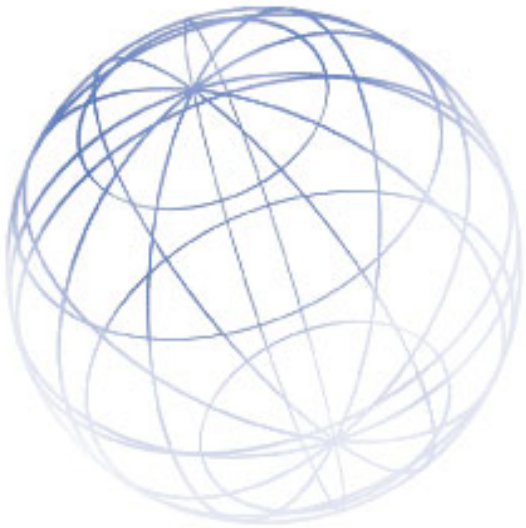
SignaCert

User Stories / Use Case Identification

Ryan McMahon

March 1, 2006



503-227-2207
115 SW Ash Street
Suite 430
Portland, OR 97204-3549

www.signacert.com

Table of Contents

Introduction **2**
Purpose 2
Audience 2
References 3
Actors **3**
Harvesting Actors 3
Validation Actors 5
Triggering Events **7**
Validation Triggers 7
Harvest Triggers 8
Trigger Matrices 9
User Stories **10**
Application Validation 10
Forensics 11
Gold Image Verification 11
Help Desk 11
System Integrity 12
Trusted Network Connect 12
Risks / Areas to Contemplate 12

Introduction

Purpose

This document is a work in progress. The intent is to provide a description of who will use and how they will use the system and its capabilities to identify the appropriate use cases.

This document will describe the basic user types and their attributes. It will also describe the types of triggers that initiate services and capabilities.

Audience

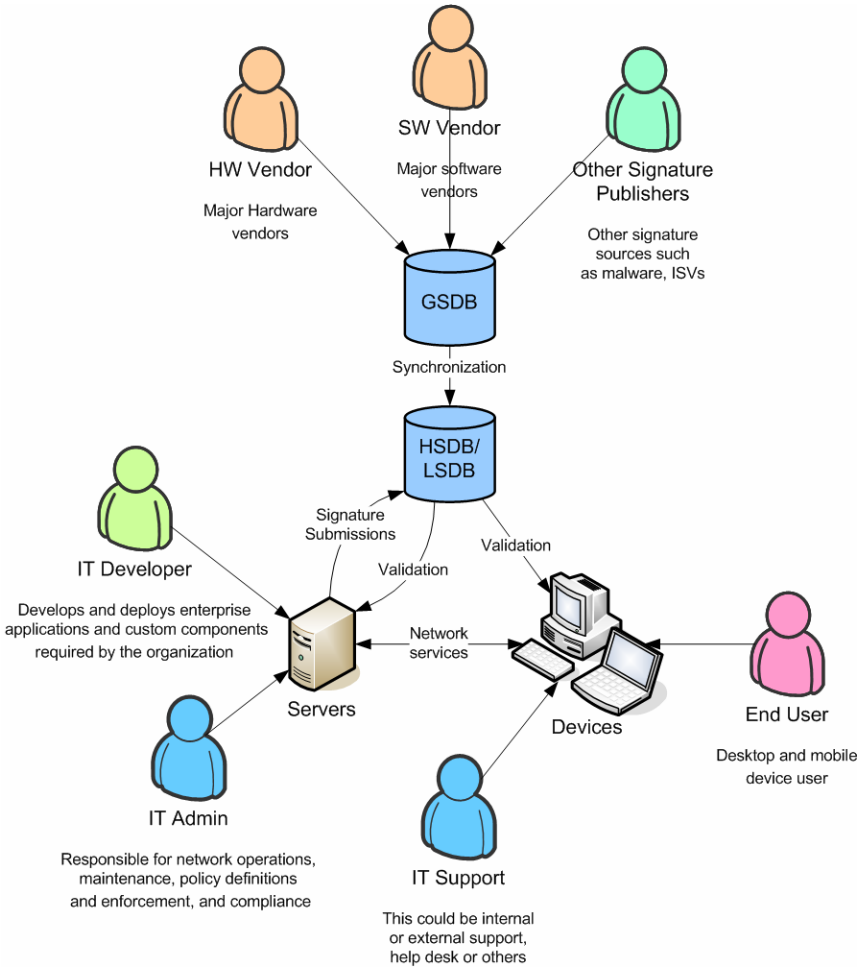
This document will be used both internally with the engineering group and externally with customers and partners. Specifically the customer audience are members of large company IT staff including the CIO, systems architects, and Sr. IT managers. Similarly, partner customers will include large company CIOs, Sr. Architects and IT managers, but will also include business line managers, such as Customer Support, and Professional Services.

References

This document builds on concepts discussed in the SignaCert Signature Repository System Description.

Actors

The following diagram describes the various actors that interact with the offerings and their most basic relationships. The section below describes in detail how each actor relates to the others and the business processes they use to interact with our offerings.



Harvesting Actors

HW Vendors

This group publishes signatures for firmware used by their devices to the signature repository. The major value for them is to help make it easier for

their customers to make sure they received the correct products, from authentic sources and to verify they are configured properly.

These actors do not receive a direct benefit from developing a harvesting relationship, but their customers' demand for improved reliability, robustness and security, will drive them to adopt. Harvesting relationships will prove to be a key early differentiator for several players in this space but, as trusted computing becomes more important, attestation capability will be required for parity.

Core Issues

- Making sure devices have not been altered
- Making sure devices are up to date
- Verifying that a device is in a known good state

SW Vendors

Much the same as HW Vendors, this group publishes signatures for application s they develop to the signature repository. The major value for them is to help make it easier for their customers to verify they received source authentic products and that they are configured properly.

This group includes operating systems vendors, enterprise application vendors, and desktop application vendors. Typically this group has significant market share in the products they produce.

These actors do not receive a direct benefit from developing a harvesting relationship, but their customers' demand for improved reliability, robustness and security, will drive them to adopt. Harvesting relationships will prove to be a key early differentiator for several players in this space but, as trusted computing becomes more important, attestation capability will be required for parity.

Core Issues

- No mechanisms for verifying / validating state of software running on end users' machines
- Customer support diagnoses are costly and may not be related to their products

Signature Sources

Other signature sources may include independent software vendors (ISVs) or malware signature sources.

ISVs represent a significant quantity of products, many are niche products and few have significant market share. These vendors will be challenged to stay up with the major software vendors in relationship to trusted computing and authenticity and attestation capabilities. Customers demand will drive integration of these capabilities. They will look to some third party to help

them solve these problems or go without as these capabilities are not easily replicated.

Malware signature sources may not have any vested interest in broadly distributing their data. Several companies differentiate themselves through the fast detection and distribution of signatures to antivirus software. Because a great deal of effort is required to do this, these vendors will guard the information and are not likely to share it until it marginal value is greatly diminished. The possibility exists that community parties that aggregate this content may seek out a solution for broad distribution of the information, but this should not be counted on.

Core Issues

- No mechanisms for verifying / validating state of software running on end users' machines
- Customer support diagnoses are costly and may not be related to their products

IT Developer

Charged with developing custom applications and for systems integrations. IT developers can be internal or external staff, but are charged with building components, middleware, or other elements required for systems integration. These guys work with the IT Admin to build a complete solutions. When development is complete, they need to roll out the components in a risk controlled way to make sure other systems are not broken or otherwise impacted.

Core Issues

- Building custom applications
- Building middleware
- Integrating existing applications (Sales, financial, CRM, etc.)
- Making sure their elements are not impacted by other systems

Validation Actors

End User

The end user is the person who uses computers or mobile devices on a daily basis. These include novice and expert computer users both, but neither are willing to jump through a bunch of extra hoops to make computing more safe (computers are complicated enough!) End users want their computers their computer to be reliable and "just work" and want the activities they use computers for to be safe and secure.

As individuals, these actors will not demand "trusted-computing" per se, but they do have a latent need to have simple, reliable, and secure computers.

Typically our users will be part of a network or organization that makes attestation services available. As a consumer they may belong to Dell's

customer support network. As a company employee, the IT department will provide these services.

Core Issues

- Keeping their computers working
- Protecting their personal information
- Protecting corporate assets

IT Support

This group is charged with deploying and maintaining end user devices as well as providing technical support.

IT support builds machines from a predefined hardware and software specification, a “gold image.” This image is specific to the HW and SW required by users and must be updated to reflect the “vintage” of devices. The quantity of gold images for a company may be large.

The typical maintenance process involves addressing issues after they are identified when they are impeding user’ ability to get work done. The amount of IT support required can have dramatic impacts on the IT budget as support costs are proportional to effort expended. Reducing the amount of support required by each end user means IT staff can support more end users with fewer people.

Typically this actor is internal to a company, but in some cases it can be external. For example, when Dell provides IT support to end users it is an external resource.

Core Issues

- Validating Gold images
- Diagnosis / Troubleshooting
- System Maintenance

IT Admin

IT Administrators are charged with operations of company IT systems. This set of actors must design, implement, and maintain systems that support the rest of the business. They must react to dynamic needs of the user population and address changing needs of business systems (integration of operations and finance systems, inclusion of MRP with shipping, etc.).

Core Issues

- System up time
- Systems patching
- Security Analyses
- Building Gold images
- Define and set policy

Triggering Events

Validation Triggers

The following describes the types of triggers that occur and under what conditions they will call the Validation processes. These triggers typically occur in a client side code that implements policy, where validation information is being called as a service. Other cases exist where server side code triggers a validation / interrogation of another device.

- **Bootup**—When a device is powered up or started, it may require attestation as a checkpoint in the startup process. This may occur at many different places in the startup process depending on the HW / SW vendors implementation. This will typically trigger a validation process, but could trigger other processes as well

- **Application start—**Starting an application should be a trigger for validating that application. This should be a policy decision implemented by the IT Admin as to whether or not this occurs. Validating an application as it is launched will allow "incremental" state validation to occur, rather than requiring a full scan on a regular basis.

- **Network connect—**When a device connects to an network, that device's state should be validated prior to granting access. This would trigger a measurement based on IT admin set policy. The measurement could be a complete scan or a partial to check the critical components on the connecting device.

- **Scheduled event—**Time based triggers allow validation at regular intervals.

- **Event triggered—**It should be possible for an event to trigger a validation. This could be based on network conditions or other events.

- **Manual validation—**There may be cases where a validation is triggered manual to allow specific elements to be validated. This could be a tool used by end users who want to validate their own system. It could also be a tool for IT support that allows them to validate specific elements as part of diagnoses.

    - **Support request—**When a user calls the Helpdesk, they should be able to trigger a validation of the callers device to start the diagnosis process. This could be triggered as part of the request to the Help desk so that the relevant information is available prior to the staffer getting on the phone.

    - **Out-of-box verification—**When a device is powered up for the first time, a validation could be triggered to make sure the

device is in the original shipped state. This validation could also be used to identify if the device need to be updated.

- **Forensic analysis—**Crash cart analysis will require a manually triggered validation of another device. This trigger is issued by the IT support staffer as part of the diagnoses.

Harvest Triggers

The following events trigger signatures to be harvested and published to the signature repositories. These triggers include both automated an manual processes.

- **SW or HW Release—**When software or hardware (with a firmware image) is released or updated, their signatures must also be updated. This process could be triggered by an automated build process (major software producer) or a manual process such as the release of ISV produced product.
- **Gold Image Definition—**When a new image is defined its configuration and signature set must be updated.
- **Release custom components—**Similarly to the Gold Image, when new or custom IT components are released, their signature sets should be captured. Typically this will be a manual process.
- **Manual Editing—**There will be cases where the signatures, their associated configuration information, or their metadata require editing. This should be an infrequent occurrence requiring special care from the publisher / harvester.
- **Manual Harvesting—**Otherwise called Self-Harvesting. This trigger occurs when an organization has limited need for automated processes, or when a target application doesn't exist and the customer needs to measure against that application. This allows signature capturing for cases where vendors are not actively publishing their signatures.
- **Historical publishing—**Customers may have a need to publish signatures captured with older systems, porting them to the signature repository. This will occur most often at SignaCert, but may be an issue for some customers that want to use the HSDB or LSDB products.

Trigger Matrices

The following matrices show the interrelationships between triggers and users and triggers and processes / functions.

Key: ⊙ = Frequently ⊙ = Infrequently - = Not applicable

Triggers	User Roles	End User	IT Support	IT Admin	IT Developer	HW Vendor	SW Vendor	Signature Source
Validation	Bootup	⊙	⊙	⊙	⊙	-	-	-
	Application start	⊙	⊙	⊙	⊙	-	-	-
	Network connect	⊙	⊙	⊙	⊙	-	-	-
	Scheduled event	⊙	⊙	⊙	⊙	-	-	-
	Manual validation	⊙	⊙	⊙	⊙	-	-	-
	Event triggered	⊙	⊙	⊙	⊙	-	-	-
	Helpdesk / support	⊙	⊙	⊙	⊙	-	-	-
	Out of box verification	⊙	⊙	⊙	⊙	-	-	-
	Forensic analysis	-	⊙	⊙	-	-	-	-
Harvest	SW or HW Release	-	-	-	-	⊙	⊙	⊙
	Gold Image Definition	-	⊙	⊙	-	-	-	-
	Release custom components	-	-	⊙	⊙	-	-	-
	Manual Editing	-	-	⊙	-	⊙	⊙	⊙
	Manual Harvesting	-	-	⊙	-	-	⊙	⊙
	Historical publishing	-	-	⊙	-	⊙	⊙	⊙

Table 1. The frequency of trigger occurrence by user.

Triggers	Processes	Authentication	Validation Application Validation	Integrity Score	Signature Submission	Configuration Submission	Edit Submissions	Auditing & Reporting
Validation	Bootup	⊙	⊙	⊙	⊙	-	-	-	-
	Application start	⊙	⊙	⊙	⊙	-	-	-	-
	Network connect	⊙	⊙	⊙	⊙	-	-	-	-
	Scheduled event	⊙	⊙	⊙	⊙	-	-	-	-
	Event triggered	⊙	⊙	⊙	⊙	-	-	-	-
	Manual validation	⊙	⊙	⊙	⊙	-	-	-	-
	Helpdesk / support	⊙	⊙	⊙	⊙	-	-	-	-
	Out of box verification	⊙	⊙	⊙	⊙	-	-	-	-
	Forensic analysis	⊙	⊙	⊙	⊙	-	-	-	-
Harvest	SW or HW Release	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
	Gold Image Definition	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
	Release custom components	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
	Manual Editing	⊙	-	-	-	⊙	⊙	⊙	⊙
	Manual Harvesting	⊙	-	-	-	⊙	⊙	⊙	⊙
	Historical publishing	⊙	-	-	-	⊙	⊙	⊙	⊙

Table 2. The frequency of trigger occurrence by process / function.

User Stories

Application Validation

Story

IT Admin is responsible for a server farm providing a high availability service for which it is unacceptable to run full file system scans due to performance reasons.

1. IT Admin builds a custom apache component, as in the golden baseline use case, and submits it to a local SDB.
2. Servers start. As modules are loaded they file components are hashed and submitted against the SDB.
3. The IT admin is notified of any modules that do not match an entry in the SDB.

Details

This story covers two use cases; a customer harvesting a custom configuration and an validation by an end user.

Forensics

- Forensics analyst obtains suspect system.
- Analyst initiates a system scan with the intention of determining which file elements are know and which are unknown.
- Elements are submitted against a SDB to determine if they exist in the database.
- Elements that do not exist in the database are subject to further forensic analysis. Elements that exist in the SDB are not forensically interesting as they are well known standard elements.

Gold Image Verification

IT admin wants to validate a standard images is composed of standard authentic components.

- IT admin creates a new standard image
- Before checking the image into the image library, the IT admin initiates the validation process to determine if all components of the image are authentic.
- Based on the knowledge of what components should be on the system, each component is checked for validity.
- Any exceptions that do not match are presented to the IT admin organized by component.
- IT admin reviews exceptions and validates the changes are actually intended.
- Assuming they are, he creates a submission of a one or more new components and submits it to a local database.

IT admin wishes to be notified whenever a system based on the system image deviates from the standard.

- A user upgrades video driver.
- IT administrator is notified that the system has a deviation. The notification includes information of what components have been deviated.
- IT admin restores component or entire system as appropriate.

Help Desk

Case 1: Diagnosing problem via SDB

- User can't browse web because their browser has been compromised so that it constantly brings up pop-up advertisements (a DLL has been modified by a Trojan).
- User calls help desk and describes problem.
- Help Desk employee initiates a scan of critical components for that specific system. They may have to ask the user to initiate this scan.
- A set of critical files that don't match the authentic state are identified. This information is sent to the help desk employee along with metadata that specified the product name and version of the mismatched files.
- Help Desk employee determines what the correct version of the software is and restores the software on the users machine.

Case 2: Before we give support we want to ensure that the user has authentic hardware and software

- Customer contacts support because firewall device is not working properly.
- Support has customer connect to device and issue a validation command. This produces a report that is sent to support automatically or manually.
- Support validates the report against their product DB and our SDB.

System Integrity

Scenarios:

1. Make sure these components are on the machine and are valid.
2. Make sure no "bad" files/components are on system.
3. Tell me when new files/components are added to system.
4. Ignore certain files/dirs.

Trusted Network Connect

1. Employee attempts VPN connection with corporate VPN server
2. Client prompts for user credentials
3. VPN server determines set of elements to validate for this specific client
4. Client calculates signatures for set of elements to validate
5. Client sends signatures to VPN server
6. VPN server validates signatures
7. VPN server determines level of access for client
8. VPN server informs client of access
9. VPN restricts level of access to network
10. Client completes connection

Risks / Areas to Contemplate

Risks / Areas to contemplate

1. Integrate vs. Write (Client apps)
2. Scan level (pertaining to above)
3. Schema
    - Composite pattern
    - Inheritance
    - Overriding
4. Access Methods
    - SOAP
    - SQL
    - HTTP Post
5. Local Population
    - On demand
    - Manual
6. Vetting process
7. User Roles