He is your friend, your partner, your defender, your dog.

You are his life, his love, his leader. He will be yours, faithful and true, to the last beat of his heart. You owe it to him to be worthy of such devotion.

Sentry Dogs Remembered:  http://cybersd.com/sd/
Everything I know about Information Security, I learned from my Sentry Dog

http://www.youtube.com/watch?v=u_23RoeJfI0
https://www.youtube.com/watch?v=ZqD4Fx5P86w

Ed Crowley, Sentry Dog Handler
US Army ‘69-’71
Today’s Topics

- Learning from a Sentry Dog
- Learning from NIST
  - Cybersecurity Framework
- Understanding Current Context
- Models: OODA, Risk
- Security Identification. Why so Hard?
- Security, Deterrence, and Accountability
- A Simple Risk Model
  - Risk and Risk Primitives
  - Selected Threats and Vulnerabilities
- Summary
- For Further Study
Selected Qualifications

- Certified Ethical Hacker – EcCouncil
- AccessData Certified Examiner – AccessData Forensic Tool Kit (FTK)
- Certified Information Systems Security Professional (CISSP) – ISC²
- Security +, Internet +, Network + -- CompTIA
- Usual Cisco, Microsoft, and Novell Certifications
- Graduate:
  - USARPAC Basic Sentry Dog School
  - US Army Military Police Academy

(http://www.youtube.com/user/bigredd21)
War Dogs ‘69

- Training intense
- Working conditions deplorable
- Lives always on the line
- ... Rewards non-existent [1.]

267th Chemical, Sentry Dog Platoon

3.2 mile perimeter. 10 meter dead area. One gate, locked and manned 24/7. Highest hill on south Okinawa. Overlooked Kadena Air Base. Enough Nerve Gas to kill everyone in the world three times.

Ref: 267th Chemical Company or Operation Red Hat
What did we protect? Nerve Gas

VX (nerve agent)
From Wikipedia, the free encyclopedia

VX, IUPAC name O-ethyl S-[2-(diisopropylamino)ethyl] methylphosphonothioate, is an extremely toxic substance whose only application is in chemical warfare as a nerve agent. As a chemical weapon, it is classified as a weapon of mass destruction by the United Nations in UN Resolution 687. The production and stockpiling of VX was outlawed by the Chemical Weapons Convention of 1993.

**Biological effects**

Further information: Nerve agent biological effects and treatment

VX is the most toxic nerve agent ever synthesized for which activity has been independently confirmed. The median lethal dose (LD_{50}) for humans is estimated to be about 10 milligrams through skin contact and the LCT_{50} for inhalation is estimated to be 30–50 mg·min/m².
Training Hazards

The process of training sentry dogs was not without its share of hazards. “In the early years, the dogs were trained as ‘attack’ dogs and were known to attack almost anything, including their handler.”15 It was considered a rite of passage for a sentry dog handler to suffer his first bite from his own dog. As the program developed, however, so did the methods of training dogs. By 1969, “the dogs were beginning to be trained as ‘patrol dogs’, much like the dogs in today’s police departments. They were trained to not attack until commanded to do so, or if the handler was in duress.”16 It was because of this aggressiveness training that dogs were not permitted to return to CONUS with their handlers upon completion of their tour of duty. The military did not believe that a sentry dog could be untrained and was not willing to risk releasing the dog into civilian life.

Employment

One of the biggest problems facing the sentry dog program was ignorance on the part of base and installation commanders as to how to best employ their new security:

Lessons Learned

As explained by this representative the Air Force has found the patrol dog to be very effective, primarily because of its great versatility. The capabilities of the sentry dog are basically to detect unauthorized penetrators, alert, and if necessary, pursue and attack the intruder. He is trained to attack savagely and to be distrustful of all persons other than his handler. As a result, he cannot be used with any degree of safety for any function other than patrolling isolated areas of an installation. On the other hand, the patrol dog has the same capabilities as the sentry dog to detect and alarm plus numerous other abilities. He
Lessons Learned

- Poorly led and poorly utilized most security groups are...
  - Cost of security: easy to understand.
  - Cost of compromise: difficult to understand

- While security vulnerabilities are real, the feeling of security may be an illusion.
  - Well meaning insiders can make lethal mistakes.

- Constant improvement i.e. lessons learned are critical.
  - Security environment evolves constantly, if you don’t, you are getting behind.
What I Learned from my Sentry Dog

1. Identifying your environment (assets, vulnerabilities, threats) is critical.

2. Effective protection requires constant education, awareness, and training.

3. An undetected intrusion, is one you can’t respond to...

4. Effective response includes planning, analysis, deterrence, and mitigation.

5. Back up/ Recovery plans always needed
Five NIST Cybersecurity Framework Functions

- **IDENTIFY**
  - Asset management
  - Business environment
  - Governance
  - Risk assessment
  - Risk management strategy

- **PROTECT**
  - Access control
  - Awareness and training
  - Data security
  - Information protection and procedures
  - Maintenance
  - Protective technology

- **DETECT**
  - Anomalies and events
  - Security continuous monitoring
  - Detection process

- **RESPOND**
  - Response planning
  - Communications
  - Analysis
  - Mitigation
  - Improvements

- **RECOVER**
  - Recovery planning
  - Improvements
  - Communications

• Resemble the five things I learned from my Sentry Dog?

• NIST Cybersecurity Framework at:
Current State of Computer Security

- Computer security today is in bad shape:
  - People worry about it a lot
  - Spend a good deal of money
  - Most systems remain insecure.

Primarily because:

- Users don’t understand security or security models.
- Security is about “risk management.” That is, balancing the loss from breaches against the costs of security.
  - Difficult to quantify.

*Examples on next two slides.*
The costs either of getting security or of not having it are not known so users don’t care much…

Consequently, vendors don’t have any incentive to make usable security.

Many users can’t distinguish between the feeling of security and actually being secure.

Butler Lampson

Information systems are a complex, “target-rich” environment comprised of technology, processes, and people.

Security is asymmetric. That is, a defender must be right every time, every way.

- An attacker only has to be right one time, one way.

Three golden rules to ensure computer security*:

1. Do not own a computer;
2. Do not power it on;
3. Do not use it.

—Robert H. Morris*

*Former Chief Scientist of the National Computer Security Center (early 80’s)
Physical Security: Mature and well established.
Digital Security: relatively new. Arguably not well established.

- 1970, new security issues surfaced, OpsSec created
- 1980, more new security issues, CompSec created
- 1990, still more new security issues, CommSec created
- 2000, and still more new security issues, Information Assurance created
- 2010, yet more new security issues, Homeland Security created
- 2014, NIST Framework for Improving Critical Infrastructure Cybersecurity created…

Anyone see a pattern?

Consequently, cyber security is populated by professionals with different and sometimes seemingly incompatible backgrounds, perspectives, goals, and visions.
As a Sentry Dog Handler, I observed and analyzed my Dog’s alerts. Greatly increasing my ability to detect and respond to intrusions.
Information Security Awareness

Why so Elusive?

Consider two different concepts that map to the same word (Security)

1. Feeling
2. Reality

These qualities are separate and distinct.

- In addition, many terms have vague or poorly understood definitions.

These two different qualities create four possible states.
Four Possible Security States

Think that you are Secure

Think that you are Insecure

Be Secure

Real Security

Illusion

Be Insecure

Illusion

Real Insecurity
To be secure or to feel secure? That is the question.
Security Products

- Market drives security
- People make tradeoffs on their feelings of security
- A smart security company makes products that make people feel secure?
  - Cheap and easy

https://www.youtube.com/watch?v=yoxo_B091bY

Another alternative:

1. Actually make products that make people secure. Hope that they notice.
   - Expensive and hard.

ADE 651 fake bomb detector
Sold to 20 countries in the Middle East and Far East, including Iraq and Afghanistan, for as much as $60,000 per unit.

The Iraqi government is said to have spent £52 million ($85 million) on the devices.

http://en.wikipedia.org/wiki/ADE_651
Security Theater

- A situation where actions are taken to make people feel secure without making them more secure.

- Security Theater Video
  [http://www.youtube.com/watch?v=GC5NBGx00H4&feature=BF&list=PL5E19028F267592B8&index=1](http://www.youtube.com/watch?v=GC5NBGx00H4&feature=BF&list=PL5E19028F267592B8&index=1)

- Feeling Secure?
Two Questions

What makes people not notice the difference between feeling secure and being secure?

• An inappropriate understanding
  • Based upon an inappropriate model...

• Lack of understanding produces an inadequate correlation between feeling and reality...
  • If you don’t know what security is, how can you increase it?
Daily, humans make security tradeoffs.

You might think that humans would be good at information security tradeoffs.…

But, you would be wrong.

Why?

Because, without training, humans respond to the feeling rather than the reality of security.

That is, human security model stuck in cave man era.
Security and Deterrence

• People that think that physical security is based on locks are wrong.
  • Locks don’t protect your house from a burglar.
    • Locks slow burglars down.
• What protects your house is deterrence.
  • While the chance of a burglar getting caught may be small, punishment is significant.
  • Consequently, for the most part, burglary is deterred.
Effective Deterrence: An Example[1]

Patrol Dog versus Sentry Dog

What is the difference between patrol and sentry dogs? The easy way is to explain the use of force rules. When a sentry dog was released the situation had evolved to the point that deadly force was also authorized. You could shoot firearms, throw grenades, explode claymore land mines, call in air support, call in artillery, or release the sentry dog to attack (if you really wanted to hurt him). A patrol dog is considered minimal force. If the situation has evolved to the point that


Accountability and the Internet?

- On the Internet, do we have accountability?
  - Without accountability, is deterrence possible?
- Do we have the ability to attribute a ‘cyber attack’ to a particular entity?
- Do we even have a commonly accepted definition of “Cyber Attack?”

_from the OECD’s “Reducing Systemic Cybersecurity Risk” by Peter Sommer._

[www.oecd.org/dataoecd/57/44/46889922.pdf](http://www.oecd.org/dataoecd/57/44/46889922.pdf) (PDF Format)
A Simple Risk Model

You are not born with a Cyber Security Risk Model...

- In contrast, a German Shepherd is born with an effective physical security model.

- Models provide means to move feeling and reality closer together
  - How can we model risk?
  - First, let's define our terms...
Risk and Risk Primitives

- **Vulnerability**
  - A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security …

- **Threat**
  - Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

- **Asset**
  - A definable piece of information, stored in any manner which is recognized as 'valuable' to the organization.

- **Risk**
  - The probability that a particular threat will exploit a particular vulnerability …

**NCSC-TG-004 Aqua Book**

See also RFC 2828

*If you know your assets, threats, and vulnerabilities, you can calculate your risk.*

In security, defining terms are important because, as we have seen, the same terms can have different meanings to different people.

A metric consisting of your enterprise's threats, vulnerabilities, and assets at a particular time would be called your security posture. Normally determined through a Risk Assessment.

For any given situation, the risk is proportional to the area of a triangle formed by the assets to be protected, the threats to the assets, and the current vulnerabilities.

- In security, defining terms are important because, as we have seen, the same terms can have different meanings to different people.
- A metric consisting of your enterprise's threats, vulnerabilities, and assets at a particular time would be called your security posture. Normally determined through a Risk Assessment.
Selected Threats

- Cloud computing illustrates a serious gap between technology implementation and the skills necessary to provide security. More than 50 percent of information security professionals reported having private clouds in place, and more than 40 percent of respondents reported using software as a service, but more than 70 percent of professionals reported the need for new skills to properly secure cloud-based technologies.

Figure 2—Top Security Threat Concerns

- Application vulnerabilities: 73%
- Mobile devices: 66%
- Viruses and worm attacks: 65%
- Internal employees: 63%
- Hackers: 55%
- Contractors: 45%
- Cyber terrorism: 44%
- Cloud-based services: 43%
- Organized crime: 38%
Knowledge is free.
We are anonymous.
We are legion.
We do not forgive.
We do not forget.
Expect us.

http://www.youtube.com/watch?v=ny1vT9A9RBC
Are criminal hackers different than ordinary criminals?

Who benefits from that feeling?
Threats Examples: Old School

Adrian Lamo
Kevin Mitnick
Kevin Poulsen

Alexey Ivanov
Vasiliy Gorshkov

Robert Hanssen
John Walker

Gary McKinnon
Mafia Boy
Vulnerabilities?

- People
  - Lack of situational awareness
  - Social engineering
  - Insiders (bribes, incompetence…)

- Processes
  - Online Financial Transactions
  - Conventional Financial Transactions
  - Credit, debit, and ATM cards

- Technology
  - Computer and Communications Systems
  - Point of sale terminals
  - VA databases, etc…

- Vulnerabilities are Dynamic
- Typically, people would be considered the weakest link.

Any organization can be modeled using a PPT model.
Technical Countermeasures

If you think technology can solve your security problems, then:
You don’t understand the problems
and
You don’t understand the technology.

B. Schneier
Technical Countermeasure: An Example
Summary

- To a lay person, the illusion of security is indistinguishable from actually being secure.
- Security is hard.
  - Doesn’t occur by accident.
- Physical security different than information security.
  - Cybersecurity draws practitioners from a wide variety of fields.
  - Draws many snake oil practitioners as well…
- Current digital environment is rapidly evolving.
- Perfect security not possible.
  - No technological silver bullets!
- Training/Models help with understanding and communicating security.
Questions???

Thanks for listening!
Stay safe! Ed Crowley

--following are some slides that I’ve removed from this presentation. But I may add them into future presentations.....
For Further Study

**ISC² Common Body of Knowledge**

- **Access Control**
  - Categories and Controls
  - Control Threats and countermeasures

- **Application Development Security**
  - Software Based Controls
  - Software Development Lifecycle and Principles

- **Business Continuity and Disaster Recovery Planning**
  - Response and Recovery Plans
  - Restoration Activities

- **Cryptography**
  - Basic Concepts and Algorithms
  - Cryptography standards and algorithms
  - Signatures and Certification
  - Cryptanalysis

- **Information Security Governance and Risk Management**
  - Policies, Standards, Guidelines and Procedures
  - Risk Management Tools and Practices
  - Planning and Organization

- **Legal, Regulations, Investigations and Compliance**
  - Major Legal Systems
  - Common and Civil Law
  - Regulations, Laws and Information Security

- **Operations Security**
  - Media, Backups and Change Control Management
  - Controls Categories

- **Physical (Environmental) Security**
  - Layered Physical Defense and Entry Points
  - Site Location Principles

- **Security Architecture and Design**
  - Principles and Benefits
  - Trusted Systems and Computing Base
  - System and Enterprise Architecture

- **Telecommunications and Network Security**
  - Network Security Concepts and Risks
  - Business Goals and Network Security
Network Solutions warns merchants after hack

Queensland Police plans wardriving mission

MI6 chief blows his cover as wife's Facebook account reveals family holidays, showbiz friends and links to David Irving

Security Guard Busted For Hacking Hospital's HVAC, Patient Information Computers

'GhostExodus' bragged about his breaches on YouTube, and tried to rally fellow hackers to conduct a massive DDoS attack
Miyamoto Musashi, Ronin

- Do not intend to rely on anything
- Respect the gods and Buddhas, do not depend on them
- Do not regret things about your own personal life
- Do not lament parting on any road whatsoever
- Do not be fond of material things
- Though you give up your life, do not give up your honor
- Never stray from the Way.

*From The Way of Walking Alone by Musashi... (1645)*
Identity Theft


Your most important weapon is the one between your ears.
Figure 1. Most Common IC3 Complaint Categories, U.S. and Alaska, 2010

<table>
<thead>
<tr>
<th>Category</th>
<th>U.S.</th>
<th>Alaska</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-delivery merchandise/payment</td>
<td>21.1</td>
<td>15.9</td>
</tr>
<tr>
<td>Identity theft</td>
<td>16.6</td>
<td>14.9</td>
</tr>
<tr>
<td>Auction fraud</td>
<td>5.3</td>
<td>10.1</td>
</tr>
<tr>
<td>Credit card fraud</td>
<td>9.3</td>
<td>9.3</td>
</tr>
<tr>
<td>Miscellaneous fraud</td>
<td>7.7</td>
<td>7.0</td>
</tr>
<tr>
<td>Computer crime/intrusion/hacking</td>
<td>6.1</td>
<td>4.4</td>
</tr>
<tr>
<td>Advance fee fraud</td>
<td>3.2</td>
<td>4.1</td>
</tr>
<tr>
<td>Spam</td>
<td>4.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Overpayment fraud</td>
<td>3.6</td>
<td>4.1</td>
</tr>
<tr>
<td>FBI-Related Scam</td>
<td>3.9</td>
<td>3.4</td>
</tr>
</tbody>
</table>

Percentage of total complaints received

Figure 2: Most common and most disruptive form of cyber-attack?

- Malicious software (virus)
- Denial of Service attack
- Other
- Data theft
- Insider information theft - including of HFT source code
- Account takeover/authorized financial transactions
- Financial theft

‘Other’ forms of common attacks reported related to: SQL Injection, Laptop Theft, Website Defacement attempts, Port scanning and spam emails, Phishing email attack, social engineering, Website scanning.

‘Other’ forms of disruptive threats included: Website defacement attempts, Port scanning and spam emails, Self-replicating email virus, Advanced Persistent threats, infrastructure damaging threats.

Source of data: 2010 Internet Crime Report

Motivations Behind Attacks
February 2013

- Hacktivism 31%
- Cyber Crime 56%
- Cyber Espionage 3%
- Cyber War 9%
- Cyber Espionage 1%
- Art?