A Commercial View of Why Testing is Critical

Dennis F. O'Brien

dob@garden.net

March 20, 2001

Pretest

Question

What you don’t know:

1. **Can’t hurt you.**
2. **Can kill you.**

Testing

- **What are you testing for?**
  - **Security? Piece? Entire Function?**
- **Review testing:**
  - **Risk**
  - **Complications (cog in bigger machine)**
  - **Consequences**

The Big Picture

- **The primary function of the part is different from the function of the assembled product**
- **The risk associated with the part is different from the risk associated with the assembled product**
- **For example, Collections of unclassified information may produce classified results**

Liability

- **Software vendors**
  - **USC BSD UNIX**
  - **Microsoft**
- **Software authors**
  - **Author of *wiz* mode in sendmail**

Testing Standards

- **Functionality**
- **Vulnerability**
  - **Error**
  - **Intentional exploitation**

Protection Strategy

- **Prevent**
- **Detect**
- **Recover**

A function of Risk Management, typically a combination of all three, in differing percentages.

Protecting your network

- **Proactive:**
  - **Intrusion Prevention**
- **Reactive:**
  - **Intrusion Detection**
  - **Recovery**

Value of Information

Government:

- **Classified Invasion plans on missing PC**
- **Lawrence Livermore incident**
- **CIA Operative list**

Corporate:

- **The secret *Coke* recipe**
- **SAT test answers (*in advance)***

Cost of Protection

- **You can pay now**
  - **You are managing protection**
- **You can pay later**
  - **Often in panic mode**
  - **Maybe too late**
  - **Maybe nothing left to recover**

Problem Evolution

- **No passwords**
- **Password guessing & later brute force cracking**
- **Exploiting known vulnerabilities**
- **Trojan horses**
- **Hijacking sessions**
- **Sniffers and distributed sniffers (Bug or feature?)**
- **DOS and DDOS attacks**

Make Security Transparent & Seamless

- **Transparent**
  - **Single Sign-on with verified trust**
  - **Out of band controls**
- **Seamless**
  - **Single Sign-on**
  - **Out of band controls**

Network Management Products Tool or Risk?

- **Network Management tool?**
- **Network Intrusion tool?**

Depends on:

- **Who is using it**
- **Their purpose**
- **Quality of the tool**

The Chief Engineer

- **In music, it's the conductor**
- **In theater, it's the choreographer**
- **In technology, it's the chief engineer**

Identification vs. Authentication

- **Identifier – Identifies who you are**
- **Authenticator – Proves who you are – Something you *know*, *have* and/or *are***
  - **Password**
  - **Digital Certificate**
  - **HTTPS**
  - **Hand-Held-Authenticator**
  - **Palm reader (Biometric)**

Implementing ***Seamless Controls***

Extending trust:

- **Pass on authenticated tokens**
- **Make sure it is verifiable**

Quality Control on the WEB

Input Validation

- **Negative quantity (shoplifting)**
- **Modify *source*, then retransmit**

Impersonation

Service Metrics

Provide QOS Metrics
Provide usage metrics
Provide a feedback loop

Threats

- Unintentional
- Intentional
  - Performed by insider
  - Performed by outsider
- Natural

Compartmentalized Network Architecture (cont'd)

- **New economy model**
- **Network-centric**
- **Dynamic / Fast response time**
- **Real time change control, where allowed**
- **Serial (simple) division of duties**
- **Every company maintains its own functional ISP dedicated to serving its best interests**

Security Management Tools

- **Host Intrusion Detection tool**
- **Network Intrusion Detection tool**
- **Application Intrusion Detection Features**

Depends on:

- **Who is using it**
- **Their purpose**
- **Quality of the tool (poor tools cause false alarms)**

E-commerce Strategy/Plan

- **Each business should have one and two year business plans where they are going relating to E-commerce and the Internet.**
- **Each business unit should have the same.**
- **They should integrate like the sections of an orchestra.**

Policy

- **Should be specific enough to deter unauthorized activities.**
- **Should be open enough to allow business units to generate revenue at every opportunity.**

Audit

- **Audits should be performed to verify compliance with *generally accepted industry standards* and *Corporate standards*.**
- **Auditors do not make policy. Audits document the degree of compliance.**
- **Auditors should have a full understanding of compensating controls.**

What's fair?

- **All is fair**
- **Hackers do not play fair**
- **Remember the TV game show "Survivor"**

Corporate consequence of no action

- ***Loss of value***
- ***Loss of shareholder value***
- ***Loss of corporate image***
- ***Loss of life***

A Trip Down Memory Lane

Background prior to 1980:

- **1970-1973 USASA Crypto.**
- **1974 dob social engineered**
- **1977 dob staff social engineered**
- **1985 C&P Tel has same scenario.**

1980 and Before:

- **Computers were interconnected via manual dialing.**
- **Then, a file transfer program was manually started. High speed is 110 baud.**
- **Printed UNIX manuals consisted of compilations of BTL papers.**
- **“One bell system, it works!”**

dob Exploitation Techniques

- **Exploit network layer**
- **Exploit host layer**
- **Exploit application layer**
- **Exploit physical controls**
- **Since security implementation is not comprehensive, exploitation of the *seams* within the security process frequently yield ripe rewards!**

E-commerce Philosophies

- **One single flat network. All security at perimeter with security department watching all.**
- **Compartment managed. Each unit is free to exist within the guidelines of the compartment above it. Allows each business unit to be different & make money, at the discretion of its management.**

Flat Network Architecture

- **One size fits all**
- **Old economy model**
- **Manual change control**
- **Complex parallel separation of duties**
- **Typically one perimeter to defend or can cause firewalls to be the greatest expense in a project.**

Compartmentalized Network Architecture

- **Typically a transport, interconnecting systems and infrastructure to support a business effort.**
- **Typically controlled by a multi-tiered approach such that any single failure will not lead to a compromise of an asset. Typically comprised of router filters, firewalls, host security, application security.**
- **Access controlled based on need.**

Network Implementation Philosophies

- **Internet was implemented from the bottom – up according to RFC's.**
- **E-commerce typically managed from the top – down**
- **An engineering organization has to fully understand the network big picture in order to manage it (health management).**

Centralize or De-centralize?

- **Security entrepreneurs hawk both extremes in the name of sound risk management.**
- **Centralized network management can be a blessing or a curse depending on how it is implemented and by who. One implementation can have an inverse risk factor from another seemingly identical one.**
- **Centralized management can bring global disaster.**

1980 and Before:

- **Xerox mass markets first, really useful, personal computer named “LISA” for about $5000.**
- **128K Macintosh becomes first computer to be educated about *people*.**
- **5 meg hard drive cost is around $2000.00.**
- **Memory consisted of little ferrite cores (donuts) with wires through them.**
- **No *practical* networks exist.**

Circa 1980 Computer Security

- Social engineering was common & involved getting the *mark* to actually *DO* something.
- 2600 was the in-band signaling (on-hook/off-hook) frequency for SF units.
- Phone *phreaks* mainly viewed as a nuisance.

Circa 1980 Computer Security (cont'd)

- **Phone *phreaks* typically under 21 years old.**
- **Typical hacker definition included creative techno-geeks.**
- **Hacker bulletin board systems emerge – *"The more you give, the more you get"***
- **Inside *jobs* never spoken of in public.**

Circa 1980 Computer Security (cont'd)

- **Almost all data communications via phone using an acoustic coupler**
- **Hop-on-hop-off used as creative way to *shift* phone costs to someone else.**
- **There were no computer banners.**
- **Law typically 10 years behind technology.**
- **Disaster recovery gains significance.**

1985 – 1990

- **ihnp4, at Indian Hill is the primary E-mail hub of the world, typically via uucp.**
- **Distributed computing emerges.**
- **Networks of networks start to evolve.**
- **Corporations embrace UNIX technology.**

1985 – 1990 (cont'd)

- **Host files becoming unmanageable, DNS emerges**
- **Sun is distributed computing leader.**
- **Lucky guy named Kevin wins many large prizes in radio contests.**

1985 - 1990 Computer Security

- **Over 100 '*T*' and Robins AFB systems compromised.**
- **Shadow Hawk (~1987) - $1300 monthly phone bill.**
- **Internet Worm by RTM, son of NSA Chief Computer Security Scientist, raises awareness.**
- **6000+ systems affected, Corporate world freaks out! TCP gains popularity.**
- **Astronomer Cliff Stoll finds computer accounting discrepancy of 75 cents.**

1985 - 1990 Computer Security (cont'd)

- **Kevin Paulson & Kevin Mitnick assist PacBell in providing telephone service.**
- **One opens recording studio.**
- **Cliff Stoll raises FBI's technology awareness.**
- **Cliff Stoll provides lesson to Mitre.**
- **SS7 Signaling problems arise. Major TELCO service loss.**
- **STP and NCP vulnerabilities identified**

1985 - 1990 Computer Security (cont'd)

- **Legion of Doom;**
- **Lenny Rose;**
- **EFF Established;**
- **Encryption techniques strengthened;**
- **Inside *jobs* still not spoken of;**
- **Steve Jackson Games (Set trip wires!) PPA of 1951.**
- **Electronic publishing & first amendment**

Circa 2000

- **Internet used as primary transport for almost all communications (VPN's, SSH, & SSL)**
- **Organized crime adopts PGP and PGP PHONE as their standard.**
- **dob learns underground stock trading BBS's more profitable than following hacker BBS's**

Circa 2000 E-commerce Security

- **Denial of service attacks start**
  - **Ping O Death**
- **Distributed denial of service attacks start.**
- **Dangerous macro executables included with attachments – (Love, Resume, next mutant)**
- **Strong(er) encryption standards adopted.**

Circa 2000 E-commerce Security (cont'd)

- **Passwords still being used as main authenticator.**
- ***Mother's Maiden Name* used for primary call center authentication.**
- **Mormon Church ancestry web site receives record web hits.**

Circa 2010

- **Last telephone disconnected.**
- **All computers on planet inter-connected to form a single virtual computer.**
- **Entire world-wide distributed network becomes centrally managed.**
- **Ethics, morality, and respect become mandatory part of education process.**
- **United Nations changes name to United Federation of Planets.**
- **Microsoft monopoly case still in progress.**

Circa 2010 Computer Security

- **First major LINUX worm/virus causes massive SNMP reconfiguration (September 2001)**
- **Investor BBS's being investigated as means of stock manipulation by day traders.**
- ***United Federation of Planets* takes over policing of the Internet.**
- **All computers on the planet have disks reformatted via integrated network management system configuration error!**
- **Last pedophile reprogrammed.**

THE END

citigroup