Information Assurance vs. Cyber Security vs. Information Security: Clarifying the Differences

Ray Klump, Lewis University, 2018

Seemingly every week brings another high-profile threat to our online lives. This week, [Spectre and Meltdown](https://meltdownattack.com/) captured all the attention, and for good reason. Unlike most of the problems we’ve heard about over the years, these vulnerabilities relate to the hardware – the physical electronics that make up the computer or phone or tablet – not the software. Hardware problems are generally harder to fix than software ones because they relate to the way the devices were actually wired at the factory. And these vulnerabilities affect *a lot* of devices, potentially [more than three billion](https://www.technologyreview.com/s/609891/at-least-3-billion-computer-chips-have-the-spectre-security-hole/). Hardware manufacturers are working with operating systems vendors to issue patches to protect users from Spectre and Meltdown, but these patches [may slow our systems down](https://www.pcworld.com/article/3245606/security/intel-x86-cpu-kernel-bug-faq-how-it-affects-pc-mac.html), particularly when it comes to reading data from your hard drive.

Interestingly, though, no one knows if a hacker has ever actually exploited Spectre or Meltdown. In other words, in theory, these vulnerabilities are very serious, because they provide an avenue for doing really damage. But, as far as we know, no one has actually taken advantage of these problems to do harm yet. So, how were these problems found, and who found them? And what kinds of knowledge and training do the researchers who discovered Spectre and Meltdown and are now trying to mitigate them have to possess?

These questions got me thinking about the variety of confusing terms we use every day to describe the effort to keep data and systems safe. Indeed, the plethora of similar sounding terms such as “information assurance”, “cyber security”, and “information security” has even caused confusion regarding academic programs and their learning outcomes. (There’s even confusion about whether “cyber security” should have a space in the middle!) And this confusion over academic programs and their outcomes has sometimes made it more difficult for companies to hire the right talent for the job.

So, let me try to draw the boundaries, however imperfectly.

*Information Assurance* is an activity organizations conduct to ensure that their systems protect private, sensitive information. Information Assurance is closely linked with *risk management*. An organization, such as a business, identifies its information assets and the systems and applications that store, process, and communicate them. It estimates the susceptibility of those information assets to attack, whether by disclosure (a loss of *confidentiality*), modification (a loss of *integrity*), or disruption (a loss of *accessibility*), and it quantifies the effect – usually in dollars – of those unwanted occurrences. From this, a risk assessment can guide an organization on how to devote personnel and capital resources optimally to protect its information. Once these protections are put in place, the practice of Information Assurance then calls for using various assessment and auditing frameworks to help an organization understand how well the controls it has deployed actually mitigate the risk.

Information Assurance specialists focus on the big business picture. They don’t concern themselves with operating systems kernels and the pitfalls of speculative instruction execution – the attack vector exploited by Meltdown, for example. Instead, Information Assurance experts seek to know how a company uses information, how valuable that information is to the company, and how exposed that information happens to be so that they can guide the organization on how to prioritize tasks to protect it. Once those protections are deployed by others, Information Assurance professionals help measure whether those protections are working.

Generally, Information Assurance professionals don’t focus as much in the actual design and deployment of those protections; they help decide what to protect and whether the protections are effective. They focus very much *on the business*. Indeed, an Information Assurance specialist could conduct all their work without ever having to bother about the esoteric details of bytes, protocols, and instruction registers. It’s all about information assets, valuations, optimization, strategy, and continuous assessment. It’s all about management, planning, auditing, and governance.

So, if Information Assurance specialists focus on these critical organizational management areas, who actually develops and deploys the plans that keep data private, sound, and accessible? That’s where Information Security and Cyber Security specialists do their work. We tend to use Information Security and Cyber Security interchangeably, but I will risk complicating things slightly by distinguishing between them. Let’s talk about Information Security first.

Take Information Security at face value: it concerns the security of information. Information is data that has meaning. From that meaning, information derives its value, the value Information Assurance professionals seek to quantify and protect. Information may be at rest, it might be in transit between two different systems, or it might be in the process of being analyzed, visualized or transformed. Regardless of its state, it must remain secure. Securing information throughout its life requires architecting and implementing operating systems, applications, file systems, and the hardware that runs them carefully and thoughtfully. Usually, Information Security professionals use existing operating systems, applications, file systems, and hardware platforms to house and secure information at rest and in transit, but sometimes they have to create new systems, or at least new ways of combining existing ones. Whether deploying existing technologies or innovating new ones, the Information Security specialist carries out the priorities the Information Assurance professional crafted and budgeted to protect the organization’s information assets. They also help the Information Assurance specialist carry out the latter part of their job – auditing and assessing and ensuring compliance with the strategy. To do this, they’ll again use existing tools, or, sometimes, they’ll create new ones, for example, to examine how an information system is being used or, in the case of a digital forensics examination, how an information system might have been breached.

So, an Information Security professional engineers the systems that address the risks identified by the Information Assurance specialist, as well as the systems that help the Information Assurance professional determine whether those risks are being mitigated effectively and continually. Information Security professionals must know their stuff when it comes to how computers represent, process, communicate, and store data and instructions. They need to possess deep technical knowledge of binary representation, computer organization, file structures, instruction processing, communications protocols. The deeper their knowledge, the better the Information Security professional will be at protecting information, whether that calls for choosing and deploying combinations of existing technologies or helping craft new ones.

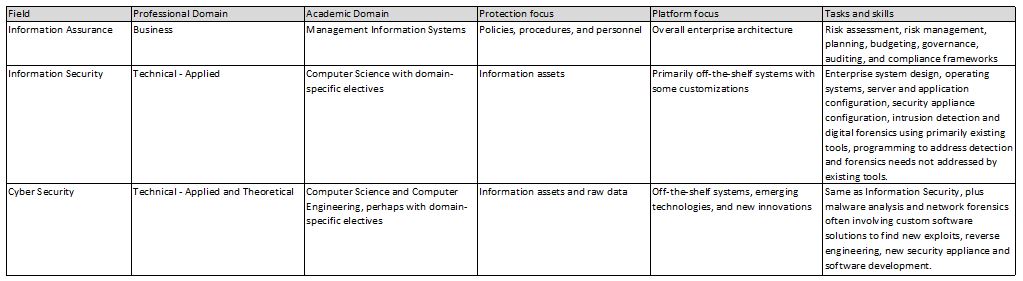
Some argue that deep technical knowledge of how computers perform their tasks isn’t required for the majority of Information Security specialists, as they spend most of their time choosing and using existing hardware and software tools. They say that, just like a driver of a car doesn’t need to know how the engine actually works or how to fix it in order to drive it, an Information Security professional doesn’t need to know how the hardware and software work in order to protect it. However, the information security challenge isn’t like driving a car. The roads don’t change all of a sudden when you’re driving, but hackers are like roadside gremlins creating new potholes, lane closures, and other pitfalls everywhere all of the time. The extreme unpredictability of the cyber landscape demands of information security specialists a commensurate technical sophistication and mastery. Qualified Information Security specialists have impressive technical chops.

Where does Cyber Security fit, then? To answer this, consider again that Meltdown and Spectre are real vulnerabilities that researchers found even though, as far as we know now, no information assets have actually been compromised through them. This, then, brings us to the difference between data and information. *Data* is raw facts and figures, independent of their meaning. *Information* comes about when we interpret and combine data to interpret meaning. We can talk about protecting data – raw facts and figures independent of and abstracted from meaning and application – just as surely as we can talk about protecting it once meaning and application have been associated with it. Regardless of purpose, origin, and destination, how might the bytes that make up data be compromised as they are collected, stored, communicated, and processed into information? This is what a Cyber Security specialist focuses on.

By asking these kinds of broader, more theoretical questions, Cyber Security professionals are able to make the kinds of findings the researchers who discovered Meltdown and Spectre discovered. Their deep understanding of how computers do what they do enables them to identify vulnerabilities even before they’re exploited. Even though they can and certainly often do work to design, deploy, and troubleshoot security systems for an organization alongside Information Security specialists, they also focus on the what-if’s, which enable them to create solutions to problems before they cause harm. They also can create the off-the-shelf solutions Information Security professionals spend the majority of their time selecting, deploying, and maintaining. And, because they deal with data in all its forms, Cyber Security specialists are usually better qualified to address vulnerabilities associated with non-traditional computing devices, such as the increasingly numerous Internet of Things (IoT) devices like sensors and cameras and voice-activated assistants that help automate modern life. As the geek’s geek, a Cyber Security specialist can do the work of an Information Security specialist, but they can also make that work easier and more effective by creating new tools and techniques.

Universities must prepare students for careers in these three areas, so it is important to identify the kinds of programs that will serve each category of student well. As Information Assurance is primarily a corporate responsibility, a college of Business is best suited to prepare the future Information Assurance professional, perhaps through its Management Information Systems program. As Information Security and Cyber Security are primarily technical pursuits, with one focusing on technical means for protecting information and the other considering how to protect even the data that underlie information, the programs that prepare future Information Security and Cyber Security professionals are typically offered by Computer Science departments. Since information, by definition, has a context that gives it its application and meaning, the future Information Security professional would do well to take application-specific coursework, perhaps even minoring in areas such as in Business, Healthcare, Urban Planning, or Public Affairs, for example. But, because of the fields’ innate technical focus, the bulk of their coursework should be taught through Computer Science.

That’s a lot of words. Let’s summarize the differences between Information Assurance, Information Security, and Cyber Security:

[](http://www.lewisu.edu/experts/wordpress/wp-content/uploads/2018/01/security-2.jpg)

No attempt at clarifying confusing terminology is perfect; otherwise, the terminology wouldn’t be confusing in the first place. But it is important, at least, to attempt to distinguish among conflicting and often mistakenly interchangeable terms so that we can prepare and hire the best people for the job. The task of protecting our online lives is an immense one with lots of opportunities that require a huge variety of skills. The fields of Information Assurance, Information Security, and Cyber Security each play invaluable roles in keeping us safe.