Securing Disruptive Technologies

Paul Blahusch
IT Security Officer
US Bureau of Labor Statistics

BLS
BUREAU OF LABOR STATISTICS
U.S. DEPARTMENT OF LABOR

www.bls.gov

Speaker Bio

Paul Blahusch

- 20+ years in IT (BLS, NIH, DoD)
- 10 years as Federal employee at BLS working exclusively in IT Security
- Agency IT Security Officer since 2005
- Certified Information System Security Professional (CISSP) since 2002

Securing Disruptive Technologies - Outline

- But first, what are *disruptive technologies*
  - "Innovations that improve a product or service in ways that the market does not expect" – wikipedia.org
- Brief history of computers and security
- Lessons-learned
- Current opportunities and challenges

Brief History of IT and Security

1960s

- MIT students begin exploring and programming the school's mainframe computer system and coin the term "hacker”.
- The DoD creates ARPANet for the electronic exchange of information paving the way for the creation of the Internet (See Gore, A.).
- “Hacker friendly” UNIX operating system and ‘C’ programming languages invented.

1970s

- Steve Jobs and Steve Wozniak found Apple Computer and begin marketing the Personal Computer (PC) – bringing computing power to the masses.
- USENET, a bulletin-board-style system for electronic communication created and quickly becomes a popular forum for the exchange of ideas in computing, networking, and, of course, cracking.

Brief History of IT and Security (Cont.)

1980s

- IBM develops and markets commodity PCs aiding in the proliferation of such hardware in the homes and offices of (malicious) users.
- The 414 gang break into systems from such top-secret locations as the Los Alamos National Laboratory, a nuclear weapons research facility.
- The Computer Fraud and Abuse Act of 1986 is voted into law.
- Morris Worm infects over 6,000 vulnerable computers connected to the Internet, leading to the creation of the Computer Emergency Response Team (CERT).
- The magazine ***2600: The Hacker Quarterly*** is created and begins discussion on topics such as cracking computers and computer networks to a broad audience.
- Clifford Stoll writes ***The Cuckoo's Egg***, Stoll's account of investigating crackers who exploit his system.

Brief History of IT and Security (Cont.)

1990s

- ARPANet traffic is transferred to the Internet, beginning connectivity as we know it today.
- The Web browser is created and sparks demand for public Internet access.
- Hacking incidents soar – Vladimir Levin (stole $10 Million from CitiBank); Kevin Mitnik (stole PII, CC#’s, source code); Kevin Paulson (hacked phones systems to win radio station prizes).
- A 19-year-old student performs numerous break-ins to US government systems during the Persian-Gulf conflict.
- US Attorney General Janet Reno establishes the National Infrastructure Protection Center.
- First annual DefCon convention to celebrate and promote hacking is held in Las Vegas.

Brief History of IT and Security (Cont.)

2000s-Today

- ILOVEYOU e-mail worm infects millions of computers.
- DDoS attacks take out heavily-trafficked Internet sites such as yahoo, cnn, amazon, and fbi.gov.
- FISMA enacted in 2002.
- In 2004, on any given day, there are approximately 225 major incidences of security breach reported to the CERT Coordination Center.
- Lost/stolen PII from governments and private companies bring focus to risk of portable media and systems. OMB memorandum follow soon after.
- Internet-based attacks become more sophisticated, customized, and focused (i.e. Spear Phishing).
- Attack targets move from operating systems to web-based applications.
- Social networking explodes; koobface virus makes appearance.
- Adversary profile changes from "script-kiddie" and recreational hacker to organized crime and nation-state.
- Number and severity of incidents continues to increase.

History – Lessons Learned

- Security lags innovative use
  - Catching up … closer today than in past
  - Increased community effort and audience
  - But “bad guys” are getting faster too
- Innovation in use of technology is usually “bottom-up” and security is “top-down” … resulting in knowledge gap
- The unknown or unsuspected leads to “pain”
- “Pain” usually leads to action … over-(re)action?

Lessons Learned – Jurassic Park

- 360 degree Risk Management
  - Dr. Ian Malcolm

    "Just because you **can** do something, doesn't mean you **should**."

- Can't secure what we don't know
  - Unknown/unsuspected risk is a "killer"
  - Raptors, raptors, raptors!!!

Today's Opportunities/Challenges

- Social Networking
  - Facebook, MySpace, Twitter, YouTube
- Cloud Computing or Software-As-A-Service (SAAS)
  - Webex, SurveyMonkey, SalesForce.com
- Ubiquitous computing and communication
  - Smartphones and handhelds
  - Wi-Fi, "hot spots", kiosks

Opportunities/Challenges of Social Networking

- Opportunities
  - Marketing & branding
  - Interaction with customers (public)
  - Interaction with partners
- Challenges
  - Viruses or other malware on social networking sites
  - Disclosure of sensitive information

Addressing Challenges of Social Networking

- Viruses or other malware on social networking sites
  - Block access to social networking sites
  - Selective content filtering
  - Funnel all access through secured host
  - Secure the end point (user PC)
- Disclosure of sensitive information
  - For “Official Use”
    - Easy – have all content for posting properly vetted
  - For “personal” use
    - All powerful Oz solution
    - Awareness and education

Opportunities/Challenges of Cloud Computing

- Opportunities
  - Cost Savings
  - Faster Deployment
  - Better Features
- Challenges
  - Lack of direct control/oversight – must be through contracts, MOUs, etc.
  - Loss of direct control of sensitive information – Who “owns” the data?
  - What if provider goes out of business?

Addressing Challenges of Cloud Computing

- Lack of Direct Control/Oversight
  - Ensure comprehensive contract provisions are in place, monitored, and enforced
    - See *Sample Contract Language for Secured Acquisition* at OMB MAX Community
  - Policy and awareness on data types permitted handled by external provider
  - All data transmissions to external provider pass through trusted insider vetting (i.e. a *gatekeeper* function)
  - Have independent “backup” plan

Opportunities/Challenges of Ubiquitous Computing

- Opportunities
  - Respondent convenience – reply to surveys how and where they choose
  - Data user choice – access to published data
  - Flexibility for data collectors – what works best & cheapest?
- Challenges
  - Endpoint security
  - Unsecured environments
  - Platform development issues

Addressing Challenges of Ubiquitous Computing

- Endpoint Security
  - Ensure similar security controls as traditional client devices (anti-virus, encryption, etc.)
- Unsecured environments
  - Secure the transmission
- Platform Development
  - Use development best practices for all platforms supported (See OWASP, SANS)

Summary

- New technology will be useful for improving Survey Information Collection
- History shows us that new technology will present new risks … that “bad things” will happen as a result of these risks … and that formal security (re)action will lag the risk
- Asking “should we” along with “can we” can help limit risk (*thanks Dr. Malcolm*)
- Partnering with your security group on new initiatives early-on can reduce risk by minimizing surprises – *we can only adequately secure what we know about*

Contact Information

Paul Blahusch
202-691-7561
blahusch.paul@bls.gov