# Securing the IT Supply Chain in the Age of Globalization

## An Interim Report

James C. Hoe (representing CyLab and CSSI)
Carnegie Mellon University
November 28, 2007

# Motivations for This Study

- Outsourcing of design and manufacturing of IT systems and components
- Potentials for deliberate tampering to degrade security or reliability

---

- What are the implications for the US government's IT infrastructure?
- What measures has the IT industry taken to mitigate the downsides?
- What more should the IT industry do in the future?

# To put it concretely

- Does it make a difference to the US government that the same ThinkPads were badged as IBM one day and Lenovo the next?
- Does it make a difference (security-wise) to the US government that an IT product is US or foreign made?
- Does it make a difference to the US government if all IT manufacturing capabilities were overseas?
- Doesn't the rest of the world have the same concerns about their reliance on US IT products?
- Doesn't the average consumer also want assurances in security and reliability?

(see answers at the end)

# CyLab/ISA Industry Study

- Input (from Industry and Government)
  - workshops of industry, government and academicians

    *(2 IS Alliance Workshops, 1 NSF Workshop)*
  - industry questionnaires and interviews
  - regular phone conferences with ISA steering committee
- Output (from CMU)
  - cataloging of current and anticipated threats in design and manufacturing tampering
  - cataloging of current industry best practices in safe-guarding against tampering
  - recommendations for further actions (policies, practices and research)

# Outline

- Introduction
- Review of the 1st IS Alliance workshop
- My current thinking on this topic
- Wrap-up

# 1st ISA Workshop Agenda

- The government's perspective—Annabelle Lee, DHS Director of Security Standards and Best Practices and co-chair of the US Government Inter-Agency Task Force on Securing the IT Supply Chain
- The industry's perspective—Industry Panel (A. Szakal, IBM; J. Carlisle, Lenovo and D. Doughty, Intel)
- An economist's perspective—Scott Borg, Chief Economist US Cyber Consequences Unit
- A software engineer's perspective—Bill Scherlis, CMU
- A hardware designer's perspective—James C. Hoe, CMU
- Where research is needed—Academic Panel
- Breakout groups

# Government's perspectives
## Annabelle Lee, DHS

- An issue "for all parts of the system no matter where the companies are located or where the products are developed"
  - increase adversary's cost
  - reduce the US government's risk of exposure
  - decrease the payoff of a successful attack
- Defense in breadth
  - protect all phases of the lifecycle (design spec → decommission)
  - many phases are owned/controlled by the private sector
- Inter-Agency Supply Chain Risk Management Working Groups
  - Acquisition Process; Education and Training; IT Assurance; and Standards, Guidelines and Best Practices

*Cyber security impacts physical security (power-grid, air traffic...)*

# Industry's Perspective

- David Doughty, Intel
  - there is no perfect security; what is "enough" security to deter attempts *(cost vs. effectiveness)*
  - more than the CPUs are susceptible *(from chipsets to the network)*
- Andras Szakal, IBM
  - greater threats on the software side
  - current practices are good *(100% assurance not the goal)*
  - need practicable framework for establishing trust between supplier and consumer *(and still test some more for yourself)*
- Jeff Carlisle, Lenovo
  - global supply chain is a reality facing every company
  - industry as a whole needs to proactively head off any problems *(real or perceived)*

# Economist's Perspective

## Scott Borg, US Cyber Consequences Unit

- Analyze supply-chain attacks as specific combinations of
  - **attackers:** { criminal gangs, disgrunttled (ex)employees, rogue corporations, ideological militants, nation-states }
  - **attacks:** { interrupt, corrupt, discredit, control } an operation
  - **motives:** { gain financially, divert value, manipulate financial instruments, make credible a coercive threat, advertise a cause, stop an opposing activity, reduce the opposer's ability to attack/defend }
- Almost all attack scenarios are unlikely due to lower-hanging-fruit alternatives, except .....
- Most probable threat (by cost-effectiveness analysis)

  $\Rightarrow$ nation-states x {*} x reduce the ability to attack/defend

  $\Rightarrow$ malicious firmware

# Software Engineer's Perspective

## Bill Scherlis, CMU

- Provenance and trust are important when we lack the technology to analyze the artifact itself (e.g., source code)
- More than processes, we need tools, analysis and techniques to improve observability in order to make acceptance evaluation possible
- Trust the tools to do more—formal methods and verification have come a long way
- Don't lump defect-types—different attributes need different technologies

*Security, dependability and quality issues go hand in hand*

# Hardware Designer's Perspective

## James C. Hoe, CMU

- High-end ICs (CPUs) are relatively safe from tampering
  - cost, technology and man-power involved are very high
  - too many low-hanging fruits (insider, software/firmware attacks) for comparable ends
- Low-end ICs carry much greater threats
  - creatable by a small entity with no accountability
  - a $2 NIC or disk controller has as much access as the CPU
  - low-margin market leaves little headroom for care
- Tampering testing is not a part of the established HW flow
  - need to extend/adapt design-for-test (DFT) to tamper detection
  - very hard to find dormant behaviors with specific triggers

*R&D needed to catch-up essentially from scratch*

# Breakout Groups 1 and 2

- Where are the most likely points of attack?
  - SW and firmware are much more vulnerable than HW
  - behaviors that can remain dormant until specifically triggered
  - insider attacks will always remain a great concern
- What are existing best practices and certifications? How to do risk analysis?
  - no consensus on the cost-effectiveness of the lifecycle model?
  - does quality assurance suffice as security assurance?
  - can we develop run-time protection against anomalies?

---

- BTW, both groups found these two questions impossible to answer except for fixed contexts *(no one-size-fits-all)*

# Breakout Group 3

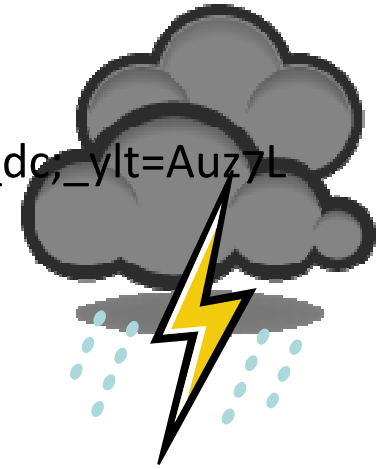
- What are the risk calculations from the government's perspective?
  - how can we trust the supply chain when we know the source countries are spying on us?
  - is there a difference between US and foreign corporations anymore?
- Can we fashion an educational agenda for decision makers
  - industry needs to be prepared to respond by
    - educating the correct issues
    - solving the correct issues
    - advocating the correct issues

# To put this study in context . . .

# Seagate/Maxtor News

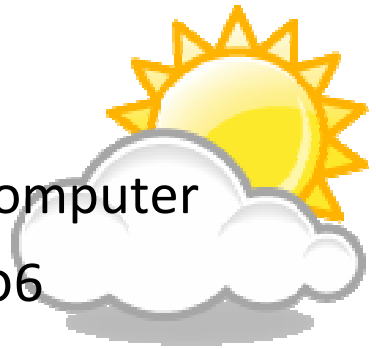
- November 12, Reuters - China virus found in Seagate drives in Taiwan:
  - "external disc drives sold in Taiwan had been infected with a virus which reportedly sent users' information to China"
  - "Investigation Bureau officials said their investigation suggested infection may have occurred when the devices were in the hands of Chinese sub-contractors during the manufacturing process"

- http://news.yahoo.com/s/nm/20071112/bs_nm/taiwan_trojan_dc;_ylt=Auz7L xdNY.q24LC92I2D1QiDzdAF



# The sky is falling?

- From Seagate's website (http://www.seagate.com/www/en-us / support/downloads/personal_storage/ps3200-sw)
  - "Seagate has traced this issue to a small number of units produced by a Maxtor sub-contract manufacturer located in China."
  - "According to Kaspersky the virus is the Virus.Win32.AutoRun.ah, a molar virus that searches for passwords to online games and sends them to a server located in China." "All of the known games affected are Chinese with the exception of World of Warcraft."
- My prognosis: *accidental, operator error*
  - lesson: don't web surf on the manufacturing-floor computer
  - this is not unique: iPods had a similar episode in 2006



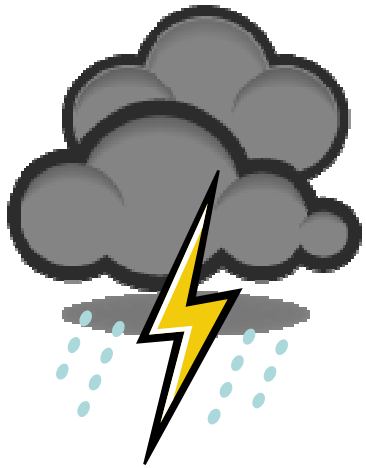
# The sky is falling?

- But, before we get too comfortable, this could also be a test-the-water precursor to something much more sinister?

- Unlikely in this case, since it is just too crude of an attempt to be useful even as an experiment

# The sky is falling?

- The incident does prove, deliberate or not, it is possible for an artifact of tampering to get through “quality assurance”
- With humans in the loop, you don’t need high-tech
- If it is an “operator error”, it can happen anywhere in the world



# The sky is falling?

- No serious IT department would fall for this
  - CMU/ECE IT reformats each new PC and reinstalls from an in-house disk image
  - presumably this is also standard practice with government agencies and major corporations

- *But does anyone reload firmware?*

# The sky is falling?

- What about the consumers?
- Are you vigilant/paranoid enough to reinstall your next brand new home PC after you unpack it?
- *How about your iPhone?*

# To Wrap-up

- The need to secure the IT supply chain is real, and it is not just a "government" problem
- The problem is encompassing and amorphous
  - policies and best practices are only road-blocks to anticipated problems
- The overall framework of solutions cannot be rigid
  - attackers are creative and fluid
  - operator-errors simply defy imagination
- The solutions have to be practicable from both supply-side and demand-side

*One cannot have perfect security, but there is no substitute for due diligence. Raise the lowest hanging fruit.*

# Some Answers

- Does it make a difference to the US government that ThinkPads were badged as IBM one day and Lenovo the next?

No difference, provided there is an objective way to prove that the ThinkPads from Lenovo really is "the same" as IBM's.

# Some Answers

- Does it make a difference (security-wise) to the US government that an IT product is US or foreign made?

No difference. A good security assessment should rely very little on assumptions based on the country of origin.

# Some Answers

- Does it make a difference to the US government if all IT manufacturing capabilities were overseas?

Yes. There are definite supply risks if this became a reality, and Moore's Law voids an IT equivalent of the "Strategic Petroleum Reserve"

Need to ensure a diverse source of supplies

# Some Answers

- Doesn't the rest of the world have the same concerns about their reliance on US IT products?

Yes. For example, the Chinese Academy of Sciences has developed a commercially viable home-grown CPU (Loongson, ST Micro Part Number STLS2E02)

# Some Answers

- Doesn't the average consumer also want assurances in security and reliability?

Yes. I do.