Government Services at Risk – The Fundamental Flaw in IT Security

Recent exploits of a flaw in the global mindset of IT has lead to a dire situation that threatens the services we rely on, the privacy we demand and the systems that we use. It is not a pleasant thought, but we are now beginning to embrace that fact that our security strategy has a gaping hole in its design.

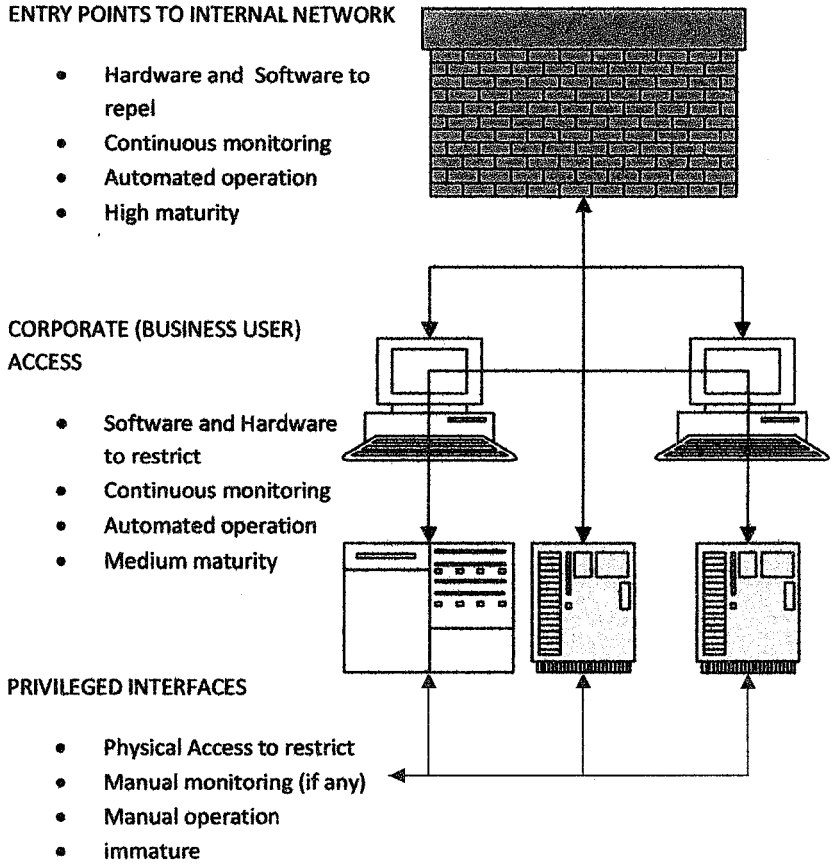
The flaw stems from approaching this challenge in a limited perspective. We think about defending ourselves from intrusion – from malicious hackers who attempt to break-in to organizational systems – much like the moat in the feudal defense strategy of castles. We have become very good at this kind of defense, but we are still vulnerable. In fact, attacks that "break-through" at least some of our defenses are a common news item. A Google news search yielded 3,928 hacking-related news stories.

Once a person is inside the story is much different. While we do limit access by business users to content and applications, we do not limit what IT specialists can do at the foundation of our IT infrastructure – what I term privileged interfaces.

Privileged interfaces are what IT specialists use to setup, configure and maintain IT hardware. By design, there are no restrictions on these interfaces. They are a master interface having complete control over each of those hardware devices we have in our IT systems (servers, databases, routers, switches, etc.).

From the graphic here, the flaw in our approach becomes clear. While we use automated and programmatic means to repel outsiders and restrict general business users, we use none of these proven techniques to people who have – or get – access to – privileged interfaces.

Because privileged interfaces are master interfaces, access here enables a person to do whatever the device can do. There are no limitations.



Who are these People?

There are two groups of people we must concern ourselves about, those who are supposed to have this access and those who penetrate our outward-facing defenses and attack us from the inside.

The people who are supposed to be there include IT staff, contractors, service technicians, and contract service provider companies. But do you know who these people really are? Does anyone in your organization know who they all are, when they were here, what they did, and why they did it? If they say that they do, then we ask: do they have systems-managed records to prove that? If we don't have system-managed record then we have no way to really know. In most cases we simply trust that these insiders will not, intentionally or unintentionally, do the wrong thing.

A New Security Breach

In addition to insiders that are supposed to be there, outsiders that break through our defenses become insiders. Our conventional wisdom fails us once again because they do not always try to enter through our firewall. They may come through the firewall (some do make it) or they may piggyback in on people that are supposed to be there.

For example, we are seeing a number of successful breaches by hackers riding people through our defenses with malware hidden on notebooks, diagnostic equipment and storage devices (like usb sticks). In this case, you don't have to take the organization's security team on; the outsider only has to compromise one person.

Potential Impacts

The impact of the lack of security on privileged interfaces ranges from inconvenience and unnecessary cost - to disaster. Services can suddenly drop out because a device is miss-configured, reprogrammed or damaged. This includes internal and external services such as those offered online.

Services can suddenly behave improperly, appearing as if they are performing as expected but incorrectly recording data or triggering operations (your driver's license records are swapped with someone else, electronic payments are rerouted to the wrong party). Sensitive data can be easily stolen, tucked away in a usb stick, a camera memory card or cell phone. Technically proficient people with access can trigger system-wide havoc, like the disgruntled worker in San Francisco that locked everyone else out of the new system. Database records – the very data that drives our society - can be copied, erased and altered. If the device can do something, then insiders can make it do that.

Privileged Interfaces must be System-Managed

It has become clear that privileged interfaces must be brought under systems-managed control. The vulnerability cannot be mitigated 100% because of the master control status of privileged interfaces. However, we can do several important things that go a long way in protecting the organization from the insider threat. We can systems-manage privileged interfaces (commonly called baseboard management controllers and specialized serial ports) with a live connection that tells us who is connected, what they are doing, what they have done and if the system is ever disconnected. We can also implement systems-managed role-based security for access, a practice in ubiquitous use in all of our other security practices.

Finally, we can record and monitor – in real time (that means sub-second) - everything that happens (down to the keystroke) through those privileged interfaces: who, what, when, where, why. We can detect many – perhaps most – errant behaviors before they can complete or their results can manifest themselves. We can review actions taken and refine our control strategy. We can even respond far faster to problems that do slip through, often before they can be completed.

In effect, we understand now that we must extend the proven practices we use in the rest of our security strategy to this foundational level of IT infrastructure. It is not our knowledge or approach to security that is our challenge; it is our limited perspective that has left this critical part of the technology each of us relies on in our daily lives out of our global security view.

Terry Schurter

[redacted]

[redacted]