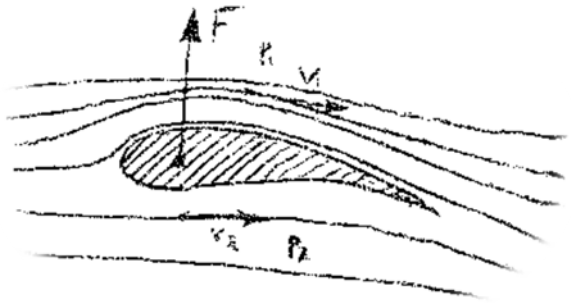
In(sta)Security: Managing the BYOD Risk

Davi Ottenheimer

flyingpenguin

flyingpenguin
the poetry of information security



Davi Ottenheimer

- 18th year InfoSec
- ISACA Platinum Level (‘97)
- Co-author

Securing the Virtual Environment: How to Defend the Enterprise Against Attack (Wiley, 2012)

Agenda

- Bring Your Own…
- Managing Risk
- Device

BRING YOUR OWN…

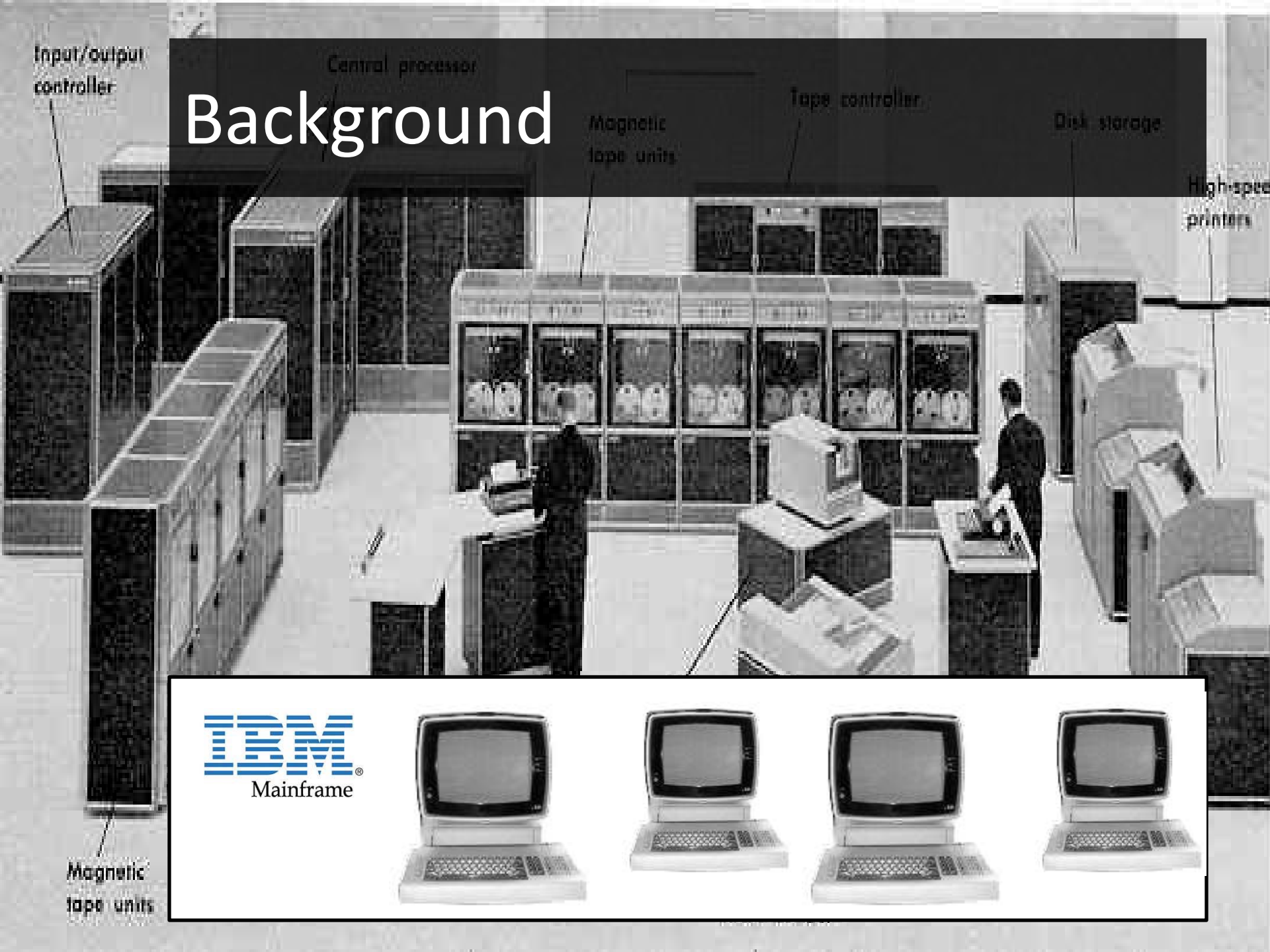
Background

- "Computing machines" solve problems
- 1952 Aiken described *scientific* problems

> "Originally one thought, that if there were a half dozen large computers in this country, hidden away in research laboratories, this would take care of all the requirements we had throughout the country."

"Portrait of a Computer Pioneer: Howard Aiken" by I. Bernard Cohen, pg 292

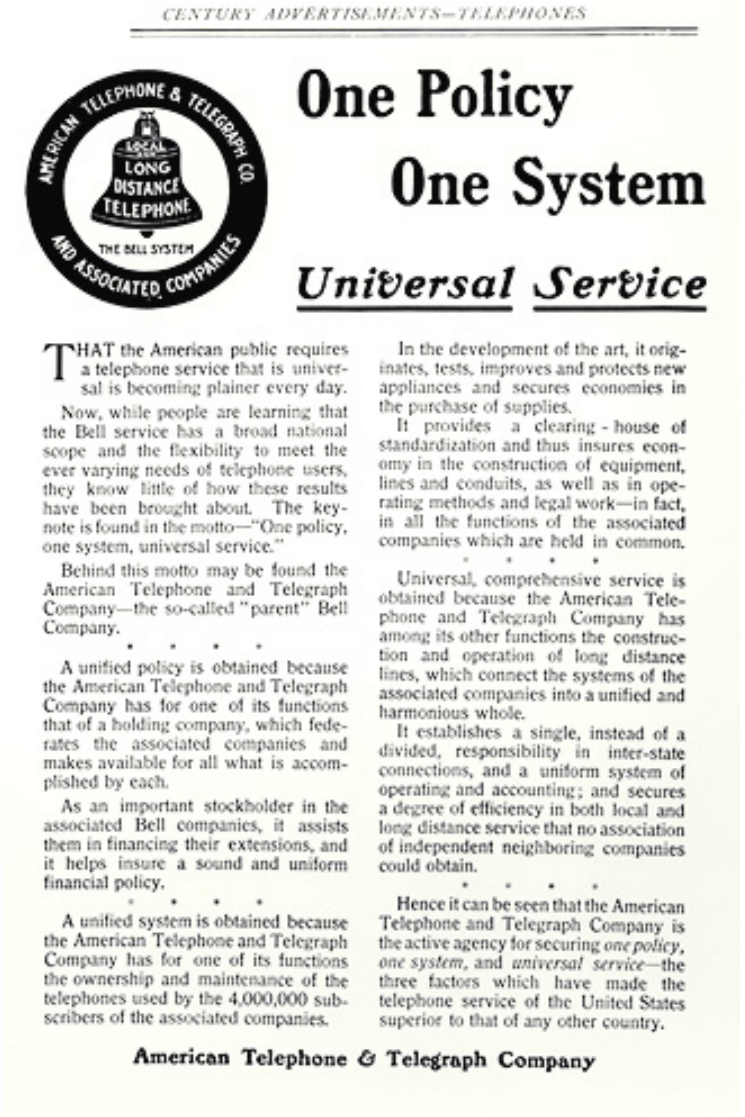
Background



IBM Mainframe

Yesterday…

- 1918 National Security
- U.S. Nationalized Telecom Industry
- "Natural Monopoly"
  - Cost Efficiencies and Long-run Averages
  - Barriers to Entry



CENTURY ADVERTISEMENTS—TELEPHONES

AMERICAN TELEPHONE & TELEGRAPH CO. AND ASSOCIATED COMPANIES — LONG DISTANCE TELEPHONE — THE BELL SYSTEM

One Policy
One System
Universal Service

THAT the American public requires a telephone service that is universal is becoming plainer every day.

Now, while people are learning that the Bell service has a broad national scope and the flexibility to meet the ever varying needs of telephone users, they know little of how these results have been brought about. The keynote is found in the motto—"One policy, one system, universal service."

Behind this motto may be found the American Telephone and Telegraph Company—the so-called "parent" Bell Company.

* * * *

A unified policy is obtained because the American Telephone and Telegraph Company has for one of its functions that of a holding company, which federates the associated companies and makes available for all what is accomplished by each.

As an important stockholder in the associated Bell companies, it assists them in financing their extensions, and it helps insure a sound and uniform financial policy.

* * * *

A unified system is obtained because the American Telephone and Telegraph Company has for one of its functions the ownership and maintenance of the telephones used by the 4,000,000 subscribers of the associated companies.

In the development of the art, it originates, tests, improves and protects new appliances and secures economies in the purchase of supplies.

It provides a clearing-house of standardization and thus insures economy in the construction of equipment, lines and conduits, as well as in operating methods and legal work—in fact, in all the functions of the associated companies which are held in common.

* * * *

Universal, comprehensive service is obtained because the American Telephone and Telegraph Company has among its other functions the construction and operation of long distance lines, which connect the systems of the associated companies into a unified and harmonious whole.

It establishes a single, instead of a divided, responsibility in inter-state connections, and a uniform system of operating and accounting; and secures a degree of efficiency in both local and long distance service that no association of independent neighboring companies could obtain.

* * * *

Hence it can be seen that the American Telephone and Telegraph Company is the active agency for securing *one policy, one system,* and *universal service*—the three factors which have made the telephone service of the United States superior to that of any other country.

American Telephone & Telegraph Company

Yesterday…

- 1961
  - 84,450,000 US Phones
  - 68,640,000 Bell **(81%)**
  - Bans Against 3rd Party

1964

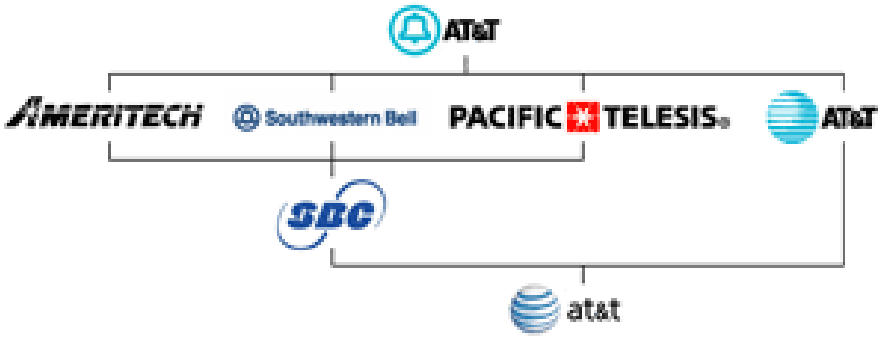
1969

- 1968
  - Federal Ruling 13 F.C.C.2d 420
  - Carterfone or "**any lawful device**" allowed (no damage to system)

http://www.cybertelecom.org/notes/att.htm

http://www.uiowa.edu/~cyberlaw/FCCOps/1968/13F2-420.html

Yesterday…



- *Customer-Owned* Innovations
- Answering Machines
- Fax Machines
- Modems !!!

Today…

2012 (41 years later)

- 80% Mobile Profits are Apple
- Rants Against 3rd Party

> We cannot be at the mercy of a third party deciding if and when they will make our enhancements available to our developers.
>
> -- Steve Jobs (http://www.apple.com/hotnews/thoughts-on-flash/)

http://news.cnet.com/8301-13579_3-57374689-37/apple-samsung-own-95-percent-of-all-mobile-phone-profits/

…or Today?

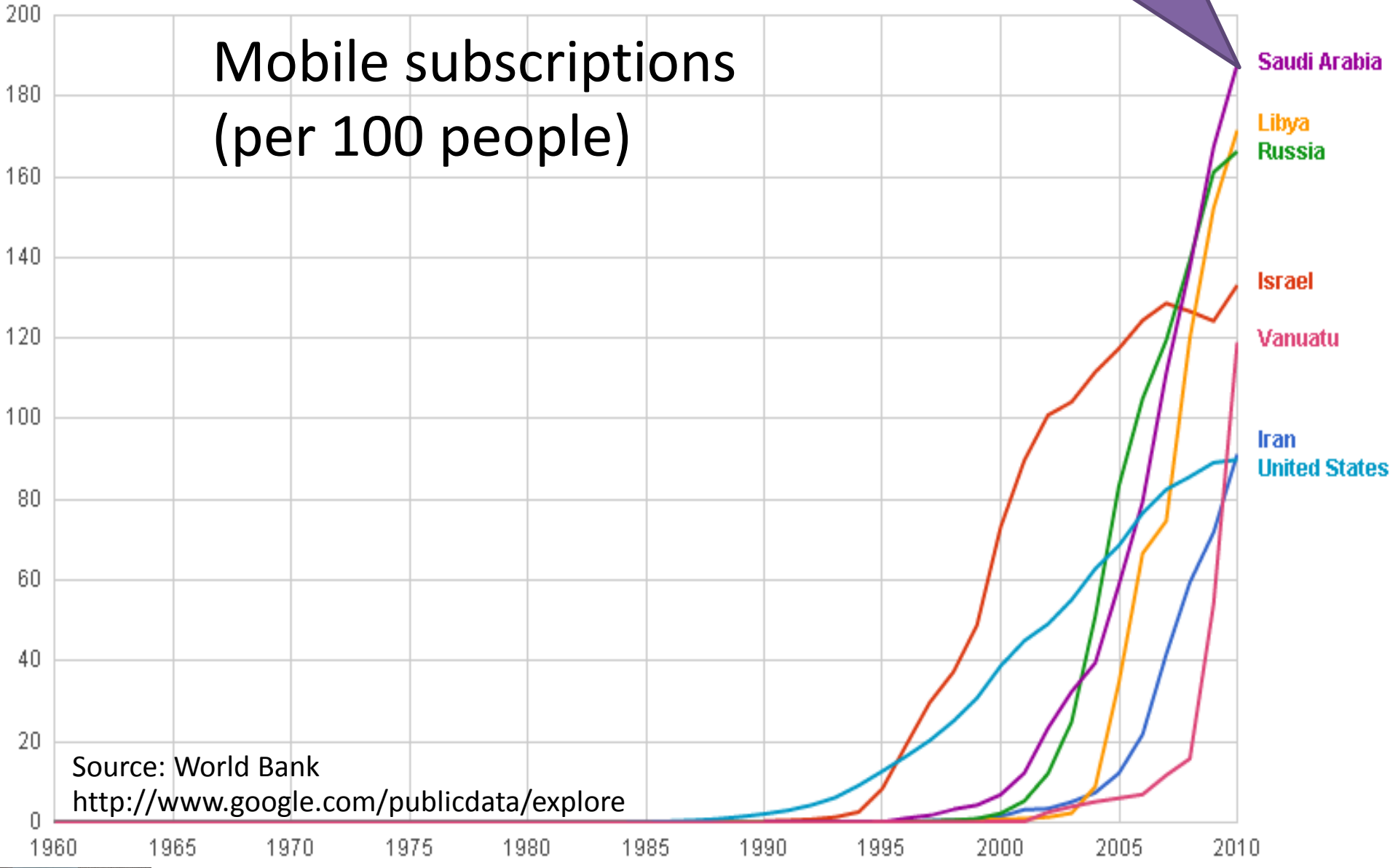
…or Today?

"…half dozen large computers in this country, hidden away…"

Technology Trend

27million people
x2 devices

Mobile subscriptions
(per 100 people)



Source: World Bank
http://www.google.com/publicdata/explore

Technology Trend

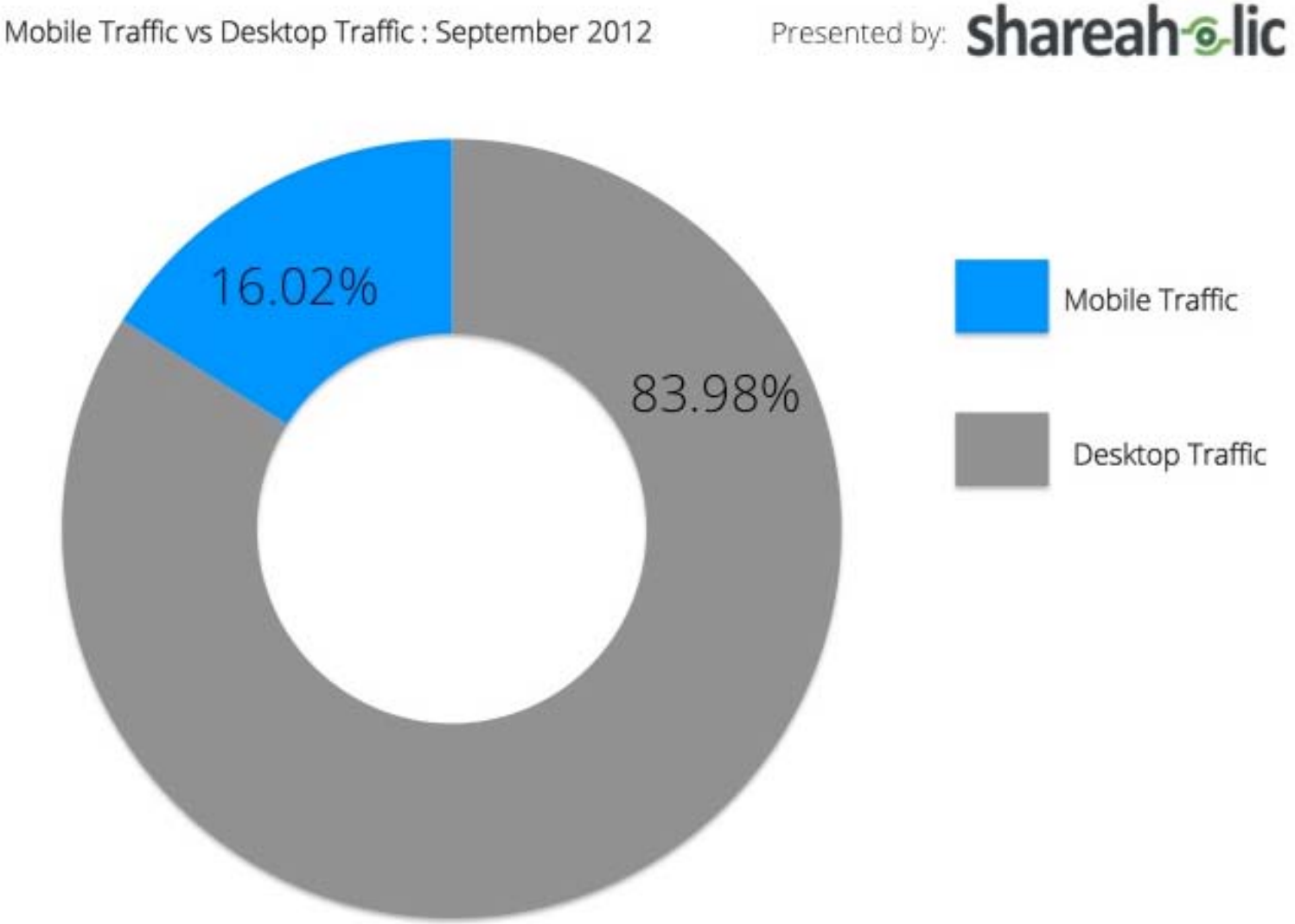
- Mobility
- Capability
- Redundancy
- Decentrality

Democratization

	Mobile Devices	M2M Traffic	More than 2
2011	5.4b	159m	7%
2016	7.4b	984m	25%

Cisco: Global Consumer Mobile Device and Connection Trends, May 16 2012

Technology Trend

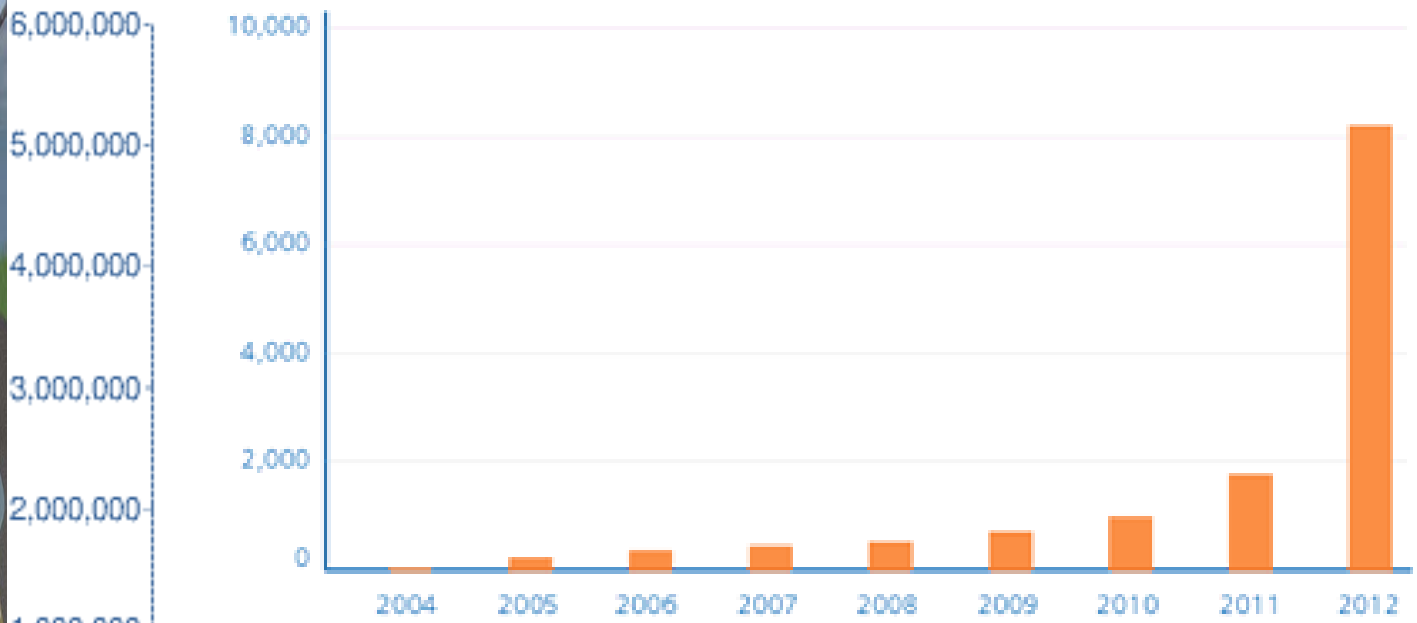


http://blog.shareaholic.com/2012/10/mobile-website-traffic-2012/

"Only 9 of the 22 tested products managed to block both variants of the exploit" (31 August 2012) *

Meanwhile…

1,200% increase in Android malware



Malware Detected by Year

Sources:

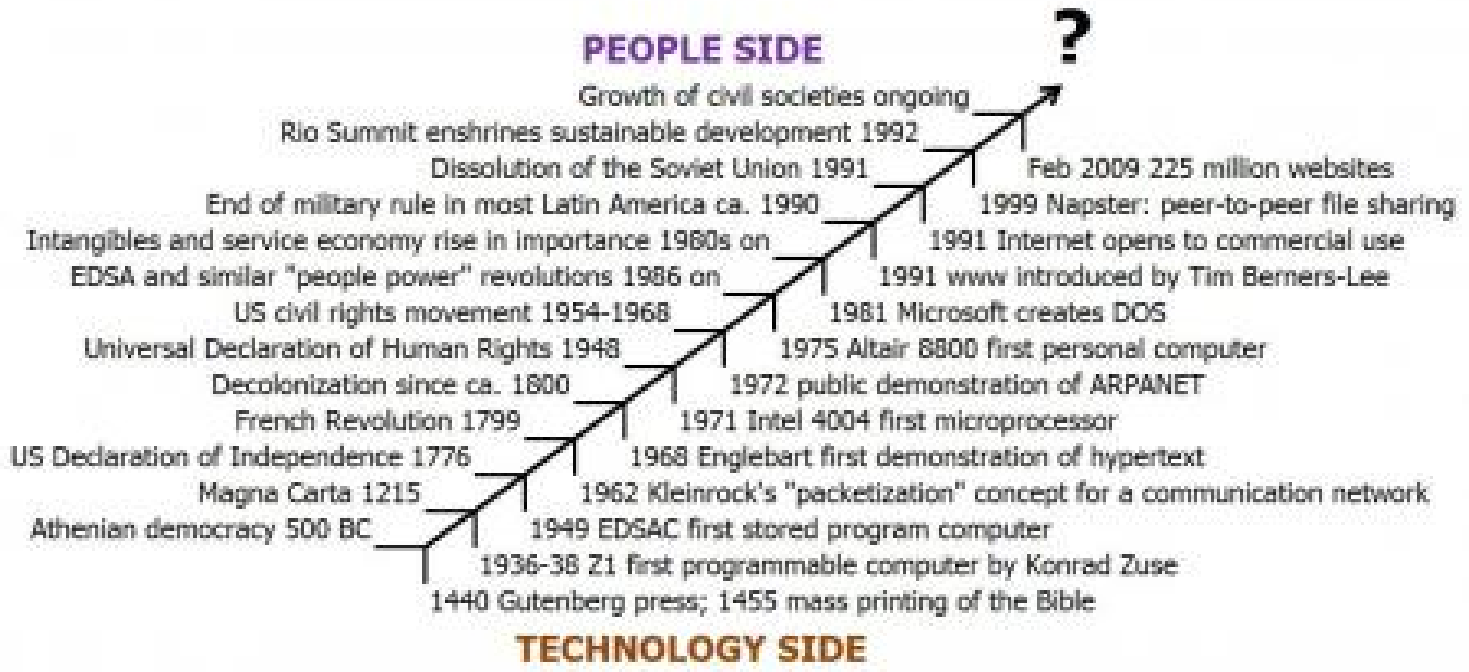
http://www.washingtonpost.com/wp-dyn/content/article/2008/03/19/AR2008031901439.html
* http://www.h-online.com/security/news/item/Only-9-of-22-virus-scanners-block-Java-exploit-1696462.html
http://www.scmagazine.com/report-finds-1200-percent-boom-in-android-malware/article/242542/

Technology *Reversion*

- 2012 Apple v. Bitdefender Clueful
  - 60,000 apps tested
  - 42.5% do not encrypt network traffic
  - 41.4% access location
  - 20% access address book
- Billions of Apps Downloaded
  - Apple 25B
  - Google 20B

Political Theory

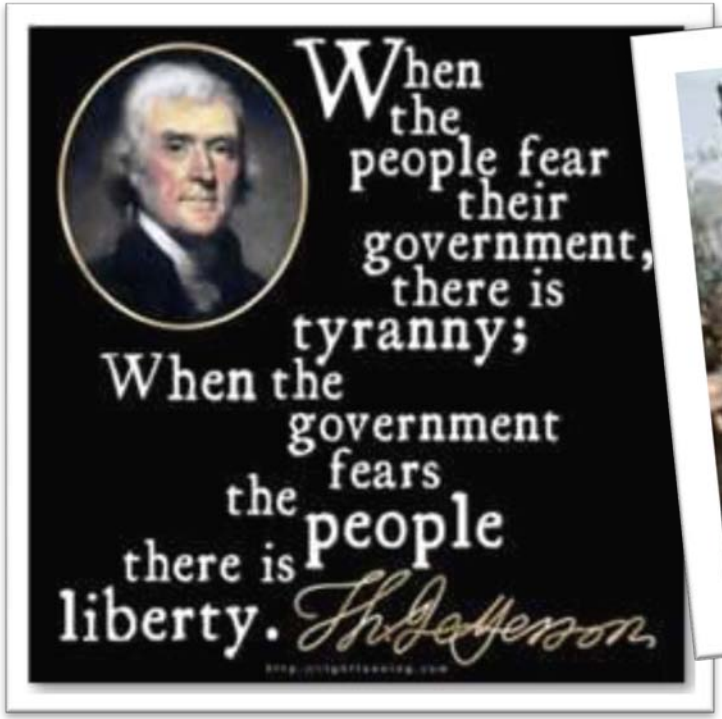
- *Modernization* – resource availability
- *Emancipation* – dissent and exploration
- *Democratization* – regulatory framework



Historical Example

- 15thC Ottoman Empire
- 19thC Nationalism, Despotism, Militarism…
- 21stC Democratization

Reversion



Auditors…Essential Role in Democratization

- Regulatory Framework
- Assessment of Compliance

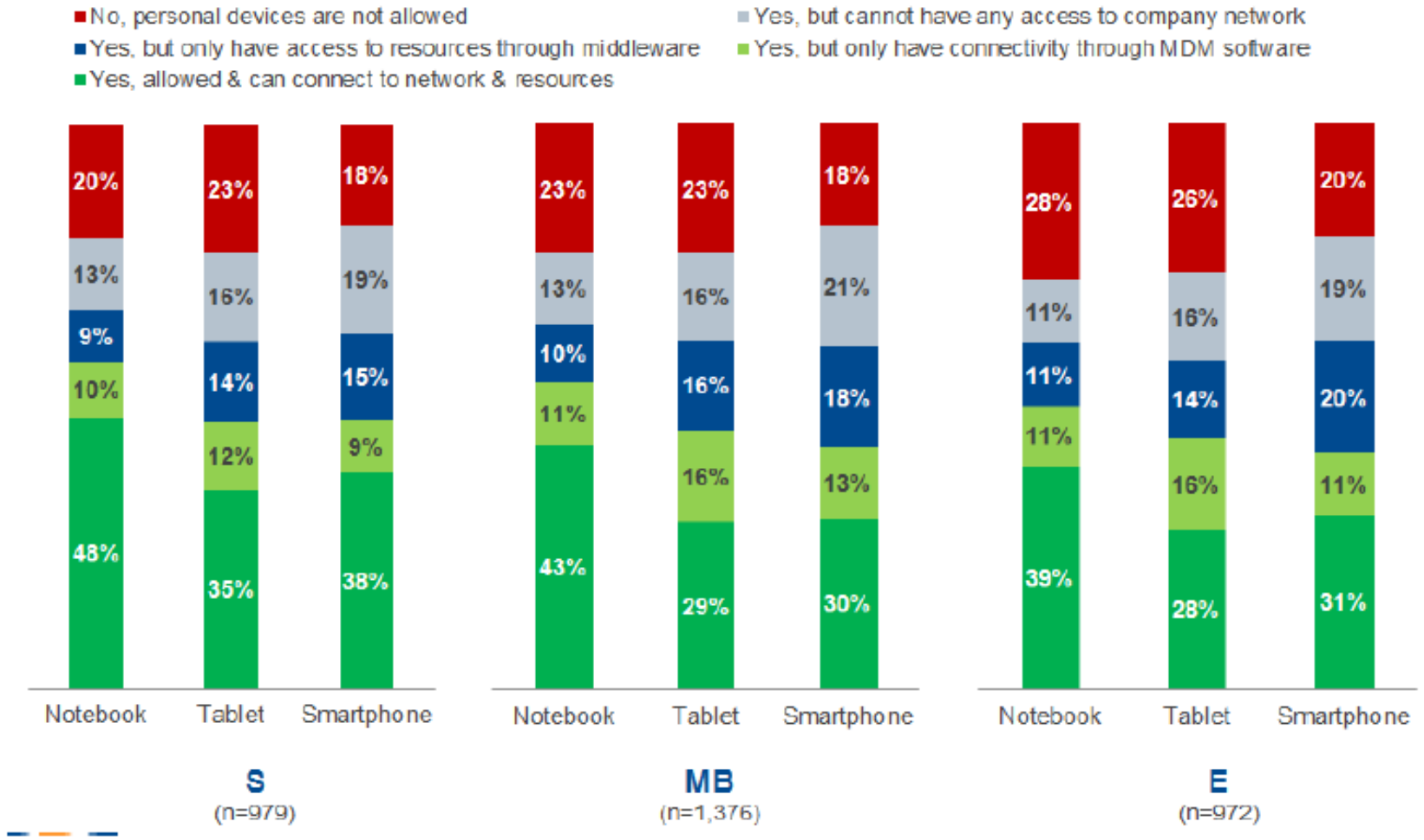
Enterprise Profile

- 90% enterprises have deployed mobiles[1]
- 86% enterprises to deploy tablets in 2012[1]
- 71% no specific policies and procedures[2]

[1] Gartner: 2012 Survey
[2] ITIC Survey 2012

Deployment Strategies

Personal devices: won't restrict them, but can't manage them yet



Kaspersky: Global IT Security Risks Survey Report 2012

Consumer Profile

- 18% own *five* devices[1]
- 75% use for sensitive apps[1]
- 41% use without permission[1]
- 30% have experienced security threat[1]

- $600 average spend per Cisco employee[2]
- 40% say device choice important[2]

[1] Juniper: Trusted Mobility Index
[2] Cisco: The Everywhere Employee

Consumer Profile

- **86% worry about data destruction by employer**
- **82% afraid of monitoring after work**
- **82% say tracking is "invasion of privacy"**

- **76% would not give employer OS access**
- **75% would not trade location for access**

http://www.maas360.com/maasters/blog/security-information/byod-beware-infographic/?A=PR
http://wingedpig.com/category/safari/hyena/

Myth of “trust nothing”

> “Disruption theory has taught us that the greatest danger facing a company is making a product better than it needs to be. There are numerous incentives for making products better but **few incentives to re-directing improvements away from the prevailing basis of competition**.

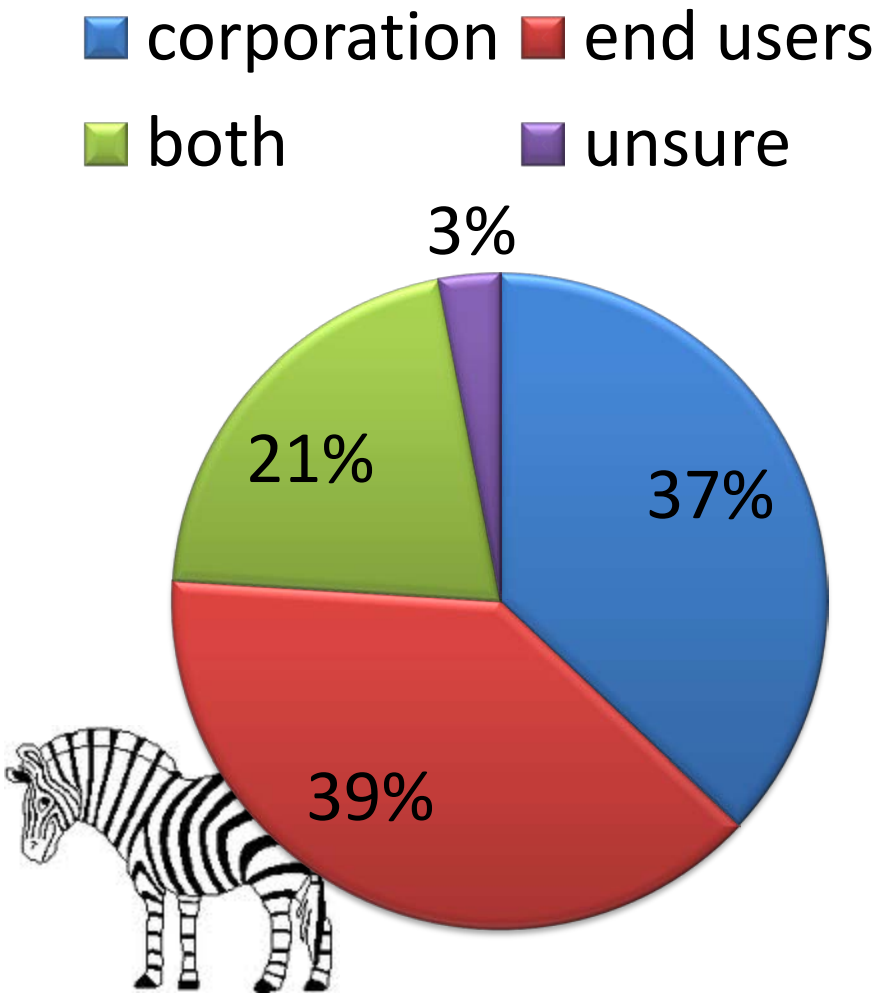
http://www.asymco.com/2012/09/18/is-the-iphone-good-enough/

Myth of “trust nothing”

> **…few incentives to re-directing improvements away from the prevailing basis of competition.**

http://www.asymco.com/2012/09/18/is-the-iphone-good-enough/

The 61% Responsibility for Security



ITIC Survey 2012

http://www.cio-today.com/news/Who-s-Responsible-for-BYOD-Security-/story.xhtml?story_id=13100BOHG3BH

MANAGING RISK

(PROTECTING YOUR HERD)

Service Provider Mindset

- “Herd” Benefits
- Pre-’68 v. Post-’68 Security Management
- Segmentation of Threats: SLAs and Zones of Control
  - Formal documentation and policies
  - Customer / Device Differentiation
  - Cost / Benefit Analysis (e.g. Help Tickets)
  - Data Custody, Possession and Control

Managing Risk

Threat	UI	OS	HW	P
Disclose				
Disrupt				
Impersonate				
Deny				

Malware

Vuln

Stolen, lost or sold

Bad App

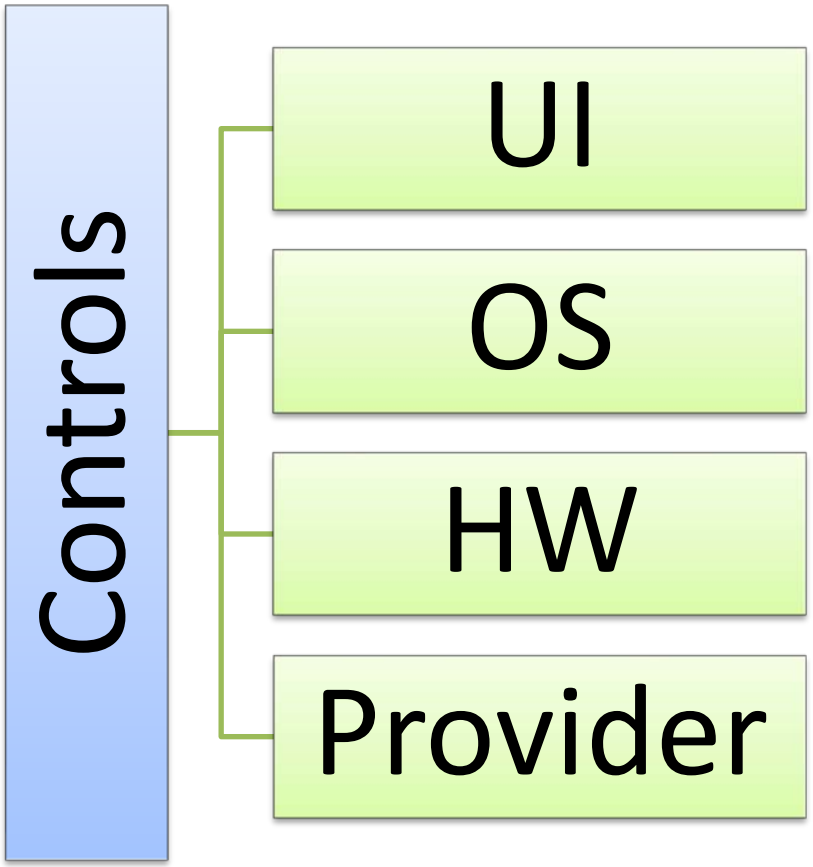
Evil Peer

Rogue AP

https://www.owasp.org/index.php/Threat_Risk_Modeling
http://www.m-cycles.com/concepts/concept01.php

Managing Risk

Managing Risk



Provider

- Lock-in
- Identity
- Location
- Connectivity
  - WiFi
  - GPS
  - SMS
  - MMS

Signals 24 hours a day
= location information

12 billion data points
every 90 seconds
-- Inrix

"like Verizon iPhone 5 users, some AT&T customers experienced hundreds of dollars in overages. One iPhone 5 user reported gobbling up to 2GB of cellular data over a three-day period while connected to Wi-Fi"

http://9to5mac.com/2012/10/01/iphone-5-carrier-data-leak-bug-might-not-be-verizon-only/

HW

- Display / Interface
- Performance
- Connectivity
  - WiFi
  - GPS
  - SMS
  - MMS
  - NFC
  - BlueTooth
  - Ports/Cables

OS

- Device
  - iOS
  - Android, Meego…
  - BlackBerry
  - Windows
  - Symbian, Belle
- Supporting System
  - Windows
  - OSX, Linux

Version	Codename	API	Distribution
1.5	Cupcake	3	0.1%
1.6	Donut	4	0.4%
2.1	Eclair	7	3.4%
2.2	Froyo	8	12.9%
2.3 - 2.3.2	Gingerbread	9	0.3%
2.3.3 - 2.3.7		10	55.5%
3.1	Honeycomb	12	0.4%
3.2		13	1.5%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	23.7%
4.1	Jelly Bean	16	1.8%

Data collected during a 14-day period ending on October 1, 2012

http://news.cnet.com/8301-1035_3-57524230-94/gingerbread-most-popular-android-flavor-at-56-percent-market-share/

App

- Versions
  - Exact
  - Up to or after…
- Controls
  - Remote Management / Policy
  - Roles, Segmentation
  - Authorization (root)
  - Encryption
  - Redundancy

Most Likely

1. Physical Loss
2. Malware / Bad App
3. MiTM
4. Peer Networking

DEVICE

Most Likely → Controls

- Physical Loss Remote
  - Lock
  - Backup
  - Monitor
  - Wipe
- Malware / Bad App
  - Black/Whitelist
- MiTM
  - Encryption
  - Identity
- Peer Networking
  - Encryption
  - Identity

Policy

- Roles and Responsibilities
- Services
  - Authentication and Authorization
  - Configuration Management
  - Auditing

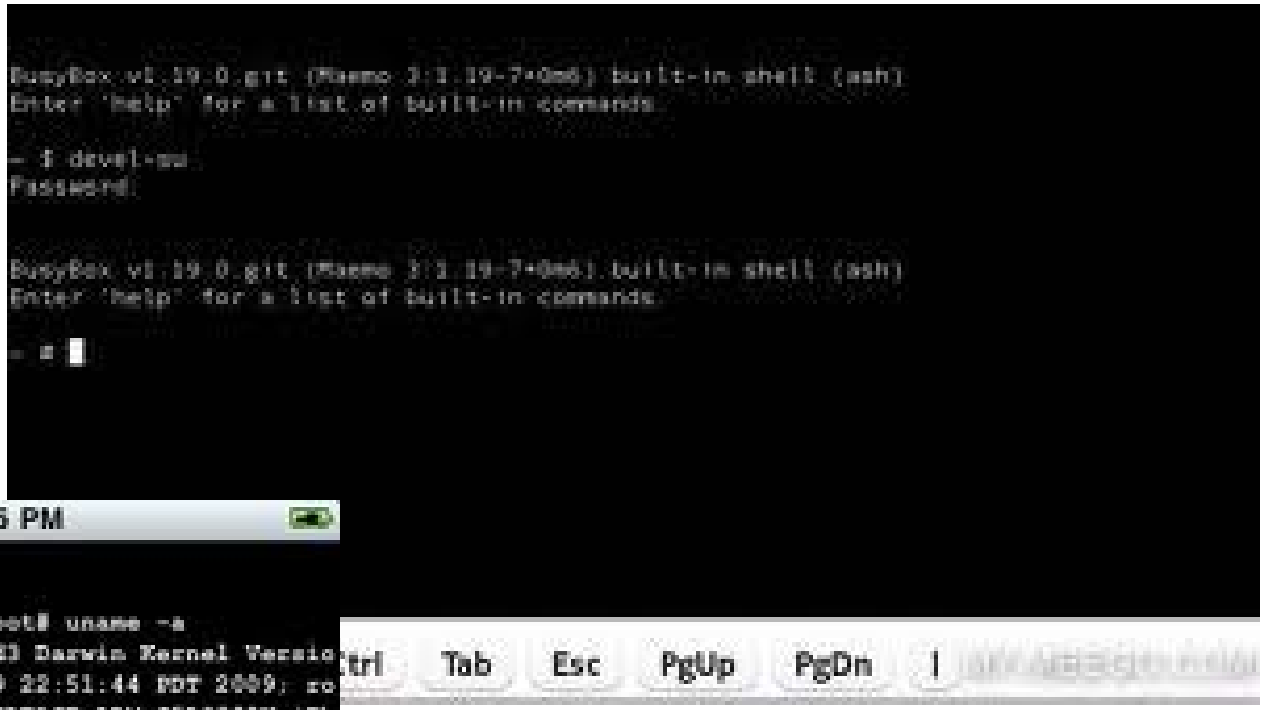
Redundancy and Control

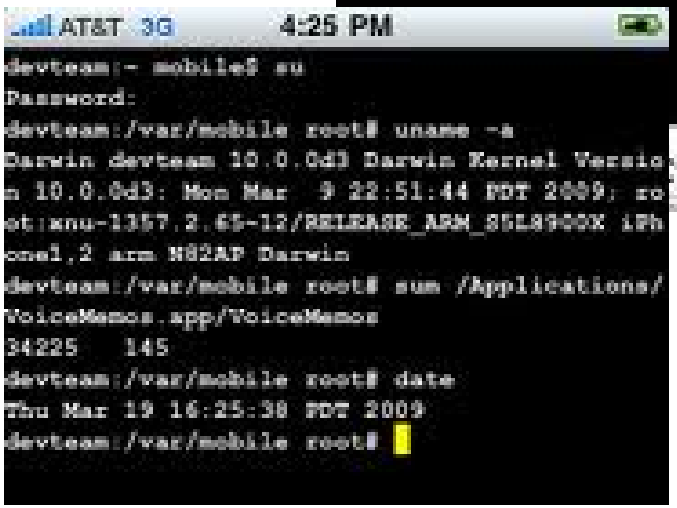
- Identities and Configurations
- Data (Including Logs)
- Applications
- Infrastructure Settings

Roles, Segmentation

- Multi-user
- Multi-mode

Authorization (root)





Encryption

- Differs by device
- Device-level only
- User-level or root?

Security Services

- Lock
- Backup
- Monitor
- Wipe
- Black/Whitelist
- Encrypt
- ID

Conclusions

- BYOD is inevitable/evolutionary
- Trust is not a myth
- Service-model of security and compliance

In(sta)Security:
Managing the BYOD Risk

Thank you!

@daviottenheimer

davi@flyingpenguin.com