By: JollyMongrel for Rootcon VII

PACKAGE TAMPERING: INJECTING A JACK-IN-THE-BOX

imageSource:
http://www.clker.com/cliparts/7/d/a/e/1207433294999107010liakad_Jack-in-the-box.svg.hi.png

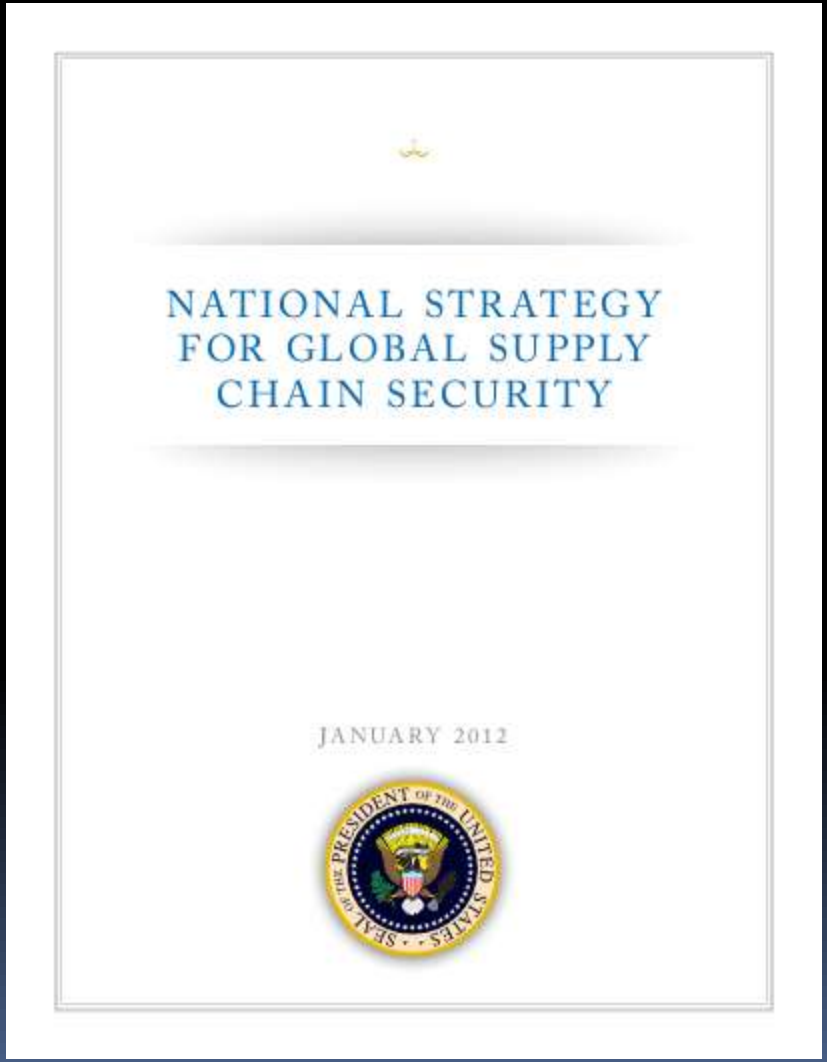
SUPPLY CHAIN FABRIC

Supply Chain | Defined

- A supply chain is a system of organizations, people, activities, information, and resources involved in moving a product or service from supplier to customer. Supply chain activities transform natural resources, raw materials, and components into a finished product that is delivered to the end customer.

State of the Supply Chain

- Fact
  - Threat to the supply chain is a Global Issue.
  - The new playing field of cybersecurity.



Supply Chain | Information

- A supply chain is defined as the set of suppliers that contribute to the content of a product or system (both hardware and software) or that have the opportunity to modify its content (*Ellison & Woody, 2010*)
- "The supply chain is now recognized as a major cyber threat affecting development and operation of computer systems and not just a threat to the transportation of material and goods from supplier to purchaser" (*Filsinger, et. al, 2012*)

Supply Chain | Information

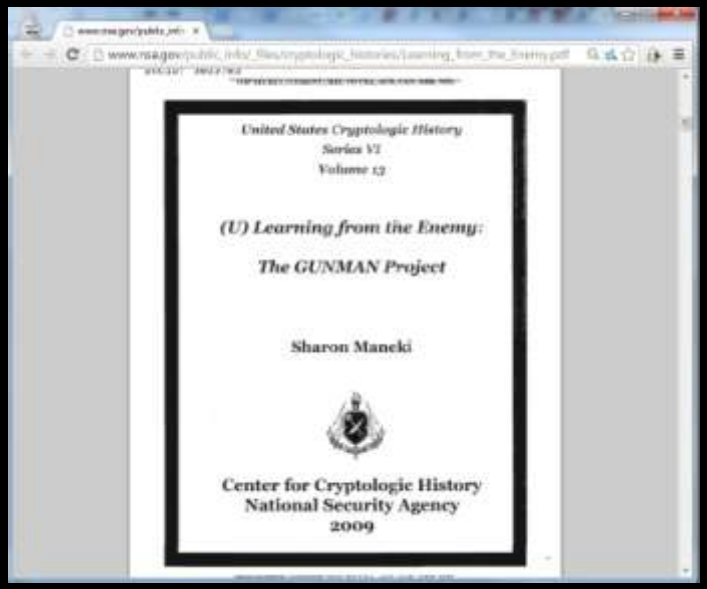
- "Federal IT systems are increasingly at risk of both intentional and unintentional supply chain compromises due to the growing sophistication of information and communications technologies (ICT) and the growing speed and scale of a complex, distributed global supply chain" (*Boyens, et. al, 2012*)
- "Threat actors can use the supply chain to insert hardware or software containing malicious logic through tampering during the development and implementation of an information system" (*Villasenor, 2011*)

IT EQUIPMENT FABRIC

Hardware based | Attacks

- Cold War Era
  - In the 1980s, Soviet agents secretly installed keylogging devices in about a dozen embassy IBM Selectric typewriters. -

    source: *http://www.nsa.gov/public_info/_files/cryptologic_histories/Learning_from_the_Enemy.pdf*



source: *http://www.mrmartinweb.com/type.htm*

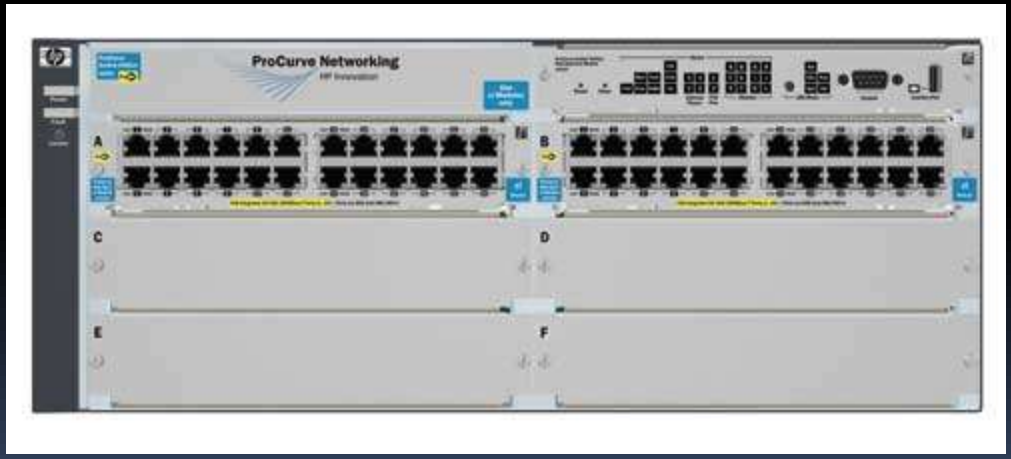
Hardware based | Attacks

- X-Box trojan

Image src:https://lh3.ggpht.com/_WWOoNoYElHQ/THWfCtl54HI/AAAAAAAAAPk/EcODQ8Bl8Xg/s320/14-Aug-26-10-pic5.jpg

Hardware based | Attacks

- Documented threats
  - CVE-2012-0133
    *"HP ProCurve 5400 zl switches with certain serial numbers include a compact flash card that contains an unspecified virus, which might allow user-assisted remote attackers to execute arbitrary code on a PC by leveraging manual transfer of this card." Source:*https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0133



Img src: http://www.hp.com/rnd/images/large/J8699A.jpg

Point of | Realization

- "Despite the potentially devastating impact that a large-scale hardware attack could have on commerce, defence, and government function, the need to proactively address hardware security remains widely underappreciated." *Source: http://www.brookings.edu/research/papers/2011/05/hardware-cybersecurity*

Packaging FABRIC

Packaging | Defined

- Packaging (as an activity) is best described as a coordinated system of preparing goods for transport, distribution, storage, retailing and use.

Tampering | Defined

Img src: http://pharmalawnews.com/files/2013/09/tylenol.png

- Tampering is interfering with, changing or damaging something that shouldn't be.

Packaging | Defined

- Packaging is best described as a low hanging fruit in the high tech supply chain to implant alien component to an IT hardware product for arbitrary purposes.

Packaging | Function

- ***Technical***
  - *Contain*
  - *Protect*
  - Measure
  - Dispense
  - *Store*
- ***Marketing***
  - *Communicate*
  - *Display*
  - *Inform*
  - *Promote*
  - *Sell*
  - Motivate

Packaging | Function

- ***Technical***
  - *Contain an eavesdropper*
  - *Protect the eavesdropper*
  - Measure
  - Dispense
  - *Store*

- ***Marketing (Social Engineering)***
  - *Communicate ill messages*
  - *Display*
  - *Dis Inform*
  - *Promote ill objectives*
  - *Sell ill ideas*
  - *Motivate them to follow the instruction to initiate the alien component.*

Packaging | Levels

- ***Primary package*** - the first wrap or containment of the product that directly holds the product for sale.
- ***Secondary package*** - A wrap or containment of the primary package.
- *Distribution package* - A wrap or containment whose prime purpose is to protect the product during distribution.
- *Unit load* - a group of distribution packages assembled into a single unit for purposes of mechanical handling, storage, and shipping.

Packaging | Levels

- ***Primary package*** - the first wrap or containment of the product to be tampered with surreptitiously.
- ***Secondary package*** - A wrap or containment of the primary package to be tampered with surreptitiously.
- *Distribution package* - A wrap or containment whose prime purpose is to protect the product during distribution to be tampered with surreptitiously and lock picked.
- *Unit load* - a group of distribution packages assembled into a single unit for purposes of mechanical handling, storage, and shipping to be tampered with surreptitiously and lock picked.

Packaging | Levels

- ***Consumer package*** - A package that will ultimately reach the consumer as a unit of sale from a merchandising outlet.
  - *An avenue to conduct a targeted attack.*
- ***Industrial package*** - A package for delivering goods from manufacturer to manufacturer.

Packaging | Levels

- ***Consumer package*** - A tampered package that will ultimately reach the consumer as a unit of sale from a merchandising outlet.
- ***Industrial package*** –A package for delivering tampered goods from manufacturer to manufacturer capitalizing on their mutual trust.
  - *An avenue to perform an attack among the weakest links of the integrators involved in product development.*

Packaging | Weaknesses

- Almost everyone can access packaging materials.
- Packaging and labeling is only controlled for Good Manufacturing Practice (GMP) and not for security.
- Material flow of printed packaging materials is very different from starting materials.

Package Tampering | Demo

- Jolly vs. Mail envelope

Package Tampering | Demo

- Jolly vs. Milk Box

Package Tampering | Demo

- Jolly vs. Softdrinks

Possible | Solutions

While the author has long believed that physical security is an understudied area to leverage a successful cyber attack, control of the quality of packaging components, specifications development, quality control testing, security audits and analysis of the product package should not be neglected. Packaging engineering should have a role in the effort of the global community in addressing supply chain security in order to control the consequential cyber attacks attributed to it. Furthermore, the following solutions are being proposed:

Possible | Solutions

- Develop solid policies and best practices on supply chain protection giving special attention on chain of custody and the exit node.
- Develop solid policies and best practices on physical security covering packaging of High Tech equipment.
- Establish packaging materials specification.
- Set up quality assurance in packaging including the recommendation of test equipment and training of personnel.
- Conduct company packaging audits as well as competition's practices.
- Develop quality control testing procedures.
- Carry out quality control testing of integrator's packaging materials.

References

- Contents derived from:
  - Soroka, W. Fundamentals of Packaging Technology, 3rd edition
  - http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf
  - http://www.nsa.gov/public_info/_files/cryptologic_histories/Learning_from_the_Enemy.pdf
  - http://www.scientificamerican.com/article.cfm?id=the-hacker-in-your-hardware
  - http://upload.wikimedia.org/wikipedia/commons/2/29/Supply_and_demand_network_%28en%29.png
  - http://nvlpubs.nist.gov/nistpubs/ir/2012/nist.ir.7622.pdf
  - www.jps.anl.gov
- Images lifted from:
  - http://www.bbc.co.uk/schools/gcsebitesize/design/images/fd_packaging_stages.gif
  - http://image.made-in-china.com/2fojooAjrTiWhMCYqV/DHL-UPS-FedEx-EMS-Service.jpg
  - http://foundationmediasolutions.files.wordpress.com/2010/02/consumer-packaged-goods.jpg
  - https://origin-ars.els-cdn.com/content/image/1-s2.0-S0377221708009806-gr3.jpg
  - http://www.machinevc.com/images/TamperProof_product.jpg
  - http://pe-energy.com/wp-content/uploads/2012/12/supply_chain.bmp
  - www.jps.anl.gov

Thank You &
God Bless us all!