אתגרי האבטחה של טכנולוגיות זיהוי פנים

למרות שפתרונות לזיהוי ביומטרי עשויים להפחית מגע פיזי ולהפחית הדבקה, עניין חיוני בימי קורונה אלה, הם גם עלולים לגרור "תופעת לוואי" כמו הגדלת הסיכון למתקפת סייבר. ממה צריך להיזהר ומה נדרש לעשות?

סטיב פובולני

ישנם 7.6 מיליארד אנשים החיים בעולם, וזהו רק מספר האנשים החיים בו כיום. גם אם נשווה בין כל האנשים שחיו לאורך ההיסטוריה, לעולם לא יימצאו שני פרצופים זהים לחלוטין. מסתבר, שיש כל כך הרבה פרטים בפנים האנושיות, הרבה יותר מכפי שאנו יכולים להבחין, כמו למשל גודל המצח, צורת הלסת, מיקום האוזניים, מבנה האף ועוד אלפי פרטים זעירים במיוחד.

אפשר להטיל ספק בחשיבות פרט זה בכל הנוגע למחקר על חולשות אבטחה וסיכוני סייבר, אולם צוות מחקר האיומים המתקדמים של חברת מקאפי (McAfee Advanced Threat Research, או בקיצור ATR) בדק סוגייה זו בהקשר של מדע נתונים ואבטחה והגיע לתוצאות מעניינות. באופן ספציפי, הצוות בדק אם מערכות ממוחשבות לזיהוי פנים רגישות לטעויות פחות או יותר מאיתנו, כבני אדם.

התבוננו היטב בארבע התמונות שלהלן. האם תצליחו לזהות מי מבניהן מזויפת ומי אמיתית?

נסו לנחש - האם אלה פנים אמיתיות? | צילום: McAfee

התשובה עשויה להפתיע, מאחר וכל ארבע התמונות מזויפות לחלוטין. הן נוצרו ב–100% על–ידי מחשבים ולא מצירוף חלקים של אנשים שונים שהורכבו יחד ביצירתיות. מערכת המכונה StyleGAN ייצרה כל אחד מהפרצופים אלה ועוד מיליונים נוספים, מאפס, בדרגות שונות של פוטו–ריאליזם.

מגבלות אבטחה

הטכנולוגיה המרשימה הזו משקפת מהפכה במדע הנתונים, טכנולוגיה מתפתחת שיכולה לבצע חישובים מהר יותר, בקנה מידה שמעולם לא היינו חשופים אליו. הדבר מאפשר חדשנות מרשימה ביצירה או זיהוי תמונות במהירות, אפילו בזמן אמת. חלק מהיישומים המעשיים של הטכנולוגיה הם בתחום של זיהוי פנים. במילים פשוטות, מדובר ביכולת של מערכת מחשב לקבוע אם שתי תמונות שונות מייצגות את אותו אדם, או לא. הטכנולוגיה המוכרת ביותר לזיהוי פנים ממוחשב מתוארכת לשנות ה–60' של המאה ה–20, אך עד לאחרונה היא הייתה לא מדויקת או איטית מדי, ולכן לא יעילה.

ההתקדמות הטכנולוגית ופריצות הדרך בבינה מלאכותית ולמידת מכונה איפשרו את פיתוחם של כמה יישומים חדשים לזיהוי פנים. בראש ובראשונה, ניתן להשתמש בהם כמנגנון אימות אמין ודי–התשובה עשויה להפתיע, מאחר וכל ארבע התמונות מזויפות לחלוטין. הן נוצרו ב–100% על–ידי מחשבים ולא מצירוף חלקים של אנשים שונים שהורכבו יחד ביצירתיות. מערכת המכונה StyleGAN ייצרה כל אחד מהפרצופים אלה ועוד מיליונים נוספים, מאפס, בדרגות שונות של פוטו–ריאליזם.

מגבלות אבטחה

הטכנולוגיה המרשימה הזו משקפת מהפכה במדע הנתונים, טכנולוגיה מתפתחת שיכולה לבצע חישובים מהר יותר, בקנה מידה שמעולם לא היינו חשופים אליו. הדבר מאפשר חדשנות מרשימה ביצירה או זיהוי תמונות במהירות, אפילו בזמן אמת. חלק מהיישומים המעשיים של הטכנולוגיה הם בתחום של זיהוי פנים. במילים פשוטות, מדובר ביכולת של מערכת מחשב לקבוע אם שתי תמונות שונות מייצגות את אותו אדם, או לא. הטכנולוגיה המוכרת ביותר לזיהוי פנים ממוחשב מתוארכת לשנות ה–60' של המאה ה–20, אך עד לאחרונה היא הייתה לא מדויקת או איטית מדי, ולכן לא יעילה.

ההתקדמות הטכנולוגית ופריצות הדרך בבינה מלאכותית ולמידת מכונה איפשרו את פיתוחם של כמה יישומים חדשים לזיהוי פנים. בראש ובראשונה, ניתן להשתמש בהם כמנגנון אימות אמין ודי–

סטיב פובולני | צילום: McAfee

גמה מצוינת לכך הוא האייפון. מאז השקת iPhone X בשנת 2017, זיהוי פנים הפך לסטנדרט החדש לאימות משתמש במכשירים ניידים. בעוד שאפל משתמשת בתכונות מתקדמות כמו עומק למיפוי פנים, מכשירים אחרים יישמו שיטות סטנדרטיות יותר המבוססות על תכונות הפנים של היעד עצמו, דברים שאנו כבני אדם רואים גם כן, כגון מיקום העיניים, רוחב האף, ותכונות אחרות שיכולות לזהות במדויק משתמש יחיד. שיטות פשטניות וסטנדרטיות כמו אלו, עלולות לסבול מטבען ממגבלות אבטחה ביחס ליכולות מתקדמות יותר, כגון צילום בתלת–מימד. במובן מסוים זה כל העניין – המורכבות שנוספה בעקבות מידע עומק היא זאת שהופכת התקפות של מניפולציות–פיקסל לבלתי אפשריות.

חששות להטיה גזענית ופגיעה בפרטיות

יישום נוסף של מערכות לזיהוי פנים הוא בתחום של אכיפת החוק. לאחרונה, לאחר שמערכות AI לזיהוי פנים הפגינו הטיה גזענית, חברת IBM הודיעה כי תבטל את תוכניות זיהוי הפנים שלה, כדי שלא ישמשו לאכיפה מוטה–גזענית בידי רשויות אכיפת החוק. בעקבותיה, חברות גדולות נוספות בתחום זיהוי הפנים פעלו באופן דומה. יתכן שהדבר מבוסס, לפחות באופן חלקי, על אירוע שזכה לחשיפה רבה, כאשר בוצע מעצר של אדם שחור על בסיס התאמת זיהוי פנים שגויה. המקרה ידוע כמעצר המוטעה הראשון שנגרם ישירות בגלל טכנולוגיית זיהוי פנים, והנושא נותר שנוי במחלוקת ומהווה גם כיום מקור לחששות הנוגעים לפרטיות. ללא ספק יידרש פיתוח משמעותי נוסף כדי לצמצם חלק מהפגמים הללו.

מערכות לזיהוי פנים נפרסו גם בשדות תעופה רבים, כדי לסייע או להחליף אינטראקציה אנושית בתהליך אימות הדרכון. עקב ההשפעה הגלובלית שהייתה לווירוס הקורונה על הצורך בריחוק חברתי, אנו אף חווים האצה חסרת תקדים ברצון ליישם פתרונות ללא מגע, כגון זיהוי ביומטרי. המגמה נובעת מדאגה לבריאות הציבור, אך כדאית מאוד גם מבחינת הרווחיות של חברות תעבורה ושדות תעופה.

פריצה למודל זיהוי פנים

בעוד שפתרונות לזיהוי ביומטרי עשויים להפחית מגע פיזי ולהפחית הדבקה, הם גם עלולים לגרור "תופעת לוואי" כמו הגדלת הסיכון למתקפת סייבר.

הרעיון של בקרת דרכונים באמצעות זיהוי פנים הוא די פשוט. מצלמה מבצעת צילום וידיאו או סטילס של הפנים שלך, ושירות וריפיקציה (אימות) משווה בינה לבין תמונה אחרת שלך שכבר קיימת במערכת. התצלום ה"חי" מעובד ככל הנראה לפורמט דומה (מבחינת גודל תמונה, סוג הקובץ) לזה של צילום היעד, ואז מתבצעת ההשוואה. אם יש התאמה, בעל הדרכון מאומת, ואם אין התאמה, גורם אנושי יבצע בדיקה מעמיקה יותר של כרטיס העלייה למטוס, תעודת זהות, או תעודות אחרות לבדיקת זהות הנוסע.

כחוקרים של איומי סייבר ושל נקודות חולשה, עלינו להיות מסוגלים לבחון כיצד הדברים עובדים – גם בצורה תקינה וגם כשיש טעות כלשהי במערכת. כאשר בחנו טכנולוגיה הולכת וצומחת זו של זיהוי פנים, ואת ההחלטות הקריטיות מאוד שהיא מסוגלת לקבל, בדקנו אם ניתן למנף פגמים בתשתית המערכתית כדי לעקוף את מערכות זיהוי הפנים. באופן ספציפי יותר, רצינו לדעת אם אנו יכולים ליצור תמונות שיצליחו להערים על המערכת הממוחשבת, ולגרום לה לסווג אותן באופן שגוי כגורם היעד שלנו.

ביומטריה היא טכנולוגיה שמסתמכים עליה יותר ויותר כדי לאמת זהות של אנשים והיא מחליפה ביעילות סיסמאות ושיטות אימות אחרות שעלולות להיות לא מהימנות. עם זאת, המחקר שלנו העלה כי ההסתמכות על מערכות אוטומטיות ולמידת מכונה מבלי להתחשב בפגמי האבטחה הטבועים במכניקה הפנימית והמסתורית של מודלים לזיהוי פנים, עלולה לספק לפושעי סייבר יכולות ייחודיות לעקיפת מערכות קריטיות, כמו למשל מערכות לבדיקת דרכונים בשדות תעופה.

למיטב ידיעתנו, גישתנו למחקר הזה מייצגת יישום ראשון מסוגו של פריצה למודל זיהוי פנים. על–ידי מינוף הכוח של מדעי נתונים ומחקר אבטחה, ניתן לעבוד בשיתוף פעולה הדוק עם ספקים ומיישמים של מערכות קריטיות אלה, כדי לתכנן מערכות אבטחה מהיסוד ולסגור את פערי האבטחה שמחלישים אותן.

אנו קוראים לקהילת האבטחה והסייבר להוציא תקן רשמי, שיוכל לזהות את אמינותן של מערכות למידת מכונה. סטנדרטים כאלה קיימים בענפים רבים של אבטחת מחשבים, כולל הצפנה, פרוטוקולים, תדר רדיו אלחוטי ורבים אחרים. אם נמשיך להעביר משימות קריטיות כמו אימות זהויות לקוסמות שחורות, מוטב שתהיה לנו מסגרת לקביעת גבולות מוסכמים לגבי גמישותן ולגבי ביצועיהן במצבים בעייתיים.

> **"ההסתמכות על מערכות אוטומטיות ולמידת מכונה מבלי להתחשב בפגמי האבטחה הטבועים במכניקה הפנימית והמסתורית של מודלים לזיהוי פנים, עלולה לספק לפושעי סייבר יכולות ייחודיות לעקיפת מערכות קריטיות, כמו למשל מערכות לבדיקת דרכונים בשדות תעופה"**

הכותב היא מנהל צוות מחקר האיומים המתקדמים בחברת מקאפי (McAfee)