Some Paths to Cybersecurity

Golden G. Richard III

Professor of Computer Science and Engineering
Associate Director for Cybersecurity at the Center for Computation and Technology (CCT)

LOUISIANA STATE UNIVERSITY
My Path

+ truancy

- Created cybersecurity program at UNO
- Founding Director, GNOCIA
- NSA CAE, CAE-R, CAE Cyber Ops Designations
- Fellow of the American Academy of Forensic Sciences

- NSA Employee, TS/SCI Clearance
- CAE-CO Internship Program
RadioShack

SOME KIND OF STOMACH FLU...
Lots of Areas to Study in Cybersecurity

Cybersecurity: "Protection of computer systems and networks from unauthorized access, attacks, and malware. Protection includes ensuring integrity of data, availability of computing resources and services."

- Digital Forensics
- Memory Forensics
- Malware Analysis
- Penetration Testing
- Vulnerability Discovery
- Reverse Engineering
- Secure Programming
- Cryptography
Why Do We Want Students to Study Cybersecurity?
The Current Situation in Cybersecurity

• Malware is rampant
• Nation-state cyberwarfare
• Virtually all of our critical infrastructure is vulnerable
• Huge shortage of skilled cybersecurity teachers, researchers, practitioners
• We keep inventing more broken stuff!
  – Smart cars
  – IoT
  – Smart contracts for blockchains
  – ...
• Help!
Malware

Easy way to remember this: "Everything I don't want to happen to my computer."
Malware Infection Vectors

- Removable Media
- Poor Physical Security
- Malicious Web Pages
- Vulnerable Software
- Email Attachments
- Weak Passwords
- Thumb Drives
Dear John,

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

We greatly appreciate your business!
Abram Brewer

Opening this could cost you a lot of Bitcoin.

src: https://blog.avast.com/a-closer-look-at-the-locky-ransomware
Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.
Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.
If you see the main locker window, follow the instructions on the locker.
Otherwise, it's seems that you or your antivirus deleted the locker program.
Now you have the last chance to decrypt your files.

Open http://flxfs3cad3kn7v.onion.cab or http://flxfs3cad3kn7v.tor2web.org in your browser. They are public gateways to the secret server.

If you have problems with gates, use direct connection:
2. In the Tor Browser open the http://flxfs3cad3kn7v.onion
   Note that this server is available via Tor Browser only.
   Retry in 1 hour if site is not reachable.
Copy and paste the following public key in the input form on server. Avoid missprints.
   H31DA5Y-VJL5FW3-7AR841Q-IXSEZ1I
   TNKMB8-2ZNA57R-45ETFA6-LZHFZ2R
   RN74A3O-UHG72X6-NZDADV-YAZH3

Follow the instructions on the server.
The list of your encrypted files:

Upload File For Decryption

Files Available To Decrypt: 1

Your comments

<table>
<thead>
<tr>
<th>Your comments</th>
<th>Our Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.12.2016 12:40 - [email]@gmail.com</td>
<td>Please download this, Half of keys: <a href="https://expirebox.com/download/79145239daecff318cf45703b44c5a74.html">https://expirebox.com/download/79145239daecff318cf45703b44c5a74.html</a></td>
</tr>
<tr>
<td>Thank you, these systems were the right ones now.</td>
<td>All keys: <a href="https://expirebox.com/download/a111bd879b56969e050f08ebe1b85f9c.html">https://expirebox.com/download/a111bd879b56969e050f08ebe1b85f9c.html</a></td>
</tr>
<tr>
<td>Please release the 2nd half of the systems. We</td>
<td></td>
</tr>
<tr>
<td>just sent another 14 BitCoins.</td>
<td></td>
</tr>
</tbody>
</table>

Leave a comment
Targeted Malware == You’re Fired.
More Mobile Malware

**Pegasus for Android:**
- Keystroke logging
- Screenshots
- Live audio capture
- Remote control of the phone
- Email, Browser, WhatsApp, Skype, Facebook, Twitter exfiltration
- Contacts, text messages, etc.

**Shedun for Android**
- Roots the phone!
- Can't be removed, must replace the device!
- Introduces adware
- Installs new apps that masquerade as legitimate apps (e.g., Facebook)

*Discovered to be pre-installed (!) on many Chinese mobile phones*

*Sorry, no demos!*
It's our friend, eh?
Malware: There's Lots of It

- 10Gb networking
- ~200TB of storage
- cybersecurity lab

30+ million malware samples
Malware Detection and Analysis: Hard

Decryption code

Encrypted code → changing encryption key creates a different “body” for each infection...

polymorphic malware

Worse: metamorphic malware—rewrites code for each infection
Tor Hidden Services (.onion sites)
Why Do We Want Students to Study Cybersecurity?
Pick 1 - 4:

- Duty
- Challenge
- Culture
- $$$
• Huge worker shortfall
• Expected 3.5 million empty chairs by 2021 (Forbes)
Your Students Don't Have to be Truants!

• No need to live at Radio Shack
• Lots of universities provide opportunities to study cybersecurity
• Some bad, lots OK, some great
• But we need students to actually enroll in cybersecurity curricula, excel, and graduate
• Why aren't universities overrun with eager students?
A Few Reasons

• Many students don't even know that cybersecurity is a career option!

• Or imagine that only elite hackers, born with knowledge of 50 programming languages, could possibly do it

• Watch CSI, "Wow", flip channel

• There are tons of opportunities

• And potentially jaw-dropping amounts of money to be made

• Let them know this is a career option before they arrive at university

• Concentrate on math, English, computer science (if available) with a goal in mind

• #DFIR!
A Few Cybersecurity Jobs

- Ransomware Negotiator
  - Help corporations and individuals with ransomware attacks.
- Application Security Administrator
  - Keep software / apps safe and secure.
- Digital Forensics Investigator
  - Examine data containing evidence of cybercrimes.
- Automotive Security Engineer
  - Protect cars from cyber intrusions.
- Blockchain Developer / Engineer
  - Code the future of secure transactions.
- Blue Team Member
  - Design defensive measures / harden operating systems.
- Bug Bounty Hunter
  - Freelance hackers find defects and exploits in code.

Some of these jobs courtesy of [https://cybersecurityventures.com/50-cybersecurity-titles-that-every-job-seeker-should-know-about/](https://cybersecurityventures.com/50-cybersecurity-titles-that-every-job-seeker-should-know-about/)
A Few Cybersecurity Jobs

• Cyber Insurance Policy Specialist
  – Consult on cyber risk and liability protection.

• Cyber Intelligence Specialist
  – Analyze cyber threats and defend against them.

• Cyber Operations Specialist
  – Conduct offensive cyberspace operations.

• Cybersecurity Hardware Engineer
  – Develop security for computer hardware.

• Cybersecurity Lawyer
  – Attorney focused on info/cyber security and cybercrime.
A Few Cybersecurity Jobs

• Security Awareness Training Specialist
  – Train employees on cyber threats.
• Source Code Auditor
  – Analyze software to find bugs.
• Counterespionage analyst
  – Thwart cyber spies from hostile nation states.
• Cryptanalyst
  – Break encryption systems.
• Cryptographer
  – Develop new encryption systems.
• Cloud Security Architect
  – Secure apps and data in the cloud.
A Few Cybersecurity Jobs

• Data Privacy Officer
  – Ensure legal compliance related to data protection.
• Data Recovery Specialist
  – Recover "lost" data from digital devices.
• Data Security Analyst
  – Protect information on computers and networks.
• Disaster Recovery Specialist
  – Plan for and respond to data and system catastrophes.
• Secure Software Engineer
  – Bake security into applications.
A Few Cybersecurity Jobs

• Ethical / White Hat Hacker  
  – Perform lawful security testing and evaluation.
• Governance Compliance & Risk (GRC) Manager  
  – Oversee risk management.
• Incident Responder  
  – First response to cyber intrusions and data breaches.
• Intrusion Detection Analyst  
  – Use security tools to find targeted attacks.
• IoT (Internet of Things) Security Specialist  
  – Improve security of IoT devices.
• IT Security Architect  
  – Implement network and computer security.
A Few Cybersecurity Jobs

- **Malware Analyst**
  - Detect, understand, and remediate malicious software.
- **Mobile Security Engineer**
  - Implement security for mobile phones and devices.
- **Network Security Administrator**
  - Secure networks from internal and external threats.
- **Penetration Tester (Pen-Tester)**
  - Perform authorized and simulated cyberattacks.
- **Red Team Member**
  - Participate in real-world cyberattack simulations.
- **SCADA Security Analyst**
  - Secure critical infrastructures (e.g., power grid).
- **Security Auditor**
  - Conduct audits on an organization’s information systems.
Jobs with Security Clearance

+ government contractors, others

• Rigorous background check
• Essentially means: clean background, honesty
• Interviews, polygraph test, etc. before employment
• Worth investigating for some students, but some important lifestyle decisions
K-12

From 6 pilots in 2014 to 300 programs by 2020

Helping teachers teach cybersecurity.
Helping students learn cybersecurity.
CAE-CO Internship Program
Details at
https://www.intelligencecareers.gov/icstudents.htm?Agency=NSA

Email me to discuss: golden@cct.lsu.edu

Qualifications
- Must be a U.S. citizen.
- Must be eligible to be granted a security clearance.
- GPA of 3.0 or higher is preferred.
- Must be a college sophomore, junior, senior, or graduate student with at least one semester remaining after the internship.
- Must be majoring in computer science, computer engineering, electrical engineering or a related discipline and have completed courses in C programming, assembly programming, networking and operating systems. Equivalent experience will be considered in lieu.
- Must be available for an operational interview and other applicable processing between December and March.
Getting Them Interested Early

1. Guest lectures from cybersecurity faculty (the answer is "yes")
2. GenCyber, other summer camps
3. Chromebooks, your time, some academic flexibility for a course or after school club in "hacking" or cybersecurity

In decreasing order of effort for you...

https://picoctf.com/teachers
https://ringzer0ctf.com
https://www.hackthebox.eu
Talk is here: cct.lsu.edu/~golden/Materials/paths.pdf

golden@cct.lsu.edu / cct.lsu.edu/~golden

Twitter: @nolaforensix