White Paper

Intel Information Technology

Computer Manufacturing

Enterprise Security

Threat Agent Library Helps Identify Information Security Risks

Intel IT developed a unique standardized threat agent library (TAL) that provides a consistent, up-to-date reference describing the human agents that pose threats to IT systems and other information assets. The TAL quickly helps risk managers identify accurately and understand the importance of relevant threat agents. The library consists of 22 standardized archetypes defined using eight common attributes; the archetypes represent external and internal threat agents ranging from industrial spies to untrained employees. The library is designed to overcome the lack of standard threat agent definitions and the problem that threat information is often fragmented and sensationalized.

Timothy Casey, Intel Corporation

September 2007

IT@Intel

Executive Summary

Our Intel IT Threat Assessment Group developed a unique, standardized threat agent library (TAL) that provides a consistent, up-to-date reference describing the human agents that pose threats to IT systems and other information assets. The TAL quickly helps risk management professionals (called risk managers in this paper) identify relevant threat agents and understand the importance of the threats.

The TAL provides a single standardized set of archetypal agent definitions ranging from government spies to untrained employees.

Threat information has historically been fragmented and sensationalized, with a lack of standard agent definitions. This made it difficult for risk managers to quickly and consistently assess risks from specific agents.

The TAL addresses these problems by providing a single standardized set of archetypal agent definitions ranging from government spies to untrained employees. To develop the TAL, we:

- Assembled a cross-functional team of security experts
- Devised eight common agent attributes and defined 22 agents based on unique combinations of these attributes
- Rated and described the threat that each agent represents to Intel. We regularly review and update this rating.

We recently published the library within Intel. Internal groups are using it both as a stand-alone tool and as part of other tools supporting standard risk assessment methodologies, helping to improve the consistency and accuracy of risk assessments.

We plan to enhance the library by developing agent definitions into full personas and by adding a matrix of common agent exploits.

Contents

Business Challenge

At Intel, risk management professionals (called risk managers in this paper) frequently assess threats to information assets such as corporate IT systems and data. To do so, they have to understand the potential human threat agents—the categories of people who can harm those information assets. Historically, however, this has been challenging.

A key problem has been the lack of industry standards or reference definitions of agents. People often have different concepts of even the most common agents, and they interpret a seemingly simple term such as "spy" very differently. This makes it difficult to share information or apply it consistently, and it leads to inconsistent profiles of the threats to systems.

Definitions in general use are often too vague to be valuable in risk management efforts. For example, people use the term "hacker" very broadly to describe almost anyone who intrudes into computer systems for any purpose. We need much more specific definitions in order to analyze and protect against threats from the possible categories of intruders such as data miners, organized crime members, and vandals.

Even if a risk management team can agree on the threat definitions, information about threats is often fragmented, sensationalized, and contradictory, making it difficult to understand the real threat and how to prioritize it. Some agents and their activities—such as people who create malware or hack into corporate systems—attract considerable publicity. This can result in the "TV news effect": the most-publicized agents appear to be the biggest threat, so they receive a disproportionately large percentage of limited mitigation resources.

In reality, there is a wide spectrum of less well known threat agents, including intellectual property thieves, members of organized crime, and well meaning but untrained employees who can unintentionally cause damage. Risk managers must carefully characterize and assess the threat from

all of these potential agents to assess overall risk to information assets. However, often there is little aggregated information available about the activity of these agents and the threat that they represent.

This lack of aggregated, consistent, up-to-date information makes risk assessment efforts considerably less efficient and more time consuming.

Risk managers might have to research potential agents and their recent activity to develop even a basic threat profile for a specific asset. In addition, risk management projects may experience "threat creep"—participants spend time repeatedly re-negotiating threat definitions as the project progresses, causing delays.

Threat Agent Library (TAL)

In 2005, we began looking for a solution to these problems. We looked for existing agent definitions that we could apply to our own projects, but we found nothing detailed enough for our needs.

We then decided to develop a library of archetypes representing the main threat agents relevant to Intel. We call this set of threat agents the Threat Agent Library (TAL). We focused our efforts on threats to information assets, although the library might also be used as a basis for identifying threats to other assets.

Our goal was to create a set of standardized definitions and descriptions of threat agents, along with a standard vocabulary for describing them. This would provide a common reference to help ensure consistent results. We also hoped that the TAL would:

- Act as a collection point for multiple, fractured threat information sources, making it easier to share information
- Enable risk management efforts to quickly identify and focus on threat agents relevant to specific assets
- Help IT professionals build system defenses appropriate for specific threats.

By including recognizable characters that embody key tactics and attributes of attackers, the TAL could enable these IT professionals to stay focused on the attacker mindset.

Developing the TAL

Intel IT assembled a cross-functional team of security specialists from different parts of Intel with expertise in corporate IT security, government security agencies, product security, law enforcement, and physical security. We believed that the team's broad experience dealing with real-world threats would enable us to counter the "TV news effect" and instead assess the real threat agents relevant to Intel. Over the life of the project, nearly two dozen senior subject matter experts contributed hundreds of hours to develop the library.

We focused on creating a finite set of archetypes representing significant threat agents, rather than attempting to define a new agent for every possible combination of agent characteristics. For example, in risk assessments involving internal spies, assessors often consider spies with dozens of combinations of money and skills available. Each of these combinations must be considered separately in the assessment, dragging the assessment out many days or weeks longer than necessary. By limiting the scope, we believed that we could develop a useful library that was compact, simple, and easily understood. Specific projects could then adapt or extend our definitions for their needs.

We tried to achieve a balance of detail and simplicity. We aimed to provide enough detail for agent definitions to be useful, while keeping the definitions simple enough for risk management professionals to quickly assimilate and use the information.

Our agents do not represent specific individuals, and our library is not intended to identify individuals or to be used for investigating actual security events.

To develop the library, we:

1. Created a simple taxonomy of eight attributes that we use to uniquely define each agent. The attributes also help risk managers identify which agents are relevant to each situation.
2. Created threat agent definitions based on the eight attributes, with a short description of each agent and its common tactics and actions. To date, we have identified 22 agents, as shown in Table 1.

Agent Attributes

We developed a common set of characteristics, or attributes, that we used to define each agent uniquely. We settled on eight attributes: intent, access, outcome, limits, resource, skill level, objective, and visibility.

Intent

This defines whether the agent intends to cause harm. Agents fall into two categories depending on their intent:

- **Hostile:** The agent starts with the intent to harm or inappropriately use Intel assets, and the agent takes deliberate actions to achieve that result.
- **Non-Hostile:** The agent is friendly and intends to protect Intel assets, but accidentally or mistakenly takes actions that result in harm.

Some Intel departments have added a third category called Environmental, to ensure that risk managers take into account uncontrollable and non-targeted threats occurring in the physical environment, such as fire, flood, pandemic, and military actions.

Table 1: Current Library of Threat Agents and Their Defining Attributes

	Intent	NON-HOSTILE			HOSTILE																	
		Employee Reckless	Employee Untrained	Info Partner	Anarchist	Civil Activist	Competitor	Corrupt Government Official	Data Miner	Employee Disgruntled	Government Cyberwarrior	Government Spy	Internal Spy	Irrational Individual	Legal Adversary	Mobster	Radical Activist	Sensationalist	Terrorist	Thief	Vandal	Vendor
Access (1)	Internal	■	■	■						■		■	■							■		■
	External				■	■	■	■	■		■			■	■	■	■	■	■		■	
Outcome (1-2)	Acquisition/Theft												■			■				■		
	Business Advantage						■	■	■			■			■							■
	Damage	■	■	■	■					■	■			■			■	■	■		■	
	Embarrassment	■	■	■		■				■	■			■	■		■	■				
	Tech Advantage						■	■	■			■	■									■
Limits (max)	Code of Conduct		■	■																		
	Legal	■													■							■
	Extra-legal, minor					■	■	■	■				■				■	■		■	■	
	Extra-legal, major				■					■	■	■		■		■			■			
Resources (max)	Individual	■	■	■						■				■						■		
	Club				■													■				
	Contest																				■	
	Team								■													■
	Organization					■	■						■		■	■	■		■			
	Government							■			■	■										
Skills (max)	None				■									■						■		
	Minimal		■															■				
	Operational			■						■											■	■
	Adept	■				■	■	■	■		■	■	■		■	■	■		■			
Objective (1 or more)	Copy					■	■		■			■	■		■							■
	Deny							■			■											
	Destroy				■					■	■								■			
	Damage									■	■								■			
	Take														■	■			■	■		
	All of the Above/ Don't Care	■	■	■										■			■	■			■	
Visibility (min)	Overt		■		■			■							■		■	■				
	Covert	■				■										■			■		■	
	Clandestine			■			■		■			■	■							■		■
	Multiple/Don't Care									■	■			■								

Source: Intel IT Threat Assessment Group, 2007

Access

This defines the extent of the agent's access to the company's assets. There are two options:

- **Internal:** Agent has internal access.
- **External:** Agent has only external access.

Outcome

This usually defines the agent's primary goal—what the agent hopes to accomplish with a typical attack. However, with non-hostile agents, such as an untrained employee, the outcome may be unintentional. The agent may use many methods to achieve this goal, and the primary goal may have secondary or ancillary effects. Possible outcomes are:

- **Acquisition/Theft:** Illicit acquisition of valuable assets for resale or extortion in a way that preserves the assets' integrity but may incidentally damage other items in the process.
- **Business Advantage:** Increased ability to compete in a market with a given set of products. The goal is to acquire business processes or assets.
- **Damage:** Injury to Intel personnel, physical or electronic assets, or intellectual property.
- **Embarrassment:** Public portrayal of Intel in an unflattering light, causing Intel to lose influence, credibility, competitiveness, or stock value.
- **Technical Advantage:** Illicit improvement of a specific product or production capability. The primary target is to acquire production processes or assets rather than a business process.

Limits

These are the legal and ethical limits that may constrain the agent. This characteristic also defines the extent to which the agent may be prepared to break the law. Options are:

- **Code of Conduct:** Agents typically follow both the applicable laws and an additional code of conduct accepted within a profession or an exchange of goods or services. Example: an auditor falls within the Information Partner agent archetype.
- **Legal:** Agents act within the limits of applicable laws. Example: Legal Adversary.
- **Extra-legal, minor:** Agents may break the law in relatively minor, non-violent ways, such as minor vandalism or trespass. Example: Activist.
- **Extra-legal, major:** Agents take no account of the law and may engage in felonious behavior resulting in significant financial impact or extreme violence. Example: members of organized crime organizations (Mobster agent).

Resource

This defines the organizational level at which an agent typically works, which in turn determines the resources available to that agent for use in an attack. This attribute is linked to the Skill Level attribute—a specific organizational level implies that the agent has access to at least a specific skill level. Options are:

- **Individual:** Resources limited to the average individual; agent acts independently. Minimum skill level: None.
- **Club:** Members interact on a social and volunteer basis, often with little personal interest in the specific target. An example might be a core group of unrelated activists who regularly exchange tips on a particular blog. Group persists long term. Minimum skill level: Minimal.
- **Contest:** A short-lived and perhaps anonymous interaction that concludes when the participants have achieved a single goal. For example, people who break into systems just for thrills or prestige (agent Cyber-Vandal) may run contests to see who can break into a specific target first. Minimum skill level: Operational.
- **Team:** A formally organized group with a leader, typically motivated by a specific goal and organized around that goal. Group persists long term and typically operates within a single geography. Minimum skill level: Operational.
- **Organization:** Larger and better resourced than a Team; typically a company. Usually operates in multiple geographies and persists long term. Minimum skill level: Adept.
- **Government:** Controls public assets and functions within a jurisdiction; very well resourced and persists long term. Minimum skill level: Adept.

Skill Level
The special training or expertise an agent typically possesses. Options are:

- **None:** Has average intelligence and ability and can easily carry out random acts of disruption or destruction, but has no expertise or training in the specific methods necessary for a targeted attack.
- **Minimal:** Can copy and use existing techniques. Example: Untrained Employee.
- **Operational:** Understands underlying technology or methods and can create new attacks within a narrow domain.
- **Adept:** Expert in technology and attack methods, and can both apply existing attacks and create new ones to greatest advantage. Example: Legal Adversary.

Objective
The action that the agent intends to take in order to achieve a desired outcome. Options are:

- **Copy:** Make a replica of the asset so the agent has simultaneous access to it.
- **Destroy:** Destroy the asset, which becomes worthless to either Intel or the agent.
- **Injure:** Damage the asset, which remains in Intel's possession but has only limited functionality or value.
- **Take:** Gain possession of the asset so that Intel has no access to it
- **Don't Care:** The agent does not have a rational plan, or may make a choice opportunistically at the time of attack.

Visibility
The extent to which the agent intends to conceal or reveal his or her identity. Options are:

- **Overt:** The agent deliberately makes the attack and the agent's identity is known before or at the time of execution.
- **Covert:** The victim knows about the attack at the time it occurs, or soon after. However, the agent of the attack intends to remain unidentified.
- **Clandestine:** The agent intends to keep both the attack and his or her identity secret.
- **Don't Care:** The agent does not have a rational plan, may make a choice opportunistically at the time of attack, or may not place importance on secrecy.

The Agents

To define the agents, we used an iterative process that began with a simple one sentence description of each agent. Our cross-functional team then progressively refined these definitions using the team's experience supplemented with outside references and expertise. Each agent has a unique set of attribute values, as shown in Table 1.

In addition to ensuring the uniqueness of each agent, this approach would enable risk managers to select relevant agents by first identifying the attributes that an agent must possess in order to represent a threat. We aimed to create agent definitions that were specific enough to be useful in risk assessments. For example, instead of defining a single agent to encompass all the current uses of the term "hacker," we defined several different agents. One of these, Cyber Vandal, represented one original meaning of the term hacker: someone who intends to intrude into systems for thrills or prestige among peers. However, we also developed other real-world agents such as Data Miner, Internal Spy, Mobster, Government Spy, and Government Cyberwarrior to cover other agents that often are described using the umbrella term hacker.

The information that we provide to risk managers includes the matrix of agents and their attributes (as in Table 1) and a text-based summary reference list including brief descriptions of the agents, their common tactics, and current ratings, as shown in Table 2.

Some Intel business units add environmental agents such as natural disasters and pandemics to the library of human agents, to ensure that assessors take them into consideration. However, providing more detail about these is beyond the scope of our group, so these business units must consult other resources, such as local authorities and Intel security SMEs within the affected area, to characterize and assess those threats.

Table 2. Summary Agent Information (Strength of Threat rating is proprietary and not included here.)

	Agent Label	Insider	Common Tactics/Actions	Description
Hostile	Anarchist		Violence, property destruction, physical business disruption	Someone who rejects all forms of structure, private or public, and acts with few constraints
	Civil Activist		Electronic or physical business disruption; theft of business data	Highly motivated but non-violent supporter of cause
	Competitor		Theft of IP or business data	Business adversary who competes for revenues or resources (acquisitions, etc.)
	Corrupt Government Official		Organizational or physical business disruption	Person who inappropriately uses his or her position within the government to acquire company resources
	Cyber Vandal		Network/computing disruption, web hijacking, malware	Derives thrills from intrusion or destruction of property, without strong agenda
	Data Miner		Theft of IP, PII, or business data	Professional data gatherer external to the company (includes cyber methods)
	Employee, Disgruntled	X	Abuse of privileges for sabotage, cyber or physical	Current or former employee with intent to harm the company
	Government Spy	X	Theft of IP or business data	State-sponsored spy as a trusted insider, supporting idealistic goals
	Government Cyberwarrior		Organizational, infrastructural, and physical business disruption, through network/computing disruption, web hijacking, malware	State-sponsored attacker with significant resources to affect major disruption on national scale
	Internal Spy	X	Theft of IP, PII, or business data	Professional data gatherer as a trusted insider, generally with a simple profit motive
	Irrational Individual		Personal violence resulting in physical business disruption	Someone with illogical purpose and irrational behavior
	Legal Adversary		Organizational business disruption, access to IP or business data	Adversary in legal proceedings against the company, warranted or not
	Mobster		Theft of IP, PII, or business data; violence	Manager of organized crime organization with significant resources
	Radical Activist		Property destruction, physical business disruption	Highly motivated, potentially destructive supporter of cause
	Sensationalist		Public announcements for PR crises, theft of business data	Attention-grabber who may employ any method for notoriety; looking for "15 minutes of fame"
	Terrorist		Violence, property destruction, physical business disruption	Person who relies on the use of violence to support personal socio-political agenda
	Thief	X	Theft of hardware goods or IP, PII, or business data	Opportunistic individual with simple profit motive
	Vendor	X	Theft of IP or business data	Business partner who seeks inside information for financial advantage over competitors
Non-Hostile	Employee, Reckless	X	Benign shortcuts and misuse of authorizations, "pushed wrong button"	Current employee who knowingly and deliberately circumvents safeguards for expediency, but intends no harm or serious consequences
	Employee, Untrained	X	Poor process, unforeseen mistakes, "pushed wrong button"	Current employee with harmless intent but unknowingly misuses system or safeguards
	Information Partner	X	Poor internal protection of company proprietary materials	Someone with whom the company has voluntarily shared sensitive data

Source: Intel IT Threat Assessment Group, 2007

Agent Ratings

The attributes of agents generally remain stable while the strength of their threat may change over time. For example, agents may engage in different activities, become increasingly common or powerful, or select different types of targets.

To ensure that Intel risk managers have an up-to-date picture of the threat that each agent currently represents to Intel, we:

- Provide a current rating for each threat agent based on factors such as the agent's recent activity. We rate the threat on a scale from low to high.
- We review and update this rating every six months and issue security briefings if significant changes occur.

To rate each threat, we assess the current level of activity of the agent and how relevant that activity is to Intel, using internal and external information such as government and industry reports. In some cases, our assessment is qualitative. In other cases, we may have good quantitative data such as help desk records of problems that are due to errors by untrained employees.

Our ratings include a description of current activities and incidents as well as background information about the agent. Abbreviated example ratings are shown in the Mobster detail box on the next page. The rated level of threat that each agent currently represents is proprietary to Intel and is not included here.

Agent Rating: Mobster

Manager of an organized crime organization

- Access: External
- Limits: Extra-legal, major
- Minimum Skills: Adept
- Visibility: Covert
- Outcome: Acquisition/Theft
- Resources: Organizational
- Objective: Take

Background

Summary: Mobsters lead organizations with a broad range of capabilities and functions, and may already be publicly known as leaders of organized crime. They are adept at utilizing their people and resources to force change in order to achieve their goal. For example, they are typically external but often can get access to insiders and other resources to drive changes facilitating even greater access.

Activity: Organized crime organization activity has increased over the past five years in the areas of technology theft and cybercrime. This rise has been well documented. The ease and relative anonymity of cybercrime especially suits the needs of these organizations, and they are expanding their capabilities in this area. Additionally, since they are relatively new to the field, they are rapidly innovating new and unpredictable methods of operation. Most crime organizations are well funded and see technology theft and cybercrime as lucrative and worth significant investment. This investment usually includes either converting or planting insider agents into government and private organizations. In some areas of the world there are strong ties between organized crime and local government.

Target: U.S. semiconductor technology is a popular target for organized crime. Processors are profitable and are easily stolen and resold on the black market. Furthermore, large technology suppliers undoubtedly represent attractive targets to a number of organizations, with nearly every business and technical area subject to attention and potential attack. More generally, other activities such as online gambling could enable the agent to blackmail employees with personal problems to provide assistance from the inside. Theft of personal identity information is a new and growing opportunity for this agent.

Evaluation Considerations: This agent is external, but it uses organizational influence to change the playing field and leverage its contacts. The agent can assert almost unlimited influence in procuring intellectual property and the sale or distribution of goods.

Mobsters use various methods, including insider manipulation and outright armed robbery. The agent's main impact is theft. The agent may resell stolen assets through covert (and difficult to trace) channels to avoid detection, taxes, and regulations. Activity is largely opportunistic with business-driven, objective-oriented, and savvy participants who are good at hiding and gaining legal protection.

Using the TAL

Risk management professionals and IT specialists can use the library to select agents by characteristics or with a pre-defined risk assessment methodology.

We believe that the library can enable risk managers to quickly select relevant agents and safely ignore the rest, potentially increasing the speed and efficiency of security assessments.

Selecting Agents by Attributes

Using this method, risk managers identify the attributes necessary to pose a threat to a specific asset. Participants then select agents based on these attributes and other relevant information.

For example, if we are concerned about recent damage to certain assets, and our assessment is that an agent had to have internal access to cause this damage, we might select the threat attribute Insider. If we identified the presence of untrained employees and a high accident rate, we might refine the selection to the threat agent Untrained Employee.

We recommend strongly that risk managers first identify attributes rather than selecting agents based on their names. Partly because people have preconceptions about the meaning of names, selecting by agent name can lead to misinterpretation, complacency, and overlooking less obvious options. Furthermore, because the library consists of archetypes rather than exact descriptions of individuals, an exact match is not possible or desirable.

Table 3. Example Questions to Identify Relevant Threat Agents

Example Questions	Agent Characteristics Identified
What is your most important asset and why?	Helps identify agents who could damage the specified asset, such as technology or intellectual property. Helps assess the greatest potential impact as well as the type of asset threatened.
Are the assets located in a country perceived to have a high rate of corruption?	Importance of government agents.
Are all the employees who use this asset regularly trained or certified on using the asset? What's your current accident rate?	Potential damage from unskilled employees.
If applicable, would violent acts toward your assets cause a significant business disruption?	Danger from violent agents.
How easily could a malicious insider impact your assets?	Danger from hostile internal agents.
How much skill would a person require to damage the asset or to gain unauthorized access?	Minimum skill level required.
Have all of your information or NDA partners been vetted to corporate security standards?	Potential threat from partners or insiders.

Source: Intel IT Threat Assessment Group, 2007

Government and Industry Collaborating to Protect IT Sector Infrastructure

In May 2007, The United States Department of Homeland Security published the IT Sector Specific Plan (IT SSP), which supports the National Infrastructure Protection Plan. The IT SSP is a planning document that provides guidance on how public and private entities will work together to protect IT sector infrastructure.

The IT SSP represents an unprecedented collaboration between public and private IT sector entities to address complex, critical infrastructure protection challenges. Public-private working groups are building upon the momentum from IT SSP development, and Intel's Threat Agent Library is being used by one of these groups to refine the sector's risk management approach and threat analysis methodology.

To learn more about the IT SSP, visit www.dhs.gov.

To help identify attributes of relevant agents, our team developed example questions, some of which are shown in Table 3. Risk managers can use these as a basis for developing a full set of questions to use when interviewing IT managers and professionals during risk assessments.

Use within Risk Assessment Methodologies

Intel is beginning to use the TAL within two risk assessment methodologies.

1. An Intel IT methodology that simultaneously addresses both general business risks and information security specific risks. The TAL is available within a tool that supports this methodology.

2. A risk model-based methodology to perform regular security evaluations of Intel's manufacturing systems.

The security evaluations in the second method rely on the expertise of the professionals who manage specific assets, such as servers and product tracking terminals. These experts provide quantitative assessments of the security of these assets based on their experience and knowledge; risk managers then include these assessments in a broader evaluation of the security of manufacturing systems.

The accuracy and consistency of these evaluations therefore depend in part on the ability of IT professionals to assess threats to the assets they manage. In turn, each IT professional's assessment depends on his or her knowledge of possible threats.

Intel manufacturing groups have begun making the TAL available to professionals in manufacturing IT. This provides them with a consistent set of information that they can use as a basis for their risk assessments, and provides them with information about potential threat agents that they might not otherwise consider. We expect that this will lead to more consistent evaluations and improve the overall accuracy of risk assessments.

Some manufacturing groups have already used the TAL in risk assessments. In one project, this reduced the time required for the risk assessment by an estimated 30 percent, saving many hours of experts' time. Before the TAL was available, participants spent a considerable amount of time discussing and reaching agreement on definitions of agents. The TAL accelerated this stage by providing predefined agents as a basis. Participants could review the definitions before meetings, further accelerating the process.

Participants then evaluate the risk that these agents pose to specific assets. The agent ratings help with this process by describing agents' activities, including which assets they target.

With the risk model-based methodology, Intel uses a spreadsheet to calculate risks based on data from participants about assets, threats, and vulnerabilities. The TAL agents have been incorporated into the spreadsheet; data developed by participants plugs directly into risk calculations, helping generate more accurate and consistent risk assessments.

The TAL may also be helpful for other purposes at Intel's massive global manufacturing organization. For example, it could provide a common language facilitating discussions about security issues among manufacturing groups worldwide.

Future

We are planning two significant TAL enhancements.

Threat Personas

Product designers increasingly use the persona technique to model potential customers. This helps the designers focus on their target audience. In that context, a persona is a description of an archetypal customer. The definition includes typical characteristics and behaviors.

We expect to use the same approach to develop threat personas that model potential attackers. Our goal is to help our system designers get a clear picture of the attacker mindset and stay focused on it during system design.

Matrix of Exploits

We plan to create a matrix listing each agent's common attacks and other exploits. We believe this will help us prepare against specific possible types of attack.

When conducting a risk assessment, this matrix will help us quickly map threats to vulnerabilities that we need to cover. As a simple example, if we determine that Mobster is a key threat agent, the matrix might show that mobsters have recently been using phishing attacks (fake emails soliciting financial or other information). Security specialists could then check training logs to determine whether users have recently received training on how to resist these attacks.

Conclusion

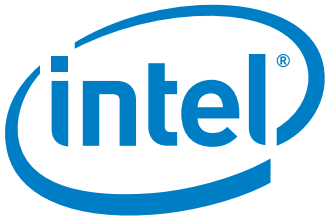
We believe that the TAL provides a valuable reference source of standardized threat agent information that can accelerate and improve risk assessments. We expect to realize benefits as we increase our use of the TAL and integrate it into our risk assessment methodologies. We believe that there is a strong need for such standardized threat agent information, and we hope that other organizations will also find the TAL useful.

Authors

Timothy Casey is a senior security analyst with Intel Information Technology.

Acronyms

TAL	Threat Agent Library
IT SSP	Information Technology Sector Specific Plan



www.intel.com/IT

Printed in USA
0907/SEP/RDA/PDF

Please Recycle
ITAI Number: 07-2202w