Threat Agents: a Necessary Component of Threat Analysis

Timothy Casey
Intel
timothy.casey@intel.com

Patrick Koeberl
Intel Innovation Lab
patrickx.koeberl@intel.com

Claire Vishik
Intel
claire.vishik@intel.com

1. INTRODUCTION

There have been significant achievements in defining and developing viable approaches to threat modeling and risk assessment techniques for a wide range of IT applications and computing environments. Most of the approaches have been qualitative, due to the difficulties in quantifying all the aspects of the threat analysis. Some quantitative approaches, especially based on the analysis of the cost of security, have been proposed as well, such as "Total Cost of Security" described in [1]. The adjacent field of requirements engineering that provides useful insight into threats and mitigations, has flourished also [2]. In qualitative studies, the focus was on introducing new taxonomies and ontologies [3], applying threat modeling techniques to new areas [4], e.g., ad-hoc networks or improving prioritization and usability of the existing approaches, such as the Common Vulnerability Scoring System [5]. Interest in applying the same models to hardware and software threat analysis is beginning to emerge [6], although the difficulties as well as the benefits of this approach are self-evident.

However, we observe that the focus of most studies continues to be on asset or vulnerability analysis, while assessments based on the types of threat agents are rarer or are treated as supplemental to other types of analysis. We believe that the mitigation techniques and planning approaches depend on the intent and abilities of the attackers, and therefore a greater emphasis on the analysis from that angle is important. Therefore, in this short paper, we are taking a more careful look at the typology of threat agents that can provide considerable insights into the likelihood and specific nature of an attack and can inform the planners about the best and pragmatic mitigation techniques.

While we recognize that the exclusive focus on perpetrators of exploits provides a limited view of a vulnerability or a threat, our experience demonstrates that increasing the weight of threat agent analysis in risk assessments helps the technologists in forming a coherent picture of the threat space and priorities of remediation. In our discussion of the threat agent, we focus on TAL (Threat Agent Library), a threat assessment tool developed at Intel and describing taxonomy of attackers. Additionally, we describe simplified example applications of the Intel TAL to illustrate its utility as part of an extensive threat analysis in an organization.

2. ANALYZING THREAT AGENTS

When risk managers assess threats to information assets, they have to understand the nature of potential human threat agents: the categories of people and organizations that can harm the information assets of an enterprise. This is a challenging task. A key problem is the lack of industry standards or reference definitions of agents. Assessors often have different concepts of even the most common agents, making it difficult to share information or apply it consistently.

Many classifications of threat agents and their activities have been developed, such as the IBM classification [7] consisting of Class 1 – 'clever outsiders', Class 2 'knowledgeable insiders' and Class 3 – 'funded organizations'. The simplicity of this coarse grained approach is attractive, but real world threat agents have widely differing intents, capabilities and resources. A threat taxonomy proposed by ISSS (Information Security Society of Switzerland) [8] describes agents, their motivations, and localization as available parameters. The taxonomy addresses three factors only: the identity of the agent, origin or place of the operations, and the nature of the motivations. Although this type of characterization is useful, the proposed parameters are not sufficient to offer detailed analyses of many situations. Some other classifications, such as [9] focus on the goals of the threat agents: unauthorized access, unauthorized modification or destruction of important information assets, and denial of authorized access.

We think that in order to effectively allocate security resources in an organization, finer grained threat agent taxonomy is useful. In addition to its comprehensive nature, a threat agent classification needs to be:

- Capable of describing the key characteristics of threat agents
- Extensible, allowing new threat agents to be added if needed
- Qualitative rather than quantitative. A quantitative approach requires values to be defined which are subjective in nature. A descriptive, label based approach is preferable.
- Composed in a fashion that can add new and useful dimensions to risk and threat analysis.
- Not ambiguous, ensuring that the main definitions are specific enough and do not need to be renegotiated for different situations
- Composed of re-usable standard components

We believe that the last point is very important: even well designed risk management projects often experience threat creep - threat definitions are repeatedly re-negotiated as the assessment progresses, making the outcomes and recommendations difficult to interpret. Publicity about some kinds of threat agents tends to inflate their potential weight in the analysis, leading to further skewing of the results. Frequently a factor that appears to be the biggest threat because of disproportionally large attention may not be a significant risk in a particular situation if all the elements of the situation are analyzed. Finally, it is important to remember that threat agents evolve as they are influenced by diverse economic, societal, political, and technological trends. The TAL (Threat Agent Library) has many of the useful features of threat agent taxonomies discussed in this section.

3. ABOUT INTEL TAL

The TAL is a standardized set of threat agent archetypes, defined in order to improve the accuracy and efficiency of the threat analysis [10]. A cross-disciplinary team at Intel developed a Threat Agent Library of 23 agent archetypes, each uniquely defined. TAL takes a detailed view of potential attackers describing multiple attributes of threat agents. There are 20+ types of hostile and non-hostile agents e.g., mobster, legal adversary, terrorist, cyber vandal, corrupt government official, government cyberwarrior, disgruntled employee or distracted, untrained or reckless employees. The taxonomy that describes each of these agents uniquely has eight attributes described below:

- Intent (hostile/accidental)
- Access (internal/external)
- Outcome (threat agent's goal)
- Limits (legal and ethical limits constraining threat agent)
- Resource level (organizational level)
- Skill level
- Objective (attack strategy)
- Visibility (overt/covert/clandestine)

We have found that this attribute set can sufficiently differentiate distinct threat agents, yet is easily understood and applied by even novice security practitioners. In addition to taxonomy attributes, outcome attributes are used for analyses, permitting the assessors to further refine the picture.

4. FROM TAXONOMY TO THREAT AGENT LIBRARY

The attribute set defined in the previous section can support the development of a library of threat agents, where each threat agent is defined by its unique set of characteristics. Starting with a simple description of each agent, an iterative process progressively refines the agent definitions. Threat agent creation needs to be a data-driven exercise; in-house experience is supplemented with outside expertise and research results.

Once defined, agents are assessed on the strength of their threat which may change over time; a threat agent rating is defined by factors including the agent's recent activity. The rating is on a scale from low to high and is re-evaluated at regular intervals to ensure continued high relevance of the library. This approach facilitates risk assessments and enables trending.

Thus, the library is a catalog of diverse agents that identify strengths and weaknesses of major threat sources. Archetypes of these agents, inclusive of their attributes, are designed based on normal behaviors, not outliers. In a similar fashion to the "persona" technique increasingly used in product development, each archetype includes a detailed description of typical characteristics and behaviors. The resulting threat "persona" can aid analysis by providing a clear picture of the attacker mindset, how he operates and who his partners are.

5. USING TAL: GENERAL APPROACH

Developing an appropriate threat model is a key element of secure product development. When conducting threat and risk assessments, we need to rank the risks in order to understand the needs for resource allocation, strength of mitigation and other parameters relevant for an organization or an environment. Threats are ranked in terms of probability and damage potential; mitigation for less probable threats may not be addressed by the security teams, and the elimination is frequently ad-hoc. The TAL can improve the approach by providing a consistent library from which to select a subset of most likely threat agents. Analysis and design decisions can then focus on these threat agents only. In this way, a more consistent and repeatable threat modeling process is supported.

How can we use the TAL to obtain new information about a security threat to an organization? The example below illustrates the adaptability of the TAL.

The evaluation of the threat to the organizational IT for an average enterprise from a government cyberwarrior may be a good example. Cyberwarfare threats rightfully receive a lot of media attention, but this, until recently, was mostly applied to operations associated, directly or indirectly, with defense activities or government operations. Consequently, enterprise IT could conclude that the need to form strong defenses from government cyberwarfare is not a priority. However, recently reported events indicated that such views may need to be revised. The users of TAL, under these circumstances, can easily revise the ranking and trending in the library and rethink the applicability of this threat to regular threat assessments because of the uniform and standardized method of defining the agent.

5.1 Components of threat assessments

Several stages can be identified when using TAL for different types of threat analyses. These stages are briefly described below for two example assessments.

Small domains or narrow targets can benefit from narrowing the focus onto a subset of 'most likely' threat agents:

- Subject matter experts examine the problem set and select a subset of 2-4 likely agents from the Threat Agent Library.
- Further analyses focus on the selected agents only.
- The descriptions of agents can be incorporated into other assessment tools, streamlining this component of the analysis. Intel is using this approach as part of a number of internal assessments, such as TARA risk assessment methodology [10].

In large domains, where all threats need to be considered, the analysis may follow a different process:

- Subject Matter Experts build a model (e.g. attack tree) to determine the most likely avenue of attack
- Agents associated with the likely avenues are included in the models, presenting the generic level of attacker skill, expertise, and economic capabilities.

5.2 Using TAL to analyze known threats: insights that we can gain

We will now apply TAL to the analysis of generic IC counterfeiting. A counterfeit IC is one which bears a validly registered trademark without the authorization of the trademark owner. The counterfeiter aims to make the IC indistinguishable from the original as far as is practicable. There are a number of routes to a counterfeit IC, and one example analysis is presented below, for device remarking.

5.2.1 *Device Remarking*

In a device remarking attack, the IC is "upgraded" by removing the existing device markings and replacing them with markings indicating a higher value device, for example changing the temperature rating from a commercial to an extended temperature range. The remarked device is then sold on to unsuspecting customers at a premium. For a simple screen printed marking, the skill level and equipment required for such an attack are not significant.

Subject matter experts begin the analysis by selecting a suitable subset of threat agents from the TAL. It is important to emphasize that threat agents be selected by attributes rather than by name. The threat agent name is simply a label identifying a set of attributes; selecting by agent name can lead to misinterpretation and overlooking of less obvious options.

Two threat agents are selected from the TAL, Mobster and Thief. Their attributes are listed in Table 1. Both agents represent a viable device remarking risk in terms of intent and capabilities; however the higher organizational resources of 'Mobster' allow this agent to produce and distribute a much greater number of remarked devices in the short time span before the remarking operation is located and shut down. Using the current and predicted threat rating associated with each agent the TAL based assessment can determine which agent to focus on.

	Mobster	Thief
Intent	Hostile	Hostile
Access	External	External
Outcome	Acquisition/ Theft	Acquisition/ Theft
Limits	Extra-legal	Extra-legal
Resources	Organization	Individual
Skills	Adept	Minimal
Objective	Take	Take
Visibility	Covert	Clandestine

Table 1 Selected Threat Agents

What insights can we gain by applying the TAL? The analysis of threat agent attributes, ratings and "personas" supports informed decision making when assessing the need to introduce anti-remarking technologies. In particular the "Skills" and "Resources" attributes of the appropriate threat agent will determine the degree to which such technologies are introduced. In addition to the technological aspects, the appropriate level of supporting legal and law enforcement activities can be assessed. Here it is the threat "persona" that provides the necessary insight into the threat agent's mindset, operations and interactions. In this way the TAL approach enables the formulation of a coherent and consistent anti-remarking strategy.

6. CONCLUSIONS AND FUTURE WORK

The standardized threat agent approach is already making an impact. It was incorporated into Intel's main business security and acquisitions risk assessment tools where it contributed to streamlining associated processes. A key manufacturing group reported a 60% improvement in total threat assessment time, reducing the negotiation period from months to days. The agent archetypes also enable focused data collection and accurate threat ranking, allowing Intel IT architecture and mitigation groups to better prioritize resources. Externally, the US DHS has incorporated the library as a methodology of the IT Sector Baseline Risk Assessment [12]. Work on TAL at Intel continues, to adapt the library for use in narrow and broad baseline analyses. The approach is being fine-tuned for new applications in today's dynamic technology environment.

7. REFERENCES

[1] Thomas, R. C. 2009. Total cost of security: a method for managing risks and incentives across the extended enterprise. In *Proceedings of the 5th Annual Workshop on Cyber Security and information intelligence Research: Cyber Security and information intelligence Challenges and Strategies* (Oak Ridge, Tennessee, April 13 - 15, 2009). F. Sheldon, G. Peterson, A. Krings, R. Abercrombie, and A. Mili, Eds. CSIIRW '09. ACM, New York, NY, 1-4.

[2] Cheng, B. H. and Atlee, J. M. 2007. Research Directions in Requirements Engineering. In *2007 Future of Software Engineering* (May 23 - 25, 2007). International Conference on Software Engineering. IEEE Computer Society, Washington, DC, 285-303.

[3] Fenz, S. and Ekelhart, A. 2009. Formalizing information security knowledge. In *Proceedings of the 4th international Symposium on information, Computer, and Communications Security* (Sydney, Australia, March 10 - 12, 2009). ASIACCS '09. ACM, New York, NY, 183-194.

[4] Cardenas, A. A., Roosta, T., and Sastry, S. 2009. Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems. *Ad Hoc Netw.* 7, 8 (Nov. 2009), 1434-1447.

[5] Fruhwirth, C. and Mannisto, T. 2009. Improving CVSS-based vulnerability prioritization and response with context information. In *Proceedings of the 2009 3rd international Symposium on Empirical Software Engineering and Measurement* (October 15 - 16, 2009). ESEM. IEEE Computer Society, Washington, DC, 535-544.

[6] Daruwala, B., Mandujano, S., Mangipudi, N. K., and Wong, H. 2009. Threat analysis for hardware and software products using HazOP. In *Proceedings of the international Conference on Computational and information Science 2009* (Houston, USA, April 30 - May 02, 2009). V. Zafiris, M. Benavides, K. Gao, S. Hashemi, K. Jegdic, G. A. Kouzaev, P. Simeonov, L. Vladareanu, and C. Vobach, Eds. Recent Advances In Electrical Engineering. World Scientific and Engineering Academy and Society (WSEAS), Stevens Point, Wisconsin, 446-453.

[7] DG Abraham, GM Dolan, GP Double, JV Stevens. 1991. Transaction Security System. In *IBM Systems Journal Journal*, v 30 no 2 (1991), 206–229.

[8] Lukas Ruf, Consecom AG, Anthony Thorn, ATSS GmbH, Tobias Christen, Zürich Financial Services AG, Beatrice Gruber, Credit Suisse AG, Roland Portm*ann, Hochschule Luzer. Threat Modeling in Security Architecture -The Nature of Threats*. ISSS Working Group. Available at: http://www.isss.ch/fileadmin/publ/agsa/ISSS-AG-Security-Architecture__Threat-Modeling_Lukas-Ruf.pdf

[9] Kim, Y., Park, G., Kim, T., and Lee, S. 2007. Security Evaluation for Information Assurance. In *Proceedings of the the 2007 international Conference Computational Science and Its Applications* (August 26 - 29, 2007). ICCSA. IEEE Computer Society, Washington, DC, 227-230.

[10] Casey, Timothy. *Threat Agent Library Helps Identify Information Security Risks.* Available at: http://communities.intel.com/docs/DOC-1151

[11] Rosenquist, Matthew*: Whitepaper: Prioritizing Information Security Risks with Threat Agent Risk Assessment.* Available at: http://communities.intel.com/docs/DOC-4693

[12] Department of Homeland Security. *Information Technology Sector Baseline Risk Assessment*. August 2009. Available at: http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf