Hack3D: Crowdsourcing the Assessment of Cybersecurity in Digital Manufacturing

Michael Linares, Nishant Aswani, and Gary Mac, New York University
Chenglu Jin, CWI Amsterdam
Fei Chen, Apple
Nikhil Gupta and Ramesh Karri, New York University

This article summarizes lessons from the past three Hack3D events, including ways in which engineers can launch surprise attacks on digital manufacturing (DM) designs. A key outcome is a taxonomy-guided security benchmark for the DM community.

Digital manufacturing (DM) security is gaining attention due to the involvement of trusted, partially trusted, and untrusted parties in the supply chain.[1] A survey and taxonomy of threats and vulnerabilities has been developed.[2] It shows that numerous attack vectors exist for the DM process chain and that only a few specialized security schemes are available for this complex cyberphysical system (CPS). For example, DM attack vectors and impacts were discussed from a cyberphysical perspective in Sturm et al.[3] Similarly, a stealthy DM tool path modification attack can go undetected.[4] These attacks highlight the need for improved quality controls, cybersecurity education, and development of DM security assessment. A methodology for detecting attacks on an artifact's intrinsic behavior is presented in Vincent et al.[5]

The DM process model was studied and a new "federated" information systems architecture was developed in Kim et al.[6] This architecture establishes requirements for end-to-end information sharing, quality control, and performance assurance. Yampolskiy et al.[7] investigate intellectual property (IP) protection for outsourced manufacturing and study an alternative model that incorporates third-party process tuning experts. They present a risk assessment focused on IP protection and make recommendations to minimize risks. Furthermore, McNulty et al.[8] survey the significance of DM for national security.

Digital Object Identifier 10.1109/MC.2021.3074192
Date of current version: 22 October 2021

0018-9162/21©2021IEEE

A variety of cybersecurity methods have been developed that are specific to DM. These approaches include hiding features in design files to make it difficult for unauthorized users to print high-quality parts.[9] Embedding identification codes inside parts has been explored.[10] The codes are obfuscated by breaking them into hundreds of segments and hiding the sections in numerous layers.[11] This article reports the outcomes of a series of crowdsourcing events focused on understanding the strengths and weaknesses of security methods for DM. We describe Hack3D (https://www.csaw.io/hack3d) designs and attack methods developed by participants and conclude with lessons learned during the event.

THE DM CPS

The DM process chain

Figure 1 illustrates the DM process chain, which includes CAD; design refinement through simulation tools such as finite element analysis (FEA); and manufacturing parts on 3D printers, followed by testing and assembly. The product design process remains the same even in traditional manufacturing, such as machining and milling. All steps involved in DM use computers and the cloud for computation, collaboration, machine control, and data acquisition and analysis. Hence, they are targets for cyberattacks.

A taxonomy of DM cyberthreats

Attacks in the DM supply chain are classified into four categories, as illustrated in Figure 2.[12] For each category, different skills and tools are needed for success. As detailed in Figure 3, DM cybersecurity threats can be classified across four attack categories (goals, methods, targets, and countermeasures). Several security methods that can be applied to the DM supply chain are available, but their strength needs to be analyzed.

HACK3D: ASSESSING DM SECURITY STRENGTH

An effective and widely used approach to assess the strength of security strategies is to conduct a red team/blue team challenge involving participants from diverse backgrounds. The objective of the Hack3D challenge is to provide a platform for these challenges to evaluate the robustness of new DM security strategies. The Hack3D research team takes the role of the blue team, designing security methods for a manufacturing process and presenting them as challenges. The approaches target a wide range of threats, including a focus on securing digital design files.

Red teams are crowdsourced from students spanning all education levels and backgrounds. Their solutions provide numerous perspectives, some of which were not considered when the blue team designed the challenges. These security assessment benchmarks

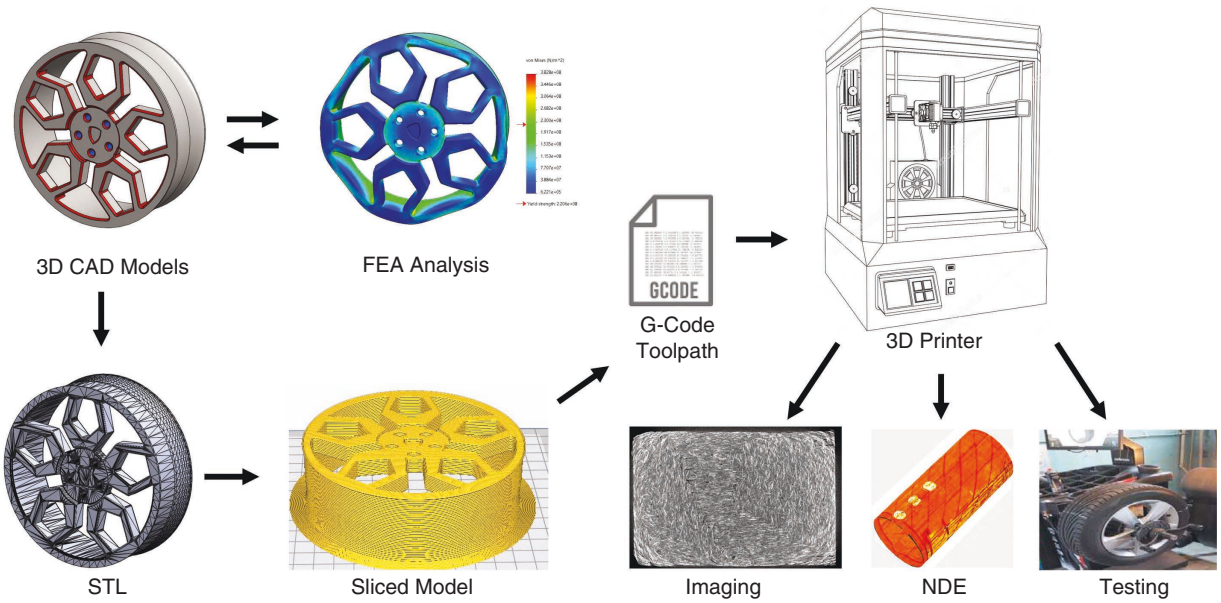

FIGURE 1. The DM CPS makes use of connected systems, such as 3D printers. FEA: finite element analysis; STL: stereolithography; NDE: nondestructive evaluation.

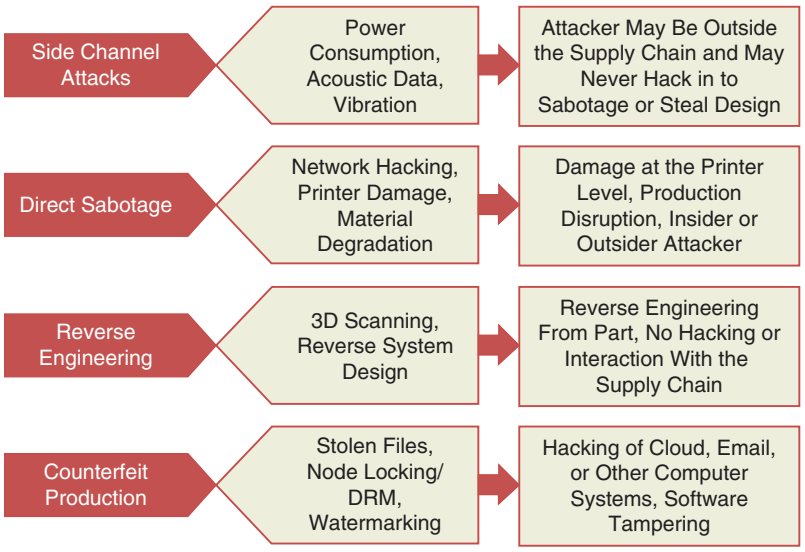

FIGURE 2. A classification of DM supply chain attacks.[1,2] DRM: digital rights management.

help determine the strengths and weaknesses of the blue team's challenges, providing qualitative and quantitative insights for the design of future DM security policies and strategies.

Each challenge investigates a pathway in the threat taxonomy from Mahesh et al.,[2] as in Figure 3. In preliminary Hack3D rounds, red teams have at least one month to solve the challenges. Final rounds were held at New York University (NYU) in 2018 and 2019 and became a virtual event in 2020 as part of the annual NYU Cybersecurity Awareness Week (CSAW), in early November. Participants have one or two days to solve the challenges in the final round.

Challenge 1 (Hack3D 2018 qualifying challenge)

Challenge. Participants received a set of XYZ coordinates in 3D space, describing the shape of a part [see Figure 4(a)]. The red teams used this information to recreate a 3D model of the object. The XYZ coordinates are visualized as a point cloud in Figure 4(b).

Threat scenario. Challenge 1 illustrated attacks that can be launched using the point cloud information of a design. These point cloud data can be generated from 3D scanners. This challenge demonstrated the ability of computer visualization software to recover a CAD model from a point cloud file representing a part. Red team participants assumed the role of an adversary to develop their own reverse engineering method to recover design files by using point cloud information.

Attacks. One red team used Microsoft Excel to convert the coordinates into a point cloud that it imported into SolidWorks. It created a mesh using GeoMagic and obtained reference curves. By combining the reference curves and

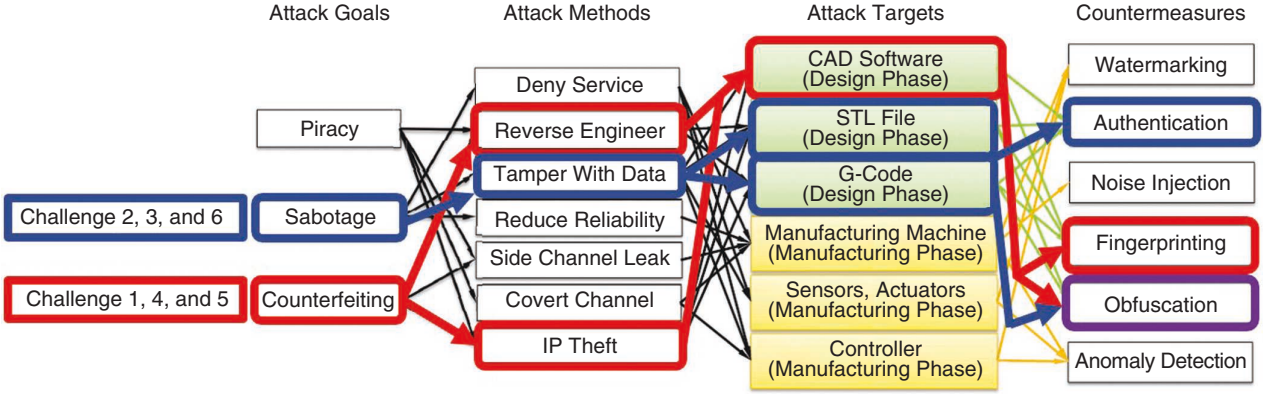

FIGURE 3. The attack vectors that Hack3D challenges have demonstrated are highlighted in a DM security threat taxonomy in Mahesh et al.[2]

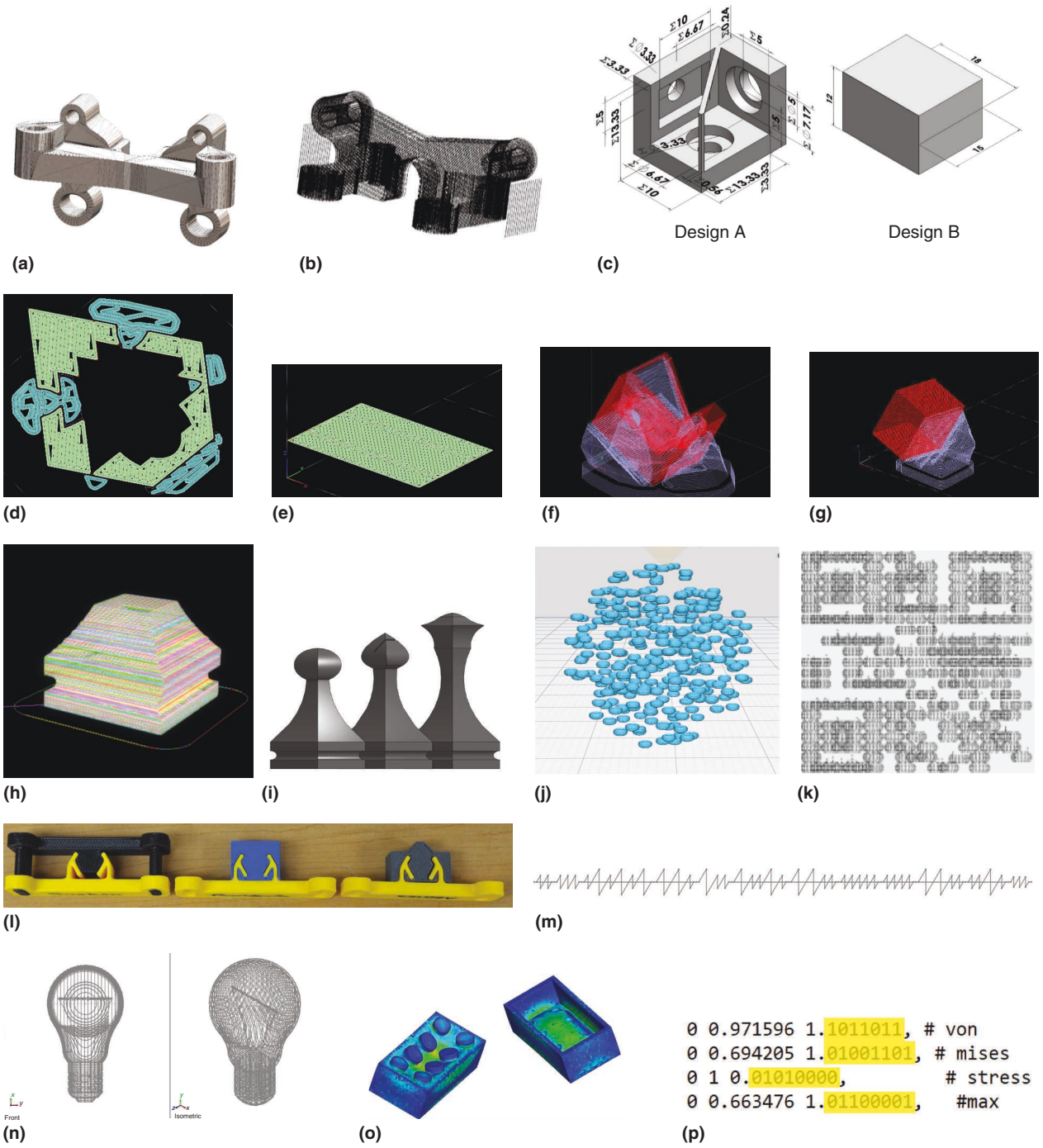

FIGURE 4. (a) In Hack3D challenge 1, participants were asked to reconstruct a 3D model, given a set of XYZ coordinates that described the design. (b) The coordinates can be visualized as a point cloud. (c) In challenge 2, participants received STL files of designs A and B. The teams had to find the slicing and printing orientations that would eliminate surface and internal defects. If printed without rotation, (d) design A will be separated in multiple segments, and (e) design B will have internal slots. The correct orientation for printing and the supporting materials for designs A and B are shown in (f) and (g), respectively. In Hack3D challenge 3, given (h) a partial (possibly damaged) G-code file, attackers have to reconstruct the original G-code file that is cut from a chess piece from among (i) three candidates. (j) If one views the 3D QR code embedded in the chess piece base from a random direction, it looks like a group of spheres. (k) However, viewed from the correct angle, the QR code is scannable. In Hack3D challenge 4, participants were given a female connector (in yellow) and a scaled-down version of its STL file. They were challenged to use this information to reverse engineer a male counterpart. Three reconstructed designs are shown in (l). (m) In Hack3D challenge 5, participants had to recreate a light bulb CAD based on the sketches. In the center of the sketches, (n) a unique code exists for participants to decode. (o) The deformed results of the linear static simulation in Hack3D challenge 6 are saved in a Virtual Reality Modeling Language (VRML) file. (p) The simulated maximum stress is stored in a binary format and hidden in the color index section of the VRML file.

the point cloud outline, the team recreated the 3D model. Another red team used the FeatureScript tool in OnShape. It developed scripts to extract information from the coordinates, draw poly lines, and delete unnecessary faces layer by layer. This way, it recreated the 234 layers and assembled them to recreate the model. A third red team of mechanical engineers used the Scanto3D tool in SolidWorks to reconstruct the 3D model.

Challenge 2 (Hack3D 2018 final challenge)

Challenge. The participants received stereolithography (STL) files for two designs [Figure 4(c)] and were asked to identify the slicing and printing orientations that would remove all surface and internal defects. The two models were designed so that if they were not sliced in a specific direction using required parameters, the prints would have internal and surface defects.

Threat scenario. This challenge mimicked a real-world situation where STL files are leaked to adversaries due to, for example, disgruntled insiders or hacked file storage servers. However, the designers were able to embed defects in the files to prevent attackers from producing high-quality products. The addition of embedded defects is an example of an obfuscation countermeasure designed by the blue team.

Attacks. Most teams sliced the models in different orientations to check whether the defects and nicks survived. Some participants created a table to enumerate all possible rotations. Since we have *x*-, *y*-, and *z*-axes and one can rotate by 360° along them, there are $360^3 \approx 4.7 \times 10^7$ combinations (considering a 1° rotation step). Although brute force tried all the combinations, the red teams came up with strategies to narrow the search space and get to the correct solution within the challenge time of 7 h.

First, participants characterized design A as a complex, open prism with several holes. The flaws were introduced through the presence of segmentation in each layer [Figure 4(d)], which decreased structural integrity. The goal was to find an orientation for design A such that each layer showed a continuous toolpath. Second, the surface area of the bottom layer was considered when participants sought the correct orientation. The bottom layer needed a larger area and more mass so that it could improve the printing quality; a larger bottom layer provides superior adhesion to the base plate. After a few trials with different orientations, some participants found the correct one for printing.

Design B is a solid box. However, inside the box, rectangular prisms were embedded with spade-shaped flaws, giving the surface several nicks [Figure 4(e)]. Participants discovered that the nicks remained if they did not turn the printing orientation, regardless of their choice for the bottom layer. By fine-tuning the rotation angle, they eventually found the correct orientations for printing the design without internal defects. The correct orientations for designs A and B are in Figure 4(f) and (g), respectively.

Challenge 3 (Hack3D 2019 qualifying challenge)

Challenge. For this task, the red teams mimicked attackers who stole a partially damaged G-code file, which modeled only the bottom part of a chess piece. Figure 4(h) presents the damaged G-code as seen in a viewer. Participants needed to solve two problems: 1) identify the correct piece among three candidates (pawn, bishop, and queen) that the partial design represented and 2) complete the design with the correct dimensions. The blue team provided an orthographic image of all candidates, as in Figure 4(i), and a text file with the true *z* heights of each piece. The blue team organizers embedded a nontrivial shortcut in the damaged G-code. They placed the design file of the top half of the chess piece in a separate text file stored in the cloud, giving view-only access to those with a link. This link was embedded as a 3D QR code in the design of the chess base given to the participants.[10]

Threat scenario. This challenge was an example of a cybersecurity threat where an adversary launches an attack to steal design files for counterfeiting. Each participant took on the role of the red team designer working on the G-code to find the hidden information to recreate the complete file. The embedded QR code was used to counter a direct sabotage attack.

Attacks. One of the teams exploited a discrepancy in the metadata in the G-code file. It noticed that a filament length in the original piece (4,290.7 mm) was different than that shown by the G-code viewer (3,198.14 mm). This offered insights into the cutoff design, and the team concluded that all the pieces had a square cross section. Next, using the provided *z* heights and the extracted height of the base piece from the G-code, it determined where the piece was cut off. It cropped the tops off of each piece, used computer vision algorithms to measure the pixel dimensions, and scaled the dimensions using information from the G-code. It reconstructed the G-code for the top of all three pieces. Since it knew the height difference between the original

and damaged pieces, it was able to deduce that the queen was the target, as that piece best matched the height. The final result had an error of 1%.

A second red team processed the image and created a profile of the edges of the pieces. This produced a 1% error in the geometry, as the processing led to a pixelated line. Based on this edge information, the team created the shell of the queen with the help of a few reference points in the G-code and filled the top and bottom layers with infill. A third team also used image processing methods. However, it took a different approach and produced a square prism at each point on the profile curve to recreate the pieces. It inferred that the target piece was the queen, based on the filament length information in the damaged G-code.

Two teams recognized the QR code embedded in the chess piece base. The QR code was segmented into small pieces and appeared as a bundle of spheres, which is shown in Figure 4(j). Only when viewed from a certain direction could the QR code be seen, as in Figure 4(k). One team extracted the QR code from the G-code and then obtained the chess piece design file stored on the cloud server.

Challenge 4 (Hack3D 2019 final challenge)

Challenge. The goal was to target the reverse engineering phase in the DM supply chain and conduct file forensics. Red team participants were given a physical print and a scaled-down version of the STL file for a female connector [the yellow parts in Figure 4(l)]. The challenge entailed the construction of a male connector with a design and dimensions compatible with the female part. Similar to challenge 3, the design of the female connector had an embedded 3D data matrix, which, when viewed from the correct orientation, had the password to a server whose Internet Protocol address and username were stored in the header of the STL file.

Threat scenario. This challenge represented reverse engineering by an adversary who has stolen design files for pirating and counterfeiting. Participants played the role of the adversary and were tasked to create the male connector, using only information about the female connector. The success of this challenge confirms that reverse engineering techniques may be used to obtain information about missing/complementary components of a design from a stolen component.

Attacks. Under a tight time constraint of 6 h, one red team was able to extract all the required information to access the design file stored on the server. The male part was designed with a snap fit and arms to prevent rotation [the left part in Figure 4(l)]. Another red team took a geometric approach and recreated a tight slide-fit male part along with the scale factor. While it was were able to get the data matrix, it could not recover the hidden message in the STL file. Hence, it did not access the file stored on the server. Its final design is the right-most one in Figure 4(l). Finally, one team manipulated the STL file and isolated a single cross section of triangles to create a profile of the female part. After fine-tuning the profile, it conducted multiple design and printing iterations of a snug fit to slide on the male connector [the middle one in Figure 4(l)]. Such a brute force approach was very time and material intensive, as the 3D part printing took more than half an hour each time.

Challenge 5 (Hack3D 2020 qualifying challenge)

Challenge. Participants were given an Initial Graphics Exchange Specification (IGES) file of a light bulb design that had all its solid body geometry removed and replaced with sketches. The challenge was to reverse engineer the light bulb CAD model from the sketches. The sketches provided an overview of what the part should look like, but it was hard to determine the dimensions precisely. Further, a hidden Morse code sketch was embedded in the center of the bulb to enable participants to obtain the original 2D drawing of the light bulb. Figure 4(m) shows the hidden code, where the short vertical lines represent dots and the long vertical lines represent dashes. The IGES file appears in Figure 4(n); it has only 3D sketches that represent the silhouette of the light bulb design created from planar section cuts of the actual model.

Threat scenario. The main purpose of this challenge was to simulate an attacker launching an IP theft attack on engineering design files. The blue team saved the design file with a unique storage method, and the red teams had to recover the file. The initial feedback from some of the teams was that the IGES file was opening as an empty, broken one. The software import options had to be modified to enable viewing the IGES file correctly. One aspect of the challenge was to help introduce the idea of playing with storage methods to better protect design information.

Attacks. Most teams approached the challenge by approximating the measurements of the light bulb features and recreating the part based on the measured dimensions. One team decided to view the IGES file in a

text editor and was able to recover the information about the original design file. The team proceeded to extract the center plane sketches to determine the radius of the glass bulb. It recreated the remaining features by analyzing the small sections of the sketches and recovered the dimensions.

The challenge file had a lot of sketches that had to be properly filtered and analyzed. Otherwise, wrong inferences about design features could have resulted. The multiple cross-sectional planar sketches misled one red team into designing asymmetric support rods. The team used this incorrect assumption in its design. The same team successfully determined that the filament had no cross-section thickness sketch but was not suspicious of the fact. It guessed that the cross section was circular but could not conclude that the filament was a coded message.

Challenge 6 (Hack3D 2020 final challenge)

Challenge. A linear static FEA simulation was conducted on a challenge model, and the results were exported to a Virtual Reality Modeling Language (VRML) file, as in Figure 4(o). The VRML file had a graphical representation of a deformed part, containing the stress result colors and facets from the simulation mesh. Based on the data, the red teams were tasked to determine the maximum value of the FEA and add back the missing interior connectors.

In the interior of the part, the blue team inscribed a code as an insignificant part number. The number referenced a line in the VRML file when viewed in a text editor. The line corresponded to the color index in the file, and that was where the red–green–blue (RGB) values of each facet were stored. The simulation maximum stress values and units of measure were converted into binary values and stored in the VRML file. The binary values replaced the digits that came after the decimal for the green intensity value in the color index, as in Figure 4(p).

Threat scenario. The attack depicted a malicious reduction in the structural integrity of a part. An adversary can access design files and inject defects into a model that carry through to the manufacturing stage. If the defects are not detected, production parts will be flawed and potentially malfunction. The blue team used this challenge to assess the effectiveness of storing simulation data within design files. The set of original simulation results hidden in the design file could be retrieved to verify the integrity of the component.

Attacks. Only one team was able to follow the clues in the VRML file, which led its members to the line containing the binary values. It successfully determined the value of the maximum stress in the part simulation. Two teams followed a different approach of conducting a new simulation to obtain the maximum stress value. They had to generate a new CAD file because they could not use the deformed model in their analyses. It was difficult to perform the simulation because there was a lot of missing information about the input data. The teams had to guess the applied load, material, and correct fixtures.

A team of computer science students realized that the file stored the RGB value of each facet and that the maximum stress values corresponded to the red facets. It located two color indices that were red in the VRML file. It tried to relate them to other information, with the hope of obtaining the maximum stress. While the team failed to uncover any further helpful information within the time constraints, this was a very creative approach.

Statistics

Twenty-four red teams registered to compete in challenge 3 of the 2019 Hack3D. Each team had two–four students who were pursuing a degree in mechanical engineering, computer science, or computer engineering. Five teams advanced to the final round. In 2020 Hack3D qualifying challenge 5, 43 teams from around the globe registered to compete. We expect to see increasing international participation in future Hack3D competitions. As more teams participate, blue team organizers can compile innovative attacks and benchmarks to evaluate security methods and uncover new attack vectors through crowdsourcing.

Lessons learned

Table 1 lists the challenges to the threat taxonomy and summarizes participants' skill sets. By analyzing the performance of the blue and read teams, the following lessons were learned:

1. *More information can be extracted from leaked files than anticipated*: For example, in Hack3D challenge 3, one team looked in the metadata of the corrupted G-code and extracted valuable information. In challenge 5, one team discovered information about the software and the designer who created the original CAD file.
2. *Prior 3D printing and CAD experience can be advantageous in reverse engineering attacks*: In Hack3D challenge 2, past experience with 3D printing helped the red teams. Theoretically,

there are around 50 million possible angle combinations, but an attacker with rich printing knowledge can quickly rule out many of them. In challenge 4, the red teams' individual design experience led to different male connector CAD models.

3. *Hackers need not necessarily be experts in DM to launch successful attacks*: In Hack3D challenge 1, commercial CAD software and add-ins gave participants without any experience an advantage. Software can aid attackers in reverse engineering situations.
4. *Multidisciplinary knowledge and skills are useful from attackers' and defenders' perspectives*: Although one does not need a deep understanding of cybersecurity to launch an attack on DM systems and supply chains, more sophisticated and novel attacks can be developed if one combines knowledge and expertise from different disciplines, such as computer science, electrical engineering, mechanical engineering, and material science. This is also why Hack3D challenges strongly encourage participants with different technical backgrounds to join forces and form cross-disciplinary teams. The skills employed by the teams in the attacks are listed in Table 1.
5. *Attacks are not created equal*: Each Hack3D challenge asks participants to achieve the same attack goal, so all successful attacks achieve the same purpose. However, since participants tackle a problem from various angles, the attacks they develop require different countermeasures. For example, reverse engineering can be thwarted by design obfuscation, and secret file leakage requires stronger access control and authentication in an IT system.
6. *Attacks can originate in any stage in the DM supply chain*: Hack3D challenges show that bad actors can launch attacks at any stage in the DM supply chain, including STL files, IGES files, G-code files, and physical prints. DM security researchers should design and deploy security measures to protect the DM supply chain end to end.
7. *The taxonomy outlines numerous defenses and attack pathways*: During three years of Hack3D events, we explored a small set of pathways through the taxonomy. We exhort the emerging manufacturing cybersecurity community to study the unexplored threat taxonomy pathways. The NYU Center for

TABLE 1. A summary of attack methods proposed by Hack3D teams.

	Threat taxonomy (goal/method/target)	Countermeasure	Information exploited	Red team skills
Challenge 1	Counterfeit/reverse engineer/CAD (point cloud)	Obfuscation	Geometric information	Reverse engineering
Challenge 2	Sabotage/tamper with data/STL	Obfuscation	Geometric information and printing parameters	CAD and 3D printing
Challenge 3	Sabotage/tamper with data/G-code	Authentication	Metadata of G-code and geometric information hidden code	Image processing, file manipulation, and CAD
Challenge 4	Counterfeit/reverse engineer/CAD (physical print)	Fingerprinting	Physical measurements hidden code	CAD file manipulation and 3D printing
Challenge 5	Counterfeit/reverse engineer/CAD (IGES)	Obfuscation	Geometric information hidden code	CAD
Challenge 6	Sabotage/tamper with data/STL (simulation)	Authentication	Geometric information, simulation information, and hidden code	CAD file manipulation and FEA

Cybersecurity will continue to do so in future Hack3D challenges.

8. *There is a huge space for attackers to explore and exploit*: Hack3D challenges follow the philosophy in Forbes et al.,[13] and they were designed to unleash the imagination of attackers. Only attack targets are defined by each challenge, and participants are free to find their own way to accomplish their goals. Participants often surprise challenge designers with their creative attacks. For example, information leakage from metadata in a G-code file was unexpected.

Securing the DM CPS is a challenging task. We conduct an annual crowdsourcing red team/blue team event to assess the strength of DM security methods and discover novel attacks. While it is in its formative years, Hack3D shows that red teams with a range of skills—and with minimal knowledge of DM and cybersecurity—can develop attacks that defeat embedded security. The defenses and attacks can be used to benchmark future versions for the DM community. The approaches documented by Hack3D offer insights into the next generation of DM security methods and their application. Consistently, we notice that red team participants obtain more information from artifacts than we anticipate, informing effective attacks. Despite a stringent timeline for solving the challenges, the red teams make significant advances, and many succeed. Clearly, multidisciplinary training is important if the emerging DM workforce is to develop unique security methods for the DM CPS. Otherwise, security personnel may not anticipate many impending attack vectors.

Hack3D will continue in fall 2021, and we project that more than 60 teams (and 180 students) will participate. Future challenges will investigate unexplored pathways through the DM threat taxonomy. All benchmarks (https://github.com/CSAWHACK3D/Competition) from the challenges can be used by the DM community to improve defenses and train the next generation of DM security practitioners. From our experience with organizing CSAW capture-the-flag and embedded security challenges,[14] we are optimistic that Hack3D attacks and defenses will become the basis for an open, accessible benchmark resource that the DM community can use, add to, and improve.

ACKNOWLEDGMENTS

Hack3D events are supported by National Science Foundation Secure and Trustworthy Computing grant DGE-1931724. Chenglu Jin was supported by the NYU Center for Cybersecurity and NYU Center for Urban Science and Progress. The views presented in this article are those of authors, not of any funding agency. We thank NYU Tandon Makerspace for supporting Hack3D. We thank the red teams and judges for participating.

REFERENCES

1. S. E. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, and R. Karri, "Manufacturing and security challenges in 3D printing," *J. Minerals, Metals Mater. Soc.*, vol. 68, no. 7, pp. 1872–1881, 2016. doi: 10.1007/s11837-016-1937-7.
2. P. Mahesh et al., "A survey of cybersecurity of digital manufacturing," *Proc. IEEE*, vol. 109, no. 4, pp. 495–516, 2021. doi: 10.1109/JPROC.2020.3032074.
3. L. D. Sturm, C. B. Williams, J. A. Camelio, J. White, and R. Parker, "Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .STL file with human subjects," *J. Manuf. Syst.*, vol. 44, pp. 154–164, July 2017. doi: 10.1016/j.jmsy.2017.05.007.
4. L. J. Wells, J. A. Camelio, C. B. Williams, and J. White, "Cyber-physical security challenges in manufacturing systems," *Manuf. Lett.*, vol. 2, no. 2, pp. 74–77, 2014. doi: 10.1016/j.mfglet.2014.01.005.
5. H. Vincent, L. Wells, P. Tarazaga, and J. Camelio, "Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems," *Procedia Manuf.*, vol. 1, pp. 77–85, Oct. 2015. doi: 10.1016/j.promfg.2015.09.065.
6. D. B. Kim, P. Witherell, R. Lipman, and S. C. Feng, "Streamlining the additive manufacturing digital spectrum: A systems approach," *Additive Manuf.*, vol. 5, pp. 20–30, Jan. 2015. doi: 10.1016/j.addma.2014.10.004.
7. M. Yampolskiy, T. R. Andel, J. T. McDonald, W. B. Glisson, and A. Yasinsac, "Intellectual property protection in additive layer manufacturing: Requirements for secure outsourcing," in *Proc. 4th Program. Protection Reverse Eng. Workshop*, ACM, 2014, pp. 1–9. doi: 10.1145/2689702.2689709.
8. C. M. McNulty, N. Arnas, and T. A. Campbell, "Toward the printed world: Additive manufacturing and implications for national security," DTIC Document, National Defense Univ., Washington, D.C., Defense Horizons 73, 2012.
9. F. Chen, G. Mac, and N. Gupta, "Security features embedded in computer aided design (CAD) solid

ABOUT THE AUTHORS

MICHAEL LINARES is a mechanical engineering undergraduate in the Tandon School of Engineering, New York University, Brooklyn, New York, 11201, USA. His research interests include novel methods of protecting the additive manufacturing industry. Contact him at michael.linares@nyu.edu.

NISHANT ASWANI is a first-year doctoral candidate at New York University Abu Dhabi, Abu Dhabi, United Arab Emirates. His research interests include 3D modeling problems, continual learning, and autonomous systems. Contact him at nishantaswani@nyu.edu.

GARY MAC is a doctoral student of mechanical and aerospace engineering in the Tandon School of Engineering, New York University, Brooklyn, New York, 11201, USA. His research interests include digital manufacturing security and developing secure and trustworthy computer-aided design files to counter threats in the 3D printing process chain. Mac received an M.S. in mechanical engineering from New York University. Contact him at gm1247@nyu.edu.

CHENGLU JIN is a tenure-track researcher in the Computer Security Group, CWI Amsterdam, Amsterdam, 1098 XG, The Netherlands. His research interests include cyberphysical system security, hardware security, and applied cryptography. Jin received a Ph.D. from the University of Connecticut. Contact him at chenglu.jin@cwi.nl.

FEI CHEN received a Ph.D. in mechanical engineering from New York University, Brooklyn, New York, 11201, USA. Her research interests include additive manufacturing security, including secure CAD model files and embedded codes for product authentication. Contact her at fionachane@gmail.com.

NIKHIL GUPTA is a professor of mechanical and aerospace engineering in the Tandon School of Engineering, New York University (NYU), Brooklyn, New York, 11201, USA. He is also affiliated with the NYU Center for Cybersecurity. His research interests include cybersecurity and machine learning in manufacturing. Gupta received a Ph.D. in mechanical engineering from Louisiana State University. He is a Senior Member of IEEE. Contact him at ngupta@nyu.edu.

RAMESH KARRI is a professor of electrical and computer engineering in the Tandon School of Engineering, New York University (NYU), Brooklyn, New York, 11201, USA. He codirects and cofounded the NYU Center for Cybersecurity. His research interests include hardware cybersecurity; processors and cyberphysical systems; security-aware computer-aided design, test, verification, validation, and reliability; nano meets security; and hardware security competitions, benchmarks and metrics. Karri received a Ph.D. from the University of California, San Diego. He is a Fellow of IEEE. Contact him at rkarri@nyu.edu.

models for additive manufacturing," *Mater. Des.*, vol. 128, no. 1, pp. 182–194, 2017. doi: 10.1016/j.matdes.2017.04.078.

10. F. Chen, Y. Luo, N. G. Tsoutsos, M. Maniatakos, K. Shahin, and N. Gupta, "Embedding tracking codes in additive manufactured parts for product authentication," *Adv. Eng. Mater.*, vol. 21, no. 4, p. 1,800,495, 2019. doi: 10.1002/adem.201800495.
11. F. Chen, J. H. Yu, and N. Gupta, "Obfuscation of embedded codes in additive manufactured components for product authentication," *Adv. Eng. Mater.*, vol. 21, no. 8, p. 1,900,146, 2019. doi: 10.1002/adem.201900146.
12. N. Gupta, A. Tiwari, S. T. Bukkapatnam, and R. Karri, "Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks," *IEEE Access*, vol. 8, pp. 47,322–47,333, Mar. 2020. doi: 10.1109/ACCESS.2020.2978815.
13. H. Forbes, D. Shaefer, M. N. Shergadwala, and J. H. Panchal, "Investigating the challenges of crowdsourcing for engineering design: An interview study with organizations of different sizes," in *Proc. Int. Des. Eng. Tech. Conf. Comput. Inf. Eng. Conf.*, American Society of Mechanical Engineers, 2020, vol. 83976, p. V008T08A039. doi: 10.1115/DETC2020-22466.
14. R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, "Trustworthy hardware: Identifying and classifying hardware trojans," *Computer*, vol. 43, no. 10, pp. 39–46, 2010. doi: 10.1109/MC.2010.299.