0', '3', '4', '5'): 0.0014 x 0.061
('0', '3', '4', '6'): 0.0011 x 0.053
('0', '3', '4', '7'): 0.0011 x 0.062
('0', '3', '4', '8'): 0.0017 x 0.1058
('0', '3', '4', '9'): 0.0014 x 0.0874
('0', '3', '5', '6'): 0.0013 x 0.0692
('0', '3', '5', '7'): 0.0012 x 0.0839
('0', '3', '5', '8'): 0.0018 x 0.1082
('0', '3', '5', '9'): 0.0015 x 0.0919
('0', '3', '6', '7'): 0.0011 x 0.0558
('0', '3', '6', '8'): 0.0016 x 0.1225
('0', '3', '6', '9'): 0.0014 x 0.096
('0', '3', '7', '8'): 0.0018 x 0.1198
('0', '3', '7', '9'): 0.0013 x 0.0954
('0', '3', '8', '9'): 0.002 x 0.106
('0', '4', '5', '6'): 0.0013 x 0.0729
('0', '4', '5', '7'): 0.0011 x 0.0562
('0', '4', '5', '8'): 0.0017 x 0.1068
('0', '4', '5', '9'): 0.0013 x 0.0862
('0', '4', '6', '7'): 0.001 x 0.0613
('0', '4', '6', '8'): 0.0016 x 0.1335

('0', '4', '6', '9'): 0.0013 x 0.0948
('0', '4', '7', '8'): 0.0017 x 0.1193
('0', '4', '7', '9'): 0.0012 x 0.0909
('0', '4', '8', '9'): 0.002 x 0.1395
('0', '5', '6', '7'): 0.0011 x 0.067
('0', '5', '6', '8'): 0.0019 x 0.1232
('0', '5', '6', '9'): 0.0013 x 0.0827
('0', '5', '7', '8'): 0.0019 x 0.13
('0', '5', '7', '9'): 0.0013 x 0.0902
('0', '5', '8', '9'): 0.0022 x 0.1104
('0', '6', '7', '9'): 0.0012 x 0.0732
('0', '6', '8', '9'): 0.0021 x 0.1151
('0', '7', '8', '9'): 0.0029 x 0.1839
('1', '2', '3', '4'): 0.0287 x 0.8569
('1', '2', '3', '5'): 0.0031 x 0.1005
('1', '2', '3', '6'): 0.0029 x 0.1847
('1', '2', '3', '7'): 0.002 x 0.1272
('1', '2', '3', '8'): 0.0023 x 0.0754
('1', '2', '3', '9'): 0.0026 x 0.1239
('1', '2', '4', '5'): 0.0028 x 0.0771
('1', '2', '4', '6'): 0.0017 x 0.056
('1', '2', '4', '7'): 0.0021 x 0.1314
('1', '2', '4', '8'): 0.0021 x 0.0766
('1', '2', '4', '9'): 0.0022 x 0.1239
('1', '2', '5', '6'): 0.0023 x 0.1645
('1', '2', '5', '7'): 0.0017 x 0.0734
('1', '2', '5', '8'): 0.0025 x 0.0815
('1', '2', '5', '9'): 0.0025 x 0.1376
('1', '2', '6', '7'): 0.0014 x 0.0635
('1', '2', '6', '8'): 0.002 x 0.0943
('1', '2', '6', '9'): 0.0022 x 0.1107
('1', '2', '7', '8'): 0.0021 x 0.1039
('1', '2', '7', '9'): 0.0025 x 0.1282
('1', '2', '8', '9'): 0.0045 x 0.2087
('1', '3', '4', '5'): 0.0017 x 0.0825
('1', '3', '4', '6'): 0.0015 x 0.0941
('1', '3', '4', '7'): 0.0013 x 0.0729
('1', '3', '4', '8'): 0.0014 x 0.0594
('1', '3', '4', '9'): 0.0013 x 0.0572
('1', '3', '5', '6'): 0.0013 x 0.0519
('1', '3', '5', '7'): 0.0016 x 0.1729
('1', '3', '5', '8'): 0.0015 x 0.0651
('1', '3', '5', '9'): 0.0018 x 0.1347
('1', '3', '6', '7'): 0.0011 x 0.0589
('1', '3', '6', '8'): 0.0013 x 0.0649
('1', '3', '6', '9'): 0.0016 x 0.1191
('1', '3', '7', '8'): 0.0013 x 0.0686
('1', '3', '7', '9'): 0.002 x 0.1824

('1', '3', '8', '9'): 0.0029 x 0.3199
('1', '4', '5', '6'): 0.0019 x 0.2056
('1', '4', '5', '7'): 0.0013 x 0.0811
('1', '4', '5', '8'): 0.0016 x 0.1079
('1', '4', '5', '9'): 0.0015 x 0.0648
('1', '4', '6', '7'): 0.0011 x 0.0512
('1', '4', '6', '8'): 0.0014 x 0.1376
('1', '4', '6', '9'): 0.0015 x 0.1168
('1', '4', '7', '8'): 0.0019 x 0.2261
('1', '4', '7', '9'): 0.0017 x 0.2042
('1', '4', '8', '9'): 0.0031 x 0.3575
('1', '5', '6', '7'): 0.0011 x 0.0575
('1', '5', '6', '8'): 0.0013 x 0.0647
('1', '5', '6', '9'): 0.0017 x 0.1143
('1', '5', '7', '8'): 0.0013 x 0.0723
('1', '5', '7', '9'): 0.0023 x 0.1822
('1', '5', '8', '9'): 0.0035 x 0.362
('1', '6', '7', '8'): 0.0013 x 0.0677
('1', '6', '7', '9'): 0.0019 x 0.2251
('1', '6', '8', '9'): 0.0036 x 0.3831
('1', '7', '8', '9'): 0.0047 x 0.3589
('2', '3', '4', '5'): 0.0253 x 0.8668
('2', '3', '4', '6'): 0.0015 x 0.0744
('2', '3', '4', '7'): 0.0012 x 0.0598
('2', '3', '4', '8'): 0.0013 x 0.0663
('2', '3', '4', '9'): 0.0012 x 0.0668
('2', '3', '5', '6'): 0.0025 x 0.1242
('2', '3', '5', '7'): 0.0015 x 0.1101
('2', '3', '5', '8'): 0.002 x 0.1028
('2', '3', '5', '9'): 0.0014 x 0.1143
('2', '3', '6', '7'): 0.0011 x 0.0557
('2', '3', '6', '8'): 0.0012 x 0.0714
('2', '3', '6', '9'): 0.0018 x 0.1652
('2', '3', '7', '8'): 0.0014 x 0.137
('2', '3', '7', '9'): 0.0011 x 0.0696
('2', '3', '8', '9'): 0.0015 x 0.0811
('2', '4', '5', '6'): 0.0018 x 0.1154
('2', '4', '5', '7'): 0.0016 x 0.163
('2', '4', '5', '8'): 0.0016 x 0.0994
('2', '4', '5', '9'): 0.0012 x 0.0621
('2', '4', '6', '7'): 0.0011 x 0.0583
('2', '4', '6', '8'): 0.0022 x 0.2115
('2', '4', '6', '9'): 0.0012 x 0.0631
('2', '4', '7', '8'): 0.0012 x 0.0779
('2', '4', '7', '9'): 0.0011 x 0.0643
('2', '4', '8', '9'): 0.0013 x 0.0803
('2', '5', '6', '7'): 0.0011 x 0.0636
('2', '5', '6', '8'): 0.0015 x 0.0714
('2', '5', '6', '9'): 0.0014 x 0.0985

('2', '5', '7', '8'): 0.0018 x 0.1466
('2', '5', '7', '9'): 0.0012 x 0.0627
('2', '5', '8', '9'): 0.0017 x 0.1023
('2', '6', '7', '8'): 0.0012 x 0.0686
('2', '6', '7', '9'): 0.0011 x 0.0569
('2', '6', '8', '9'): 0.0014 x 0.073
('2', '7', '8', '9'): 0.0014 x 0.0783
('3', '4', '5', '6'): 0.0204 x 0.8674
('3', '4', '5', '7'): 0.0011 x 0.0686
('3', '4', '5', '8'): 0.0011 x 0.055
('3', '4', '5', '9'): 0.001 x 0.0599
('3', '4', '6', '7'): 0.0011 x 0.1168
('3', '4', '6', '8'): 0.001 x 0.0547
('3', '4', '6', '9'): 0.0009 x 0.0508
('3', '4', '7', '8'): 0.001 x 0.0648
('3', '4', '7', '9'): 0.0008 x 0.0518
('3', '4', '8', '9'): 0.0009 x 0.0579
('3', '5', '6', '7'): 0.0011 x 0.0823
('3', '5', '6', '8'): 0.0014 x 0.1141
('3', '5', '6', '9'): 0.0011 x 0.0987
('3', '5', '7', '8'): 0.0011 x 0.0748
('3', '5', '7', '9'): 0.0016 x 0.2018
('3', '5', '8', '9'): 0.001 x 0.0552
('3', '6', '7', '8'): 0.0009 x 0.0565
('3', '6', '7', '9'): 0.0009 x 0.0631
('3', '6', '8', '9'): 0.0015 x 0.1575
('3', '7', '8', '9'): 0.0011 x 0.1484
('4', '5', '6', '7'): 0.0079 x 0.7552
('4', '5', '6', '8'): 0.0014 x 0.1001
('4', '5', '6', '9'): 0.0016 x 0.2911
('4', '5', '7', '8'): 0.0017 x 0.1404
('4', '5', '7', '9'): 0.0009 x 0.0538
('4', '5', '8', '9'): 0.0016 x 0.299
('4', '6', '7', '8'): 0.001 x 0.0574
('4', '6', '7', '9'): 0.001 x 0.1126
('4', '6', '8', '9'): 0.001 x 0.0628
('4', '7', '8', '9'): 0.0019 x 0.2476
('5', '6', '7', '8'): 0.007 x 0.7282
('5', '6', '7', '9'): 0.001 x 0.0711
('5', '6', '8', '9'): 0.0015 x 0.0721
('5', '7', '8', '9'): 0.0013 x 0.0902
('6', '7', '8', '9'): 0.0064 x 0.6603

+

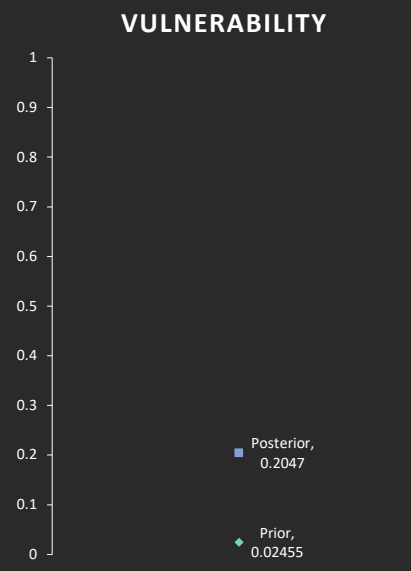
≈ 0.2047

Bayes Leakage Algorithm

1. Find distribution on secrets
2. Pick most likely secret ← prior vulnerability
3. For all outputs:
   1. Isolate secrets that could produce the output
   2. Sum secrets' probabilities ← prob. of output (PO)
   3. Normalize probabilities
   4. Pick most likely secret ← prob. of success (PS)
4. Σ(PO x PS) for all outputs ← posterior vulnerability
5. Leakage: prior vs. posterior (+/x)

5. Leakage

- Multiplicative leakage = post / prior = 8.3x
- Additive leakage = post – prior = 0.18
- Summary:
  - Using the button keypad moves your vulnerability up to 20%, a 1 in 5 chance
  - Pay the extra $30 for the touchscreen



43

43

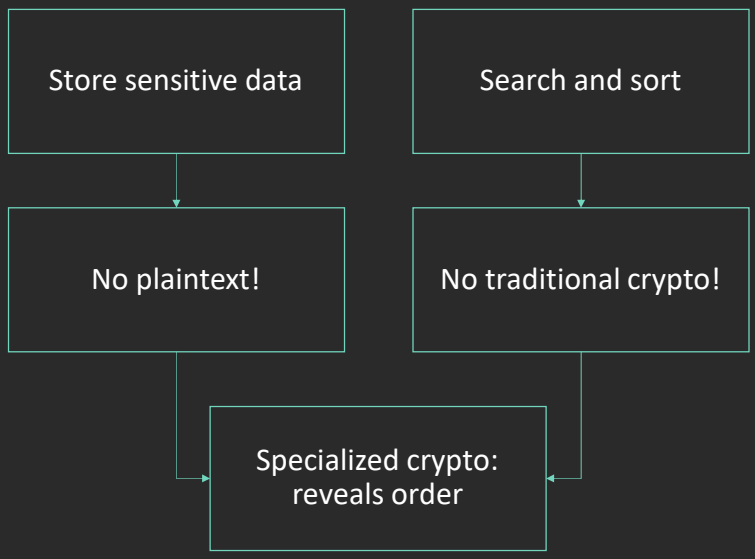
Order-Reveaing Encryption

A Formal Information-Theoretic Leakage Analysis of Order-Revealing Encryption
Mireya Jurado, Catuscia Palamidessi, Geoffrey Smith
34th IEEE Computer Security Foundations Symposium (CSF21)

44

44

Motivation

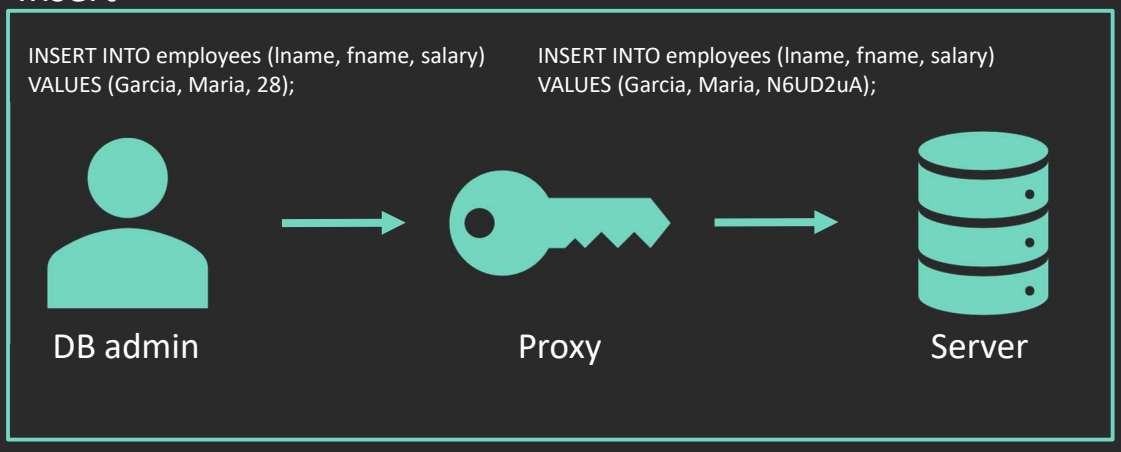


45

45

Order-Revealing Encryption (ORE)

Insert

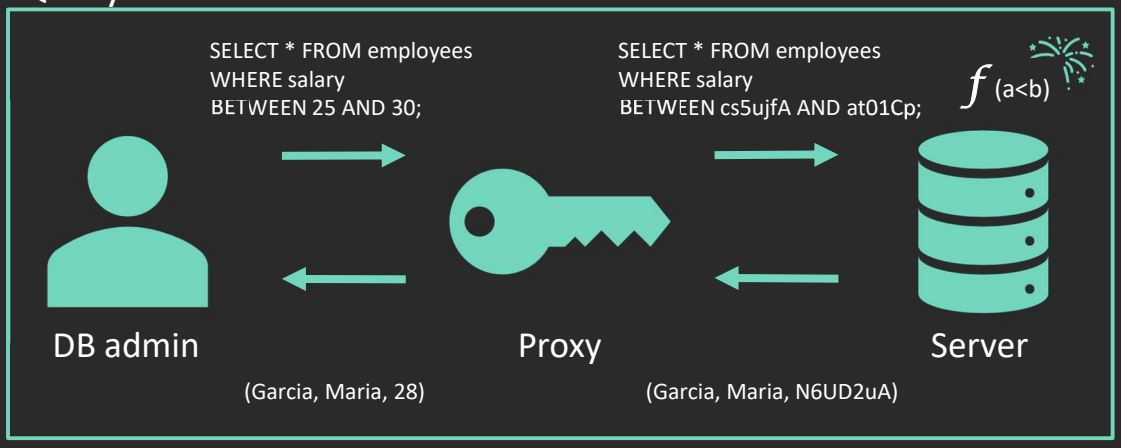


46

46

Order-Reveaing Encryption (ORE)

Query

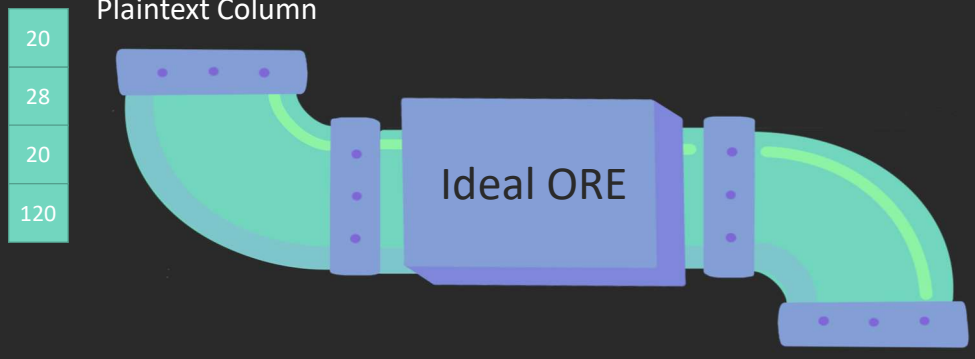


47

47

Ideal ORE

Plaintext Column

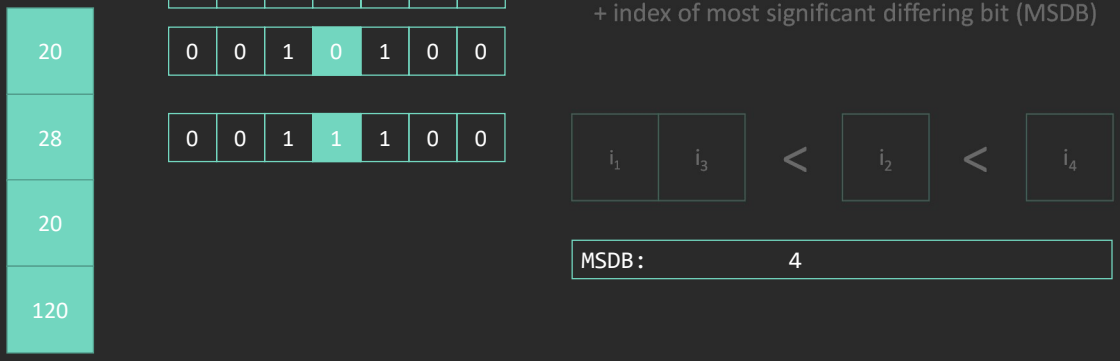


Order of indices i_1 i_3 < i_2 < i_4

48

48

CLWW ORE

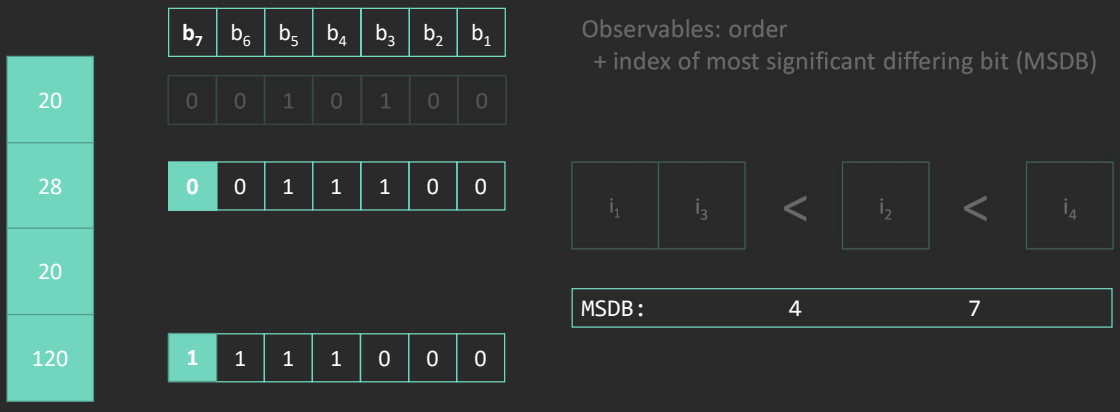


Chenette, Lewi, Weis, & Wu, Practical Order-Revealing Encryption with limited leakage. *Fast Software Encryption* (2016)

49

49

CLWW ORE



Chenette, Lewi, Weis, & Wu, Practical Order-Revealing Encryption with limited leakage. *Fast Software Encryption* (2016)

50

50

CLWW ORE

Plaintext Column

20
28
20
120

Order of indices i_1 i_3 < i_2 < i_4

+ index of most significant differing bit

MSDB: 4 7

51

51

MSDB Intuition

Secret Guess	Observable Output	Secret Guess
125 … 127	MSDB info narrows down the secret	11 … 65
i_1 i_3 < i_2 < i_4	i_1 i_3 < i_2 < i_4	i_1 i_3 < i_2 < i_4
MSDB: 2 1	MSDB: 4 7	MSDB: 6 7

52

52

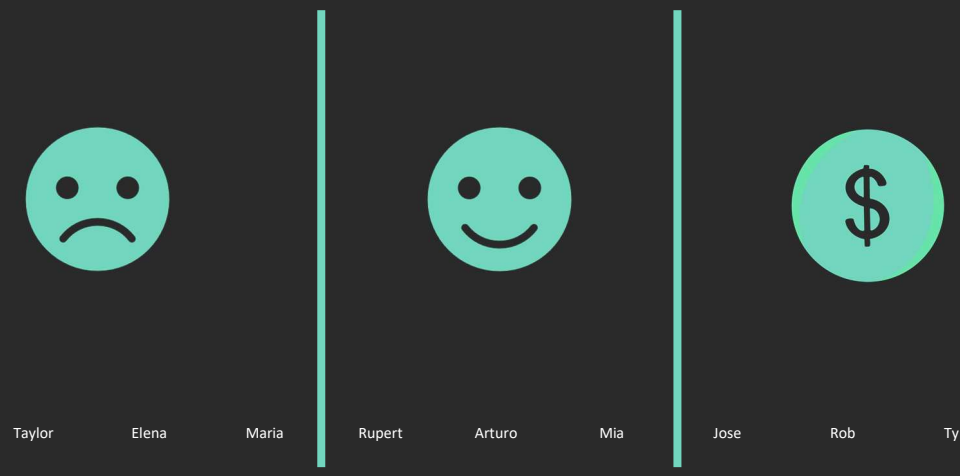

With 7-bit secret & 4 people
no output
268,435,456
...
just order
341,376
i_1 i_3 < i_2 < i_4
order + bits
32,768
i_1 i_3 < i_2 < i_4
MSDB: 4 7
53

53


Bucketing adversary
Employee Salaries
100
90
80
70
60
50
40
30
20
10
0
Taylor
Elena
Maria
Rupert
Arturo
Mia
Jose
Rob
Tyra
$/Hr
54

54

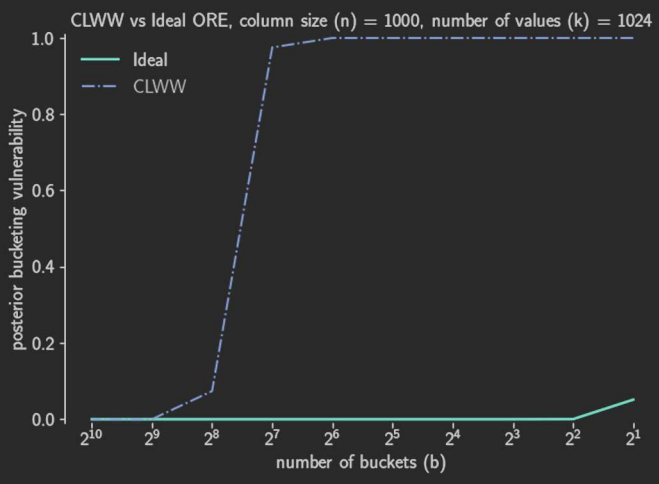
Bucketing adversary



55

55

Bucketing Vulnerability



56

56

Call to Action

Apply QIF:
- Quantify leakage exactly

Apply QIF principles:
- ID secret
- ID observables
- ID adversary
- Approximate distribution on secrets

Preventative Measure:
- Disassociate observables from secrets

Resources:
- Book: The Science of Quantitative Information Flow (2020)
- Blog: sprayonsecurity.com

57

57