Section 2: Week 5: Analyze Threat Prevention and Response Solutions

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

July 5, 2020

North Central University

# Analyze Threat Prevention and Response Solutions

## Industry Tools to Prevent Intrusion and Malware

Cisco, Intel Security (Mcfee), and IBM are the top three leaders in network intrusion prevention solutions (Gartner, 2015).

Table 1: Intrusion Prevention Systems

|  |  |  |
| --- | --- | --- |
| Vendor | Strengths | Weaknesses |
| Cisco | * Market leader in network technologies | * Expensive * Requires multiple consoles |
| Intel Security (McAfee) | * Easy to configure * Extensive signature collection * Low false positive rates | * Requires multiple management platforms * Not strong enterprise presence * Rebranding risk as business priorities shift |
| IBM | * Very low false positives * Included in many IBM server purchases * Quality reporting | * Not a strategic supplier * The incomplete solution requires third-party extensions |

Figure 1: Gartner Magic Quadrant



Many endpoint protection solutions are moving into the cloud to reduce management costs for small to midsized businesses. When evaluating the platform differences, they mostly vary in terms of alerting capabilities and reporting dimensions (Brame, 2019).

Table 2: Top Endpoint Protection Products

|  |  |
| --- | --- |
| Product | Market Segment |
| Symantec Endpoint Protection Cloud | Enterprise |
| Bitdefender Gravity Zone | Small businesses |
| ESET Endpoint Protection | Different SKUs |

## Control Models

Table 3: Control Models

|  |  |  |
| --- | --- | --- |
| Model Name | Description | Notes |
| Access-Control Matrix  (Bellovin, 2005) | A matrix of subjects (rows) and objects (columns) that describes their rights | * Defines explicit transition states that are hard to verify holistically * Only primitive permissions available |
| Mandatory Access Control (MAC) (Techotopia, 2016) | A set of security labels that form an abstract policy | * Rigorous collection of rules * Transcends a specific technology stack * Administrator defined controls |
| Discretionary Access Control (DACL) (Techotopia, 2016) | ACL that can be manipulated by the object owner | * Fine-grained control to specific identifies * User-defined controls per object |
| Role-Based Access Control (RBAC) (Techotopia, 2016) | Aligns the permissions with the person's job/role in the company | * More scalable across enterprise environments * Fits the policy to the model, not model to policy * Users have one role vs. DACL has many groups |
| Bell-LaPadula Confidentiality (Massachi, u.d.) | Uses security containers to isolate content into a given context | * Designed for mainframe terminal isolation * Read Down/Trust Up model allows for injection into other containers * UNIX abandoned model for DACL * Only cares about confidentiality |
| Biba Integrity Model  (Conrad, 2017) | Expands on the Bell-LaPadula model to add integrity | * Prevents the injection into more protected containers (e.g., anonymous into top-secret) * Adds integrity checks for writing * Use where integrity >> confidentiality (e.g., GPS and time systems) * Opposite of Bell-LaPadula |
| Lipner Model (Young, u.d.) (Kennedys, 2016) | Shows BLP and Biba can be adapted to be commercial policy | * Formalizes idea that users are not always programmers * Programs will have errors * Managers and auditors need access to system state and logs |
| Clark-Wilson  (Wright, 2008) | Analyzes the integrity of a policy for data systems | * A formalized notion of information integrity * Prevents corruption from fault or maliciousness * Confirms data transition tables are not corrupt * Delineates certification and enforcement rules |
| Brewer-Nash (Chinese Wall) (Brewer & Nash, 1989) (Jennot, 2019) | Protects against dynamic conflicts of interest | * Uses information flow to make access decisions * Accessing an object blocks the other in a set * Multiple iterations expand on these central ideas * Originally was binary interest not contextual |
| Graham-Denning (tehjk723, 2016) | Uses eight primitives to describe interactions between subjects within a domain | * Expands the idea of subjects to be within a given domain * Useful for applications that need additional isolation from other rights (e.g., web browsers) |

# References

Bellovin, S. (2005, September 12). *Access Control Matrix*. Retrieved from Columbia University: https://www.cs.columbia.edu/~smb/classes/f05/l03.pdf

Brame, D. (2019, December 27). *The best-hosted endpoint protection and security software for 2020*. Retrieved from PC Mag: https://www.pcmag.com/picks/the-best-hosted-endpoint-protection-and-security-software

Brewer, D., & Nash, M. (1989). The Chinese Wall Security Policy. *IEEE Symposium on Security and Privacy*, 206-214. doi:https://doi.org/10.1109/SECPRI.1989.36295

Conrad, E. (2017). *Eleventh Hour CISSP.* Retrieved from https://www.sciencedirect.com/book/9780128112489/eleventh-hour-cissp

Gartner. (2015, November 16). *Magic Quadrant for Intrusion Prevention*. Retrieved from Cisco: https://www.cisco.com/c/dam/assets/global/CN/partners/pdfs/Gartner2015\_Magic\_Quadrant.pdf

Jeannot, F. (2019, February 2). *Brewer and Nash security model*. Retrieved from Fanck Jeannot: https://www.franckjeannot.com/brewer-and-nash-security-model/

Kennedys, S. (2016). *Lipners Model*. Retrieved from Catholic University: https://www.coursehero.com/file/39442960/Lipners-Modelpdf/

Massachi, S. (u.d.). *Bell-LaPadula*. Retrieved from Computer security - a brief look: https://sites.google.com/site/cacsolin/bell-lapadula

Techotopia. (2016, October 27). *The mandatory, discretionary, role, and role-based access controls*. Retrieved from Techotopia: https://www.techotopia.com/index.php/Mandatory,\_Discretionary,\_Role\_and\_Rule\_Based\_Access\_Control

tehjk723. (2016, May 2). *Week 7 Graham-Denning access control model*. Retrieved from WordPress: https://tehjk723.wordpress.com/2016/05/02/week-7-graham-denning-access-control-model/

Wright, C. (2008). The IT regulatory and standards compliance handbook. *How to Survive Information Systems Audit and Assessments*, 73-114. doi:https://doi.org/10.1016/B978-1-59749-266-9.00005-9

Young, B. (u.d.). *Foundations of computer security*. Retrieved from University of Texas: https://www.cs.utexas.edu/~byoung/cs361/lecture24-4up.pdf