УДК 681.3

Лашко Богдан В'ячеславович, студент.
Скриль Максим Васильович, студент.
Поночовний Юрій Леонідович, к.т.н., с.н.с.
Полтавський національний технічний університет імені Юрія Кондратюка

АНАЛІЗ ЗАГРОЗ КІБЕРБЕЗПЕКИ 3D-ПРИНТЕРІВ

***Анотація**. За останні роки технологія 3D-друку набула широкого поширення, а самі принтери стали більш інтелектуальними. Тому вони стають цікавим об'єктом для зловмисників. Атаки зловмисників на 3D-принтери можуть призвести до перехоплення контролю, викрадення особистих даних та інтелектуальної власності й нанести матеріальних збитків.*

***Ключові слова:** 3D-принтер, кібербезпека, кібератака.*

Вступ

3D-принтери тривалий час могли собі дозволити тільки спеціалізовані компанії, які відчували необхідність в швидкому створенні прототипів готових виробів, або випуску малих партій продукції.

В останні роки вартість 3D-принтерів значно знизилася, що привернуло до них увагу звичайних споживачів. Виробники старанно стимулюють цей попит, та додають цим пристроям різні можливості для більш зручного використання. Але зі збільшенням можливостей, пов'язаних із підключенням принтера до мережі Інтернет для віддаленого керування та обміном даними, він може втратити управляння і навіть стати загрозою для користувача.

1 Огляд 3D принтерів

Технологія 3D-друку вже відома довгі роки. Першим пристроєм для створення 3D-прототипів вважається американська SLA (технологія 3D-друку, заснована на отвердінні рідкого матеріалу під дією променя лазера) – установка, яку розробив і запатентував Чарльз Халл у 1986 році [4]. З того часу технологія 3D-друку активно розвивалася, збільшувалася її точність, були створені нові технології 3D-друку, які дозволяють друкувати різноманітними матеріалами. Довгий час 3D-принтери були дорогим задоволенням, але за останні роки ціна на них знизилася і тому вони стали більш доступні.

3D-принтер – це пристрій, що використовує метод пошарового створення фізичного об'єкта за цифровою 3D-моделлю.

Через свою доступність, найбільшої популярності набула технологія з пошаровим наплавленням матеріалу (англ. Fused deposition modeling (FDM)) [3]. Суть її полягає в наступному. У друкуючій голівці матеріал (розплав з пластику, металу, ливарного воску, шоколаду) попередньо розігрівається до температури плавлення і надходить в робочу камеру. Сопло-дозатор випускає розплавлений матеріал у вигляді нитки, яка укладається на робочий стіл. Після цього платформа опускається нижче на товщину одного шару, щоб можна було сформувати наступний шар (рис. 1).

Доступність 3D-друку дозволяє проводити сміливі експерименти та дрібносерійне виробництво в архітектурі, будівництві, медицині, освіті, ювелірній справі, поліграфії, виготовлення рекламної та сувенірної продукції. У багатьох випадках використати 3D-принтер набагато дешевше, ніж використання дорогих форм для лиття або прес-форм, або застосування інструментальних верстатів.

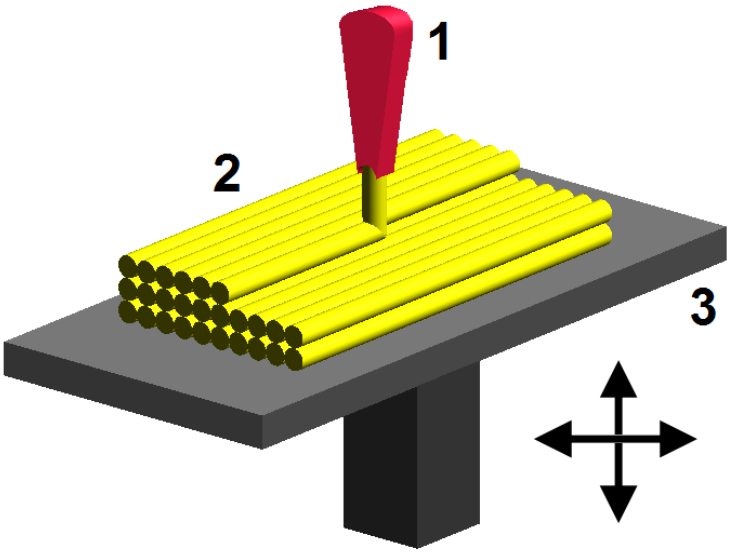

Рис. 1. Процес нанесення шарів розплаву (1 - сопло-дозатор, 2 - розплав, 3 – стіл)

До того ж не обов'язково володіти навичками 3D-моделювання, десятки тисяч 3D-моделей доступні для безкоштовно завантаження в мережі Інтернет.

Можливо, в найближчому майбутньому 3D-принтер стане таким же невід'ємним атрибутом нашого побуту, як холодильник, мікрохвильова піч або телевізор.

3 Актуальність питань кібербезпеки

Проблеми кібербезпеки із розвитком інформаційних технологій є все більш актуальними. Кожен новий гаджет – смартфон, комп’ютер, годинник, 3D-принтер або телевізор підключений до мережі Інтернет несе потенційну небезпеку. Кібербезпека - це процес, а не одноразове рішення. Туму потрібно постійно пам'ятати про інформаційну безпеку.

Кібербезпека – це захист комп'ютерних систем від крадіжки чи пошкодження їх обладнання, програмного забезпечення або інформації, а також від порушення або дезорієнтації послуг, які вони надають [2].

Найбільшими ризиками, які виникають в результаті модернізації техніки, є зберігання особистих даних в мережі [1]. Метою кібербезпеки є досягнення та збереження ресурсів організацій чи користувачів.

Недостатня увага виробників до кібербезпеки своєї продукції на рівні проектування відкриває двері для зловмисників і дає можливість використовувати недоліки в незаконних цілях. Чим далі, тим винахідливішими стають хакери і тим більш руйнівними можуть бути наслідки їхніх дій.

Кіберзлочинність постійно вдосконалюється і йде в ногу з технологіями, що в свою чергу, ускладнює виявлення і протидію протиправних дій. Остання масштабна кібератака відбулася 12 травня 2017 року через вірус WannaCry. Було інфіковано понад 200 тисяч користувачів в 74 країнах світу. Тому для підтримки захисту на високому рівні, потрібно постійно вдосконалювати системи кібербезпеки.

4 Загрози кібербезпеки для 3D принтерів

З кожним роком виробники 3D-принтерів намагаються зробити їх розумнішими для збільшення зручності у використанні. Однак у принад прогресу є і своя зворотна сторона, оскільки з появою нових функцій, таких як віддалене керування принтером та обмін даними з користувачем, 3D-принтер може в руках зловмисника стати загрозою для особистих даних, інтелектуальної та матеріальної власності.

Як і інші пристрої, які взаємодіють із комп’ютером чи смартфоном користувача та мережею 3D-принтер може бути використаний зловмисниками.

При втраті контролю над 3D-принтером можуть виникнути наступні загрози:

- використання пристрою для DoS чи DDoS-атаки;
- псування 3D-принтера;
- псування друкованого виробу;
- стеження за користувачем (за наявності відеокамери);
- викрадення файлів користувача;
- загроза пожежі;
- друк заборонених законом виробів.

Атаки типу «відмова в обслуговуванні», «розподілена відмова в обслуговуванні» (англ. DoS attack, DDoS attack, (Distributed) Denial-of-service attack) – напад на комп'ютерну систему з метою зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

Атака полягає в надсиланні до атакованого комп'ютера, або мережевого устаткування великої кількісті зовнішніх запитів (часто безглуздих або неправильно сформульованих), таким чином атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним. При втраті управління, 3D-принтер може генерувати такі запити за командами зловмисників. Таким чином, атакованим може виявитися як користувач 3D-принтера так і інші користувачі мережі.

Маючи доступ до налаштувань 3D-принтера зловмисник може встановити некоректні значення роботи пристрою, що може призвести принтер до поломки. А якщо зміна налаштувань була зроблена в процесі друку то виріб який друкувався в даний момент буде зіпсований. Це може нанести великих збитків, оскільки деякі матеріали коштують великих грошей, а час друку може досягати десятків годин. До того ж можуть бути внесені зміни які з першого погляду будуть не помітні, але при подальшому використанні виробу можуть призвести до поломки та призвести до більш важких наслідків.

Якщо на 3D-принтер встановлена камера то зловмисник може слідкувати (якщо це дозволяє зона огляду камери) за приміщенням в якому знаходиться камера, або за виробом який друкується.

Для друку виробів на 3D-принтер потрібно завантажити файл, який потрібно роздрукувати. А отже цей файл опиняється під загрозою викрадення.

В деяких технологіях 3D-друку використовуються високі температури, при внесенні змін в процес контролю нагріву та охолодження може виникнути загроза пожежі.

Друкуючи якийсь заборонений виріб, наприклад зброю, злочинець може скомпрометувати користувача.

Таким чином при відсутності захисту при роботі з 3D-принтером і не дотриманні норм безпечного користування пристроєм, користувач може втратити контроль над пристроєм, що в свою чергу загрожує особистим даним, інтелектуальній та матеріальній власності.

5 Висновок

3D-принтери набувають все більшого поширення, особливо в бізнесі, де втрата інтелектуальної власності, або затримка виробництва може коштувати мільйонів доларів. Тому при виборі 3D-принтерів потрібно звертати увагу на їх захищеність від загроз стороннього доступу до пристрою та даних з якими він працює. А при їх використанні дотримуватися правил безпеки: не користуватися пристроєм з незахищеної мережі, встановлення складних паролів для доступу до управління, не встановлювати не перевірене програмне забезпечення на 3D-принтер, комп'ютер чи смартфон.

Посилання

1. *3222.ua - КІБЕРБЕЗПЕКА-ПРОБЛЕМА СТОЛІТТЯ! [Електронний ресурс] – Режим доступу до ресурсу: http://3222.ua/article/kberbezpeka-problema_stolttya.htm.*
2. *en.wikipedia.org - Computer security [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Computer_security.*
3. *uk.wikipedia.org - 3D-принтер [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/3D-принтер.*
4. *3dtoday.ru - Что такое 3D-принтер [Електронний ресурс] – Режим доступу до ресурсу: http://3dtoday.ru/wiki/3Dprinter.*

Authors:
Bogdan Lasho, Skryl Maksym, Ponochovnyi Yuri

Cyber threat analysis for 3D-printer

Abstract. In recent years, 3D-printing technology is widespread, and most printers have become more intelligent. Therefore, they are an interesting target for the attacker. Attacker control over the 3D-printer can lead to identity theft, intellectual property and cause material damage.

Keywords: 3D-printer, cyber security, cyber-attacks.

Авторы:
Лашко Богдан Вячеславович, Скрыль Максим Васильевич, Поночовный Юрий Леонидович

Анализ угроз кибербезопасности 3D-принтеров

Аннотация. За последние годы технология 3D-печати получила широкое распространение, а сами принтеры стали более интеллектуальными. Поэтому они становятся интересным объектом для злоумышленников. Атаки злоумышленников на 3D-принтеры могут привести к перехвату контроля, похищения личных данных и интеллектуальной собственности, нанести материальный ущерб.

Ключевые слова: 3D-принтер, кибербезопасность, кибератака.