McRoberts SECURITY TECHNOLOGIES SINCE 1876

The Latest IT Trends

July 23, 2015

Trending Technologies

- OS Vulnerabilities
- Cloud-computing
- Internet of Things
- Managed Services

MSFT vs. APPLE

Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0
Microsoft Windows Vista	34	23	11	0
Microsoft Windows RT	30	22	8	0

Unix/Linux is Safe Right?

- **Ubuntu**
  39 total vulnerabilities 7 high severity 27 medium severity 5 low severity
- **Red Hat Enterprise**
  27 total vulnerabilities 6 high severity 17 medium severity 4 low severity
- **openSUSE**
  20 total vulnerabilities 9 high severity 9 medium severity 4 low severity
- **Fedora**
  15 total vulnerabilities 3 high severity 9 medium severity 3 low severity
- **Windows**
  68 total vulnerabilities 47 high severity 20 medium severity 1 low severity
- **Android**
  6 total vulnerabilities 4 high severity 1 medium severity 1 low severity
- **Safari**
  70 total vulnerabilities 3 high severity 67 medium severity 0 low severity

Recent Vulnerabilities

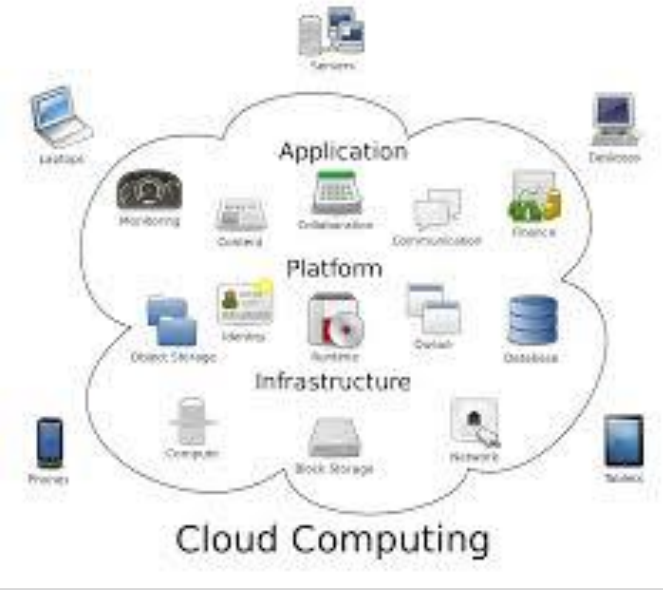
- Kaspersky Lab revealed a cybercriminal gang raided up to 100 financial institutions internationally for an estimated $1 billion. (March 2015)
  - "The most glaring thing that stood out for me [in the Kaspersky report] is that they had patches available for well over a year yet those systems weren't patched."

  Lonny Brooks, Manager of Security Services at Xamin, Inc.

- 45 MSFT vulnerabilities (June 2015)
  - MS-15016 Windows Kernel
    - 8 total flaws
    - Memory failure
  - MS-15056 Internet Explorer
  - MS-15057 Windows Media Player

Cloud Computing

- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
  - **The NIST Definition of Cloud Computi**
  - **NIST Special Publication 800-145**
- Advantages
  - Availability
  - Access
  - Provisioning
  - Auto-Recover



Security Implications

- Shared Platform
- Enterprise Id
- Privacy
- Pooling exploits
  - APIs
  - Mngt Interface
  - Resource Hoard

Internet of Things

- The *Internet of Things* (IoT) is the network of objects or "*things*" embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices.

  -Wikipedia

- Examples of Port Automation
  - Intelligent buildings
  - Automated equipment
    - Robots, cars, and cranes
  - Refrigeration Monitoring
  - Automated Ports
    - Port of Hamburg, Germany
    - Rotterdam, Netherlands

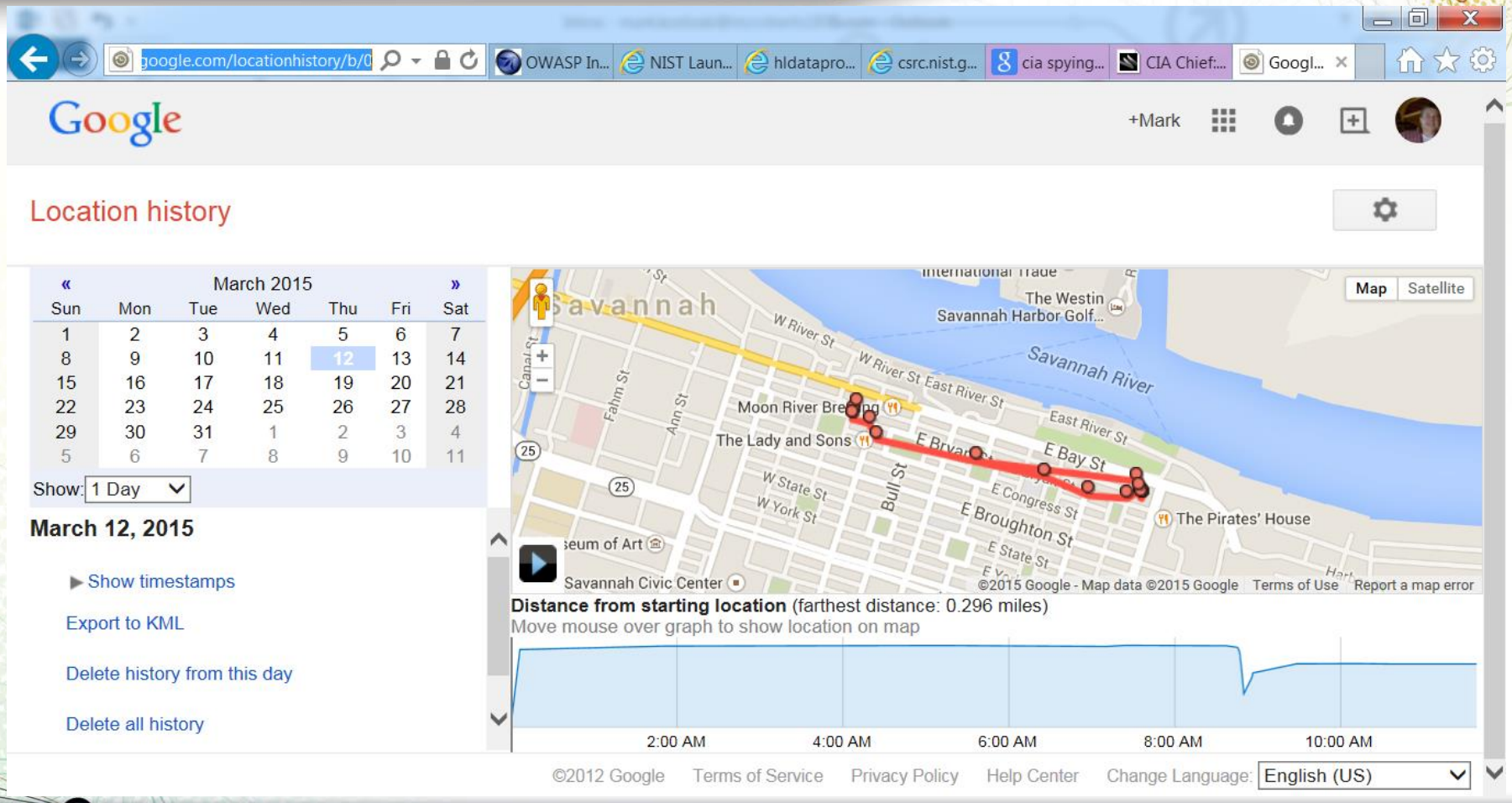
Security Implications

- FTC Warns of the Huge Security Risks in the Internet of Things
- Cyber-Physical System (CPS)
  - NIST Preliminary Draft
- Manufacturers Security
  - Security is not the primary goal
  - Embedded systems lack standards/framework
  - Globalization

Security Implications

- Huawei Defends Equipment Security- 2013
  - Largest Telecom in the world
- U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts
  - Mapped the Iranian network
- How the NSA can 'turn on' your phone remotely (well not really)
- iRobot's latest Roomba robot is designed for hackers

Security Implications



Managed Services

- Limited Resources
  - Budget
  - Personnel
  - Utilities/Tools
- Scalable
- Industry Compliance
  - Identify
  - Protect
  - Detect
  - Respond/Recover