Secret Sharing

CS 5158/6058 Data Security and Privacy

Spring 2018

Instructor: Boyang Wang

Problem Setting

- I have a secret message m, and we have 3 users, Alice, Bob, and Charlie
  - E.g. m = 123-456-789 (my SSN)

- I want to share message m with the 3 users.
- Attacker can compromise at <u>most 2 users</u>

- Goal: I can still recover this m & minimizing the privacy leakage if (at most 2) users are compromised

Solution 1

- 3 users: Alice, Bob & Charlie
- Secret message: m = 123-456-789

- Solution 1: I give
  - Alice a copy of 123-456-789
  - Bob a copy of 123-456-789
  - Charlie a copy of 123-456-789
  - I delete my copy of SSN
- I contact any user, I can recover SSN

Solution 1

- Solution 1: I give
  - Alice a copy of 123-456-789
  - Bob a copy of 123-456-789
  - Charlie a copy of 123-456-789

- Attacker compromises any user, then my entire SSN is completely leaked
- Not very good solution

Solution 2

- 3 users: Alice, Bob & Charlie
- Secret message: m = 123-456-789

- Solution 2: I give
  - Alice 123-xxx-xxx
  - Bob xxx-456-xxx
  - Charlie xxx-xxx-789
  - I delete my copy of SSN
- I contact all 3 users, I can recover my SSN

Solution 2

- Solution 2: I give
  - Alice 123-xxx-xxx; Bob xxx-456-xxx; Charlie xxx-xxx-789

- Attacker compromises (at most 2 users)
  - Alice + Bob: 123-456-xxx
  - Alice + Charlie: 123-xxx-789
  - Bob + Charlie: xxx-456-789
- Attacker gets at most 2/3 information, better than S1

Solution 2

- Cincinnati Bell or Duke Energy
  - Custom Service: Please provide last 4 digits of SSN
- Attacker compromises Bob + Charlie
  - Bob + Charlie: xxx-456-789
  - Last 4 digits: 6789
- Custom Service thinks Attacker is me
  - Attacker can change my services

Solution 3

- 3 users: Alice, Bob & Charlie
- Secret message: m = 123-456-789

- Solution 3:
  - I give Alice 1xx-4xx-7xx
  - I give Bob x2x-x5x-x8x
  - I give Charlie xx3-xx6-xx9
  - I delete my copy of SSN
- I contact all 3 users, I can recover my SSN

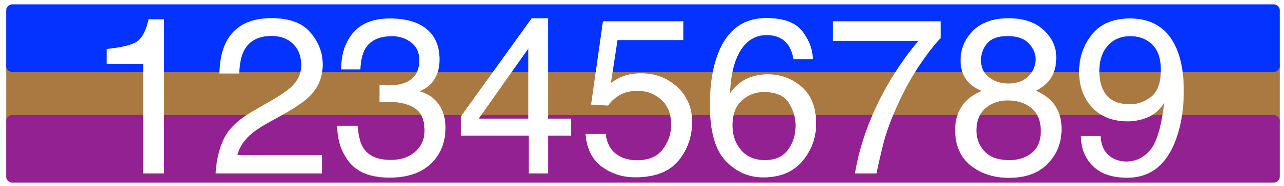
Solution 3

- Solution 3: I give
  - Alice 1xx-4xx-7xx; Bob x2x-x5x-x8x; Charlie xx3-xx6-xx9

- Attacker compromises (at most 2 users)
  - Alice + Bob: 12x-45x-78x
  - Alice + Charlie: 1x3-4x6-7x9
  - Bob + Charlie: x23-x56-x89
- Attacker cannot have last 4 digits, better than S2

Solution 3

- Attacker compromises (at most 2 users)
  - Alice + Bob: 12x-45x-78x
  - Alice + Charlie: 1x3-4x6-7x9
  - Bob + Charlie: x23-x56-x89
- Attacker gets 2/3 information, which makes brute-force much easier
  - Only need to guess another 3 digits.



- <u>Solution 4:</u>
    - Horizontally divide 123 456 789 into 3 pieces
    - Alice blue piece, Bob brown piece, Charlie purple piece
    - I contact all 3 users, can recover my SSN

- Attacker compromises Alice + Bob

- Attacker compromises Bob + Charlie

123456789

- Attacker compromises Alice + Charlie

123456789

- Still easy to recover/guess almost all information
- Any other solutions?

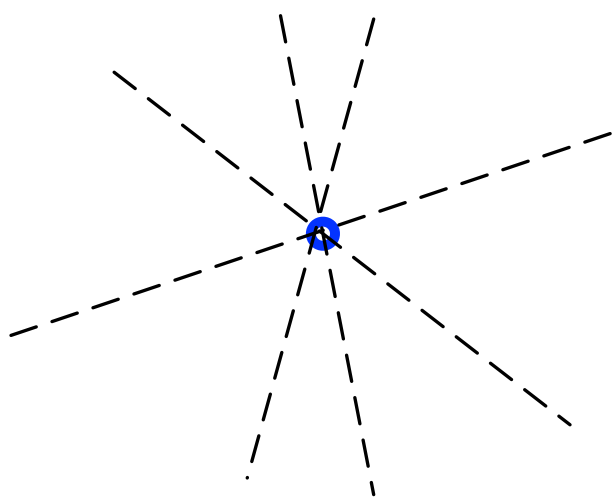
Secret Sharing

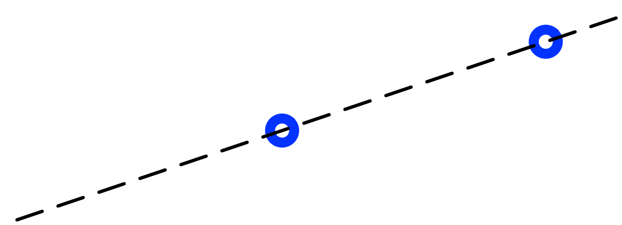
- I divide my SSN into 3 pieces with SS
  - Give Alice 1st piece
  - Give Bob 2nd piece
  - Give Charlie 3rd piece
  - I contact all 3 users, I can recover my SSN

- Attacker compromises any 1 or 2 users
  - 0 information about my SSN
  - Better than all the previous solutions

Shamir Secret Sharing

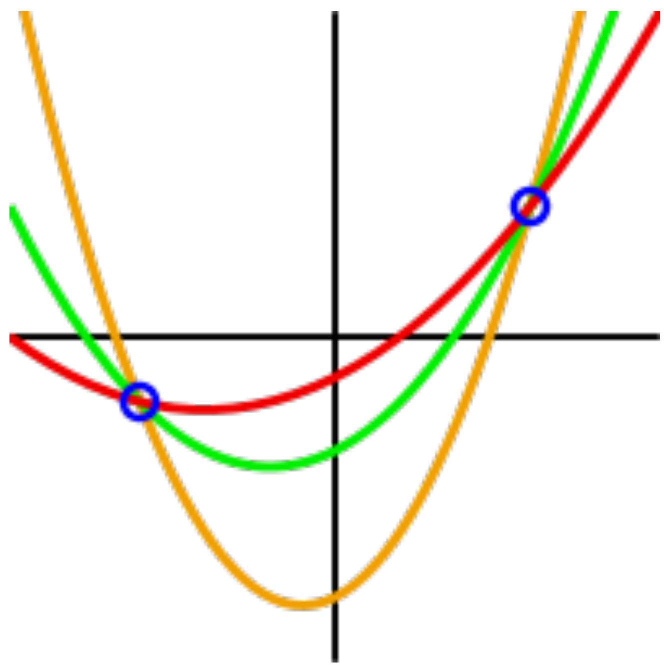
- Basic idea:
  - Given 1 point, infinite number of lines
  - 2 points define a unique line





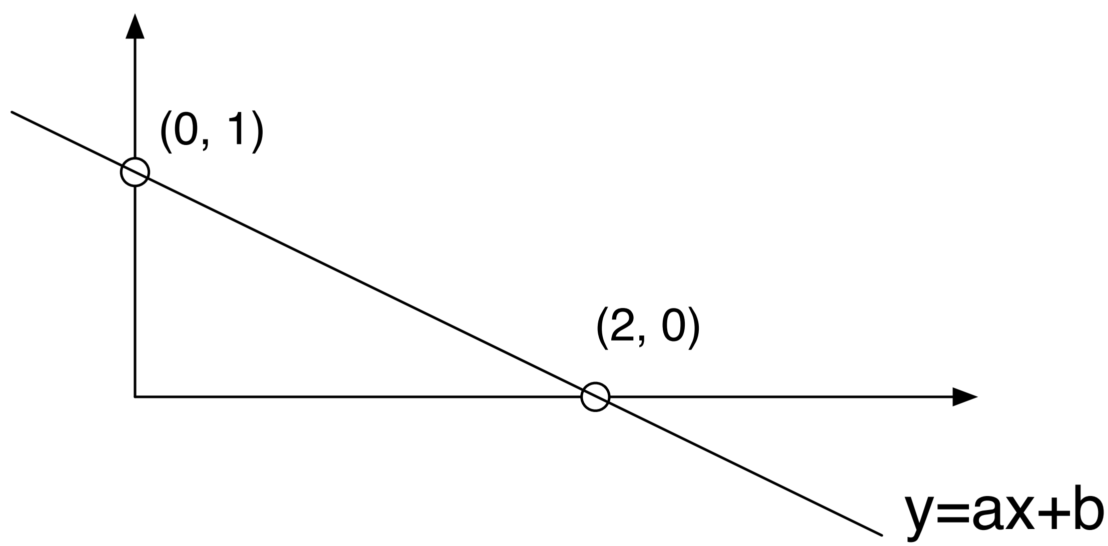
Shamir Secret Sharing

- Basic idea:
  - Given 2 points, infinite number of parabolas
  - 3 points define a unique parabola



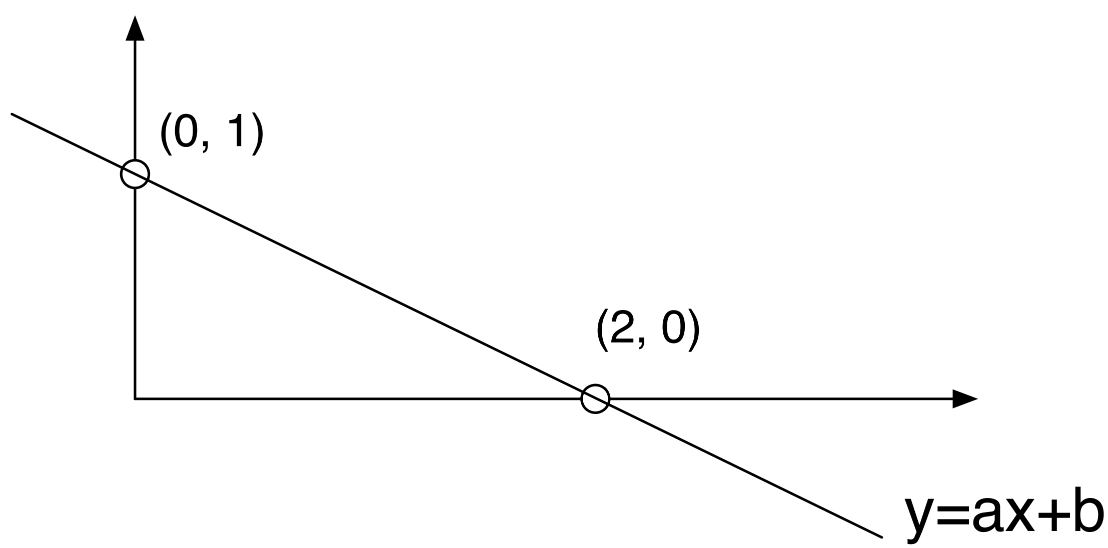
Shamir Secret Sharing

- Basic idea:
  - k points define a unique k-1 degree polynomial
  - E.g., 2 points define a unique 1 degree polynomial
    - y = ax + b



Shamir Secret Sharing

- 1 degree polynomial: $y = ax + b$
- Given 2 points $(x_1,y_1) = (0,1)$, $(x_2,y_2) = (2,0)$
  - $1 = y_1 = ax_1 + b = 0*a + b \longrightarrow b = 1$
  - $0 = y_2 = ax_2 + b = 2*a + 1 \longrightarrow a = -1/2$
- polynomial is $y = -0.5x + 1$



Shamir Secret Sharing

- I set c as a secret message m
- Randomly choose a and b
- Obtain a 2-degree polynomial $y = ax^2 + bx + c$
- Generate 3 random points with $y = ax^2 + bx + c$
- Give 1 point to Alice;1 point to Bob; 1 point to Charlie

- Attacker compromises (at most) 2 users
  - 2 points does not recover the polynomial (i.e., m)
  - Attacker has 0 information about my SSN

Shamir Secret Sharing

- 3 points define a unique 2 degree polynomial
- $y = ax^2 + bx + c$

- I set c as a secret message m
- Randomly choose a and b
- Generate <u>3 random points</u> with $y = ax^2 + bx + c$
- Give 1 point to Alice;1 point to Bob; 1 point to Charlie

- <u>With 3 points, I can recover polynomial, i.e., m</u>

Shamir Secret Sharing

- <u>Example:</u> 2 degree polynomial: $y = ax^2 + bx + c$
- Assume secret is $c = m = 1234$
- I choose $a = 94$ and $b = 166$
- $y = 94x^2 + 166x + 1234$

- I choose $x_1 = 1$, $x_2 = 2$, $x_3 = 3$
  - $y_1 = 94*1 + 166*1 + 1234 = 1494$
  - $y_2 = 94*4 + 166*2 + 1234 = 1942$
  - $y_3 = 94*9 + 166*3 + 1234 = 2578$

Shamir Secret Sharing

- I choose $x_1 = 1$, $x_2 = 2$, $x_3 = 3$
  - y1 = 94*1 + 166*1 + 1234 = 1494
  - y2 = 94*4 + 166*2 + 1234 = 1942
  - y3 = 94*9 + 166*3 + 1234 = 2578
- I obtain 3 points $(x_1, y_1) = (1, 1494)$, $(x_2, y_2) = (2, 1942)$, $(x_3, y_3) = (3, 2578)$

- I give Alice (x_1, y_1), Bob (x_2, y_2), Charlie (x_3, y_3)
- I delete polynomial $y = 94x^2 + 166x + 1234$

Shamir Secret Sharing

- Alice has $(x_1, y_1) = (1, 1494)$
- Bob has $(x_2, y_2) = (2, 1942)$
- Charlie has $(x_3, y_3) = (3, 2578)$

- Attacker compromises Alice + Bob
  - $(x_1, y_1) + (x_2, y_2)$ cannot recover polynomial

- Attacker compromises Alice + Charlie
  - $(x_1, y_1) + (x_3, y_3)$ cannot recover polynomial

Shamir Secret Sharing

- Alice has $(x_1, y_1) = (1, 1494)$
- Bob has $(x_2, y_2) = (2, 1942)$
- Charlie has $(x_3, y_3) = (3, 2578)$

- Attacker compromises Bob + Charlie
  - $(x_2, y_2) + (x_3, y_3)$ cannot recover polynomial
- Attacker has 0 info about my secret
- I get the 3 points, can recover my secret (with some computation)

Shamir Secret Sharing

- Practice: 2 degree polynomial: $y = ax^2 + bx + c$
- Assume secret is $c = m = 1234$
- I choose $a = 94$ and $b = 166$
- $y = 94x^2 + 166x + 1234$

- I choose $x_1 = 4$, $x_2 = 5$, $x_3 = 6$
  - $y_1 = ??$
  - $y_2 = ??$
  - $y_3 = ??$

Shamir Secret Sharing

- Practice: 2 degree polynomial: $y = ax^2 + bx + c$
- Assume secret is $c = m = 1234$
- I choose $a = 94$ and $b = 166$
- $y = 94x^2 + 166x + 1234$

- I choose $x_1 = 4$, $x_2 = 5$, $x_3 = 6$
  - $y_1 = 94*16 + 166*4 + 1234 = 3402$
  - $y_2 = 94*25 + 166*5 + 1234 = 4414$
  - $y_3 = 94*36 + 166*6 + 1234 = 5614$

Shamir Secret Sharing

- <u>Practice:</u> 2 degree polynomial: $y = ax^2 + bx + c$
- Assume secret is $c = m = 1234$
- I choose $a = 94$ and $b = 166$
- $y = 94x^2 + 166x + 1234$

- Can I choose $\mathbf{x_1 = 0}$ and give Alice (x_1, y_1)?

Shamir Secret Sharing

- Practice: 2 degree polynomial: $y = ax^2 + bx + c$
- Assume secret is $c = m = 1234$
- I choose $a = 94$ and $b = 166$
- $y = 94x^2 + 166x + 1234$

- Can I choose $\mathbf{x_1 = 0}$?
  - $y_1 = 94*0 + 166*0 + 1234 = 1234 = c = m$
  - I give Alice (x_1, y_1)
  - Attacker compromises Alice, learns secret m

Problem Setting Changed

- There is a secret message m, and we have **2** users, Alice and Bob
  - E.g. m = 123-456-789 (my SSN)

- I want to share message m with the **2** users.
- I recover secret m by contacting the **2** users
- Attacker can compromise at most **1** user

Problem Setting Changed

- I want to share secret m with the **2** users.
- I recover secret m by contacting the **2** users
- Attacker can compromise at <u>most **1** user</u>

- <u>Example:</u> which polynomial should I use?
  - 1 degree: $y = ax + b$
  - 2 degree: $y = ax^2 + bx + c$
  - 3 degree: $y = ax^3 + bx^2 + cx + d$

Shamir Secret Sharing

- I want to share secret m with the **2** users.
- I recover secret m by contacting the **2** users
- Attacker can compromise at <u>most **1** user</u>

- I need to 2 points to recover secret m
- 2 points define a unique 1 degree polynomial
- So I choose 1 degree: $y = ax + b$
- With 1 point, attacker cannot recover the polynomial

Shamir Secret Sharing

- <u>Practice:</u> 1 degree polynomial: $y = ax + b$
- Assume secret is $b = m = 1234$
- I choose $a = 41$
- $y = 41x + 1234$

- I choose $x_1 = 1$, $x_2 = 2$
  - $y_1 = ??$
  - $y_2 = ??$

Shamir Secret Sharing

- Practice: 1 degree polynomial: $y = ax + b$
- Assume secret is $b = m = 1234$
- I choose $a = 41$
- $y = 41x + 1234$

- I choose $x_1 = 1$, $x_2 = 2$
  - $y_1 = 41*1 + 1234 = 1275$
  - $y_2 = 41*2 + 1234 = 1316$
- I give Alice (x_1, y_1) and give Bob (x_2, y_2)

Problem Setting Changed

- There is a secret message m, and we have **7** users, Alex, Matt, Kurt, Kyle, Ryan, Dan and Will
  - E.g. m = 123-456-789 (my SSN)

- I want to share message m with the **7** users.
- I recover secret m by contacting the **7** users
- Attacker can compromise at <u>most **6** users</u>

Problem Setting Changed

- I want to share secret m with the **7** users.
- I recover secret m by contacting the **7** users
- Attacker can compromise at most **6** users

- Practice: which polynomial should I use?
  - 5 degree: $y = ax^5 + bx^4 + cx^3 + dx^2 + ex + f$
  - 6 degree: $y = ax^6 + bx^5 + cx^4 + dx^3 + ex^2 + fx + g$
  - 7 degree: $y = ax^7 + bx^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h$

Shamir Secret Sharing

- I want to share message m with **7** users.
- I recover secret m by contacting any **7** users
- Attacker can compromise at most **6** users

- I need to 7 points to recover secret m
- 7 points define a unique 6 degree polynomial
- So I choose 6 degree polynomial
- With 6 points, attacker cannot recover the polynomial

Problem Setting Changed

- There is a secret message m, and we have **7** users: Alex, Matt, Kurt, Kyle, Ryan, Dan and Will
  - E.g. m = 123-456-789 (my SSN)

- I want to share message m with **7** users.
- I recover secret m by contacting any **4** users
  - E.g. Alex, Matt, Kurt and Will
  - E.g. Kurt, Kyle, Ryan and Dan
- Attacker can compromise at most **3** users

Problem Setting Changed

- I want to share message m with **7** users.
- I recover secret m by contacting any **4** users
- Attacker can compromise at <u>most **3** users</u>

- <u>Practice:</u> which polynomial should I use?
  - 3 degree: $y = ax^3 + bx^2 + cx + d$
  - 4 degree: $y = ax^4 + bx^3 + cx^2 + dx + e$
  - 6 degree: $y = ax^6 + bx^5 + cx^4 + dx^3 + ex^2 + fx + g$

Shamir Secret Sharing

- I want to share message m with **7** users.
- I recover secret m by contacting any **4** users
- Attacker can compromise at <u>most **3** user</u>

- I need to 4 points to recover secret m
- 4 points define a unique 3 degree polynomial
- So I choose 3 degree: $y = ax^3 + bx^2 + cx + d$
- With 3 points, attacker cannot recover the polynomial