Sniffing out insider threats

February 19 2008

A rapid way to spot insider threats from individuals within an organization such as a multinational company or military installation is reported in the current issue of the *International Journal of Security and Networks*. The technology uses data mining techniques to scour email and build up a picture of social network interactions. The technology could prevent serious security breaches, sabotage, and even terrorist activity.

Gilbert Peterson and colleagues at the Air Force Institute of Technology at Wright Patterson AFB, in Ohio are developing technology that could help any organization sniff out insider threats by analyzing email activity or find individuals among potentially tens of thousands of employees with latent interests in sensitive topics. The same technology might also be used to spot individuals who feel alienated within the organization as well as unraveling any worrying changes in their social network interactions.

Security efforts have tended to focus on outside electronic threats, explain Peterson and colleagues. However, they point out that it is insiders that pose the greatest threat to an organization. Insiders are members of the organization who may have access to sensitive information for legitimate purposes but who could betray that trust for illegitimate reasons.

An aggrieved employee, saboteur, or terrorist infiltrator with access to such information could potentially cause great harm. Spotting the potential for an insider attack quickly without recourse to huge numbers

of investigators is essential to preventing such an occurrence.

Peterson and his colleagues have developed an approach to assist investigators looking for such insider threats based on an extended version of Probabilistic Latent Semantic Indexing (PLSI). This extended technology can discern employees' interests from e-mail and create a social network graph showing their various interactions.

The researchers explain that individuals who have shown an interest in a sensitive topic but who have never communicated to others within the organization on this subject are often the most likely to be an insider threat. The software can reveal those people either with a secret interest in that topic or who may feel alienated from the organization and so communicate their interest in it only to those outside the organization.

Another important signal of alienation or a potential problem is a shift in the connections between an individual and others within the organization. If an individual suddenly stops communicating or socializing with others with whom they have previously had frequent contact, then the technology could alert investigators to such changes.

The research team has tested their approach on the archived body of messages from the liquidated Enron company e-mail system. Their PLSI results unearthed several individuals who represented potential insider threats. However, it should be noted that the individuals under indictment are the bosses of the organization. It was the core of the organization that is responsible for the illegal behavior, says Peterson. The team points out that while internet activity was not available for Enron, it is generally available from the same sources that supply e-mail history logs and so could be used to search more widely for insider threats. He adds that by turning the domain 'on its ear' in effect, the identify of the whistleblower could be revealed.

Source: Inderscience Publishers