



The following questions were posed to the panel members prior to the SEMI Software Symposium. The In-Depth Security team reviewed the questions and answered them in preparation for the panel discussion. Not all of the questions were asked at the symposium, but all are important!

1. What is the most pressing security risk facing the semiconductor manufacturers? Suppliers? What can be done to solve it?

A: Semiconductor manufacturing trends today are; increased outsourcing, increased partnering, new business models, increased complexity and innovation, higher overall costs, more regulatory requirements and a disturbing increase in the volume of security incidents.

The most pressing risk facing semiconductor manufacturers is an interruption of operations. Computer induced interruptions directly lead to lower yields and productivity. A close second is Intellectual Property theft in the form of socially engineered attacks. And, most socially engineered attacks are accidental!

For suppliers, the ability to service the client is the most pressing security risk. If a supplier cannot deliver on the service levels promised, the client's reputation is severely tarnished. IP theft is an issue with suppliers as well.

The solution is to budget for security from the start. Design security into the business models, the design of the products, and ultimately into the products and services being delivered. And remember that security is a service – not a product or process. Security is an ongoing commitment to specific goals.

2. What level of security is required and/or recommended for hardware devices connected to the network? What level of encryption is required?

A: The level of security depends on the importance of the information that can be gleaned from that device (data classification), or the importance that the device itself remains functional. Security and availability are always in tension.

Never encrypt with keys less than 128-bit in length if you don't want it to be cracked relatively easily. Also, don't use "proprietary" encryption schemes – they don't have the peer review required to prove their muster.

3. Should desktop applications and/or web applications that have been written to access security enabled hardware on the network also have security? If so, why?

A: Absolutely. When we design process equipment, safety interlocks are implemented such that hardware interlocks and software interlocks function independently. That is, either one being "tripped" will cause the device in question to stop functioning. The reasoning here is that if one depends on the other - **IF EITHER FAILS, THEY BOTH FAIL**. The same can be said of security devices. It won't matter how secure the hardware is if the software designed to interface with the hardware is not secure (this is especially true for operating systems). **IF ONE IS NOT SECURE, BOTH ARE NOT SECURE**.

Security should be considered through all aspects of the computing infrastructure. Even if a web server and client browser are completely hardened - if physical controls are lacking, an intruder could plug-in and perform an attack very easily (for example, a "man-in-the-middle" attack).

4. Is there any risk for virus or Trojan infection to network devices that only implement read-only memory or shares?

A: Anything that uses truly read-only memory should not be susceptible to acquiring a virus, but when does anything use truly read only memory anymore? It seems that everything is EEPROM, flash, etc. and never a true ROM.



Some FlashROM's are susceptible to viruses. One example is the Intel Endeavour motherboard. This motherboard does not handle ROM update failures well and can be updated by malicious malware downloaded via the web or circulated by other means.

5. Is it possible to share detailed equipment data with my customer without exposing or enabling reverse engineering of my own proprietary algorithms?

A: Assume that NOTHING is impossible to reverse engineer, given enough motivation, time, and financial resources; the only question is what constitutes "enough".

6. It seems that much of the security protection emphasis from Microsoft and other major media players is for protection of intellectual property owned by the media (i.e. music and video). What work is being done to protect the user's proprietary and/or own personal data from being used by the end-user/consumer?

A: Sarbanes-Oxley (SOX) places the burden on corporate leaders to perform due diligence in keeping personal data secure, but the rules are not black/white – yet. Proprietary solutions (like Infracore/InTether and Sealed Media) can secure documents via encryption/wrapping and have added functionality (for example, privilege revocation AFTER "objects" have been distributed).

Finally, the RIAA has resorted to legal challenges in lieu of an effective digital/technical solution.

7. Are there any architectural changes (i.e. charge per email, or digital certificates) in the works by Microsoft or others to deal with the huge problem of SPAM? What about changes being looked at by the government?

A: Microsoft as introduced "Caller ID for Email" and their own Coordinated Spam Reduction Initiative (CSRI). Both of these initiatives are directly target at reducing SPAM.

Google's Gmail (free email service) just implemented Yahoo's (ouch!) authentication mechanism for insuring the integrity of the sender. Google did this even before Yahoo. Spam exists, first, because it works. Second, because of the anonymity of the senders. And third, because SPAM is low cost relative to print or telemarketing.

The US Government's Operation Web Snare targets spammers. Early results show a 10% reduction is attributable to this effort. Of course, some believe that the reductions are attributable to the hurricanes in Florida keeping spammers offline.

The government enacted the CAN-SPAM Act, but the net effect of the bill was nil. 60% of the internet's traffic is SPAM and 43% of that originates in the US. We are the problem.

8. It seems our (semiconductor) industry has placed a much larger emphasis on protecting against outside threats in regards to protection of intellectual property, as compared to the insider threat. How significant is the insider threat risk?

A: The Computer Security Institute's 1998 Computer Crime Survey (conducted jointly with the FBI) reported the average incurred cost of an outsider (hacker) penetration at \$56,000, while the average insider attack cost a company \$2.7 million.

Recent presentations by an FBI Cybercrime Special Agent quoted the reported numbers today are about 53% internal attacks and 47% external. The internal threat percentage is falling potentially due to 2 things – internal control personnel are becoming more aware of security issues AND the volume of external threats has risen significantly.

With risk in the areas of lost productivity, lost revenues and bad PR, the insider threat can be most effectively mitigated by 1) performing background checks, including criminal background, 2) implementing better management practices for at-risk roles and 3) create awareness of the policies and consequences for misbehavior. Understanding the personalities drawn to IT and specifically the roles that possess the tools/skills/motivation to do bad things is critical.



The semiconductor industry as a whole is behind in their approach to security. Borders are heavily fortified via larger portions of the IT security budget while the internal threats are often overlooked.

What to do? Separate your IT Security group from your IT group and join it with the physical security team. Quit searching briefcases for cameras and tape recorders and secure your infrastructure from iPods and USBdrives and file sharing.

With the typical turnover rate at most factories, and general lack of user-level controls on factory PCs, insider threats are very real!

9. Keeping up with all of the details of the latest security risks and responsibilities is difficult for small companies. Is security something that can be realistically outsourced? What are the pros and cons of outsourcing your security?

A: Yes, in fact, security SHOULD be outsourced! It's a service not unlike an insurance policy or maintenance contract. Internal IT departments are trained to keep infrastructure tuned and functional. They are not typically trained to be infrastructure security experts. Also, internal IT departments cannot provide the unbiased and broad approach that outsourced security firms can because they are being asked to examine their own work.

However, when outsourcing anything, you must insure that the provider has advantages over an internal approach. Things to look for include trust, integrity, domain expertise and flexibility of the provider. Transaction costs in terms of legal matters (copyrights, ownership) may have an impact.

Finally, A company may have trade secrets or vital customer information that not everyone within the company has access. However, the outsourcing provider will have access to the information. The security of the company's information is dependent on the security that the vendor provides at their data center. Look for a good track record by the supplier in providing these services. Review the processes of the provider with an eye on security specifically.

10. In the design of new products, is security something that should be considered from the beginning? To guard against insider threats, should security design information, be compartmentalized within the company?

A: Security should definitely be considered from the beginning – it's much more expensive to add it after an incident. (Security is like the quality movement of the early 90's)

Compartmentalized security is a good idea, provided that the "free flow of ideas" that "innovation" companies seem to need/value is not inhibited. The question should be, "HOW CAN WE PROTECT DATA INSIDE THE COMPANY, WITHOUT CUTTING OFF ONE DIVISION FROM ANOTHER; HOW DO WE KEEP DIVISIONS FROM RE-INVENTING THE WHEEL WHEN DATA IS COMPARTMENTALIZED?"

11. What are the security pros and cons to using open-source solutions?

A: Con: everybody sees the code, so they can more easily figure out how to exploit holes in it. And, people will share the holes they find.

Pro: everybody sees the code, so they can more easily figure out how to plug holes in it. And, people will share the plugs they find.

12. Pure binary data is difficult to protect – it is easy to slip in other data instead of or along with the packet of data. XML helps prevent this as the data is easily readable; however we then suffer from bloated messages. Is there some combination that provides good features of both types of data formatting?

A: It's all data. To securely transmit or store data, security must exist at all the levels (business, application, and network) to effectively provide security. As processor speeds increase, the ability to encrypt/decrypt at acceptable rates increases. Add hardware cryptographic devices to the mainstream distribution of systems and the problem is partially mitigated.



XML adds metadata and as such, will require additional effort on the part of the processors involved in its creation and movement.

13. Are the needs of the semiconductor industry really unique as compared to other industries?

A: The security needs of the semiconductor industry are fairly non-unique – most industries want to protect their data from the wily hacker and/or internal threat but the TIMING in semiconductor is somewhat unique.

For example, when a factory is up/running, the security shields are up. However, when a problem occurs that impedes the production floor, shields go down!?

Similar industries include pharmaceuticals and chemical processing – both have high levels of intellectual property and market timing issues.

14. In what ways can use of the security features of .NET save me time and money? What are the system requirements?

A: .NET mitigates “buffer overflows” by removing the vulnerabilities introduced in C and C++ languages. Programmers have variable input strings checked by the development environment itself and spend little time working the security issues manually.

Visual Studio.NET development system requirements are:

450-megahertz (MHz) Pentium II-class processor,
600-MHz Pentium III-class processor recommended

Windows Server 2003
Windows XP Pro, Tablet
Windows 2000 Pro, Server

At least 160MB of RAM

2GB of Hard disk space
CD-ROM or DVD-ROM
SVGA (1024x768) or higher monitor/adaptor resolution
Microsoft mouse or equivalent

(per Microsoft web site)