A Security Ontology for Incident Analysis

Clive Blackwell
Information Security Group,
Royal Holloway, University of London,
Egham, Surrey. TW20 0EX. UK.
C.Blackwell@rhul.ac.uk

ABSTRACT

We have developed a new security incident ontology that considers organizations and their systems in their entirety, rather than software alone. This includes the corresponding defensive classes to the offensive incident categories, as adverse events should also be considered from the defender's viewpoint taking its goals and specific circumstances into account. We have created a three-layer security architecture comprising the social, logical and physical levels that allows the planning of comprehensive defensive measures with complete and reinforcing attack surfaces that span all levels. These ideas allow a holistic analysis of incidents, including human and physical factors, rather than from a technical viewpoint alone, that can give comprehensive defense-in-depth to prevent, detect or recover from incidents. We will use OWL to give a well-defined semantics to the ontology, which could be used to give a formal basis to security incidents.

Categories and Subject Descriptors

K.4.2 **[Social issues]**: Abuse and crime using computers
K.6.5 **[Security and protection]**

General Terms

Security, Design, Management, Human Factors

Keywords

Incident ontology, taxonomy, security architecture

1 INTRODUCTION

1.1 Problems with security ontologies

We describe some issues with existing security ontologies and then indicate some possible solutions provided by our ontology. Existing ontologies are useful within their limited domains, but they generally lack theoretical underpinning and are incompatible with each other. They usually give subjective and incomplete descriptions of security incidents and their causes, using a small set of pre-defined categories, which are described informally in natural language using ad hoc and special vendor terms with uncertain meaning.

Most existing taxonomies focus on incident features rather than the corresponding defensive aspects. Their utility is uncertain if they do not clarify the information from events visible to the defense, or map to defensive concerns. For instance, grouping incidents by type is not immediately useful, if incidents in the same class can cause different effects that are detected and responded to in different ways.

We consider incidents within a wider system context and from multiple perspectives to give a broader and deeper analysis. We extend the focus to organizations and their systems, and include additional categories to represent defensive concerns, as the defender's goals, system structure and valuable resources provide the context for incidents. This includes the defensive system architecture that can protect against component weaknesses with multiple reinforcing attack surfaces [1] to give defense-in-depth. We include people and their attributes such as their motivation, knowledge and awareness, as they are ultimately responsible for causing and responding to incidents.

We extend the defensive analysis to include protective measures before and after the active incident. Proactive measures include deterring the perpetrator, good situational awareness and system hardening. We also consider reactive measures to recover from an incident's effects by repairing the system, overcoming undesirable outcomes, fixing exploited system weaknesses and responding to third party victims.

In addition, most taxonomies do not sufficiently consider the progression of an incident through its stages and the relationships between its components. Our ontology allows the decomposition of complex incidents into their atomic stages along with their causes and effects, which allow analysis of incident progression, and the relationships between the elements, which aid the determination of effective defensive measures.

Our dual defensive taxonomy is nearly symmetrical to the offensive taxonomy in structure, but must examine the response of the defender who has to operate with an incomplete and possibly incorrect view of incidents. We can show how the defense can improve its situational awareness and response capability to anomalous events using an extended and adapted OODA loop [2], which stands for Observe, Orient, Decide, and Act. It was originally developed by USAF Colonel John Boyd from his analysis of the success of US fighter pilots in the Korean War. We can apply the OODA loop to link the perpetrator's activities to the detected observations, inferences and subsequent response of the defender [3].

1.2 Architectural Security Model

We have designed a three-layer architectural security model to investigate and evaluate organizational security that is inspired by Neumann's eight-layer model [4], [5]. Neumann presents a practical classification system for attacks, which starting from the highest and outermost layer are the external environment, user, application, middleware, networking, operating system, hardware and internal environment. We have simplified the eight layer conceptual model to analyze security incidents, and ended up with three layers, which are the social layer (people and organizations) and physical layer along with the middle logical layer containing computers and networks. This allows a holistic representation and analysis of incidents including human and physical factors, rather than as technical events alone.

The social or organizational layer contains the abstract representation of organizations by their attributes including their goals, policies and procedures. It also includes people and their characteristics such as their goals, knowledge and beliefs. All incidents are initiated by people at the social layer and are only effective if they meet a social goal such as obtaining money, power, prestige or pleasure. These subjects use lower layer entities to meet their objectives. Even social engineering attacks directly targeting people at the social layer often use lower layer services such as the phone or email to avoid detection.

The logical layer is the intermediate layer that contains intangible computational entities including computers, networks, software and data. People cannot operate directly at this layer, but use agents to act on their behalf, such as their user accounts to issue commands, run programs, execute processes and use applications.

The physical layer is the bottom layer that contains tangible objects including buildings, equipment, paper documents, and the physical aspects of computers, their components and peripherals. In addition, it contains electromagnetic radiation such as radio waves, electricity and magnetism that are used to transmit and store data. Physical incidents include destruction of objects, theft of hardware and documents, and snooping on communications.

All higher layer entities including people and information have a physical existence as well as a higher layer representation that must be considered when analyzing possible security breaches. We conclude that effective defense must involve comprehensive protection with complete attack surfaces that span all three levels.

2 OUR ONTOLOGY

2.1 Extension of Howard and Longstaff's incident taxonomy

We investigate the incident phases with an extension of Howard and Longstaff's taxonomy [6], [7] for network security incidents that show the different classes of entity involved in attacks and their relationships, shown in figure 1. The categories are attacker, tool, vulnerability, action, target, unauthorized result and objectives. The *attacker* uses a *tool* to perform an *action* that exploits a *vulnerability* on a *target* causing an *unauthorized result* that meets its *objectives*.

We extend Howard and Longstaff's conceptual taxonomy to include the social and physical aspects of systems using our architectural model, and also develop a corresponding defensive taxonomy, which allows comprehensive modeling of incidents and their effects. We explicitly link our classification to Howard's taxonomy and give our rationale for the differences category by category.

We extend the taxonomy to include accidental incidents, and therefore, we prefer to use the term *perpetrator* to *attacker* as the incident initiator. Perpetrators execute incidents deliberately to meet their objectives, but they do not necessarily intend harm, which may be caused by unforeseen consequences. Some incidents are caused by lower-level entities like the environment or a system without intent, as intention is a social-level concept.

We prefer to organize the incident within stages rather than events. A *stage* comprises a coherent set of events with a common purpose that makes a complete step towards completing the incident. The incident stages include accessing the system, using the targeted resource and escaping without detection. Howard's action category does not separate the actions into these distinct classes of initial access and subsequent use of the target, nor the exit and subsequent use of the resource by the perpetrator.

We have separate entities for the *perpetrator*, and their *agents* who may perform some stages on its behalf. The agent has differing goals, concerns and abilities and chooses when to act, and so its motivation and relationship to the perpetrator is important. For example, it may intend to be helpful, when acting as an unwitting accomplice in a social engineering attack.

We prefer to use the designation *method* rather than *tool* as the means used, because means is more general and can include the actor's internal abilities and knowledge as well as tools. The original taxonomy has the stage where the *vulnerability* occurs, which is at the design, implementation or configuration stage. We elaborate the specific *vulnerability* exploited with its different types and attributes like the other categories.

We should consider the long-term social-level impact on the objectives of the involved parties, not only the immediate effects, as the important consequences might be remote and indirect from immediate events. Many stages do not achieve a social level effect for the perpetrator, as they are only means to achieve the objective. However, third party stage actors should meet their objectives by performing stage actions; otherwise, they would not be executed.

Perpetrators achieve their aims by first breaching the fundamental security services, usually at lower layers, to access and use the target. However, the major impact occur at the social layer on the availability of financial and tangible resources, or by causing psychological or reputational damage, which should be considered separately, rather than focusing purely on the supporting security goals. Therefore, we distinguish the *immediate effect* of a stage usually at a lower layer from the *ultimate effect*, which is the final outcome at the social level intended to meet the perpetrator's objective. An immediate effect is only the result of a stage that defeats the security controls to enable access and use of the targeted resource, which is a means to the end of achieving the perpetrator's objective.

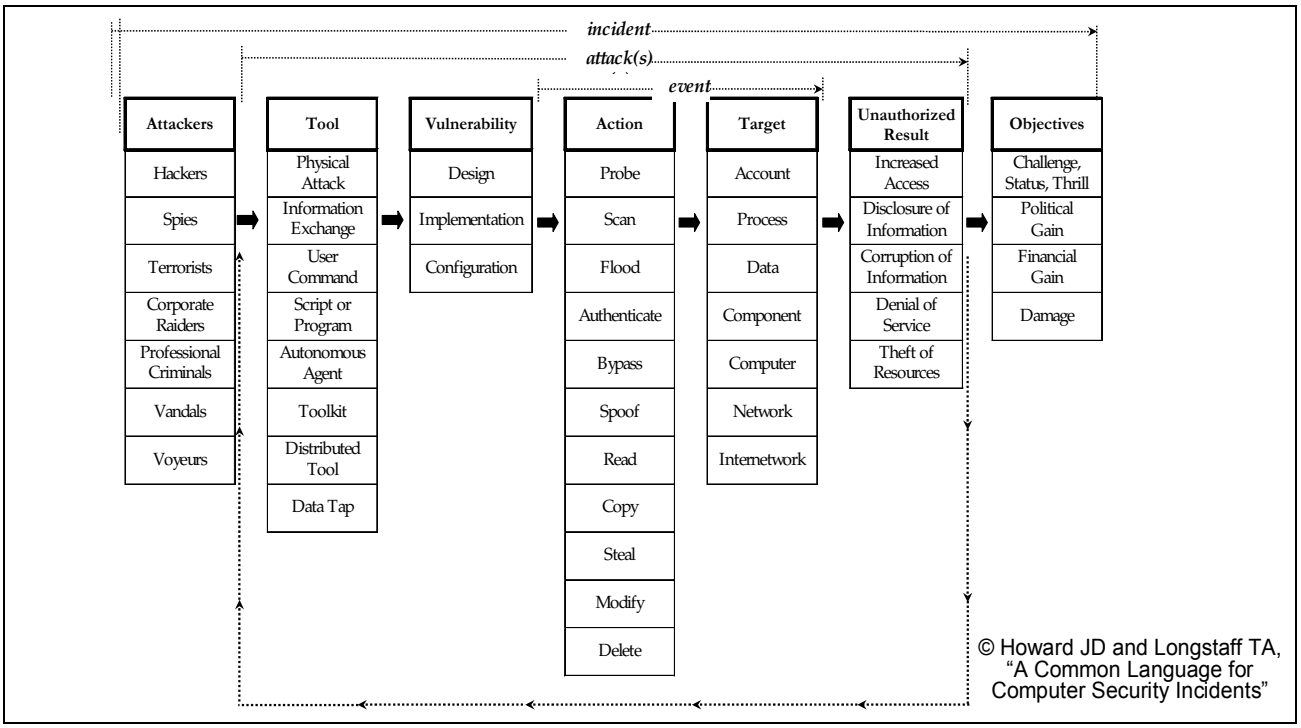

Figure 1 Howard and Longstaff's Security Incident Taxonomy

We call this class *immediate effect* rather than *unauthorized result*, as the outcome may be unacceptable even if it is authorized. The immediate effects affect confidentiality, integrity and availability, or more generally Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege using Microsoft's STRIDE [8] classification, by passing through protective controls.

In our extended taxonomy, in an active *stage* of an incident, the *actor* (*perpetrator* or its *agent*) employs a *method* to perform an *action* that exploits a *vulnerability* with an *immediate effect* on a *target* usually at lower levels. An *incident* is a chain of related *stages* intended to eventually cause the social-layer *ultimate effect* that meets its psychological or financial *objective* at the expense of or with the *ultimate target*.

The ultimate effect is missing from Howard's table, and implicit from the unauthorized result, leaving the analysis incomplete. The purpose and ultimate effect of fraud is to gain money, whereas the compromise of credit card details is an immediate effect resulting from an intermediate stage. The ultimate effect for the perpetrator is financial gain, access and control over valuable resources, increased power, abilities and knowledge, psychological pleasure and reputation, which are positive objectives. The incident may also have negative goals such as saving effort, avoiding harm, or causing damage to a victim, which reverses the directionality of the above categories.

The ultimate effect field gives the effect on the perpetrator. The ultimate effect on the defender and any other victim is considered within our dual defensive taxonomy, which depends upon the impact on its abilities to meet its goals, which may be completely different to the ultimate effect on the perpetrator. The *ultimate target* may be the victimized social-level entity if the perpetrator has an intentional negative psychological objective towards them, such as an organization they hold a grudge against. Alternatively, it could be a resource such as money when the perpetrator has a positive objective of tangible gain, where the negative effect on the victim may be incidental. The incident may also damage third party victims either deliberately or inadvertently.

2.2 Defense

Howard and Longstaff focused on offense within their incident taxonomy, and did not elaborate many important defensive aspects. Several incident features should be examined from both sides, because their appearance and significance depend on each party's objectives, perspective, circumstances and awareness. We separate the categories into two sets of interrelated classes based on their relevance to each side, where each offensive class is matched by a corresponding defensive class with related purposes and attributes, as shown in table 1.

Our ontology distinguishes the different ultimate effects for the perpetrator and the victim, because of their differing goals and interests. For example, recovery may be the most difficult, time-consuming and expensive part of an incident for the victim. The defender has positive objectives to achieve its goals, and negative objectives of avoiding undesirable incidents using its controls for defensive reactions. Either there is a corresponding category in the defense classification comparable to the offensive class, or the same category appears in both halves, viewed differently by each party in recognition of their differing concerns.

In the active stage of the incident, the *defender* employs a *control* to constrain the perpetrator's action with a corresponding *reaction* to avoid or limit an undesirable *immediate effect* on or with the *target*. The immediate defensive reactions should avoid or

recover from the immediate effects on the accessibility, confidentiality, integrity, availability and trustworthiness of its resources.

The defense also attempts to stop or limit the immediate effects, usually on lower-level logical or physical resources, from causing a social-level ultimate effect on its goals such as reputation and profitability. The indirect effect to the defense may vastly outweigh the value of the resources directly targeted. The *defender* tries to stop the *immediate effect* from translating to the social level to cause an *ultimate effect* on the *ultimate target* to ensure that it still achieves its *ultimate objectives*. The defense may also limit the *ultimate effect* after the incident by instituting recovery measures, or by achieving its objectives in another way.

Table 1 Comparison of offensive and defensive categories

Offensive categories	Defensive categories
Perpetrator	Defender and third party victim
Objective	Positive objective to achieve goals Negative objective to avoid incidents
Method	Positive method and negative control
Threat	Vulnerability
Agent	Employee or service provider
Action	Positive action and control reaction
Immediate target	Immediate target
Immediate effect	Immediate effect
Intended ultimate target	Ultimate affected target valuable to the defense
Ultimate effect for perpetrator	Ultimate effect on defender and third party victims

The defender may not be able to respond fast enough from the limited information available during incidents to avoid permanent damage. Our ontology is made more useful by incorporating Boyd's OODA loop [3] to analyze the interrelationships between the incident actions and their observable manifestations to inform the selection of appropriate defensive reactions based on current awareness, capabilities and goals [4]. The defender may attempt to defend against an anomalous event, a particular stage or complete incident using concentric OODA loops with different spatial and temporal scopes. We may then be able to defend systematically against incidents with multiple controls at different locations and levels by providing defense-in-depth with several reinforcing and complete attack surfaces.

3 CONCLUSION AND FURTHER WORK

We need to understand incidents thoroughly to implement systematic defense-in-depth, as no single control can give complete protection. We simplified Neumann's model [6] to give a three-layer architectural security model that includes incident locations and scope. We extended Howard and Longstaff's taxonomy [7], [8] by expanding and elaborating its categories, and by designing an analogous defensive classification scheme to give the defensive viewpoint, which may be used for defensive reaction based upon inferences from observable incident behavior.

Our ontology considers entire systems holistically including defensive goals, system architecture, surrounding context and protection mechanisms, which is more dependable than ad hoc techniques relying upon the expertise of analysts, as threats will be missed because systems are becoming increasingly complex. The discovery of all relevant categories, their structure, attributes and relationships aids detection of possible exploitable weaknesses, and the relationships between offensive and defensive classes help determine possible avoidance and remediation measures.

We need to develop automated tools and procedures for incident analysis, which could help the defense through a more complete, systematic and accurate analysis of security incidents. This requires a comprehensive, consistent, objective and precise ontology to describe and analyze security incidents. We will use the Web Ontology Language (OWL) [9] that has well-defined semantics to formalize our ontology to give it a theoretically sound grounding that will be conceptually clearer than the tabular representation above, and the machine-readable classification will allow automation of incident analysis.

Our object-oriented ontology may also provide a common framework for extending and unifying existing software taxonomies such as CWE [10]. They do not consider many system factors such as defensive goals and system structure, which is important, as we are interested in how systems fare, not in the performance of their software and other components.

4 References

[1] M Howard (2004). "Attack surface: mitigate security risks by minimizing the code you expose to untrusted users". MSDN magazine (November 2004), at http://msdn.microsoft.com/en-us/magazine/cc163882.aspx.

[2] JR Boyd (1986). "Patterns of Conflict", at http://committeeofpublicsafety.files.wordpress.com/2009/11/poc.pdf. Updated version by C Spinney and C Richards (2007), at http://committeeofpublicsafety.files.wordpress.com/2009/11/patterns_ppt.pdf.

[3] C Blackwell (2010). "Improved Situational Awareness and Response with Enhanced OODA Loops". 6th CSIIR Workshop. ACM Press.

[4] PG Neumann and D Parker (1989). "A Summary of Computer Misuse Techniques". Proceedings of the 12th National Computer Security Conference.

[5] PG Neumann (2000). "Practical Architectures for Survivable Systems and Networks". SRI International, at www.csl.sri.com/neumann/survivability.pdf.

[6] JD Howard (1997). "An Analysis of Security Incidents on the Internet, 1989 – 1995". PhD thesis. Carnegie-Mellon University, at www.cert.org/research/JHThesis.

[7] JD Howard and TA Longstaff (1998). "A common language for computer security incidents". Sandia National Laboratories, at www.cert.org/research/taxonomy_988667.pdf.

[8] F Swiderski and W Snyder (2004). "Threat Modeling". Microsoft Press.

[9] W3C OWL Working Group (2009). "OWL 2 Web Ontology Language Document Overview". W3C (27 Oct 2009), at www.w3.org/TR/owl2-overview.

[10] MITRE. "Common Weaknesses Enumeration". The MITRE Corporation, available at http://cwe.mitre.org.