Legal Informatics, Privacy and Cyber Crime

Part Four: Defenses

Sandro Etalle

03/05/2018

2017/2018

BOLOGNA BUSINESS SCHOOL
Alma Mater Studiorum Università di Bologna
About this part of the course

• Topic: principles of defense techniques

• Underlying Material: This part is covered by the slides, there is no book/article to study
How can we stop/detect Cyber-Threats?

- **Type one: advanced attack** (here are the phases)
  - Phishing? Watering hole?
    - Difficult to block/detect
  - Communication with the C&C?
    - Detectable only if the workstation in question does not usually connect to the internet
  - Detection of anomalies on Internal Network behavior?: should be detectable
    - Ukraine: upload of malicious firmware to the serial-to-ethernet devices
    - Havex: detection of OPC scan
    - Stuxnet: propagation in backoffice and reprogramming of PLC

- **Type two: Careless and disgruntled employee. Vendors and outsourcer.**
  - For these threats there is no common pattern, and it is impossible to block all “unwanted” activities without

- Is it possible to block these activities without putting at risk business continuity? **NO.**
- Prevention is not viable; detection/monitoring is
MONITORING and detection mechanisms
Monitoring approaches

- Look for the “bad” (a.k.a. blacklisting)
- Block undesired behavior, allow all the rest
- Threat detection based on previous knowledge and content matching
- Detection technologies: signature-based IDS/IPS, anti-virus, sandboxing

- Accept the “good” (a.k.a. whitelisting)
- Allow desired behaviour, block the rest (or alert)
- A threat is anything that your network and devices are not support to do
- Detection technologies: flow-, rule-, anomaly-based, application whitelisting
3 shades of acceptance-based systems

- malicious
- well-known
- good

very specific whitelisting (deep protocol)
generic whitelisting (e.g. WA firewalls)
anomaly detection

Note:
- the size of circles is arbitrary
- these are just examples
3 shades of Rejection-Based systems

- malicious
  - well-known
    - very specific signatures
    - less specific rules, emulation
    - generic experimental stuff

- good

Note:
- the size of circles is arbitrary
- these are just examples
Signature-based IDS/IPS and anti-virus

- Host- (anti-virus) or network-based (most IDS/IPS) blacklisting
- Several renowned open-source projects
  - Snort
  - Suricata

- Simple idea, easy to use: use a database of well-known attacks and bad inputs
- Highly effective against mainstream attacks

- Require signatures and frequent updates
- **Cannot cope with unknown and emerging threats**
- There are not many known ICS threats
Sandboxing technologies

- Network-based
- Simulate real environments to monitor file and process behavior (e.g. e-mail attachments)
  - Does the process write/set “weird” memory areas
  - Does the file make “unusual” system calls
- Open-source projects
  - Cuckoo Sandbox + Suricata
- Can detect both known and unknown threats
- Effective also against “dormant” malware

- Effective only for Windows files and attachments, not for ICS
Flow-based systems

- Extract network flows meta-information
- Quantitative analysis
  - # connections per minute
  - # bytes
  - # IPs
- Fast analysis, can handle Gbps of data simultaneously
- Can detect known and unknown threats
- Can only detect threats that have quantitative effects (e.g. DoS / bandwidth peaks, horizontal / vertical scans, bruteforce attacks)
- Do not look at content (protocol messages) and context
- **Missing:** actionability, accuracy
Rule-based detection (manual whitelisting)

- Mostly network-based (e.g. Firewalls)
- Rules specify allowed (or disallowed) behavior
  - “Read operations are allowed”
  - “Write operations are disallowed from Windows workstations”

- Typically allow for more context information
- Can detect both known and unknown threats

- Require (lots of) manual work
- Manual configuration = error-prone
Anomaly-based detection

- Detect uncommon/ abnormal/ anomalous activity
- Different ways of detecting an “anomaly”
  - Machine-learning techniques
  - Content-based (payload) analysis
  - Specifications of good behavior
- Configuration (semi-)automatic: reduce configuration effort
- Can detect both known and unknown threats
- Might be difficult to fine-tune
- Might lead to (many) false alarms
- Works only on specific systems
Different environment, different technology

- ICS have limited power and resources
- Host-based solutions (anti-virus) and agents are not an option
- Network monitoring is the way to go

- Anomaly-detection is not the best choice for a very dynamic environment
- ...but it could work in a more predictable environment such as ICS networks

- There are not many known threats for ICS networks
- Blacklisting is less effective
- Whitelisting approaches fit better
- (and security is only part of the problem)
Coming back to ICS

- There is no “silver bullet”
- Several approaches are required at the same time (defense in depth)

Here “anomaly detection” is impossible

Here is where “anomaly detection” and “whitelisting” are possible (still not easy)
In practice, systems look often like...
Define threat model and security strategy

- Many organizations do not perform a risk assessment before choosing the right technology(ies)
  - What are the most valuable assets?
  - What are the biggest threats?