

## **IT Project Failures**

**Michael Kringsman**

**May 12th, 2008**

# **FBI: Counterfeit Cisco routers risk “IT subversion”**

Posted by Michael Kringsman @ 6:05 pm

An internal Federal Bureau of Investigation presentation states that counterfeit Cisco routers imported from China may cause unexpected failures in American networks. The equipment could also leave secure systems open to attack through hidden backdoors. The scope of the problem is broad and results from a complicated supply chain originating in Shen Zhen.

From a narrow project failures perspective, network problems caused by this equipment should be treated as any other hardware malfunction. Of course, the entire concept of third parties using compromised hardware to infiltrate public and private systems in the United States is another matter entirely.

Faulty networking hardware can be a nightmare to troubleshoot and fix. For example, the U.S. Customs and Border Protection (CBP) location at Los Angeles Airport (LAX) suffered a failed router last year; the problem delayed 20,000 passengers before technicians successfully isolated and repaired the issue.

The following slides, pulled from the larger presentation, indicate how seriously the FBI is taking this threat to national security.



# FBI Criminal Investigation: Cisco Routers

The overall classification of this presentation is  
**UNCLASSIFIED**

Section Chief Raul Roldan  
Supervisory Special Agent Inez Miyamoto  
Intelligence Analyst Tini Leon

January 11, 2008

## Search Warrants Executed



# Counterfeit Equipment



- **Routers**
  - Models: 1000 and 2000 Series
- **Switches**
  - Models: WS-C2950-24, WS-X4418-GB (for CAT4000series)
- **GigaBit Interface Converter (GBIC)**
  - Models: WS-G5483, WS-G5487
- **WAN Interface Card (WIC)**
  - Models: VWIC-1MFT-E1, VWIC-2MFT-G703, WIC-1DSU-T1-V2

# Counterfeit Products



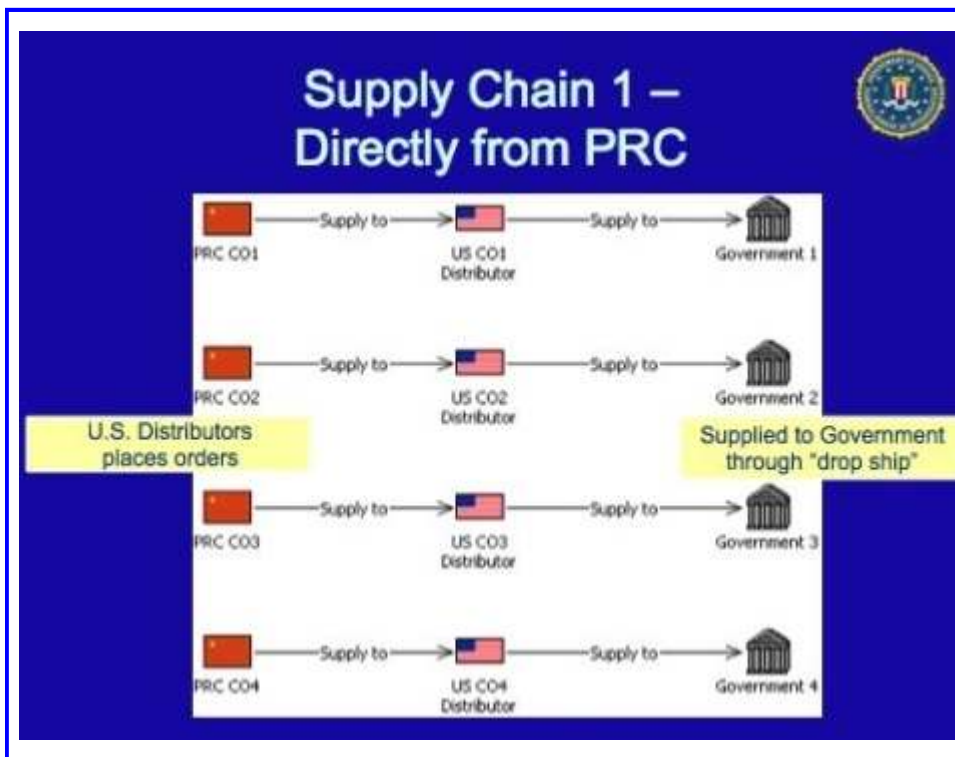
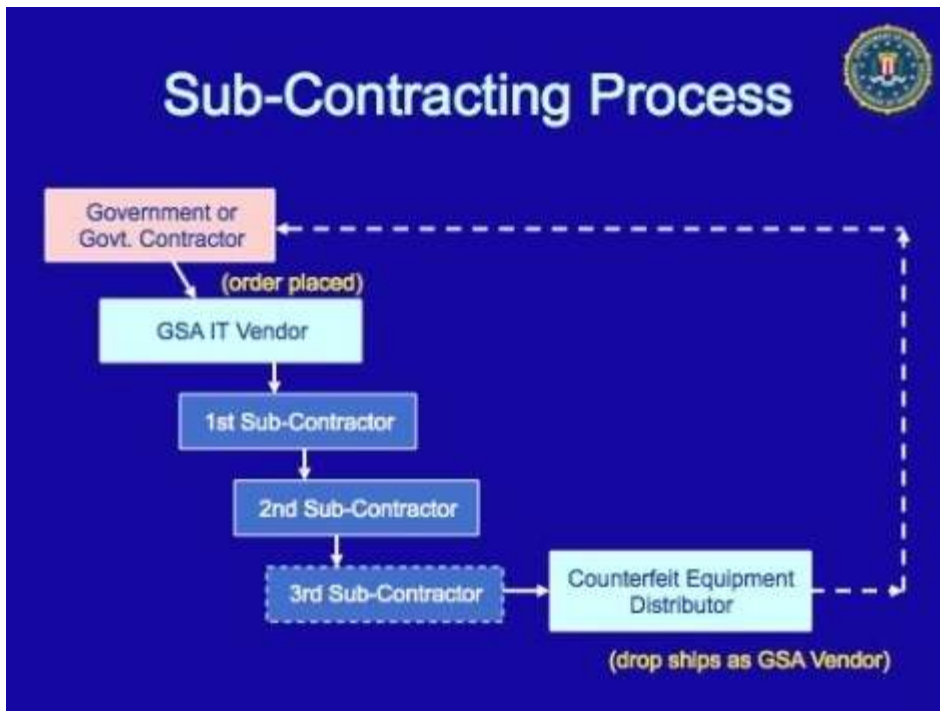
Source: [http://www.zdnet.com/page-ny-warn\\_used\\_cisco\\_interface\\_cards\\_like\\_these.aspx](http://www.zdnet.com/page-ny-warn_used_cisco_interface_cards_like_these.aspx)

## Cost Comparison Example

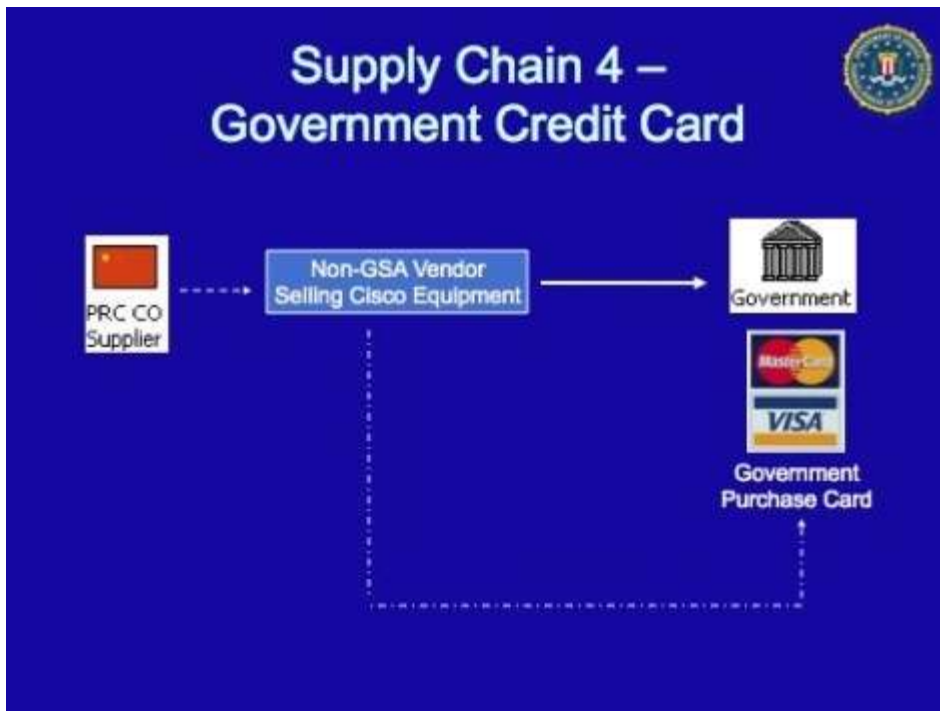
- **Counterfeit**
  - 1721 Router
  - \$234.00
- **Genuine**
  - 1721 Router
  - \$1,375.00

## Cisco Identified Problems

- **Problems**
  - Low manufacturing standards
  - Higher failure rate
  - Duplicate MAC addresses of routers and switches can shut down an entire network
- **Examples**
  - In 2002, duplicate MAC addresses shut down an end user's network in Pittsburgh
  - In 2004, a government agency conducted a network upgrade to its North American weather communication system—it failed upon installation
  - Cisco 1721 router installed in a network caught fire due to a faulty power supply







### Scope of the Problem

- Alliance for Gray Market and Counterfeit Abatement (AGMA) & KPMG White Paper
  - 1 in 10 IT products sold are counterfeit
  - 10% IT products counterfeit
    - \$100 billion

Source: RFEA/AGMA/AGMA, "Measuring the Costs of Counterfeiting in the Information Technology Industry," 2002



## The Threat

- **IT Subversion/Supply Chain Attack**
  - Cause immediate or premature system failure during usage
  - Gain access to otherwise secure systems
  - Weaken cryptographic systems
- **Requires "intimate access to target system"**

Source: Committee on National Security Systems, Framework for Complete Risk Allocation For National Security Systems in the Era of Globalization, November 2008

Michael Krigsman is CEO of Asuret, Inc., a software and consulting company dedicated to reducing software implementation failures. See his full profile and disclosure of his industry affiliations.

Copyright © 2008 CNET Networks, Inc. All Rights Reserved. [Privacy Policy](#) | [Terms of Use](#)