Security Assessment Technique for SDN

김 그 린
greenkim@konkuk.ac.kr

Contents

1. Introduction (1/2)

- SDN is rapidly moving from vision to reality
  - Host of SDN-enabled devices in development and production
  - The combination of separated **control** and **data plane functionality** and **programmability** in the network have found their commercial application in cloud computing and virtualization technology
- The SDN architecture can be exploited to enhance network security
  - Provision of highly reactive security monitoring, analysis and response time
  - The **central controller** is key to this system
    - Deploy traffic analysis or anomaly-detection

%SDN : Software Defined Networks

1. Introduction (2/2)

- However, the same attributes of centralized control and programmability associated with the SDN platform introduce network security challenges
  - An increased potential for Denial-of-Service attacks
    - Centralized controller and flow-table limitation in network device
  - Another issue of concern based on open programmability of the network is trust
    - Between applications and controllers
    - Between controllers and network devices
- An Assessment technique for SDN security is required

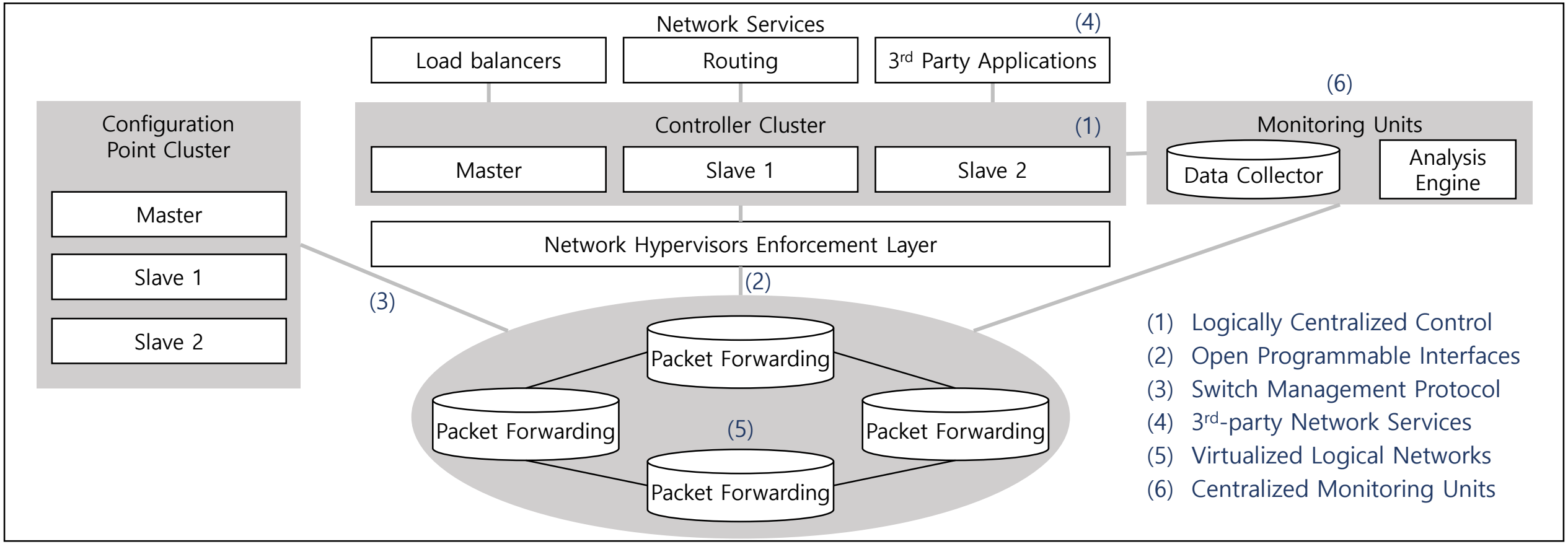
2. Security Analysis of SDN (1/4)

- The basic properties of a security communications network
  - Confidentiality
  - Integrity
  - Availability of information
  - Authentication
  - Non-repudiation

  → Secure data, network assets and communications transactions

2. Security Analysis of SDN (2/4)

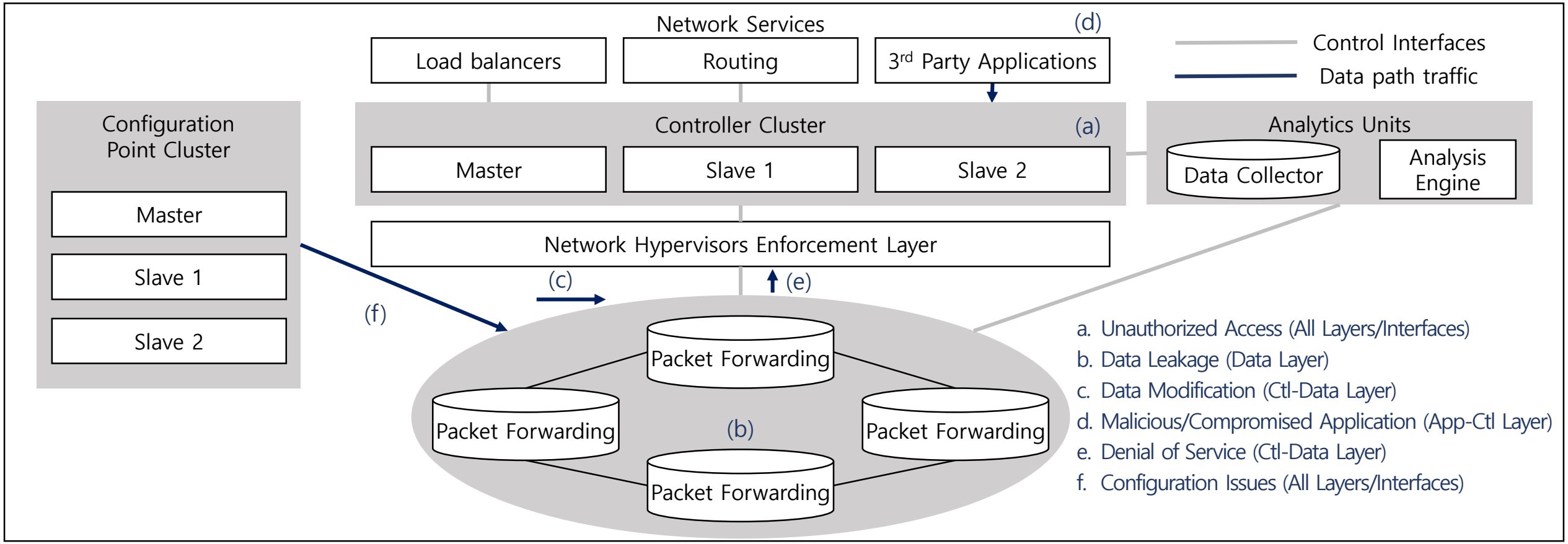
- SDN Characteristics



'A Survey of Security in Software Defined Networks', IEEE Communications Surveys & Tutorials, 2015.

2. Security Analysis of SDN (3/4)

- SDN Potential Attack and Vulnerabilities



'A Survey of Security in Software Defined Networks', IEEE Communications Surveys & Tutorials, 2015.

2. Security Analysis of SDN (4/4)

- Categorization of Security Issues

Security Issue/Attack	SDN Layer Affected or Targeted				
	Application Layer	App-Ctl Interface	Control Layer	Ctl-Data Interface	Data Layer
Unauthorized Access e.g. • Unauthorized Controller Access/Controller Hijacking • Unauthorized/Unauthenticated Application	 X	 X	X X	X	X
Data Leakage e.g. • Flow Rule Discovery (Side Channel Attack on Input Buffer) • Credential Management (Keys, Certificates for each Logical Network) • Forwarding Policy Discovery (Packet Processing Timing Analysis)			 X	 X	X X X
Data Modification e.g. • Flow Rule Modification to Modify Packets (Man-in-the-middle attack)			X	X	X
Malicious/compromised Applications e.g. • Fraudulent Rule Insertion	X	X	X		
Denial of Services e.g. • Controller-Switch Communication Flood • Switch Flow Table Flooding			X	X	X X
Configuration Issues e.g. • Lack of TLS(or other Authentication Technique) Adoption • Policy Enforcement • Lack of Secure Provisioning	X X X	X X X	X X X	X X	X X
System Level SDN Security e.g. • Lack of Visibility of Network State			X	X	X

'SDN Security: A Survey', IEEE SDN for Future Networks and Services, 2013.

3. Security Assessment Technique for SDN

3.1 Taxonomy of issues

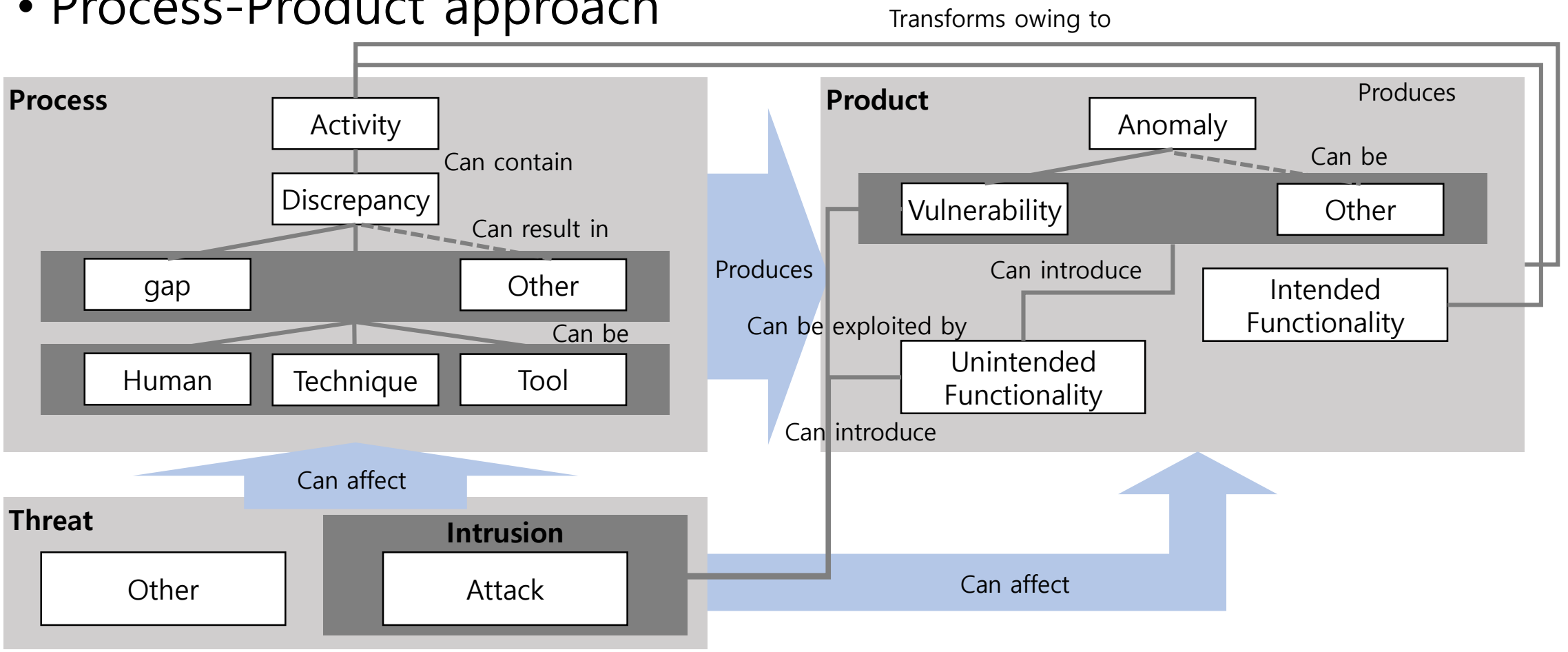
3.2 Assessment Technique

3.1 Taxonomy of issues (1/2)

- The key idea in security assessment is using **process-product approach**
  - In determining the **possible problems**, inconsistencies during **process implementation** and obtaining of the **products**
  - One of the fundamental concepts behind the idea of the approach is the concept of '**gap**'
    - 'gap' could be defined as **a set of discrepancies** of any single process that can introduce some **anomalies** (e.g. **vulnerabilities**) in a product and/or cannot reveal (and eliminate) existing anomalies in a product

3.1 Taxonomy of issues (2/2)

- Process-Product approach



"Cyber Security Lifecycle and Assessment Technique for FPGA-based I&C systems", Design & Test Symposium, 2013

3.2 Assessment Technique

- Each '**gap**' should be represented in a form of formal description
  - To perform the description, the most convenient is **IMECA** technique
    - **Intrusion Modes and Effects Criticality Analysis**
    - **Modification to FMECA** technique that takes into account possible intrusions into the system
    - During the Security Assessment, IMECA can be used in addition to standardized FMECA for **safety-related domains**
      - each **vulnerability** can become a **failure** in a case of **intrusion** into such systems
  - Each identified gap can be represented by a single local IMECA table and each discrepancy inside the gap can be represented by a single row in that local IMECA table

4. Case study of Security Assessment Technique (1/3)

- Based on Categorization of SDN Security Issues from **'SDN Security: A Survey'**, it is possible to choose several types of intrusions
  - **Controller hijacking**
  - **Man-in-the-middle**
  - **Denial of Service**
- Following table shows application of IMECA technique for analysis of theses intrusions

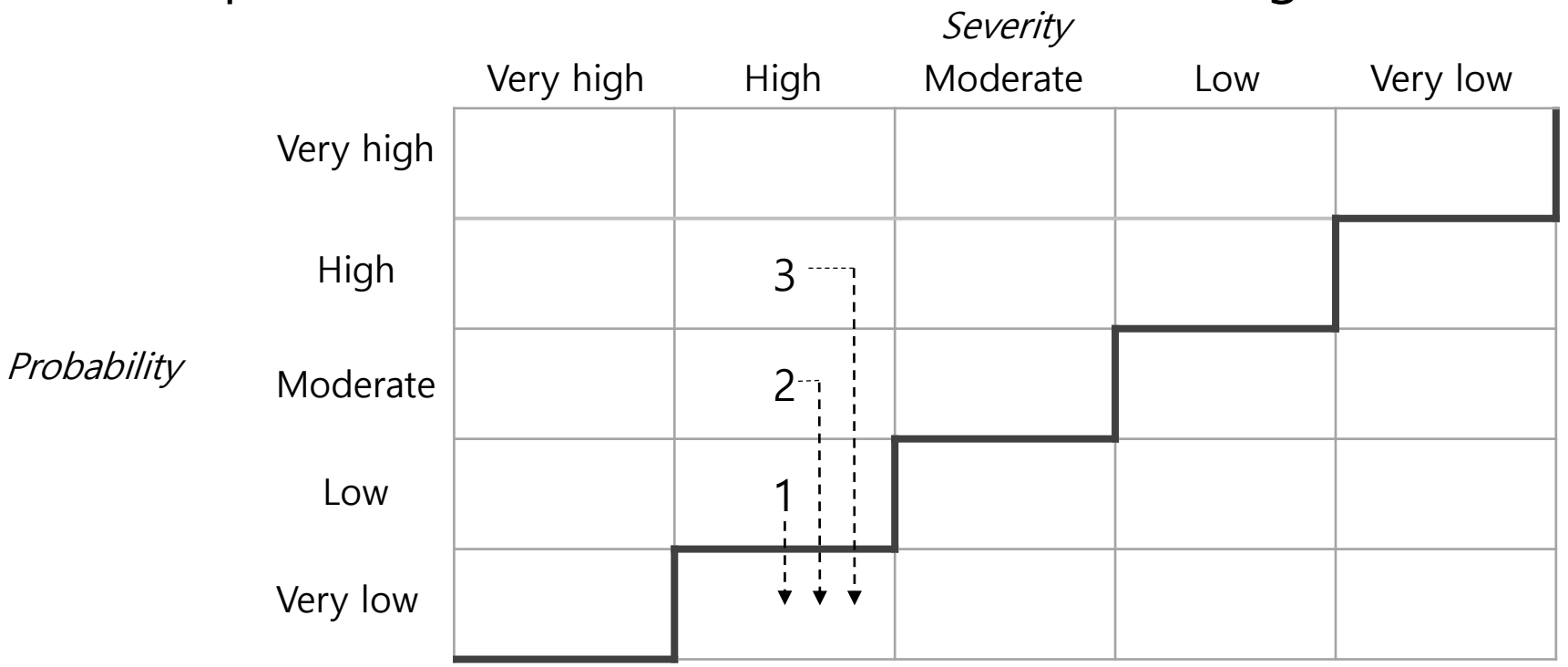
4. Case study of Security Assessment Technique (2/3)

- Intrusion Modes and Effects Criticality Analysis

GAP No	Attack mode	Attack nature	Attack cause	Occurrence Probability	Effect Severity	Type of effects				
						Application Layer	App-Ctl Interface	Control Layer	Ctl-Data Interface	Data Layer
1	Controller hijacking	Active	• Weak authentication	Low	High	-	-	• Gain access to network resource • Manipulate the network operation		
2	Main-in-the middle	Active	• Weak Authentication • Weak confidentiality	Moderate	High	-	-	• Have control over the entire system • Insert/Modify flow rules in the network devices • Allow packets to be steered through the network to the attacker's advantage		
3	Denial of Service	Active	• Weak protection • Resource limitation of flow table	High	High	-	-	• Lead to fraudulent rule insertion and rule modification		

4. Case study of Security Assessment Technique (3/3)

- Criticality matrix (Adapted from ISO 31000:2009)
  - Each of the numbers inside the matrix row number of IMECA table
  - Acceptable values of risks are below the diagonal



5. Conclusion

- A secure SDN does not exist
  - Hidden vulnerabilities are still possible in SDN
  - Security Assessment should be perceived as a repeatable process
- Assurance of SDN security is not possible without taking in to account all specific features of technologies in use
  - In addition to improving SDN, it is necessary to focus on developing rules and best practices that establish and maintain security of SDN

6. Future work

- Compare the IMECA Assessment technique with other methodology such as STRIDE
- Compare SDN Security between various Controllers
  - ONOS
  - OpenDaylight
  - ROSEMARY
  - Ryu
  - SE-Floodlight
- Research and Categorize Security solutions and SDN Security Enhancement
- Recommend Best Practices

References

1. Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, Carl Landwehr. "Basic Concepts and Taxonomy of Dependable and Secure Computing". Jan 2004.
2. M. Coughlin. "A Survey of SDN Security Research".
3. S. Scott-Hayward, S. Natarajan, S. Sezer "A Survey of Security in Software Defined Networks". Communications Surveys & Tutorials, IEEE, 2015.
4. S. Scott-Hayward, G. O'Callaghan and S. Sezer "SDN security: A survey", Future Networks and Services, IEEE, 2013.
5. R. Kloeti, "OpenFlow: A Security Analysis," Available: ftp://yosemite.ee.ethz.ch/pub/students/2012-HS/MA-2012-20- signed.pdf, 2013.
6. Kevin Benton, L. Jean Camp, Chris Small. "OpenFlow vulnerability assessment", Proceedings of the second ACM SIGCOMM workshop on Hot topics software defined networking. 2013.
7. Diego Kreutz, Fernando M. V. Ramos, Paulo Verssimo, "Towards secure and dependable software-defined networks", Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. 2013.
8. A. Gorbenko, V. Kharchenko, O. Tarasyuk, A. Furmanov "F(I)MEA- technique of Web Services Analysis and Dependability Ensuring", Lecture Notes in Computer Science, 2006.
9. E. Babeshko, V. Kharchenko, A. Gorbenko, "Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring", DepCoS-RELCOMEX, 2008.
10. O. Illiashenko, V. Kharchenko, A. Kovalenko, "Cyber Security Lifecycle and Assessment Technique for FPGA-based I&C systems", Design & Test Symposium, 2013.
11. ISO/IEC 27000, Information technology-Security techniques-Information security management systems-Overview and vocabulary, International Organization for Standardization and International Electrotechnical Commission, 2009.
12. ISO/IEC 27001:2005, Information technology-Security techniques- Information security management systems-Requirements, International Organization for Standardization and International Electrotechnical Commission, 2005.
13. ISO/IEC 27002:2005, Information technology-Security techniques-Code of practice for information security management, International Organization for Standardization and International Electrotechnical Commission, 2005.
14. ISO 31000, Risk Management, Risk assessment techniques, International Organization for Standardization and International Electrotechnical Commission, 2009.

KU KONKUK UNIVERSITY

Thank You