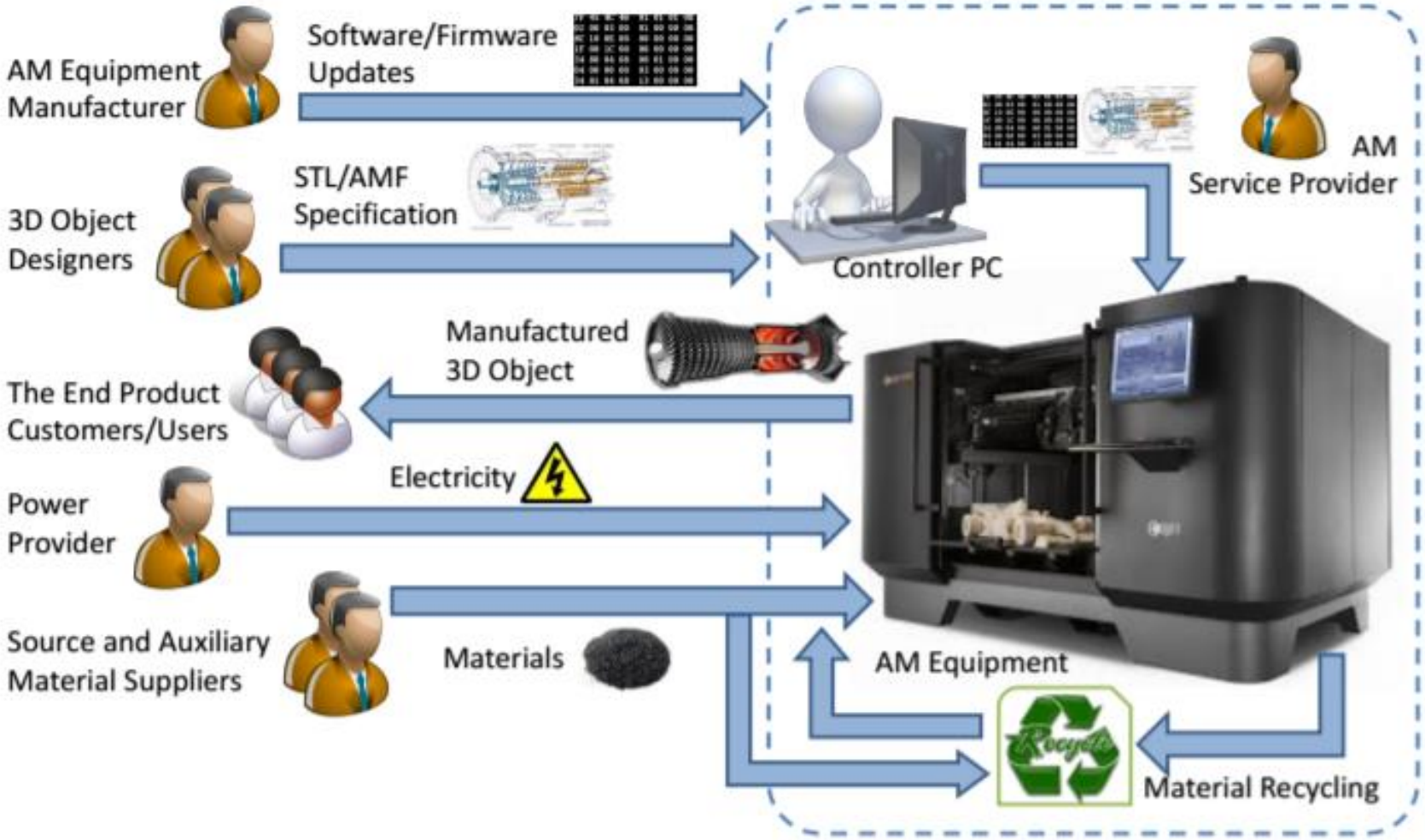
3D Printing and Cybersecurity

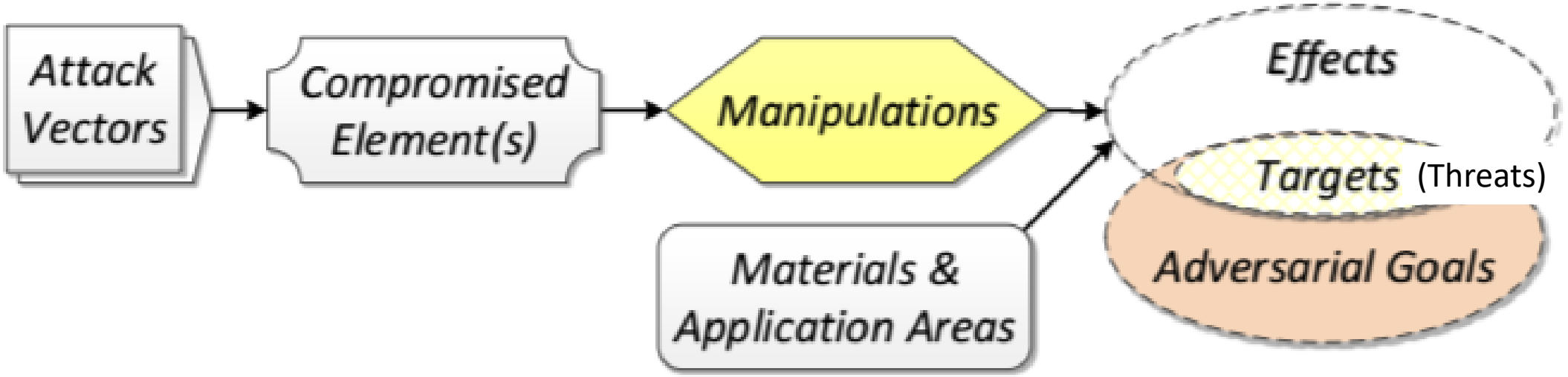
Yair Karin

Additive Manufacturing Workflow

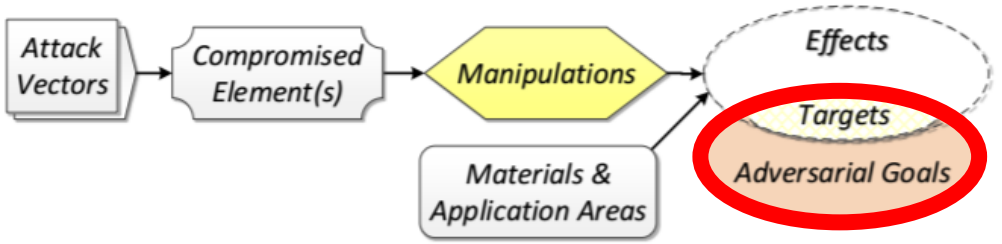


[1]

Attack on/with 3D Printer



[1]



Adversial Goals

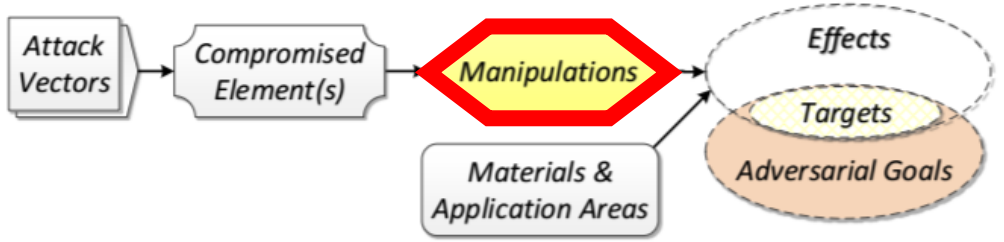
- Sabotage of manufactured part
- Sabotage of the AM printer
- Intellectual property (IP) theft

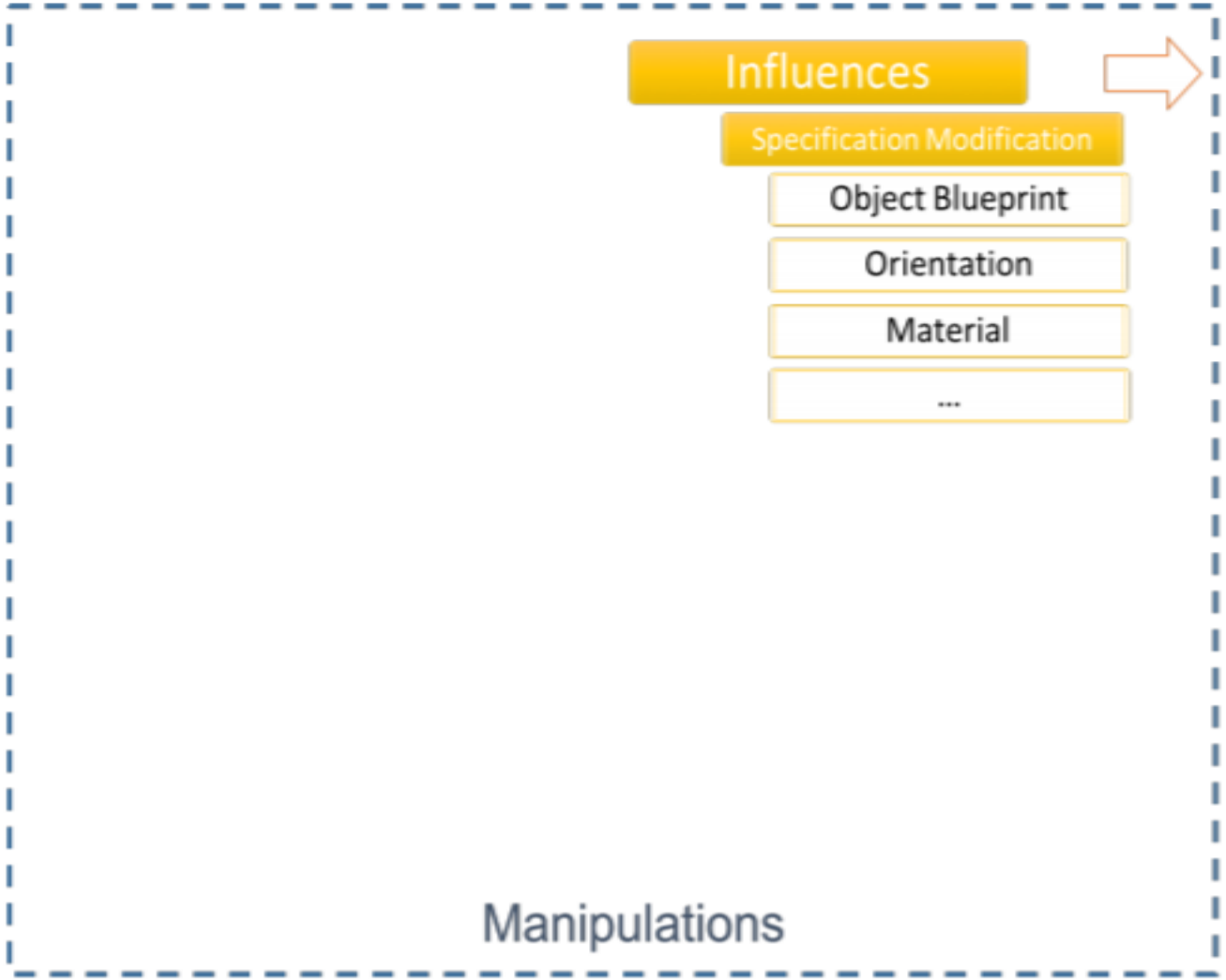
- Can you think of more?

[2]

[8]

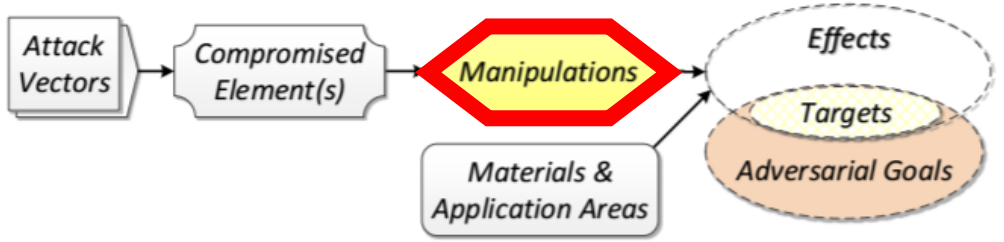
Manipulations

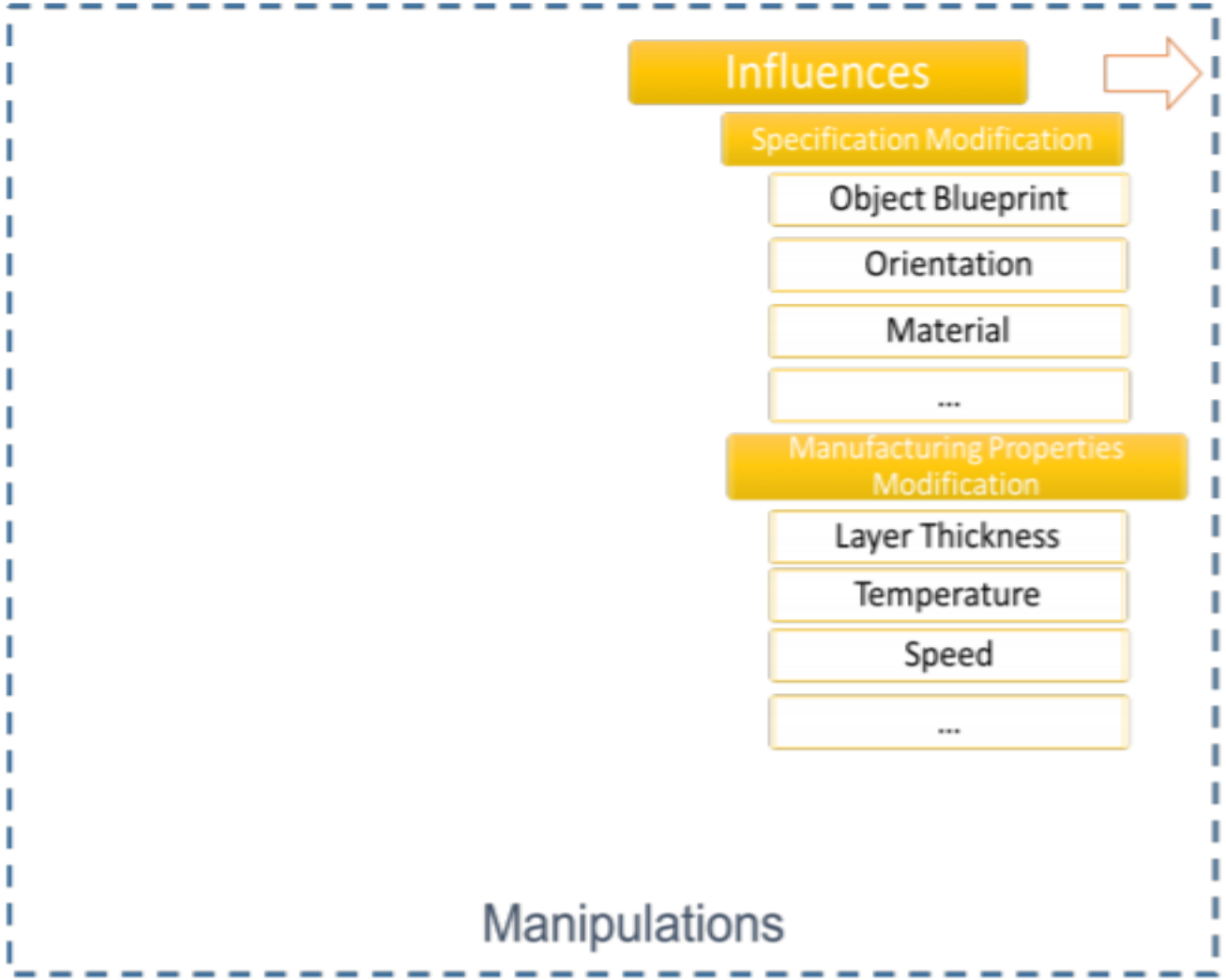




[1]

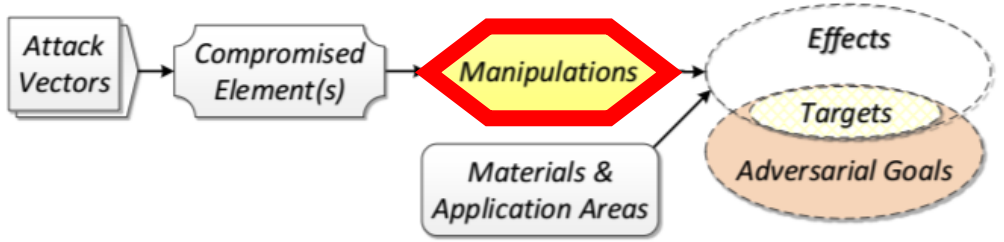
Manipulations

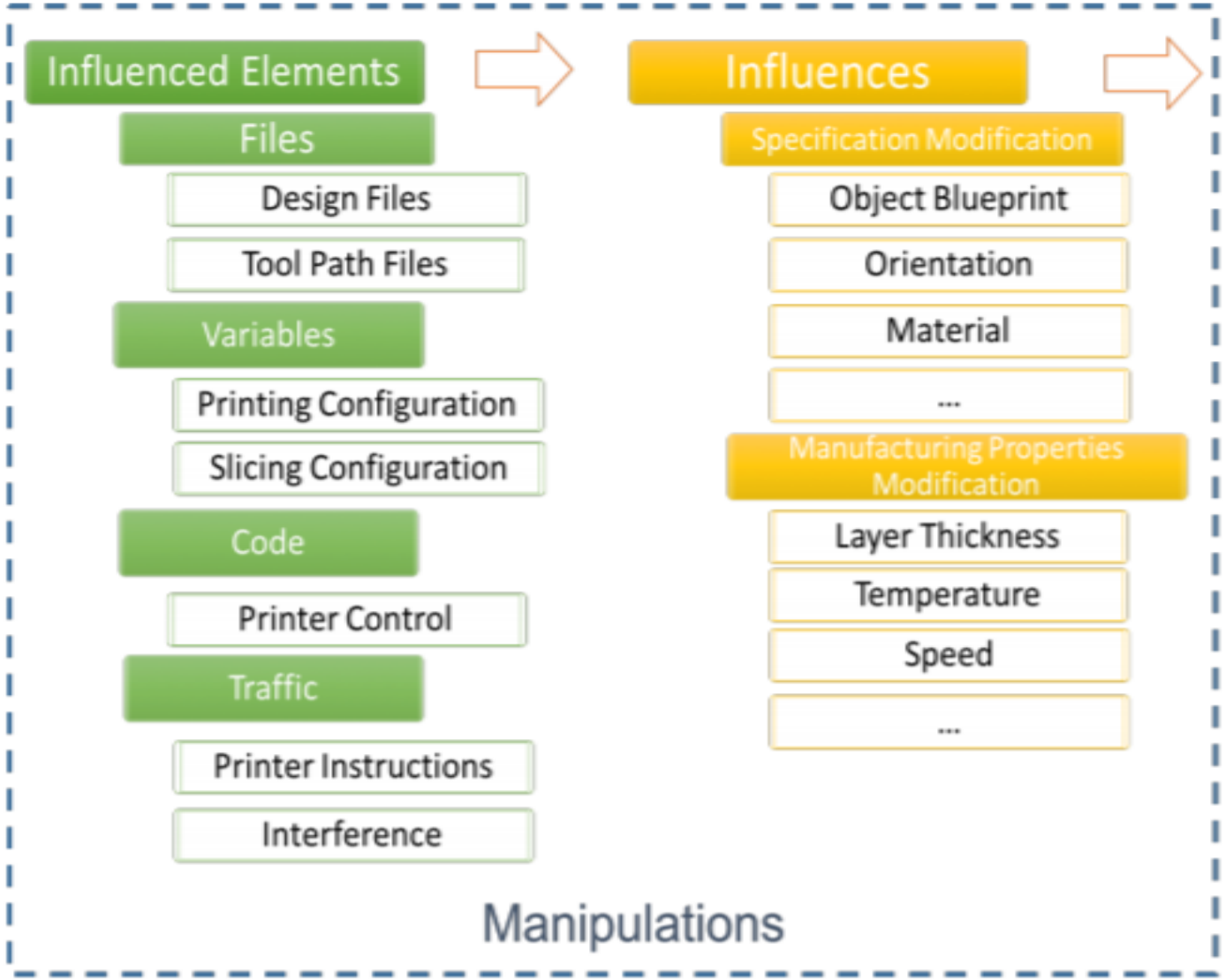




[1]

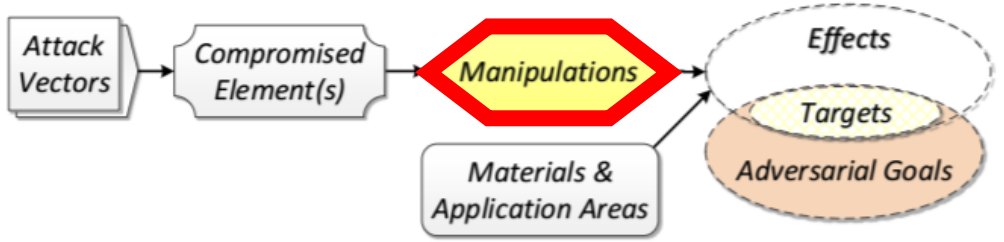
Manipulations

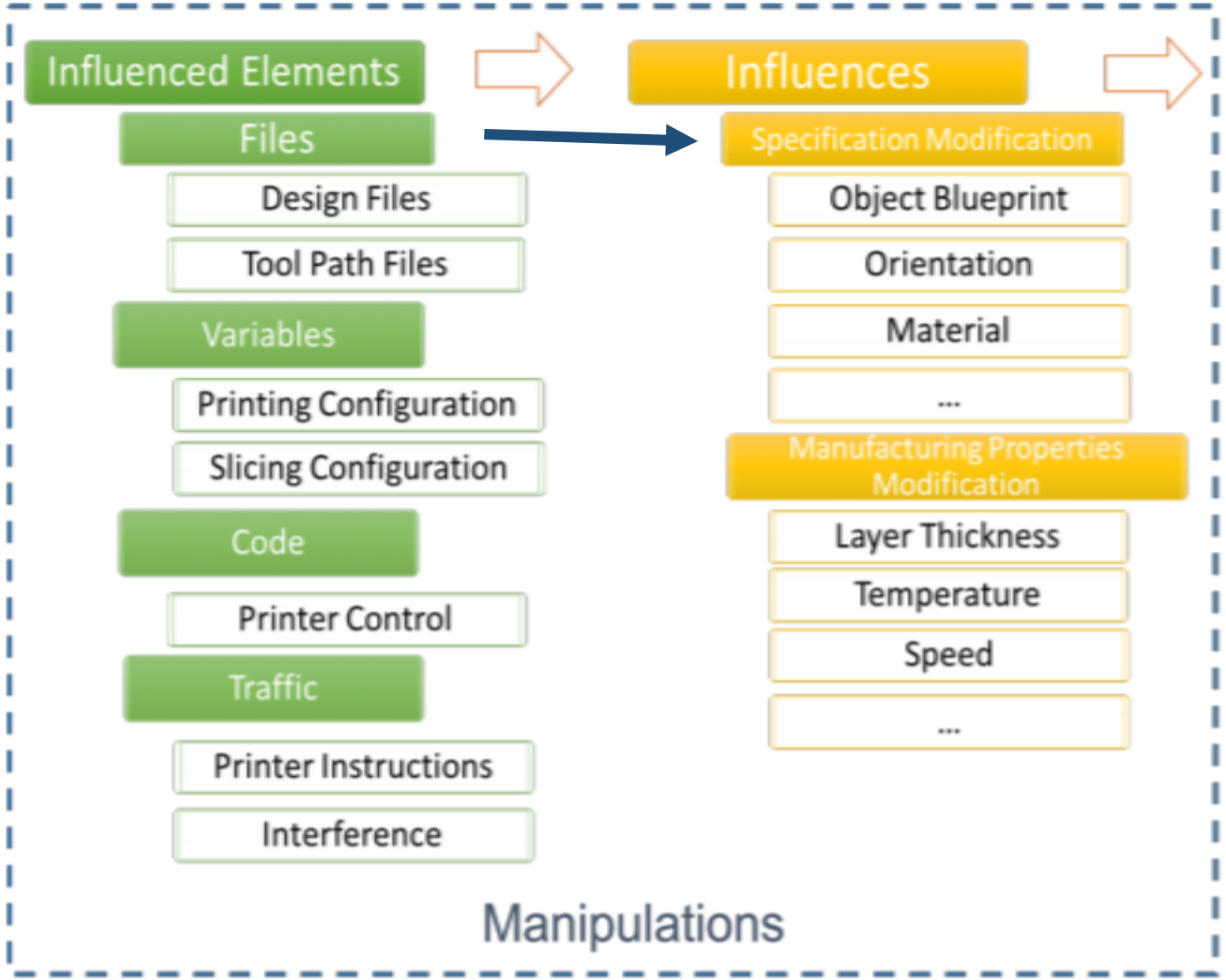




[1]

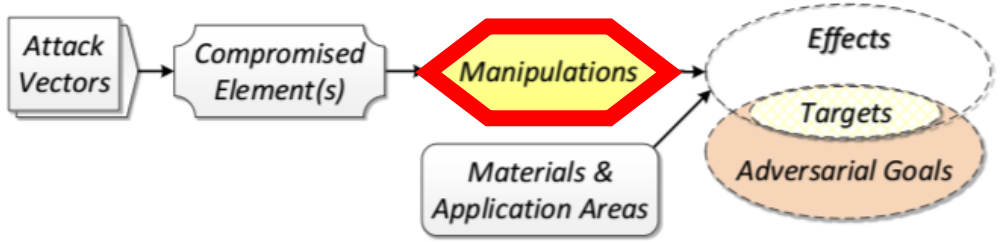
Manipulations

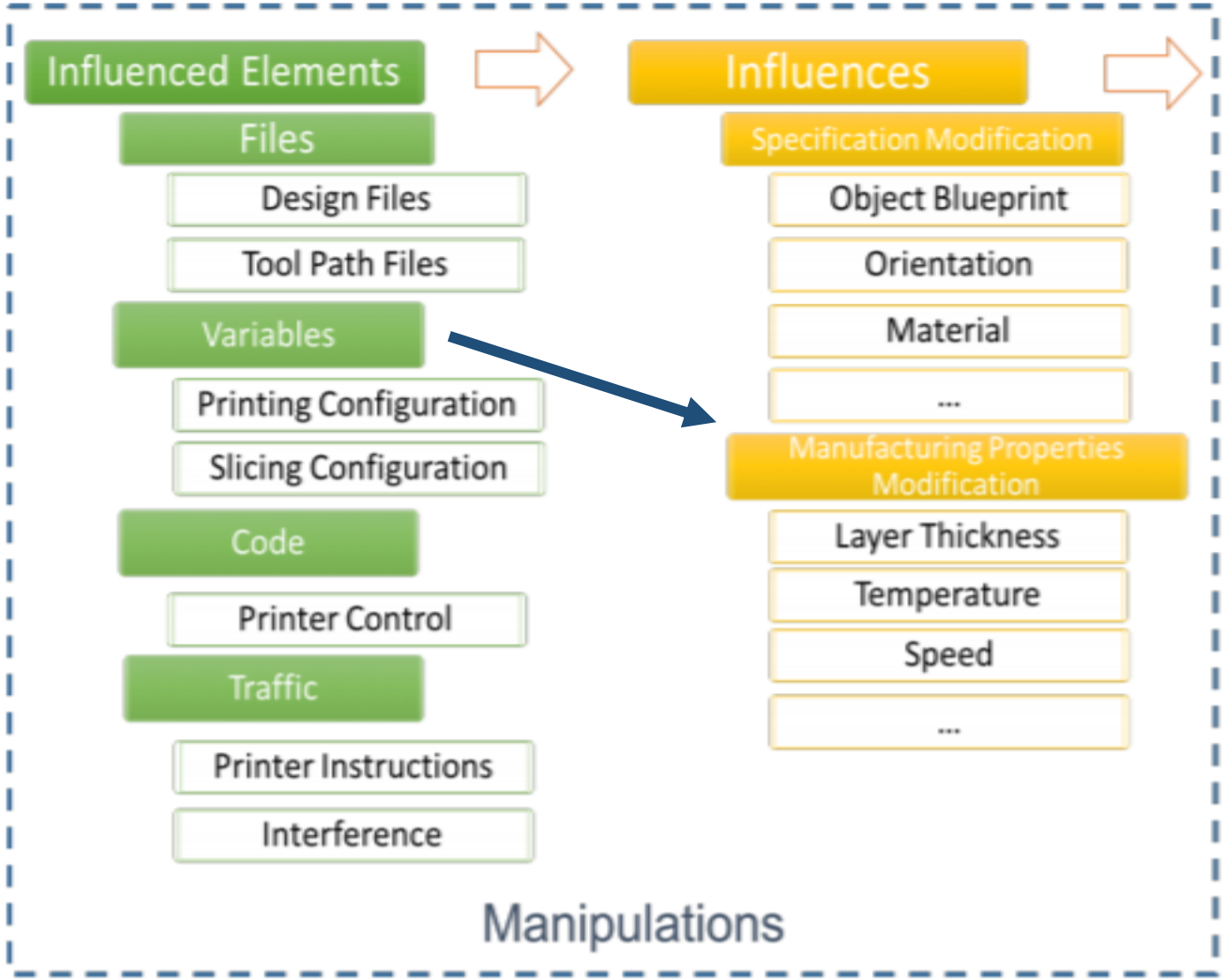




[1]

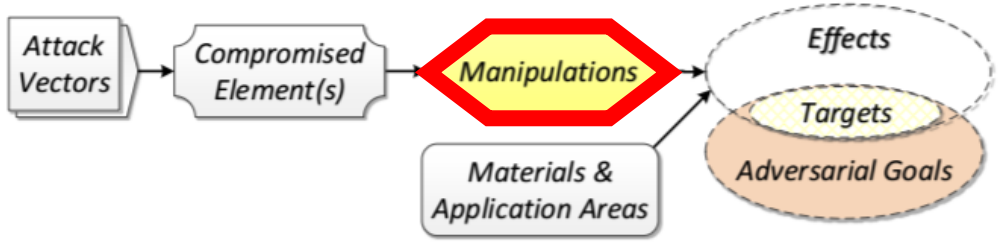
Manipulations

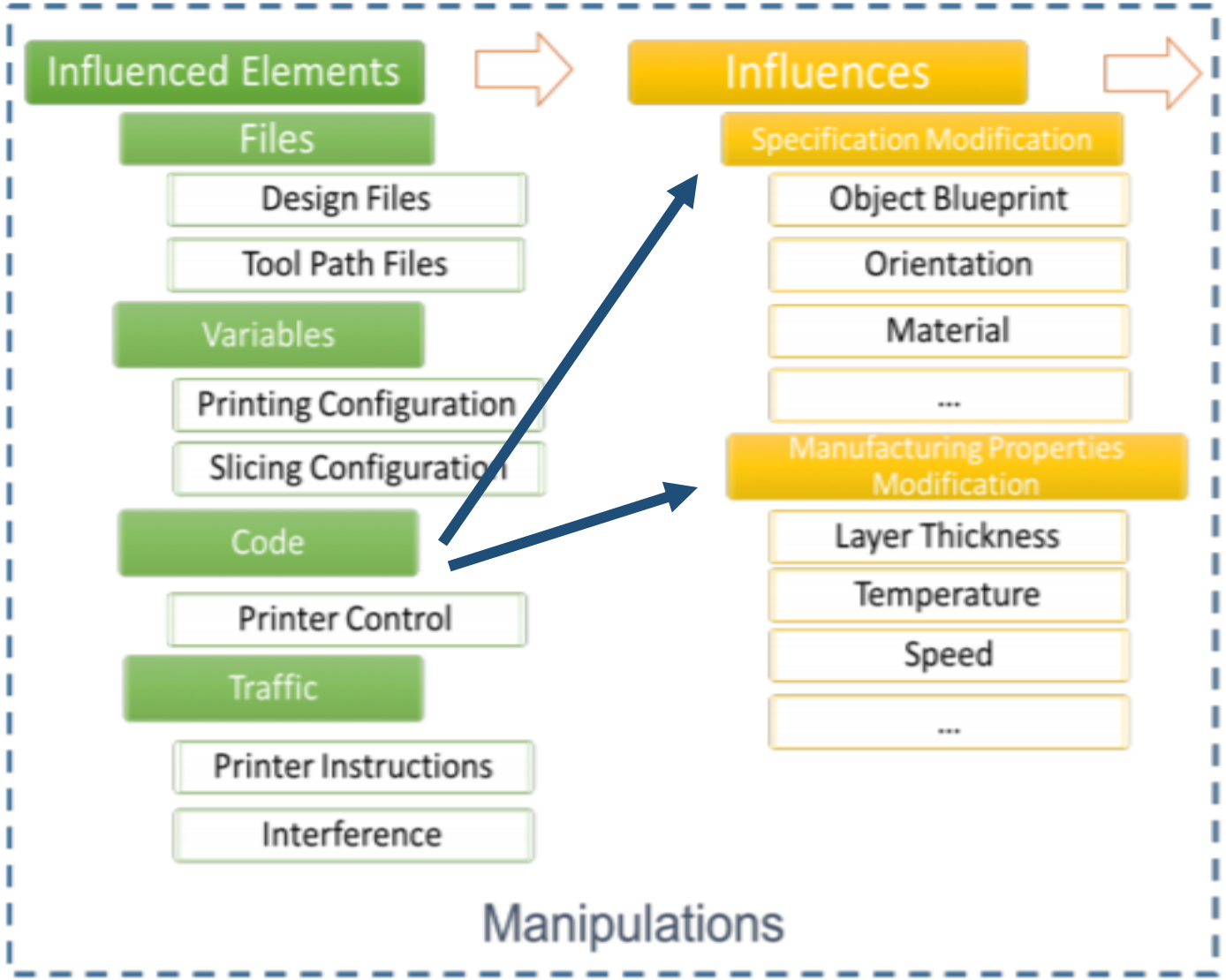




[1]

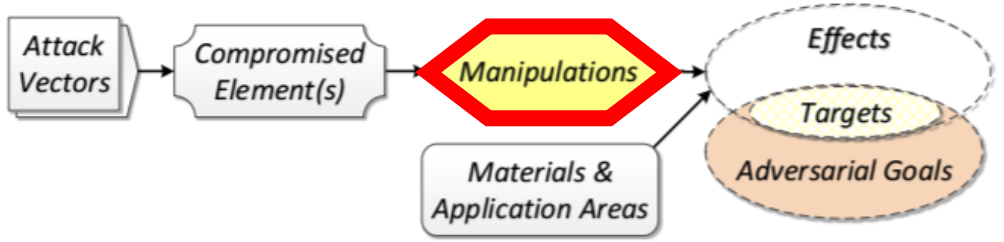
Manipulations

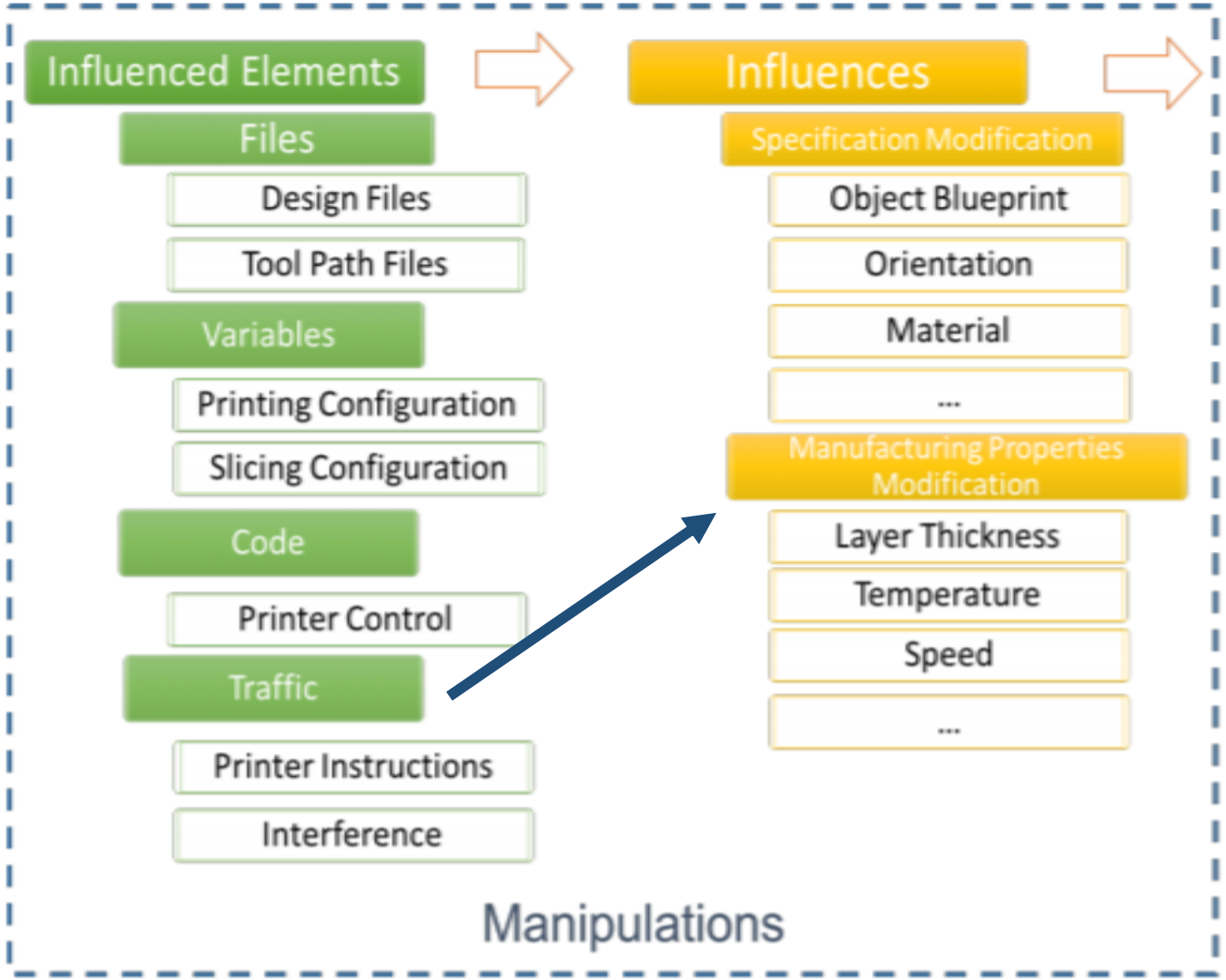




[1]

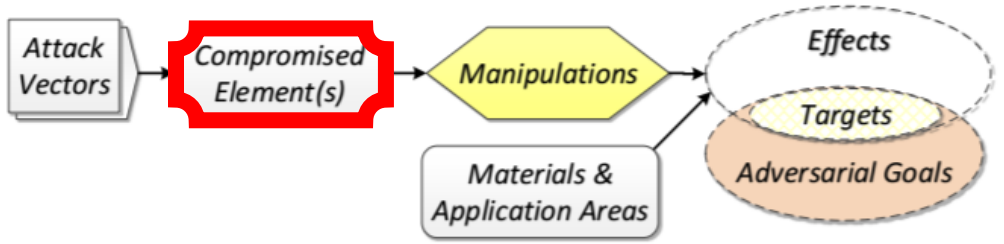
Manipulations

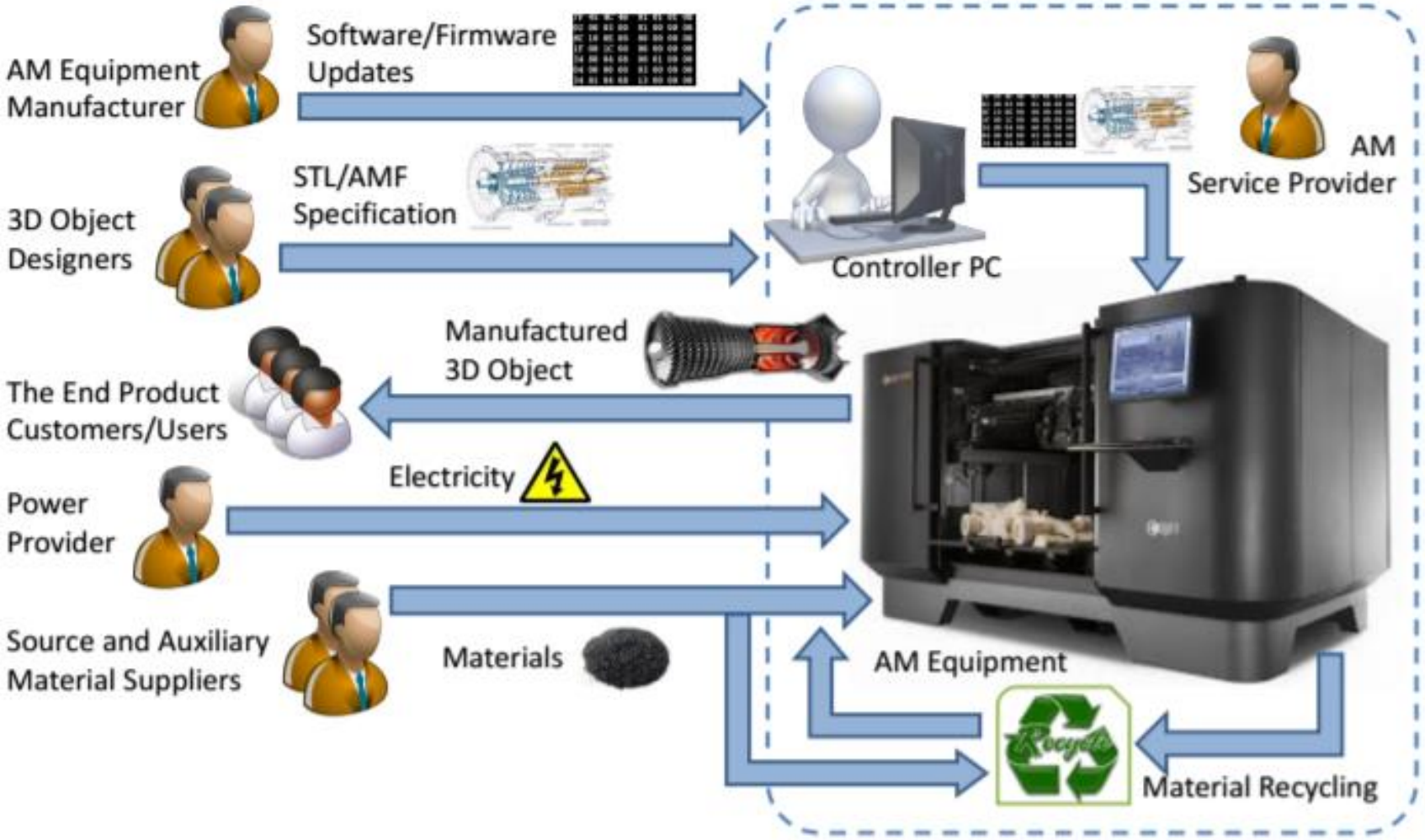




[1]

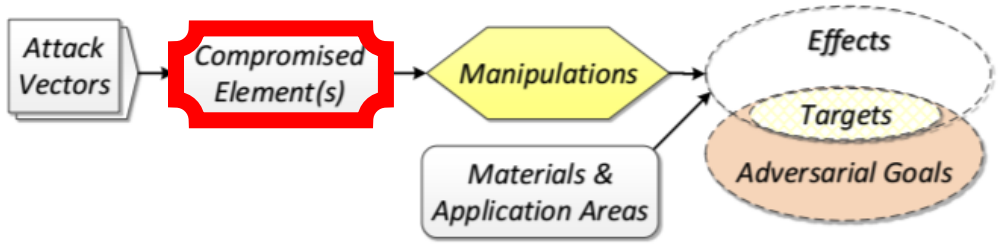
Compromised Elements

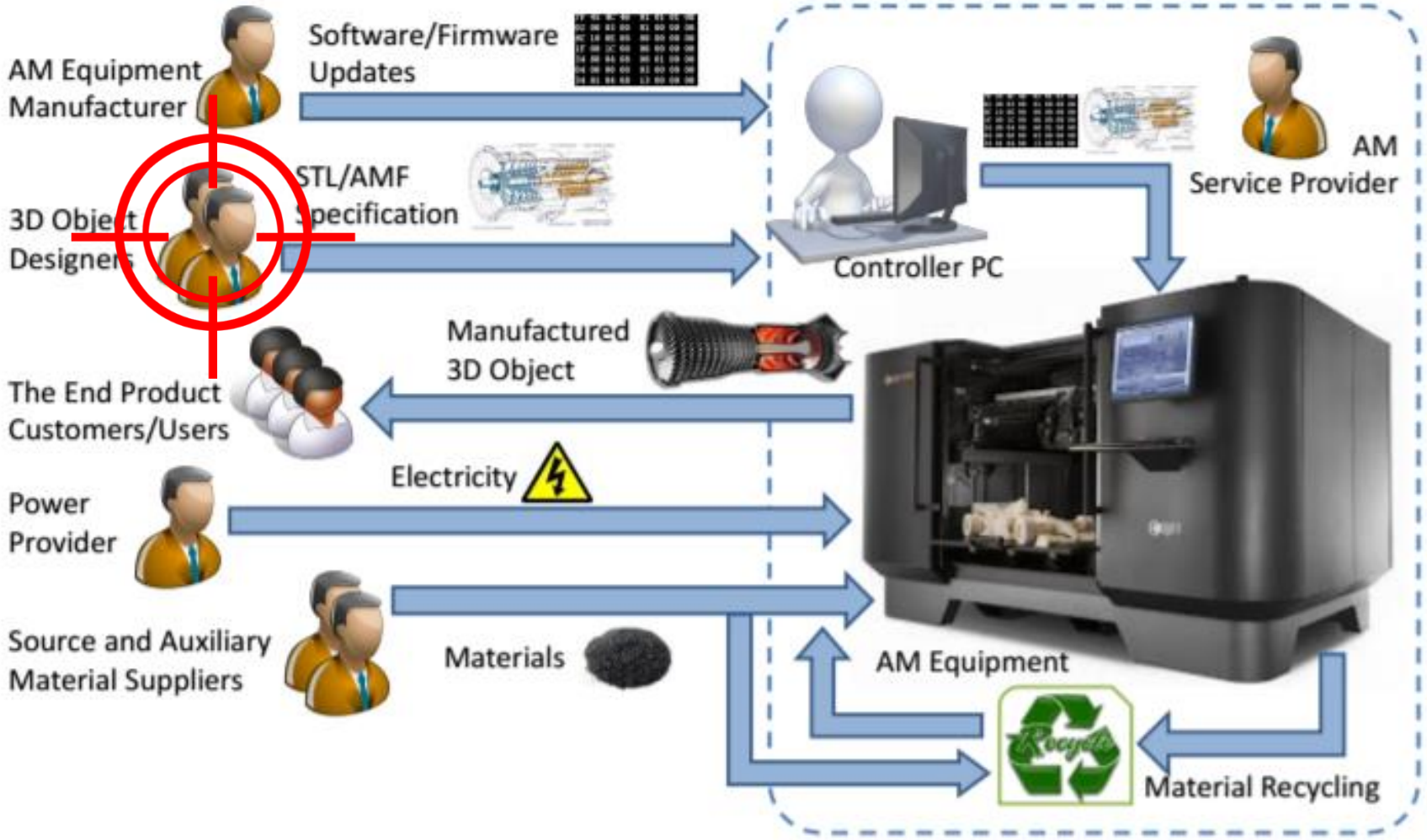




[1]

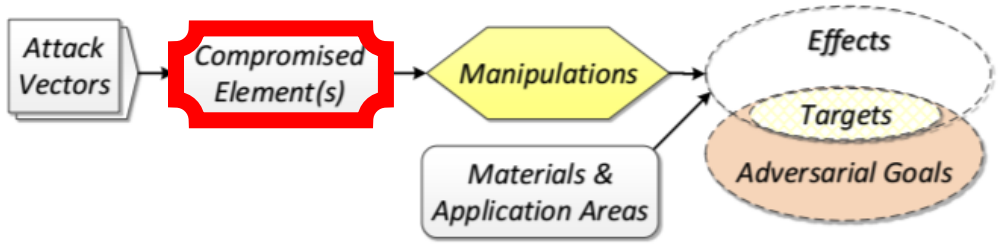
Compromised Elements

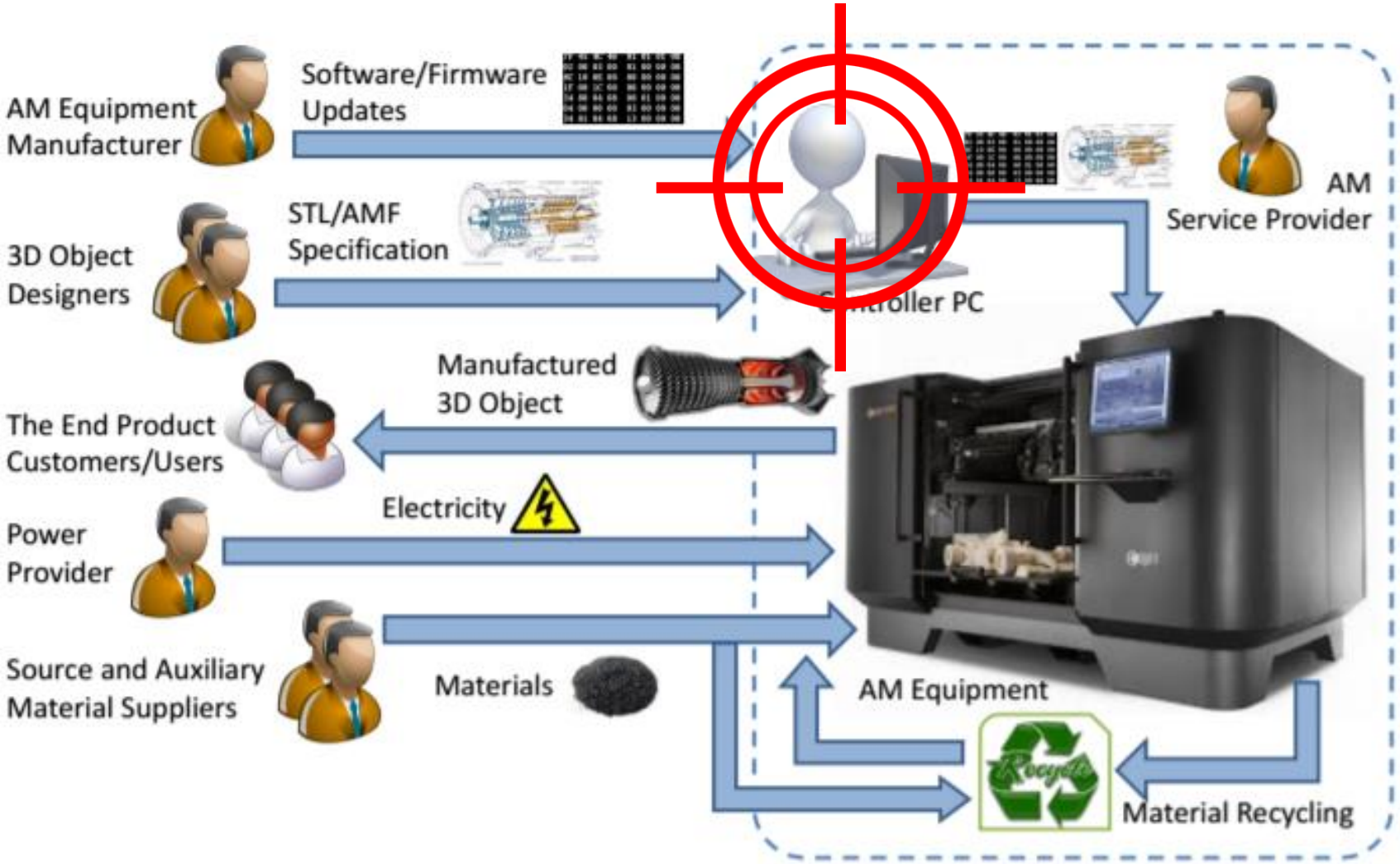




[1]

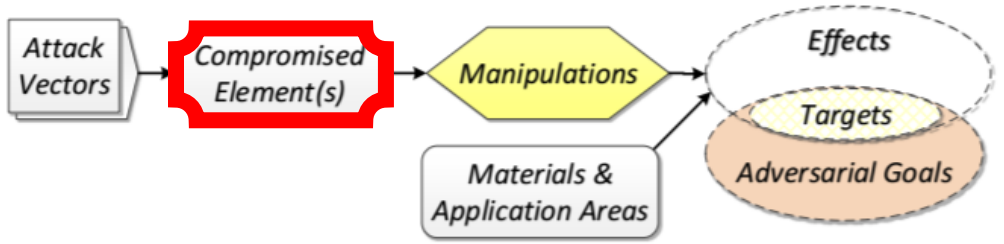
Compromised Elements

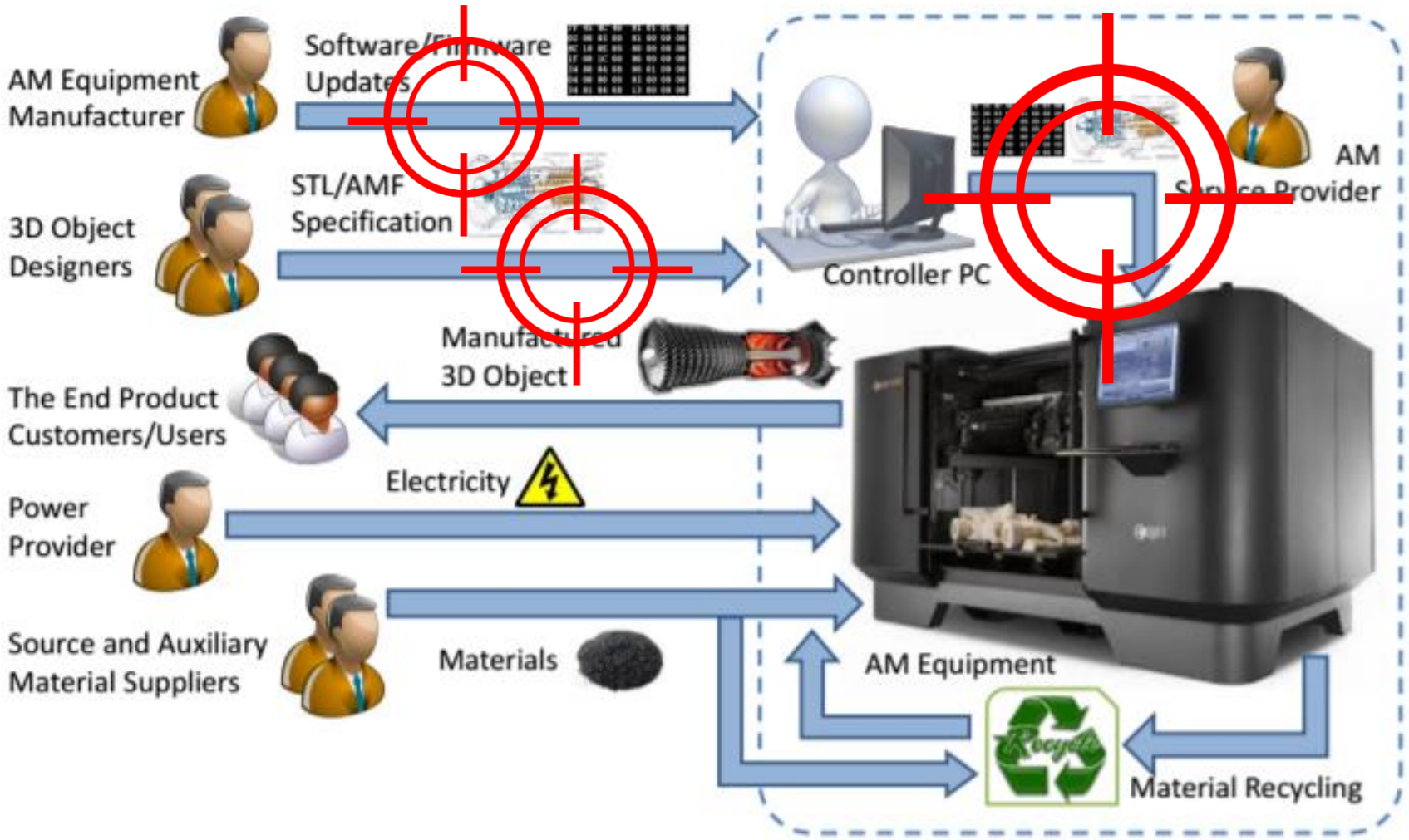




[1]

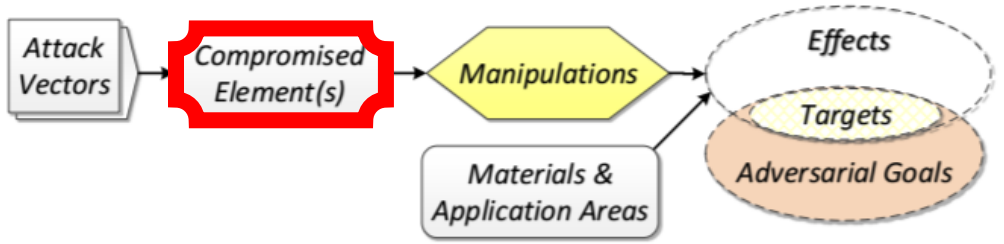
Compromised Elements

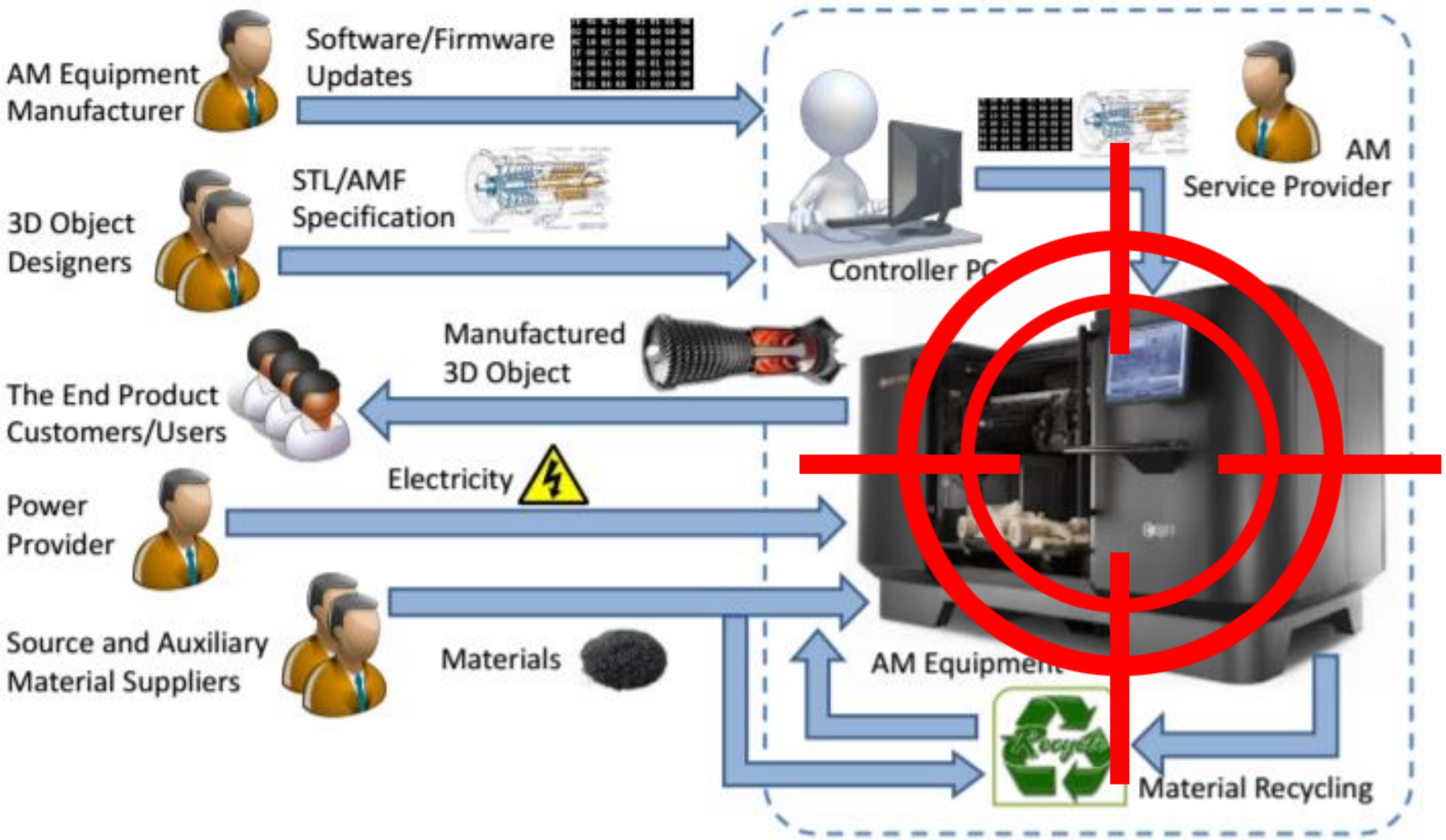




[1]

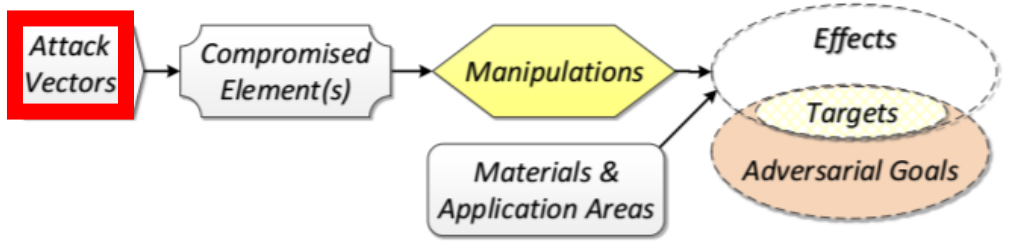
Compromised Elements



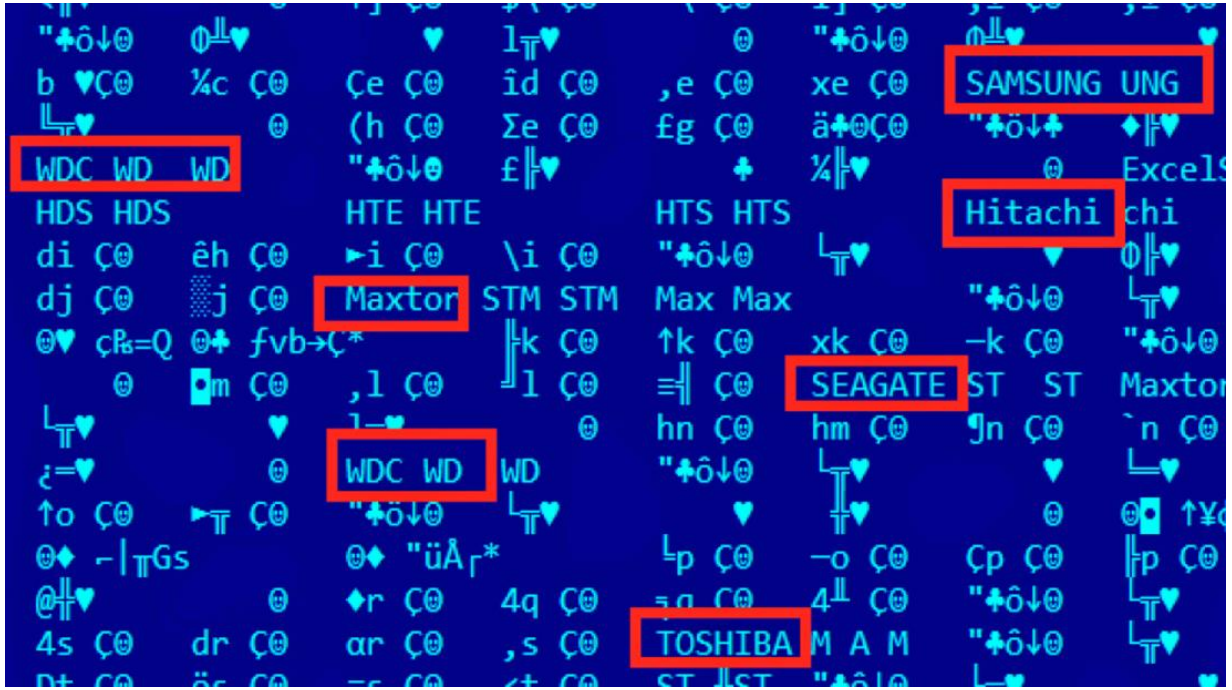


[1]

Attack Vectors



- Software Attacks:
  - General infiltration methods
  - Code injection into AM files
  - Software supply chain
- Hardware/firmware
  - Hardware trojans
  - Firmware updates
- Network
  - General network attacks
  - Protocol vulnerabilities

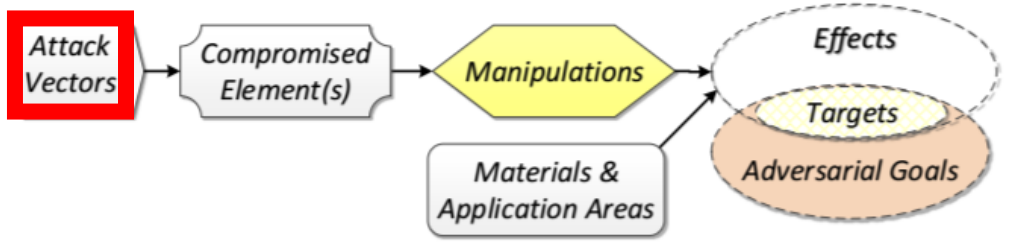


[7]

Bonus question: what is this?

And so much more…

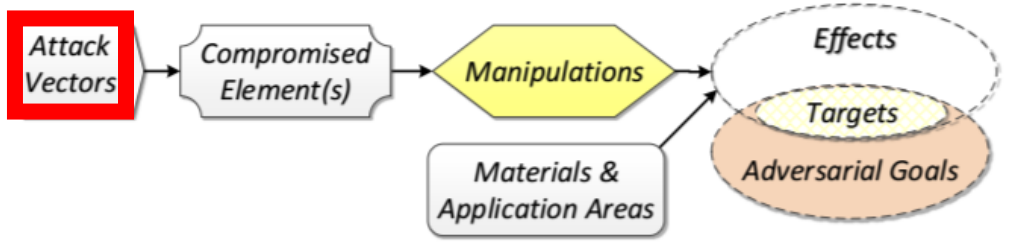
ACAD/Medre.A



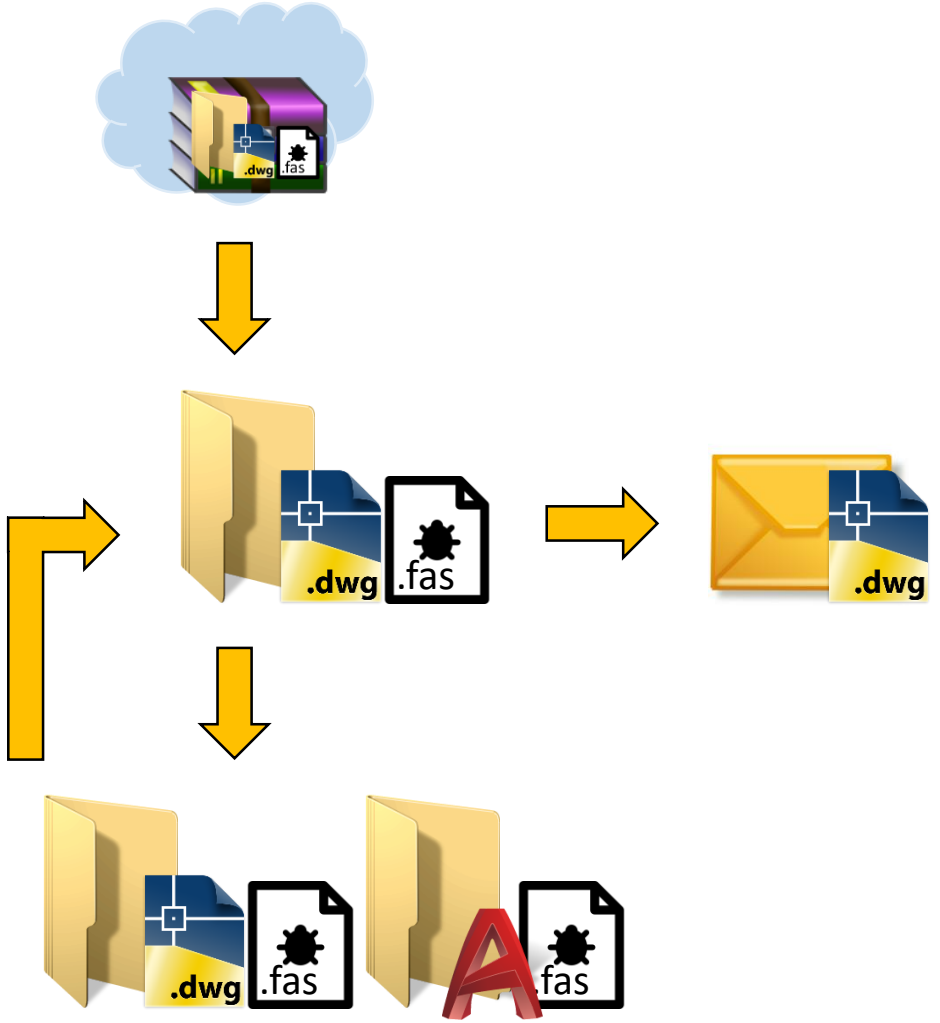
- Discovered by eset.
- Steals AutoCAD drawings.
- Written in AutoLISP.
- Over 100,000 designs leaked!

[3]
[4]
[9]

ACAD/Medre.A



1. User extracts files into directory
2. User opens the .dwg, .fas runs.
3. .fas copies itself to AutoCad directory and **current project directory** (why??).
4. .fas sends the model via email.
5. Further distribution.

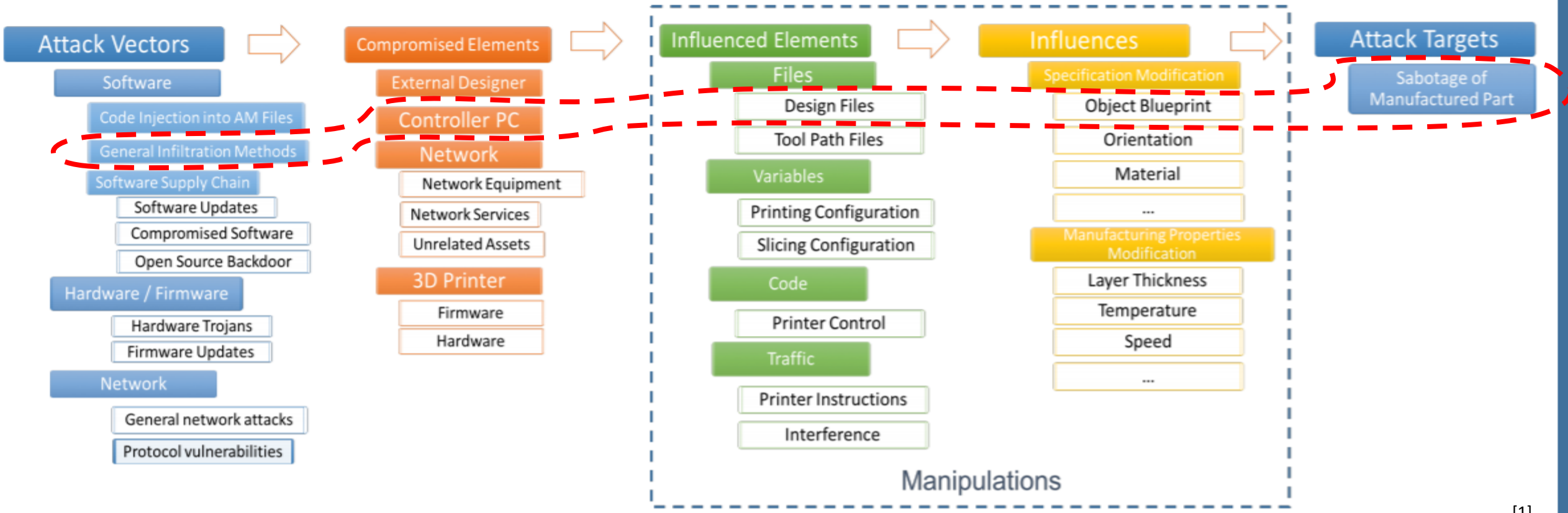


An Example – dr0wned

[5]

[6]

Attack Flow

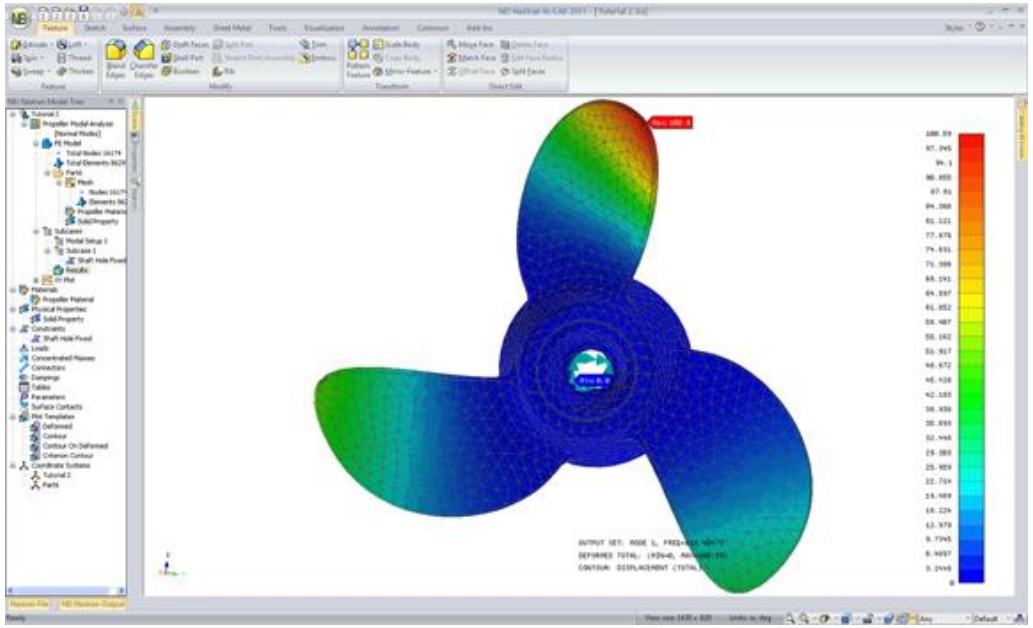


[1]

Solution?

- Methods of integrating a signature within the printed object.
- Software security of the entire 3D printing flow.
- Physical tests of the printed object.

- More research!



FEA - Finite Element Method [10]

Questions?

Bibliography

1. “dr0wned – Cyber-Physical Attack with Additive Manufacturing”. Sofia Belikovetsky, Mark Yampolskiy, Jinghui Toh, Yuval Elovici
2. http://img.etimg.com/thumb/msid-55952298,width-310,resizemode-4,imglength-102138/.jpg
3. https://www.welivesecurity.com/media_files/white-papers/ESET_ACAD_Medre_A_whitepaper.pdf
4. http://www.eset.hk/enews/autocad/en/img/autocad-02e.jpg
5. https://dronebuff.com/wp-content/uploads/2014/08/DJI-Phantom-2-Vision-Plus.jpg
6. https://www.youtube.com/watch?v=zUnSpT6jSys
7. https://cdn.arstechnica.net/wp-content/uploads/2015/02/hd-classes.jpg
8. http://gailbwilliams.co.uk/wp-content/uploads/2016/03/oh-the-horror.jpg
9. https://www.brandsoftheworld.com/sites/default/files/styles/logo-thumbnail/public/0017/8923/brand.gif?itok=FB8tX8KV
10. http://digitaleng.news/virtual_desktop/wp-content/uploads/2011/08/20110823NEi_in_CAD.jpg