Introduction

The capillary diffusion of technology in our society has an important consequence. Hardware has to be properly analyzed during acquisition and qualification phases of the supply chain. We're surrounded by electronic devices and appliances that in many cases perform critical functions in areas such as telecommunications, defense and health. Because of that, it's crucial to validate electronic components they contain. Any one of those devices could be equipped with a software or hardware backdoor with serious repercussions. The presence of hardware backdoors in particular represents a nightmare for the security community.

In this post, I'll explore some of most insidious backdoor hardware attacks and techniques for prevention and detection.

Hardware attacks

One of the main consequences of the world economic crisis was budget cuts for manufacturing and security validation, in both public and private sectors. Unfortunately, the cost is considered the factor that most influences the final choice for buyers. This led to the decline in the use of authorized resellers.

Orders today are usually made directly to manufacturers located in the Far East due to cheaper production costs. Those areas are considered to be conflicting because their governments are responsible for the majority of cyber attacks against western companies.

The risk of acquiring hardware components with a backdoor is concrete. Asian governments aren't exclusively accused of stealthily designing backdoors. Recently, Edward Snowden revealed that the NSA requested that the US manufacture to plant a backdoors in exported products.

Malicious hardware modifications from insiders represent a serious threat. System complexity, the large number of designers and engineers involved in every project and the delocalization of production in risky countries due to low cost poses a security threat.

A malicious individual could alter a small component in the overall system for espionage or sabotage. Such attacks can be especially devastating in security-critical industries, such as the military.

The introduction of hardware Trojans could happen in each phase of the supply chain, depending on the methods adopted by attackers and on the technology used for hacking.

Common hardware attacks include:

- Manufacturing backdoors, for malware or other penetrative purposes; backdoors aren't limited to software and hardware, but they also affect embedded radio-frequency identification (RFID) chips and memory
- Eavesdropping by gaining access to protected memory without opening other hardware
- Inducing faults, causing the interruption of normal behavior
- Hardware modification tampering with invasive operations; hardware or jailbroken software
- Backdoor creation; the presence of hidden methods for bypassing normal computer authentication systems
- Counterfeiting product assets that can produce extraordinary operations, and those made to gain malicious access to systems

Hardware attacks pertain to the following devices:

- Access control systems such as authentication tokens
- Network appliances
- Industrial control systems
- Surveillance systems
- Components of communication infrastructure

Attackers could also act at lower levels to affect the work of microcircuits, fundamental components of any electronic device. Recently researchers have explored the possibility of modifying hardware behavior by managing the concentration of dopant in electronic components or altering its polarity.

Scientists Adam Waksman and Simha Sethumadhavan provided further ideas of types of hardware backdoors:

- **Ticking time bombs–** An attacker could program a time bomb backdoor into HDL code that automatically triggers backdoors after a pre-determined fixed amount of time after the power-on of a device. A device could be forced to crash or operate maliciously after a determined number of clock cycles. It's clear that this type of attack could be very dangerous. An attacker could design a kill switch function that could be undetectable by any validation methods.
- **Cheat codes**– An attacker could program backdoor triggers based on specific input data, otherwise known as "cheat codes." A "cheat code" is secret data that the attacker uses to identify themselves to hardware backdoor logic. It'll then initiate a malicious operation mode. Of course, the code must be unique to avoid being accidentally provided during validation tests. As opposed to time bombs, this kind of backdoor needs a second attack vector, the "cheat code." The attacker could provide "cheat codes" which send a single data value containing the entire code (single-shot "cheat codes") or a large cheat code in multiple pieces (sequential "cheat codes.")

Means and motivations

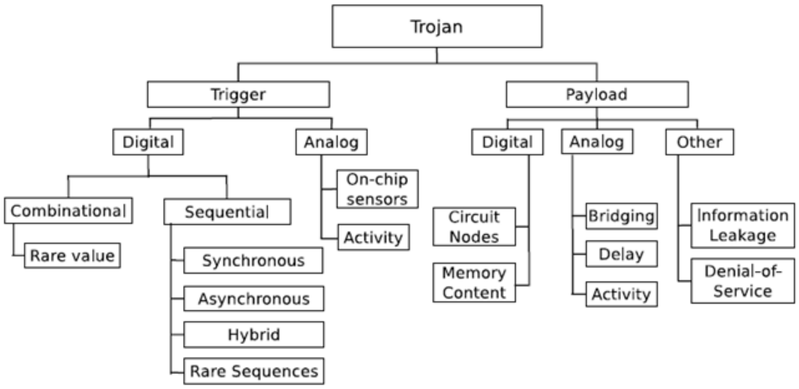
Hardware attacks aren't exclusive to state-sponsored operations. Criminal organizations could be interested to commercialize counterfeiting products or steal sensitive information to resell. Asian countries are the main areas where manufacturers have production plants. But cheap production costs could hide serious threats. The main motivations of hardware attacks are:

- Hardware cloning
- Breaking services, obtaining them with piracy
- Imitating user authentication for system access
- Information leakage
- Unlocking devices, to gain access to an internal shell or to increase control of a system
- Unlocking hidden features

China is considered the most dangerous adversary for the western world. But they're also a primary hardware manufacturer, from defense to consumer goods. Acquiring hardware components from China has raised an intense security debate. In the past, the Department of Defense has been aware of receiving processors vulnerable to tampering. Some of them were complex enough to easily conceal Trojans or backdoor circuitry installed by unknown third parties. Component failures were detected in defense contractors such as Boeing, Raytheon, BAE, Northrop Grumman, and Lockheed.

After discovering that, the DoD has pushed to launch a program to evaluate hardware that reliably detects tampering operations at the circuit or chip level. Hardware validation requires accurate verification of any component of imported systems. Authenticity and security must be assured before including components in mission-critical systems.

Often, officials at the Department of Homeland Security have warned of weaknesses in the technology supply chain that result in importing devices pre-infected with malware and backdoors that leave the units vulnerable to exploitation.



Hardware Trojan Taxonomy: Chakraborty, Narasimhan & Bhunia (2010)

Backdoor malware is no longer a secret. Kill switches and backdoors could be easily hidden in network devices from the same manufacturer and could be used to sabotage or spying by criminals or foreign states.

In 2011, the US government released the White House Cyber Policy Review, warning of risks related to the delocalization of manufacturing plants:

"The emergence of new centers for manufacturing, design, and research across the globe raises concerns about the potential for easier subversion of computers and networks through subtle hardware or software manipulations. Counterfeit products have created the most visible supply problems, but few documented examples exist of unambiguous, deliberate subversions."

Real or alleged case studies

Most recently, intelligence agencies have banned Lenovo PCs due to backdoor vulnerabilities.

That worrying news was reported by the Australian Financial Review. The article revealed that intelligence sources confirmed the ban was initiated in the mid-2000s, after a series of hardware and firmware tests on Lenovo chips.

The details are classified, but the general notion was that Lenovo PCs include vulnerabilities that could provide remote access to intruders.

Lenovo PCs banned by intelligence agencies from countries including the US, UK and Australia.

"AFR Weekend has been told that British intelligence agencies' laboratories took a lead role in the research into Lenovo's products. Members of the British and Australian defense and intelligence communities say that malicious modifications to Lenovo's circuitry – beyond more typical vulnerabilities or 'zero-days' in its software – were discovered that could allow people to remotely access devices without the users' knowledge. The alleged presence of these hardware 'back doors' remains highly classified."

Intelligence agencies fear cyber espionage from the Chinese government, recognized as the most dangerous collector of western intellectual property and sensitive information.

Lenovo isn't the unique. Chinese firms accused of espionage in the past include Huawei and ZTE. They have long attracted suspicion from international intelligence agencies. The former head of the CIA and NSA, Michael Hayden, publicly maintains that Huawei spies for the Chinese government.

The companies incriminated are all market leaders. The possibility that hardware backdoors are hidden in their products is a nightmare for foreign governments.

The perfect backdoor

The main vulnerability concern is the design of backdoors that could avoid detection mechanisms. Deliberate vulnerabilities could be introduced at different levels of production with different effects on compromised devices.

Backdoors could be substitute a component of a device or add supplementary circuits. Both methods are functionally efficient, but aren't feasible, due to the difficulty of hiding hacks upon careful inspection.

Because of that, researchers worldwide are evaluating new methods for designing hardware backdoors. Rakshasa firmware malware and dopant-level hardware Trojans are some of the most interesting possibilities.

Rakshasa backdoors

Backdoors are usually supported by software. Flaws, including bugs, are common in software that runs on most devices. Fortunately, this type of backdoor is easier to detect and immunize.

Last year, researcher Jonathan Brossard mentioned during the Black Hat security conference in Las Vegas, that a new strain of malware is nearly impossible to remove once it compromises a device. Brossard named his agent "*Rakshasa*", defining it a "*permanent backdoor*" that's hard to detect, and nearly impossible to remove.

It's clear that he didn't find a new vulnerability, but demonstrated how much harder is to detect that type of backdoor. *"It's a problem with the architecture that's existed for 30 years. And that's much worse."*

The abstract demonstrates that permanent backdooring of hardware is possible. Rakshasa is able to compromise more than a hundred different motherboards. The impact could be devastating. Rakshasa malware infects the host BIOS, taking advantage of a potentially vulnerable aspect of traditional computer architecture. Any peripheral, such as a network card or a sound card can write to the computer's RAM or to smaller portions of memory allocated to any of the other peripherals.

First, there are backdoor disabling features such as NX, essential for protection against malware, viruses, and exploits. It also removes fixes for System Management Mode (SMM), in operating mode in which all normal execution (including the operating system) is suspended and special software, usually firmware or a hardware-assisted debugger, and is executed in high-privilege mode.

With these few steps, the attacker has properly compromised security of the machine, allowing malware to completely erase hard disks and install a new operating system.

"We shall also demonstrate that preexisting work on MBR subverts such as bootkiting and preboot authentication software brute force can be embedded in Rakshasa with little effort."

Due the mechanism of infection, in order to sanitize a PC, it's necessary to flash all the devices simultaneously to avoid that happening during a disinfection of a single device. That's because it could affected by other compromised components.

"It would be very difficult to do. The cost of recovery is probably higher than the cost of the laptop. It's probably best to just get rid of the computer." said Brossard.

Rakshasa has been developed with open source BIOS software, including the Coreboot project and Sea BIOS, and because of their compatibility with most hardware, it's hard to detect.

When the machine boots up, malware downloads all the malicious code it needs. Of course it disables the resident antivirus and stores the code in memory. In doing so, it avoids leaving traces on the hard disk that could be detected as infectious.

The most important issue about Rakshasa malware isn't related to how it can infect victims randomly. But Brossard alerted the scientific community to the possibility of using it as a backdoor in hardware. In many cases doubt has been raised about if backdoors are present in Chinese devices, telecommunications in particular.

Hardware qualification is a serious problem. Let's consider the impact of a compromised device in a military environment, or in any large systems.

"The whole point of this research is to undetectably and untraceably backdoor the hardware. What this shows is that it's basically not practical to secure a PC at all, due to legacy architecture. Because computers go through so many hands before they're delivered to you, there's a serious concern that anyone could backdoor the computer without your knowledge."

In a paper for Intel, Brossard said:

"There is no new vulnerability that would allow the landing of the bootkit on the system." The company's statement argues that it wouldn't be possible to infect the most recent Intel-based machines that require any changes to BIOS to be signed with a cryptographic code. and it points out that Brossard's paper "assumes the attacker has either physical access to the system with a flash programmer or administrative rights to the system to deliver the malware. In other words, the system is already compromised with root/administrative level access. If this level of access was previously obtained, a malicious attacker would already have complete control over the system even before the delivery of this bootkit."

But the above scenario isn't far from what could happen in a manufacturing plant that's compromised by hackers.

Hardware backdoors inserted at gate level

We've discussed the possibility of designing backdoors based on supplementary circuits, electronics component substitution and firmware. But the research is also evaluating more sophisticated methods based on the manipulation of dopant chemical elements.

Recently, a team of experts, composed by researchers Georg T. Becker, Francesco Ragazzoni, Christof Paar and Wayne P. Burleson, published a study on stealth dopant-level hardware Trojans.

The study describes how it is possible to conduct a hardware-based attack introducing legitimate circuits that aren't detectable as Trojans.

"In this paper we propose an extremely stealthy approach for implementing hardware Trojans below the gate level, and we evaluate their impact on the security of the target device. Instead of adding additional circuitry to the target design, we insert our hardware Trojans by changing the dopant polarity of existing transistors."

The possibility of infiltrating supply chains with hardware Trojans is a target for governments. The repercussions could be critical, considering the penetration of technology in military and commercial sectors.

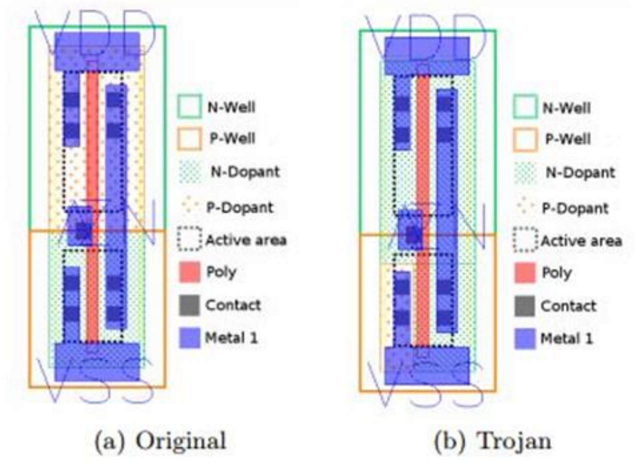
Now, the security community has focused its research on designing hardware backdoors by modifying motherboard circuitry or wiring. This technique could be ineffective by a careful process of hardware qualification.

Another factor to consider is that an attacker would have access to layout masks and additional spaces for inserting malicious circuits that would be easy to detect. The researchers demonstrated how to modify a circuit introducing hardware Trojans able to elude detection. Backdoors are implemented at the gate level. That's done by hanging the dopant polarity of existing transistors, instead of introducing supplementary hardware.

In the past, research has been conducted without successfully altering the behavior of hardware by changing the concentration of dopant element. Now, researchers have changed polarity with a specific foundry setting.

"Since the modified circuit appears legitimate on all wiring layers (including all metal and polysilicon), our family of Trojans is resistant to most detection techniques, including fine-grain optical inspection and checking against 'golden chips.'"

By modifying the conductive behavior of electrical components with the addition of dopant, the researchers were able to insert their stealthy hardware Trojan. This was done on Intel's random number generator design used in Ivy Bridge processors, as well as in a side-channel resistant SBox implementation.



(a) Original (b) Trojan

Figure – Figure of an unmodified Trojan inverter gate and backdoored one

The paper details how to compromise Intel Ivy Bridge processors by pulling off a side channel attack that leaked secret keys from the hardware. The attack is operated on dopant polarity of hardware components. Therefore, a backdoor is undetectable by optical inspection. The principle proposed by research is summarized in the following abstract:

"A gate of the original design is modified by applying a different dopant polarity to specific parts of the gate's active area. These modifications change the behavior of the

target gate in a predictable way and are very similar to the technique used for code-obfuscation in some commercial designs."

The study demonstrated that the backdoor created with this technique isn't detectable. That raises serious questions about hardware qualification and the delocalization of production in places where the cost of manufacturing is cheap. A similar backdoor is able to elude hardware Trojan detection mechanisms in post-manufacturing and pre-manufacturing processes.

The researcher specified that detection is possible but not practicable due to the complex analysis necessary on every single component. Because of the large volume of devices being produced, that's not practical.

"Even if chips are manufactured in a trusted fabrication, there is the risk that chips with hardware Trojans could be introduced into the supply chain. The discovery of counterfeit chips in industrial and military products over the last years has made this threat much more conceivable."

"A dedicated setup could eventually allow one to identify the dopant polarity. However, doing so in a large design comprising millions of transistors implemented with small technologies seems impractical and represents an interesting future research direction. We exploit this limitation to make our Trojans resistant against optical reverse-engineering."

By attacking Ivy Bridge, researchers were able to get their Trojan onto the processor at the sub-transistor level:

"Our Trojan is capable of reducing the security of the produced random number from 128 bits to n bits, where n can be chosen. Despite these changes, the modified Trojan RNG passes not only the Built-In-Self-Test (BIST) but also generates random numbers that pass the NIST test suite for random numbers."

The study illustrates the feasibility and efficiency of a new type of sub-transistor level Trojan that only needs dopant modification, leaving the layout mask unchanged. No additional electronic components nor gates are added. The method doesn't change metal, polysilicion or the active area. That makes detection by optical inspection impracticable.

Backdoor prevention and detection

Hardware vulnerabilities are usually difficult to detect. Electronics devices could be preloaded with spyware or other malware that could be used to disable or extract data from host systems, or to sabotage the target hosting network.

A fundamental aspect of hardware backdoors that makes them hard to detect is that they can lie dormant during verification and can be triggered to wake up later.

In literature there are several techniques to detect the presence of hardware backdoors, even though it's often difficult. The main problem is assembling hardware systems from components designed by untrusted designers, or procured from untrusted third-party manufacturers or subcontractors.

The military is increasingly dependent on commercial components to build its systems. In most cases, hardware is manufactured outside of US borders. The DoD is aware of the possible presence of backdoors or malicious software that could harm its systems. The principal concerns for US Defense are related to the security of the global supply chain.

"Devices are assembled from hundreds or thousands of components each coming from different parts of the world making it impossible to verify the trustworthiness of every supplier."

To respond to the need of security, DARPA has started a program codenamed Vetting Commodity IT Software and Firmware (VET.) It's inviting security experts to "look for innovative, large-scale approaches to verifying the security and functionality of commercial information technology devices bought by the DoD."

The goals of the ambitious program are to define of a set of tests for component validation, and to determine how to prove an absence of malware. The following goals are described on the DARPA website:

- *Defining malice: Given a sample device, how can DoD analysts produce a prioritized checklist of software and firmware components to examine and broad classes of hidden malicious functionality to rule out?*
- *Confirming the absence of malice: Given a checklist of software and firmware components to examine and broad classes of hidden malicious functionality to rule out, how can DoD analysts demonstrate the absence of those broad classes of hidden malicious functionality?*
- *Examining equipment at scale: Given a means for DoD analysts to demonstrate the absence of broad classes of hidden malicious functionality in sample devices in the lab, how can this procedure scale to non-specialist technicians who must vet every individual new device used by DoD prior to deployment?*

"Rigorously vetting software and firmware in each and every device is beyond our present capabilities, and the perception that this problem is simply unapproachable is widespread. The most significant output of the VET program will be a set of techniques, tools and demonstrations that will forever change this perception."

Prevention

The best way to prevent the insertion of hardware backdoors is to tightly control the entire production process. Use a trusted design team, use component design that's free of backdoors and release it to a trusted foundry. Trusted people, clean production environments and self made tools provide assurance that products are free of backdoors.

In reality, this sort of production chain is impractical for most every products due to high costs and duration of the production process.

Prevention could be implemented in different phases of production:

- The design level- the ability to create trusted circuits using untrusted EDA tools is the primary goal for detection at this stage. Principal solutions fully account for the use of all hardware resources, leaving no time frame for the execution of malicious features.
- The fabrication level- provide both hardware specifications and a list of "security-related properties." Customers and manufactures must agree how to turn these concepts into a formal mathematical codification procedure. The IP producer writes the Hardware Description Language (HDL), they also produce evidence that the specified hardware fulfills all requirements. That can then be checked by a theorem, proven when the IP is delivered to the consumer.
- The post-fabrication level– to cut down the attacker's window of opportunity, reconfigurable logic could be placed between the output of some ICs and the input of other ICs, disguising some of the design from an attacker who has access to the Register Transfer Level.

Detection

Detection mechanisms are used to discover the presence of a hardware backdoor. Once found, a malicious component could be removed from a design. That applies if one is discovered at the Register Transfer Level, or an IC could isolate it to avoid triggering backdoor.

Security experts have focused backdoor detection at the post-fabrication phase, due to how critical the fabrication process is. It's considered to be the weakest link in the product development cycle.

Backdoor production is an arms race that involves attackers developing new evasion techniques, and defenders are exploring new methods for prevention and detection. Despite various detection techniques that exist, none of them is capable of identifying every kind of backdoor.

Principal detection methods could be grouped in the following categories:

- **Destructive methods**– A form of detection completely destroys the analyzed component. Due to this, it's considered useful. Hardware components are completely reverse-engineered, an activity that is expensive and time consuming. Reverse-engineering processes are generally performed by Chemical Metal Polishing followed by an Scanning Electron Microscope (SEM) image reconstruction and analysis. Verification of the circuits is usually performed through visual comparison. The methods are ineffective if the backdoor has been added prior to fabrication. *"In this case the IC would have to be completely reverse engineered through the reading of the logic gate layout and reconstruction of an RTL description. This makes the reverse engineering problem much more difficult."*
- **Non-destructive methods** – A form of detection that doesn't destroy the component, they're classified as being either invasive, or non-invasive depending on if the techniques leave the design unaltered. Invasive methods are used to modify the design of components to control the embed feature for backdoor detection. An example of an invasive method is the insertion of an additional I/O for each module to allow execution of self-testing circuitry specifically designed to test anomalous events. Non-invasive hardware Trojan detection is performed by comparing the "performance" of a component with a known "good copy," used as reference model. Non-invasive hardware backdoor detection can be done either at runtime or at test-time.

Interfering with a hardware backdoor

Researchers Adam Waksman and Simha Sethumadhavan mentioned various techniques to make backdoor design undetectable to attackers in their study "Silencing Hardware Backdoors."

The researchers proposed to hide backdoor scrambling input that that reaches hardware at runtime. That makes it difficult for malicious components to acquire the information they need to perform malicious activities.

The following are methods for disabling backdoor triggers:

1. ***Power resets***– *The technique prevents untrusted units from detecting or computing how long they've been active, thus preventing time-based attacks.*
2. ***Data obfuscation***– *The technique encrypts input values to untrusted units to prevent them from receiving special codes, thus preventing them from recognizing database triggers.*
3. ***Sequence breaking***– *The technique pseudo-randomly scrambles the order of events entering untrusted units to prevent them from recognizing sequences of events that can serve as data-based triggers.*

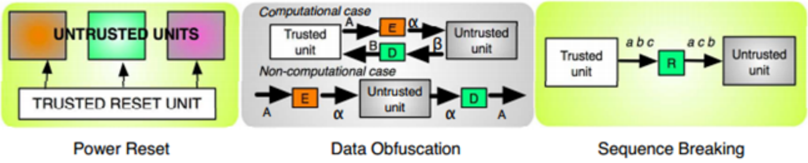


Figure – Silencing backdoor techniques

Conclusion

Due to the wide diffusion of electronic components, the problem of hardware qualification is considered crucial. Microcircuits and firmware are present in every device around us, from our cars to sophisticated defense systems.

Each product requires careful verification. Also, consider sectors that aren’t considered critical, such as consumer devices. The effect of hardware backdoors hidden in their circuits could be catastrophic, due the globalization of manufacturing activities, a foreign government could intentionally compromise the production plant to insert malicious backdoors in a component destined for the global market.

Today, we’re far from the possibility of analyzing every device distributed in the market for the previously stated reasons. It’s time to start carefully considering the risks related to the lack of hardware qualification in each industry. The cyber strategy of each government today needs to define the means and methods to guarantee satisfactory security levels in every hardware component. That’s the only viable strategy to avoid devices that are tainted with hardware backdoors.

References

http://securityaffairs.co/wordpress/16748/hacking/spy-agencies-ban-on-lenovo-pcs-due-to-backdoor-vulnerabilities.html

http://securityaffairs.co/wordpress/7786/hacking/rakshasa-is-it-possible-design-the-perfect-hardware-backdoor.html

http://securityaffairs.co/wordpress/17875/hacking/undetectable-hardware-trojan-reality.html#!

http://www.toucan-system.com/research/blackhat2012_brossard_hardware_backdooring.pdf

http://securityaffairs.co/wordpress/1198/cyber-crime/hardware-qualification-a-must-in-a-cyber-strategy.html

http://www.darpa.mil/NewsEvents/Releases/2012/11/30.aspx

https://www.ideals.illinois.edu/bitstream/handle/2142/35322/Edwards_Nathan.pdf

https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&ved=0CGQQFjAE&url=http%3A%2F%2Fwww.dtic.mil%2Fcgi-bin%2FGetTRDoc%3FAD%3DADA547668&ei=oRtHUuO4FsWrtAa63YCACw&usg=AFQjCNH3gt2JT4VuIsQ4VLrPkp7Vr4xwOg&sig2=NMrLhCdNn8DLB9LyxJNr_Q&bvm=bv.53

http://www.cs.columbia.edu/~simha/preprint_oakland11.pdf

http://people.umass.edu/gbecker/BeckerChes13.pdf

http://www.infosecisland.com/blogview/15095-DHS-Imported-Devices-Infected-with-Malware.html

http://www.eecs.berkeley.edu/~csturton/papers/defeating-uci-oak11.pdf