Corporate IT Forensics in the New Decade

Hong Kong
March 2010
Bruce Nikkel

Presentation Overview

- The growth and evolution of digital forensics
  - Pre-Y2K computer forensics
  - Post-Y2K digital forensics
  - Factors influencing digital forensics and progress made
- The state of corporate IT forensics today
  - The established digital forensics community
  - Current problems still to solve
- Corporate IT forensics beyond 2010
  - Where digital forensics is headed
  - Challenges to face
  - Areas of change and adaptation

Pre-Y2K Computer Forensics

- Significant factors influencing computer forensics before 2000
  - 1980s: home computers & BBS dial-up
  - 1990s: Internet access
- New kinds of criminal activity, new sources of evidence
  - New "Computer Crime"
  - Evidence primarily limited to storage media (Computer disks, floppies, etc.)
- Digital Forensics Progress
  - Formal computer forensics mostly limited to Law Enforcement
  - Corporate organizations dealt with intrusions and security incidents, but not in a forensic context
  - Beginnings of a scientific research community

Post-Y2K Digital Forensics: Influencing Factors

- September 11, 2001 tragedy
  - Changed global views on the importance of security and incident response
  - New priorities for disaster recovery, incident management, investigation, and forensics
- Corporate accounting scandals
  - Enron, Andersen, WorldCom, and others
  - Sarbanes-Oxley (SOX) requiring digital evidence collection capability, investigation and incident response processes
- Growth of intellectual property concerns
  - IP/Brand related abuse
  - file sharing and copyright violations
- Corporate reliance on Internet technology
  - Internet fraud, phishing, infrastructure attacks
  - Computer related employee misconduct

Post-Y2K Digital Forensics: Progress

- Became a formal scientific discipline
  - Theory, Abstractions, Models, Frameworks
  - Practical tools, methods, procedures
  - Corpus of literature and professional practice
  - Confidence and trust in results
- Professional community
  - International peer reviewed journals and conferences
  - Practitioner best practice
  - Formal standards and procedures
- Expanded scope of Digital Forensics: now includes
  - Network forensics (captured traffic, remote collection)
  - Software forensics (malware/code analysis)
  - Live system forensics (memory, running processes)
  - Embedded devices (mobile phones, PDAs, GPS, etc.)
- Arrival of anti-forensics or counter-forensics

Digital Forensics Today

- The current state of digital forensics
  - Thriving scientific research community
  - Experienced and professional community of practitioners
  - Rigorous and formalized processes and methodology
  - Well established fundamental tools and techniques
  - Significant growth in the corporate sector
- The coming decade: beyond 2010
  - What existing problems need solving?
  - What new expectations and requirements will be demanded?
  - Which challenges we must face and overcome?
  - How must digital forensics change and adapt?

Challenges Beyond 2010

- Forensic Readiness
  - Less reliance on accidentally found evidence, more preparedness and planning for evidence collection
  - Building forensic capability into IT infrastructure and applications as a standard component, from the initial design phase
  - Having processes, tools and trained staff available in advance, for performing forensic work
- Information Security
  - Forensic tools can be powerful and invasive
  - Must be carefully controlled and responsibly used
  - Policies to ensure access is restricted to authorized investigators and forensic analysts
  - Adequate protection of copied data during storage and transfer, in the short term as well as the long term

Challenges Beyond 2010

- Legal and Regulatory Compliance
  - Jurisdiction differences and forensic requirements are different around the world, complex to implement globally
  - Some forensic activity may be restricted: privacy law, wiretapping law, etc.
  - Some forensic activity may be mandated: data retention, evidence collection process, etc.
- Risk sensitive forensics
  - Balancing the cost and effort of forensic work with the likelihood of finding evidence
  - Technical depth: you can always dig deeper, but when do you stop?
- Adopting new cost effective and efficient solutions
  - Moving data to the tools vs. moving the tools to the data (for example: integrating e-discovery tools into backup systems)
  - Replacing suspect hard disks, instead of forensic imaging in the field
  - Separating forensic acquisition role from forensic analysis role

Challenges Beyond 2010

- External ownership of corporate IT Infrastructure
  - Complex, multi-party infrastructure outsourcing
  - Externally hosted/shared applications
  - Cloud computing
  - Certain aspects of technical forensic computing may not be feasible or sensible in these environments
- Shift in evidence location
  - Less reliance on client PC disks as a regular evidence source, more reliance on server logs and archived data
  - Evidence increasingly found on external infrastructure, requiring cooperation with external parties
  - Increase in electronic data devices and storage which cannot be easily analyzed: iPhone, iPad, and other restricted access devices
  - Social networking sites, blogs, external public applications

Challenges Beyond 2010

- Increase in data volume
  - Large amounts of data can be collected from large corporate IT infrastructures
  - Modern hard disk sizes: TBs are common, working with forensic images this size is cumbersome and time consuming
  - Large data sets require scalable and stable forensic tools
  - Improved reliance statistical analysis, anomaly detection, data mining, correlation
  - Data retention is a challenge: how long? how much detail?
- Complexity of finding evidence
  - Hard to maintain up-to-date forensic capability for rapidly changing technology
  - Many layers of data encapsulation and abstraction, increasing levels of technical detail
  - Difficulty analyzing proprietary, undocumented technologies
  - Encryption: secure email, protected files and file systems, key escrow/recovery processes

Challenges Beyond 2010

- E-Discovery and digital forensics
  - E-discovery branching off from traditional technical forensics
  - requires the processes of digital forensics, but not always the technical depth
  - less concerned with low level disk sectors and system artefacts, more concerned with search and collection of regular documents and emails
- Increased external forensic support and cooperation
  - Outsourcing partners
  - Competitors
  - Law Enforcement
  - Forensics community
- Research and practitioner community:
  - Developing digital forensics education programs
  - Forensic tool testing and validation processes (with approved list)
  - Involvement by formal international standards bodies (ISO/IEC, IETF, ITU, etc.)
  - Cooperation/interaction with LE and Corporate entities

Thank you for listening