


☐

I'm not robot

  
reCAPTCHA

Continue

## Exploratory social network analysis with pajek pdf download

Information about social networks improves how you use the web. By talking about different social networks, you will be able to use the ones that are most suitable for your taste. Social networks cover every topic imaginable. Understanding which social networks are safe and which are not is an important step. Tom's guide is supported by his audience. When you buy through links on our site, we can earn affiliate commissions. Read more See more See more See more See more See more View more Scams from organized crime groups hurts financial institutions the most, the best way to fight a criminal network is to keep it as an organization and analytics software helps institutions do it by providing a glimpse of the big picture, according to Chris Swecker. The former assistant director of the FBI who retired in 2006 after 24 years of service and moved on To become director of corporate security for Bank of America Corp. until 2009, he sat down with ComputerWorld Canada to discuss financial sector fraud and analytics software on a recent visit to SAS Institute Inc. in Toronto. Swecker, currently an independent consultant on corporate financial crime strategies, regulatory compliance and control measures for business and government, considers fraud to be a business in general. I do not want to say that all scams are a network. There are many opportunistic, one-off scam that takes place every day. But those that ache financially the most are network organized groups, he said. Many activities, especially on the Internet, are organized crime, according to Swecker. Have you heard of sensitive credit card information being stolen and sold on the Internet in these deep, dark carding websites... this is a criminal network, he said. These groups have a type of supply chain, he explained. They steal data, sell it to another group, repackage it and sell it to another group that uses it to steal money one way or another from a channel that financial institutions provide as an ATM or ATM, he said. Swecker suggested going after scammers as a broader fraudulent network and working with law enforcement to dig it up. That's where the analytics part comes in - it helps you put some context around the content of your data so you understand your data better, he said. The best way to fight the net, according to Swecker, is to be able to see it. As in good law enforcement, when you're working on an organized crime case, or you're working on al Qaeda or working on a gang or working in La Cosa Nostra, you have to understand who the participants are, he said. Instead of giving them out one-by-one for traffic violations, you can get them as an organization and you'll have them all gone at once and the only way to do that is to have good intelligence, good data and run a really strong analysis against it to see the whole picture, he said. SAS's new Social NetworkIng Analysis (SNA) tool literally does this, according to Wesley Gill, executive head of corporate risk management at SAS Canada. Introduced by SAS earlier this year, SNA software collects data from multiple sources, links individuals who share key information or engage in transactions with each other and then represents associations using a unique network visualization interface. It takes a huge amount of data, executes links and visualizes associations so investigators can see different participants and relationships between them, Gill explained. You literally see the rings show up and where the activity is organized or not, he said. SNA is one of four parts of the SAS fraud framework, which includes business rules, anomaly detection, and predictive models that work together to score and label individuals, accounts, products, and networks. The framework consolidates alerts from multiple systems and provides a corporate view of exposure to fraud and risk. This hybrid approach, according to the SAS, increases fraud detection and reduces the number of false alarms. The framework is targeted at banks, insurance and government. Banks, insurers and the government have vast amounts of data on individuals, Gill pointed out. What SNA does is take all the information that people have provided through the proper course of business, and through analysis and data integration capabilities, data references to see where they are common, he said. An organization can have something as simple as a cell phone number and quickly process it against all other information it has stored on everyone else to see if there is any relationship between the number and past fraudulent activities or activities that have behaved like fraudulent activities, he explained. Swecker refers to SNA as looking for malignant social networks. Criminals commit fraud 24 hours a day, so generally what you find when you build it is a wider network of scams than an organized Russian criminal group, he said. We all have social networks and they are generally benign social networks, but if you lock in someone who is an internet criminal and you have enough data available, you can actually link your social network, he said. SNA also analyzes behavior that suggests fraud that can help with internal fraud cases by detecting actions that are not consistent with appropriate behavior, such as access to databases that should not, coming in after hours, transferring large amounts of data, etc., noted Swecker. Meanwhile, predictive analysis can be used to determine the likelihood that an individual will become a bad customer, and whether an individual is too much risk to even start a business with Gill pointed out. Need amount of data, but the more data you have, the better the results, Gill said. As your data gets richer, your ability to predict becomes better and you get fewer false positives, he said. The idea is that you constantly self-learn as you go, he said. Predictive models are constantly evolving, Gill noted. We actually work with institutions when it comes to monitoring how well modules work so that when the model deteriorates over time, they can go back and be re-cast or re-tuned to the current behavior that's going on, he said. If you can predict, you can prevent it, Swecker said. Being predictive goes hand in hand with being preventive, he stressed. Everyone wants to be preventive now, and when they are successful, you won't hear anything about it. It's a bad thing that didn't happen, he said. Analytics have a big role to play in fighting crime, according to Gill, who suggested the SNA is ahead when it comes to technology. But that must continue to evolve, he added. Social networks are here today. It's a head start. But we don't want to stagnate with that, he said. The second thing to keep in mind is that the whole area of crime continues to evolve... those who try to protect themselves from it will have to move as fast as the criminal side because they are sophisticated, said Gill. Cybercrime is traditionally under-reported, under-prosecuted and under-investigated in all sectors, according to Swecker. Historically, it's hard to prosecute. No one likes to put their vulnerabilities out there for the public to see, he said. In the U.S., if a sensitive portion of customer data is compromised, it becomes a privacy event and must be reported, he explained. But if an institution is not required to report a breach, they will generally only fix the problem, he said. There is legislation that requires activity above a certain dollar level to be notified to the federal government, and also legislation requiring reporting suspicious activity that does not raise the threshold, Noted Gill. Institutions very quickly inform customers because they know it is in their best interest because if they get a bad reputation or they haven't done that, they're going to lose their business, he said. Swecker gives financial institutions an A when it comes to cybersecurity in general. Many institutions have really good firewalls and great protection, and it has become very difficult to physically hack without the help of an insider, he said. But more can always be done to protect institutions from insider activities such as data theft, he noted. Data is more valuable than money. It's money and it's more damaging when you take it and steal it and sell it then if you've just embezzled money directly from the bank, he said. Gill also gives banks an A grade. But while banks may be doing well today, they must continue to invest in they do, he warned. Criminals, on the other hand, are always looking for new ways to come and carry out activities... the whole area continues to evolve, he said. The financial industry is arguably the most critical of critical infrastructure and a target of almost everyone, Swecker stressed. These include organised crime circles, kyberterrorists who are fixed on economic goals, terrorists trying to fund their activities, and hostile foreign governments. One offensive strategy the organization may take, according to Swecker, is to bring some uncertainty to sales of customer data. One of the biggest vulnerabilities cybercriminals have is trust in themselves in their carding sites, he said. Cybercriminals rely on trust, their relationships and the names they use online, Swecker said. If you can undermine that and create uncertainty in your own black markets, I see it as a vulnerability, he said. If you look at an FBI investigation called Dark Market, they actually created the seeds of distrust among several Russian carding websites and at least temporarily knocked the carding site out and took some major players, said Swecker. Financial fraud is the third fastest growing breach category, according to a 2009 joint study on Canadian IT security practices from the Rotman School of Management at the University of Toronto and Telus Corp., which reported an 88 percent increase last year. Many organizations absorb fraud into their operating costs and see it as part of their daily business, but as fraudulent activities grow and costs rise, organizations will have to start focusing more on this area, noted Gill. Follow me on Twitter @jenniferkavur. Copyright © 2009 IDG Communications, Inc. Inc.