Business Process Security

Managing the new security challenge with X-Tra Secure

Bartjan Wattel
ThunderStore BV
's-Hertogenbosch, The Netherlands
info@thunderstore.com

Abstract: The process of security is destined to fail if it does not protect the process of business. Despite a record investment in security by corporations around the globe, the frequency, variety and financial cost of attacks continues to rise. And while most organizations focus their defenses on external threats from hackers and virus authors, the real security challenge is much closer to home. If security professionals want to avoid falling into the trap of trying to protect everything all the time, they need to refocus their defenses on authorized users and the resources they have access to.

Key words: business process security, X-Tra Secure, security policy, monitoring, privileges

1. THE HOLE IN THE FENCE

The rush to protect the enterprise from the Internet has resulted in a widely adopted security strategy that is full of gaping holes, and one which often has security administrators facing the wrong way.

Traditional security thinking will always be flawed for two fundamental reasons:

- It assumes that the most serious attacks come from beyond the corporate perimeter;
- It assumes that the most serious attacks will come from hackers, virus authors, and other unauthorized outsiders.

M. Gertz et al. (eds.), *Integrity, Internal Control and Security in Information Systems*

For this reason most security spending had been focused on keeping hackers and virus authors from penetrating the outermost perimeter. And most of the technology focus has been on security tools that will defend these types of attacks, most notably network monitoring, intrusion detection, firewall, and anti virus.

But the significant increase in attacks on corporate networks has exposed perimeter security as little more than fighting wild fires. As the security team rushes to patch a newly discovered breach in the perimeter, two more appear.

And just as they think they have accurately mapped the perimeter, it changes again. The growing army of mobile, home, and tele workers has extended the corporate perimeter into hotels, taxis, and employee living rooms.

According to IDC there are now more than 38 million home and mobile workers in the United States, and growing fast. And every time an employee takes an unprotected laptop out of the office, they punch a hole straight through the perimeter that might only be discovered by a successful attack.

The perimeter will continue to grow, to incorporate branch and international offices, and to accommodate the need for customers, partners, and suppliers to access corporate intranets. And the increase in use of wireless devices and wireless networks will not only reshape the already fluid perimeter, it will introduce an entirely new set of security vulnerabilities already discovered in wireless protocols.

And while security professionals have long recognized the importance of increasing security awareness amongst employees, the focus of this awareness is usually on external intruders, and not on the employees themselves.

The role of security policy has been recognized as the foundation of any effective security strategy, but security professionals have yet to find a way to enforce that security policy around the clock, on every employee, and for every business process, short of stationing a security guard at every desktop, laptop, and wireless device.

2. THE USER SECURITY TRAP

Perimeter defenses like firewalls and intrusion detection systems are essential components in any defense, but their effectiveness is severely limited when the threat is trusted, and is located behind the perimeter.

"Employees are your security," claimed former hacker Mudge in an interview with CIO magazine. He was echoing a widely held view, even in the hacking community, that employees and authorized users now play a critical role in security. According to the most recent security survey by the Computer Security Institute and the FBI, 86% of respondents cited trusted insiders as a major security concern.

An earlier report from the CSI found that while the average cost of an attack by an outside hacker cost $57,000, the average cost on an attack by a trusted insider was $2.1 million, or thirty-six times as much.

And while many organizations acknowledge the role employees must play in protecting the enterprise, that role is usually limited to better vigilance and awareness against those very same external attacks on the perimeter.

Few companies have been able to successfully address the more important user security challenge – that of their own everyday behavior in the workplace, and their compliance with security rules and policies.

According to a recent report by research group Forrester "despite an expected 300 percent spending increase on information technology security spending over the next four years, bad decision-making will leave U.S. companies almost as vulnerable to security breaches as they are today."

Why? The report explains that "rather than focusing on key business assets, companies will waste billions of dollars on external security spending, falling into the trap of trying to protect everything."

The view is shared by research firm Gartner Group: "Despite the recent notoriety of external attacks, internal threats continue to pose the greatest threat to the exposure and compromise of sensitive corporate information. Identifying vendors who offer a realistic solution to this very complex monitoring problem will be the next challenge facing all security professionals."

By overlooking the security vulnerabilities of their own automated business processes, says Forrester, companies put themselves at great risk.

"A company is not secure if it installs a firewall system, but does not have application security in place to ensure an approved user does not fraudulently wire money to his Swiss bank account or does not trade above his daily limit," said Lorenzo De Leon, CEO of Saecos Corporation, a Chicago-based security firm focused on the financial community.

3. SECURITY IN AN IDEAL WORLD

How much easier security would be if policies could be created and tested with ease, distributed instantly to all users, and never challenged, ignored, or circumvented by a single user.

For any security policy to be worth the time invested in developing it, it must meet certain minimum requirements. It must be easy to create, and administrators must be able to test it thoroughly before it's cast in stone. There must be an easy way to distribute the policy to potentially tens of thousands of users, across dozens of offices, speaking many different languages.

Users must have no choice but to comply with every element of the policy, whether they like it or not. And if they don't like it, it must be explained to them the consequences of any alternatives.

Ideal Security Scenarios

- An employee attempting to send in clear mode a sensitive document that is supposed to be sent encrypted, might be halted, reminded of the specific security rule relating to sensitive documents, told why the rule is important, and informed that the document cannot be sent unencrypted. If the user agrees, then the document is automatically encrypted and sent. The policy is effective, the user is educated, and security is maintained.
- An employee attempting to open a databases file with anything other than Microsoft Access (a policy rule), when the rules state that Access is the only options available, is unable to open the database.
- An employee seeking access to specific applications after 7pm when the rules forbid any access to such applications after 5 pm, is denied access, informed why, and a record of the event is sent to security administrators.

- An employee who downloads a file from the internet and attempts to save it on a local hard drive, when the relevant security rule insists that such files be stored only on a specific server, will be unable to save the file to that drive.
- Any document containing sensitive information such as customer credit card data is automatically encrypted when an employee attempts to transfer the document to a removable disc, or send it across the internet or any non-secure channel.

While these scenarios may seem too unreasonable to realize, success in making them a reality could forever change the way users impact security.

4. THE IMPORTANCE OF BUSINESS PROCESS SECURITY

Core to the foundation of every enterprise are its business processes. Computer systems, networks, even the workforce are just contributors to the processes that create product, drive revenues, and generate profits. Networks, intranets, and computer systems simply support these processes.

The effects of attacks on networks and computer systems can always be mitigated, but attacks that compromise the availability and integrity of critical business processes can cause irreparable harm to very core of the enterprise. And the applications and information that enable these business processes are vulnerable to the very people entrusted with their safe use.

According to Forrester "businesses will focus their security efforts on trying to hold onto customers, ignoring the more potent threats waiting to pounce from inside the company itself....despite multibillion-dollar spending, firms will miss the new challenge: business-process security."

In order for security to become truly effective, it must change its focus from the outer perimeter, and instead target security at the applications and data that enable all critical business processes.

To achieve this, the enterprise must focus on the trusted user, to minimize the vulnerability created by inappropriate user behavior, and to maximize the effectiveness of security policies designed to protect business processes from dishonest, malicious, careless, or reckless users.

“There is an emerging need for auditing and security solutions that enable companies to monitor the authorized activity of their employees, contractors and business partners,” according to Gartner.

"There is a new security equation. It's not just about keeping the bad guys out; it's also about enabling the good guys to do what they are entitled to do, and only what they are entitled to do," said Saecos CEO De Leon.

5. THE IMPACT OF POLICY ON BUSINESS PROCESS

A good security policy is not difficult to create, and security professionals have a wealth of guides, templates, tools, and experience with which to create the perfect policy. The real challenge lies in making policy work, a process that must include testing, distribution, compliance monitoring, enforcement, education, and updating.

In that ideal security world, a policy designed to protect business processes should:

- Focus on how users access and use applications, information, and business processes;
- Eliminate the need to simply trust users to do the right thing;
- Automatically monitor all access and use for compliance;
- Correct inappropriate behavior as it happens, without adding to the administrative overhead or burdening security;
- Teach users why the behavior was incorrect, by explaining to them in real time the official policy for that action;
- Test and simulate any policy for effectiveness before it’s launched, to avoid confusing the user;
- Gather the necessary evidence and forensics, in case the user continuously ignores policy rules, or engages in criminal behavior;
- Automate this process to free security teams from the task of manually identifying policy breaches or inappropriate behavior, halting the action, informing the user, and correcting any harm.

Given these significant challenges it’s easy to understand why business process security is so essential to business integrity, and why the effective enforcement of policy is so difficult

6. THE X-TRA SECURE RESPONS

From its roots in the early anti virus industry, ThunderStore recognized the importance and value of linking individual behavior to the individual. The firm also recognized a major security challenge – to find a way to enforce the correct behavior on individual users and employees, in compliance with corporate policies, but to do so in a way that did not burden security administrators or users, and which didn't impact the pace and drive of the business.

Their response is called **X-Tra-Secure**, reflecting its position as a complimentary defense to existing security solutions to manage a significant threat - protecting the integrity of information, applications and business processes from careless or malicious actions by authorized users.

X-Tra-Secure solves the current disconnect between desired activities and actual behavior of "authorized users" through enforcement of agreed security rules that ensure the necessary compliance with corporate information, business and security policies.

At the core of the technology is the X-Tra-Secure Framework, which logs, monitors and analyzes the activities of "authorized users" and then enforces the desired behavior as it happens." X-Tra Secure™ enforces an organization's policies in real time, with or without notifying the user.

By using X-Tra- Secure™, companies no longer have to depend solely on the knowledge, behavior, good will and discipline of users. Instead, X-Tra-Secure™ keeps users in compliance with policy and holds them accountable.

7. THE BENEFITS OF X-TRA SECURE

- Delivers Business-Process Security by applying a policy-based management system that monitors and controls user activities and assigned privileges against corporate policies, standards and guidelines;
- Promotes policy awareness;
- Guarantees compliance;
- Encourages and enforces desired behavior;
- Eliminates dependence on user cooperation;
- Eliminates dependence on user cooperation;
- Reduces the total cost of ownership;

- Enables enterprises to deliver accountability above and beyond authorization and authentication.

8. HOW X-TRA SECURE WORKS

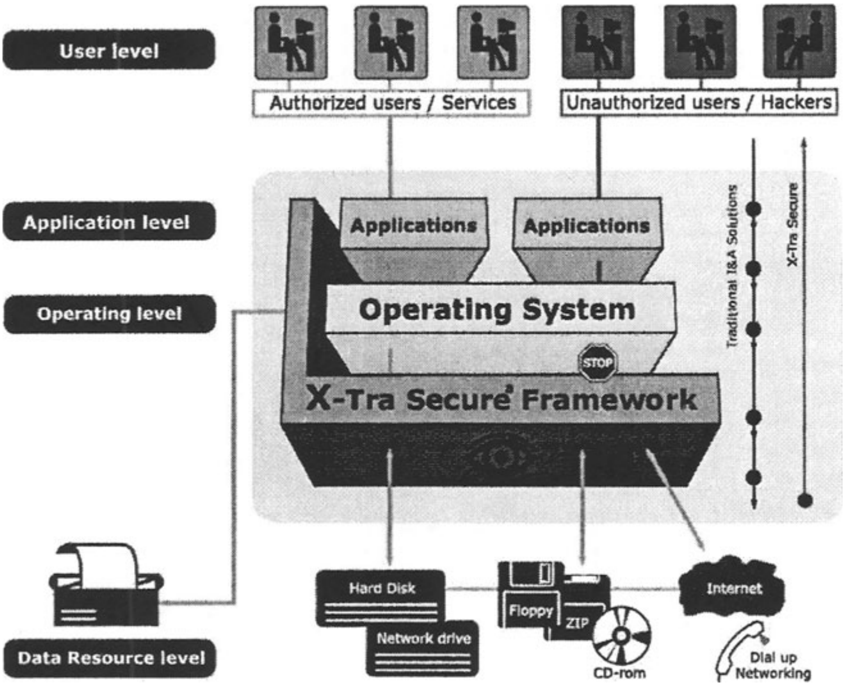
X-Tra-Secure actively monitors, logs, analyses and enforces security policy in business information systems. The **X-Tra-Secure** Framework monitors and manages how users are allowed to handle corporate information and data, by comparing user activities and assigned privileges against a set of rules that are based on corporate information and security policies.

Activities that attempt to violate these rules (such as unauthorized copying and/or printing of confidential files, or transmission of unencrypted information) are prevented. As a result, companies do not have to rely on voluntary employee compliance with information, business and security policy. **X-Tra-Secure** encourages and enforces policy compliance automatically.

9. THE X-TRA SECURE™ FRAMEWORK

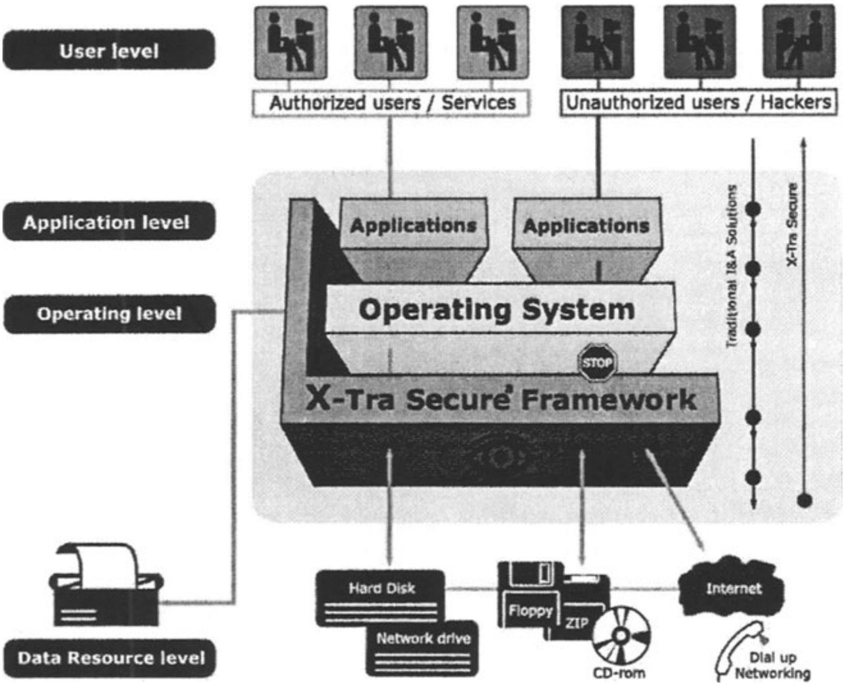
The **X-Tra Secure™** framework occupies a strategic position below the network operating system level where it is able to monitor and analyze all data before it reaches the operating system. For each operation, **X-Tra-Secure™** poses questions such as: Should this file be copied, moved, or deleted? Should the file be stored locally? Should it be opened by a particular application?

Should the contents of a Website be stored locally? If an assigned policy rule attached to a file attempts to perform a violation, **X-Tra-Secure™** will immediately intercept and stop the request, before it reaches the operating system.



X-Tra-Secure™ Technology can log, monitor, analyze and enforce predefined policy and rules with respect to any type of data or application. For example, it can identify critical words (and or semantics), sentences and strings (e.g. credit card numbers) before files are opened, saved, read, copied, deleted or sent. This capability can be coupled with X-Tra-Secure's ability to attach security rules to files. As a result, certain rules can be invoked if the file is determined to contain critical pieces of information.

This combination of existing features, combined with a suite of new tools and planned enhancements, makes X-Tra-Secure the perfect complement to existing security mechanisms, and the Number One choice for managing Business Process Security.


User level
Authorized users / Services
Unauthorized users / Hackers
Application level
Applications
Applications
Operating level
Operating System
STOP
X-Tra Secure Framework
Traditional I&A Solutions
X-Tra Secure
Hard Disk
Network drive
Floppy
ZIP
CD-rom
Internet
Dial up Networking
Data Resource level