ISE® North America Executive Forum

Keynote Presentation

Security's Dirty Little Secrets

William Hugh Murray, CISSP

William Hugh Murray

Bill Murray is a management consultant and trainer in Information Assurance specializing in policy, governance, and applications. He is Certified Information Security Professional (CISSP) . He has more than fifty years experience in information technology and more than forty years in security. During more than twenty-five years with IBM his management responsibilities included development of access control programs, advising IBM customers on security, and the articulation of the IBM security product plan. He is the author of the IBM publication Information System Security Controls and Procedures. He has been recognized as a founder of the systems audit field and by Information Security Magazine as a Pioneer in Computer Security. In 1999 he was elected a Distinguished Fellow of the Information System Security Association. In 2007 he received the Harold F. Tipton Award in recognition of his lifetime achievement and contribution.

Security's Dirty Little Secrets

"Look, Daddy, the Emperor's naked!"

This presentation will identify and expose things that we, that is, security executives, all know to be true, pretend that they are not. and consistently fail to address. These things represent flaws in the way we think. They are impediments to the way we act. They contribute to, may be the cause of, our current state of insecurity and its resistance to improvement.

Hopefully, exposing these things will enable us to address them. It will empower us to make changes that otherwise seem impossible. The presentation will make suggestions and attempt to justify them.

“M&M” Security

Hard and crunchy on the outside…

…soft and chewy on the inside.

- *Flat network*
- *Any to any connectivity*
- *Open ports*
- *Permissive policies*
- *Mutually trusting nodes*

Retail Payment System is Broken

- Mag-stripe stores and passes credit card numbers in the clear
- Credit card are vulnerable to fraudulent re-use
  - “card not present” (e-commerce) transactions
  - counterfeit mag-stripe cards (ATMs, POS
- Millions of vulnerable merchant systems
  - Tens of millions of users
  - Third-party provided hardware and software
  - Remote access
  - Weak user authentication
  - Flat enterprise network
- PCI DSS is a “Band-Aid”
- EMV is too little, too late
- Few EMV cards, even those have mag-stripes

Continued Reliance on Reusable Credentials

Target

Neiman-Marcus

P. F. Chang

UPS Store

Home Depot

eBay

JP Morgan Chase

Dairy Queen

Kmart

Staples

et. al.

What do these all have in common?

- *Breached*
- *But we know about it*
- *Retailers?*
- *"Bricks and Mortar?"*
- *Remote Access*
- *Gullible users*
- ***Weak authentication!***
- *Flat networks*
- *Of mutually trusting systems*

Orphan Data

"No mama, no papa, no Uncle Sam…"

- No asset inventory
- No classification
- Enterprise data copies on
  - Desktops
  - Laptops
  - Forgotten servers
  - User-owned devices
  - Other

Perfect as the Enemy of the Good

"I know how to break that!"

Of course you do.

You also know how to break passwords but you continue to rely on them.

This argument is only used against mechanisms that we are not already using.

e.g., Token-based one-time-passwords.

Tolerance for Unchecked Inputs

Buffer overflows

SQL Injection

Stack overflows

Cross-site scripting

Other

von Neumann Architecture

Operating systems

Languages

APIs

Input editors

Escape mechanisms

Education

Training

Supervision

Accountability

Glorification of Rogue Hackers

- Landreth
- Mitnick
- Morris
- Murphy
- Lamos
- Zatko
- Abignale
- et. al.

Hacking :

- Starts with an adrenaline rush
- Is addictive
- Escalates
- Recidivism is high
- Referred to in the media as "research"
- "Researchers" are even hired by government and law enforcement

Irresponsible Disclosure

- Shellshock
- Bugzilla
- Heartbleed
- MBTA Charlie Card
- BEAST

- “NVPs “
- Vulnerabilities
- Exploit code
- Market
- Reduces Cost of attack
- No other industry does this

Tolerance for chewing gum and duct tape

Microsoft Windows

Microsoft Internet Explorer

Adobe Reader

Adobe Flash

Oracle Java

Google Chrome

Mozilla Firefox

Wordpress

Sources of vulnerability

- Backwards compatibility
- Permissive policies
- Gratuitous features and functions
- Late and incomplete binding
- User programming
- Preference for early over good
- Poorly understood and expressed security requirements
- Security rather than securability
- False economics
- General tolerance for shoddy

Failure to Measure

"Most under-measured function in American Enterprise."

- William Thomson
- W. Edwards Deming
- Indicator of functional maturity
- View as binary

Lessons Learned/Best Practices

- ***Restrictive policies***
  - *zero trust*
  - *mutually suspicious*
  - *least privilege*
  - *Application only*
- ***Exploit Cheap Hardware***
  - *Firewalls*
  - *Proxies*
  - *Mobiles*
- ***Strong Authentication***
  - *Token based*
  - *Out of band*
  - *EINs , MAC addresses*
  - *2-way SSL*

Lessons Learned/Best Practices

End-to-end Crypto by default

- *TLS*
- *IPSEC*
- *VPN*
- *Terminate on the application*

One-time Digital Tokens for PCI

- *"Chip" (EMV) card*
- ***Visa (EMV) Token Service***
- *e.g., Apple Pay (via "Near Field Communication" to "contactless" reader)*
- *e.g., Square Wallet (via QR Tag to Starbucks optical reader)*
- *Mag-stripe emulation (MST) to mag-stripe readers.*

Lessons Learned/Best Practices

Resist System Contamination

- "write" *Access Control ("lockdown")*
- *Microsoft EMET (Enhanced Mitigation Experience Toolkit)*
- *TripWire*
- *Strongly Typed Data Objects (iOS, AS/400)*
- *Isolate*

Measure and report

- *Policy*
- *Standards*
- *Service Level*
- *Time to breach or compromise, detection, mitigation*
- *Risk*