Booz | Allen | Hamilton

Counterfeit Detection: Like Computer Security but worse!

Dr. Allan Steinhardt
Booz Allen Science Fellow and Senior Executive Advisor
IEEE Fellow

- **A walk down (Cyber) Memory Lane**
- The grudging acceptance of Cyber as a board room, not boiler room, topic
- How did cyber earn a seat at the C-suite?

- **The counterfeit threat**

- **CCO: Chief Counterfeit Officer? CSCO: Chief Supply Chain Officer?**

May 2016

The Counterfeit Challenge and Computer security: The past is prelude

- The dark ages: Computers as appliances
  - Department of washing machines?
  - When HVAC fails in C-suite meeting…..
  - Hanging chad? Gore vs Bush
  - Root users, Wizards, and spies oh my……
  - Are engineers truly human? Glass ceiling?

- Middle ages: Cracks in the upper echelons of corporate/governance elites
  - Why are there no facility managers in VP, SES meetings?
  - Why are there now, reluctantly, CISO, CIO, etc. amongst VPs?
  - Could a Cyber warrior ever be a service chief?
  - What can us nerds do to help widen the cracks?

- Today: Revenge of the Nerds: Entering the C-suite
  - Building trust
  - Resource trades: Steve Jobs……
  - No longer HVAC
  - Today we can explain the threat, and explain the solutions to laymen
  - But how do we do this in counterfeit detection?

Defining the Counterfeit Threat

Federal

In 2011, the Missile Defense Agency said a **single system** contained approximately **800 counterfeit** parts and cost $2 million to fix.

A 2012 US Senate Committee investigation revealed **~1,800 cases of suspect counterfeit electronic parts** in just part of the supply chain over a two year period 2009-2010

- **Feels the early lazy days with Cyber Hacking**

Some vague statistics, **4th page news**.

Today in **Cyber:** Russia: Crimea cyber war
OPM hack, Wikileaks, Snowden, Target, Anonymous etc.
Sony-N Korea, 1st major event on US soil used as a weapon

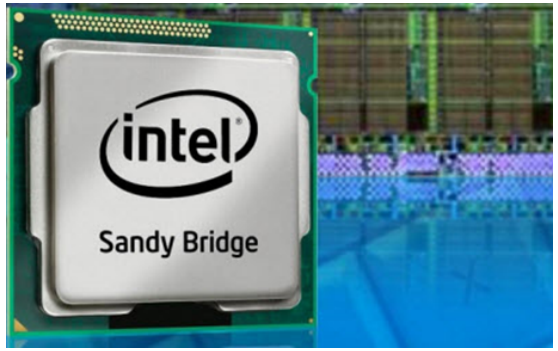
- **Counterfeit: next stage in escalation?**

-Crash cars, airplanes, trains, power blackout?
-Loose a war before it starts? [car key FOBs disabled?]
-counterfeit can be a portal into Cyber IP theft, or simply piracy and resale, or a weapon.
-Piracy and prepositioning in full swing today…..

Commercial

- Commercial HW developers must contend with untrustworthy suppliers and counterfeit ICs introduced into the supply chain.
  - Costs to mitigate risks
  - Costs to replace failed parts
  - Lost sales
  - Lost brand value or damage to image

Intel press release on Jan 31, 2011 announce issue with a support chip



A support chip "Cougar Point" for Sandy Bridge has issues with the SATA port.

A transistor in the 3Gbs PLL clocking scheme was biased incorrectly (disables the transistor)

Malicious or careless?
Bug or trojan?

Scope of the Counterfeit Problem

[redacted]

"***No type of company or organization has been untouched*** ***by counterfeit electronic parts. Even the most reliable of parts sources have discovered counterfeit parts within their inventories.***"

- U.S. DEP'T OF COMMERCE, DEFENSE INDUSTRIAL BASE ASSESSMENT: COUNTERFEIT ELECTRONICS 7 (2010)

Taken together with the value of domestically produced and consumed counterfeits, the significant volume of digital and fake products being distributed via the Internet, and the loss of economic development, harm to health and safety, reduced technology transfer, and innovation: **the total magnitude of counterfeiting and piracy worldwide is estimated to be well over *US$600 billion***

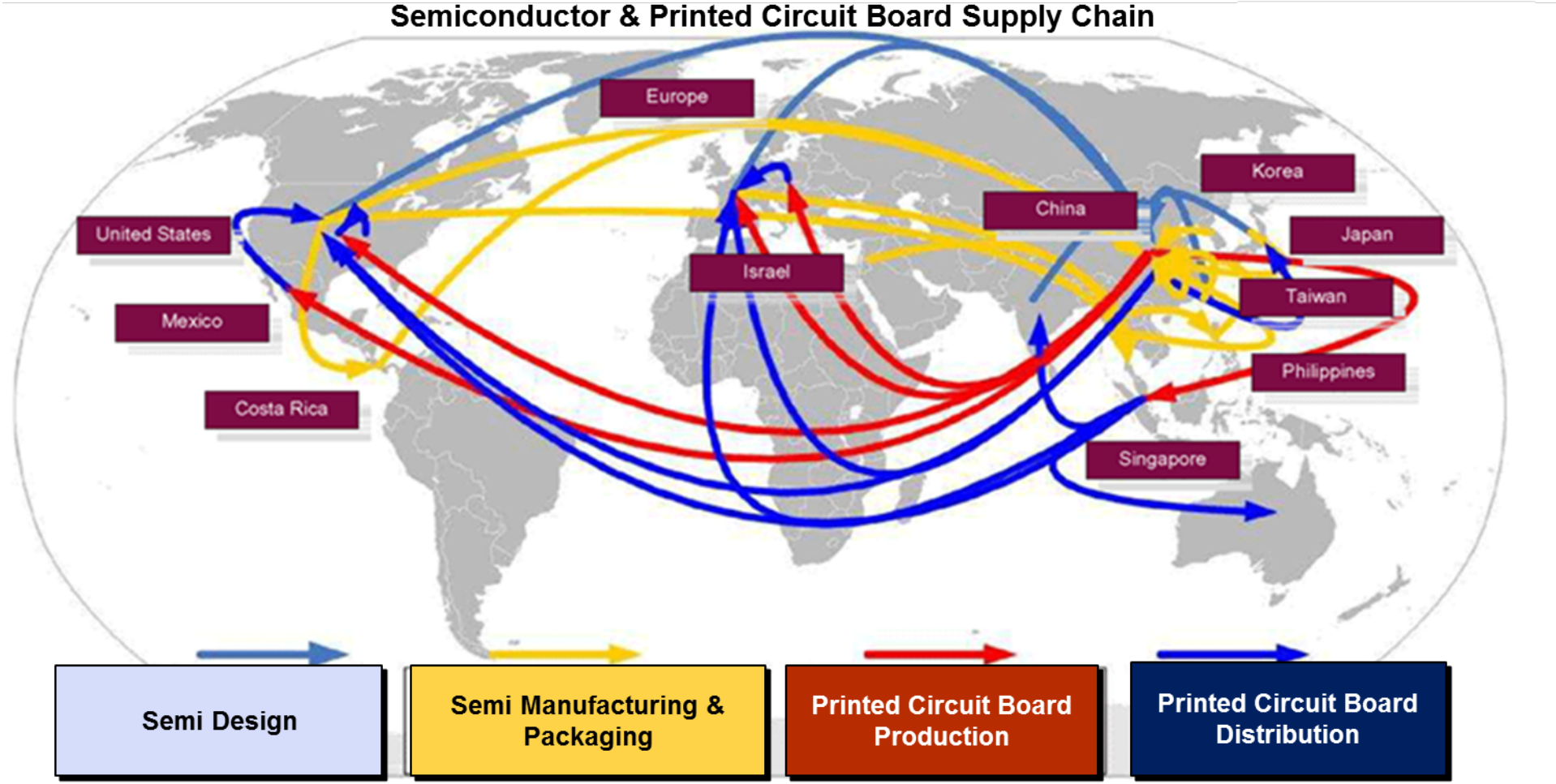
- International Chamber of Commerce http://www.iccwbo.org/advocacy-codes-and-rules/bascap/about/

And in 2012, market research firm IHS iSuppli reported that the five most prevalent types of semiconductors reported as counterfeits represented **$169 billion in potential risk per year** for the global electronics supply chain.

Sadly this type of data does very little to turn the needle, if computer hacking history is a guide…..
Remember: if no one is in the C-suite meetings the trades will not include counterfeit mitigation

Global Supply Chain

Federal agencies and commercial organizations are more dependent than ever on a ***global supply chain*** which inherently creates ***a lack of trust*** *as well as lack of accountability*



Gartner: 6.4 Billion non-computing machines connected to the internet

Booz | Allen | Hamilton

Counterfeit and physical layer will increasingly be the Cyber attack vector of choice

Source: IDC Manufacturing Insights & Booz Allen analysis

Conclusions and a look forward: To the C-suite and beyond

- The computer world of 1's and zero's remains extremely vulnerable
- Only recently is there anything approaching a senior presence in cyber amongst decision makers
- Without this presence technology solutions are ignored and irrelevant
- The above is true in spades in Counterfeit/physical layer attack
- Today senior decision makers can understand basic cyber threats:
  - Not a good idea to have siri on and a camera on while in sensitive meetings
  - "passw@rd" is not the greatest password
  - Going into battle with location aware option on your cell phone probably not idea
  - OPM: list of all blackmailable offenses and foreign contact in enemy hands undesireable
- Our challenge, and it is an **important and urgent one:**
  - How do we give senior decision makers ways they can understand and relate to counterfeit?
  - Bad examples: FPGA PUF ring oscillations, clock drift from PLL upset, etc. etc.
  - Good examples? Not so easy, we are back in the dark ages of cyber! **The appliance is the threat!**