Security 101: Overview of Information Assurance

Dr. Barbara Endicott-Popovsky
ICS Department UHM
UW/UHM Center for IA and Cybersecurity
Russian President Vladimir Putin is praising the hack that broke into the Democratic National Committee and leaked internal emails online -- but says Russia was not behind it.

Cyber security experts have fingered two hacking groups working with the Russian government in the DNC hack, which the FBI is also investigating, and Democratic officials say the breach was part of the Moscow's attempt to influence the presidential election in favor of Donald Trump. The hack resulted in the ouster of several top DNC officials, including its former chair.

Thursday, Putin said the hack was a public service because it exposed the DNC's apparent favoritism of Clinton during the Democratic presidential primary, but claimed, "I don't know anything about it."

"Listen, does it even matter who hacked this data?" Putin said. "There's no need to distract the public's attention from the essence of the problem by raising some minor issues connected with the search for who did it."

"The important thing is the content that was given to the public," he added.
iClicker Question:

• Based on what you have read and heard about this hack how certain are you that the Russians did it?

  a. **Very sure:** The Russians did it, no doubt! They’re evil!
  
  b. **Sure:** I accept the news media reports—they know what they’re talking about.
  
  c. **Neither sure or unsure:** I’ve just heard about it and have no opinion.
  
  d. **Unsure:** How do they know for sure—on what evidence?
  
  e. **Very unsure:** Attribution is very difficult to determine absolutely on Internet communications. For example, someone could hijack Russian servers.
iClicker:
A: Very Sure
B: Sure
C: Neither sure or unsure
D: Unsure
E: Very unsure
Thought question

• Assuming that this is an attack on the US electoral process, would this be an act of war?
  — For that matter, when is an intrusion a “hack” (a simple crime) and when is it an act of war?
  — How will we know?

• These are today’s stakes! What ever happened to the kids staying up all night on Jolt hacking into the Pentagon?
Cyber War

Agenda

• Context
• Overview Threat Landscape
• Threat Spectrum Evolution
• Breach Trends
• Strategies for Organizations and Industries
• Do Controls Work?
• Changing our Mental Models
How did we get here?

CONTEXT
Information System Security Revolution

1960-1980

Computer Security

1985

INFOSEC

1995 -

Information Assurance

Networks

Packet

Switch

Gateway

File

Server

Bridge

Packet Switch

File Server

Gateway

Other Networks
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Agricultural Age</th>
<th>Industrial Age</th>
<th>Information Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wealth</td>
<td>Land</td>
<td>Capital</td>
<td>Knowledge</td>
</tr>
<tr>
<td>Advancement</td>
<td>Conquest</td>
<td>Invention</td>
<td>Paradigm Shifts</td>
</tr>
<tr>
<td>Time</td>
<td>Sun/Seasons</td>
<td>Factory Whistle</td>
<td>Time Zones</td>
</tr>
<tr>
<td>Workplace</td>
<td>Farm</td>
<td>Capital equipment</td>
<td>Networks</td>
</tr>
<tr>
<td>Organization Structure</td>
<td>Family</td>
<td>Corporation</td>
<td>Collaborations</td>
</tr>
<tr>
<td>Tools</td>
<td>Plow</td>
<td>Machines</td>
<td>Computers</td>
</tr>
<tr>
<td>Problem-solving</td>
<td>Self</td>
<td>Delegation</td>
<td>Integration</td>
</tr>
<tr>
<td>Knowledge</td>
<td>Generalized</td>
<td>Specialized</td>
<td>Interdisciplinary</td>
</tr>
<tr>
<td>Learning</td>
<td>Self-taught</td>
<td>Classroom</td>
<td>Online</td>
</tr>
</tbody>
</table>
Smashing
Industrial Age
Infrastructure!
Surprise!!
The Sorcerer’s Apprentice

http://www.youtube.com/watch?v=4ryFOztZrrc
Certificate in IA and Cybersecurity
ICS 426, 425 and 491
iClicker Question:
Before discussing the threat landscape, how do you feel about your online security in general?

A: Very Safe
B: Safe
C: Okay
D: Not safe
E: Vulnerable
What’s coming at us?

OVERVIEW OF THREAT LANDSCAPE
# World Internet Usage and Population Statistics

**June 30, 2016 - Update**

<table>
<thead>
<tr>
<th>World Regions</th>
<th>Population (2016 Est.)</th>
<th>Population % of World</th>
<th>Internet Users 30 June 2016</th>
<th>Penetration (% Population)</th>
<th>Growth 2000-2016</th>
<th>Users % of Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>1,185,529,578</td>
<td>16.2 %</td>
<td>339,283,342</td>
<td>28.6 %</td>
<td>7,415.6%</td>
<td>9.4 %</td>
</tr>
<tr>
<td>Asia</td>
<td>4,052,652,889</td>
<td>55.2 %</td>
<td>1,792,163,654</td>
<td>44.2 %</td>
<td>1,467.9%</td>
<td>49.6 %</td>
</tr>
<tr>
<td>Europe</td>
<td>832,073,224</td>
<td>11.3 %</td>
<td>614,979,903</td>
<td>73.9 %</td>
<td>485.2%</td>
<td>17.0 %</td>
</tr>
<tr>
<td>Latin America / Caribbean</td>
<td>626,054,392</td>
<td>8.5 %</td>
<td>384,751,302</td>
<td>61.5 %</td>
<td>2,029.4%</td>
<td>10.7 %</td>
</tr>
<tr>
<td>Middle East</td>
<td>246,700,900</td>
<td>3.4 %</td>
<td>132,589,765</td>
<td>53.7 %</td>
<td>3,936.5%</td>
<td>3.7 %</td>
</tr>
<tr>
<td>North America</td>
<td>359,492,293</td>
<td>4.9 %</td>
<td>320,067,193</td>
<td>89.0 %</td>
<td>196.1%</td>
<td>8.9 %</td>
</tr>
<tr>
<td>Oceania / Australia</td>
<td>37,590,704</td>
<td>0.5 %</td>
<td>27,540,654</td>
<td>73.3 %</td>
<td>261.4%</td>
<td>0.8 %</td>
</tr>
<tr>
<td><strong>WORLD TOTAL</strong></td>
<td><strong>7,340,093,980</strong></td>
<td><strong>100.0 %</strong></td>
<td><strong>3,611,375,813</strong></td>
<td><strong>49.2 %</strong></td>
<td><strong>900.4%</strong></td>
<td><strong>100.0 %</strong></td>
</tr>
</tbody>
</table>

**Notes:**
2. CLICK on each world region name for detailed regional usage information.
3. Demographic (Population) numbers are based on data from the US Census Bureau, Eurostats and from local census agencies.
4. Internet usage information comes from data published by Nielsen.
**Equation 1: Mathematical model of hacker behavior**

\[ M = f \left( P(v) - (c_1 + c_2) \right) \]

where:
- \( M \) = Hacker motivation
- \( P \) = the probability of not failing to intrude
- \( v \) = the value of success to the hacker
- \( c_1 \) = the cost to the hacker
- \( c_2 \) = the consequences to the hacker

**Troubling Reality**

"In the world of networked computers every sociopath is your neighbor."

**Dan Geer**
Chief Scientist - In-Q-Tel

"Now 100,000,000+"
“A highly computerized society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems…relies entirely on computer networks.” — *Foreign Government Newspaper*

### Information Age Threat Spectrum

<table>
<thead>
<tr>
<th>National Security Threats</th>
<th>National Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Info Warrior</strong></td>
<td>Reduce U.S. Decision Space, Strategic Advantage, Chaos, Target Damage</td>
</tr>
<tr>
<td><strong>National Intelligence</strong></td>
<td>Information for Political, Military, Economic Advantage</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Shared Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Terrorist</strong></td>
</tr>
<tr>
<td><strong>Industrial Espionage</strong></td>
</tr>
<tr>
<td><strong>Organized Crime</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Institutional Hacker</strong></td>
</tr>
<tr>
<td><strong>Recreational Hacker</strong></td>
</tr>
</tbody>
</table>
Critical Infrastructure:
An Irresistible Target

Vulnerabilities…

… gas and oil, telecommunications, water supply systems, emergency services, government services, electrical power systems, transportation, banking and finance.
Why now is so urgent:

THREAT SPECTRUM EVOLUTION

Source: GBA
Today’s Criminals Come in Many Forms...all of which can do great harm

• Script kiddies

• Hacktivists

• Cyber Criminals

• APTs / Nation States


Source: GBA
Different Faces, Same Basic Process


Source: GBA
Common Script Kiddie Attack Progression

1. **Script Kiddie enjoys hacking and wants to build reputation**
2. **Identifies Target Website(s)**
3. **Scans for Vulnerabilities**
4. **Defaces Website or Steals Data from Database**
5. **Exploits Vulnerabilities**
6. **Publicly Posts Data Breach Information and/or boasts about what they did**

Source: GBA
• Hacked 259 websites in 90 days

• Stole and leaked information

• Defaced corporate websites

Screenshot of Defacement by 15 Year Old

Source: GBA
Nation State Actors: Advanced Persistent Threats

- Highly Skilled
- Nation State Sponsored
- Example: RBN

- They have more time, and more resources than you
- If you are targeted, they WILL get into your system

http://rbnexploit.blogspot.com/

Source: GBA
Methodology / APT Attack Progression

The details change, but the process is generally the same

Information cited from:

Source: GBA
Workspace 1 (workbooks)

- Discuss who put the script kiddy out of business and why.
- If nation states and nation state/criminals are the most devastating adversaries, what are the implications to the average person/average company doing business online?
Study the data!

BREACH TRENDS
Top 9 Patterns of Intrusion

92%

The universe of threats may seem limitless, but 92% of the 100,000 incidents we’ve analyzed from the last 10 years can be described by just nine basic patterns.
Malicious Intrusion Trends

Figure 17.
Percentage (blue bar), and count of incidents per pattern. The gray line represents the percentage of incidents from the 2015 DBIR. (n=64,199)

Source: Verizon DBR 2016
Motivations Behind Attacks

Motivations Behind Attacks
January 2016

Cyber Crime - 60.6%
Hacktivism - 27.7%
Cyber Espionage - 7.4%
Cyber Warfare - 4.3%
Malicious Trends and Motives

Which countries got attacked the most and how (2016)

http://www.hackmageddon.com/2016/02/16/january-2016-cyber-attacks-statistics/
Malicious Trends and Motives

http://www.hackmageddon.com/2016/02/16/january-2016-cyber-attacks-statistics/
Security Poll

iClicker:
After learning about the threat landscape, now how do you feel about your online security?

A: Very Safe
B: Safe
C: Okay
D: Not safe
E: Vulnerable
• Describe how your own online behavior will change as a result of understanding the threats that are out there.

https://www.stopthinkconnect.org/
How to manage in this context

STRATEGIES FOR ORGANIZATIONS AND INDUSTRIES
Industry Status

• Industry lags government
  • Lack of awareness
    – Literacy
    – Risks
  • Profit margins
  • Standards of care
  • Legal liability concerns

• Critical infrastructure 85% private
Change in Perception Required

Today

Where we need to go

Compliance is not enough!

COMPLIANCE ≠ SECURITY

Security Paradigm Shift

In terms of security....

Be Paranoid

Be Proactive

Be Vigilant

Source: GBA
Basic IA Principles

Security Services

The CIA of IA

Confidentiality
Who can see the information?

Integrity
How do you verify changes?

Availability
Can information be accessed when needed?

IA Design Approach

Security Design

(Threats + Vulnerabilities \& Controls)

Threats

Vulnerabilities

Controls
Security Goals

• Confidentiality (secrecy)
  – Only authorized parties can access an asset

• Integrity
  – Only authorized parties can modified an asset

• Availability
  – Assets are accessible/modifiable by authorized parties at appropriate times
  – Authorized parties cannot be denied access to the asset

• Audit
  – An attacker cannot hide its tracks
  – Forensic analysis is possible
Test your knowledge

iClicker:
Which of the following security goals am I applying if I make my Web site accessible from 9:00 A.M. to 3:00 P.M.?

A: Confidentiality
B: Integrity
C: Availability
D: Audit
Test your knowledge

iClicker:
Which of the following security goals would prevent people without appropriate access from modifying files?

A: Confidentiality
B: Integrity
C: Availability
D: Audit
Test your knowledge

iClicker:
Which of the following security goals would require only an authorized person can gain access to information?

A: Confidentiality
B: Integrity
C: Availability
D: Audit
ICISO Perspective

Goal of System

Policy

Procedures and Practices

Security Awareness Training

Mechanisms

Secure and Forensic Ready system

IA Audit Feedback
Workspace #2

• Describe the three security services and how they work together
• Describe how the McCumber Cube is used to manage cybersecurity in organizations
What do we do with the pesky humans in the system?

DO CONTROLS WORK?
Trusting Controls
Assumes:

• Design implements your goals

• Sum total of controls implement all goals

• Implementation is correct

• Installation/administration are correct
Bottom line assumption:

You Will Never Own a Perfectly Secure System!!!
Requires Change in Strategy for Managing Networked Systems

• Today’s network defense strategy
  - On defense
  - Incident response focus on patch and recover
  - Avoidance of legal pursuit

• Proposed network defense strategy
  - On offense
  - Assume breach
  - Incident response focus on forensics
### Survivability Strategy

<table>
<thead>
<tr>
<th>Survivability Strategy</th>
<th>Tools</th>
</tr>
</thead>
</table>
| **Resistance**         | • Firewalls  
                         • User authentication  
                         • Diversification |
| **Recognition**        | • Intrusion detection systems  
                         • Internal integrity checks |
| **Recovery**           | • Incident response  
                         • Replication  
                         • Backup systems  
                         • Fault tolerant designs |

CMU 3R model of Survivability
## 4R’s of Accountable Systems

<table>
<thead>
<tr>
<th>Survivability Strategy</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resistance</strong></td>
<td>Firewalls</td>
</tr>
<tr>
<td>Ability to repel attacks</td>
<td>User authentication</td>
</tr>
<tr>
<td></td>
<td>Diversification</td>
</tr>
</tbody>
</table>

| **Recognition**        | Intrusion detection systems |
| 1) Ability to detect an attack or a probe | Internal integrity checks |
| 2) Ability to react or adapt during an attack |

| **Recovery**           | Incident response |
| 1) Provide essential services during attack | Replication |
| 2) Store services following an attack | Backup systems  |
|                        | Fault tolerant designs |

| **Redress**            | Digital Forensics |
| 1) Ability to hold intruders accountable in a court of law. | Legal remedies |
| 2) Ability to retaliate | Active defense |

---

Balance Risk vs. Cost

Costs:
- Solution
- Value
- Potential losses

Risks:
- Likelihood
- Potential impacts
Workspace 3 (workbooks)

• Recall that the 2016 Verizon Data Breach Report indicates that miscellaneous errors are the most significant intrusion trend.
• Is managing the technology, or the people using the technology, or both, more important to cybersecurity in an organization?
• Justify your answer.
Eliminating our scotomas

CHANGING OUR MENTAL MODELS
<table>
<thead>
<tr>
<th></th>
<th>Agricultural Age</th>
<th>Industrial Age</th>
<th>Information Age</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wealth</strong></td>
<td>Land</td>
<td>Capital</td>
<td>Knowledge</td>
</tr>
<tr>
<td><strong>Advancement</strong></td>
<td>Conquest</td>
<td>Invention</td>
<td>Paradigm Shifts</td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td>Sun/Seasons</td>
<td>Factory Whistle</td>
<td>Time Zones</td>
</tr>
<tr>
<td><strong>Workplace</strong></td>
<td>Farm</td>
<td>Capital equipment</td>
<td>Networks</td>
</tr>
<tr>
<td><strong>Organization Structure</strong></td>
<td>Family</td>
<td>Corporation</td>
<td>Collaborations</td>
</tr>
<tr>
<td><strong>Tools</strong></td>
<td>Plow</td>
<td>Machines</td>
<td>Computers</td>
</tr>
<tr>
<td><strong>Problem-solving</strong></td>
<td>Self</td>
<td>Delegation</td>
<td>Integration</td>
</tr>
<tr>
<td><strong>Knowledge</strong></td>
<td>Generalized</td>
<td>Specialized</td>
<td>Interdisciplinary</td>
</tr>
<tr>
<td><strong>Learning</strong></td>
<td>Self-taught</td>
<td>Classroom</td>
<td>Online</td>
</tr>
</tbody>
</table>
IT Management Evolution

- **Mainframe**
  - Access
    - Limited lists
    - Sign in logs
    - 7/24 attendants
  - Perimeter defense
    - Closed areas
    - Cypher locked doors
  - Disc forensics

- **Distributed processing**
  - Authentication
  - Firewalls
  - Network forensics
  - IDS
  - Forensic readiness
  - Drive security to physical layer
Forensics as a Security Service: Revised McCumber Cube

Embedding Hercule Poirot in Networks: Addressing Inefficiencies in Digital Forensics Investigations ...

B. Endicott-Popovsky, PhD, UW
D. Frincke, PhD, PNNL
Research Gap

• A comprehensive methodology to embed Forensic Readiness:
  
  • Knowledge of a detective
    – Rules of evidence
    – Legal requirements
    – Courtroom admissibility standards

  • Knowledge of networks
"Frankly, I miss the old days of John Dillinger and Al Capone."
Workspace #4

• What is the value of adding non-repudiation as a service of computer security?
• How would you describe forensic readiness?
Thought question

• We began with the conundrum of cybercrime vs. cyber war as it applies to the DNC hack.
• We have reviewed the threat landscape and the escalation of challenges facing us online.
• Besides realizing we may already be in WWIII, what other dramatic societal changes are implied by going digital?

October is National Cyber Security Awareness Month

https://staysafeonline.org/ncsam/
RESISTANCE IS FUTILE.
PREPARE TO BE ASSIMULATED?

Species 8472

Courtesy: K. Bailey/E. Hayden, CISOs
Backup
CYBER UNEMPLOYMENT RATE = 0%

Certification
- CISSP
- GIAC
- CEH

Experience
- Internship
- Apprenticeship
- Public Service

Education
- Certificate
- AA/BS / MS
- SFS

Job/Career
- Analyst
- Engineer
- Architect
- Auditor

A supply, not a demand problem
INPUT

Managing Security in the Cloud:
Innovative Scholarship for Service Program

- Master Degree
- PCE Certificate
- Seminar - 1 cr/4TF
- Professional Orgs
- Internships
- Research Participation

Year 1 Year 2 Year 3 Year 4

Secure Code
Military studies
Pedagogical research

OUTPUT

Expert IA Graduates
- SFS Scholars
- Transitioned Military

Education Programs
- 4 Master degrees
- 4 Certificates
- PhD’s
- MOOC’s

Research
- NSA/DoD
- NSF
- Secure Code
- Military studies
- Pedagogical research

- NIST
- DHS
- PNNL

Symposia, Conferences, UW-TV Lecture Series, PRCCDC
Pacific Rim Collegiate Cyber Defense Contest (PRCCDC)


NOTE: UW won Nationals in 2011 and 2012!!
iClicker Question:

- Based on this and other recent hack news, how safe do you feel about your photos and personal information are online?
  
  a. **Very safe:** I rarely think about computer security, as I have protected my devices with appropriate security measures.
  
  b. **Safe:** I think about my photo and information security from time to time. I am typically worried when I read about it in the news.
  
  c. **Okay:** I think about security on a regular basis, but feel safe because I keep my devices up-to-date and use security measures.
  
  d. **Not safe:** I worry about security a lot and tend to only use social media on a limited basis.
  
  e. **Vulnerable:** I am constantly worried about security and rarely do anything on a network unless I know it is safe.

- Why do you feel this way?
iClicker:

A: Very Safe
B: Safe
C: Okay
D: Not safe
E: Vulnerable