The Internet Security Alliance

Securing the Supply Chain for Electronic Equipment: A Strategy and Framework

by Scott Borg

Background on This Project

This short paper is based on sixteen months of meetings, papers, and discussions organized by the Internet Security Alliance in collaboration with Carnegie Mellon University. Two major conferences were involved, and over a hundred experts from industry, government, and academia contributed. Drawing on this material, Scott Borg devised the strategy and framework presented here. This strategy and framework have been endorsed by the board and member companies of the Internet Security Alliance, who are currently helping to develop this work further.

The Danger of Malicious Firmware

There is a serious danger that the supply chain for electronic components, including microchips, could be infiltrated at some stage by hostile agents. These hostile agents could alter the circuitry of the electronic components or substitute counterfeit components with altered circuitry. The altered circuitry could contain "malicious firmware" that would function in much the same way as malicious software. If the electronic components were connected to any network that enemy attackers could access, the malicious firmware could give them control of the information systems. Even if the malicious firmware was not connected to any network accessible to the attackers, it could still contain logic bombs that could cause terrible harm. A logic bomb in a weapons system, for example, could lie dormant until the system engaged in certain activities indicating a high degree of mobilization. These symptoms of mobilization could then trigger the logic bomb. The logic bomb could shut down the larger information system or, worse, turn the equipment controlled by the information system against those operating it.

Once malicious firmware has been inserted into electronic components, it can be almost impossible to detect. Because it is in the hardware, the malware will remain in place even when all the software has been upgraded or replaced. The circuits in which the malware would be hidden are microscopically small and enormously complex. What's more, like malicious software, it is possible to look directly at malicious firmware and not see anything wrong with it. Cleverly written malware will perform the kinds of operations that the system is routinely supposed to perform. It will just perform those operations at exactly the wrong time.

To prevent malicious firmware getting into government, military, and critical infrastructure systems, a number of government officials have proposed severe counter-measures. These counter-measures would require the design, fabrication, assembly, and distribution of the electronic components destined for government systems to be carried out domestically, in strictly controlled facilities, under constant and close supervision, by carefully vetted personnel, and with numerous verification procedures. The idea would be to institute these counter-measures by government mandates and as provisions in government contracts.

The Economic Obstacles

The problem is that this sort of security program would not be economically viable. The costs of supplying electronic components in this way would be much greater than the government would be willing or able to pay. If the government suddenly demanded stringent supply chain security of this kind, the companies involved would simply stop supplying the government. The electronic manufacturers that also supply broad, non-government markets could walk away from the government business quite easily. The few specialty manufacturers that only supply the government would be put in an impossible economic situation and would simply go out of business.

There are no regulatory policies that could easily change the response of the electronics industry to government demands for strict supply chain security. The high costs of imposing such security are partly due to the multi-national nature of electronics production. This multi-national production is competitively necessary. Imposing costly requirements on American companies would limit their ability to compete internationally. Protecting less competitive operations by public subsidies is not a sustainable national policy. Any subsidies, whether they take the form of tariffs or price supports, tend to make the subsidized industries less and less competitive over time. In the electronics industry where international competition drives rapidly falling costs, this would be especially true.

Where electronic components are concerned, the conflict between economic requirements and security requirements seems insurmountable.

Being Realistic about the Adversaries

Despite the seriousness of this problem, it's important to keep it in perspective. There are actually limited motives and limited targets for malicious firmware. It is very expensive and very time-consuming to infiltrate a supply chain deeply enough to insert malicious firmware. Once the firmware was employed in a cyber attack, it would be difficult to employ it again. Anyone profiting from a supply chain would be reluctant to insert firmware that would discredit that supply chain. The losses would simply be too great. While many attackers could achieve their ends by means of malicious firmware, nearly all of them could achieve the same ends cheaper and faster by employing malicious software.

The one group of attackers who would be seriously interested in malicious firmware would be nation states. Nation states would be interested in installing sleeper, one-use attack tools, because part of their job is to prepare defensive tools that would only be used in an extreme circumstance. They are willing to put up with very long preparation times if they can obtain capabilities that are long lasting. They are very interested in targeting hard-to access systems, such as highly protected military, intelligence, and infrastructure facilities. They are happy to invest in dormant capabilities that would go for long periods without any interaction or operation. Finally, when larger security issues were at stake, nation states would be willing to sacrifice the profits they would otherwise be making from their part of the global supply chains.

There are also certain circumstances in which large criminal conspiracies would be interested in utilizing malicious firmware. These are cases where the criminals could obtain large profits by corrupting electronic equipment where there was no software to corrupt. One example would be credit card readers, which were recently corrupted in the supply chain, allowing thieves to steal tens of millions by hijacking information from European retail transactions. Another example would be automated security systems, where criminals that can tamper with the supply chains can get themselves physical access to otherwise secure facilities.

Apart from nation states and very specialized criminal conspiracies, however, there are hardly any attackers who would be interested in employing malicious firmware. This means that, although malicious firmware is a very severe and important problem, it is nonetheless a very limited problem.

The Strategy

What, then, is to be done about this? The answer is to solve the problem of malicious firmware in a way that produces other security benefits at the same time. That way, these other benefits can justify the necessary security expenditures.

While businesses are not currently suffering significant losses from malicious firmware, they are constantly suffering *other* losses from security problems in their global supply chains. Many of these other losses are already large and threaten to become much larger. Businesses are regularly threatened with interruptions in their own supply chains that cause production delays and greatly increase their costs. Businesses are threatened with quality control problems among their suppliers that can greatly damage their brands. Businesses face problems with counterfeit products that cause them to lose sales and to suffer further damage to their brand when these products prove defective. Perhaps, most important, businesses are threatened with losses of intellectual properties that could undermine their future ability to compete.

The key to solving the problem of malicious firmware is to make the entire global supply chain more secure, so that it can cope with these other threats as well. This means that any measures to protect against malicious firmware must be part of a more comprehensive security program. This emphasis on a more comprehensive approach also makes sense in more basic ways: security measures are by nature complementary and need to be applied together to be effective.

The Framework

From a business standpoint, there are four kinds of cyber attacks that are possible at each stage of the supply chain:

1) Cyber attackers could interrupt the operation.
2) Cyber attackers could corrupt the operation (including inserting malware).
3) Cyber attackers could discredit the operation (undermining trust, damaging brand value).
4) Cyber attackers could undermine the basis for the operation (loss of control, loss of competitively important information).

For each of these different kinds of cyber attacks, there are different remedies, some of which can be identified by brief bullet points.

1) Protection against interruption:
    - Continual, mandatory sharing of production across supply chain.
    - Maintaining alternative sources.
2) Protection against insertion of malware:
    - Strict control of environments where key intellectual property is being applied.
    - Logical tamper-proof seals.
    - Physical tamper-proof seals.
    - Effective sealing and tracking of containers.

3) Protection against undermining trust:
    - Logging of every operation and who is responsible.
4) Protection against loss of control of information:
    - Versioning as a tool for protecting intellectual properties.

There are five different supply chain stages to which the remedies need to be applied:

I. The Design Phase.
II. The Fabrication Phase.
III. The Assembly Phase.
IV. The Distribution Phase.
V. The Maintenance Phase.

Each of these phases can be further divided into the basic sequences of operations that need to be carried out during that phase. The Design Phase, for example, can be divided into the overall product design (which divides further into the specification of electronic inputs and out puts and the specification of overall physical design features), the detailed product design (which divides into the schematic diagrams created using circuit design software, the physical circuit layouts created using circuit layout software, and the physical assembly engineering and design), and the creation of production masters (which divide into wafer mask production and the creation of prototypes, templates, and molds). These generic divisions are remarkably uniform for different electronic components.

If we combine the list of remedies with the stages of the supply chain to which they need to be applied, we get a "Remedies for Stages Grid."

	REMEDIES			
STAGES				

This framework should provide a systematic way of identifying and applying the relevant security measures to the electronics supply chain. It should also be helpful in identifying the areas where new security techniques need to be developed.

The Legal Support

In order for this security framework to be instituted effectively, certain legal relationships are necessary between the global component suppliers, the assemblers, and the overseeing company.

1) There need to be rigorous, unambiguous contracts, delineating the security measures.
2) There need to be locally responsible corporations with a long term interest in complying.
3) There need to be local ways of overcoming agency problems, motivating executives and workers.
4) There needs to be adequate provision for verifying that security measures are being properly implemented.
5) There needs to be local enforcement of agreements at all levels.

The legal incentives created by these measures do not need to be strong enough to deter the infiltration of the supply chain by potential attackers. They just need to be strong enough to motivate widespread compliance with the relevant monitoring procedures. If these are well designed, they will normally provide adequate warning of breakdowns in the security procedures.

Meeting the Government's Needs

After the framework for securing the electronics supply chain has been established, the specific techniques have been developed, and the legal support in place, it may still be necessary for the government to pay a premium for the high degree of security it needs for critical systems. But, by this point, the premium needed should be a relatively modest one. The measures necessary for reducing the risk from malicious firmware will be part of a broader program that is being widely applied to secure all the key aspects of the electronic supply chain.