'Instant replay' for computer systems shows cyber attack details

October 30 2017

A new cybersecurity system developed by researchers at the Georgia Institute of Technology and known as Refinable Attack INvestigation (RAIN) will provide forensic investigators a detailed record of an intrusion, even if the attackers attempted to cover their tracks. Credit: Georgia Tech

Until now, assessing the extent and impact of network or computer

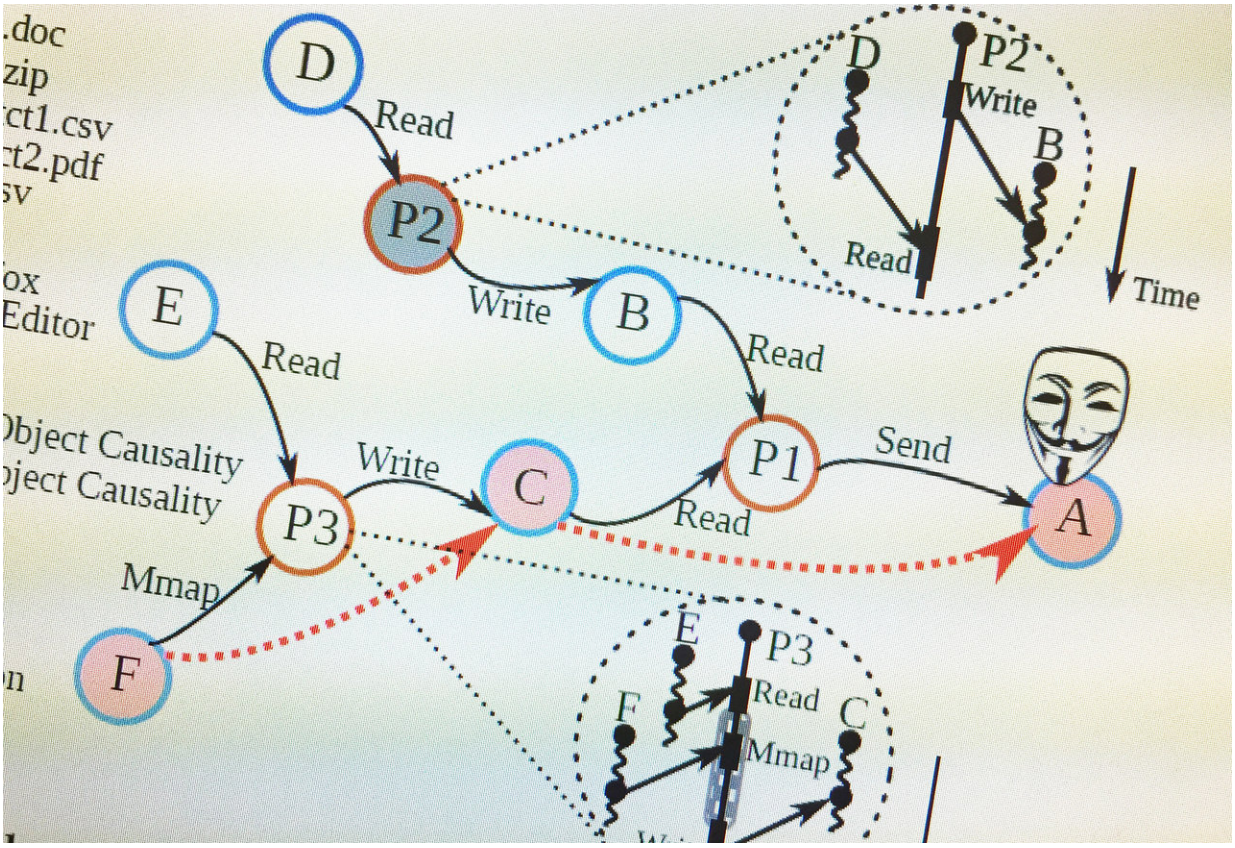
system attacks has been largely a time-consuming manual process. A new software system being developed by cybersecurity researchers at the Georgia Institute of Technology will largely automate that process, allowing investigators to quickly and accurately pinpoint how intruders entered the network, what data they took and which computer systems were compromised.

Known as Refinable Attack INvestigation (RAIN), the system will provide forensic investigators a detailed record of an intrusion, even if the attackers attempted to cover their tracks. The system provides multiple levels of detail, facilitating automated searches through information at a high level to identify the specific events for which more detailed data is reproduced and analyzed.

"You can go back and find out what has gone wrong in your system, not just at the point where you realized that something is wrong, but far enough back to figure out how the attacker got into the system and what has been done," said Wenke Lee, co-director of Georgia Tech's Institute for Information Security & Privacy.

The research, supported largely by the Defense Advanced Research Projects Agency (DARPA) and also by the National Science Foundation and Office of Naval Research, is scheduled to be reported October 31 at the 2017 ACM Conference on Computer and Communications Security (CCS).

Existing forensic techniques can provide detailed information about the current status of computers and networks; from that information, investigators can then attempt to infer how attacks unfolded. Digital logs maintained by the systems provide some information about attacks, but because of concerns about data storage issues, usually don't record enough detail. Other programs provide snapshots in time, but those snapshots may miss important details of an attack.



A new cybersecurity system developed by researchers at the Georgia Institute of Technology and known as Refinable Attack INvestigation (RAIN) will provide forensic investigators a detailed record of an intrusion, even if the attackers attempted to cover their tracks. Image shows a schematic of how the system prunes information about system operation. Credit: Georgia Tech

The RAIN system continuously monitors a system and logs events that it recognizes as potentially interesting. That ability to selectively record information likely to be useful later allows a trade-off between realistic overhead - in terms of system performance and data storage - and useful levels of detail. The system "effectively prunes out unrelated processes and determines attack causality with negligible false positive rates," the

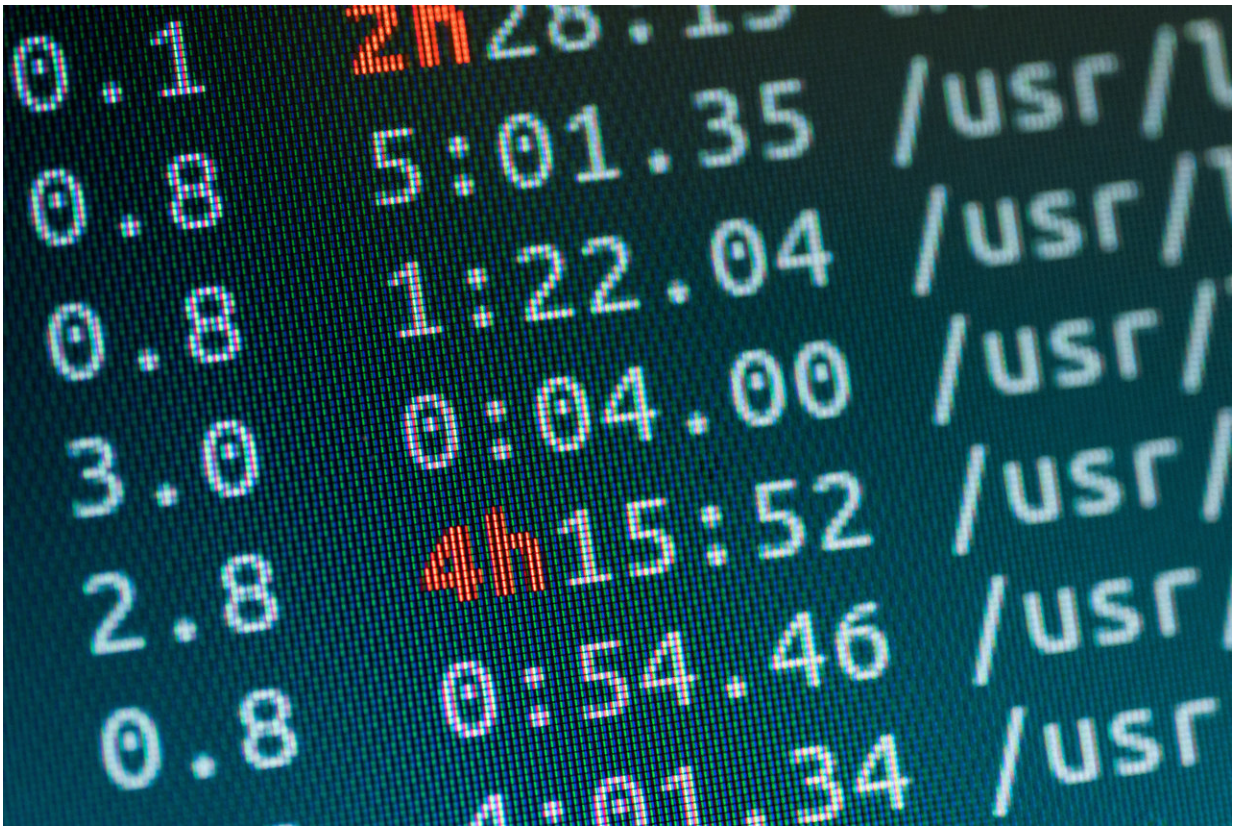
authors wrote in their conference paper.

In addition to its selectivity in recording events, RAIN creates a multi-level review capability that is coarse at first, then more detailed when specific events of interest are identified. Timing of the activities - the inputs, environment and resulting actions - are also synchronized to help investigators understand a complex sequence of activities.

"During the replay of an event, we use binary dynamic instrumentation tools to do the extraction of the appropriate information," said Taesoo Kim, an assistant professor in Georgia Tech's School of Computer Science and one of the paper's co-authors. "We organize information in a hierarchical way, and for each level apply a different type of automated analysis. At the deepest layer, we can tell what happened at the byte level."

The hierarchical approach allows still more flexibility in how the analysis is done after an attack.

"These fine-grained analyses, which can be extremely useful when investigating an attack, would be too expensive to perform on a deployed system; but our hierarchical approach allows us to run these analysis off-line, and only when necessary," said Alessandro Orso, associate chair of Georgia Tech's School of Computer Science and another co-author.



A new cybersecurity system developed by researchers at the Georgia Institute of Technology and known as Refinable Attack INvestigation (RAIN) will provide forensic investigators a detailed record of an intrusion, even if the attackers attempted to cover their tracks. Credit: Georgia Tech

Even with RAIN's selectivity, storing the relevant information requires significant capacity, but the advent of inexpensive storage makes that practical, said Kim. For instance, an average desktop computer might generate four gigabytes of system data per day, less than two terabytes per year. That amount of storage can now be purchased for as little as $50 per year.

"I think we are getting into an affordable range of storage cost," Kim said.

Assessing the damage done by intruders now often takes weeks or months. Beyond accelerating that process, RAIN could help the operators of high-value military or commercial computer networks continually improve their security by providing a level of visibility that is impossible today, Lee said.

"When this is deployed, organizations can have complete transparency, or visibility, about what went wrong," he explained. "The operators of any network housing important data would want to have something like this to replace a manual process with a much more precise and automated technique."

The research team is in the third year of a four-year project funded by DARPA. Additional improvements are being made to the system with a goal of transitioning it to industry.

"This would likely become an independent system that does the logging and interface for other security systems to understand what has happened," Lee explained. "This could be the first product that actually logs the necessary information to reconstruct, or replay, and analyze events that have happened on a computer system, for the first time enabling automated forensics."

Provided by Georgia Institute of Technology