

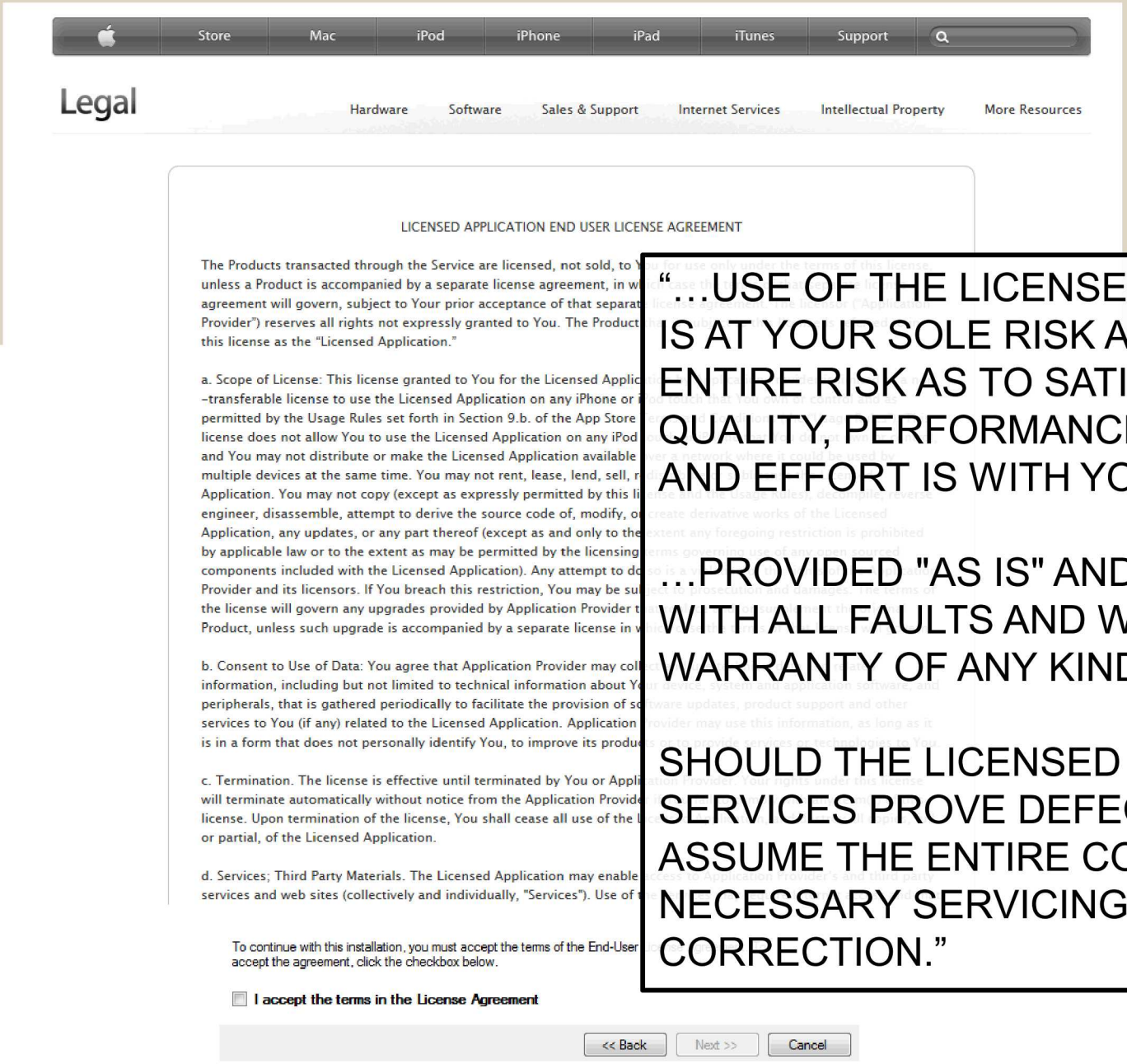
Cyber Security Update for Economic Forum

Mike Vahle

CIO - Sandia National Laboratories

February 24th, 2015

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.



"…USE OF THE LICENSED APPLICATION IS AT YOUR SOLE RISK AND THAT THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT IS WITH YOU.

…PROVIDED "AS IS" AND "AS AVAILABLE", WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND…

SHOULD THE LICENSED APPLICATION OR SERVICES PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION."

About Phishing

• “Phishing” is the practice of using electronic communication to manipulate a target into doing something counter to the target’s interests.

Maintenance Issues

Things are not always as they appear

Example Email -Phishing

Greetings from Amazom.com,

We wanted to notify you that an Amazom.com Gift Card was sent to you on 9 Dec 2013 16:04:40 GMT.

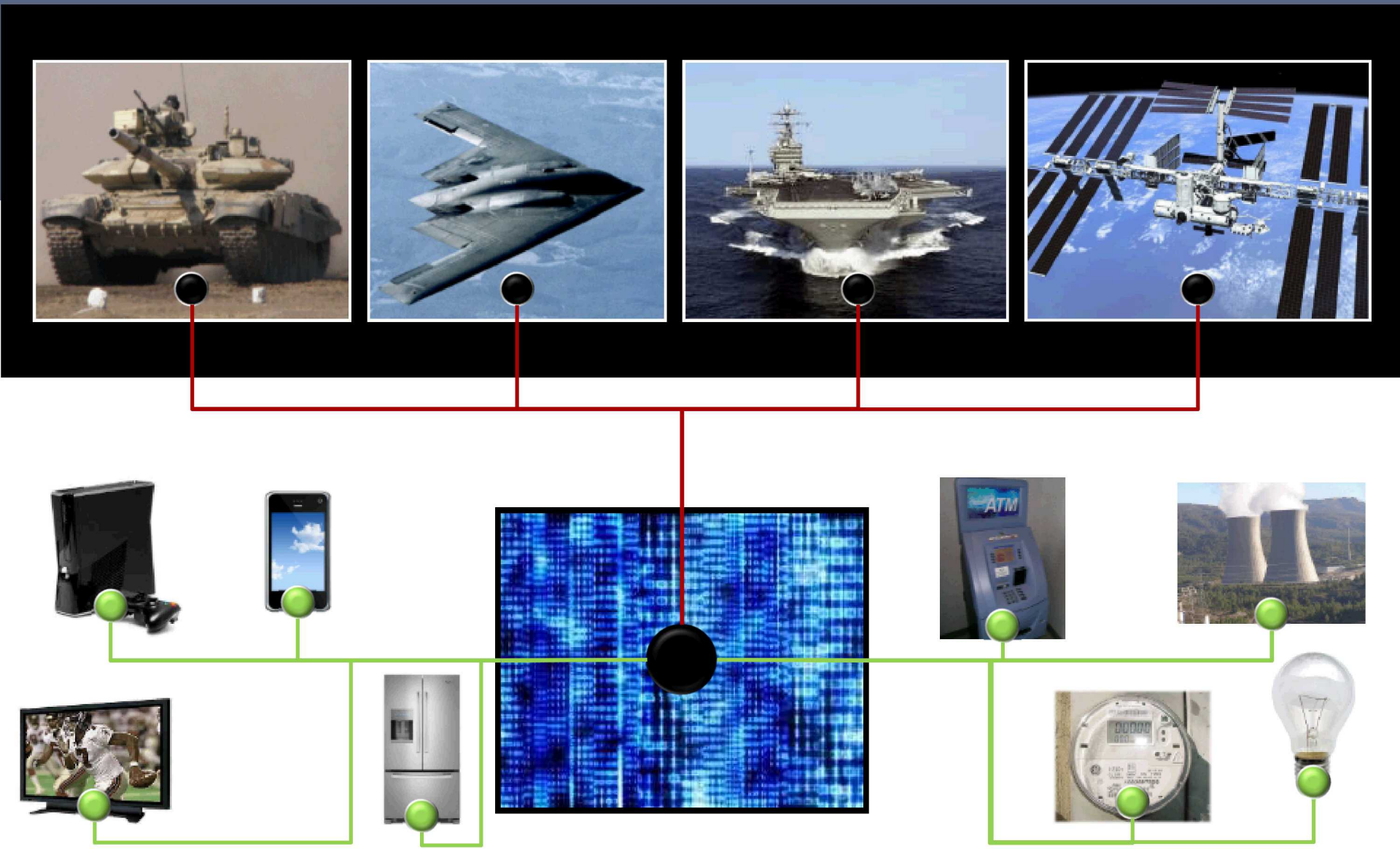
Details:

Order # 314-2520202-8371419 from 9 Dec 2013 10:49:24 GMT
Sent to:
Message: Happy Early Holidays!

Click here to redeem your gift card.

Please note: This e-mail was sent from a notification-only address that cannot accept incoming e-mail. Please do not reply to this message.

The “Internet of Things” is the 5th domain of conflict



Recent Cyber Events Impacting Business

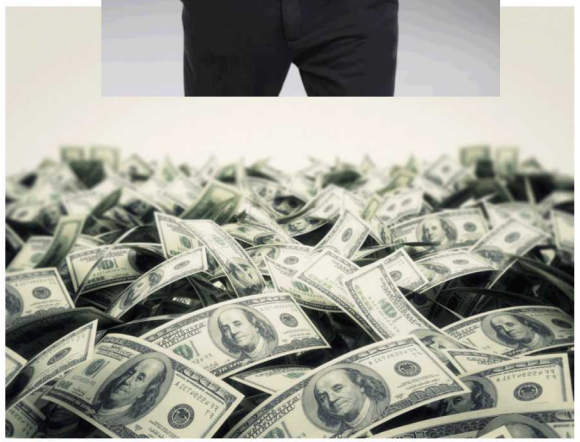
TARGET

THE HOME DEPOT®

Cyber Theft of Intellectual Property

- The Center for Strategic and International Studies (CSIS) produced a study in June 2014 which estimates that cybercrime costs business approximately $445 billion annually worldwide. The cost is about 200,000 U.S. jobs annually.

- Cybercrime is a tax on innovation. In 2013, CSIS researchers found that the United States notified 3,000 companies that they had been hacked. CSIS estimated that the United States lost about $100 billion.



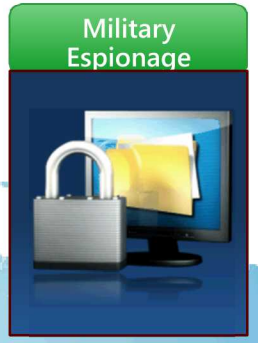
Zero-Day Threat

Advanced Persistent Threat (APT)

Today's Threat Environment

- Threats are real; even in Albuquerque. Example: Attack on Journal Web Site – January 2015

Today's Threat Environment



Sony PlayStation Network Shut Down 'Indefinitely' Following Attack 5/11

Home Depot is hacked – initial estimates exceed Target loss 8/14

Mandiant releases APT1 – calls out China for cyber espionage 2/13

Russian PM's twitter account is hacked 8/14

Ebay Hacked – 1000s of Accounts Deleted, Auctions Vanished, Millions Lost 9/14

A win for the good guys… FBI/Microsoft team to shut down $500M botnet 6/14

Target's point of sale system yields financial data of 40M 12/13

Hacked ATMs net cyber criminals $45M 5/13

RSA security firm hit by 'sophisticated' hackers 3/11

PII of 100,000+ is stolen from DOE 7/13

HeartBleed – secure web browsing compromised, impacts 75% of internet 4/14

OPM is hacked – security clearance info taken 7/14

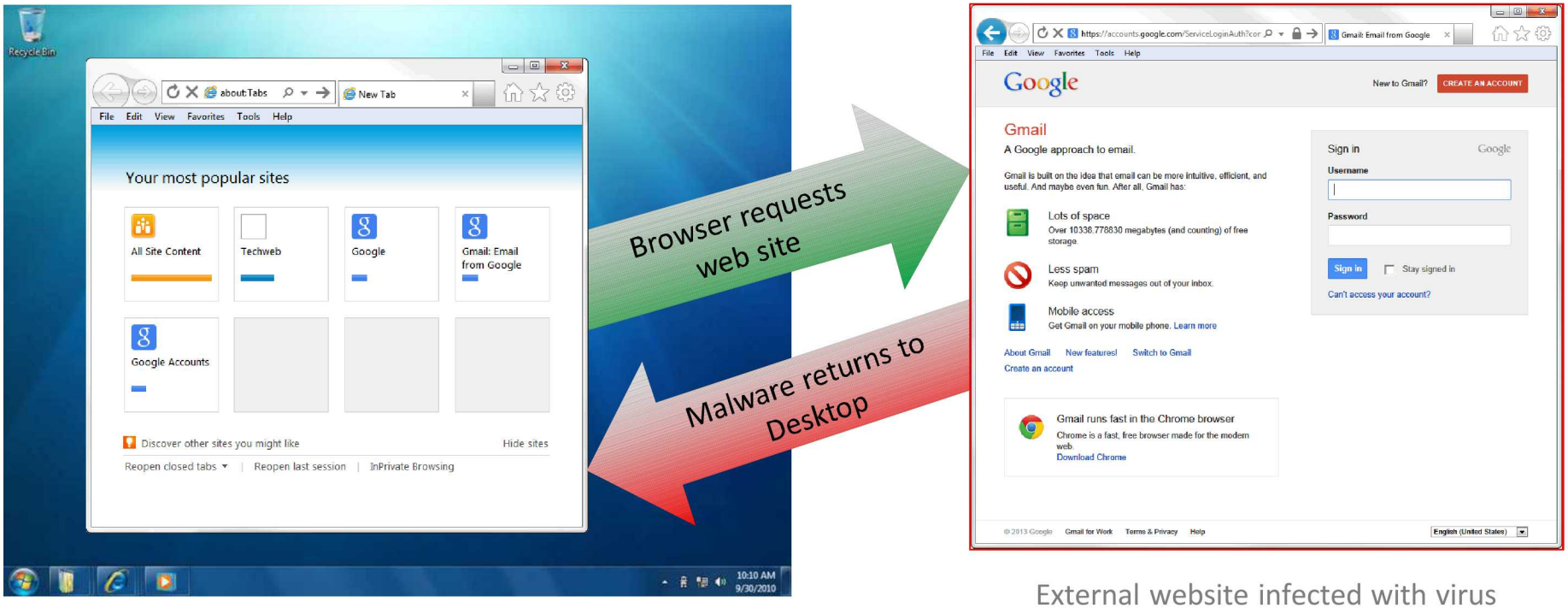
Apple iCloud gives up personal Information and photos 8/14

Typical Desktop Configuration

How it works

Desktop Computer - Trusted

Outside Web Browser - Unsecure

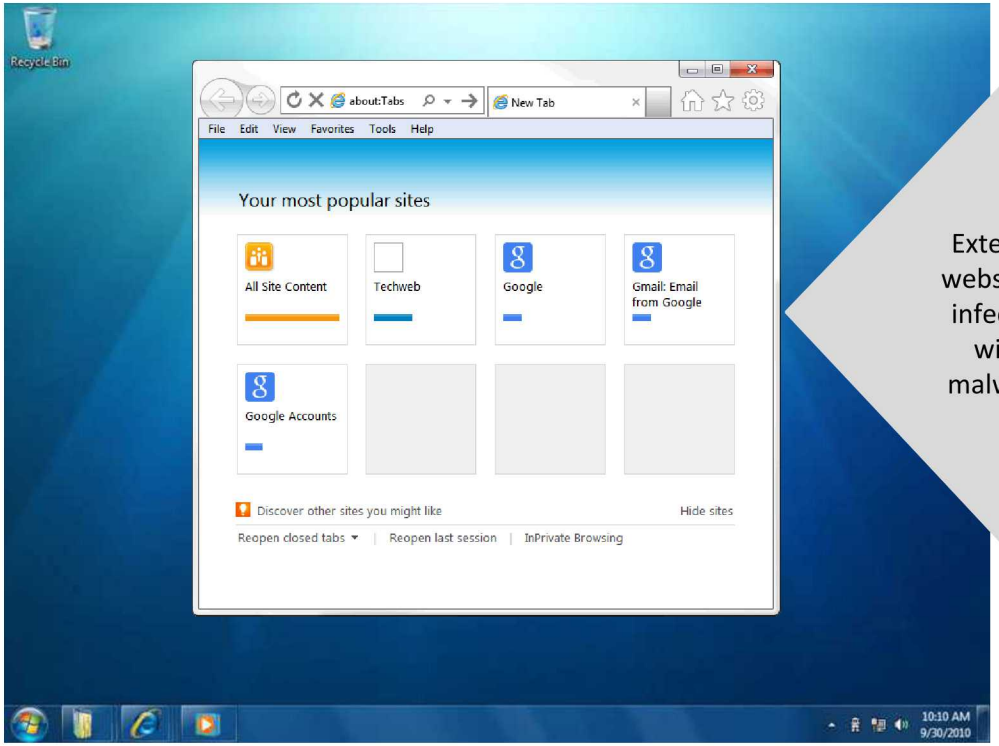


External website infected with virus

- Huge attack surface
- We can only protect against known attack vectors
- Virus is downloaded onto the trusted computer

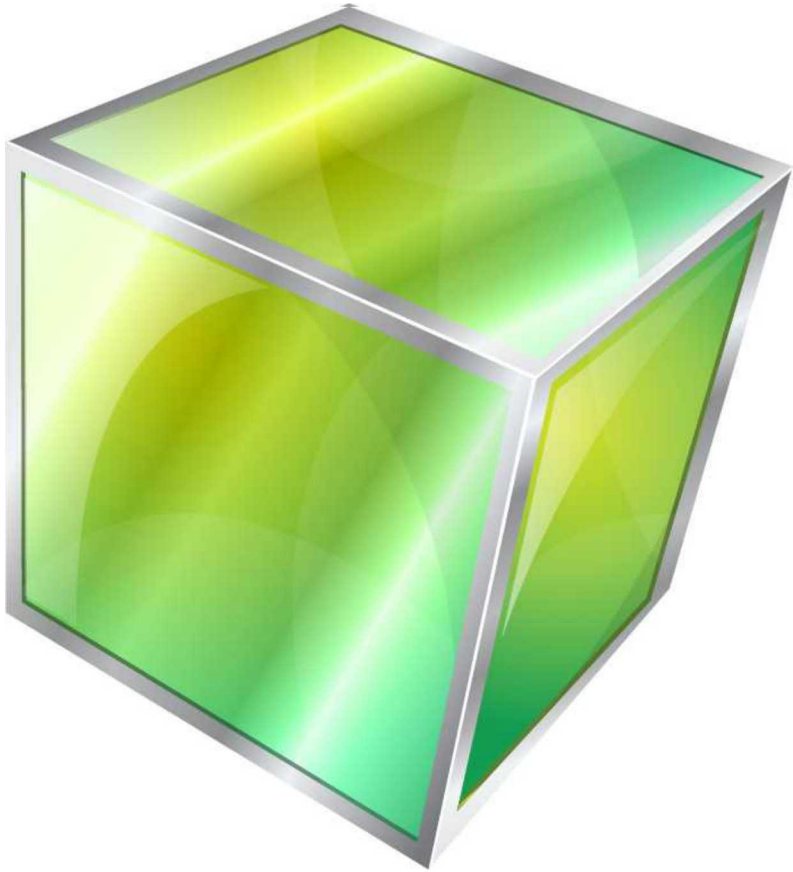
Micro-Virtualization as a Security Solution

Desktop Computer - Trusted



External website is infected with malware

Outside Web Browser - Untrusted



Future: Vehicle To Vehicle (V2V)

Backup Slides