Max-weight rooted-subtree problem and computer security

Geir Agnarsson, George Mason University, Fairfax VA – 22030

Abstract

Consider a rooted tree T with $n \in \mathbb{N}$ non-root vertices provided with two functions: $p : V(T) \to \mathbb{Q}$ on the vertices and $c : E(T) \to \mathbb{Q}$ on the edges, and two fixed numbers $B, G \in \mathbb{Q}^+$. We consider the *Game-Over Attack Strategy (GOAS)* of determining whether or not there is a rooted subtree $T' \subseteq T$ such that (i) $p(T') = \sum_{u \in V(T')} p(u) \geq G$ and $c(T') = \sum_{e \in V(T')} c(e) \leq B$. That the general form of this problem is NP-complete, is not the whole story. There are many special cases that can be solved in polynomial time in n, and these cases can be viewed as models for many security protocols in computer networks. The somber conclusion one can draw is that *hacking into a computer system is theoretically easy!* – This is joint work with Ray Greenlaw and Sanpawat Kantrabutra.

Keywords: rooted tree, decision problems, optimization problems, NP-completeness, computer security.