Internet of Things meets Hardware Cybersecurity

Serge Leef

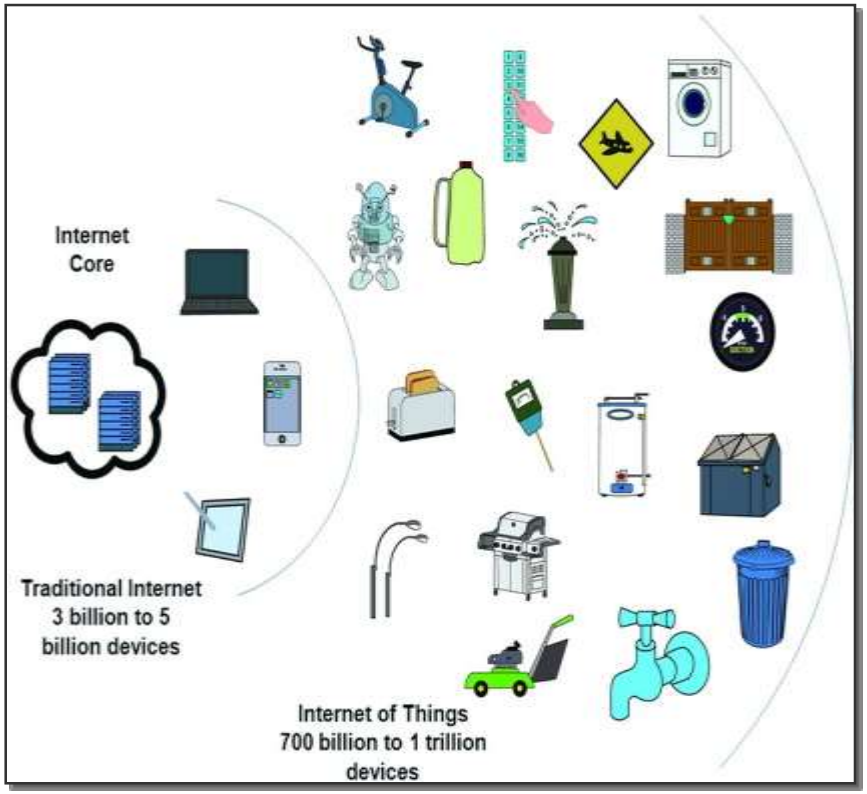
Vice President and General Manager

- New Ventures
- System Level Engineering Division

Mentor Graphics®

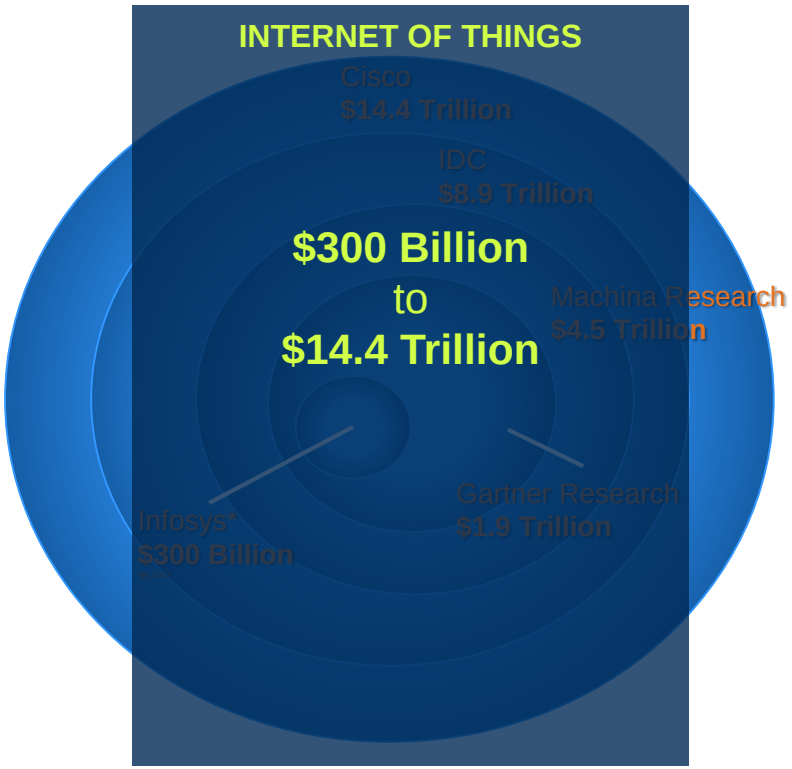
IoT: Emergence of Intelligent Systems

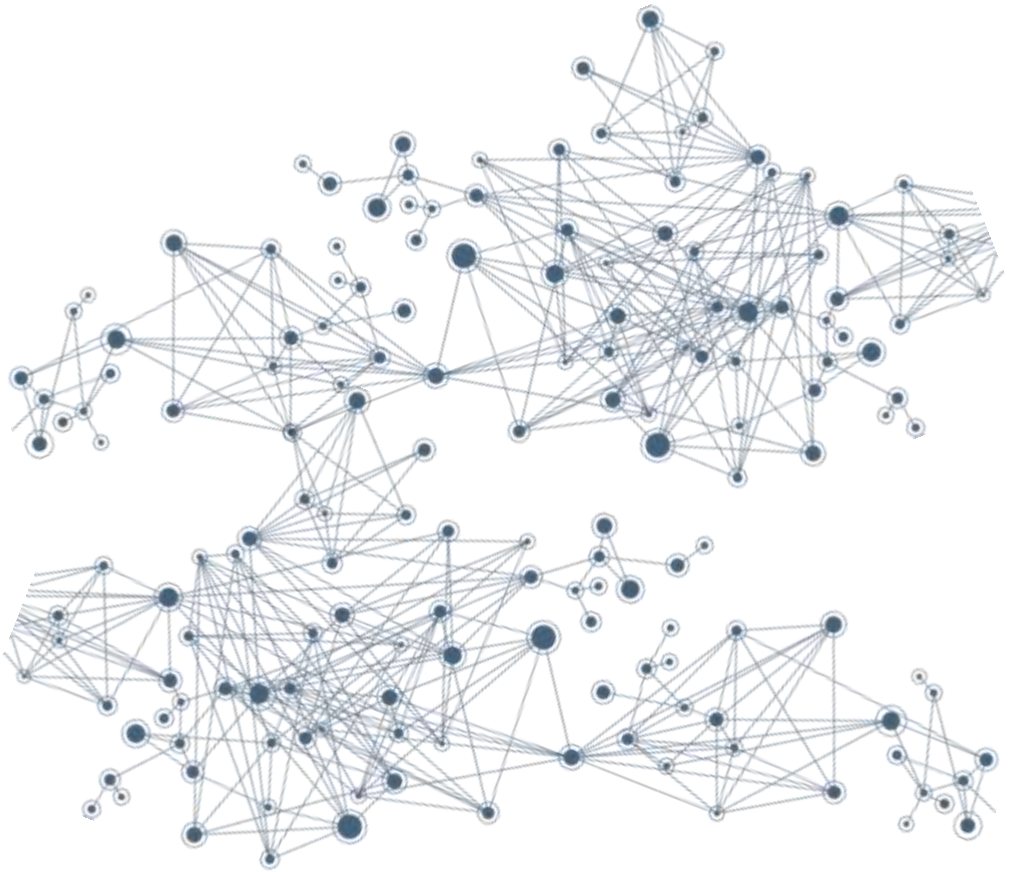
- Intelligent Systems / **Internet of Things**
  - 75B Devices will be connected by 2020 (Morgan Stanley)
  - Execute native or cloud-based applications
  - Data collection & analytics
  - Explosive growth potential
- Internet of Things
  - Uniquely identified "things"
  - Machine-to-machine communication
  - Cloud infrastructure
  - Cyber-physical systems
- Edge-node design
  - Electronics, Controls, Software
  - Multi-physics, Communications



© 2010 Mentor Graphics Corp.
www.mentor.com

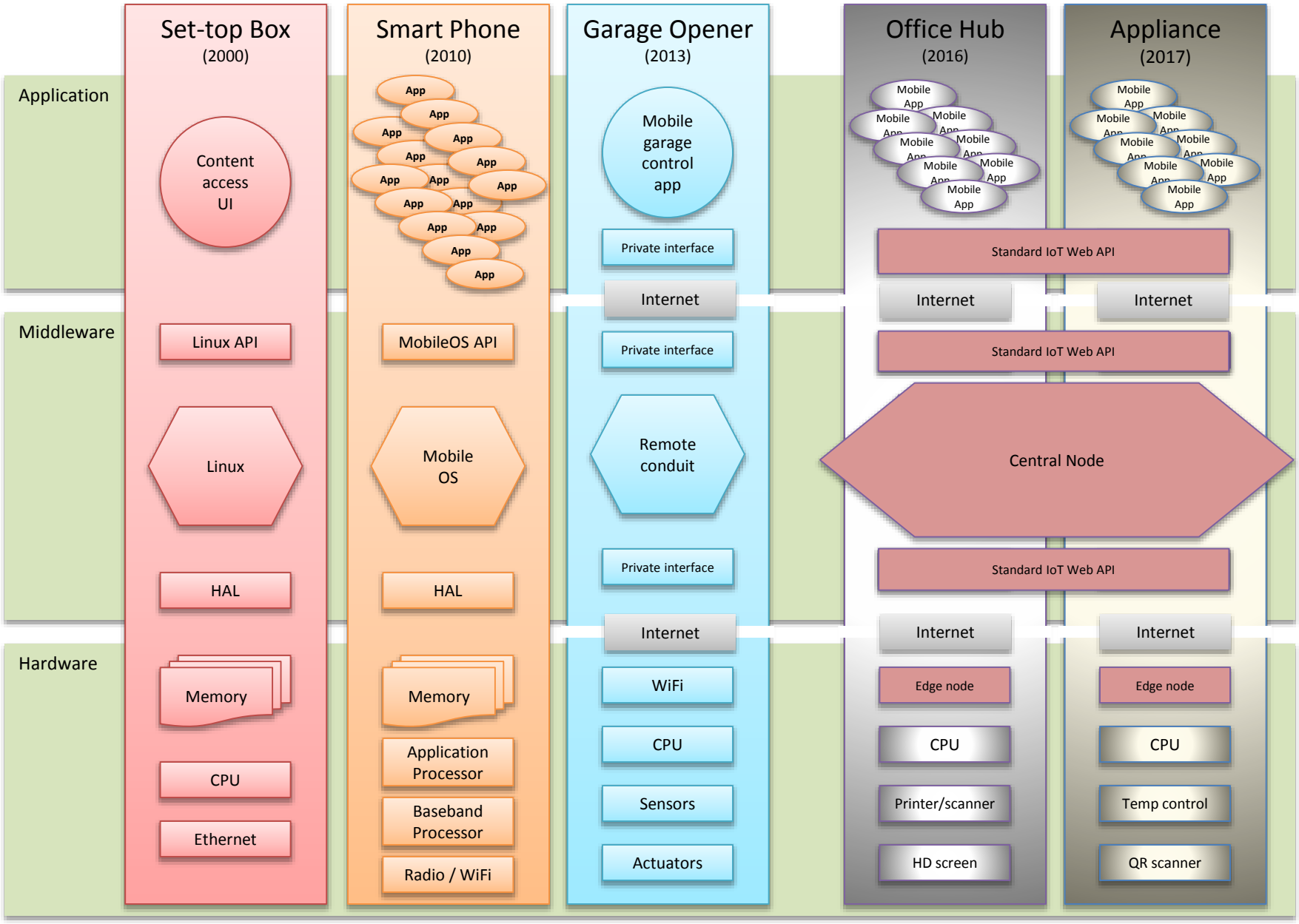
IoT Projected Market Size Generates Excitement



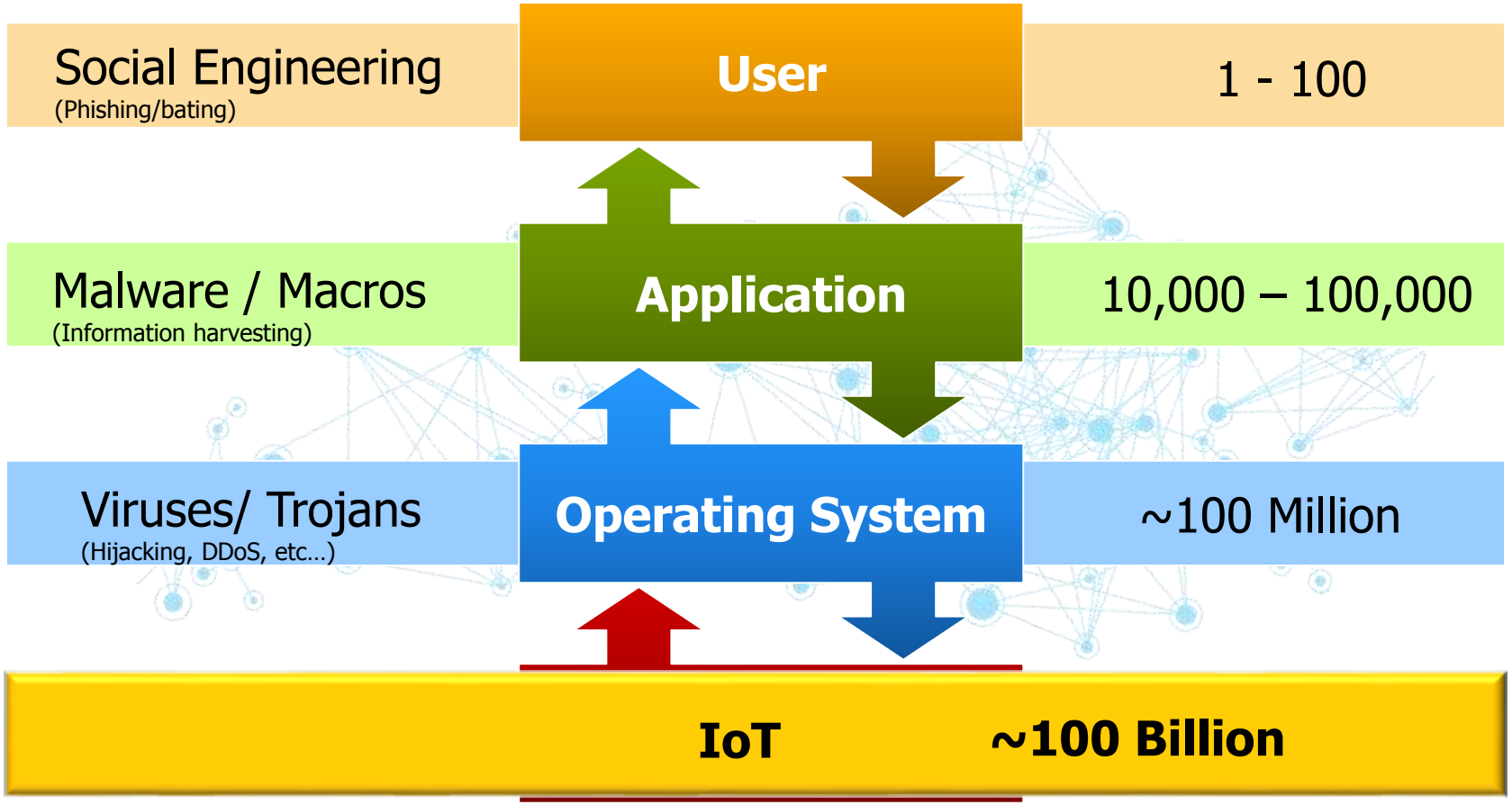


© 2010 Mentor Graphics Corp.
www.mentor.com

Embedded systems moving into IoT world



We used to believe that hardware is the "Root of Trust", but… not anymore



© 2010 Mentor Graphics Corp.
www.mentor.com

IoT World is Already Under Attack

Proofpoint Research: Internet of Things (IoT) Cyber Attack Security

In January 2014, Proofpoint researchers discovered proof of a much-theorized but never before seen Internet of Things (IoT) cyber-attack. Proofpoint has observed what we believe to be an industry first of devices, including some home appliances (TVs, a refrigerator), sending malicious email spam.

As our researchers were analyzing email-borne threats, they observed a recent cyber attack campaign where more than 25 percent of the malicious email (over 750,000 messages) came from things that were not conventional laptop or desktop computers, but rather members of the Internet of Things; a "Thingbot'-net".

Specifically, researchers observed a series of cyber attack campaigns:

- From Dec 23rd through Jan 6th
- Three campaigns per day, approximately 100k emails per campaign
- Over 450k unique IP addresses, over 100k were from IoT devices

A more detailed examination suggested that while the majority of mail was initiated by "expected" IoT devices such as compromised home-networking devices (routers, NAS), there was a significant percentage of attack mail coming from other non-traditional sources, such as connected multi-media centers, televisions and at least one refrigerator.

Additionally, observing the devices:

- A vast number of the devices are running embedded linux servers (usually busybox)
- Some use mini-httpd, some apache
- Some are ARM devices, some are MIPS (or something very similar) others are based on an embedded Realtek chipset (for example, media players)
- Some are believed to be game consoles
- Some are NAS devices (one specific brand has open telnet, open ssh and an SMTP server - all unsecurable)
- Some set-top boxes were also seen as exploited

This proof of a systematic compromise of IoT devices and its subsequent use of those Thingbots to further attack other networks is something we've never seen before. This suggests an unfortunate future for both home users and enterprises, the latter of whom now faces an even larger volume of malicious attack capacity.

Worse, these compromised home appliances provide a mechanism where users can unknowingly expose their work environment to such cyber attacks. All a user has to do is use a remote RDP connection, or conceivably simply take an action like checking their fridge from their work PC. If a classic drive-by or even a redirect has been installed, the work PC is now compromised (though this is arguably more farfetched). Clearly, as the trend towards smart devices and BYOD increases, the risk of enterprise exposure increases correspondingly, exponentially.

SiliconANGLE » The Internet Of Things Is Under Attack!

The Internet of Things is under attack!

MELLISA TOLENTINO | JANUARY 30TH

READ MORE

Tweet 22 | 0 | Like 3 | Share 6

Most of us enjoy using some kind of Internet of Things device these days – after all, IoT devices run the whole gamut of smaller gadgets, including smartphones, tablets, cars, homes, wearable devices and home appliances that are connected to the Internet, as they make our lives so much easier.

Unfortunately, as with anything that connects to the Internet, it can be exploited by hackers, and though some of you may think that hacking an Internet connected refrigerator is not a big deal, cybercriminals can use information from that to access your other online accounts.

Internet security firm Proofpoint recently described how it had uncovered the first proven IoT-based attack which involved 750,000 malicious email communications coming from over 100,000 everyday consumer gadgets, including home-networking routers, connected multi-media centers, televisions and at least one refrigerator.

'Bash' bug could let hackers attack through a light bulb

By Jose Pagliery @Jose_Pagliery September 25, 2014: 12:54 PM ET

2K TOTAL SHARES | 815 | 274 | 271 | 151

NEW YORK (CNNMoney)

Say hello to the bash bug, a lesson in why Internet-connected devices are inherently unsafe.

Computer security researchers have discovered a flaw in the way many devices communicate over the Internet. At its most basic, it lets someone hack every device in your house, business or government building – via something as simple as your "smart" light bulb.

With this flaw, criminals can potentially break computers or steal private and government information.

HP: Most IoT Devices Lack Security, Open To Attack

Thu, 07/31/2014 - 3:18pm

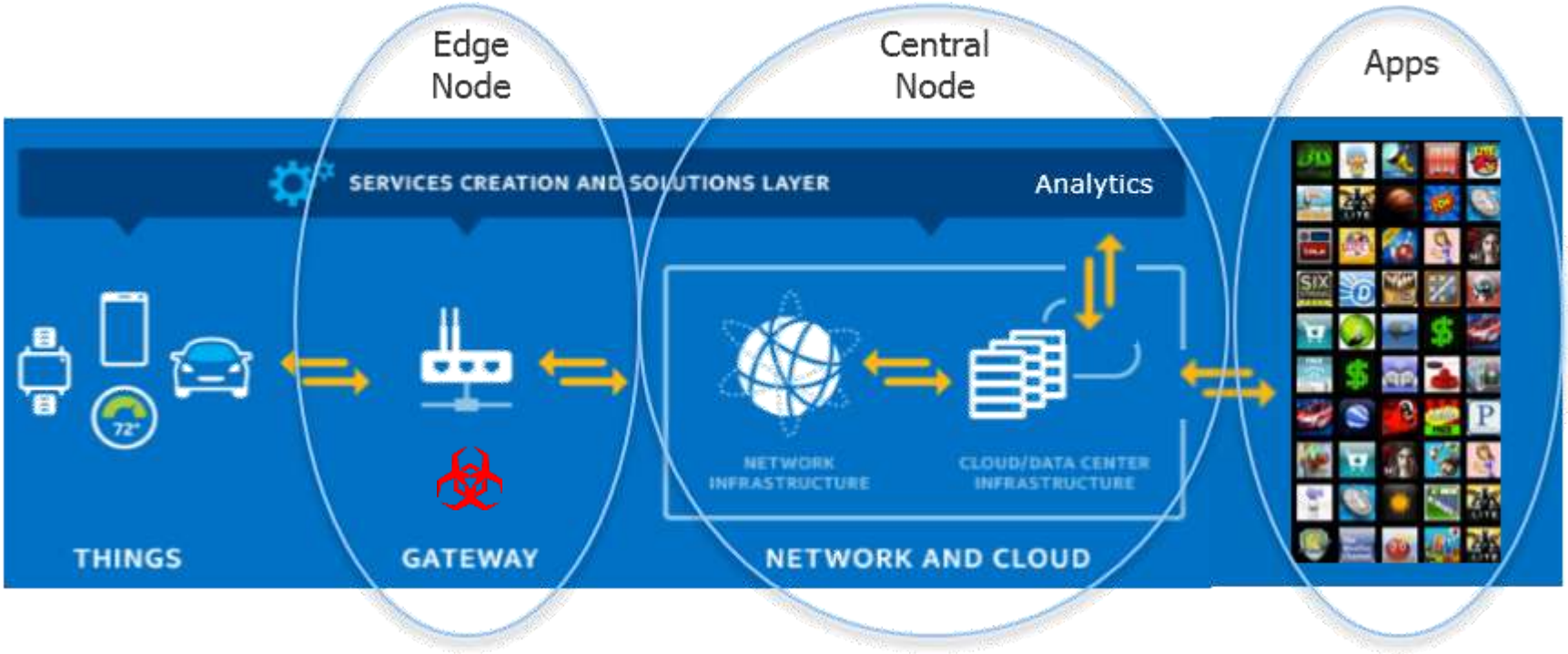
by Jon Minnick, Associate Editor, Manufacturing Business Technology

Get today's manufacturing headlines and news - Sign up now!

A recent study from Hewlett-Packard reveals that 70 percent of Internet of Things (IoT) devices — including sensors and connected infrastructure — are seriously vulnerable to attack. The Internet of Things State of the Union Study from HP's Fortify on Demand division came about after hearing a lot about IoT, but saw nothing that focused on the complete picture of IoT security.

© 2010 Mentor Graphics Corp.
www.mentor.com

IoT Topology Coming into Focus and Edge Nodes are wide-open to attacks

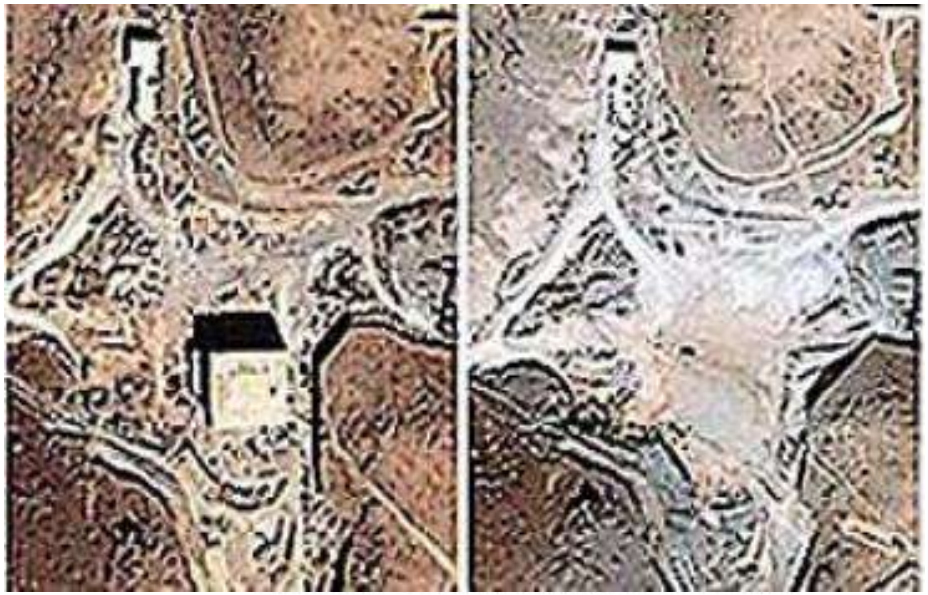


© 2010 Mentor Graphics Corp.
www.mentor.com

Syrian Radar Case

“September 2007, Israeli jets bombed a suspected nuclear installation in northeastern Syria. Among the many mysteries still surrounding that strike was the failure of Syrian radar, supposedly state of the art, to warn the Syrian military of the incoming assault. It wasn’t long before military and technology bloggers concluded that this was an incident of electronic warfare and not just any kind. Post after post speculated that the commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden “backdoor” inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips’ function and temporarily blocked the radar”

Source : IEEE spectrum, 2007



Stuxnet Virus Likely Delivered by "Infected" USB Flash Drive

"Stuxnet, a 500-kilobyte computer worm that infected the software of at least 14 industrial sites in Iran"

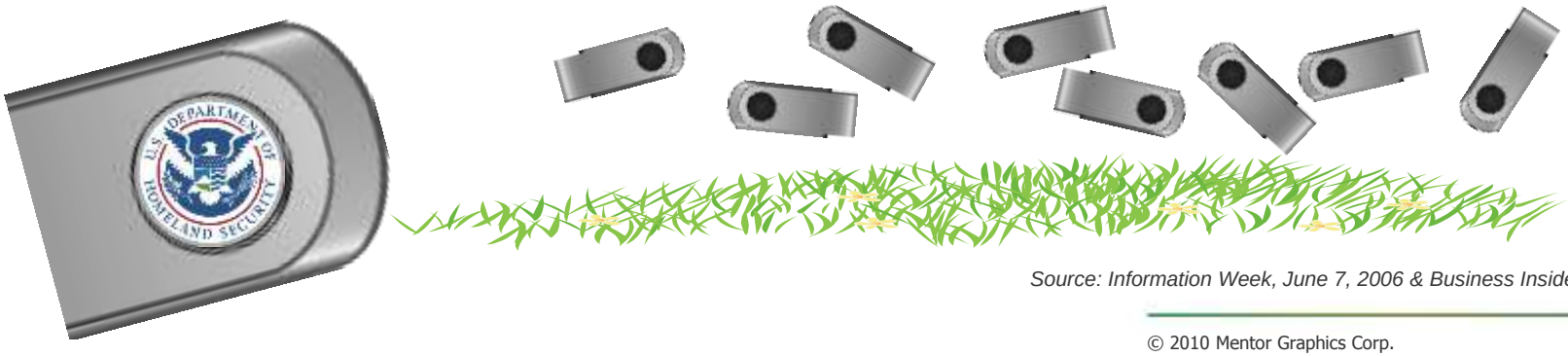
IEEE, "The Real Story of Stuxnet", February 26, 2013

© 2010 Mentor Graphics Corp.
www.mentor.com

The "Candy Drop"

- Security firm hired to test data security of credit union
  - — Scattered 20 infected USB flash drives in parking lot, picnic and smoking areas
  - — 15 were plugged into company computers
  - — Passwords, logins and other information were compromised

- U.S. Department of Homeland Security Test
  - — USB flash drives scattered in government parking lots
  - — 60% of those found were plugged into networked computers
  - — 90% of those with official logos were plugged in



Source: Information Week, June 7, 2006 & Business Insider, July 24th 2013

© 2010 Mentor Graphics Corp.
www.mentor.com

Hardware Attack Types

- 'Side-Channel' Attacks - (SECRET EXTRACTION)

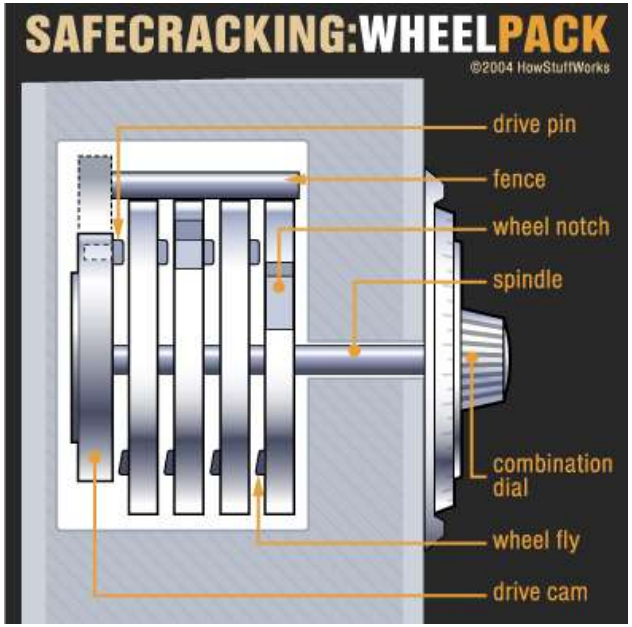
- Counterfeit Chips - (SUPPLY CHAIN VULNERABILITY)

- Malicious Logic inside Chip - (TROJANS)

© 2010 Mentor Graphics Corp.
www.mentor.com

Side-Channel Attacks

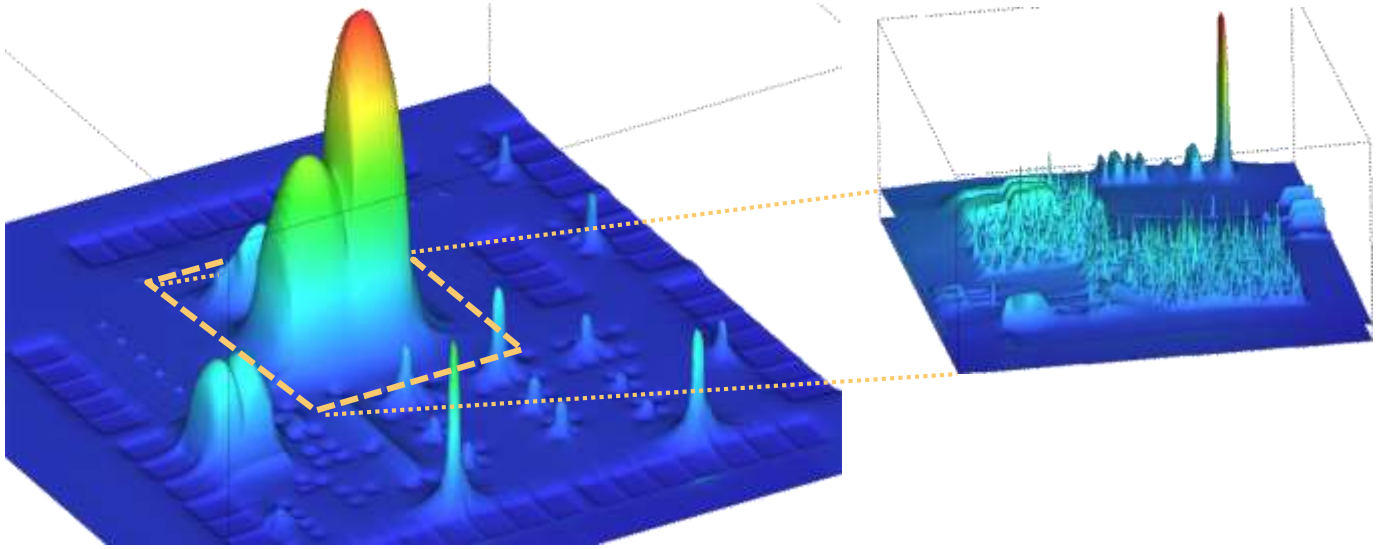
To crack safes, it's essential to know how they work



© 2010 Mentor Graphics Corp. Company Confidential
www.mentor.com

DPA: Differential Power Analysis

- Thermal images can help in locating cryptographic circuits
  - Attempts to enter candidate keys should exercise crypto
  - This results in visible power dissipation



- Subsequently, different power dissipation patterns can be observed based on correct or incorrect key entry attempts
- Keys can then be inferred

© 2010 Mentor Graphics Corp.
www.mentor.com

Set-Top Boxes Side-Channel Attacks
Delaying Time-to-Crack Is Measure of Success

STRONG Digital HD TV Receiver PVR Recorder Set Top Box Decoder Media Player

From Australia

$63.41

0 bids

H.264/ MPEG-4 HD PV
TV Receiver S
FTA Media P

From China

Top Rated Plus

Was
Buy

13 Watchers

Wintal STB14HD hd
set top box w/ Multimedia USB Playback/Player

From Australia

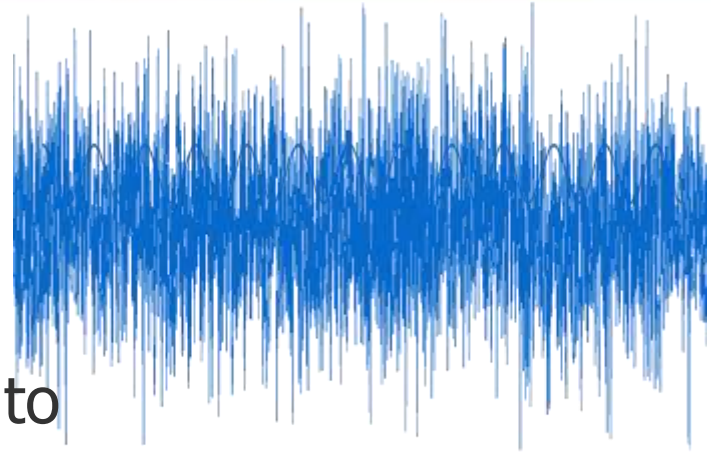
Buy It Now

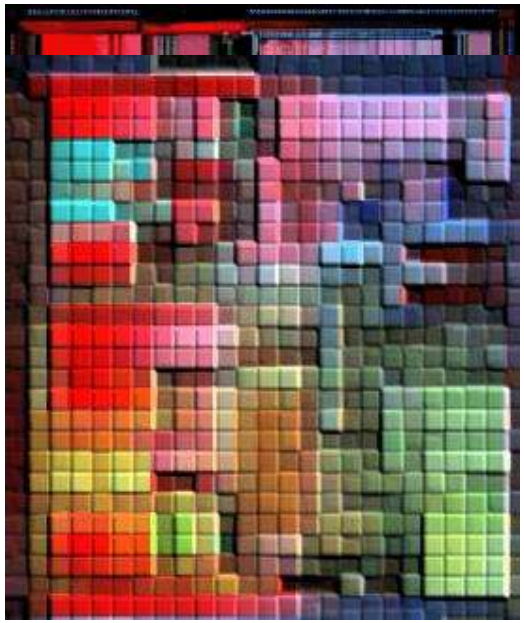
34 Watchers

© 2010 Mentor Graphics Corp.
www.mentor.com

Countermeasures for Side-Channel Attacks

- Decrease **signal-to-noise ratio**
- Incorporate **randomness** into cryptography
- **Pre-charge** registers and buses to mitigate power-leakage signatures
- Use **fixed-time algorithms** to reduce data-related timing signatures
- **Camouflaging** structures from reverse engineering



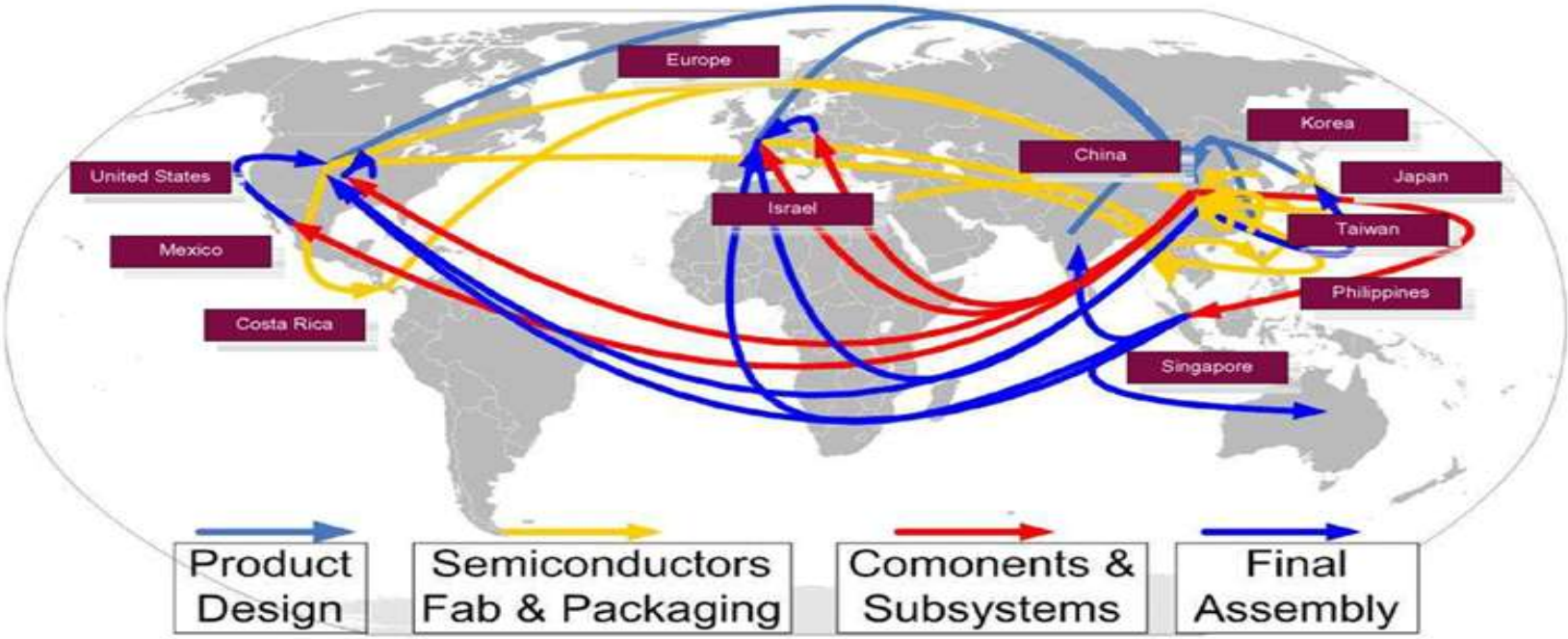


© 2010 Mentor Graphics Corp.
www.mentor.com

Lifecycle for a Single IC

JSF (Joint Strike Fighter) Case Study

Global nature of supply chain makes chain-of-custody unworkable



Component changes hands 15 times before final install

Source: IDC Manufacturing Insights & Booz Allen analysis

© 2010 Mentor Graphics Corp.
www.mentor.com

Counterfeit and recycled chips

More than a Backyard Industry!

Millions of Scrap Boards

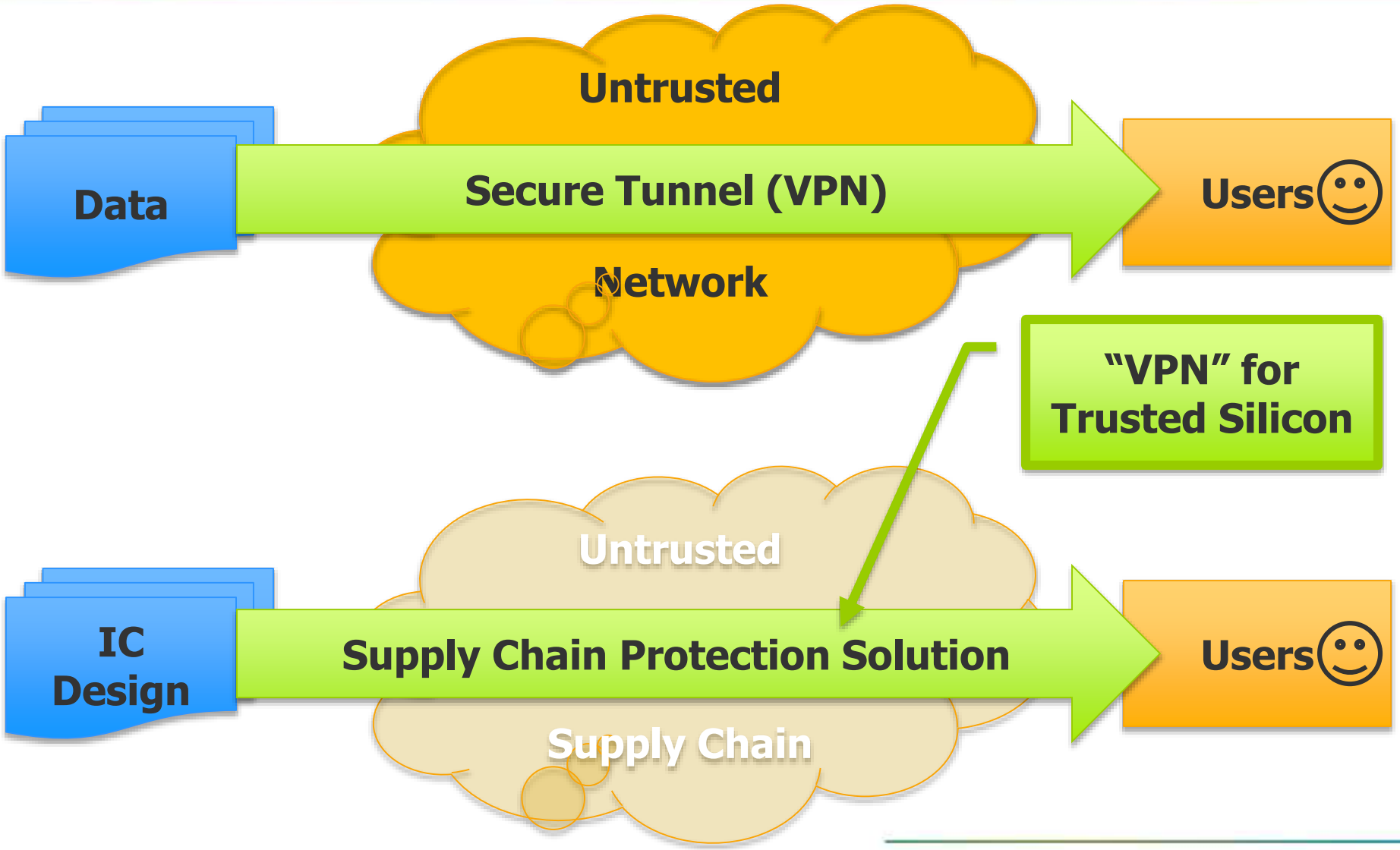
Component Removal

Sorted by size, similarity and lead count

Re-processed

© 2010 Mentor Graphics Corp.
www.mentor.com

Creating Secure Silicon in an Untrusted Environment — VPN for Silicon



© 2010 Mentor Graphics Corp.
www.mentor.com

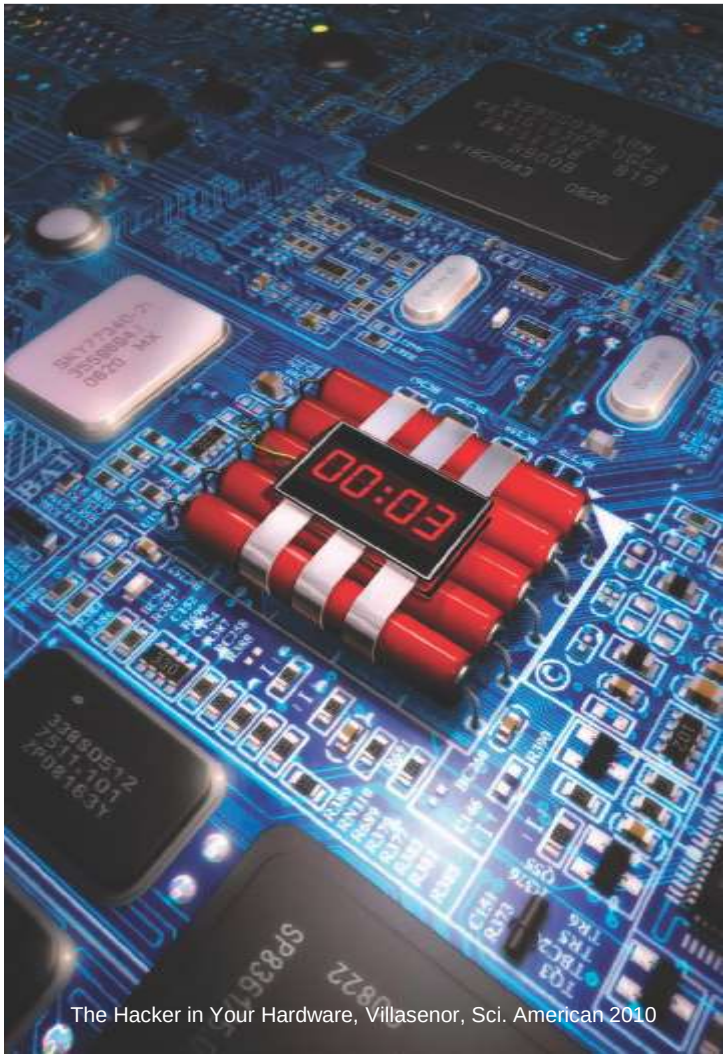
Possible Activation Solution: Logic Encryption

- Add gates throughout a design connected to a key
  - Generate a 256 bit encryption key
  - Inject 256 gates throughout the design
    - Gates inserted are pre-determined by the bit in the key

- Manufacturing
  - Use potentially un-trustworthy fab
  - Place a 256 bit key in tamper-proof location in the design after fabrication
- Global key vs. unique key (PUFs)

© 2010 Mentor Graphics Corp.
www.mentor.com

What Are Hardware Trojans?

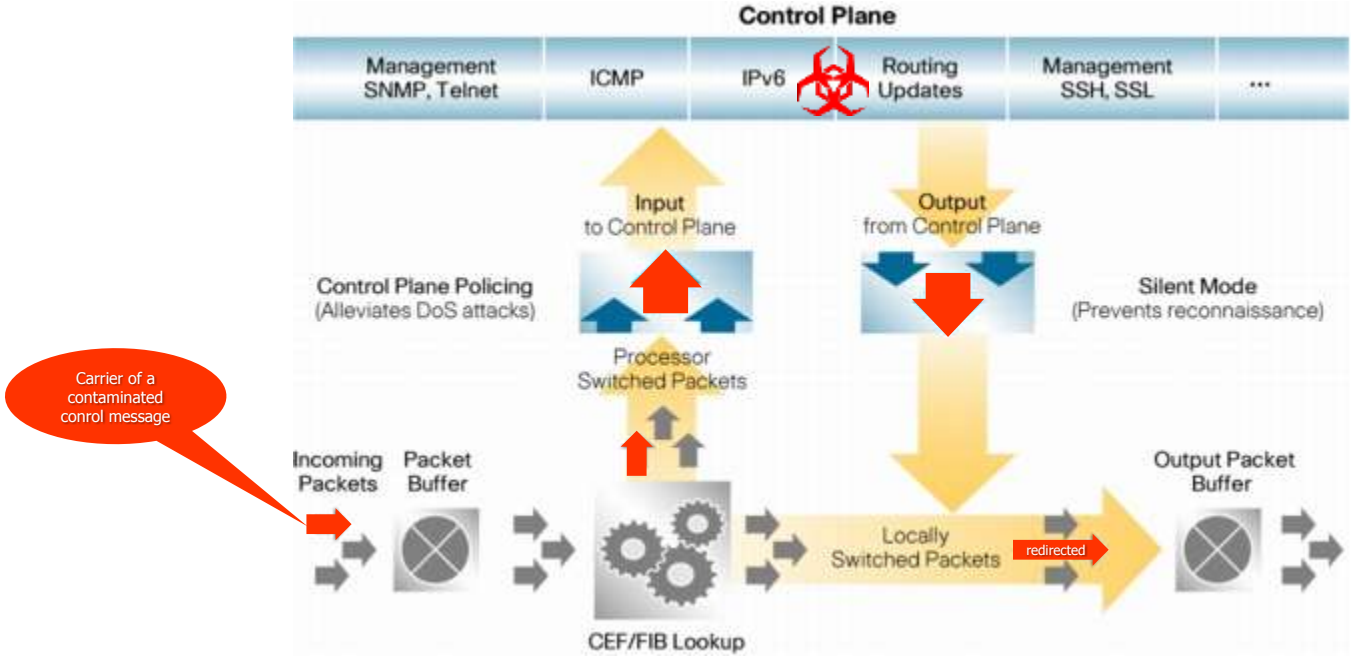


The Hacker in Your Hardware, Villasenor, Sci. American 2010

- Rogue hardware injected into the design/chip
  - Untrusted cores (design phase)
  - Untrusted fab (fab phase)
  - Triggered subsequently
    - Special date/time
    - Receipt of special signal
- Payload = Malicious Action
- Types of Attacks
  - Kill switch: Breaking the system
  - Backdoor: Gaining access to the system. e.g., sending confidential data off-chip

© 2010 Mentor Graphics Corp.
www.mentor.com

Threat Example



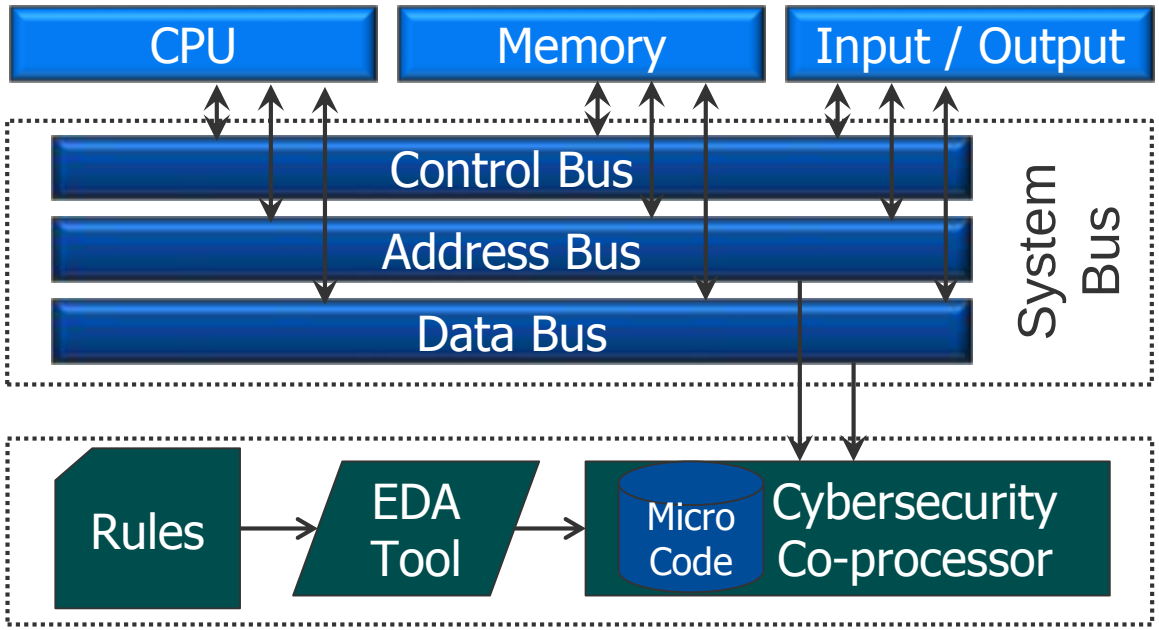
- Unpublished control message travels around the internet and is unrecognized and ignore by most routers
- When a router containing a hardware Trojan in the control plane sees such message, it takes action to re-direct data

Source: Cisco web site

© 2010 Mentor Graphics Corp.
www.mentor.com

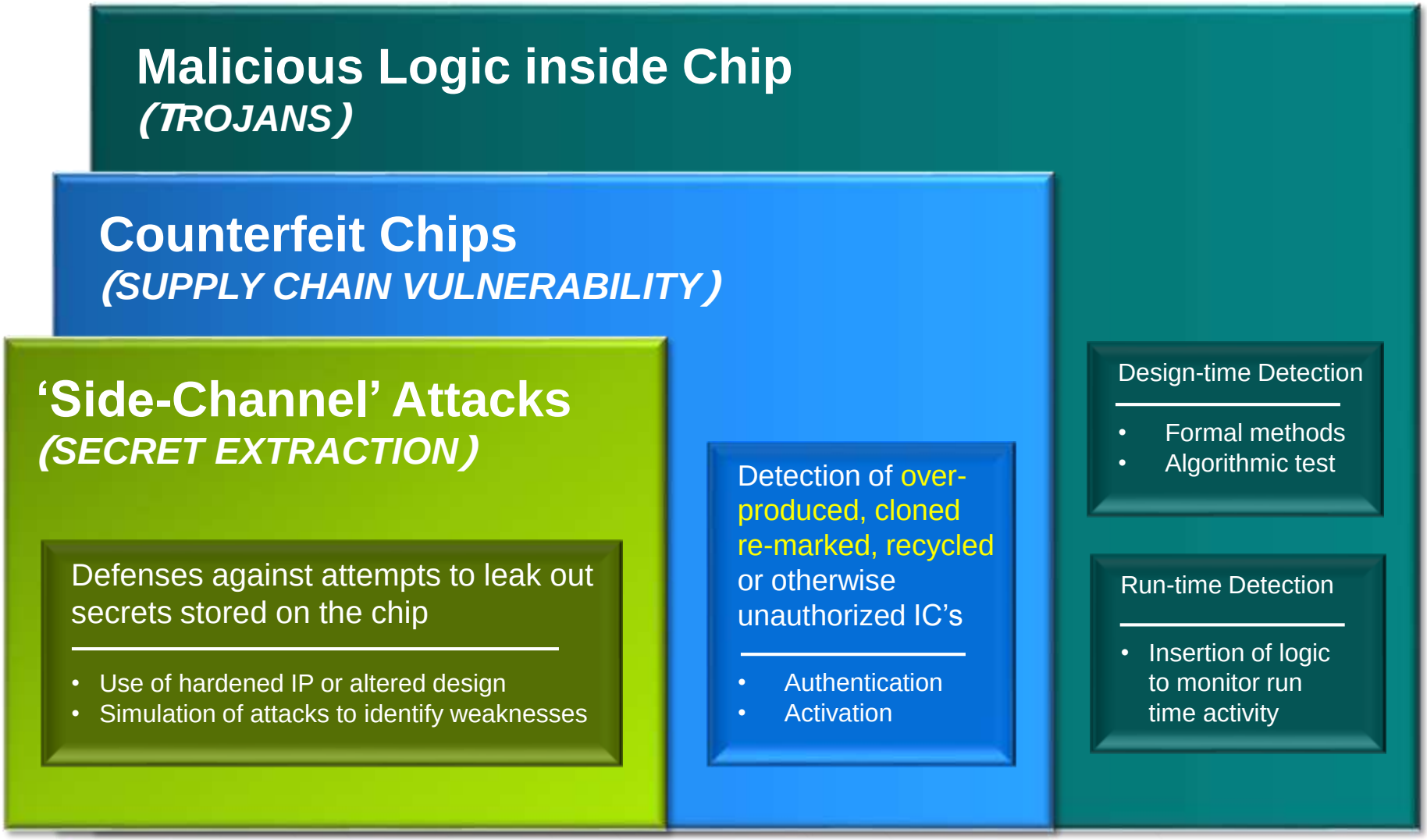
Run-time Detection via Co-processor

- Co-processor for run-time Trojan detection
  - Include co-processor in the design as an IP block
- Issues targeted
  - Peripherals with hidden functionality
  - Prevention of undeclared communications



© 2010 Mentor Graphics Corp.
www.mentor.com

Countermeasures



© 2010 Mentor Graphics Corp.
www.mentor.com

Countermeasures Don’t Need to Be Perfect

© 2010 Mentor Graphics Corp.
www.mentor.com

Summary

System design and integration take new forms with evolution and pervasiveness of cloud, sensors, social networking, gaming and mobility enabled by rapidly advancing silicon

A huge opportunity exists to combine all these technologies in intelligent ways to create high-value, domain-specific user experiences

Edge node security needs to be considered up-front

© 2010 Mentor Graphics Corp.
www.mentor.com

www.mentor.com