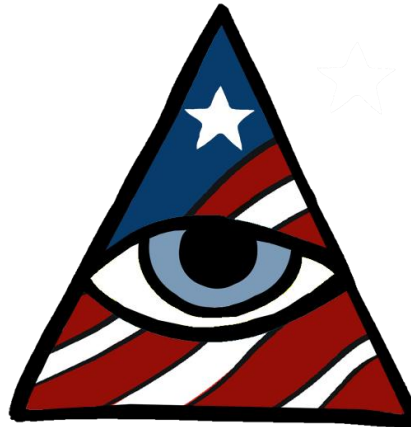


# *Android Security: a Deep Dive*

David Gewirtz, Director

U.S. Strategic Perspective Institute



U.S. STRATEGIC PERSPECTIVE INSTITUTE  
*Helping to solve some of America's toughest problems*

# Special thanks

This event would not have been possible without these individuals and groups:

## **INCOSE Space Coast & ITEA-CF**

- Elizabeth Hood
- Sam Harbaugh
- David Grow
- Joe Vandeville
- INCOSE Orlando
- UCF Bus. Incubation Program
- First Methodist Church, Melbourne, FL

## **Experts and contributors**

- Internet Press Guild experts
  - Tom Henderson
  - Jason Perlow
  - Wayne Rash
  - Karen Heyman
  - Daniel Grotta
- T-Mobile and Dell
- United States Secret Service



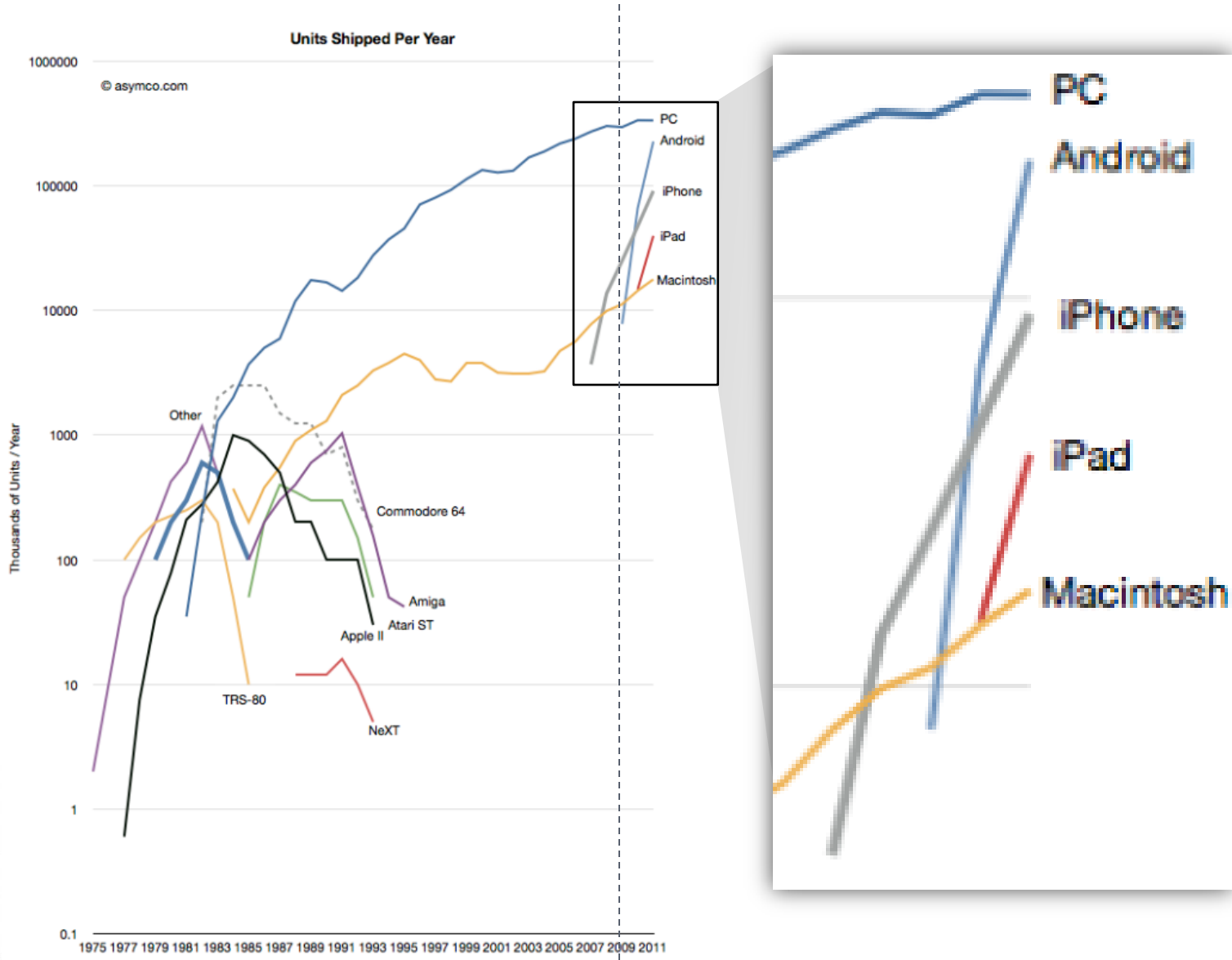
# *What you're going to learn*

- Why Android matters so much
- Understanding the security threat
- Ten tips for staying safe
- A look at Android's future



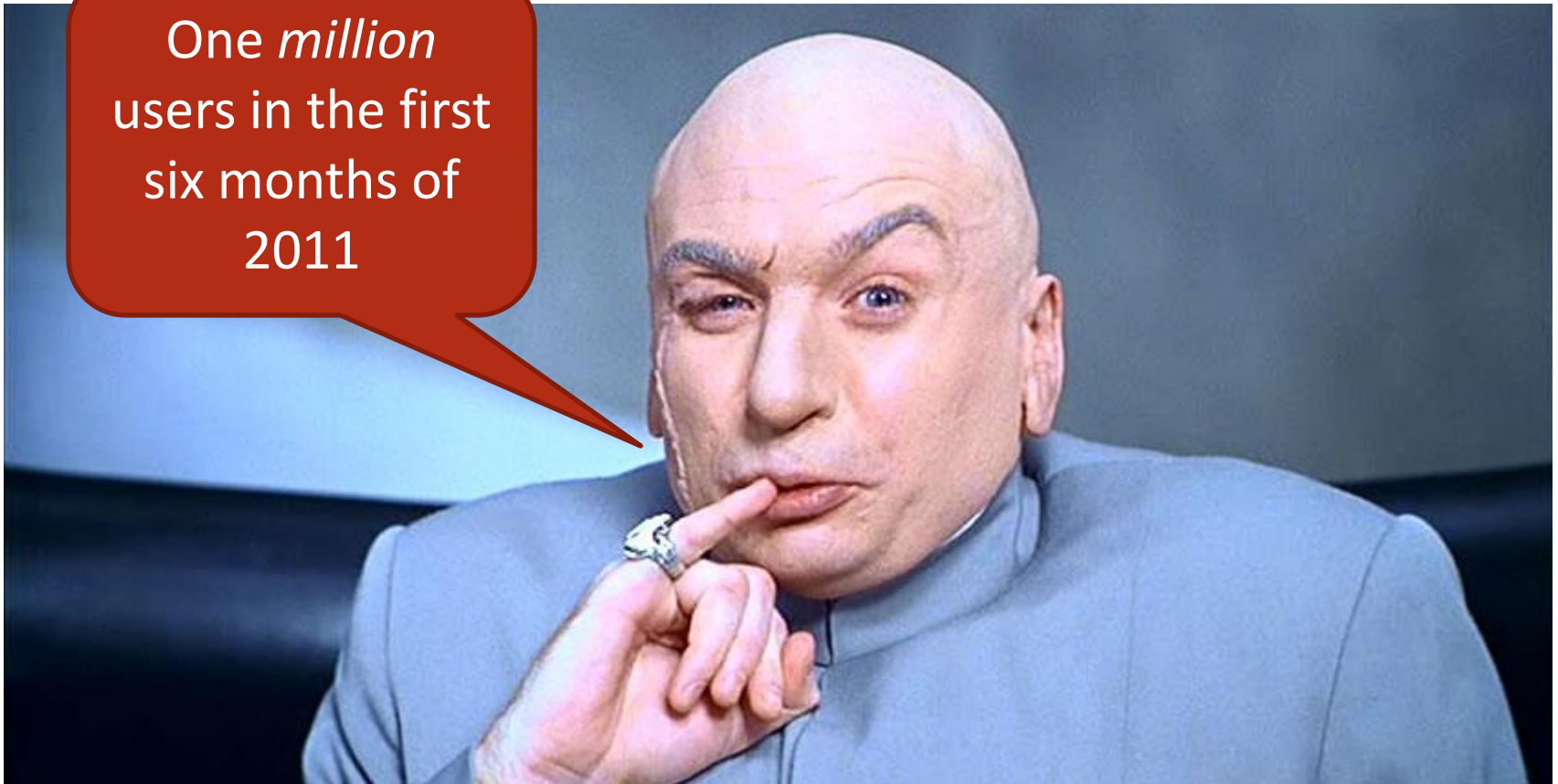
# Why Android matters so much

It took  
PCs  
30 years  
to reach  
Android's  
numbers...  
and that  
took just 2  
years



# *Android users affected by malware*

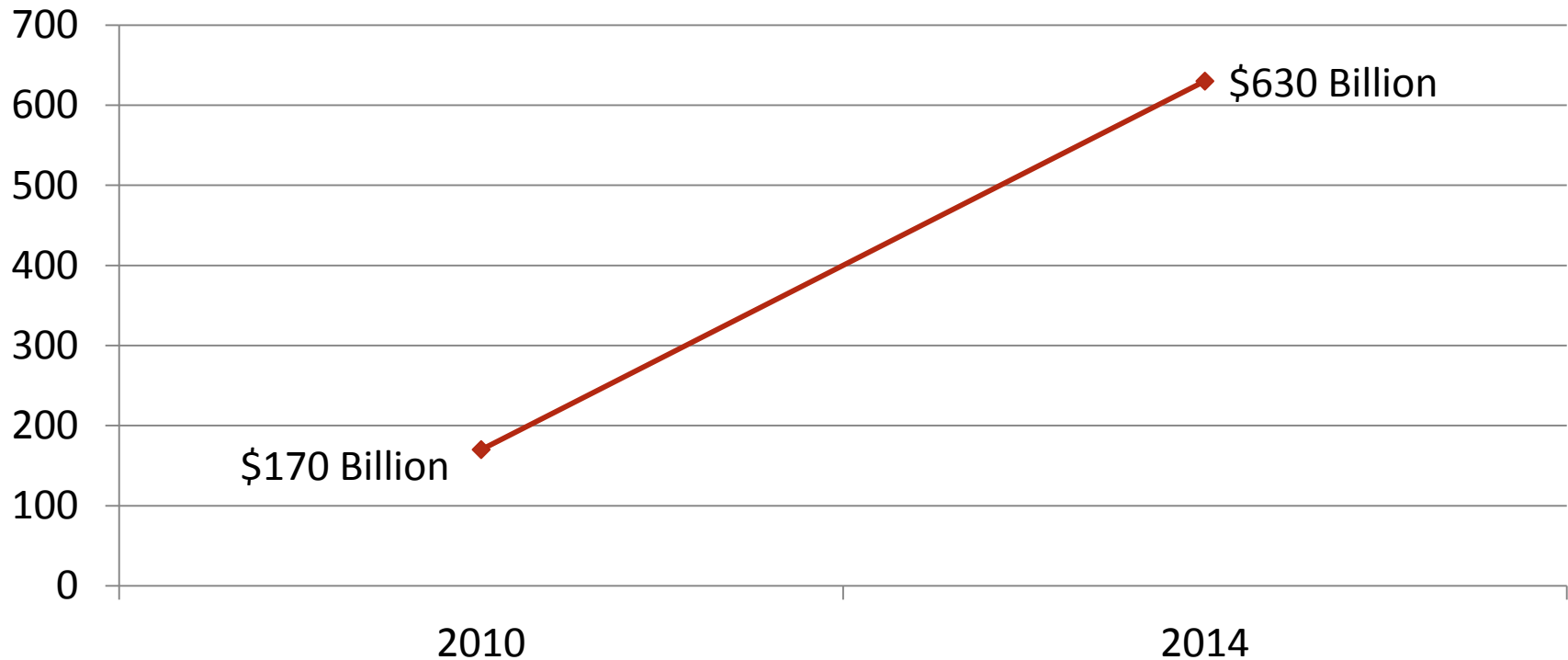
One *million*  
users in the first  
six months of  
2011



Source: Lookout 2011 Mobile Threat Report  
Image courtesy *Austin Powers*

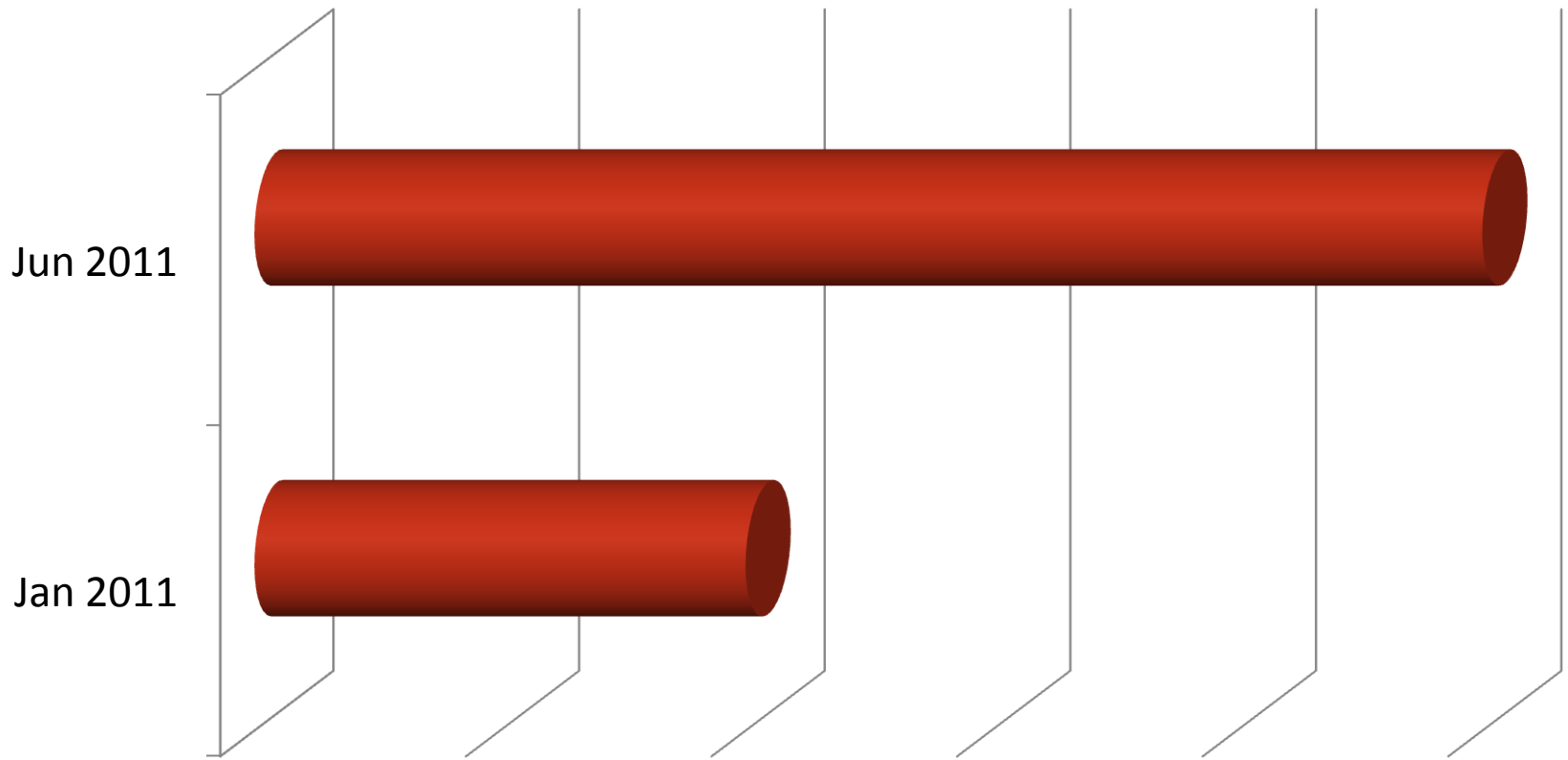
# Why smartphones are a target

## Value of mobile payment transactions



Source: Lookout 2011 Mobile Threat Report

# *Likelihood of encountering malware*



An increase of 250% in six months!



Source: Lookout 2011 Mobile Threat Report

# *Motives for cyberattack*

- Break something
  - » DDoS, basic vandalism
- Co-opt something
  - » Take it over, zombie bots
- Steal something: secrets or money
- Cause something to give wrong information
- Change the expected behavior of a system
- Just for the lulz

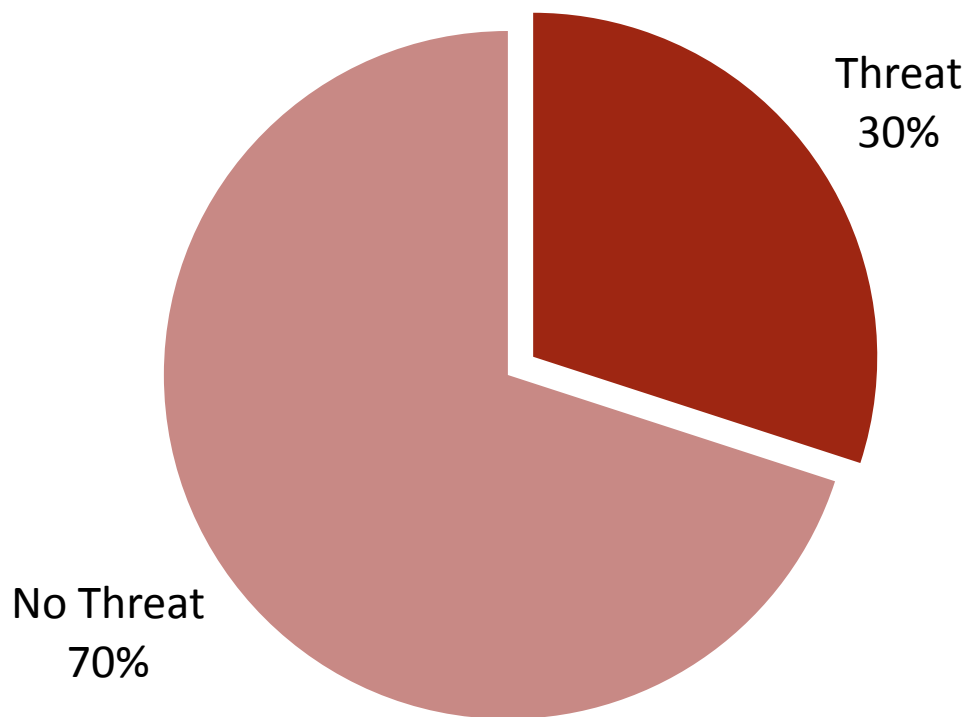


# *What the bad guys can do to you*

- They could install a 'bot' on your phone
- They could log your email and texts
- They could steal your bank and credit card login information
- They could steal your medical identity
- They could turn your phone into a P2P network node
- They could make your phone crash
- They could use you to attack or do bad things to your friends and family... and society



# *Web threats on your Android device*



One in three users have experienced a Web-based threat in 2011



Source: Lookout 2011 Mobile Threat Report

# *Smartphone bugging software*

- Can be ordered and downloaded online, like most other software programs
- Can be installed from a smartphone web browser
- Once installed, completely hidden from apps and tasks
- Range in price from \$39 to \$349 depending on how many features wanted
- Not just for Android
  - » BlackBerry bugging goes back at least to 2008
  - » iPhone requires jail-breaking to run bugging software



# *Bugging capabilities*

- Remote environment listening
  - » Call the target phone and turn the mic into a listening device
- Remote call listening
  - » Specify a list of numbers you're interested in
  - » Get a text message when one of those numbers is called or calls
  - » Call the target and listen in to the conversation
- Can also get recordings and review later

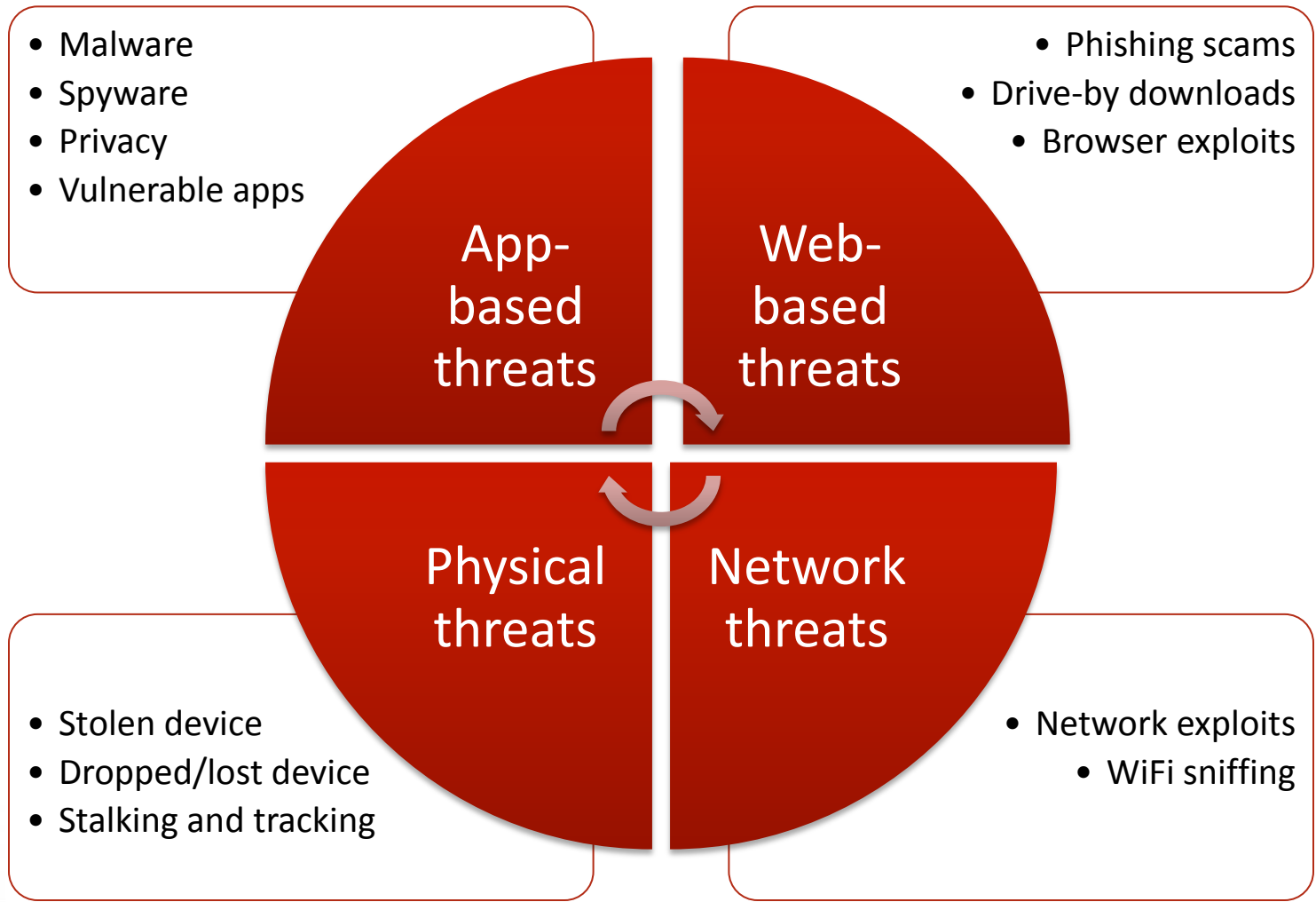


# *More bugging capabilities*

- Spy or stalker can send a text message to the phone and remotely control all capabilities
- Notify spy when SIM card or phone number is changed, with updated information
- Spy gets copies of all emails and text messages sent to or received by the phone
- Track location with GPS
  - » Like iPhone Find-my-Friend, but without permission



# Types of mobile threat vectors



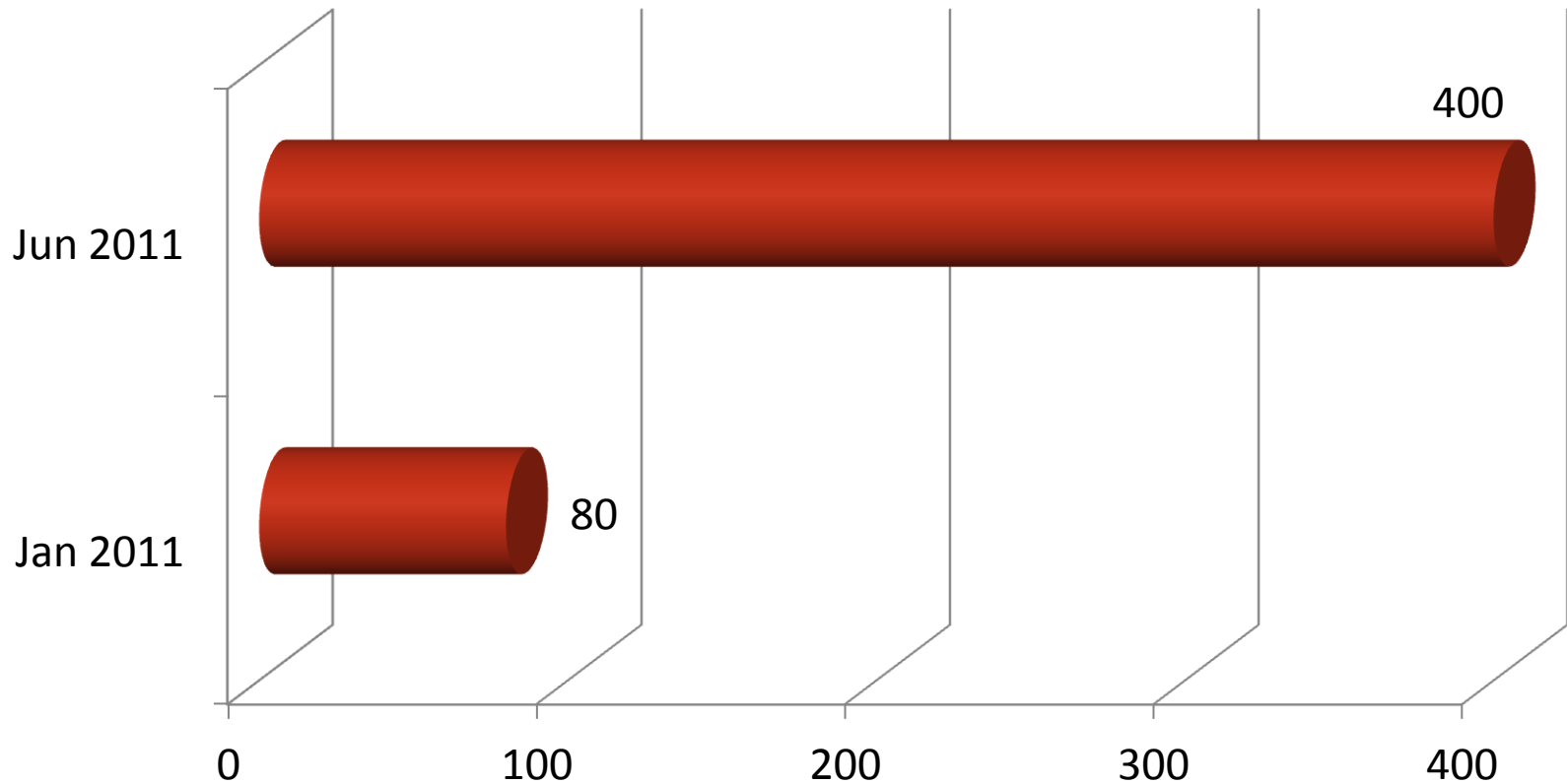
# *How much data can a phone\* hold?*

Type of data	Physical equivalent	How much on the phone?
Document pages	Harry Potter novels	7,000 sets of all seven novels
Document pages	King James Bible	25,000 King James Bibles
Document pages	WikiLeaks cable dump (about 1.6GB)	About 40 times the confidential information Bradley Manning stole from the State Dept.
Photographs (8 megapixel)	Photo album holds about 300 photos	About 300 photo albums worth (lots more for lower-res pix)
Video	DVD holds about 2 hours worth	About 10 full DVD movies worth
1080p HD Video	Blu-ray holds about 2 hours worth	About 3 full Blu-ray movies worth in highest quality video



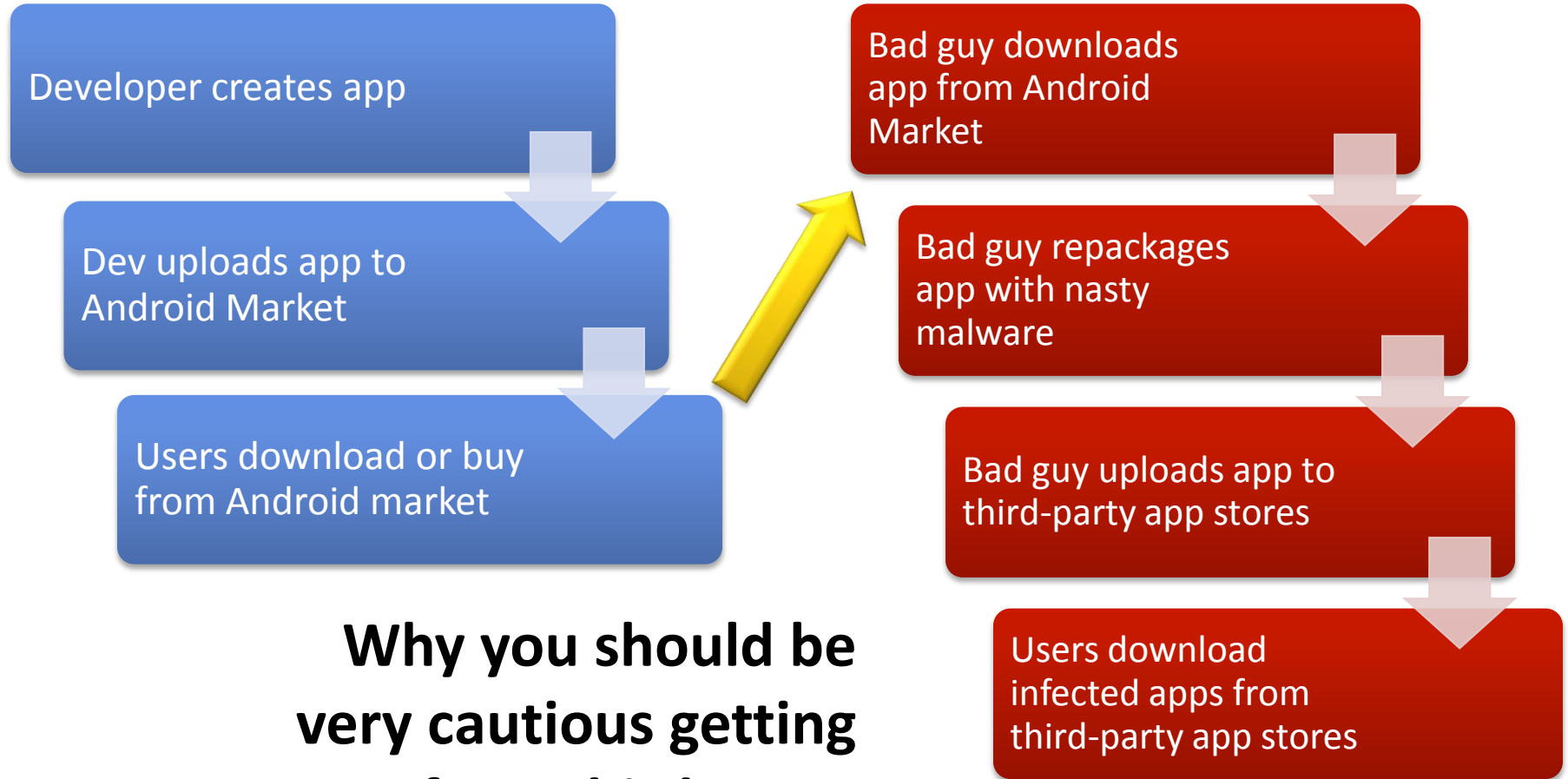
\*Assuming 64GB memory

# *Android apps infected with malware*



Source: Lookout 2011 Mobile Threat Report

# Repackaged apps threat



**Why you should be very cautious getting apps from third-party app stores**



# *How botnets make money*

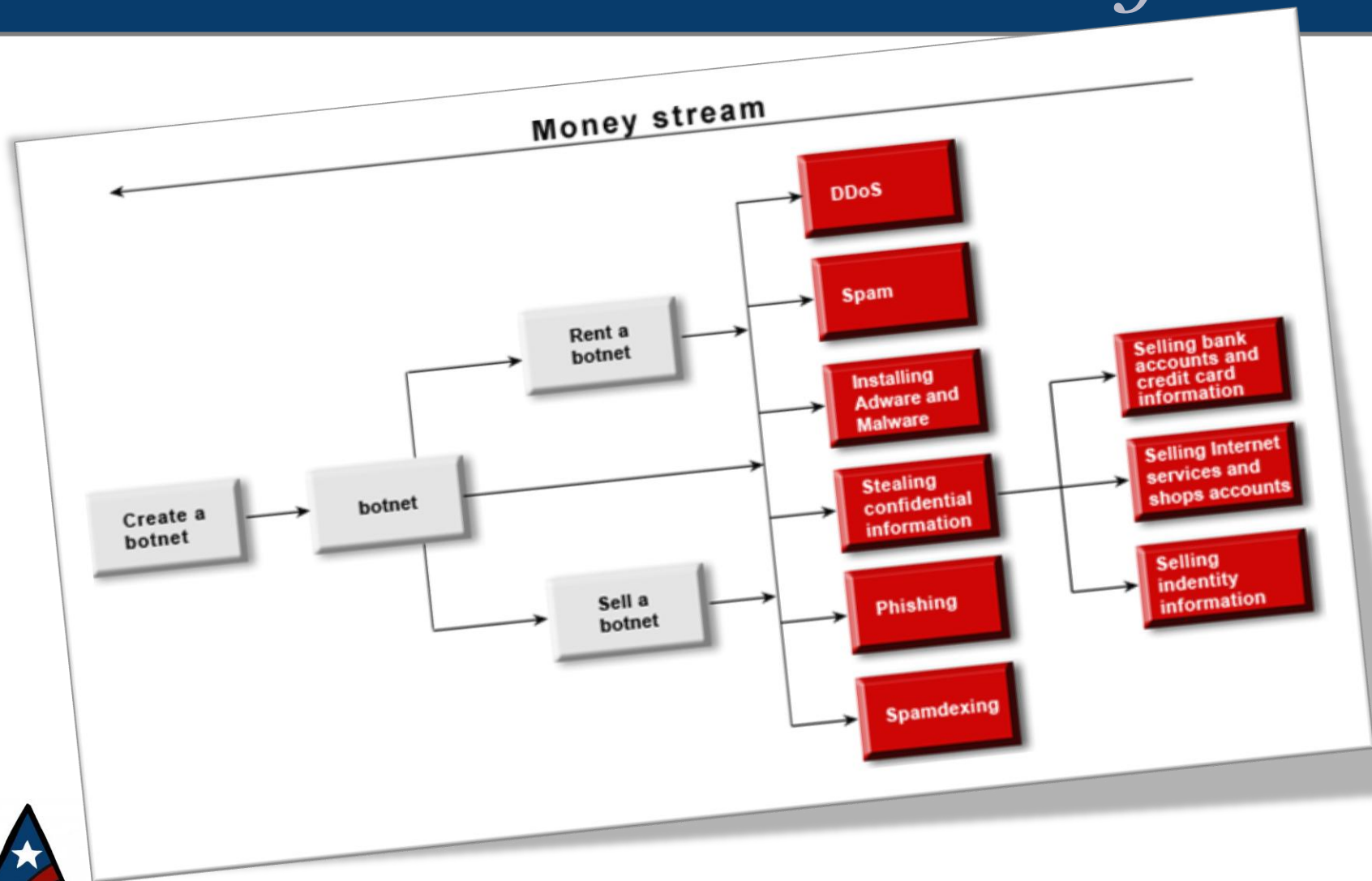
- DDoS attacks
- Theft of confidential information
- Phishing
- Spam
- Search engine spam
- Adware and malware installation
- Click fraud
- Leasing and selling botnets



\$\$\$  
This is a  
billion-  
dollar  
business

Source: SecureList

# Show me the botnet money



# *Categories of malware criminals*

- Carders
  - » Traffic in and exploit stolen financial data
- Hackers / Security Technologists
  - » Perform targeted intrusions for harvesting of data
  - » Develop exploits and exploit toolkits
  - » Decryption services
  - » Anonymity services (proxies, criminal-run VPNs, private messaging systems, etc.)
  - » Provide security engineering and consulting services
- Spammers
- Bot Herders
  - » Build and run botnets, which have a variety of criminal uses



Source: United States Secret Service

# *More types of malware criminals*

- Money Launderers
- Renegade Hosters and Internet Developers
  - » Provide stable platform for criminal business, i.e., criminal sites
  - » “Bulletproof Hosts” for phishing, malware drop sites, etc.
- Malware Developers
  - » Creation/dissemination of specialized crimeware
- Document Forgers
  - » Produce counterfeit drivers’ licenses, passports, checks, etc.
- Information Services
  - » Research services for identity theft
- Specialized Hardware Providers
  - » ATM skimmers, card production equipment, etc.
- Calling Services
  - » Provide fraudulent telephone calls to defeat out-of-band authentication
- Drop Managers
  - » Recruit and manage “drops” or money mules



Source: United States Secret Service

# *Android malware attacks*

## **DroidDream**

- Hit 250K users in 2011
- Botnet node
- Connects to remote server and accepts commands
- At least 80 variations
- Some download updates and other malware

## **GGTracker**

- Uses malvertising to trick users into visiting malicious web site
- Web site looks like Android Market
- Specifically targets US customers
- Charges \$10 to user phone bills
- Later variants distributed on Android market in fake apps



# *Security exploits in the wild*

## **Android**

- DroidDream malware
- Exploits Exploidy and RageAgainstTheCage
- Broke security sandbox
- Gained root access
- Installed apps without user intervention

## **iPhone and iPad**

- JailbreakMe
- Used flaws in Safari to allow users to Jailbreak their devices
- Non-malicious
- Not yet working in iOS 5



# Security model comparison

Category	Android	iPhone and iPad
Security model	Controlled by permissions	All apps are sandboxed
Inter-app communication	Open and free	Minimal
App distribution	Open distribution	Curated by Apple
Level of freedom	High	Minimal unless jailbroken
Security reliance	Relies on user knowledge	Relies on iOS sandbox
Malware incidence	Relatively high and growing	Relatively low
Can be hardened for military use	Yes, quite extensively	Not really



# Security fix pattern

## Android

- Google regularly updates
- Distributes to Android Open Source Project
- Sent to manufacturers who merge with their own updates
- Can take quite a while

## iPhone and iPad

- Apple can push fixes much faster
- Until iOS 5, required users to sync with iTunes
- Less than 50% of iOS users sync to perform updates\*



\*Source: David Chartier, former Macworld editor

# *Mobile impact on IT*

- Mobile is everywhere
- Mobile will be an added load on your data center
- It's also an additional way to manage your data center
- And it will also be an added security problem
- It can reduce your costs at the workstation
- But increase your costs at the server
- Plus, there's all those user-supplied toys you need to learn to manage and account for
- You will need flexible mobile policies and policy training
- Mobile standards change crazy rapidly



# *The two sides of mobile backup*

## **Backing up mobile**

- Safely securing data from mobile devices
- Backup in case of loss or theft
- Distributing mobile information as part of workflow
- Cloud storage options
- Challenges due to mobile device restrictions (i.e., iOS)

## **Getting at your data everywhere**

- Mobile productivity
- Getting at something from your desktop when away
- Disaster recovery
  - Re-spawning an HQ and data center from a collection of mobile hardware
- Redundancy and replication
- Security



# *The mobile security challenge*

## **Inside your walls**

- What can your people bring inside the building?
  - Malware and viruses
  - Spyware and tunnels
  - Exploits and hacks
- What can they take out?
  - What do you care about?
  - What are your trade secrets?
  - What data do you protect?



## **In the field**

- Mobile devices now need to get inside the firewall
- What happens if a device falls into the wrong hands?
- What can be sucked out?

### **Best Practices**

1. Develop secure, encrypted tunnels and VPNs for all remote access
2. Choose/recommend devices based on security availability
3. Install intrusion detection and prevention systems on your network

# *Ten tips for staying safe*

The Online Safety  
FOUNDATION

# TIPS



Special thanks to Tom Henderson, ExtremeLabs

# *Mobile device management*

#1

- Manage policy
- Manage security
- Manage unapproved app detection
- Whitelist/blacklist
- Reduces costs, risks
- Excellent for enterprise



Special thanks to Tom Henderson, ExtremeLabs

# *Types of mobile management*

#2

- Carrier-provided
- Cloud-provided
- Private hosted
- Individual users should use antivirus and antimalware software
- Be careful where you get it or buy it from



Special thanks to Tom Henderson, ExtremeLabs

# *Enable remote wipe and kill*

# #3



- Android has its own Master Clean feature
- Also, ActiveSync-compatible products
- Controlled by Microsoft Exchange
- Enforce many policies easily
- Great for companies using Exchange



Special thanks to Tom Henderson, ExtremeLabs

# *Google Market has no real QA*

# #4



- Do not trust apps from Google Market
- Amazon Market somewhat more trustworthy
- Use extreme caution installing any apps
- Stay away from third-party app stores



Special thanks to Tom Henderson, ExtremeLabs

# *Do NOT root your phone*

#5

- No matter how strong the temptation
- Rooted phones own every piece of data and access
- Rooted apps can do anything at will
- Don't come crying to me



Special thanks to Tom Henderson, ExtremeLabs

# *https:// is your friend*

#6

- Secured Web browsing is as important on your phone as anywhere else
- Use secure Web addresses on your phone as well as your desktop



Special thanks to Tom Henderson, ExtremeLabs

# *Big Brother may be watching*

#7



- Be aware when using sync and cloud features
- Your phone is subject to Patriot Act, HIPPA, and all other gov compliance and secrecy acts
- Treat your phone as if Big Brother is watching
- Then, of course, Google is certainly watching



Special thanks to Tom Henderson, ExtremeLabs

# *Check your logs regularly*

#8

- Make sure your phone is doing its backups
- Make sure it is not doing something unexpected (bots)
- Your phone may not alert you, so you need to check logs



Special thanks to Tom Henderson, ExtremeLabs

# *Consider using two phones*

#9

- One for business and compliance
- One for play and personal use
- Remember that your personal phone will have personal info



Special thanks to Tom Henderson, ExtremeLabs

# *Be aware when you install*

#10

- Be aware of the capabilities you are giving your apps
- Be aware of the privacy you are giving to vendors



Special thanks to Tom Henderson, ExtremeLabs

# Quick intro to virtualization

## What is virtualization?

- The physical computer becomes software
- The OS, the drivers, the UI, everything runs in software
- One physical box can host many virtual machines
- Lots of flexible benefits (alternate OSs, scalability, efficiency)
- More horsepower means more concurrently running VMs

## Virtualization uses

- Virtual hosted desktop
- Development environments
- Secure testing environments
- Legacy continuity
- Server consolidation
- Someday: virtualized phones and tablets



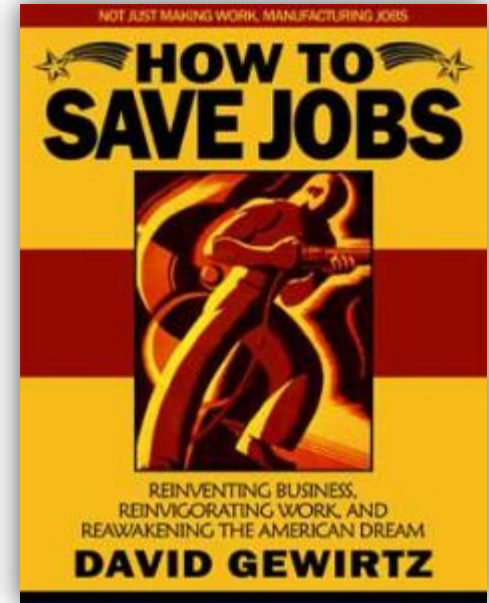
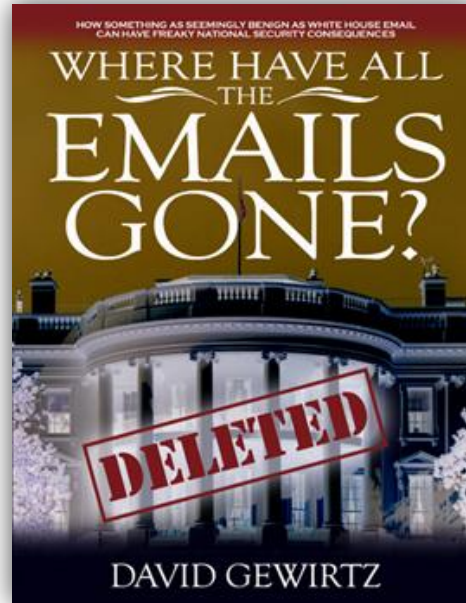
# *The future: virtualizing Android*

- ZDNet's Jason Perlow strongly recommends Android migrate to a virtual machine architecture
- Virtualization makes Android easier to develop by providing a universal system image that is transportable across different device types
- Virtualization allows for isolation of distinct OS containers including all applications and data for different security levels



# Q&A and free resources

- [USSPI.org](http://USSPI.org)
- [David@USSPI.org](mailto:David@USSPI.org)
- [@DavidGewirtz](https://twitter.com/DavidGewirtz)
- [ZD.Net/DGlectures](http://ZD.Net/DGlectures)
- [ZD.Net/govblog](http://ZD.Net/govblog)
- [ZD.Net/DIYblog](http://ZD.Net/DIYblog)
- [ZATZ.com](http://ZATZ.com)



**Free from [USSPI.org/download](http://USSPI.org/download)**

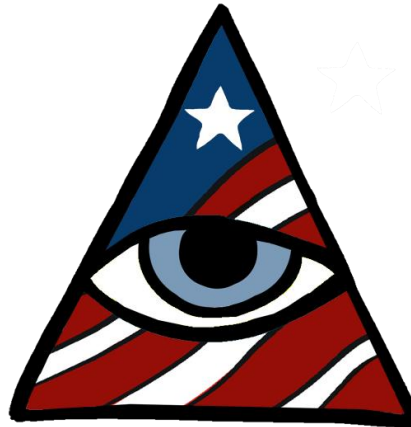


**Plus fascinating video interviews at  
[YouTube.com/DavidGewirtzTV](http://YouTube.com/DavidGewirtzTV)**

# *Android Security: a Deep Dive*

David Gewirtz, Director

U.S. Strategic Perspective Institute



U.S. STRATEGIC PERSPECTIVE INSTITUTE  
*Helping to solve some of America's toughest problems*