INL/EXP-22-68166-Revision-0

Protecting Smart Buildings with STIG

August 2022

Faith Kimberley Coslett

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/EXP-22-68166-Revision-0

Protecting Smart Buildings with STIG

Faith Kimberley Coslett

August 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Protecting Smart Buildings with STIG

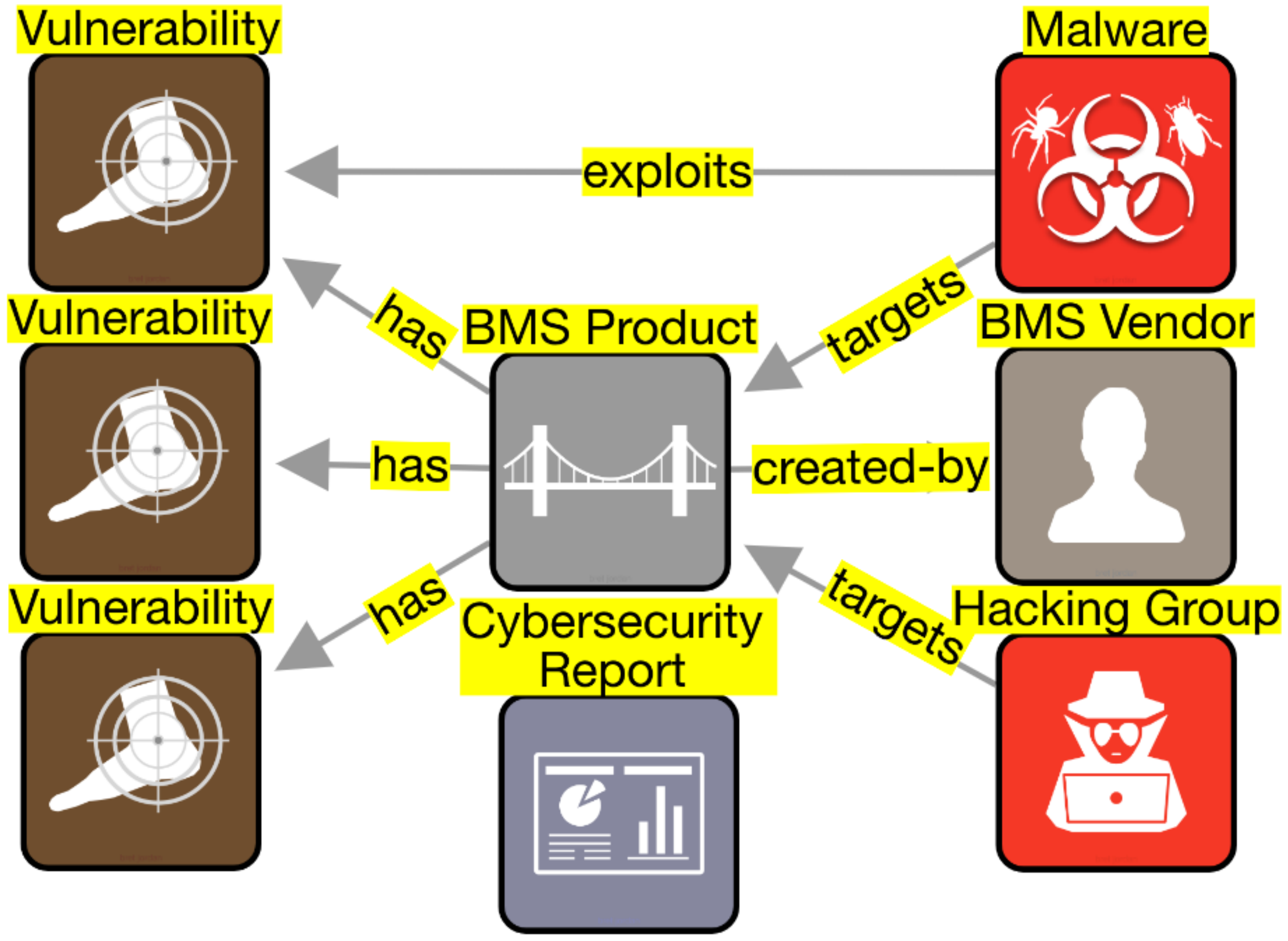
Intern: Faith Coslett (D520) | CEDAR Lab, University of Wyoming | Mentors: Rita Foster (D520), Zachary Priest (D520), Mike Borowczak (UWyo)

Problem

- Smart buildings are common now, whether they're businesses, hospitals, or homes
- They have **Building Management Systems (BMS)** that digitally control physical systems like security, HVAC, appliances, alarms, and networks
- All these can fall victim to cyber attacks
- Not only can they be controlled by hackers, but they can allow access to other devices through the **Internet of Things (IoT)**
- Attacks on BMS are getting more common and can result in hospitals shutting down, ventilation being cut off, intruders bypassing all locks, and spying in your own home
- This threat is new, so many people don't recognize the importance of good BMS defense

Goals

- Consolidate tons of BMS product and weakness information into one location
- Make BMS cybersecurity data useful and easy to share



Vulnerability

Malware

exploits

Vulnerability

has

BMS Product

targets

BMS Vendor

has

created-by

Vulnerability

has

Cybersecurity Report

targets

Hacking Group

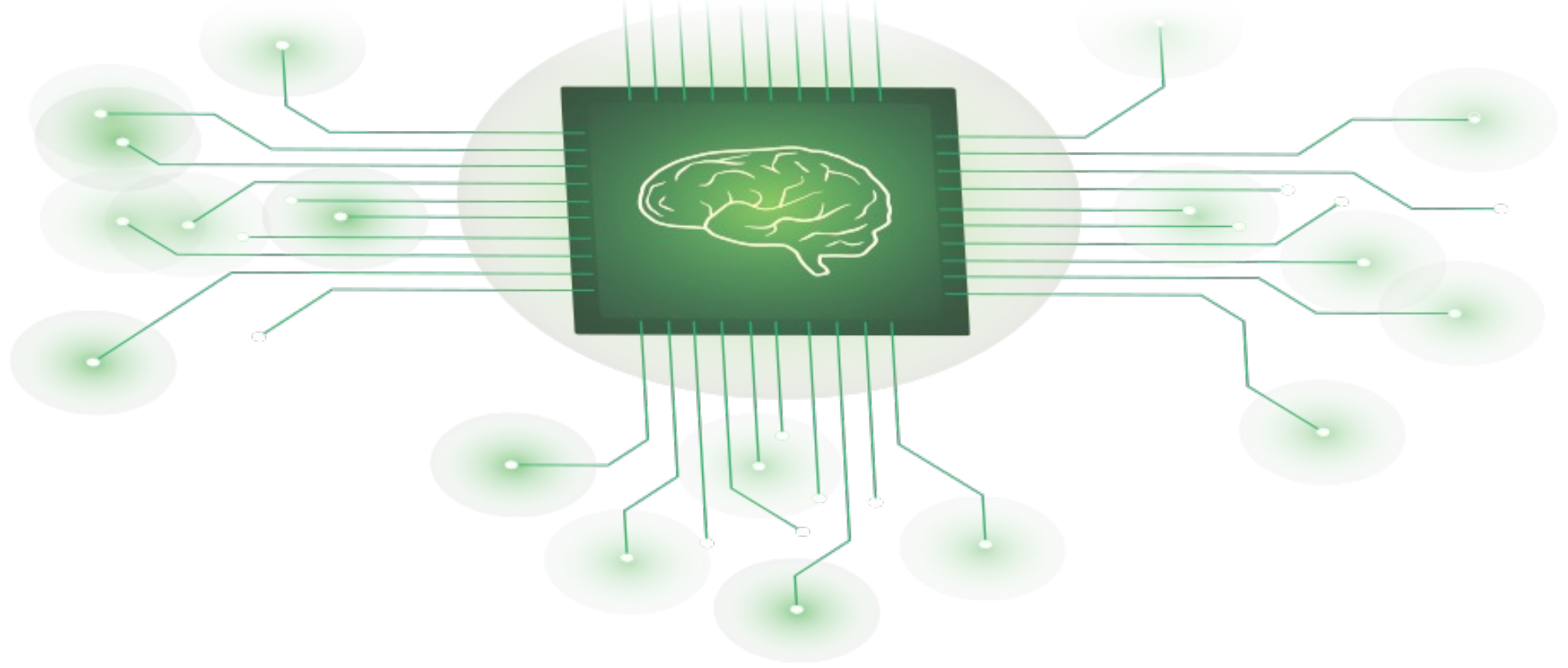
The above is a generalized STIG graph showing what one part of the real file looks like. Each icon contains inner details about the object it represents.

Solution

- Cybersecurity improvements rely on fast information sharing and responses to attacks
- **Structured Threat Intelligence Graph (STIG)** is an INL product that represents cybersecurity data from dozens of sources and thousands of words as an intuitive graph
- Graphs made in STIG create **Structured Threat Information Expression (STIX)** code, an industry standard for sharing cybersecurity info
- Creating the BMS attack surface in STIX would make it unified, actionable threat intelligence

STIG

Structured Threat Intelligence Graph



Methods

- Researched the top BMS producers and products across different sectors: residential, commercial, industrial, medical, military, and hospitality
- Found each product's history of vulnerabilities and attacks
- Created a comprehensive graph in STIG with all the information

Results

- Large visual file of where widely-used BMS technology is vulnerable
- All vendor, product, and vulnerability information collected in one place
- Since this info is in STIX, it can be shared, expanded, and automated into defense systems quickly
- This ease of analysis allows for better defenses ahead of time, faster response times to an attack, and safer product choices by customers

https://github.com/idaholab/STIG
www.inl.gov
INL/EXP-22-68166

University of Wyoming

CEDAR

INL Idaho National Laboratory