The following describes the problem we call Dangerous Secrets (DS). We have two storage nodes in our network, one in Paris and one in New York. We have a set of information secrets \( S = \{s_1, \cdots, s_n\} \) and a collection \( F = \{f_1, \cdots, f_m\} \) of dangerous subsets of \( S \). That is, each \( f_j \) is a subset of \( S \), and the \( f_j \) need not be disjoint. Our problem is to partition the information secrets \( S \) between the Paris node and the New York node. In particular, each information piece \( s_i \) in \( S \) is to be stored at exactly one of the two locations. The constraint is that, for security and privacy reasons, no dangerous subset \( f_j \) may reside in its entirety at either of the nodes. That is, the partition of \( S \) must be such that, for each \( f_j \), the partition specifies that at least one member of \( f_j \) is to be stored in Paris, and that at least one member of \( f_j \) is to be stored in New York.

**Problem:** Given an instance of DS defined by sets \( S \) and \( F \), determine if there exists a partition of \( S \) between Paris and New York that obeys the constraint with respect to the subsets \( f_j \in F \)?

Prove that DS is NP-complete.

**Hint:** Consider first establishing as a lemma the NP-completeness of the problem described in Sipser, Problem 7.24. Establishing this lemma, of course, would require a formal proof.

**ANSWER:**

First, NAE-3SAT is NPC. Clearly in NP, guess a solution and verify in poly time.

Transform 3SAT to NAE as suggested.

Let \( A \) be any assignment satisfying given instance \( I \) of SAT. Extend \( A \) as follows to assignment \( A' \) for instance \( I' \) of NAE. \( A' \) assigns the single new variable \( b=F \). Now consider the clause \( c_j = \{z_1, z_2, z_3\} \) of \( I \) and the corresponding clauses \( \{y_1, y_2, z_j\} \) and \( \{z_j', y_3, b\} \) of \( I' \)

\( z_j \) is assigned in \( A' \) based on the assignment in \( A \) of \( y_3 \):

If \( y_3 \) is assigned \( F \) in \( A \), assign \( z_j=F \). This \( A' \) NAE-satisfies these two clauses of \( I' \) because exactly one literal, \( z_j' \), is true in \( \{z_j', y_3, b\} \). Further, since \( A \) satisfies \( c_j \), it assigns at least one of \( y_1 \) and \( y_2 \) T. Since \( z_j=F \) in \( A' \), \( \{y_1, y_2, z_j\} \) has at least one true and one false literal.

If \( y_3 \) is assigned \( T \) in \( A \), consider the assignment of \( y_1 \) and \( y_2 \) in \( A \). If both are false, \( A' \) assigns \( z_j=T \). Then \( \{y_1, y_2, z_j\} \) has exactly one true literal, \( z_j \), and \( \{z_j', y_3, b\} \) has exactly one true literal, \( y_3 \). If exactly one of \( y_1 \) or \( y_2 \) is false, assign \( z_j \) arbitrarily and each of these clauses clearly has at least one true and one false literal. Finally, if \( y_1 \) and \( y_2 \) are both \( T \) in \( A \), assign \( z_j=F \). Then \( \{y_1, y_2, z_j\} \) has the false literal \( z_j \), while \( \{z_j', y_3, b\} \) has the false literal \( b \).

We assign each \( z_j \) in \( I' \) in this manner, and the resulting \( A' \) satisfies \( I' \) in the NAE sense.
does (NOT A'). Clearly this property is true, since if A' sets to T,F any pair of literals appearing in clause ck, (NOT A') sets to F,T these literals, preserving NAE satisfaction of ck.

As a result of the above observation, we may assume that an A' satisfying assignment of I' is such that A' assigns b=F, since if A' assigns b=T, we just consider the NAE satisfying assignment (NOT A') instead. Now claim that for each pair of clauses \{y_1, y_2, z_j\} and \{z_j', y_3, b\} in I' corresponding to clause cj={y_1, y_2, y_3} in instance I of SAT, it must be the case that A' assigns at least one of y_1, y_2, y_3 to T. To see this, suppose A' assigns each of y_1, y_2, y_3 to F. Then, in order for \{y_1, y_2, z_j\} to be satisfied, z_j=T in A'. But then each of z_j', y_3, and b is assigned F by A' and \{z_j', y_3, b\} is not satisfied. Consequently, A' assigns at least one of y_1, y_2, y_3 true, and, consequently, A' restricted to the yi variables of instance I satisfies this instance of 3SAT.

This transformation from 3SAT to NAE-SAT only doubles the number m of clauses and adds only m+1 variables and hence can be constructed in poly time. Hence NAE-SAT is NPC.

Now consider our problem DS. DS is clearly in NP, since we can guess a partition and verify in poly time that the constraint is satisfied. We now show the problem 3NAE reduces to DS.

Let I be an instance of 3NAE defined by variables U and clauses C. Map to instance I' in which the set S of secrets is the set of variables from U, and their complements. That is, if U={x_1,...,x_n} then S={x_1,x_1', ..., x_n, x_n'}. The set F of dangerous secrets consists of the set C of clauses (each of which is a subset of S) plus additional subsets Q={x_i, x_i'} for each xi in U.

Suppose I is a satisfiable instance of NAE. Let A satisfy I in the NAE sense. To obtain a partition of U which satisfies the dangerous secrets constraint, place each xi assigned T by A in Paris, and each xi assigned F by A in NY. Place the complementary xi' in the opposite city. Note then that if xi' is F under A, then xi is T under A and placed in Paris, and hence xi' is placed in NY. Similarly, if xi' is T under A, it is placed in Paris. Consider a dangerous subset fj corresponding to clause cj={y_1,y_2,y_3}. Since A satisfies cj in the NAE sense, at least one of y_1,y_2,y_3 is T and at least one is F. Hence, in I', at least one of these members of fj is placed in Paris, and at least one is placed in NY. Also, clearly, each added dangerous subset {xi,xi'} in Q is split, by the way the partition is defined (xi and xi' are always placed in opposite cities). Hence, the partition thus formed obeys the constraint of DS.

Now suppose I' is an instance of DS which has a partition that obeys the constraint, and let P be one such partition of S. Form an assignment A to the variables of U as follows. If P places xi in Paris, A assigns xi=T, otherwise, U places xi in NY, and A assigns xi=F. Note that we are not free to "assign" the complemented literals values; the value of a negative literal is a consequence of the assignment to the corresponding variable (the positive literal). Hence, the need for the Q subsets. (That is, without Q, a partition would be free to assign xi and xi' to the same city, and we would lose the connection with a valid satisfying assignment.)

Claim this assignment A satisfies in NAE sense instance I. Let cj={y_1,y_2,y_3} be a clause of I. Then fj is a dangerous subset of I' consisting of y_1,y_2,y_3. At least one of y_1,y_2,y_3 is thus placed in Paris, call this secret ya, and at least one of the y_1,y_2,y_3 is placed in NY, call this secret yb. Now, if both ya and yb are positive literals (members of U), then ya is
assigned $T$ and $yb$ is assigned $F$ and $cj$ is satisfied. If $ya$ is positive and $yb$ is negative (the complement of some $zb$ in $U$), note that since $yb$ is placed in $NY$, and since $\{yb, yb'\}$ is a dangerous subset in $I'$ (one of the $Q$ clauses), it must be that $zb$ (which is $yb'$) is placed in Paris. Hence $yb'$ is assigned $T$ by $A$ and $yb$, its complemented literal, evaluates to $F$. Hence, $cj$ is satisfied in the NAE sense. A symmetric argument is used if $ya$ is negative and $yb$ is positive. Finally, if both $ya$ and $yb$ are negative literals, then again, because of the $Q$ clauses, the uncomplemented $za$ must be placed in $NY$ and hence assigned $F$ and the uncomplemented $zb$ must be placed in Paris and hence assigned $T$. Hence, under $A$ we have $ya=T$ and $yb=F$ and again $cj$ is satisfied in the NAE sense.

Since each clause $cj$ is satisfied in the NAE sense by $A$, $I$ is a satisfiable instance of NAE. The transformation doubles the number of variables ($S$ is twice the size of $U$) and adds $n$ $Q$-subsets of cardinality 2 each. Hence, the transformation is performed in polynomial time, establishing that $DS$ is NPC.