CYBERSECURITY FRAMEWORK REQUIREMENTS TO QUANTIFY VULNERABILITIES BASED ON GQM

MOHAMMAD SHOJAESHAFIEI

DR. LETHA ETZKORN

DR. MICHAEL ANDERSON

UNIVERSITY OF ALABAMA IN HUNTSVILLE

CONTENTS:

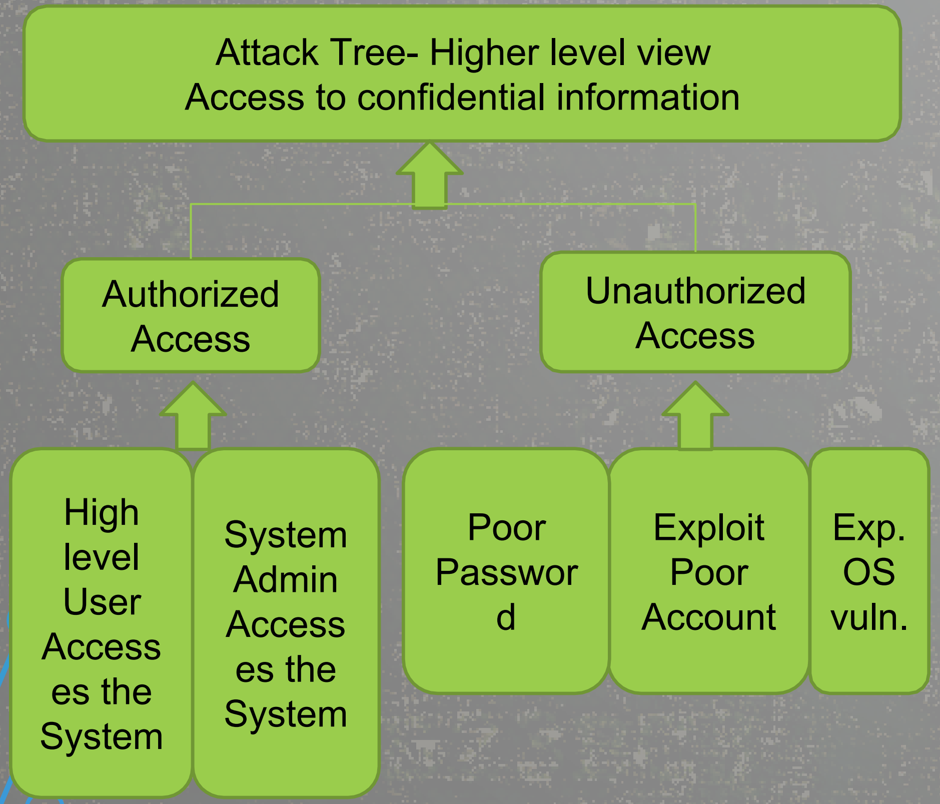
INTRODUCTION

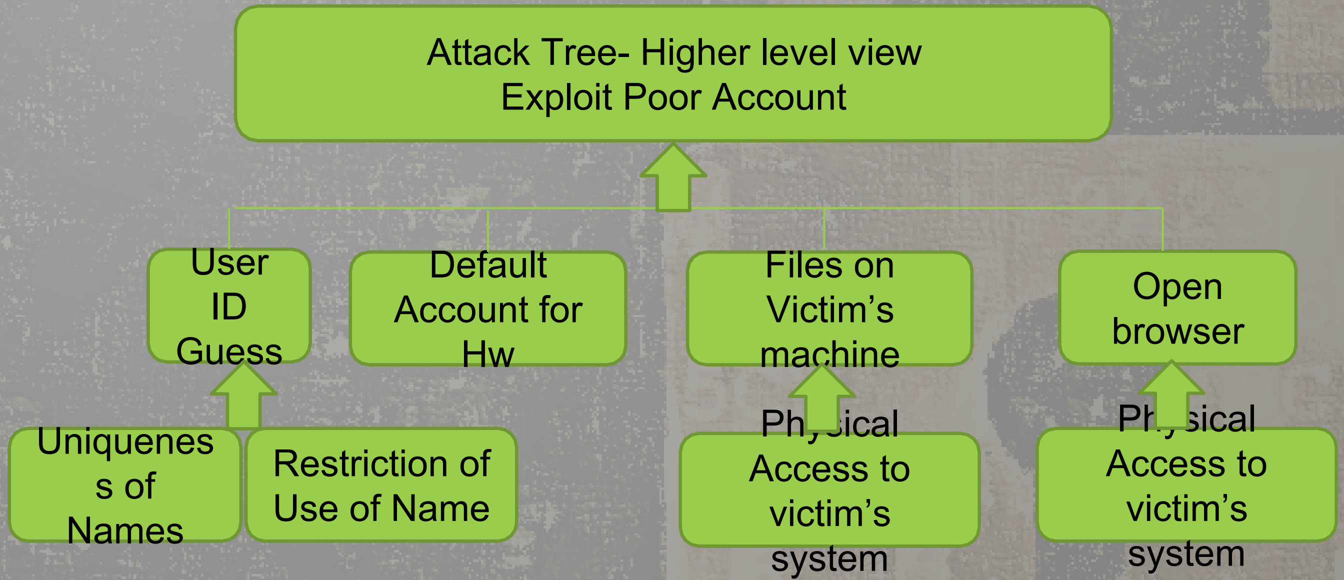
- *Almost all organizations depend on cybersecurity and related indispensable technologies.*
- Almost 40 million people were impacted due to cyber breach on Target store.
- Deficiencies of software code or design lead to majority of cyber attack and each of these vulnerabilities has different impact on Availability, Confidentiality, Integrity and Accuracy.
- The most important component of any organization to build up security is security requirements.
- Research conducted by Semantec proves significant number of attacks are due to lack of security on early stage of development life cycle.

REQUIREMENTS ENGINEERING

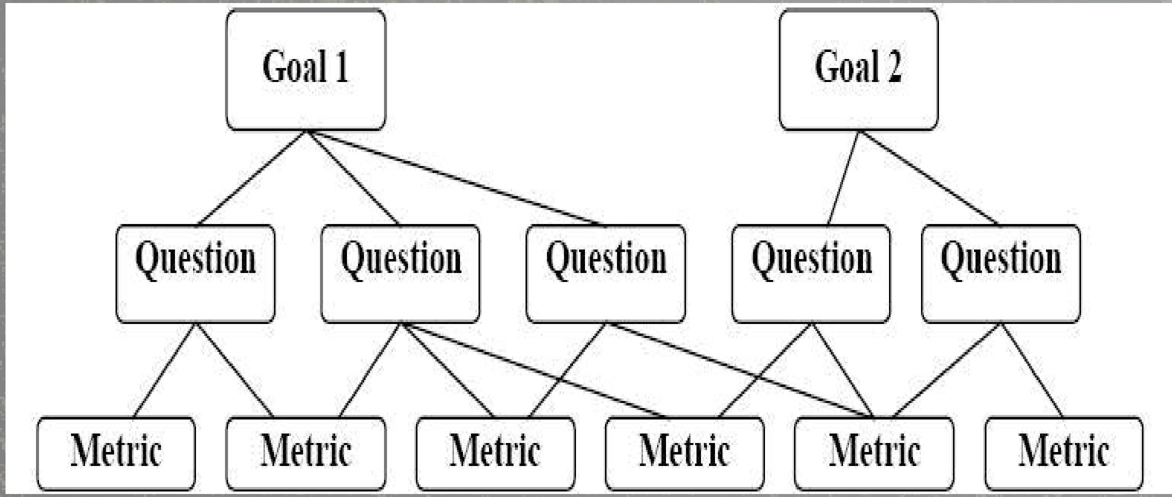
- Requirements engineering cost 10 to 200 times more in correction process once the system has been deployed.
- But there is not sufficient attention for requirement engineering in lots of security projects.
- Different models to support security requirements elicitation such as MSRA , Misuse cases, Secure UML, GBRAM and SQUARE .
- SQUARE has got the most attention because of its advantages compared to the other models.
- It is a well-defined method for security requirements analysis. It is the only method which considers Confidentiality, Availability and Integrity goals explicitly while it comprises threat and risk assessment coupled with quality assurance.

REQUIREMENTS ENGINEERING





GOAL QUESTION METRICS PARADIGM



- GQM; A systematic approach to integrating goals with quality perspective and based on the needs of the project.
- GQM is widely accepted in software engineering as the goal standard to create metrics framework.
- Goal is defined for the project, question tries to characterize the goal with respect to security issues and metrics provide measurements to answer the question.
- Goals are tailored to the needs of the project and the actual trend of flow from the goal refinement that is traceable to the quantifiable questions.

GOAL QUESTION METRICS PARADIGM

- Security requirements identifications in SQUARE outline the security goals and helps to apply GQM to achieve appropriate metrics.

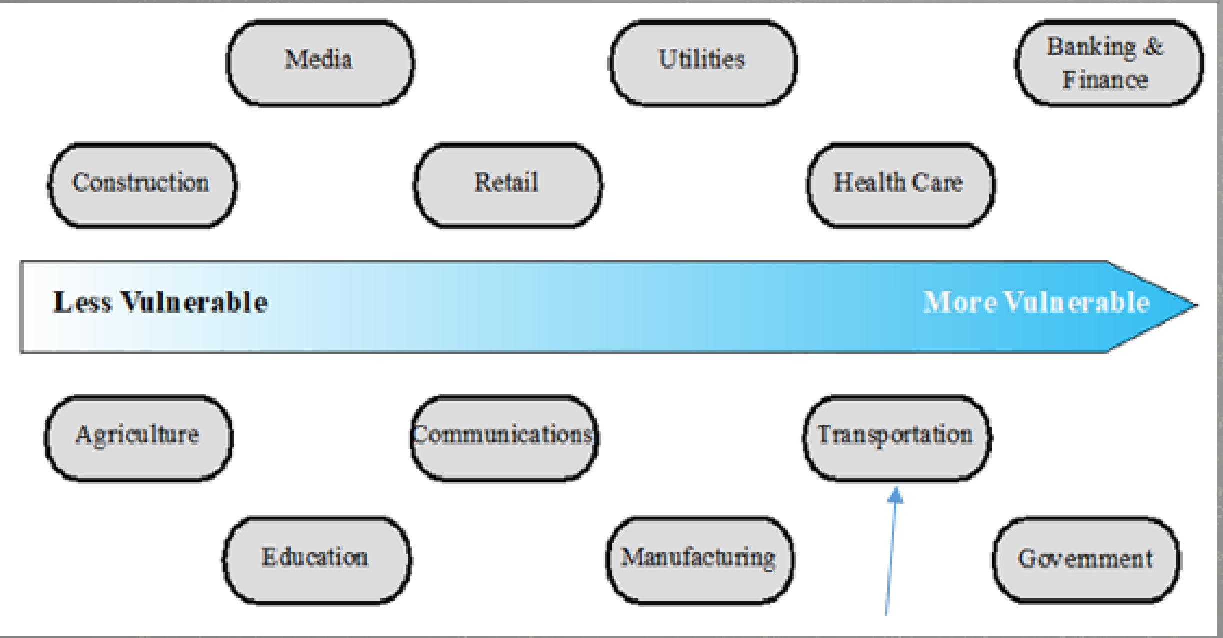
Question derived from the Goal	**Metrics derived from the Question**
How does the system identify the users?	Evaluation method by the procedure all level user identified to use the system.
How does the system authenticate the users?	Common methods such as Name, password, ID, Fingerprint, etc.
How does the system lock the user account?	A certain number of failed login attempts for each user
How does the system grant authorization?	based on the predefined policy such as personal, role-based or group-based

SECURITY STANDARDS

- ISO 27001 known as ISO/IEC 27001:2005
- Provides checklist of controls in security
- Confidentiality, Integrity and Availability
- NIST SP800-53

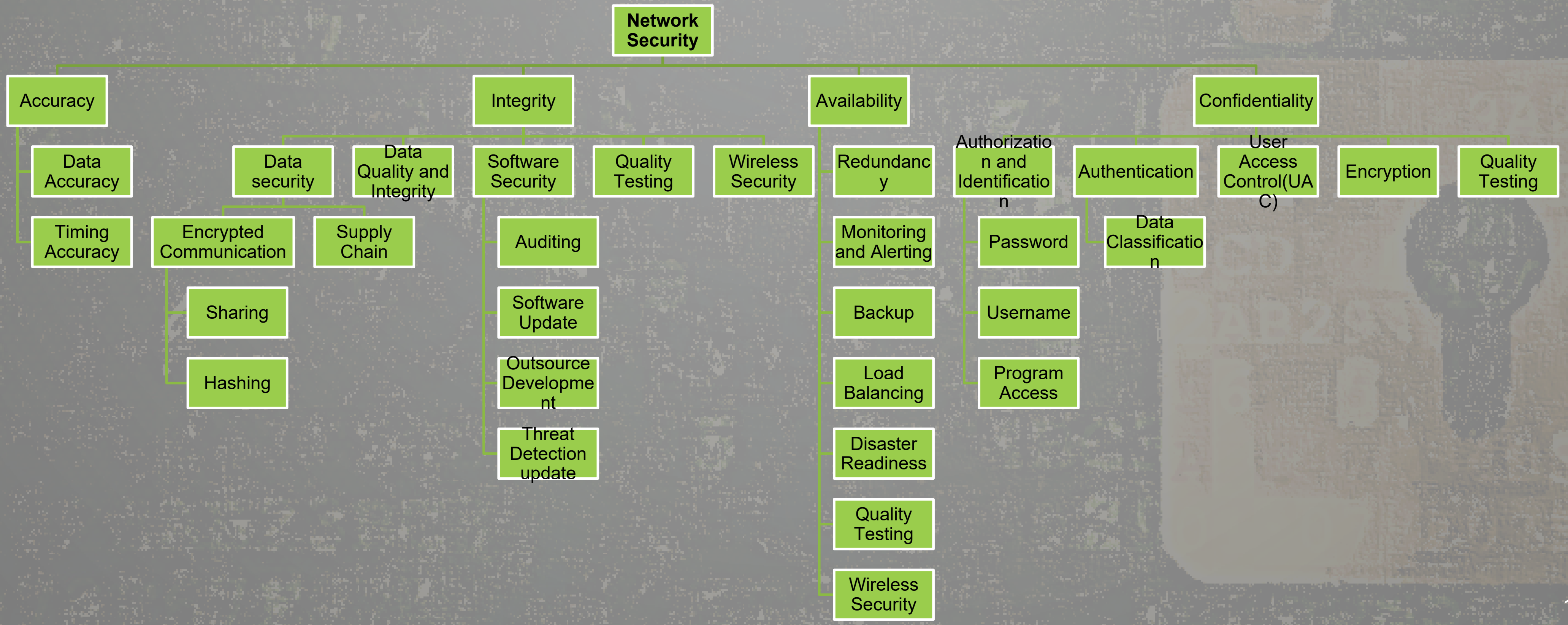
A.10.7.1	**Management of removable media**	**Control: there shall be procedures in place for the management of removable media.**
A.10.7.2	Disposal of media	Control: media shall be disposed of securely and safely when no longer required, using formal procedures.
A.10.7.3	Information handling procedures	Control: procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.
A.10.7.4	Security of system documentation	Control: system documentation shall be protected against unauthorized access.

WHY DOT?



- DOT is one of the most susceptible organizations to cyber attacks.
- Security metrics have never been applied to DOT.

REQUIREMENTS ANALYSIS BASED ON SECURITY FACTORS AND SUB-FACTORS



REQUIREMENTS ANALYSIS BASED ON SECURITY FACTORS AND SUB-FACTORS

- Question 1:
- Does DOT select and monitor outsourced providers in compliance with laws in the country for data storage, location, and translation?
- Question 2:
- How many times a year does DOT conduct network-layer vulnerability scans as prescribed by industry best practices?

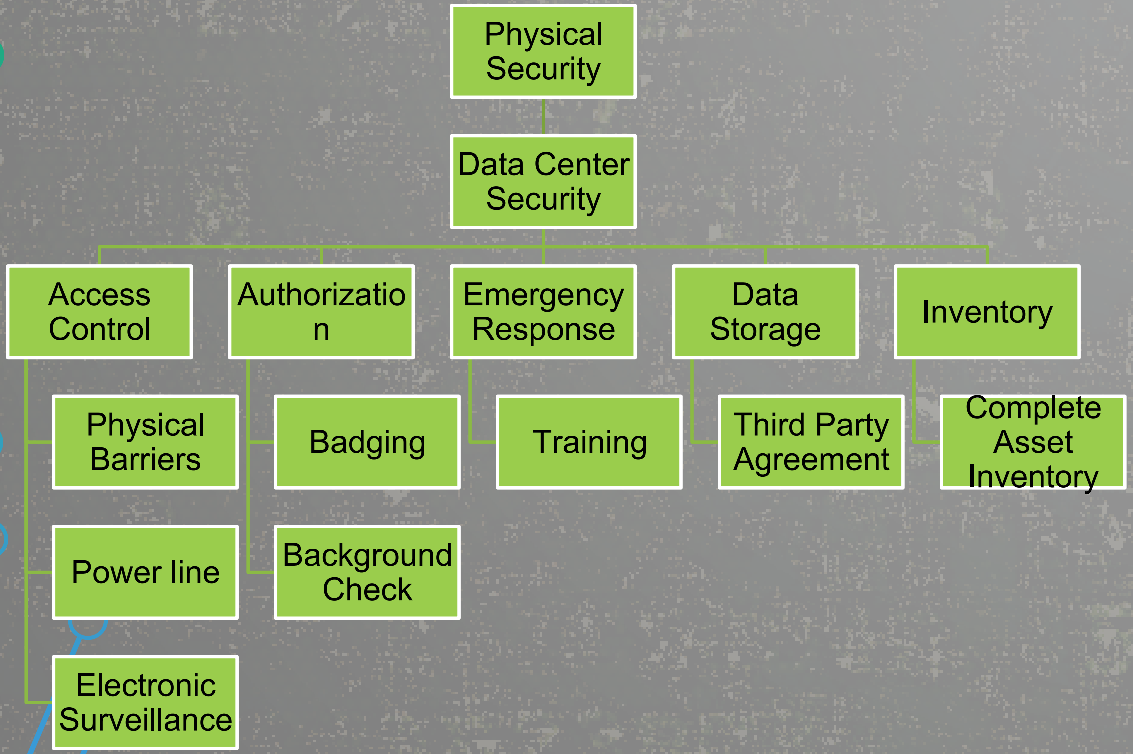
Domain	ISO 27001 2005	ISO 27001 2013	NIST SP800-53
Supply chain management and transparency; third party agreement	A.6.2.3 A.10.2.1 A.10.8.2	A.15.1.2, A.13.2.2, A.9.4.1 A.10.1.1	CA-3 MP-5 PS-7 SA-9

Domain	ISO 27001 2005	ISO 27001 2013	NIST SP800-53
Threat and Vulnerability Management Vulnerability	A.12.5.1 A.12.5.2 A.12.6.1	A.14.2.2, A.14.2.3 A.12.6.1	CM-3 CM-4 CP-10 RA-5 SA-7 SI-1 SI-2 SI-5

OTHER ASPECTS OF SECURITY

- Cloud security! Cloud attack, e.g. Cross VM attack.
- Security requirements model can be helpful. How?
- Q1. Is there any implementation for identity management?
- Q1.1 Is authorization included in implementation?
- Q1.2 Is authentication included in implementation?
- Q1.3 Does User Access Control work properly in the system?
- Q1.4 Is encryption designated for data security?
- Q1.5 Is data security architecture using industry standard?
- Q1.6 If the virtual infrastructure is used, does the cloud solution include independent hardware restore and recovery capability?

PHYSICAL SECURITY



- All components should be consider from different perspective.
    - Authentication, Authorization, Data privacy, Perimeter security.
    - Uninterruptible power supply, bulletproof glasses, reinforced wall.
    - Air conditioning, building should be strong enough against hurricane.
    - Firewalls are the main part of perimeter security for package transmission security.

SECURITY METRICS

- Assume we want to develop a security metric model for the third-party stage of DOT.
- Main Question: How are third-party software updates (Adobe, Java, etc.) installed on DOT’s computers?
- Answers:
  - It is not important to stay current (0)
  - Whenever software update prompts on the system (2)
  - We use software to check for updates and prompt us to install (4)
  - They are managed and updated network-wide from a console (5)
  - Others:---(0-5)

SECURITY METRICS

- Sub-Question 1: Does the software update strategy for software X correctly represent the application of third-party software update policy?
- Sub-question 2: What is the ratio of the updates that do not put the software at the risk of vulnerability to the total number of updates that are predetermined by the third-party?
- Consider a total set of software updates in the model as $TSU = \{so_{1,\ldots,} so_n\}$ and the successful software updates as $SSU=\{ssu_{1,\ldots,} ssu_n\}$ such that $SSU \subseteq$ TSU. The metric is expressed as follows; where RSSU stands for the ratio of software updates that meet the requirements of third-party software update policy.
- $RSSU = \frac{SSU}{TSU}$


Thank You