SUMMER WORKSHOP ON CYBER SECURITY

TRACK 001
SESSION 01-03
INSTRUCTOR: FRED L. WILSON

Texas Tech University and Angelo State University
August 12-16, 2013

Supported by National Science Foundation
Cybersecurity

Dr. Fred L. Wilson

- Assistant Professor
- Department of Physics and Geosciences, and
- Adjunct, Center for Security Studies
- Angelo State University
- fwilson@angelo.edu
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.
SOMEBODY BLABBED

...don't talk about ship movements!
...don't talk about war production!

BUTTON YOUR LIP!
Will we face a cybersecurity “Pearl Harbor”? 
Far more likely we will have a “Bengazi” type attacks.
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.
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 dependant on the net, and it’s being used right now to transfer everything from friendly email to extremely sensitive data.
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.”

Cybersecurity

-- Stanley Konter, CEO of Savannah’s Sabre Technologies
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.
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
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)
1. Malware

- Malware, short for malicious software, includes viruses, worms, spyware, Trojan horse programs, etc. Malware has been a steady contender as a top threat for the past several years, and makes our top list of threats for 2010. While it is not a new threat concept, many banks still do not have adequate controls to reduce the risk to a manageable level, and new types of malware are introduced daily.
2. Social Engineering

- Most traditional social engineering attacks capitalize on the desire to please “customers.” Many of these attacks actually originate from foreign terrorist groups, some of which are funded by foreign governments. Many of the people attacking us are in a sense just showing up for work each day.
3. Mobile devices

- IT departments feel increased pressure to support more mobile devices on the network. With the craze of the iPhone and other such smart phones, there is a push (generally from upper management) to expand the types of supported mobile devices. Sometimes a smart phone can seem indispensable and we wonder how it was ever possible to work without it! However, high-risk companies must always maintain a balance between accessibility and security.
4. Data Loss

- Not a day goes by without some news clip about a company losing a laptop, backup tape, or USB drive with confidential customer information on it. The company must then notify their customers of the potential breach.
Are we running a “candy store?”
5. Internet attacks

- Everyone relies more and more on the Internet as a mechanism for promoting and delivering products and services. By moving to the Internet, we are expanding our threat landscape from local or regional threats to global threats. We must be diligent to take the care needed to protect the system from unwanted attacks.
National Infrastructure Protection Center

- To combat threats the National Infrastructure Protection Center (NIPC) was created.
- NIPC is located in the FBI headquarters in Washington, DC
- NIPC brings together representatives of public and private organizations to protect critical infrastructures.

http://ecommerce.hostip.info/pages/770/National-Infrastructure-Protection-Center-NIPC.html
What Are the Threats?

- Q. What’s the biggest cyber threat facing America today?
  - Organized terrorism?
  - Bored, curious, kid?
Origin is NOT obvious

- According to the FBI, it is difficult to quantify the origins of threats since computer intrusions occur daily from several sources. The origination of these intrusions and the intent of the intruders is usually not obvious.
Forms of Threats

- Threats come in several forms
  - Computer Intrusion (hacking either passive or active)
  - Denial of Service Attacks (DOS)
  - Virus and Worms deployment.
State of the Industry

According to the 2003 Computer Security Institute and FBI annual study on security, 95% of respondents detected computer security breaches in the previous 12 months.

“Companies will spend nearly $24 billion on network security in 2004 and it is expected this amount could triple in the next two years.”
Cyber Security Risks

The British security consulting firm mi2g calculated that the number of malicious hacking attacks worldwide jumped from about 8,000 in 2000 to 31,000 in 2001, and projected attacks to exceed 80,000 in 2004. The hacking continues to grow exponentially.
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
Recognizing Viruses

Nimda (note the garbage in the subject)

Both e-mail messages have executable attachments with the virus payload.

Sircam (note the "personal" text)
Trojan Horse Attack

Trojan Horse is activated when the software or attachment is executed.

Trojan Horse arrives via email or software like free games.

Trojan Horse releases virus, monitors computer activity, installs backdoor, or transmits information to hacker.
Denial of Service Attacks

In denial of service attacks (DOS), a hacker compromises a system and uses that system to attack the target computer, flooding it with more request for services than the target can handle. In a distributed denial of service attack, hundreds of computers (known as zombies) are compromised, loaded with DOS attack software, and then remotely activated by the hacker.
Spamming Attacks

- Sending out e-mail messages in bulk. It’s electronic “junk mail.”
- Spamming can leave the information system vulnerable to overload.
- Less destructive, used extensively for e-marketing purposes.
Security

- The quality or state of being secure – to be free from danger.
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.
How good is encryption?

- Sherlock Holmes story “The Case of the Dancing Men”
The first message

- Elsie sees the following set of characters
Simple Substitution Cipher

- Easy to crack
- Example: newspaper cryptogram, online puzzles, etc.
Strategies for breaking

- Codebreakers have their own strategies for breaking a cryptogram, especially simple substitution.
  1. Look for patterns
  2. Do a frequency analysis
  3. Trial and error till you can guess a word
Holmes Problem

Criminal message 1.

Criminal message 2

Elsie's Reply

Criminal's message 3
Replace Icons

- It is much easier if we assign each character a letter from a random alphabet. We choose a random alphabet so we are sure we do not put any patterns in place that might mislead owing to an artifact. The random alphabet I chose is:

  G W U C B H O P Q X A Z D J L T V R E M F Y K S N I
Messages now read:

- G W U C B C G O C P Q G X C A
- Z D J C C Q P L C
- X C T C B
- C Q P L C T B C T G B C V
- D J C C V V U A M D F
Frequency Analysis

- C is by far the most frequently appearing letter. We assign C = e and we find:
  
  G W U e B e G O e P Q G X e A

  Z D J e e Q P L e

  X e T e B

  e Q P L e T B e T G B e V

  D J e e V V U A M D F
Use known information

- G W U e B e G O e s l G X e A
- Z D J e e l s i e
- X e T e B
- e l s i e T B e T G B e V
- D J e e V V U A M D F
Educated guesses

- G W U e B e G O e s l G X e A
- c o m e e l s i e
- X e T e B
- e l s i e T B e T G B e V
- o m e e e V V U A M o F
Work with word patterns

- G W U e B e G O e s l G X e A
- c o m e  e l s i e
- X e T e B
- e l s i e  T B e T G B e  V
- o m e e e V  V U A  M o F

Summer Workshop on Cyber Security August 12-16, 2013 - Track 01, Session 01-03, TTU & ASU
Closer to readable. Note “V”

- G W h e r e G O e s l G X e A
- c o m e e l s i e
- X e T e r
- e l s i e T r e T G r e V
- o m e e V V h A M o F
Substituting “V” = t

- G W h e r e G O e s l G X e A
- c o m e e l s i e
- X e T e r
- e l s i e T r e T G r e t t o m e e t t h A M o F
A solution is at hand

- am here aOe slaney
- come elsie
- never
- elsie prepare t o meet thy god
Some things remain uncertain

- a m h e r e a b e s l a n e y
- c o m e e l s i e
- n e v e r
- e l s i e p r e p a r e t o m e e t t h y g o d
Good Cypher can be simple

- John McCain and the other “residents” of the Hanoi Hilton used a simple tap code. This requires memorizing a matrix

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C/K</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>G</td>
<td>H</td>
<td>I</td>
<td>J</td>
</tr>
<tr>
<td>L</td>
<td>M</td>
<td>N</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>Q</td>
<td>R</td>
<td>S</td>
<td>T</td>
<td>U</td>
</tr>
<tr>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
</tr>
</tbody>
</table>
Double Agent “Snow” Cipher

- SNOW needed a simple to use but hard to crack way of contacting German Intelligence.
Select a KEYWORD

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>C</td>
<td>A</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>O</td>
<td>A</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>N</td>
<td>C</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>G</td>
<td>G</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>R</td>
<td>I</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>A</td>
<td>L</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>T</td>
<td>N</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>U</td>
<td>N</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>L</td>
<td>O</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>A</td>
<td>O</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>T</td>
<td>R</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>I</td>
<td>S</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>O</td>
<td>T</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>N</td>
<td>T</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>S</td>
<td>U</td>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>
Construct a Grid

- Number of columns = letters in key word
- Number of rows: arbitrary. Should not be square but should be of the order of columns
Insert “bogus” squares

- This helps defeat attacks on the code and is easy for the sender and receiver to remember but difficult for the hacker.
<table>
<thead>
<tr>
<th>Prog.</th>
<th>Sq. No.</th>
<th>Row</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>18</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>26</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>35</td>
<td>3</td>
</tr>
<tr>
<td>10</td>
<td>45</td>
<td>3</td>
</tr>
<tr>
<td>11</td>
<td>56</td>
<td>4</td>
</tr>
<tr>
<td>12</td>
<td>68</td>
<td>5</td>
</tr>
<tr>
<td>13</td>
<td>81</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prog.</th>
<th>Sq. No.</th>
<th>Row</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>175</td>
<td>12</td>
</tr>
<tr>
<td>6</td>
<td>169</td>
<td>12</td>
</tr>
<tr>
<td>7</td>
<td>162</td>
<td>11</td>
</tr>
<tr>
<td>8</td>
<td>154</td>
<td>11</td>
</tr>
<tr>
<td>9</td>
<td>145</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>135</td>
<td>10</td>
</tr>
<tr>
<td>11</td>
<td>124</td>
<td>9</td>
</tr>
<tr>
<td>12</td>
<td>112</td>
<td>8</td>
</tr>
<tr>
<td>13</td>
<td>99</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>C</td>
<td>O</td>
</tr>
<tr>
<td>----</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>7</td>
</tr>
</tbody>
</table>

**CONGRATULATIONS**

Summer Workshop on Cyber Security August 12-16, 2013 - Track 01, Session 01-03, TTU & ASU
Dealing with Numbers

- Numbers are assigned using the same KEYWORD
- $C = 1$, $O = 2$, $N = 3$, $G = 4$, $R = 5$, $A = 6$, $T = 7$, $U = 8$, $L = 9$
- I and S can be used interchangably for 0
<table>
<thead>
<tr>
<th>Key</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>1</td>
</tr>
<tr>
<td>O</td>
<td>2</td>
</tr>
<tr>
<td>N</td>
<td>3</td>
</tr>
<tr>
<td>G</td>
<td>4</td>
</tr>
<tr>
<td>R</td>
<td>5</td>
</tr>
<tr>
<td>A</td>
<td>6</td>
</tr>
<tr>
<td>T</td>
<td>7</td>
</tr>
<tr>
<td>U</td>
<td>8</td>
</tr>
<tr>
<td>L</td>
<td>9</td>
</tr>
<tr>
<td>A</td>
<td>(6)</td>
</tr>
<tr>
<td>T</td>
<td>(7)</td>
</tr>
<tr>
<td>I</td>
<td>0</td>
</tr>
<tr>
<td>O</td>
<td>(2)</td>
</tr>
<tr>
<td>N</td>
<td>(3)</td>
</tr>
<tr>
<td>S</td>
<td>0</td>
</tr>
</tbody>
</table>
Entering the message

- Place the date at the beginning or the end
- Begin entering letters in the column corresponding to the day of the month
- If Date > 15 then subtract 15 from the date and begin in that column
- A short message will be easily broken, so the KEYWORD and grid size should be appropriate to the message.
Clear Text Message

- 22MAY43 0810
- FOR OSS LONDON COL BRUCE
- HITLER NATIONALIZED CHEMISCHE FABRIK FRANKFURT AND BORMANN THREATENED HARM TO KAPPLERS FAMILY IF HE TRIES TO FLEE GERMANY
Enter message, skip “blanks”

- Enter the message in the grid, skipping the blank spaces
- The message being sent on the 22, we begin in column 7 (22-15).
- Randomly selected letters are placed in the blanks.
Filling in the “Blanks”

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0.279092</td>
<td>B</td>
</tr>
<tr>
<td>B</td>
<td>0.049521</td>
<td>W</td>
</tr>
<tr>
<td>C</td>
<td>0.330764</td>
<td>A</td>
</tr>
<tr>
<td>D</td>
<td>0.355181</td>
<td>I</td>
</tr>
<tr>
<td>E</td>
<td>0.864453</td>
<td>C</td>
</tr>
<tr>
<td>F</td>
<td>0.619268</td>
<td>Z</td>
</tr>
<tr>
<td>G</td>
<td>0.93866</td>
<td>D</td>
</tr>
<tr>
<td>H</td>
<td>0.725351</td>
<td>N</td>
</tr>
<tr>
<td>I</td>
<td>0.309557</td>
<td>L</td>
</tr>
<tr>
<td>J</td>
<td>0.48318</td>
<td>M</td>
</tr>
<tr>
<td>K</td>
<td>0.604875</td>
<td>J</td>
</tr>
<tr>
<td>L</td>
<td>0.444884</td>
<td>Q</td>
</tr>
<tr>
<td>M</td>
<td>0.481902</td>
<td>K</td>
</tr>
<tr>
<td>N</td>
<td>0.383664</td>
<td>F</td>
</tr>
<tr>
<td>O</td>
<td>0.88406</td>
<td>Y</td>
</tr>
<tr>
<td>P</td>
<td>0.705249</td>
<td>S</td>
</tr>
<tr>
<td>Q</td>
<td>0.569163</td>
<td>P</td>
</tr>
<tr>
<td>R</td>
<td>0.928376</td>
<td>X</td>
</tr>
<tr>
<td>S</td>
<td>0.704388</td>
<td>H</td>
</tr>
<tr>
<td>T</td>
<td>0.962521</td>
<td>V</td>
</tr>
<tr>
<td>U</td>
<td>0.802024</td>
<td>U</td>
</tr>
<tr>
<td>V</td>
<td>0.784222</td>
<td>E</td>
</tr>
<tr>
<td>W</td>
<td>0.23389</td>
<td>O</td>
</tr>
<tr>
<td>X</td>
<td>0.708418</td>
<td>R</td>
</tr>
<tr>
<td>Y</td>
<td>0.682405</td>
<td>G</td>
</tr>
<tr>
<td>Z</td>
<td>0.353632</td>
<td>T</td>
</tr>
</tbody>
</table>
Encrypting the message

- Read across, row by row, ignoring blank spaces.
- Write the letters in groups of 5
- ICOLB DINPW CEFEF OAEOH KTLTG HOMHL OECAF HENCI RZEBM GNRRR RDTOI TRAEA MADSB LSSRU YRLNN EFOES CICGM ITKAL RRLHE ENAZO FMAMN OESQI NEJOT MAANF TUUYD KREIQ TDAOO CKCAT NLNFO BFTSY HPAEY SINRQ
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 Scheerer (“theprez38”)
James “Kelly” Brown
Ben “TheX1e” Smith

Foreword by Joe McCray
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
NSTISSC Model

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

Confidentiality

INFORMATION

Integrity

Availability
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
- Data
- Processes
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
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
Machines overtake Mankind

% Network Traffic

Mankind

Machines


0 25 50 75 100

6Bn

20Bn

Summer Workshop on Cyber Security August 12-16, 2013 - Track 01, Session 01-03, TTU & ASU
Everything will be in Cyberspace

Covered by a hierarchy of computers!

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