dr0wned – Cyber-Physical Attack with Additive Manufacturing

Jean Daniel Prestes Massucatto

Introdução

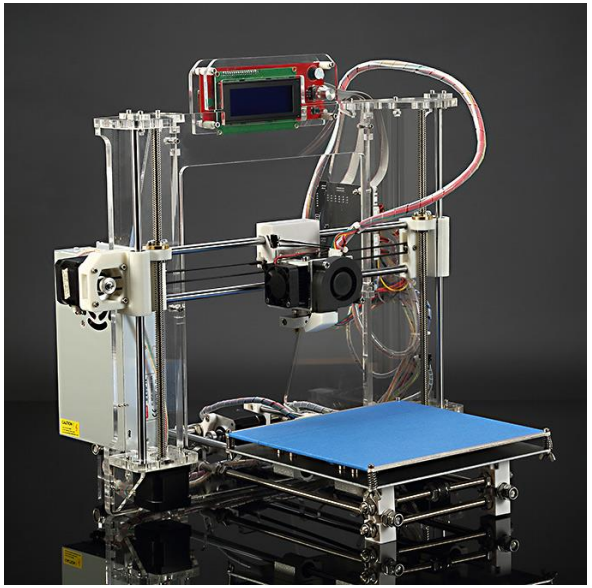
- Com a imersão das impressoras 3D, muitas vulnerabilidades começaram a ser exploradas, tornando as impressoras alvos de sabotagem.

- O objetivo do artigo é mostrar como essa sabotagem pode ocorrer, reduzindo a vida útil de uma peça e levando a queda de um drone no meio do voo.

Impressões 3D

- Impressões 3D são hoje consideradas uma forma emergente de fabricação caseira (manufatura).
- São amplamente usadas para produzir peças, incluindo componentes para sistemas de segurança críticos.
- São altamente dependentes de sistemas computacionais para elaborar suas peças, sendo altamente passíveis de sabotagem.

Impressões 3D



Impressões 3D

- Principais tipos de materiais - Plástico ABS e PLA.
- Baseia-se na fusão de camadas de material.
- Possuem vantagens econômicas e ambientais muito maiores se comparadas métodos tradicionais de manufatura, os quais se dão por ferramentas de corte para reduzir um bloco de material até o tamanho e formato desejado.
- Possuem vantagens de poderem ser produzidas mais rapidamente e sob demanda, reduzindo o desperdício de material, e sobretudo poder ser construídas peças com uma estrutura interna mais complexa.

Impressões 3D

- A primeira prova experimental de que uma impressora 3D poderia ser comprometida foi apresentada em 2013 na *XCon2013* por Xiao Zi Hang.

- De acordo com seu experimento um ataque pode modificar resultados impressos, incluindo o tamanho do modelo, posição e integridade dos componentes etc.

Impressões 3D

- Existem diversas publicações que analisam a possibilidade de comprometimento de impressoras 3D, nos quais os autores analisam toda a cadeia de processo de criação de uma peça 3D, encontrando diversos vetores de ataque que podem ser facilmente **explorados.**

- O foco inicial é voltado para redes e comunicações. Particularmente o estágio de recebimento do design da peça.

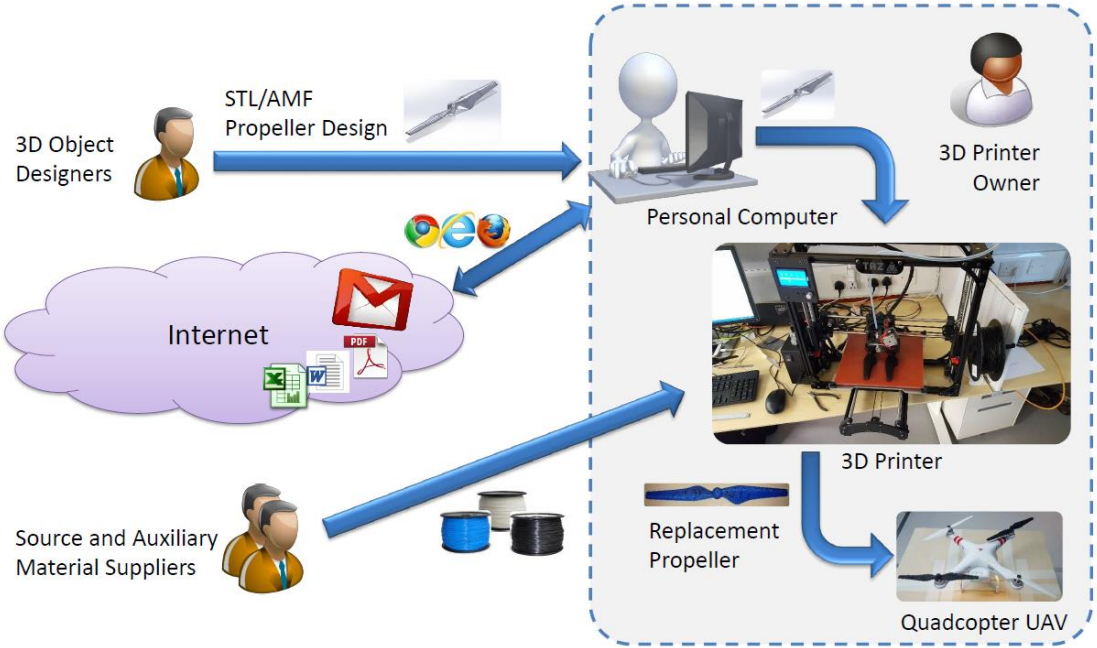
Impressões 3D

- Uma publicação recente analisou softwares open-sources comumente usados em impressoras 3D de mesa e outras 3 aplicações gráficas que utilizam G-Code para realizar a comunicação com a impressora 3D. E em cada um desses programas, análises do código fonte, e análises da comunicação entre a impressora 3D e o computador revelaram inúmeras vulnerabilidades.

Cenário de Ataque

- Para o artigo proposto foi considerado um cenário envolvendo um usuário doméstico com uma impressora 3D, o qual supostamente está produzindo hélices de reposição para um quadricoptero UAV.
- A vítima procura por si mesmo um modelo 3D do objeto desejado
- A impressora 3D é controlada por um computador pessoal que envia comandos **G-code** através da conexão USB

Cenário de Ataque



Cenário de Ataque

- Para a realização do artigo diversas suposições foram necessárias.
- Primeiro assumir que o usuário não mantém seu software atualizado, comportamento da maior parte dos usuários.
- Segundo, que o usuário utiliza o mesmo computador para navegar na internet, ler emails, realizar download de documentos, jogar, etc.

Cenário de Ataque

- No cenário apresentado o atacante deseja destruir o drone da vítima. O atacante pode conseguir isso sabotando a hélice de substituição impressa em 3D da vítima para que ela falhe em alta altitude, resultando em danos ao drone.
- Isso significa que o ataque deve passar por inspeções visuais básicas e testes mecânicos manuais, e não afetar a integração da hélice, para que o usuário irá instalar a hélice de substituição sem suspeitas.
- A hélice é impressa usando plástico ABS, um dos tipos mais usados, pela durabilidade, força, flexibilidade, resistência a altas temperaturas e absorção de choque.

Seleção da cadeia de ataque

- **Alvo** - O objetivo é que a hélice quebre após um tempo relativamente curto. Isso significa que a sabotagem da hélice deve apresentar um defeito, levando ao acúmulo de tensão mecânica, resultando em um rápido rompimento da hélice. No entanto, deve sobreviver por um breve momento para não levantar suspeitas.

Seleção da cadeia de ataque

- **Manipulações** - Embora a seleção da categoria de manipulação seja relativamente direta, a definição exata da modificação não é.
- Mesmo que o adversário tenha uma proficiência AM moderada, é extremamente difícil calcular o impacto de um defeito na resistência mecânica e na fadiga, embora esses fatores tenham sido intensamente estudados e sejam bem compreendidos na ciência dos materiais.
- Portanto, assume-se que o adversário deve experimentar vários defeitos antes de identificar uma escolha satisfatória.

Seleção da cadeia de ataque

- **Elemento comprometido** - A especificação do objeto, em várias representações, se move entre diferentes dispositivos no fluxo de trabalho. Ele se origina na criação de um objeto 3D que é transferido para o PC do controlador como arquivo um arquivo STL. Do computador controlador é transmitido para a impressora 3D como uma sequência de comandos de código G. Qualquer elemento ao longo deste caminho, se comprometido, pode modificar a especificação do objeto.

Seleção da cadeia de ataque

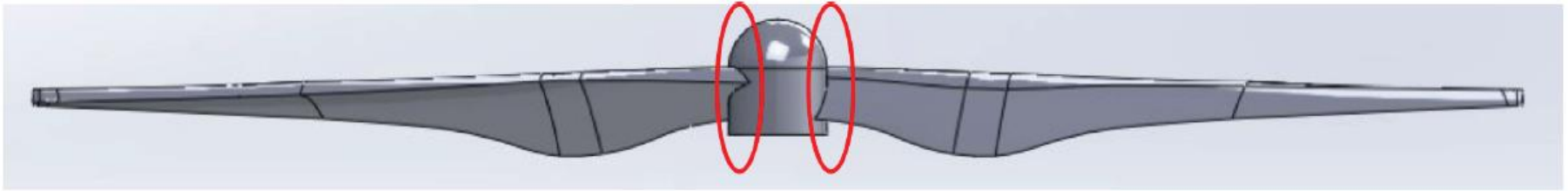
- **Elemento comprometido -** Para o artigo proposto o modo de comprometimento escolhido foi através da internet.
- Pois pela suposição inicial o computador que controla a impressora 3D é o mesmo computador que o usuario usa para trefar pela internet, até mesmo atrás de modelos de arquivos STL.
- **Vetor de Ataque** - No artigo a forma de ataque utilizada foi *phishing attack* e arquivos compactados no formato WinRAR.

Definindo manipulações

- Algumas experiências e testes são necessários para verificar se a manipulação do objeto leva a sabotagem da hélice ou não. Portanto assume-se que o atacante possua recursos disponíveis semelhantes aos da vítima para realizar os testes.
- **Objetivos do defeito** - O defeito deve ser indetectável visualmente, e difícil de ser percebido em testes manuais básicos. Em adição, a hélice deve quebrar após um curto período de uso em condições normais.

Definindo manipulações

- **Local do defeito** - As hélices são responsáveis por transformar o torque dos motores em força de impulso. O design original da hélice foi projetado para suportar a força de impulso que atua sobre ele quando os motores estão rodando em máxima velocidade.
- - A força de elevação faz com que as hélices se dobrem para cima durante o voo, e é nessa parte onde a atacante irá focar.



Definindo manipulações

- **Mudanças testadas** - Primeiramente foi feita uma mudança nos furos entre as lâminas e a cabeça da hélice, mudanças que não afetaram muito a capacidade da hélice.
- Em seguida pequenas lacunas foram inseridas no modelo 3D entre as lâminas e a parte central da hélice gerando 3 partes separadas. A ideia principal desta mudança foi que se as lacunas fossem suficientemente pequenas, a impressão em 3D ainda sairia uma peça totalmente conectada e um ponto de ruptura artificial estaria criado.

Definindo manipulações

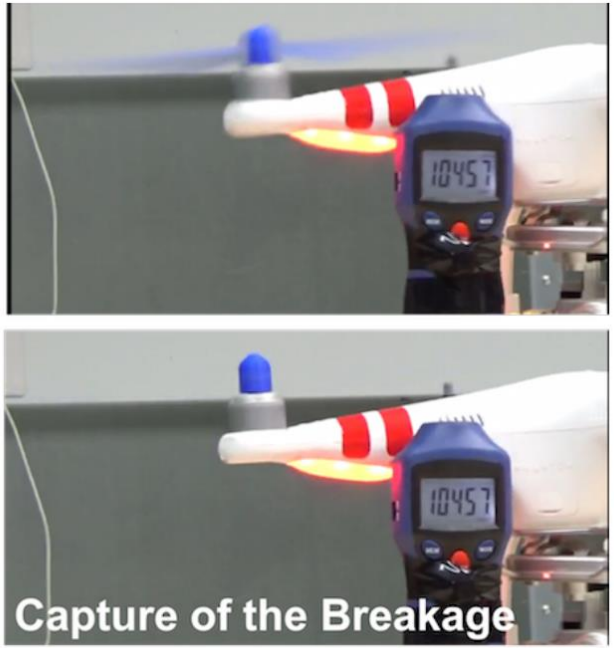
- O tamanho das lacunas foi encontrado de forma empírica. (0.1mm)
- Deve-se notar que, como o defeito é introduzido em um ponto de união das lâminas e da base, a mudança no padrão de impressão neste ponto permanecerá despercebida por uma simples inspeção visual da hélice impressa.

Definindo manipulações

Definindo manipulações

- Testes foram realizados a fim de criar um ambiente de testes controlado e reprodutível.
- Duas hélices foram instaladas no quadricoptero, uma não modificada e a outra sabotada.
- Dois fatores foram medidos, o tempo em que a hélice quebrou e o RPM atingido naquele momento.

Definindo manipulações



Execução do Ataque

- **Sabotagem** - O ataque apresentado foi realizado em 3 etapas.
  - Comprometer o computador pessoal da vítima.
  - Ter acesso aos arquivos originais da hélice.
  - Mudar os arquivos, incluindo os defeitos necessários para a elaboração do ataque.

Execução do Ataque

- **Comprometendo o PC controlador** - A Fim de realizar o infiltramento no PC da vítima, foi criado um arquivo executável malicioso.
- O arquivo teve sua extensão e nome mudado para parecer simplesmente um arquivo PDF inocente, compactado pelo WinRAR.
- A vítima recebe um email com link para download desse arquivo, e uma vez que a vítima pressione o mouse duas vezes sobre o arquivo um ***reverse shell*** é aberto em plano de fundo e o atacante pode obter controle total do sistema.

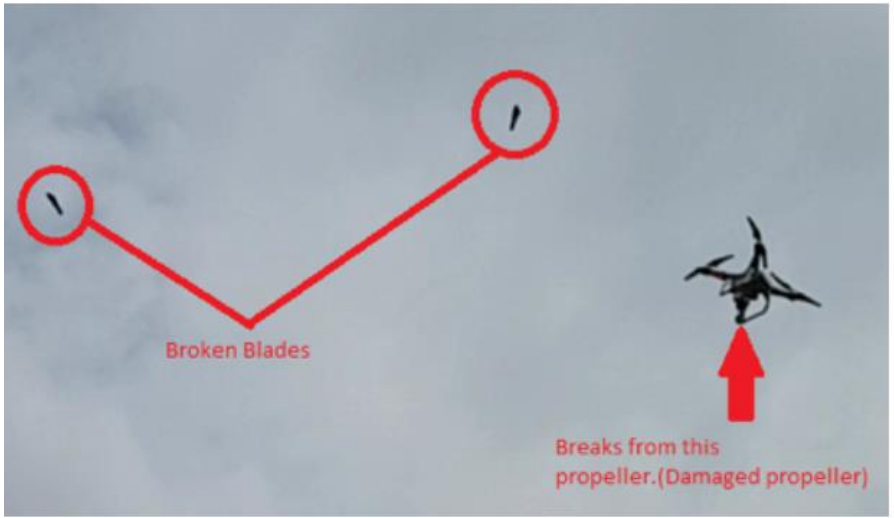
Execução do Ataque

- **Manipulando arquivos de design** - O próximo passo consistiu em encontrar e fazer o download dos arquivos STL necessários e modificá los utilizando uma ferramenta como SOLIDWORKS, e através de testes testar a eficiência da modificação.
- **Trocar os arquivos de design** - Após a modificação dos arquivos, usar o ***reverse shell*** aberto e trocar os arquivos originais pelos arquivos modificados

Execução do Ataque

- **Testes de campo** - Em um primeiro momento o teste foi feito usando as quatro hélices impressas em impressora 3D, o drone foi capaz de permanecer voando por mais de 5 minutos.
- Quando uma das hélices foi trocada, pela hélice maliciosa, o tempo de voo do drone foi de 1 minuto e 43 segundos.
- Considerando a altura da queda do drone, um dos motores foi danificado, a câmera que estava no drone foi totalmente destruída e o chassi quebrado.

Execução do Ataque



Viabilidade do Ataque

- A viabilidade do ataque depende de diversos fatores, mas mais importante que isso a habilidade de comprometer um ambiente de impressão 3D, e de identificar a peça a ser sabotada.
- Uma vez que a manipulação não interrompe o fluxo de fabricação e o uso do computador controlador por parte do atacante pode ser breve, seria difícil para mecanismos de segurança detectar essa invasão.
- Testes requerem equipamento especializado e caro.

dr0wned – Cyber-Physical Attack with Additive Manufacturing

Jean Daniel Prestes Massucatto