CS 542 – Introduction to Software Security
Exercise 1.3: Thinking Like an Attacker

Binhao Chen (bchen276@wisc.edu), Steven Yang (yang558@wisc.edu)

Due: 2:30pm, September 20, 2022

A. What are SCADA systems? Give three examples of "critical infrastructure" where SCADA systems are used.

SCADA systems are also known as Supervisory Control and Data Acquisition systems. They are used to allow industrial organizations to monitor, gather,and process real-time data. They can also directly interact with devices such as valves, pumps, motors, and so on.

1. Water/Wastewater management firms use SCADA systems to monitor the performance of storage tanks, pumps, and other equipment.
2. Power plants use SCADA to monitor every phase of generating electricity from fuel input to electrical output so that they are able to respond immediately to fluctuations in demand.
3. Food production uses SCADA to control the exact amount of ingredients required. It can also control the temperature and time needed to process food.

B. What is a malware "dropper"?

A malware dropper is a malicious program that contains the malware and is designed to facilitate the delivery and installation of the malware to the victims' computers or other devices in such a way as to avoid detection by the victims or the virus scanners.

C. What is a "zero day"?

The term "zero-day" refers to a kind of unidentified vulnerability that is discovered by the attackers before the victims are even aware of it, so before they can issue a patch. This is also the reason why this type of vulnerability is named "zero day" as the vendors/developers have "zero days" to fix it. Attackers can exploit it without any mitigation done by the victim.

D. What is an "air gap"?

"Air gap" is a security countermeasure based on the idea of creating an insurmountable interface between two systems (normally the digital assets we are hoping to protect and the attacks/sabotages that are generally malicious), such that there are no direct or indirect connections between them. This strategy seeks to ensure the total isolation of a given system electromagnetically, electronically, and physically. As the name suggests, the simplest form of "air gap" could be implemented by disconnecting the digital asset from any network and placing a physical distance between it and anyone who might want to access it. The "air-gapped" system should have restricted access so only a few authorized users can access the system.

E. What is an "beaconing"?

"Beaconing" is a term that refers to a continuous cadence of communication between two systems. Those communication signals periodically go between the victim's machine/device and the attacker's command-and-control server. That allows the attackers to control the malware remotely,

and then lets attackers know whether they have successfully invaded the system so they can then send commands and carry out an attack.

F. What is an "exfiltrating"?

"Exfiltrating" describes the unauthorized transfer of data from a computer or other device and either sharing it with unauthorized third parties or moving it to other systems. An attacker extracts data files from the victim's system without authorization. This is a typical case of Information Disclosure in the STRIDE model. An "exfiltrating" can be carried out manually by an individual with physical access to the data storage system, but it can also be an automated process through malicious programs over the network.

G. Describe the attack surface used in Stuxnet.

The attack surface used in Stuxnet is mainly the uncovered vulnerabilities in the industrial-control system made by the German firm Siemens. These vulnerabilities in the specific control system (Siemens' PCS 7, or Process Control System 7) are targeted by Stuxnet. The first discovered variant of Stuxnet had to be passed on a USB drive carrying an infected configuration file for Siemens controllers, where is exactly the attack surface used in Stuxnet.

H. What is different about this type of attack from previously published ones.

The most notable difference is that Stuxnet was the first targeted weaponized cyberattack against industrial control systems. Instead of simply hijacking targeted computers or exfiltrating data from the targeted systems, it escaped the digital realm to cause destruction to physical equipment/machines that are controlled by computers. Before Stuxnet, it was still widely believed that industrial systems were either immune to cyber-attacks (due to the ambiguity and isolation of systems) or would not be targeted by hackers or other cyber threats.

I. What was the goal of Stuxnet?

The goal of Stuxnet is to prevent Iran from successfully developing nuclear bombs by destroying the centrifuges that were used to enrich uranium. The small warhead is aiming at one cascade and spinning up the rotors, while the big one is aiming at six cascades and manipulating valves.

J. How did it mask its affect?

Stuxnet prerecorded the input values for the cascade protection system's sensors for a period of 21 seconds. Then it replays those 21 seconds in a constant loop during the execution of the attack. Neither human operators nor software alarms thought it was abnormal.