Автор: Пепел © Babr24.com НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МОЛОДЕЖЬ, ТОМСК 24652
28.09.2021, 23:12 1158

Исследования ученого ТГУ помогут отражать хакерские атаки

Молодой ученый Института прикладной математики и компьютерных наук ТГУ Антон Николаев исследует атаки на системы, созданные на основе машинного обучения, и механизмы их предотвращения. Результаты его работы должны стать основой для создания новых подходов защиты нейронных сетей от хакерских нападений.

Машинное обучение учит компьютер самостоятельно находить решения различных задач с помощью заранее загруженных данных и специальных алгоритмов. Сейчас его методы все активнее используются в самых разных областях человеческой деятельности.

> «Те или иные методы и алгоритмы, работающие в данных областях, подвержены всевозможным атакам. Сложность (как для атакующего, так и для защищающего) заключается в том, что обозначенные системы крайне сложны в своем устройстве, и защита, как и нападение, требуют сложного многоуровневого подхода на всех этапах взаимодействия системы с пользователем», - говорит аспирант ИПМКН ТГУ Антон Николаев.

Успешная атака на систему, работающую на базе машинного обучения и различных обучающихся алгоритмов, может привести к критичным последствиям разной степени опасности. Так, например, внедрение в биометрические коды может открыть доступ к секретным данным или даже финансовым счетам в онлайн-банках, а взлом систем автономного вождения и вовсе привести к возникновению реальной угрозы человеческой жизни.

Механизмы атак могут быть самыми разными.

> «Самые популярные включают генерацию некоторых небольших изменений в объекте (звуке, изображении, тексте) или, проще говоря, специального «шума», который ведет к тому, что система неправильно распознает или классифицирует данный объект, – объясняет Антон Николаев. – Например, определенного рода наклейка на дорожный знак может заставить систему распознавания дорожных знаков увидеть вместо одного знака другой. Или же специальный макияж на лице может заставить систему распознавания лиц увидеть в одном человеке другого».

Замещать одни результаты другими злоумышленникам удается из-за «зазоров», появление которых не исключено в процессе машинного обучения. Задача аспиранта ИПМКН ТГУ – выявить наиболее эффективные методы приближения к границам таких «зазоров» или пограничных значений. Это позволить понять, каким образом можно снизить число подобных «слабых звеньев» при атаках и в эксплуатации. На основе итогов исследований молодой ученый создаст новые алгоритмы для защиты методов машинного обучения от внешнего влияния.

Автор: Пепел © Babr24.com НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МОЛОДЕЖЬ, ТОМСК 24652
28.09.2021, 23:12 1158
URL: https://babr24.com/?ADE=219436 Bytes: 2570 / 2440 Версия для печати Скачать PDF

Автор текста: **Пепел**.

эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта