filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

La stampante 3D

04 Febbraio 2020
Gabriele Amato, Beatrice Amato, Mauro D'Ercole

Indice:

1. Introduzione

> **La *digital fabrication* sta rivoluzionando la produzione industriale, mettendo in secondo piano la produzione di massa a favore di una produzione più mirata e soprattutto personalizzata.**

Attraverso la ***stampa 3D***, le possibilità di produrre oggetti sta diffondendosi ancora di più arrivando potenzialmente fin dentro le nostre case.
Di seguito proponiamo una riflessione sulle implicazioni nell'uso di questa tecnologia in ambito di protezione e tutela della proprietà intellettuale dei manufatti e prototipi realizzabili.

2. Stampa 3D: misure di sicurezza per la tutela del patrimonio e per evitare le frodi aziendali

In modo del tutto analogo ad una stampante da ufficio, che converte file digitali di elaborazione testo, in pagine stampate, **la stampante 3D legge il file di disegno derivanti da un sistema CAD (computer aided design) creando modelli di prodotti tridimensionali.**
Questi file indicano precisamente alla stampante come applicare in successione i vari strati di materiale (plastiche, polimeri, metalli, etc) in modo da trasformare un disegno in un prodotto tangibile.
Il Software di progettazione crea modelli che sono dettagliati a livello di micron. I progettisti costruendo oggetti con geometrie sempre più complesse, dovranno descriverli digitalmente con un dettaglio sempre più preciso. **Più dettagliato è il modello, e più dati di conseguenza sono necessari**.
Via via che le aziende inizieranno ad impegnarsi in una produzione di tipo additivo, tipico della stampa in 3D, vi saranno conseguentemente sempre più avanzate tecnologie di progettazione, strumenti di calcolo per eseguire simulazioni, per testare e monitorare la qualità e la durata dei prodotti.

L’impatto dovuto all’introduzione della stampa 3D nei processi industriali sarà molto importante. Questa evoluzione produrrà enormi quantità di dati detti “Big Data”, che per poter essere gestiti necessiteranno di opportuni strumenti per il loro supporto.

I Chief Information Officer (CIO), ovvero i manager responsabili della funzione aziendale “tecnologie dell'informazione e della comunicazione”, dovranno effettuare investimenti significativi nei MES (Manufacturing Execution Systems) i sistemi di gestione della funzione produttiva, nella gestione dei loro dati, e delle altre tecnologie necessarie per supportare ambienti di produzione additiva.

In un recente articolo sul Wall Street Journal sono stati espressi i pareri di due esperti, Cotteleer e Brinker, entrambi appartenenti al settore tecnologie digitali di Deloitte.

"*I CIO e i loro team di gestione dati saranno chiamati a gestire insiemi di dati sempre più grandi, che dovranno essere facilmente immagazzinati, reperiti e manipolati*."

> ***"In questo momento, nessuno ingegnerizza un prodotto senza un CAD ed un sistema di controllo di versione. Con la stampa 3D, i sistemi di “versioning” dovranno migliorare, perché la gestione di tutti questi dati diventerà sempre più complessa."***

Oggi vi è una grande fiducia nella funzionalità e durata dei prodotti che correntemente utilizziamo, questo è stato ottenuto tramite gli sforzi degli specialisti che hanno nel tempo dedicato centinaia di anni a studiare le proprietà dei materiali utilizzati e la messa a punto dei processi qualitativi di fusione, colata e fucinatura dei prodotti.

Le aziende impegnate nella produzione additiva dovranno convalidare in modo analogo i loro prodotti. Questo può comportare un uso estensivo di simulazioni per dimostrare che i prodotti fabbricati con i nuovi processi additivi siano sicuri, durevoli e affidabili almeno come quelli creati utilizzando tecniche e materiali più tradizionali.

"*I software di simulazione rendono possibile alle aziende il test di nuovi prodotti in un ambiente computer-generated, sottoponendoli virtualmente, alle sollecitazioni che incontreranno nel mondo reale. Questo processo può aiutare le aziende a capire i punti di forza e di debolezza dei loro progetti, e dei materiali che si utilizzano*."

Poiché la produzione additiva crea tipicamente gli oggetti strato dopo strato, i produttori sentiranno il bisogno e avranno anche l'opportunità, di monitorare la produzione in un modo completamente nuovo.

Il monitoraggio dei prodotti mentre si formano potrebbe ragionevolmente produrre Terabyte di dati (1 Terabyte=1012 byte = mille miliardi di byte).

Il CIO dovrà determinare quale parte dei dati sia utile e debba essere mantenuta, e quale invece debba essere eliminata e con quale frequenza. La capacità di gestire ed analizzare dati diventerà sempre più importante quando le tecnologie di stampa 3D saranno impiegate nella produzione di dispositivi medici, componenti per motori, e altri elementi da cui dipende la sicurezza umana.

È ipotizzabile che la tecnologia di archiviazione dati della seconda metà del 21° secolo sarà sempre più basata su materiali biologici e tecnologia organica, come il DNA/RNA. I meta-materiali biologici saranno sempre più utilizzati al posto dell' attuale tecnologia basata sul petrolio, metalli, ed elettronica. **Prendendo spunto da processi esistenti in natura si riescono ad ottenere migliori prestazioni ad un costo inferiore** .

Le aziende, producendo i propri prodotti in un modo completamente diverso, dipenderanno sempre di più dalle tecnologie e dalla capacità di monitoraggio che l'IT (Information Technology) potrà loro fornire, oltre agli strumenti e i dati necessari per effettuare le simulazioni, il monitoraggio, e i processi di collaudo.

> **Forse la più grande lezione che abbiamo imparato nel 21° secolo, per quanto riguarda l'effetto della tecnologia sulla società, è che le infrastrutture diventano sempre più fragili all'aumentare della propria dipendenza tecnologica. Questa purtroppo è una tendenza irreversibile.**

I dati, come tutte le informazioni memorizzate in forma digitale, sono particolarmente vulnerabili allo spionaggio industriale, al cyber-crime hacking, e a cyber-war tra i vari poteri nei differenti scenari geopolitici.

La competizione economica tra le potenze mondiali, e le battaglie sulla proprietà intellettuale tra le gigantesche corporation del libero mercato globalizzato indurranno certamente al furto di progetti stampabili in 3D, molto prima di quanto si possa pensare.

In un futuro, in presenza di processi produttivi additivi, l'attenzione dello spionaggio si sposterà sull'attacco ai file 3D memorizzati digitalmente.

Si immagini che una società abbia creato un disegno rivoluzionario di nuovo oggetto utilizzando un software di modellazione 3D.

Per produrlo, utilizzando metodi tradizionali, l'azienda dovrebbe investire molto denaro in stampi per la fusione e attrezzature delle macchine per forgiare, forare e lucidare il prodotto, e avrebbe bisogno di tecnici altamente qualificati per sorvegliare l'intero processo produttivo.

Nel mondo della produzione additiva, i criminali informatici industriali possono impadronirsi del file CAD con il disegno dell' oggetto, e prima che qualcuno si accorga che sono state violate le difese informatiche della società, tramite una stampante 3D da € 50.000, potrebbero iniziare a produrre questo nuovo oggetto di cui è stato rubato il disegno.

Con la stampa 3D, i requisiti patrimoniali per la contraffazione tendono a calare considerevolmente.

Una sfida che le aziende dovranno affrontare e risolvere è quella di trovare un nuovo modo di identificare i propri prodotti.

Ciò può essere realizzato utilizzando una marchiatura o un altro identificativo, o progettando prodotti in modo che possono essere facilmente identificabili, se contraffatti. Per esempio questa seconda strategia sembra quella perseguita dalla LEGO per i suoi mattoncini.

Molte delle sfide riguardanti la proprietà intellettuale e di sicurezza che si presentano con la stampa 3D suonano già familiari agli addetti. In questo momento c'è molto fermento intorno alla fabbricazione additiva e il suo potenziale effetto sulla proprietà intellettuale, ma questo tipo di preoccupazioni non sono nuove.

Quando i masterizzatori DVD furono facilmente disponibili divenne evidente che potevano essere usati per copiare e trasferire grandi quantità di dati riservati, e quindi le organizzazioni hanno affrontato le stessa sfida sulla sicurezza di base che si trovano ad affrontare oggi con la stampa 3D.

La protezione dei dati per i file stampabili in 3D sta per diventare più importante della protezione delle informazioni personali, delle comunicazioni aziendali e, eventualmente, anche dei database militari.

3. La protezione dei copyright

La protezione dei copyright è una delle questioni più delicate in assoluto per l'industria della stampa 3D, quali sono i possibili rimedi?

Il formato STL (Stereolitoghraphy) **utilizzato prevalentemente nella stampa può essere paragonato** , dal punto di vista della tutela del patrimonio aziendale, **al formato MP3 che tutti conosciamo e che ha portato nel mondo della musica una bufera che ha travolto l'industria musicale e in seguito anche quella dei film**.

La diffusione del formato MP3 ha facilitato la copia elettronica e l'ascolto delle canzoni scavalcando, in modo spesso illegale, il modello di distribuzione dei contenuti in vigore.

La stampa 3D essenzialmente potrebbe portare ad un fenomeno analogo, un disegno in formato STL utilizzabile teoricamente da chiunque possieda la stampante adatta permette la duplicazione di un oggetto "reale" in modo difficilmente controllabile.

> **Ci sono aziende che già adesso stanno utilizzando la stampa 3D e che, probabilmente, si apriranno al commercio del formato digitale.**

LEGO, ad esempio, afferma che monitorerà tutti i modi in cui la stampa 3D verrà utilizzata commercialmente e adotterà le azioni necessarie per tutelare i propri diritti – anche per assicurarsi che i consumatori siano sempre in grado di distinguere chiaramente quando stanno acquistando un prodotto LEGO di alta qualità – e quando, invece, stanno acquistando un'imitazione.

Il punto di vista dell'azienda è quindi essenzialmente quello di tutelarsi confidando nella notorietà del marchio e del prodotto.

Ma che cosa succede in un mondo dove qualcuno cerca di creare qualcosa di nuovo e vuole tutelarsi dall'utilizzo improprio di quello che è il frutto del suo duro lavoro? Ora questo è dematerializzato e spesso rappresentato solamente da una manciata di bit messi assieme.

La stampa 3D necessita di diversi passaggi e, potenzialmente, ognuno di questi può essere oggetto di attacchi volti a danneggiare e/o copiare il lavoro svolto.

Il primo passaggio, quello del disegno, normalmente viene preparato in azienda e il risultato deve essere protetto, e monitorato l'accesso in modo analogo a tutti i documenti aziendali importanti.

> **Il principale valore aziendale è quindi il disegno ed essendo realizzato in formato elettronico è facilmente duplicabile e modificabile.**

I passi successivi, trasformazioni in formato STL stampabile e, soprattutto lo slicing e la stampa vera e propria debbono essere oggetto di una cautela particolare, perché spesso questi passaggi possono essere effettuati anche da aziende che offrono servizi di stampa 3D all'esterno in "outsourcing".
Ma che cosa può essere attaccato da malintenzionati?
I dispositivi fisici, i dati e il software, i servizi online, e i risultati della stampa.
Come può avvenire?
Modificando il software o la configurazione, i dati del disegno, il firmware dei dispositivi.
Quando può verificarsi l'attacco?
Bisogna considerare il beneficio per l'attaccante, il costo dell'attacco, la percentuale di successo dello stesso.
Non dimentichiamo che l'attacco potrebbe avere come scopo il solo danneggiamento con eventuale perdita di immagine del proprietario e non il furto dell'oggetto.
Ad esempio si potrebbe modificare mediante il software il comportamento della stampante in modo da stampare un oggetto difettoso o danneggiare la stampante stessa forzando movimenti fuori dai limiti o lavorando a temperature eccessive.
La scelta di affidarsi ad aziende esterne è spesso obbligata, in quanto dotarsi preventivamente delle stampanti in grado di trattare diversi tipi di materiali può essere oneroso e la velocità con cui procede lo sviluppo rende un modello obsoleto dopo pochi mesi, **inoltre la stampa 3D sta cominciando anche a produrre "catene di montaggio" che permettono la realizzazione di prototipi multicolore e multi-materiale in modo rapido**.
Ma quali sono i rischi che si corrono? Affidarsi ad un fornitore esterno può dare garanzie?
Si trovano nel web aziende che offrono il servizio di stampa 3D ma spesso non si ha la certezza che offrano garanzie sul trattamento dei nostri disegni.

> **Cominciano così a nascere compagnie di stampa 3D che hanno come focus la sicurezza e il controllo.**

Un possibile approccio, potrebbe ad esempio, essere quello di permettere l'accesso remoto a tutte le fasi da parte del cliente.
Si parte da una connessione protetta al cloud dove vengono parcheggiati i disegni.
Quando i disegni sono disponibili è possibile controllare ogni fase del processo e monitorare la stampante fisica per verificarne il funzionamento e che il processo avvenga senza manomissioni da parte di qualcuno non autorizzato.

Si potrebbe ipotizzare il monitoraggio ambientale della stanza e della macchina utilizzata per la stampa (tramite telecamera/microfoni) per evitare operazioni non autorizzate e la relativa registrazione. Questo tipo di approccio offre una sicurezza percepita molto alta in quanto la visione reale del processo è estremamente rassicurante e evita intrusioni e/o manomissioni grossolane.
Siamo del tutto sicuri che non ci possano essere manipolazioni e/o copie non autorizzate?

> **In ambito informatico, come in altri ambiti, la sicurezza assoluta non esiste, occorre considerare con attenzione tutti gli aspetti e adottare, caso per caso, tutti gli accorgimenti possibili per evitare un utilizzo fraudolento del nostro patrimonio;**

ad esempio:

1. Selezionare e verificare accuratamente i nostri partner e cautelarsi dal punto di vista legale
2. Monitorare con cura i nostri sistemi alla ricerca di virus ed accessi non autorizzati
3. Controllare con cura tutto il sistema di lavoro delle stampe 3D sia dal punto di vista ambientale che hardware e software
4. Affidarsi a professionisti di fiducia e di comprovata esperienza in materia

Esaminiamo le criticità relative alla stampa di oggetti 3D utilizzando un servizio di stampa interno o in outsourcing, i punti principali nei quali si potrebbero verificare furti del disegno possono essere:

1. **Trasmissione dei file**
   Problema: La trasmissione può essere intercettata (mail, upload di file), un malintenzionato potrebbe utilizzare a suo piacimento il disegno
   Soluzione: Criptazione del file mediante chiavi asimmetriche. La cifratura del file con la chiave "pubblica" del ricevente, permette solo a quest'ultimo la decrittazione.
2. **Conservazione del file**
   Problema: Accesso da parte di persone non autorizzate
   Soluzioni: Politiche rigorose sugli accessi solamente ad un insieme prefissato di macchine/utenti, blocco dell’utilizzo chiavette USB, utilizzo di nomenclature che non permettano di ricondurre facilmente il disegno al Cliente/Oggetto, in modo che gli operatori non conoscano la provenienza degli stessi, monitoraggio degli accessi ai singoli file tramite un sistema di audit
3. **Elaborazione delle immagini e preparazione alla stampa**
   Problema: La persona che ha accesso al disegno in questa fase potrebbe effettuarne delle copie
   Soluzione: Monitoraggio e verifica puntuale dell'operato dell'addetto, con macchine virtuali di interfacciamento stampante che non possano accedere alla rete esterna o a dispositivi non autorizzati e che al termine del lavoro facciano “rollback” automatico eliminando tutte le tracce del lavoro eseguito
4. **Stampa**
   Problema: Stampa di copie non autorizzate
   Soluzione: Dispositivi Hardware che "contino" le copie stampate
5. **Logistica**
   Problema: Sottrazione del prototipo o del prodotto finito

Soluzione: Imballaggio diretto degli oggetti finiti in contenitori sigillati con segnalatori di posizione GPS e allarmi per apertura non autorizzata.
Controllo degli oggetti in attesa di spedizione.
Spedizione con corrieri sicuri

4. Crittografazione di file 3D

Un altro contributo interessante è estratto dall'articolo che riguarda la "Crittografazione di file 3D: il prossimo Step nella sicurezza della stampa?" di Alexey Churchwell
Qualsiasi file 3D, essendo una informazione di tipo digitale, può essere facilmente condiviso, il che significa che tutto ciò che serve è un luogo dove scaricarlo, una stampante e si può produrre l'oggetto. **Questo è un bellissimo aspetto della stampa 3D ma nel contempo la sua maledizione**.
Essendo possibile condividere qualsiasi cosa, in questo sono compresi anche i progetti di oggetti pericolosi. Quando i file per la prima pistola stampata in 3D sono stati rilasciati, sono stati subito sequestrati dal governo degli Stati Uniti. Purtroppo però, i file erano già stati diffusi su Internet, e sono ancora disponibili in alcuni siti in formato "torrent", un tipo di file utilizzato per condividere contenuti personali.
Siti come Thingiverse, che permettono di caricare i modelli 3D creati dagli utenti, combattono questo fenomeno filtrando il materiale pericoloso o protetto da copyright. Forse una nuova applicazione di crittografia dei file 3D potrebbe cambiare la situazione.

> **Matthew Plummer-Fernandez, un appassionato di stampa 3D, ha recentemente progettato un'applicazione che consente di crittografare - e decifrare - i file 3D, solamente con un codice di protezione opportuno.**

La crittografia in realtà cambia il modo in cui il file appare; anziché l'oggetto che il file dovrebbe effettivamente stampare, se ne vedrebbe una forma distorta.
Da un lato, questo tipo di applicazione è importante per motivi di sicurezza. Se è necessario effettuare un progetto per un'ultima invenzione, o si vuole fabbricare un modello esclusivo di un prodotto, la crittografia consente di trasferire i dati in modo sicuro: in pratica è possibile fare in modo che nessun altro possa accedervi.
Ovviamente sarà necessario un codice per aprirlo, ma tale informazione potrebbe essere fornita in un sito separato senza alcuna difficoltà.
Un' altra soluzione per condividere i file di progettazione 3D mediante l'invio di messaggi di posta elettronica, o sui siti di file sharing, o tramite lo scambio di schede SD, è stata presentata al Mobile World Congress nel febbraio 2013, dove una startup Estone chiamato Fabulonia ha effettuato una dimostrazione di streaming di progetti 3D dalla Germania ad una stampante 3D a Barcellona, Spagna.
Questa società propone una tecnologia sicura di streaming 3D che codifica e memorizza i dati con un metodo che rende i file inaccessibili agli estranei. Solo le persone autorizzate sono in grado di accedere a tali file.
Il dispositivo è stato progettato per essere collegato con specifiche stampante 3D, di tipo Makerbot 2 o 2X, e deve essere collegato tra la rete e la stampante 3D.

È possibile creare un account ed iniziare caricare i file, che verranno criptati rendendoli pronti per essere condivisi e stampati in modo sicuro, in locale o in remoto.

5. Gli hacker

Un altro interessante articolo che vale la pena citare è "*Come gli hacker possono infiltrarsi in una stampante 3-D Printer*" di John Paul Titlow

Un ricercatore cinese sostiene che, essendoci sempre più stampanti 3-D di tipo "consumer" presenti sul mercato, dovremmo essere preoccupati per la loro sicurezza.

Con l'avanzare della rivoluzionaria stampa 3D, le cose stanno diventando molto interessanti. Che ci si creda o no, una stampante 3-D può essere violata.

Per ogni balzo in avanti della tecnologia, vi sono i conseguenti rischi e insidie.

Questo argomento è stato al centro di una recente presentazione proposta da un ricercatore cinese sulla sicurezza Claud Xiao alla XCon 2013 Security Conference a Pechino. Xiao, che fa ricerca sulla sicurezza per una società di antivirus cinese, ha illustrato i modi in cui gli hacker possono sfruttare le vulnerabilità all'interno di una stampante 3-D o della rete a cui è collegata.

È tutto abbastanza teorico, ma i dettagli sono specifici ed abbastanza plausibili per fare venire ad un qualsiasi amministratore IT qualche preoccupazione.

Perché qualcuno dovrebbe attaccare una stampante 3-D? Che cosa ne potrebbero ottenere? Come ogni forma di pirateria informatica, la motivazione può variare da qualcosa di poco più di una innocua birichinata ad una vera e propria guerra cibernetica. **Qualunque sia l'obiettivo finale, ottenerne l'accesso per fare danni non è cosa di poco conto**.

Naturalmente i danni, variano a seconda del tipo di apparecchiatura. Una RepRap, un sistema open source di prototipazione rapida, è ovviamente un bersaglio più facile dell'ultimo modello industriale di 3D Systems.

Dopo avere analizzato l'intero flusso di elaborazione del modello di dati 3-D e del relativo metodo di controllo della stampante, si è riscontrato che quasi tutti i software correlati, il firmware, e i servizi di download on-line non salvaguardano la sicurezza, quando si utilizzano le stampanti "consumer" di tipo RepRap.

Nella maggior parte dei casi, quando i dati del modello o i dati di configurazione vengono trasferiti o memorizzati, o il comando di controllo è trasferito o eseguito, non c'è alcuna autenticazione o verifica, il che significa che il potenziale aggressore può facilmente effettuare delle modifiche.

Per trovare un punto debole in questo flusso di elaborazione dei dati, si potrebbe iniettare del codice malevolo "malware", il quale potrebbe influenzare l'output della stampante, carpire file CAD sensibili, o addirittura modificare il firmware della stampante e prenderne il controllo. È anche possibile che questo "malware" possa annidarsi nei file CAD utilizzati per stampare i modelli 3-D, che sono liberamente distribuiti online.

A seconda della natura dell'attacco, i risultati possono variare ampiamente. **In primo luogo, c'è il rischio che la proprietà intellettuale di un'azienda o altre informazioni sensibili possano essere carpite**.

Come già è stato visto con l'hacking di stampanti su carta a getto d'inchiostro, infiltrarsi in quelle 3-D può consentire di intercettare i file STL o altri dati del modello 3-D ancora prima di essere inviati alla stampante.

Se si sta stampando una cover per iPhone appena scaricata da Thingiverse, ciò probabilmente non avrebbe molta importanza. Ma se un'azienda sta lavorando su prototipi per un nuovo prodotto top secret, un ambizioso concorrente, potrebbe carpire informazioni non autorizzate.
Se si considerano i tipi di industrie che saranno inclini a utilizzare la stampa 3-D, ad esempio medico, industriale e militare è possibile immaginare il motivo per cui varrebbe certamente la pena fare hacking dei dati del disegno 3-D presente all'interno di una stampante.
Con la tattica giusta, si potrebbe anche influenzare il comportamento della stampante. Questo potrebbe essere qualcosa di innocuo come interrompere il processo finale di stampa del progetto del proprio compagno di Università, in modo da produrre qualcosa di goliardicamente osceno.

> **Altresì potrebbe fornire agli hacker un modo per danneggiare fisicamente la stampante stessa, iniettando un codice "malvagio", questo potrebbe alterare la logica del firmware della stampante, causando il fatto che la macchina stampi oggetti danneggiati o, peggio, danneggiare se stessa.**

Ad esempio provocandone deliberatamente il surriscaldamento, si potrebbe rendere inutilizzabile una macchina molto costosa.
Un fatto del tutto analogo a quanto è avvenuto con il **"worm" Stuxnet**, **un virus informatico creato e appositamente diffuso dal governo USA** (nell'ambito dell'operazione iniziata da Bush nel 2006 che consisteva in un "ondata di attacchi digitali" contro l'Iran) **in collaborazione col governo Israeliano, nella centrale nucleare iraniana di Natanz, allo scopo di sabotarne le centrifughe per interrompere l'arricchimento dell'uranio tramite l'esecuzione di specifici comandi da inviarsi all'hardware di controllo industriale responsabile della velocità di rotazione delle turbine, al solo scopo di danneggiarle**.
Questa ricerca serve ad avvisare le aziende, che utilizzano le stampanti 3-D a livello industriale, che vi sono questioni di sicurezza non ancora esplorate su queste macchine sempre più diffuse.
È ragionevole pensare che tutte le stampanti probabilmente siano sotto tiro, in particolare modo quelle utilizzati per i lavori più importanti, o quelle stampanti di dimensioni desktop, utilizzate da hobbisti e designer.

TAG: *3D printing, innovative technology, copyright*
