LSU Researchers Use AI to Track Cybercrime in Louisiana and Beyond

LSU MEDIA CENTER

LSU cybersecurity researchers are developing a new tool, called HookTracer, to speed up cybercrime investigations using AI.

With increased and more sophisticated computer capabilities always come new ways for hackers to hide, spy, steal and sabotage. As technology evolves quickly, it's difficult for "good guys" to stay ahead of—or even become aware of—cyberattacks. This is why LSU cybersecurity experts are developing a new tool, called HookTracer, using artificial intelligence, or AI, to reveal cybercriminals and cybercrime both known and unknown.

HookTracer can be used by investigators, such as Louisiana State Police's Cybercrime Unit, to stop—or at least understand and mitigate—cyberattacks. Whether it's attempts to disrupt critical energy infrastructure or hold schools and businesses for ransom, Louisiana ranks high on the list of U.S. states most at-risk of cybercrime—in fact, the highest among all Southern states, besides Florida.

> **"Cybercrime is flourishing among Louisiana-based networks...Our state's heavy saturation of the nation's most critical infrastructure makes it an enticing target for cybercriminals. Investigating these crimes is a labor-intensive effort, even for the most highly trained analysts. That's why Louisiana State Police always is looking for new tools and methodologies, such as those developed by LSU, to make the process more efficient."**
>
> ***Devin King,*** *Louisiana State Police cybercrime analyst*

Devin King, cybercrime analyst with Louisiana State Police, says cybercrime is flourishing among Louisiana-based networks and that he's always looking for new tools, such as LSU's HookTracer.

Cyberattacks can take many forms on a vast variety of software and hardware, but often, hackers insert code that in some way changes normal operations in a computer's operating system. For example, malware, or malicious software, can monitor webcams and microphones, copy data saved to the clipboard, or snoop on whatever is typed on a keyboard—while sneakily covering its own tracks. Both good and bad software can do this, making the detection of malware extra difficult.

HookTracer's focus is on a particular kind of behind-the-scenes malware technique, called application programming interface, or API, hooks. These are used by good and bad programs alike to tell operating systems what to do, so they can work effectively and be nimble and responsive.

While a user interface connects a computer to a person, APIs connect computers or pieces of software to each other, so they can work better together. Their very purpose is to hide the internal details of how a system works, exposing only those parts a regular user would care about.

Most of the time, if a computer program seems intuitive and easy to use, it's because considerable complexity was engineered to become invisible to the user. This convenient obfuscation, however, offers ample opportunities for hackers. As new versions of software and hardware emerge, cybercrime investigators are faced with constantly moving targets.

"Previous research in memory forensics we've done at LSU has addressed the problem of detecting the presence of API hooks, but a related issue is that we've been using heuristics—rules of thumb—to differentiate between benign and malicious hooks," said Professor Golden G. Richard III, who is the director of the LSU Applied Cybersecurity Lab. "When malware changes behavior, this can result in malicious hooks being marked as benign and therefore not examined by an investigator."

Malware is an umbrella term for viruses, worms, ransomware and spyware—but not bugs, as the harm they cause is unintentional. To address the amount of complexity and sometimes subtle variations between hardware, software and malware combinations, the LSU cybersecurity researchers behind HookTracer are using AI to help investigators identify cyberattacks that might not be an exact match with other and previously known attacks, yet similar in significant ways—perhaps by accessing a certain location in the computer's

memory or following a specific sequence of steps. AI is exceptionally good at discovering “close enough” patterns in vast amounts of data, just as deep learning for facial recognition can learn to recognize a person both with and without glasses.

“For cyber-intrusion investigations, Louisiana State Police routinely collects evidence from a multitude of hosts running in victim networks,” King said. “Sifting through that data and finding ‘bad’ is one of the most critical steps. A large part of our investigative effort is spent going down rabbit holes to rule out false positives and negatives to ensure ‘bad’ is actually what was found. The ability to quickly make that determination is key.”

The LSU researchers are working to make HookTracer both flexible and explainable—both important features in memory forensics and data security with legal implications. A common problem with AI is that the outcome, a decision or answer, often is provided without any of the underlying reasons for why a certain decision was made, or a specific answer reached. Coherent explanations, however, are critical for investigators who need to validate their investigative process and potentially use their findings as evidence in legal proceedings. HookTracer’s multi-level attention network, a desirable feature of AI developed by the LSU team, makes it possible for the tool to shift its focus based on what it’s learning in relationship to previous experience and then communicate its revised priorities to investigators.

LSU Associate Professor Mingxuan Sun leads the development of the AI and machine learning components of HookTracer. She works to make the technology more robust, yet transparent and explainable, which is important when the goal is to gather evidence of cybercrime.

– Photo: LSU

“A deep neural network is infamous for its complexity and can be very hard to explain, so we must work on different strategies to make sure we have a better understanding of not only the AI’s decisions, but also why those decisions were made,” said Mingxuan Sun, associate professor in the LSU Division of Computer Science and Engineering and lead developer of the AI components of HookTracer. “If we get a music or movie recommendation based on an AI algorithm, we may just try it, even if we don’t know why it was recommended to us, since the cost in clicks, time or dollars is low. But when lives and livelihoods are on the line, as they are in security as well as medical applications, we need more power of explanation.”

LSU’s cybersecurity team will use something called “adversarial training” to make HookTracer’s AI more robust and less gullible, just like putting on makeup shouldn’t throw off facial recognition or a sticker on a stop sign shouldn’t land a self-driving car in a ditch. By intentionally trying to trick the AI with lookalikes and manipulated data, the AI can learn to see through them. Not only will this adversarial learning make HookTracer less likely to allow malware to evade detection, it will also make the tool more adaptable and useful across platforms and data types.

From the start, HookTracer was built to integrate with the open-source Volatility memory analysis framework, one of the premier memory forensics platforms in the world. This is because Andrew Case, a core developer of Volatility, has been part of the LSU Applied Cybersecurity Lab since 2017, providing students with a direct connection to industry.

“HookTracer’s greatest strength is that it uses malware’s code against itself by emulating the instructions in a sandboxed environment,” Case said. “This allows the decisions made by HookTracer to be driven directly by the activity of malicious code. Few other projects in the field allow for such power in a scalable way, and it gives our students the ability to quickly develop new malware detection capabilities that can be immediately applied in the field.”

Case and Richard recently presented a research paper at BlackHat, the premier cybersecurity conference in the world, held in Las Vegas last month. Like HookTracer, the paper offers new ways to fight malware that leverages API hooks. Titled “New Memory Forensics Techniques to Defeat Device Monitoring Malware,” it covers all three major operating systems: Linux, Mac and Windows.

Professor Golden G. Richard III (left) is faculty lead on the LSU cybersecurity initiative, director of the LSU Applied Cybersecurity Lab, and member of the HookTracer development team. He was recently interviewed by LSU President William F. Tate IV (right) for his On Par with the President podcast.

– Photo: LSU

As cybersecurity defenders and computer security services companies have become wiser to weaknesses in the kernel of computers, adding new patches and safeguards, more and more malware attacks are now happening in what computer programmers call "userland," programs and apps that interact with the kernel and normally have fewer privileges—unless those privileges are somehow escalated, which is a key objective of malware.

You can think of it like a restaurant, where userland is the dining room. In a normal scenario, guests, or computer users, can place orders with waiters, or applications, who deliver food, but neither the guests nor the waiters can go into the kitchen, or the kernel, themselves to cook. Once it was discovered that a guest had somehow bribed a sous-chef in the kitchen to send all the expensive butter out the back door and replace it with margarine, the restaurant owners, or Linux, Mac and Windows, installed cameras in the kitchen, making it harder to bribe and otherwise manipulate the kitchen staff. A bad guest, however, can still order 99 chocolate souffles at once, overloading the kitchen, which would be called a denial of service, or DOS, attack, bribe a waiter or take advantage of an unsuspecting waiter by changing their nametag and hypnotizing them to access the walk-in-fridge.

Uncovering exactly what happened to the "butter" in the world of cybersecurity is known as memory forensics. Case and Richard are among the top memory forensics researchers in the world and developed HookTracer specifically to help with incident response, which involves explaining how a computer crime took place and gathering evidence.

The U.S. Cybersecurity and Infrastructure Security Agency, or CISA, recently reemphasized the importance of memory forensics in investigations of cybersecurity incidents and vulnerabilities, further increasing national demand for memory forensics expertise.

"Memory forensics wasn't widely adopted when we first started working on problems in memory forensics around 2006, but a lot of people are realizing that it's incredibly important," Richard said. "Today, we see lots of malware you simply cannot find using traditional forensics techniques, such as examining copies of hard disks. HookTracer eliminates more of the gaps where malware can hide."

Richard's team has been collaborating with Louisiana State Police as part of the LSU FIREStarter and more recently LSU FIREStarter 2 initiatives, which give students hands-on training in incident response, an ongoing effort funded by the Louisiana Board of Regents and with real-time threat data provided by Louisiana State Police. Students also gain experience with the latest memory forensics tools, such as HookTracer.

"The capability to perform memory and volatile data analysis is the backbone of any cybercrime investigative unit," King said. "It's the 'DNA analysis' of the cyber world."

Read more:

"Spyware Hunters Are Expanding Their Toolset" (WIRED)

"LSU Announces Strategy and Commitment to Become Leader in Cybersecurity, Military Studies" (LSU)

From Hacker to Cyber Defender with LSU's Dr. Golden Richard III (LSU, On Par with the President)

Cybersecurity at LSU

Publish Date:
9-20-2022

Center for Computation & Technology
2003 Digital Media Center • Telephone: +1 225/578-5890 • Fax: +1 225/578-8957