IT Security in the Hybrid World

Randy Marchany
Virginia Tech IT Security Office and Lab
Threats
Hacker Attack Goals – over 30 years

Hacker attack goals are 1 or more of the following:

- **DATA theft/disclosure** aka data breaches
- **ATTACK** other sites using hacked assets
- **DESTRUCTION** of company data (deletion or ransomware).
- **DEFEND** accordingly
15 TYPES OF CYBER ATTACKS

- Man-In-The-Middle (MITM)
- Phishing & Spear phishing
- Drive-By Attacks
- Botnets Attacks
- Social Engineering Attacks
- SQL Injection Attacks
- Malware Attacks
- Cross-Site Scripting (XSS)
- Password Attacks
- Denial Of Service (DoS)
- Distributed Denial Of Service (DDoS)
- Inside Attack & Data Breaches
- Cryptojacking Attacks
- Load Balancing Attack
- Crypto Mining Attacks

Time it takes a Hacker to Brute Force your password

<table>
<thead>
<tr>
<th>Numbers of Character</th>
<th>Numbers Only</th>
<th>Lowercase Letters</th>
<th>Upper and Lowercase Letters</th>
<th>Numbers, Upper and Lowercase Letters, Symbols</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
</tr>
<tr>
<td>5</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
</tr>
<tr>
<td>6</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
<td>1 sec</td>
</tr>
<tr>
<td>7</td>
<td>Instantly</td>
<td>Instantly</td>
<td>25 secs</td>
<td>5 secs</td>
</tr>
<tr>
<td>8</td>
<td>Instantly</td>
<td>5 Secs</td>
<td>22 mins</td>
<td>1 hour</td>
</tr>
<tr>
<td>9</td>
<td>Instantly</td>
<td>2 mins</td>
<td>19 hours</td>
<td>3 days</td>
</tr>
<tr>
<td>10</td>
<td>Instantly</td>
<td>58 mins</td>
<td>1 month</td>
<td>7 months</td>
</tr>
<tr>
<td>11</td>
<td>2 secs</td>
<td>1 day</td>
<td>5 years</td>
<td>41 years</td>
</tr>
<tr>
<td>12</td>
<td>25 secs</td>
<td>3 weeks</td>
<td>300 years</td>
<td>2k years</td>
</tr>
<tr>
<td>13</td>
<td>4 mins</td>
<td>1 year</td>
<td>16k years</td>
<td>100k years</td>
</tr>
<tr>
<td>14</td>
<td>4 mins</td>
<td>51 years</td>
<td>800k years</td>
<td>9m years</td>
</tr>
<tr>
<td>15</td>
<td>6 hours</td>
<td>1k years</td>
<td>43m years</td>
<td>600m years</td>
</tr>
<tr>
<td>16</td>
<td>2 days</td>
<td>34k years</td>
<td>2bn years</td>
<td>15bn years</td>
</tr>
<tr>
<td>17</td>
<td>4 weeks</td>
<td>800k years</td>
<td>100bn years</td>
<td>1tn years</td>
</tr>
<tr>
<td>18</td>
<td>9 months</td>
<td>23m years</td>
<td>6tn years</td>
<td>100tn years</td>
</tr>
</tbody>
</table>

Are you in green zone?

ISOAG 2022 Marchany copyright 2022
A Brave New World
Different Approach

• Data Protection is key
  • Find, Tag, Encrypt

• Data Flow
  • Where does our data go?

• Logs are crucial
  • Who, What, When, Where, How, Why

• Resilience
  • Can’t prevent ransomware attack
  • Recovery is key
Border? What Border?

• Internet 1.0 – static servers, endpoints
• Internet 2.0 – static servers, mobile endpoints
• Internet 3.0 – mobile servers (containers, serverless),
  mobile endpoints (laptops, phones, tablets, IoT, ICS)
• Internet 3.5 – Work From Home (WFH)

• The new border is data, not the device or the network
Zero Trust Networks (ZTN) Characteristics*

Vendors usually don’t mention the 1st 3 Pillars

• Pillar 1: The network is always assumed to be **hostile**
• Pillar 2: Assume the hostiles are already **inside your network**
• Pillar 3: Network locality (segmentation) is **not sufficient** for deciding trust in a network
• Pillar 4: **Every** device, user and network flow is authenticated and authorized
• Pillar 5: **Policies** must be dynamic and calculated from as many sources of data as possible

*“Zero Trust Networks: Building Secure Systems in Untrusted Networks”, Evan Gilman, Doug Barth*
Times are a’changing – Gartner Predictions

- "Through 2023, government regulations requiring organizations to provide consumer privacy rights will cover 5 billion citizens and more than 70% of global GDP."
- "By 2025, 80% of enterprises will adopt a strategy to unify web, cloud services and private application access from a single vendor's SSE platform."
- "Sixty percent of organizations will embrace zero trust as a starting point for security by 2025. More than half will fail to realize the benefits."
- "By 2025, 60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements."

Another View

• “As we move our data outside of the firewall, we have to adopt a zero-trust type model,” [Chris] Townshend said. “We are shifting our security enforcement out to the data itself, and you have to have a security policy that follows that user no matter where that user is or what device they are using to access the data”
  • “The new cyber landscape”, Patrick Marshall, GCN Magazine, vol 37, #1

• In other words, data & identity become the border.
Can you name the assets you are defending?

Do you have visibility across your assets?

Can you detect unauthorized activity?

Can you accurately classify detection results?

Who are your adversaries? What are their capabilities?

Can you detect adversary activity within your environment?

Can you detect an adversary that is already embedded?

During an intrusion, can you observe adversary activity in real-time?

Can you confidently deploy proven countermeasures to evict and recover?
What’s Changing?

• Border Monitoring
  • Line Speeds >100Gb, moving to 300-500Gb in 5 years
    • Bad News: Inline IDS/IPS/DLP not practical w/o impacting performance
    • Good News: some vendors are adjusting

• North-South traffic more important than East-West

• Vulnerability Scanning
  • ISP may interfere thinking it’s an attack and block it

• Incident Response
  • Cutting off net access no longer under your control

• Cloud
  • Email, File sharing, Incident response, high risk data inventory affected
What’s Changing?

• VPN
  • Not necessarily a “security” feature
  • Home system may still be accessed from the net
  • Does force your packets to go thru your net
  • What services require VPN
    • ERP, etc.?
  • What services don’t require VPN
    • Email, Slack, Zoom, Teams?
A New Strategy
Net Access isn’t Equal

- Some areas have no internet access
- Some areas have poor internet access
- ISP rate based charge structure
  - Work zoom, school zoom, work downloads, streaming services = more expensive internet plans/fees

EDITORIAL COMMENT – My Opinion only (Flame Retardant Suit On)
- #WFH shows the Net has become a utility.
- It should be regulated as such.
- 21st Century version of Rural Electrification Project
Where Does It Go When It Goes Home?

• PROBLEM: Once data is on your home net, you lose data visibility

• Home systems become exfil targets
  • Infostealer class malware looks for PII
  • Attacker dumps from the home system
  • We don’t know if/when/where it went but the home ISP may

• SOLUTIONS (?)
  • TAG your data files (web bug)
  • File phones home instead of computer
  • Lot of work to implement
Your Work Computer Became Your Home Computer

• Hopefully not!
• WFH not new but # of WFH computers has INCREASED
• Will your company tools work outside of your work network?
  • Active Directory?
  • Authentication? 2 factor?
  • Software Licensing?
  • Virtual Private Network (VPN)?
• If you use your home computer for work, you must follow your office’s security requirements on it.

  • **Create a separate userid for work stuff.** Keeps personal separate from work.
    • Browser history, photos, personal sensitive data vs. work sensitive data. Can limit ransomware damage.

• When you’re done #WFH, you can delete that account
And Now Some Geek-Speak

• Can your IT scan computers at your house?
  • Probably not. May be blocked by your ISP

• Can you “disconnect” a host from your network?
  • ISP will get abuse complaints not your org.

• What network traffic visibility exists from computers at your house?
  • None probably unless you require VPN.

• What type of logs will you need to collect in this new WFH environment?
5 steps to WFH

Someone creating a tremendous sense of urgency, often through fear, intimidation, a crisis or an important deadline.

Almost every home network starts with a wireless (often called Wi-Fi) network. This is what enables all of your devices to connect to the Internet. Most home wireless networks are controlled by your Internet router or a separate, dedicated device. They connect the same way: by broadcasting a signal so devices connect. Think of broadcast as a key part of protection. The following steps to:

1. **Home Security**
   - When a site asks you to create a password, create a strong password: the more characters it has, the stronger it is. Using a passphrase is one of the simplest ways to ensure that you have a strong password. A passphrase is nothing more than a password made up of multiple words, such as “bee honey bourbon.” Using a unique passphrase means using a different one for each device or online account. This way if one passphrase is compromised, all of your other accounts and devices are still safe.

2. **Password Security**
   - Change the default administrator password. The administrator account is what allows you to then configure the settings on your wireless network. An attacker can easily find the default password that the manufacturer has provided.

3. **Password Security**
   - Can’t remember all those passphrases?
     - Use a password manager, which is a specialized program that securely stores all your passphrases in an encrypted format (and has lots of other great features, too). Finally, enable two-step verification (also called two-factor or multi-factor authentication) whenever possible. It uses your password, but also adds a second step, such as a code sent to your smartphone or an app that generates the code for you. Two-step verification is probably the most important step you can take to protect your online accounts and it’s much easier than you may think.

4. **Password Security**
   - Not sure how to do these steps?
     - Ask your Internet Service Provider, check their website, check the documentation that came with your wireless access point, or refer to the vendor’s website.

5. **Password Security**

Ultimately, the best way to protect your home network is to be vigilant and always be aware of the latest threats. Stay informed and update your software and devices regularly. And remember, a strong password is just the first step in securing your home network. By following these steps, you can help protect your devices and online accounts from potential threats.
5 Steps to WFH Securely

Make sure each computer, mobile device, program and application running the latest software.

5 Kids & Guests

Something you most likely don’t have to worry about at the office is children, guests or other family members using your work laptop or other work devices.

Children and other people using your devices can accidentally erase or modify information, or, perhaps even worse, accidentally infect the device.

Make sure family and friends understand they cannot use your work devices.

Cyber attackers are constantly looking for new ways to get into the software your devices are using. Meanwhile, the company is hard at work fixing them by installing these updates promptly, you make it much harder for someone to hack you. To stay current, simply enable automatic updating whenever possible. This rule applies to almost any technology connected to a network, including not only your work devices but Internet-connected TV’s, baby monitors, security cameras, home routers, gaming consoles or even your car.

https://www.sans.org/security-awareness-training/fact-sheet/
WFH Security Steps - Employees

<table>
<thead>
<tr>
<th>Secure your home office (Physical)</th>
<th>Secure your home router – change default password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Separate work and personal devices</td>
<td>Encrypt your devices (bitlocker, FileVault, dm-crypt, etc., Android, IOS)</td>
</tr>
<tr>
<td>Use supported and updated OS versions, software</td>
<td>Automated login for work devices at home</td>
</tr>
<tr>
<td>2FA work device logins</td>
<td>Enable “Find my device” feature</td>
</tr>
<tr>
<td>Wipe HW before share, sell or dispose. Backup first!</td>
<td>Use a VPN</td>
</tr>
<tr>
<td>Use antivirus, anti-malware software</td>
<td></td>
</tr>
<tr>
<td>Invest in a password manager</td>
<td></td>
</tr>
</tbody>
</table>

https://www.upguard.com/blog/working-from-home-security-tips
## WFH Security Steps - Employers

<table>
<thead>
<tr>
<th>Invest in Cybersecurity Training</th>
<th>Manage your 3rd party vendors and service providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement adequate email security practices</td>
<td>Use access control</td>
</tr>
<tr>
<td>Invest in Cyber hygiene – may include home devices</td>
<td>Ensure web apps use secure connections (HSTS)</td>
</tr>
<tr>
<td>Use metrics to monitor cybersecurity performance</td>
<td>Enforce password strength rules on work devices</td>
</tr>
<tr>
<td>Invest in password managers</td>
<td>Encrypt all company devices</td>
</tr>
</tbody>
</table>
Simple Steps to Protect Your Computer

• Password protect your userid, screen lock
• Update your OS & software
• Think before click
• You have a firewall already
• Adjust browser security, privacy settings

• Encrypt sensitive data
  • Use Microsoft Office tool
  • Remember your password!


• https://privacy.net/how-to-secure-your-computer/
Your Home Network and Work Network

• Your home network is an extension of the work network

• Does your home **computer** meet any regulatory requirements imposed on the data you use?

• Does your home **network** meet any regulatory requirements imposed on the data you use?
Security attacks

- Rogue App requests service
- Hack to home network
- Malware installed in access point
- Hack to wireless LAN
- Malware installed in IoT device

Networked thermostat

ISP gateway

Wireless access point

To ISP

Ethernet

https://wavecomp.ai/blog/security-in-iot-devices/
WFH, IoT, Mobile, Oh My!
Times are a’changing – Gartner Predictions

• "By 2025, threat actors will have weaponized operational technology environments successfully to cause human casualties."

• "Through 2025, 30% of nation states will pass legislation that regulates ransomware payments, fines and negotiations..."

• "By 2025, 70% of CEOs will mandate a culture of organizational resilience to survive coinciding threats from cybercrime, severe weather events, civil unrest and political instabilities."

• "By 2026, 50% of C-level executives will have performance requirements related to risk built into their employment contracts."

• Source: https://campustechnology.com/articles/2022/06/23/gartners-top-8-cybersecurity-predictions-for-the-coming-year.aspx?s=ct_nu_050722
What’s a Thing?

• A Thing is physical object that contains 1 or more devices
• Sensor – sense the physical environment
  • Thermometers, Thermostats, weight scales
  • Measure something
• Actuator – affect the physical environment
  • Brakes, pedals, pistons
  • Does something

The Internet of ransomware things...

If you don’t send us cash, your reputation will be in the trash.

I’ll start your car, but only to take you to your bank to make a transfer.

Send me $25 or I’ll tell everyone on your social network that you were stupid enough to buy an internet-connected broom!

I’m turning off the heat until you warm up my bank account!

My alarm system is going to go off randomly throughout the night, unless you “donate”...

The next time you leave, it’ll cost you 100 bucks to get back into the house, unless you give me $75 now!

I’ll be burning the toast if you don’t get me some dough!

ISOAG 2022  Marchany copyright 2022
Schneier’s Example – Car Attack*

- Confidentiality, Availability, Integrity
- Confidentiality
  - Know who you are so we target your car
- Availability
  - Disable your car’s brake system
- Integrity
  - Change the settings on your car’s “stay in lane” feature
  - Tell it to be 2 ft to the left of the center line

*"Click Here to Kill Everybody", by Bruce Schneier, ISBN: 978-0-393-60888-5
Amazon Echo Saves All Your Voice Data, Police Are Now Accessing It, Here’s How to Hear & Delete It

By Matt Agorist - December 28, 2016
Default Passwords

June 23, 2014

This page serves as a repository for the default passwords for various devices and applications.

Hardware devices listed include network devices such as routers, modems, and firewalls, along with various storage devices and computer systems. This is a substantial list, but it is not regularly updated. Revision numbers are therefore included where applicable in order to ensure accuracy.

If your device’s listed password is incorrect or if you would like to submit a password for inclusion on this list, please send an email to support@datarecovery.com with this page’s URL (http://datarecovery.com/rd/default-passwords/) in the subject line.

All of these admin passwords are provided for research purposes and for legal, legitimate use.

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model/Name</th>
<th>Revision</th>
<th>Protocol</th>
<th>User</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>3Com</td>
<td>-</td>
<td>1.25</td>
<td></td>
<td>root</td>
<td>letmein</td>
</tr>
<tr>
<td>3com</td>
<td>3comCellPlex7000</td>
<td>-</td>
<td></td>
<td>tech</td>
<td>tech</td>
</tr>
<tr>
<td>3COM</td>
<td>AccessBuilder</td>
<td>7000 BRI</td>
<td>SNMP</td>
<td>SNMPWrite</td>
<td>private</td>
</tr>
<tr>
<td>3COM</td>
<td>AirConnect Access</td>
<td>01:50-01</td>
<td>Multi</td>
<td>(none)</td>
<td>Marchany</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Copyright 2022</td>
</tr>
</tbody>
</table>
Summary

• Data Protection is key
  • Find, Tag, Encrypt

• Data Flow
  • Where does our data go?

• Logs are crucial
  • Who, What, When, Where, How, Why

• Resilience
  • Can’t prevent ransomware attack
  • Recovery is key
Contact information

• Randy Marchany, Marchany@vt.edu, 540-231-9523 (direct line), 540-231-1688 (office), Twitter: @randymarchany, Blog: randymarchany.blogspot
• http://security.vt.edu
References

• https://github.com/RUB-NDS/PRET
• https://www.nationalcyberscholarship.org/
• https://security.vt.edu
• https://foundation.mozilla.org/en/privacynotincluded