PHYS.ORG

Managing the tradeoffs between privacy and performance

June 27 2012, by Kurt Pfitzer

Venkitasubramaniam, shown here at a poster presentation by electrical engineering and computer engineering seniors, seeks in his research to quantify the tradeoffs between utility and privacy in networks.

When you go online to pay a bill or buy an airline ticket, says Parv Venkitasubramaniam, your transaction is subject to inevitable tradeoffs between privacy and utility.

While you expect your personal data to be protected from malicious actors, you also want the speediest possible transmission of data and completion of your transaction.

You can't have both to the extent you might wish, says Venkitasubramaniam, an assistant professor of electrical and computer engineering.

"Our research shows fundamental tradeoffs do exist," he says. "You have to pay in terms of performance for the privacy you desire."

Venkitasubramaniam studies network security in hopes of improving anonymity, which means protecting the identities of communicating parties and the paths along which data flow. He recently received a five-year CAREER Award from the National Science Foundation.

His goal is to gain a quantitative understanding of the tradeoffs between utility and privacy and to write algorithms that let consumers know how much privacy they can expect according to the amount of utility they desire.

"One person's idea of privacy is not the same as another's. We want to design flexible algorithms that accommodate the desires of all classes of consumers—those who want utility and don't care about privacy, those who prefer privacy and aren't too concerned about utility, and everyone in between.

"Our algorithms will tell users what to expect based on their desire for utility or privacy."

When timing is enough

Venkitasubramaniam is particularly interested in protecting network users against adversaries who gain valuable information about users or networks based on the timing of data transmission.

Network security experts seek hacker-proof encryption codes, he says, but adversaries can gain information about users or networks based solely on the timing of data transmission and the size of data packets. Encryption codes, he adds, do not guard against timing-backed information retrieval.

"Adversaries need only detect the frequency and bandwidth of data-packet transmission. Once they have this information, they can launch an attack. They can jam someone, spoof an address or launch denial-of-service attacks once they know the location of certain servers.

"Previous quantitative models did not consider the complete window of information available to adversaries. We were the first group to do this and the first to compute the fundamental relationship between privacy and utility."

Applications of this work include transportation and healthcare networks, and the energy-distribution network, or "smart grid."

"Each network wants to hide information but does so in a different way," says Venkitasubramaniam. "A smart grid, for example, inadvertently reveals the timing and pattern of energy requests. Our tools must understand the utility, or energy savings, you can get out of the grid versus the privacy you may have to sacrifice.

"For the grid customer, utility is the ability to cut energy use and costs based on pricing and energy-availability information. You as a customer respond in a certain manner to signals transmitted by the grid. But this reveals your usage patterns.

"The question is whether you can get meaningful utility out of the grid or any other network and still maintain your privacy.

"Our mathematical framework enables us to characterize the fundamental trade-offs between anonymity and network performance and to derive insights into the strategies and likely behavior of network adversaries."

Provided by Lehigh University

Citation: Managing the tradeoffs between privacy and performance (2012, June 27) retrieved 26 April 2024 from https://phys.org/news/2012-06-tradeoffs-privacy.html