Summer Workshop on Cyber Security

Friday 18 July, 2014
Instructor: Fred L. Wilson

Texas Tech University and Angelo State University
July 14-18, 2014

Supported by National Science Foundation
Cybersecurity

Dr. Fred L. Wilson
Professor Emeritus, Rochester Institute of Technology

- Department of Physics and Geosciences
- Angelo State University
- fwilson@angelo.edu

Summer Workshop on Cyber Security July 14-18, 2014 TTU & ASU
Cybersecurity from an Intelligence Perspective
Cybersecurity from an Intelligence Perspective

Summer Workshop on Cyber Security July 14-18, 2014 TTU & ASU
Robert “Bud” McFarlane

Robert "Bud" McFarlane served as national security adviser to President Ronald Reagan from 1983 to 1985. During that time the administration faced the deadly attack on the U.S. Marine barracks in Beirut; the abduction of the CIA's Beirut station chief, William Buckley; the bombing of the U.S. embassy annex in Beirut; the hijacking of TWA 847; and the commandeering of the Achille Lauro in the Mediterranean Sea.
Cybersecurity

• The events of Sept. 11 2001 proved that terror attacks on nonmilitary targets could be crippling to our national infrastructure.

• A week after the first anniversary of the day that changed everything, the White House released a 60-page draft plan called the National Strategy to Secure Cyberspace, which also points out that US businesses--and individuals--are potential targets for cyber-terrorism.
What is Cybersecurity?

Cybersecurity is Cyberspace is a worldwide network of computers and the equipment that connects them, which by its very design is free and open to the public (the Internet)

We’ve become increasingly dependent on the net, and it’s being used right now to transfer everything from friendly e-mail to extremely sensitive data.

Cybersecurity is far more than software antifragility. It encompasses every part of the system.
Exercise

• I Am the National Intelligence Advisor, and have access to more information than agencies have.
• You will be CIA, FBI, DIA, Cybersecurity Command, NSA, and Homeland Security.
• Group yourselves in your agency.
Situation

**NSA**

• NSA has worked with Cybersecurity Command to form a list of the most wanted cyberterrorists. At the top of the list is an unknown hacker known only as “MC.” A. J. Kahn is second on the list.
MTAC is Attacked

• Meanwhile DIA has determined that the **Multiple Threat Alert Center** or MTAC has been attacked. It is clear that there was unauthorized access. MTAC is a room which used to keep track of ongoing persons or groups under investigation. The room also has a console where various small screens above the console enable the techs to see a live video feed of events as they happen.
MTAC

• In the center of the room is a large screen which various agents including use to hold conference-calls with members of other agencies including the CIA and FBI
Agent Has Died

• FBI determines that A. J. Kahn is the hacker who accessed MTAC. They also learn that an agent, James Hunt has been killed.
Homeland Security

- Homeland Security recognizes the work is that of a New York based terrorist cell
- HS wants to know who outed James Hunt.
Major Response Team

- The Major Response team captures Kahn who they believe was responsible for the attack on MTAC and thus Hunt’s death. On the most wanted cyberterrorist list and was also responsible for a cyber attack on MTAC which resulted in the death of an undercover agent.
• Analyzing the hacker's computer, agents are led to a warehouse where they find evidence of a bomb containing the Ebola virus having been built. Now it is even more essential to get the hacker to talk.
Hard Drive Analysis Productive

• An agent who is extremely tech savvy, plows through all of Kahn’s logic in order to arrive at the conclusion that indeed Khan *did* know MC’s IP address.
MC’s IP Address Gived Up

• 192.168.254.1
What’s Next?

• MC still has to be captured.
Why No Cyber “Pearl Harbor”

• Basic robustness of the system
• Lack of crippling targets for a single attack
• Resources available to cyber insurgents
What Part Is Most Vulnerable?

• “Cybercriminals are ditching the old strategy of exploiting software vulnerabilities, choosing instead to rely on deceit and deception, according to a new security report released this week.”

  • Jonathan Tan (May 16, 2014)
  • [http://www.techgoondu.com/2014/05/16/microsoft-hackers-using-deception-to-overcome-improved-cybersecurity/#.U7Gq07TIsxE](http://www.techgoondu.com/2014/05/16/microsoft-hackers-using-deception-to-overcome-improved-cybersecurity/#.U7Gq07TIsxE)
Far more likely we will have a “Benghazi” type attacks from insurgents.
Dragonfly
Cybersecurity

• Leadership must always start from a clear-eyed view of how things really are. Only then can we begin to address how we can get from where we are to where we need to be.
Antifragility

• The aim (or what should be the aim) of cybersecurity programs is to create a more resilient nation.
Anticipation-Response

Anticipation

Knowing what to EXPECT

Knowing what to LOOK FOR

Response

Knowing what to DO

Knowing what has HAPPENED

Monitoring

Learning

Summer Workshop on Cyber Security July 14-18, 2014 TTU & ASU
There were aircraft losses during the Vietnam War. Thousands of U.S. fixed-wing aircraft were lost to ground fire of antiaircraft artillery (AAA), surface-to-air missiles (SAMs), and fighter interceptors (MiG)s. The great majority of U.S. combat losses in all areas of Southeast Asia were to AAA. The Royal Australian Air Force also flew combat and airlift missions in South Vietnam, as did the Republic of Vietnam. Among fixed-wing aircraft, more F-4 Phantoms were lost than any other type in service with any nation.
Reason

- Navy and Air Force refused to coordinate tactics and intervention methods
- Avoidance was based on faulty assumptions
- Fragility was owing to old-fashioned technology instead of state-of-the-art missile technology
- Services were warned by DIA but chose to ignore intelligence analysis.
14 October 1965 - First Chinese Nuclear Test

• On 16 October 1964, the People’s Republic of China conducted its first nuclear test, making it the fifth nuclear-armed state
• At the outset, its efforts were backed by substantial Soviet assistance, including advisors and technical equipment.
• The third test in 1965 was an air burst
Policy Errors

- Contents of mushroom cloud contained lithium
- No need whatsoever for lithium in a pure fission device
- U.S. Army Basic Strategic Estimate ignored analysis that specified the weapon must be a boosted weapon
Rationale?

• “It is against Army policy for the Chinese to have such a weapon, therefore you cannot make that statement in an analysis.”

• Personal statement to me by a Lt. Col. In 1965
High-level Software Design

Customer order products scenario rattikorn.hewett@ttu.edu

Customer Interface

Material Requirements Planning

Master Production Schedule

Bill of Material

Job shop simulator

Login

Validate Login

no

yes

Browse product

Place Product Order

Verify Order and Charge

yes

no

Cancel

Update Demands & Input Parameters

Schedule Product Plan

Determine Parts Requirements

Simulate Parts/Products Manufacturing

Record Material Order

Place Material Order

Record Finished Products

Record Orders

Billing to Customer

CI

MRP

MPS

BOM

JOB

Record

Finished Products

Customer Interface

Material Requirements Planning

Master Production Schedule

Bill of Material

Job shop simulator
Customer orders products (0.4)

Manager adjusts demands/requirements (0.2)

Supplier acknowledges material order (0.4)
Drawdown Curves

Figure 4-1. *Drawdown Curve and Attack Price of a BMD System*

Probability of target survival (percent)

Number of attacking RVs

Attack price

Summer Workshop on Cyber Security July 14-18, 2014 TTU & ASU
Follow-On or Simultaneous

\[ p(t) = p_1 \times p_2 = 0.85 \times 0.85 = 0.72 \]
Drawdown Curves

Figure 4-1. *Drawdown Curve and Attack Price of a BMD System*

Probability of target survival (percent)

Number of attacking RVs

**Attack price**
Complications

- 1. Cost to attacker
- 2. Weakest Link
- 3. Achilles’ Heels
- 4. Conservative estimates
- 5. Expectation value vs. likely outcomes
- 6. Sophistication of attackers
- 7. Cost to defense
- 8. Deliberately weak defense
Complications

1. Cost to attacker
2. Weakest Link
3. Achilles’ Heels
4. Conservative estimates
5. Expectation value vs. likely outcomes
6. Sophistication of attackers
7. Cost to defense
8. Deliberately weak defense
Probabilistic Model

Probability density function:

\[
\text{In[1]}:= \text{Plot[Table[PDF[MaxwellDistribution[\sigma], x], \{\sigma, \{.5, .75, 1.5\}\}],}
\]
\[
\{x, 0, 5\}, \text{Filling -> Axis, PlotRange -> All}\]

\[
\text{Out[1]}=
\]
Complications

1. Cost to attacker
2. Weakest Link
3. Achilles’ Heels
4. Conservative estimates
5. Expectation value vs. likely outcomes
6. Sophistication of attackers
7. Cost to defense
8. Deliberately weak defense
Figure 4-4. Catastrophic Failure of the Defense Because of an Achilles’ Heel

Targets surviving (percent)

Performance if offense exploits Achilles’ heel

Performance against all other tactics

Achilles Heel

Summer Workshop on Cyber Security July 14-18, 2014 TTU & ASU
Complications

• 1. Cost to attacker
• 2. Weakest Link
• 3. Achilles’ Heels
• 4. Conservative estimates
• 5. Expectation value vs. likely outcomes
• 6. Sophistication of attackers
• 7. Cost to defense
• 8. Deliberately weak defense
Offensive vs. Defense

![Graph showing the comparison between targets surviving (percent) and attack intensity (RVs per aimpoint). The graph compares the 'Offense view' and the 'Defense view.'](Image)
Complications

• 1. Cost to attacker
• 2. Weakest Link
• 3. Achilles’ Heels
• 4. Conservative estimates
• 5. *Expectation value vs. likely outcomes*
• 6. Sophistication of attackers
• 7. Cost to defense
• 8. Deliberately weak defense
Probabilistic Model

Probability density function:

\[
\text{In[1]:=} \quad \text{Plot}[\text{Evaluate@Table[PDF[MaxwellDistribution[\sigma, x], \{\sigma, \{0.5, 0.75, 1.5\}\}, \{x, 0, 5\}], Filling \to \text{Axis}, \text{PlotRange} \to \text{All}]}
\]
Complications

• 1. Cost to attacker
• 2. Weakest Link
• 3. Achilles’ Heels
• 4. Conservative estimates
• 5. Expectation value vs. likely outcomes
• 6. Sophistication of attackers
• 7. Cost to defense
• 8. Deliberately weak defense
Complications

• 1. Cost to attacker
• 2. Weakest Link
• 3. Achilles’ Heels
• 4. Conservative estimates
• 5. Expectation value vs. likely outcomes
• 6. Sophistication of attackers
• 7. Cost to defense
• 8. Deliberately weak defense
Complications

1. Cost to attacker
2. Weakest Link
3. Achilles’ Heels
4. Conservative estimates
5. Expectation value vs. likely outcomes
6. Sophistication of attackers
7. Cost to defense
8. Deliberately weak defense
Overall Vulnerability

Components of System

• Software analysis considers at most two components of vulnerability

• Vulnerability may be analyzed probabilistically
Probability Analysis

Probability Distribution

\[ R_\pi = \frac{A}{\frac{B}{\pi} e^{-1}} \]

Terms

- R is risk (normalized 0 < R < 1)
- \( \pi \) is probability of failure
- A, B are normalizing constants
- R is actually a probability density, where the integral overall values of \( \pi \) yields 1.
Probabilistic Model

Probability density function:

In[1]:= Plot[Evaluate@Table[PDF[MaxwellDistribution[\[sigma], x], \{\[sigma], (.5, .75, 1.5)\}], \{x, 0, 5\}, Filling \[Rule] Axis, PlotRange \[Rule] All]

Out[1]=

![Graph of probability density functions](image-url)
Example of Environmental Analysis

Red = High Hazard
Yellow = Medium Hazard
Green = Low Hazard
Blue = Unbroken

Fig. 2. Sample output from detailed explosive analysis: glazing hazard in existing facility (left) and glazing hazard in upgraded facility (right)
Levels of Risk

• A combination of the impact of loss rating and the vulnerability rating can be used to evaluate the potential risk to the facility from a given threat.
Levels of Risk

• A sample risk matrix is depicted. High risks are designated by the red cells, moderate risks by the yellow cells, and low risks by the green cells.
Federal Security Risk Management

**Federal Security Risk Management**

- Identity Assets and Mission
- Determine Credible Threats
- Vulnerability to Threat
  - Impact of Loss: Very High, High, Moderate, Low
  - Devastating, Severe, Noticeable, Minor
- Risk Rating Interpretation
  - These risks are very high. Countermeasures recommended to mitigate these risks should be implemented as soon as possible.
  - These risks are moderate. Countermeasures implementation should be planned in the near future.
  - These risks are low. Countermeasures implementation will enhance security, but is of less urgency than the above risks.

**Determine Risk Level for Each Threat**

**Determine Acceptability of Risk**

**Purpose**

1. To evaluate the risk to the facility.
2. To quantify risk and establish what risks are acceptable.
3. To determine what measures and costs are required to reduce unacceptable risks to an acceptable level.

**Flowchart depicting the basic risk assessment process**
Always-On, High Speed

• “The problem has gotten more prevalent with always-on, high-speed internet access. Attackers are always out there looking for that type of computer.”

  » -- Stanley Konter, CEO of Savannah’s Sabre Technologies

Cybersecurity
What is Cyberspace?

• Konter is referring to the fact that whenever your computer is connected to the Internet, that connection goes both ways.

• Attackers are mostly malicious pranksters, looking to access personal and business machines, or disrupt net services with virus programs proliferated via e mail, most often, just to prove they can.
So What Does it Mean?

• “Cyberspace” is a metaphor for describing the non-physical terrain created by computer systems.

• Insurgents have three prerequisites for attacks
  – Opportunity
  – Motive
  – Means
Any Online System is in Cyberspace

• Online systems, create a cyberspace within which people can communicate with one another, do research, or simply window shop.

• Like physical space, cyberspace contains objects and different modes of transportation and delivery.

• Unlike real space, exploring cyberspace does not require any physical movement other than pressing keys on a keyboard or moving a mouse.
Cyberspace Battleground

• Every day we see an increase in the number of threats against critical infrastructures.
• These threats come in the forms of:
  – Hacking (computer intrusion)
  – Denial of service
  – Virus deployment
Cyber Attack Trends

Lower Sophistication

- Internet social engineering attacks
- Network sniffers
- Packet spoofing
- Session-hijacking
- Cyber-threats & bullying (not illegal in all jurisdictions)
- Automated probes and scans
- GUI intrusion tools
- Automated widespread attacks
- Widespread, distributed denial-of-service attacks
- Industrial espionage
- Executable code attacks (against browsers)
- Analysis of vulnerabilities in compiled software without source code

To Highest Sophistication

- Widespread attacks on DNS infrastructure
- Widespread attacks using NNTP to distribute attack
- "Stealth" and other advanced scanning techniques
- Windows-based remote access trojans (Back Orifice)
- Email propagation of malicious code
- Wide-scale trojan distribution
- Distributed attack tools
- Targeting of specific users
- Anti-forensic techniques
- Wide-scale use of worms
- Sophisticated botnet command and control attacks
Top 5 Emerging Cyber Threats

• 1. Malware (steady threat)
• 2. Social Engineering (rising threat)
• 3. Mobile devices (rising threat)
• 4. Data Loss (steady threat)
• 5. Internet attacks (rising threat)
We fail to have an adequate model for Cybersecurity in the face of insurgency.
Structure

- This is the “infrastructure,” and refers both to the system vulnerable to attack and to the mechanisms available to insurgents. It also includes existing environment of the system that makes it a target of insurgency.
Insurgency Trajectories

Preinsurgency 
- Days to years

Early (growth) 
- 3-5 years

Middle (mature) 
- 3-5 years

End (resolution) 
- 2+ years

Rapid insurgent victory

Poor government response

Decision by occupying power to withdraw

De facto insurgent political victory

Stalemate

Primary insurgency trajectories - Representative alternate paths

Preinsurgency activities include the emergence of insurgent leadership, creation of initial organizational infrastructure and possibly training, acquisition of resources, and unarmed, political actions, such as organized protests.

Insurgent strength is a subjective measure of the size of a movement, its ability to mount attacks and inflict causalities, popular support, logistics capacity, and/or territorial control. The insurgency trajectory will vary according to insurgent and government actions.

The decision by an occupying power to withdraw is commonly made four to seven years into the conflict.
Preinsurgency Trajectories

Preinsurgency activities include:

1. Emergence of insurgent leadership
2. Creation of initial organizational infrastructure and possibly training
3. Acquisition of resources
4. Political actions (organized protests.)
Preinsurgency

Trajectories

Insurgent Strength

- Insurgent strength is a subjective measure of:
  1. Size of a movement;
  2. Ability to mount attacks and inflict damage;
  3. Popular support;
  4. Logistics capacity;
  5. Structural control.

Preinsurgency activities include the emergence of insurgent leadership, creation of initial organizational infrastructure and possibly training, acquisition of resources, and unarmed, political actions, such as organized protests.

Insurgent strength is a subjective measure of the size of a movement. Its ability to mount attacks and inflict causalities, popular support, logistics capacity, and/or territorial control. The insurgency trajectory will vary according to insurgent and government actions.

The decision by an occupying power to withdraw is commonly made four to seven years into the conflict.
Preinsurgency

Trajectories

Decision to “Withdraw”

• The decision by system management to abandon the system is commonly made four to seven years into the onset of attacks:

---

Preinsurgency activities include the emergence of insurgent leadership, creation of initial organizational infrastructure and possibly training, acquisition of resources, and unarmed, political actions, such as organized protests.

Insurgent strength is a subjective measure of the size of a movement. Its ability to mount attacks and inflict causalities, popular support, logistics capacity, and/or territorial control. The insurgency trajectory will vary according to insurgent and government actions.

The decision by an occupying power to withdraw is commonly made four to seven years into the conflict.
Function

• This dimension concerns the processes by which an established authority maintains order in a cybersystem. It is what computer scientists are most familiar with.
Security Administration

- This is separate from the structural and functional security inherent to system design (such as the now 50-year-old idea of passwords,)
- It involves the methods of legal, and physical means of preventing attacks.
- Non-state actors feel no constraints (other perhaps than getting caught) from attacking.
Perception and Polarization

• This refers to the ability of an actor to shape effectively how a population interprets and understands events and issues (perception) in order to drive the allegiance of the population towards themselves and away from the other actors (polarization.)
What drives insurgents?

1. Uncertainty
2. Breakdown of tradition, and
3. The “Other”
Organizational Elements of an Insurgency
Networked Insurgencies

- Other insurgencies
- Government
- Guerrillas
- Leadership
- Auxiliary
- Underground
- Opportunist
- Criminal network

Summer Workshop on Cyber Security July 14-18, 2014 TTU & ASU
How these are perceived primes individuals and groups for changing their perceptions
Techniques to Alter Perceptions

1. Attribute uncertainty,
2. Attribute breakdown of tradition, to

The “Other”
One-Dimensional Approaches are Bound to Fail
Design Concept

Frame an operational environment

**Current state**
- What is going on?
  - Understand the current conditions of the operational environment.

** Desired end state**
- What should the environment look like?
  - Visualize desired conditions of the operational environment.

Frame the problem
- What are the obstacles impeding progress toward the desired end state?

Develop an operational approach
- What broad general actions will resolve the problem?

Develop the plan
- Using the military decisionmaking process

Continuous assessment and reframing as required

Summer Workshop on Cyber Security July
14-18, 2014 TTU & ASU
Transition Framework

Eliminate the insurgency's guerrilla element from an area
Set the conditions for host-nation security forces to take lead responsibility for securing the populace
Empower host-nation institutions to address the core grievance
<table>
<thead>
<tr>
<th>Insurgent perspective</th>
<th>Phase III / II (Guerrilla / war of movement)</th>
<th>Phase I (Latent / insipient)</th>
<th>Phase I (Latent / insipient)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>interinsurgent perspective</strong></td>
<td>Clear stage (Offense)</td>
<td>Hold stage (Defense)</td>
<td>Build stage (Stability)</td>
</tr>
<tr>
<td>People's perspective addressing root causes</td>
<td>Hostile (Limited)</td>
<td>Neutral (Immediate problems)</td>
<td>Positive (Underlying issues)</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enemy (insurgent) capacity</td>
<td>Host-nation government capacity</td>
</tr>
<tr>
<td>Population capacity</td>
<td>Coalition capacity</td>
</tr>
<tr>
<td>Host-nation security force capacity</td>
<td></td>
</tr>
</tbody>
</table>
The distinction between structural and functional dimensions matters.
1. Structures are the forums responsible for functions.
2. In stable societies both are interdependent
3. In insurgency this breaks down (structures and authorities are in place but are not functional.)
Perception and Polarization

1. Structures are the forums responsible for functions.
2. In stable societies both are interdependent.
3. In insurgency this breaks down (structures and authorities are in place but are not functional.)
4. A failing counterinsurgency is not inept, it is inevitably losing the perception war.
Perception and Polarization


7. Moving from asymmetrical to conventional attacks reflects insurgents’ perception of growing equilibrium between insurgents and counter-insurgency operations.

8. Perception and polarization dimension must act as the paradigm through which planning is analyzed and assessed.
Identity Formation

In-group identity formation → Out-group identity production → In-group identity formation
Identity Formation and Production

• Both are critical in the perception and polarization dimension
  – Actors seek to harness and shape dynamics
  – Three factors: uncertainty, tradition, and “Other” are critical to the two actions.
Drivers of Identity
Insurgents’ Inherent Advantage

1. An occupying power is an easy “sell” as the “Other”;

2. Similarly, obvious lying emerging from the system is a powerful push towards breakdown of the population.

3. Insurgents have a nuanced understanding of their clientele or local population.
Clean Up Costs of Cyber Attacks

- **SirCam**: 2.3 million computers affected
  - Cleanup: $460 million
  - Lost productivity: $757 million
- **Code Red**: 1 million computers affected
  - Cleanup: $1.1 billion
  - Lost productivity: $1.5 billion
- **Love Bug**: 50 variants, 40 million computers affected
  - $8.7 billion for cleanup and lost productivity
- **Nimda**
  - Cost still to be determined
Forms of Security

• Physical Security: addresses the issues necessary to protect the physical items, objects, or areas of an organization from unauthorized access and misuse.
• Personal Security: addresses the protection of the individuals or group of individuals who are authorized to access the organization and its operations.
• Operations Security: protection of the details of a particular operation or series of activities.
More Forms of Security

- Communications Security: concerned with the protection of an organization’s communications media, technology, and content.
- Network Security: the protection of networking components, connections, and contents.
- Information Security: protection of information and its critical elements, including the systems and hardware that use, store, or transmit that information.
Who Needs Security?

Anyone who uses a computer:

• 1. To protect the organization’s ability to function;

• 2. To enable the safe operation of applications implemented on the organization’s IT systems;

• 3. To protect the data the organization collects and uses; and

• 4. To safeguard the technology assets in use at the organization.
Information Security Threats

**Overt Acts**
- Human Error or Failure (accidents, mistakes)
- Espionage or Trespass (unauthorized access and data collection)
- Sabotage or Vandalism (destruction of systems or information)

**Others**
- Compromises to intellectual property
- Software attacks (viruses, worms, macros, denial of service)
- Forces of nature (fire, flood, earthquake, lightning)
Information Security Threats

• Quality of Service Deviations from Service Providers (power and WAN service issues)
• Technical Hardware Failures or Errors (equipment failure)
• Technical Software Failures or Errors (bus, code problems, unknown loopholes.)
• Technological Obsolescence (antiquated or outdated technologies.)
Acts of Human Error or Failure

People climb mountains because “They are there.”

People become hackers “Because they are there.”

Defense against the Black Arts
How Hackers Do What They Do and How to Protect against It

Jesse Varsalone
Matthew McFadden

with
Sean Morrissey
Michael Schearer (“theprez38”)
James “Kelly” Brown
Ben “TheX1le” Smith

Foreword by Joe McCray

Copyright Material

Summer Workshop on Cyber Security July 14-18, 2014 TTU & ASU
Shoulder Surfing

Shoulder surfing takes many forms. Some may not be obvious
Who are the hackers?

Traditional Hacker
- Traditional Hackers are likely juvenile, male, delinquent, and computer savvy.

Modern Hacker
- Modern hackers are usually 12-60, male or female, unknown background, with varying technological skill levels. May be internal or external to the organization.
Information Security

• Tools that are necessary for successfully applying information security
  – Policy
  – Awareness
  – Training
  – Education
  – Technology
NSTIISSC Model

- The National Security Telecommunications and Information Systems Security Committee model of information security.
Dilemma of Security

• The problem that we cannot escape in computer security is that we can have security only if everyone understands what security means, and agrees with the need for security.

• Security is a social problem, because it has no meaning until people defines what it means to them.
The Biggest Security Hole

• In practice, most users have little or no understanding of security.
Trust is the basis of Security

• Every security problem begs the question: “Whom or what do we trust?”
• In daily life we trust some things: police, the cashier
• We use technology to guard against things we don’t trust
  – Lock the car
  – Set the home security alarm
  – Withhold credit card numbers
Computer and Network Security

The same scenario applies for cyber security elements

People: the biggest threat (weakest link)

Social Engineering: manipulation of people in order to obtain information about and access to a system

Procedures: The ways tasks are accomplished (step-by-step)
Procedures are SENSITIVE!

- Obtaining procedures by an unauthorized used constitutes a threat to the integrity of the information.
Components of an Information System

- People
- Hardware
- Software
- Processes
- Data
Computer as subject of crime

Computer as object of crime

Hacker

Remote System
Access vs. Security

• It is impossible to be perfectly secure. Security is not an absolute, but should be considered a tradeoff between protection and availability.

• Unrestricted access to a system is possible, but unwise, and a threat to data integrity.

• Total security means no one has access at any time to anything.
Balancing Security and Access

Too much security makes access hard and users abandon the system. Too easy access makes a security hole for the network.
Security Implementation

Top-Down Approach – By Upper Management

CEO
  └── CFO
  └── CIO
  └── COO
    └── CISO
     └── Security Mgr
     └── Security Admin
     └── Security Tech
    └── VP-Systems Mgr
    └── Systems Admin
    └── Systems Tech
    └── VP-Networks Mgr
    └── Network Admin
    └── Network Tech

Summer Workshop on Cyber Security July 14-18, 2014 TTU & ASU
Encryption

• The process of converting messages, information, or data into a form unreadable by anyone except the intended recipient.
• The root of the word encryption “crypt” comes from the Greek kryptos, meaning hidden or secret.
Encrypt-Decrypt Process

Different keys are used to encrypt and decrypt message

Recipient's Public Key

Recipient's Private Key
Machines overtake Mankind

% Network Traffic

Mankind

Machines

6Bn

20Bn


Summer Workshop on Cyber Security July 14-18, 2014 TTU & ASU
Everything will be in Cyberspace

Covered by a hierarchy of computers!

Fractal Cyberspace: a network of ... networks of ... platforms
Recommendations

Talk and Teach

1. *We need to start talking publicly about cyber war.*

Rationale

This is certainly true. The threat of cyberwar is going to consume the sorts of resources we shoveled into the nuclear threat half a century ago, and a realistic discussion of the threats, risks, countermeasures, and policy choices is essential. We need more universities offering degrees in cyber security, because we need more expertise for the entire gamut of threats.
Recommendations

Defend Networks Better

2. *We need to better defend our military networks, the high-level ISPs, and our national power grid.*

Rationale

There is no doubt that it should be done. The two parts of that triad currently in commercial hands are simply too central to our nation, and too vulnerable, to be left insecure. Their value is far greater to the nation than it is to the corporations that own it, which means the market will not naturally secure it. Regulation is necessary.
Recommendations

Defend Networks Better

3. *Reduce cybercrime*

Rationale

Even without the cyber warriors bit, we need to do that. Cybercrime is bad, and it’s continuing to get worse. Yes, it’s hard. But it’s important.
## Recommendations

<table>
<thead>
<tr>
<th>Defend Networks Better</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4. International cyberwar treaties.</strong></td>
<td>We need to start thinking about them, talking about them, and negotiating them now, before the cyberwar arms race takes off. There are all kind of issues with cyberwar treaties. However full of loopholes they might be, their existence will do more good than harm.</td>
</tr>
</tbody>
</table>
Defend Networks Better

6. *Decisions about cyberwar need to be made as far up the command structure as possible.*

Rationale

Key decisions are *what weapons to build, what offensive actions to take, whom to target.* Because of its nature, it can be easy to launch a small-scale cyber attack, and it can be easy for a small-scale attack to get out of hand and turn into a large-scale attack. We need the president to make the decisions, not some low-level military officer ensconced in a computer-filled bunker late one night.
Survival

• “It is not the strongest of the species that survive, nor the most intelligence, but the one most responsive to change”

• Charles Darwin
Thank You!