The Toughest Problem in Information Security

Protecting corporate IT resources from Internal Threats

The Case for Intrusic's Compromise Detection System

Intrusic, Inc.
281 Winter St.
Waltham, MA 02451

www.intrusic.com

Draft Material

Introduction

The information security market has traditionally been divided into two distinct camps – technologies that are designed to “keep the bad guys out” and those products that are designed “to let the good guys in”. But what happens when the “bad guys” obtain legitimate credentials or when the “good guys” abuse their privileges by compromising the confidentiality and integrity of corporate data or violating company policy or government regulations?

Can you answer these basic questions about your IT assets?

- Does an *unauthorized* person already have *authorized* access to your network, systems, applications or data?
- Is an employee, partner, supplier or customer accessing information that they shouldn’t?
- Can you assure that you are in compliance with government regulations or internal company policies regarding confidentiality and integrity of corporate information?

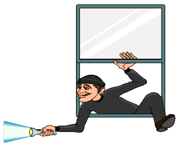
Established information security vendors have always avoided claims of protecting companies from the internal or insider security threat. And for good reason. The internal security threat is a very difficult problem to solve. Yet the financial harm from someone compromising your infrastructure, data or policies can easily dwarf the damage caused by external attacks such as viruses, worms, spyware, spam, denial of service, or amateur hackers. Today organizations need a new approach to internal IT security which enables them prevent their IT infrastructure, enterprise data, corporate policy and compliance with government regulation from being compromised.

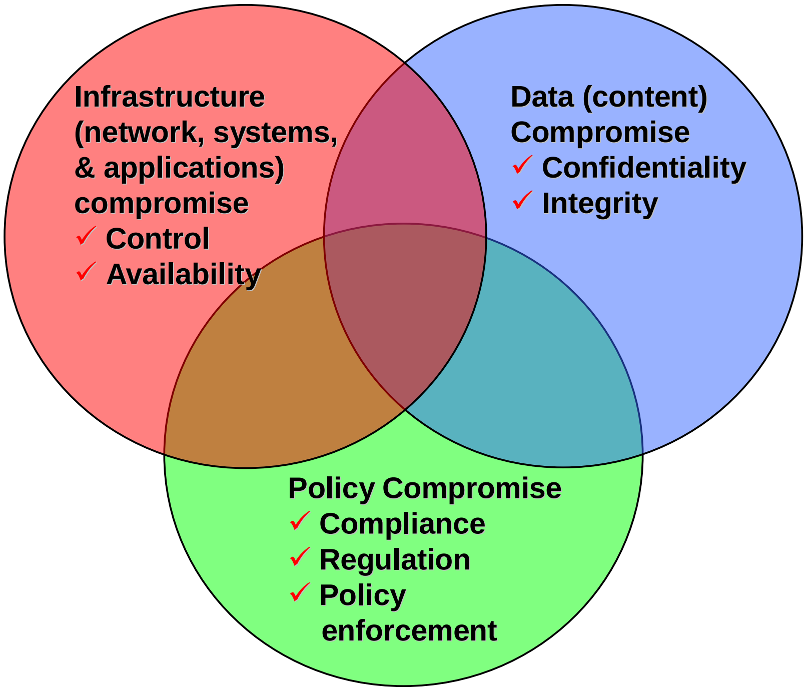
What is the Internal Security Threat?

Most of us are aware of external security threats like viruses, worms, spyware, spam and hackers which threaten the availability of corporate IT resources. Technologies like anti-virus, intrusion detection/prevention, anti-spyware, anti-spam, and firewalls have evolved to help protect organizations from these types of attacks. Yet none of these technologies can prevent someone with authorized access from gaining control of the corporate IT infrastructure or compromising the confidentiality and integrity of critical corporate data. **Not every person who has credentials is authorized and those that are authorized should not be able to do anything they want with the organization’s IT resources or data.**

Internal security threats can come from sources like:

- Sophisticated hackers who have illegitimately gained authorized access to your IT infrastructure
- Internal employees who abuse their privileges
- External employees who access the internal network remotely
- Ex-employees who still have authorized access
- Customers, partners and suppliers who have been given access to the internal network, systems and data
- Outsourced IT management



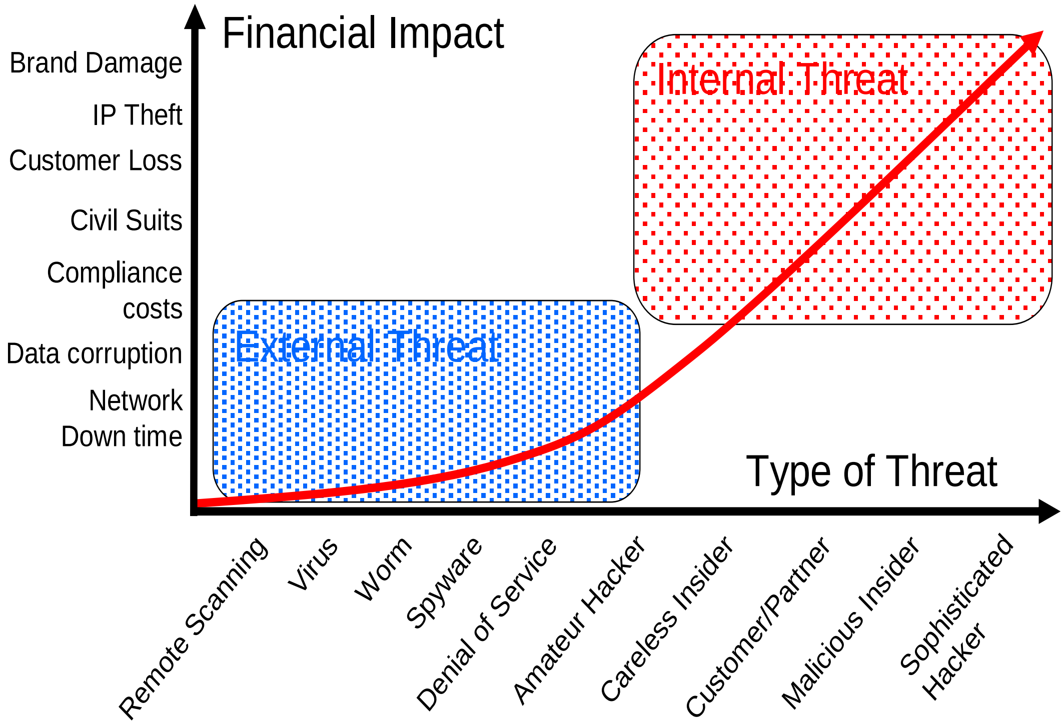


Worm or virus attacks and amateur hackers indiscriminately create havoc by bringing down networks or vandalizing Web sites. The perpetrators of these attacks are mainly after the thrill and notoriety. However, recently we have seen these random attacks give way to more sophisticated hackers who target specific organizations for monetary gains. With worms and viruses at least you knew you were under attack because the damage was immediately evident. The sophisticated hacker on the other hand uses stealth to “fly below the security radar” and evade detection. Their ability to benefit monetarily is dependent on going unnoticed. Therefore they are careful **not** to disrupt operations. To go unnoticed they need to obtain legitimate credentials which they can do in any number of ways. A sophisticated hacker may have access to your IT resources for months before they are discovered because they appear to be a legitimate user to conventional security approaches.

Employees, partners, suppliers and customers who have been granted access to your IT resources sometimes abuse their privileges.   They may inadvertently expose corporate information to compromise by transferring data to unauthorized outsiders or by exposing IT resources to unknown individuals using insecure technologies like encrypted tunnels to external sites, instant messaging, Web mail, peer-to-peer (Kazza, eDonkey, etc.) and other file transfer mechanisms. Sometimes these insiders are overtly acting in a malicious fashion for financial gain or other personal reasons. Suppliers and partners may abuse their access to snoop around the network or download proprietary information from your network to theirs.

In other situations insiders may have access to systems, applications and data that they are not supposed to have. This access may violate government mandates such as California Senate Bill 1386, HIPAA, Sarbanes-Oxly as well as critical infrastructure regulations like NERC/CIP in the energy sector or other US or foreign government privacy regulations.

Why should I Care?



Internal security threats can affect the control and availability the IT infrastructure including the internal network, host systems (desktops, notebooks & servers), applications and databases. By exerting control over system and network resources they could control key functions, bring the network down, crash key servers or disrupt critical applications. Of course someone with access to the IT infrastructure could just lay low and snoop around looking for valuable information. In this case you might never know they are there until it is too late.

Identity theft is on the rise. When confidential information such as credit card numbers, social security numbers, home addresses, drivers license numbers, and credit histories are compromised, it becomes costly to try to repair the damage not to mention the loss of customer confidence. CardSystems, Lexus/Nexis, DSW Shoe Warehouse, BJ's Wholesale, and Polo Ralph Lauren, are examples of companies that have been in the press recently because they failed to protect confidential information. The compromise can usually be traced to either an external hacker who somehow gained legitimate access or to an insider who abused his/her privileges.

Not only are there real financial losses when data is compromised, there is the negative publicity associated with internal security breaches. Few organizations have appeared above the fold in the Wall Street Journal because they were the victim of a virus, worm, spyware or spam attack. However, the companies mentioned above have all endured unwanted publicity and financial losses because they failed to protect their IT resources from the internal threat.

By the same token someone who has access to corporate information could compromise the confidentiality of that information. Proprietary information could easily be sent out of the company by email, Web mail, instant messenger, peer-to-peer, or other file transfer mechanisms. To evade notice this information could be sent over encrypted channels or simply zipped up and sent as an email attachment.

Keep in mind that someone with access to corporate data need not steal the information to cause harm. A malicious insider could compromise the integrity of that information by changing, deleting or otherwise corrupting the data. If you cannot rely on the integrity of medical records, clinical drug studies, engineering specifications, financial data, etc. then business could be severely disrupted or lives could even be put at risk.

Compromise of confidential data is not the only risk. Unauthorized individuals that gain legitimate credentials which enable them to control IT systems and applications could affect the integrity of those systems. Imagine if a terrorist gained access to the control systems of a nuclear power plant, 911 emergency systems or the hospital systems that monitor patient status.

Besides financial and public relations damage, organizations who fail to protect the confidentiality and integrity of IT resources could risk "material defects" in their compliance with government regulations. California Senate Bill 1386 mandates disclosure when confidential data has been compromised. HIPPA mandates the confidentiality of health care information and Sarbanes/Oxley legislation also requires executives to ensure the integrity of financial information. Governments outside the United States have even stricter privacy and confidentiality laws and organizations that do business in those countries are bound by those regulations.

Doesn’t My Current Security Technology Protect Me?

Most organizations have implemented security technologies designed to prevent external attacks, identify legitimate users and control what authorized users can do. Firewalls are nearly ubiquitous devices designed to separate the internal network from the Internet. Intrusion detection/prevention devices block worms and exploitation of known infrastructure vulnerabilities. Anti-virus, anti-spyware, and anti-spam block a wide menagerie of malicious software. User ID’s & passwords and two-factor authentication devices like tokens or digital certificates are used to authenticate legitimate users. Access controls in operating systems and databases restrict the type of access a user can have.

But by definition an internal threat negates all of these security functions. An internal threat appears to these technologies as an authorized user because they have legitimate credentials. Even if these credentials have been obtained by illicit means, the credentials grant them access to key resources none-the-less.

While the bulk of deployed security technology tries to “keep the bad guys out”, we routinely poke holes in these products in order to grant outsiders access to our internal IT resources. Virtual Private Network (VPN) connections enable remote employees or partners to access our networks. If someone compromises a remote VPN connection they can have the same access as someone inside our building.

Social engineering, “man-in-the-middle”, “phishing”, “key stroke logging” and “dumpster diving” are just a few examples techniques widely used by hackers to obtain legitimate credentials. Some of these exploits could be blocked by more advanced approaches such as biometric authentication. However most organizations still rely on conventional ID’s and passwords and are reluctant to incur the administrative overhead involved in more advanced forms of authentication.

Even the most advanced authentication methods cannot solve the problem of trusted users who we willingly grant credentials to. Once you are an “insider”, you become nearly invisible to perimeter-based security devices. Evidence of insider abuse may be captured in audit logs, but few organizations have the resources to review these logs and some have turned off logging because of the amount of storage they consume.

What about new Technologies like Anomaly Detection or Content Inspection Systems

Recently there are some new technologies that purport to deal with the “insider threat”.

Network anomaly detection (NAD) products look at network connections (called flows) between devices on the network. They can tell what devices connect to other devices, how long they remain connected, how much they send and how they communicate with one another. After they establish a base-line of “normal” behavior they look for significant changes or “anomalies” in that behavior which may indicate unusual or unwanted activity.

The NAD technique is useful for deciding how to partition the internal network (if two devices have no need to communicate with one another, than set the rules in the router so they can’t). NAD is also useful for detecting a worm outbreak which originates from an infected machine on the network.

However, since NAD is a technique based only on summaries of network connections and statistical profiles, it has no knowledge of when a system or application has already been compromised. In addition, NAD does not capture or analyze information on the *content* of communications between devices. Therefore it cannot detect when corporate data is being compromised. And finally, NAD has no concept of data policy or regulation so it cannot tell you if you are in compliance with government regulations or when corporate policy has been compromised.

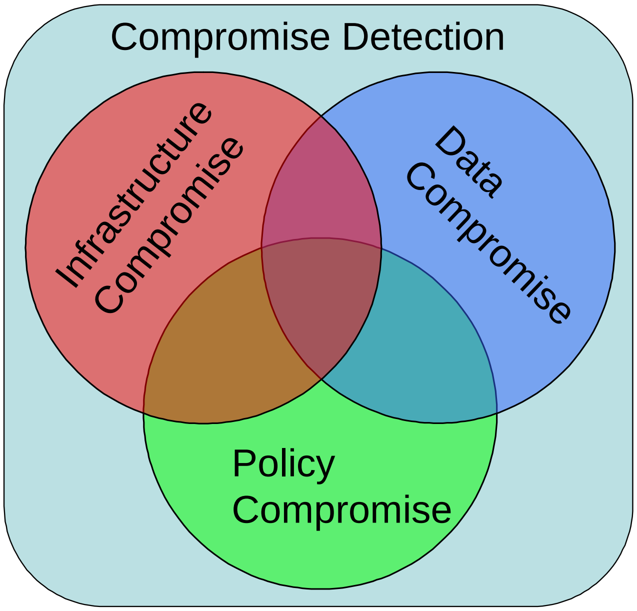
On the other hand content inspection systems (CIS) do understand the content of some network communications. They usually reside at the ingress/egress points of the organization and under certain conditions they can tell you when confidential information is transferred outside the company.

However, to detect specific information leaving the company the data must be identified somehow to the CIS device. This means the CIS database must be constantly updated to keep up with an ever changing list of confidential information. Since CIS products focus on data leaving the company, they provide no protection when information is merely accessed by an unauthorized person or downloaded within the internal network even if this is against corporate policy.

More importantly, because CIS have such a narrow purpose, they are not designed to detect when the network, systems, applications themselves have been compromised. They do not address policy and compliance. And they can be easily be circumvented by compressing (zipping), encrypting the data or sending the information through an encrypted channel (SSL tunnel for example).

A sophisticated hacker or malicious insider is unlikely to send confidential information out of the company using his/her regular email account.

OK, How Can Intrusic Protect Me from the Internal Security Threat?



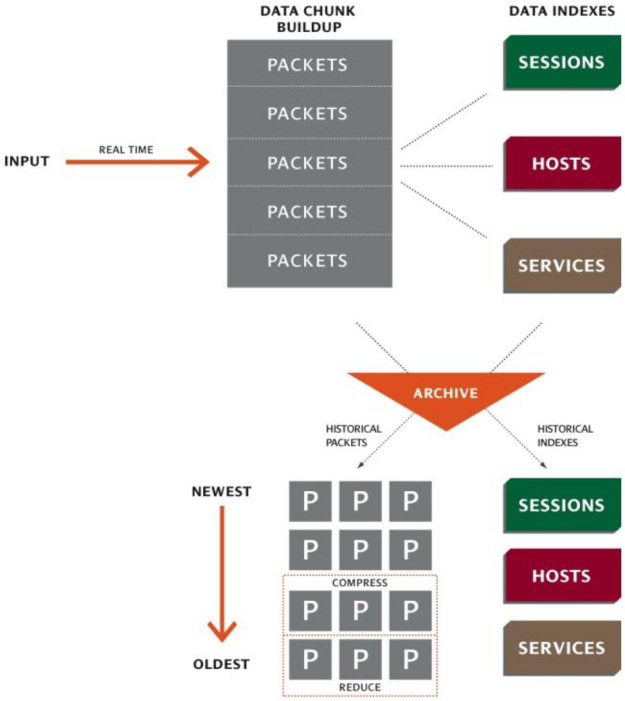
As we have seen above, some security products can detect anomalies in your infrastructure which might indicate that it is under attack, but these products have no concept of data compromise. On the other hand some technologies can detect when data is moved out of the company, but they can tell you nothing about an unauthorized person who might already own your infrastructure. And none of these technologies can provide insight into policy violations. Trying to solve the internal security problem with established security technologies is like three blind men trying to describe an elephant by touch. One feels the tail and describes a rope, another feels the leg and thinks it's a tree. Another touches the trunk and says it's a hose. What's needed is a strategy that puts it all together and enables you to see the entire picture by combining next generation anomaly detection, content inspection, and policy compliance into one solution. At Intrusic we call this "Compromise Detection".

How does it work? Intrusic's Compromise Detection System (CDS) works by capturing all communications traveling between devices on the internal network as well as communication to destinations outside the corporate network. Information on network connections (sessions) is gathered including source and destination information, communication type, duration, and connection type similar to the information gathered by NAD products. But unlike NAD, Intrusic then delves deep into the payload of the network traffic to understand the content that is being communicated as well as the transfer mechanism being used.

This information is automatically categorized and stored away for analysis and forensic purposes in a database. As the information is gathered, Intrusic uses multiple, patented analytic techniques to identify data, infrastructure, and policy compromise without any pre-configuration or "learned baseline." Instead, Intrusic's analytics look for variations from a fundamental model of how networks, systems, applications and services operate which we call the "physics of networks". A single anomaly is not usually sufficient to trigger an alert. Instead, the analytical engine looks back through the accumulated information for corroborating evidence of an actual compromise. This enables us to virtually eliminate false alarms.

Below are some examples of the infrastructure & data compromises Intrusic CDS will show you:

- Backdoors
- Trusted path exploitation
- Reverse tunnels
- Encrypted or covert control channels
- Remote exploitation & control
- Data harvesting
- Man in the middle
- Session hijacking & sniffing
- Stepping stone administration
- Clear text credentials
- Unauthorized data transfer
- Data transfer over instant messaging or Web mail
- Encrypted data transfers
- Bulk file downloads from internal servers
- Unauthorized data access



Since the content of the communications is stored away, you can drill down on any alert to see specific details about that compromise including the actual documents, PDF's, spread sheets, presentations, or confidential information such as credit card numbers, Social Security numbers, health care information, etc. Intrusic's Compromise Prevention solution even understands industry specific data such as DNA or chemical formulas. You will know the exact data that was involved in the attempted compromised.

Some of the content Intrusic CDS recognizes:

- MS offices files (Word, Excel, PowerPoint, etc.)
- Images
- Video
- PDF's
- CAD drawings
- Credit card numbers
- Social Security numbers
- DNA data
- Financial data
- Health care data
- Any customer specific data which is predefined

Because the Intrusic CDS understands the content of communications between departments and organizations, it can tell you when confidential information has been accessed, downloaded, or transmitted by an unauthorized person or in violation of established policies.

Some of the policies and regulations CDS can help enforce:

- Sarbanes/Oxley
- HIPPA
- GLBA
- NERC/CIP (energy & SCADA systems)

Give me an example of how Intrusic CDS works: A sophisticated hacker might compromise a remote users PC using a common method like "phishing"[1] or trick the user into installing a key stroke logger[2]. After he has control of this PC he can utilize the VPN connection to gain access to resources inside the corporate network. Once inside the network the sophisticated hacker can move from server to server looking for weaknesses that he can exploit. He may install a network sniffer to pull clear text credentials off the wire, install a back door, or gain administrative rights to one of the machines by exploiting a vulnerability on that device.

[1] Phishing is a method of presenting the user with a Web page or Web form which appears to be from a legitimate Web site, but is really the hacker's site. The user enters his credentials into the fake form thinking it is legitimate and the hacker now has his credentials.

[2] A key stroke logger is a program surreptitiously installed on your machine (like spyware). The program captures all the key strokes typed on the keyboard and send them to the hacker. Using this method you can capture ID's and passwords when the user logs in as well as other critical information.

STAGE 1
Entry
STAGE 2
Reconnaissance
STAGE 3
Residency
STAGE 4
Action

Once the hacker has obtained administrative rights, they can set themselves up as a legitimate user and no longer need to gain access through the remote users PC. At this point the hacker will take up residence in the network and start looking around for useful information that he can exploit. When he finds confidential data he will attempt to move the data out of the enterprise using a variety of techniques. For example he could set up an encrypted tunnel to transfer information through. Or he could simply compress the information (zip it) and send it through Web mail.

In this particular example Intrusic's CDS would detect the hacker moving from system to system inside the network. It would detect any back doors or network sniffing deployed by the hacker. It would detect the hacker snooping around for information and ultimately it would detect the attempt to access confidential information, set up encrypted channels or move information out of the organization.

How does Intrusic CDS enforce policy and ensure compliance? Intrusic CDS understands connections between devices on the network, what organizations those machines belong to and the content communicated between machines. Once you have that knowledge it become easy to enforce a corporate policy or to ensure compliance with government regulations. You can create a set of rules which reflect your information security policy or reflect government compliance and Intrusic CDS will notify you when these policies are violated.

The following are some examples policies a customer might create:

- No unauthorized file transfers to external destinations
- No encrypted file transfers to external destinations
- No access to financial data from departments outside of accounting
- No access to engineering data from non-engineering departments.
- No access to HR data outside of the HR department
- No Instant Messaging allowed
- No file transfers via Web mail
- No file transfer via instant messaging
- No peer-to-peer communications allowed
- Remote Control Channels such are only allowed from the System Administration Network
- No clear-text control channels of any kind are allowed

Does it scale? The Intrusic Compromise Prevention Solution is a distributed, scalable, and passive internal network based security system. Multiple network sensors gather, analyze and store information at line speeds. Each sensor can store Terabytes of information which translates to weeks of historical coverage for analysis. Correlation across multiple sensors is provided by a central server which maintains summary information, coordinates analysis across multiple sensors and provides for central alerting, reporting and management. This architecture enables the Intrusic solution to scale up to handle the largest corporate networks at minimal operational cost.

Summary

There is no question that the internal information security problem is the toughest issue facing IT organizations today. How do you defend the organization from itself? The conventional wisdom has been that this problem is too difficult to solve with technology. We must continue to trust our employees and partners and hope that the sophisticated hackers don't target us. Our only defense is employee education and an occasional audit.

A few years ago this might have been true. But new technology like Intrusic's CDS is beginning to change conventional wisdom. Many organizations are discovering that there is technology that can tell them when their network has been compromised by an outsider. This technology can tell them when the confidentiality and integrity of critical information is at risk from trusted employees or partners. Intrusic customers are also discovering that this new technology can give them visibility into policy violations and regulatory compliance that they can't get by any other means. By combining a deep understanding of how networks, systems, and applications behave with the ability to understand the content of network communications, Intrusic is leading the way to solving the toughest problem in IT security, the internal security problem.