Defense at Hyperscale: Technologies and Policies for a Defensible Cyberspace

Jason Healey
Senior Research Scholar, Columbia University SIPA
@Jason_Healey
Outline

1. De-buzzwording This Talk
2. Bad Guys Finish First
3. A More Defensible Cyberspace
4. Payout for Getting it Right (or Wrong)
Not Trying to Make This an RSA Talk...

• Forget “Hyperscale” and “Defensible”

• Substitute “Internet and connected devices” instead of “cyberspace” if that helps
Core Ideas
Beyond Buzzwords

• No central strategy behind infosec today
  – To drive our actions
  – To judge between competing public goods
  – To measure our overall strategic progress against
Core Ideas

• “Making __________ more defensible” is the strategy
  My Organization
  My Sector
  Cyberspace as a whole

• Being defensible means solutions with *advantage* and *scale*
• To find future advantage and scale, we must know what has so succeeded in the past
Outline

1. De-buzzwording This Talk
2. Bad Guys Finish First
3. A More Defensible Cyberspace
4. Payout for Getting it Right (or Wrong)
Bad Guys Finish First

“Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought.”
Bad Guys Finish First

“Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought.”

O>D
Bad Guys Finish First

“Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought.”

Lt Col Roger Schell (USAF) in 1979
Why is O>D?

A dollar (or hour) spent on attack buys far more than a dollar spent on defense.
Why is O>D?

1. Internet architecture

“The Internet is not insecure because it is buggy, but because of specific design decisions.” (David Clark, 2015)

A dollar (or hour) spent on attack buys far more than a dollar spent on defense
Why is O>D?

1. **Internet architecture**
   “The Internet is not insecure because it is buggy, but because of specific design decisions.” (David Clark, 2015)

2. **Software weaknesses**
   “Today there are no real consequences for having bad security or having low-quality software of any kind. Even worse, the marketplace often rewards low quality.” (Bruce Schneier, 2003)

A dollar (or hour) spent on attack buys far more than a dollar spent on defense.
Why is O>D?

1. **Internet architecture**
   “The Internet is not insecure because it is buggy, but because of specific design decisions.” (David Clark, 2015)

2. **Software weaknesses**
   “Today there are no real consequences for having bad security or having low-quality software of any kind. Even worse, the marketplace often rewards low quality.” (Bruce Schneier, 2003)

3. **Attacker initiative**
   “Attacker must find but one of possibly multiple vulnerabilities in order to succeed; the security specialist must develop countermeasures for all”  
   *(Computers at Risk report, 1991)*

A dollar (or hour) spent on attack buys far more than a dollar spent on defense
Why is O>D?

1. **Internet architecture**
   “The Internet is not insecure because it is buggy, but because of specific design decisions.” (David Clark, 2015)

2. **Software weaknesses**
   “Today there are no real consequences for having bad security or having low-quality software of any kind. Even worse, the marketplace often rewards low quality.” (Bruce Schneier, 2003)

3. **Attacker initiative**
   “Attacker must find but one of possibly multiple vulnerabilities in order to succeed; the security specialist must develop countermeasures for all” (Computers at Risk report, 1991)

4. **Incremental and mis-aimed solutions**
   "We need more secure products, not more security products.” (Phil Venables, 2004)

A dollar (or hour) spent on attack buys far more than a dollar spent on defense
Why is O>D?

1. **Internet architecture**
   “The Internet is not insecure because it is buggy, but because of specific design decisions.” (David Clark, 2015)

2. **Software weaknesses**
   “Today there are no real consequences for having bad security or having low-quality software of any kind. Even worse, the marketplace often rewards low quality.” (Bruce Schneier, 2003)

3. **Attacker initiative**
   “Attacker must find but one of possibly multiple vulnerabilities in order to succeed; the security specialist must develop countermeasures for all”  
   (*Computers at Risk* report, 1991)

4. **Incremental and mis-aimed solutions**
   "We need more secure products, not more security products.” (Phil Venables, 2004)

5. **Complexity and high cost of control**
   Resulting complex systems: “processes that can be described, but not really understood ... often discovered through trial and error” (Charles Perrow)

A dollar (or hour) spent on attack buys far more than a dollar spent on defense
Why is O>D?

1. Internet architecture
   “The Internet is not insecure because it is buggy, but because of specific design decisions.” (David Clark, 2015)

2. Software weaknesses
   “Today there are no real consequences for having bad security or having low-quality software of any kind. Even worse, the marketplace often rewards low quality.” (Bruce Schneier, 2003)

3. Attacker initiative
   “Attacker must find but one of possibly multiple vulnerabilities in order to succeed; the security specialist must develop countermeasures for all” (Computers at Risk report, 1991)

4. Incremental and mis-aimed solutions
   "We need more secure products, not more security products.” (Phil Venables, 2004)

5. Complexity and high cost of control
   Resulting complex systems: “processes that can be described, but not really understood ... often discovered through trial and error” (Charles Perrow)

6. Troublesome humans:
   Even the best and most secure technological systems can be bypassed when human users are lazy, confused or downright tricked.

A dollar (or hour) spent on attack buys far more than a dollar spent on defense
Outline

1. Bad Guys Finish First
2. De-buzzwording This Talk
3. A More Defensible Cyberspace
4. Payout for Getting it Right (or Wrong)
If the problem is $O > D$

the solution must be $D > O$ (or even $D >> O$)

Is this even possible?
Key Questions to Tackle D>0
Results from NY Cyber Task Force

1. What is a defensible cyberspace and why hasn’t it been defensible to date?

2. What past interventions have made the biggest difference at the largest scale and least cost?

3. What interventions should we make today for the biggest differences at the largest scale and least cost?
What Would a Defensible Cyberspace Look Like?
Results from NY Cyber Task Force

Defensible = “Defense Advantage”

1. Agile response and decision-making
2. Instrumented and measurable
3. Multi-stakeholder and collaborative
4. Well-governed and policed
5. Few externalities
6. Resilient: Recovers readily

A dollar (or hour) spent on defense buys far more than a dollar spent on attack!
What past interventions have made the biggest difference at the largest scale and least cost?
## To slash or to trim

Emission reductions by policies/actions, bn tonnes CO₂ equivalent

<table>
<thead>
<tr>
<th>Policy/Action</th>
<th>Cumulative emissions</th>
<th>Period</th>
<th>Annual emissions*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Montreal protocol¹</td>
<td>135.0bn</td>
<td>1989-2013</td>
<td>5.6bn</td>
</tr>
<tr>
<td>Hydropower worldwide²</td>
<td>2.8bn</td>
<td>2010</td>
<td>2.8bn</td>
</tr>
<tr>
<td>Nuclear power worldwide²</td>
<td>2.2bn</td>
<td>2010</td>
<td>2.2bn</td>
</tr>
<tr>
<td>China one-child policy³</td>
<td>1.3bn</td>
<td>2005</td>
<td>1.3bn</td>
</tr>
<tr>
<td>Other renewables worldwide²</td>
<td>600m</td>
<td>2010</td>
<td>600m</td>
</tr>
<tr>
<td>US vehicle emissions &amp; fuel economy standards¹⁴</td>
<td>6.0bn</td>
<td>2012-25</td>
<td>460m</td>
</tr>
<tr>
<td>Brazil forest preservation⁵</td>
<td>3.2bn</td>
<td>2005-13</td>
<td>400m</td>
</tr>
<tr>
<td>India land-use change⁶</td>
<td>177m</td>
<td>2007</td>
<td>177m</td>
</tr>
<tr>
<td>Clean Development Mechanism⁷</td>
<td>1.5bn</td>
<td>2004-14</td>
<td>150m</td>
</tr>
<tr>
<td>US building &amp; appliances codes⁴</td>
<td>3.0bn</td>
<td>2008-30</td>
<td>136m</td>
</tr>
<tr>
<td>China SOE efficiency targets⁸</td>
<td>1.9bn</td>
<td>2005-20</td>
<td>126m</td>
</tr>
<tr>
<td>Collapse of USSR³</td>
<td>709m</td>
<td>1992-98</td>
<td>118m</td>
</tr>
<tr>
<td>Global Environment Facility¹⁰</td>
<td>2.3bn</td>
<td>1991-2014</td>
<td>100m</td>
</tr>
<tr>
<td>EU energy efficiency¹¹</td>
<td>230m</td>
<td>2008-12</td>
<td>58m</td>
</tr>
<tr>
<td>US vehicle emissions &amp; fuel economy standards¹⁴</td>
<td>270m</td>
<td>2014-18</td>
<td>54m</td>
</tr>
<tr>
<td>EU renewables¹¹</td>
<td>117m</td>
<td>2008-12</td>
<td>29m</td>
</tr>
<tr>
<td>US building codes (2013)¹²</td>
<td>230m</td>
<td>2014-30</td>
<td>10m</td>
</tr>
<tr>
<td>US appliances (2013)¹²</td>
<td>158m</td>
<td>2014-30</td>
<td>10m</td>
</tr>
<tr>
<td>Clean technology fund¹³</td>
<td>1.7bn *project lifetime†</td>
<td>na</td>
<td></td>
</tr>
<tr>
<td>EU vehicle emission standards¹⁴</td>
<td>140m</td>
<td>2020</td>
<td>na</td>
</tr>
</tbody>
</table>

*CATEGORIES:
- Energy production
- Transport
- Other regulations
- Global treaties
- Land & forests
- Other

See following panel for sources and explanations

*Annual emissions are cumulative emissions divided by the relevant period. The estimate for the current emissions avoided under the Montreal protocol is eight billion tonnes of CO₂e. The annual figure for the collapse of the USSR refers to the years 1992-98. ¹Cars and light trucks ²Heavy trucks
Game-Changing Solutions
Results of NY Cyber Task Force

Requires two components:

• **Advantage**: Dollar of defense must buy more than a dollar of attack

• **Scale**: Dollar of defense should give 10x, 100x, or even 1,000,000x the benefits – hyperscale
Least Game-Changing Solutions

• Generally impose far higher costs to the defender than the attacker
  – **Technology**: Compliance and other solutions featuring checking-the-box
  – **Policy**: Wassenaar Agreement to limit “cyber weapons”
Game-Changing Technologies
With Scale and Advantage

1. Automated Updates
2. Cloud-Based architecture
3. Encryption
4. Secure default configurations
5. Authentication beyond passwords
6. Mass vulnerability scanning
7. Kerberos
8. Built-in NAT for home router
9. Address space layout randomization (ASLR) and kernel memory protection
10. DDoS protection
Game-Changing Technologies
With Scale and Advantage

Automated updates:

Including, but not limited to Microsoft Update. “Once Microsoft got vested in security they were in the best position to do something about it”

(Jeff Moss, Jeff Schmidt)

1. Automated Updates
2. Cloud-Based architecture
3. Encryption
4. Secure default configurations
5. Authentication beyond passwords
6. Mass vulnerability scanning
7. Kerberos
8. Built-in NAT for home router
9. Address space layout randomization (ASLR) and kernel memory protection
10. DDoS protection
Game-Changing Technologies With Scale and Advantage

Cloud-Based architecture:

Including related technologies like virtualization and containerization.

"When deployed properly, the cloud provides several critical security advantages over perimeter-based models including greater automation, self-tailoring, and self-healing characteristics of virtualized security."

(Ed Amoroso, Phil Venables)

1. Automated Updates
2. Cloud-Based architecture
3. Encryption
4. Secure default configurations
5. Authentication beyond passwords
6. Mass vulnerability scanning
7. Kerberos
8. Built-in NAT for home router
9. Address space layout randomization (ASLR) and kernel memory protection
10. DDoS protection

(Ed Amoroso, Phil Venables)
Game-Changing Technologies
With Scale and Advantage

Encryption:

One of the few places in all computer science where, if properly implemented, the defense has all the advantages against the attacker (Steve Bellovin)

“Effective enough that it dissuades most from breaking it; there are usually other, less costly means available to the attacker.” (Wade Baker)

1. Automated Updates
2. Cloud-Based architecture
3. Encryption
4. Secure default configurations
5. Authentication beyond passwords
6. Mass vulnerability scanning
7. Kerberos
8. Built-in NAT for home router
9. Address space layout randomization (ASLR) and kernel memory protection
10. DDoS protection
Game-Changing Technologies
With Scale and Advantage

Secure default configurations:

“Some vendors have made some progress here (particularly Microsoft), and it makes a huge difference. The most impactful parts of the USG Configuration Baseline are when vendors just incorporate it into their standard configuration.”

(Senior Government Official)

1. Automated Updates
2. Cloud-Based architecture
3. Encryption
4. Secure default configurations
5. Authentication beyond passwords
6. Mass vulnerability scanning
7. Kerberos
8. Built-in NAT for home router
9. Address space layout randomization (ASLR) and kernel memory protection
10. DDoS protection
Kerberos: “Changed the way the entire world did authentication” (Phil Venables)

Authentication beyond passwords: Not just authentication, but a slew of multi-factor solutions such as algorithmic and the like (Bruce Schneier)

1. Automated Updates
2. Cloud-Based architecture
3. Encryption
4. Secure default configurations
5. Authentication beyond passwords
6. Mass vulnerability scanning
7. Kerberos
8. Built-in NAT for home router
9. Address space layout randomization (ASLR) and kernel memory protection
10. DDoS protection
Game-Changing Technologies
With Scale and Advantage

Mass vulnerability scanning:

“Solutions like nmap gave an easy and fast enterprise-wide view making fixing them far easier”

(Mike Aiello)
Game-Changing Technologies
With Scale and Advantage

1. Automated Updates
2. Cloud-Based architecture
3. Encryption
4. Secure default configurations
5. Authentication beyond passwords
6. Mass vulnerability scanning
7. Kerberos
8. Built-in NAT for home router
9. Address space layout randomization (ASLR) and kernel memory protection
10. DDoS protection

Built-in NAT for home router:

“Built-in NAT (simple firewall) has been extremely effective in stopping direct front door assaults against systems with open ports and unknown running services.”

(Marc Sachs)
Game-Changing Technologies
With Scale and Advantage

Address space layout randomization (ASLR) and kernel memory protection:

“Measures like stackguard and ASLR moving from research (ca 2000) to mainstream (ca 2008) defeated slew of common attacks ... prioritizing security over compatibility.”

(Jose Nazario, Dan Geer)

1. Automated Updates
2. Cloud-Based architecture
3. Encryption
4. Secure default configurations
5. Authentication beyond passwords
6. Mass vulnerability scanning
7. Kerberos
8. Built-in NAT for home router
9. Address space layout randomization (ASLR) and kernel memory protection
10. DDoS protection
Game-Changing Technologies
With Scale and Advantage

DDoS protection:

“If an org can afford Cloudflare, etc., they can withstand hundreds of Gbps and stay online ... not ‘solved,’ but defenses can substantially mitigate impact, unlike so many other issues.”

(Richard Bejtlich)
Additional Possibilities: Beau Woods
I Am the Cavalry and Atlantic Council

• **Language choice**
  
  – With C it's really hard to prevent errors and the failure modes are catastrophic to the software stack. By contrast something like Ruby on Rails has the penalty for failure of a nerf football

• **Controls Retirement**
  
  – We keep adding one control after another in pursuit of better defense in depth. Most organizations are up to their neck in DiD and it's suffocating them without benefit. Old controls like AV aren't really helping but they're costing 8-10B per year.
  
  – Radically different IT thinking obviates some of these old expensive things by fixing root causes not apparent ones
  
  – Related: Retire legacy infrastructure (Phil Venables)

• **MAC not DAC**
  
  – Mandatory Access Control is like whitelisting on steroids. The entire OS is hostile to untrusted code. Especially effective in Mobile, IoT, and other places

• **Software Supply Chain**
  
  – Modern software platforms are 80-90 percent assembled rather than written
  
  – DevOps is an application of supply chain theory to agile development allowing us to run faster and stay safer

• **Software Bill of Materials**
  
  – Even the best vulnerability scanners have high degree of false positives and negatives. SBOMs are precise and accurate
Possible Next-Gen Game-Changers
Ongoing Work of the NY Cyber Task Force

• Return of Formal Methods, like DARPA’s High-Assurance Cyber Military Systems
  “Not unhackable completely. There are certain obvious pathways for attackers that have all been shut down in a way that’s mathematically proven to be unhackable for those pathways.” (Arati Prabhakar)

• Compiler-Generated Software Diversity:
  “After every 100th download of a given app ... re-compiles that app with a strong diversity compiler making the next 100 downloads different from the previous 100. This prevents mass exploitation, though at a cost: it is no longer possible to confirm whether a given binary corresponds to a given source blob.” (Dan Geer)

• Security solutions for IoT
  If you think cyberspace is insecure today, just wait for the coming Internet of Things. “The first 5 billion devices won’t be like the next 50 billion. Modern cars are computers on wheels, and cutting edge patient care is delivered over the Internet. If we get this right, the promise will transform society; if we get this wrong we eliminate the resilience we seek.” (Beau Woods)

• Security score cards like BitSight to drive insurance, behavior (Phil Venables)
• Data-level protection (Greg Touhill)
How Do Techs Become Real Game-Changers
Ongoing Work of the NY Cyber Task Force

1. Take Away Entire Classes of Attacks (Arati Prabhakar)
2. Take User out of the Solution (Bruce Schneier)
3. "Those responsible make a change that helps all their users” (Jeff Moss)
4. “Improve security by decreasing cost of control” (Phil Venables)
5. Minimize Consequence - agility, detection, and resilience (Art Coviello)
Operational and Policy Game-Changers

Harder to Measure

• Creation of the first CERTs in late 1980s
• Operational innovations: kill chain
• Automated threat sharing – STIX, TAXII, CyBox
• Institutionalized bug bounty programs
• Volunteer groups: Conficker, NSP-SEC, I am the Cavalry
• Industry Alliances: ICASI, Cyber Threat Alliance
• Budapest Convention on cyber crime
Operational and Policy Game-Changers

- International norms along with indictments and threat of sanctions
- FireEye: massive reduction of detected Chinese intrusions from ~70/month to less than 5/month
- What other solution have we ever implemented for such success at so little cost?

Operational and Policy Game-Changers

- USG policy of “bias” to not retain vulnerabilities, but disclose to vendors
- USG “discloses far more vulnerabilities than it decides to keep secret, in one year keeping only about two for offensive purposes out of about 100 the White House reviewed”
Operational and Policy Game-Changers

• USG policy bias to disclose to US companies when they’ve been pwned

• Result: Law Enforcement now #1 source for breach notification (esp for botnet takedown), per Verizon

http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
Outline

1. De-buzzwording This Talk
2. Bad Guys Finish First
3. A More Defensible Cyberspace
4. Payout for Getting it Right (or Wrong)
Implications

• Only potential futures aren’t just
  – O>D (continued status quo)
  – D>O (defense advantage)

• Could be far worse, O>>D
  – or far better, D>>O

• Atlantic Council and Zurich Insurance Group modeled the economic impact of getting it right (or horribly wrong)
Possible Futures...

Best case is “Cyber Shangri-La” where D>O
Worst case is “Clockwork Orange Internet” where O>>D

Economic Impact Through 2030

Best case: ~$30 trillion
Worst case: ~$90 trillion
Difference in government control less impactful, still meaningful: $30 trillion
If Future Possibilities are “Fat Tail Distribution” Then Far More Potential Variability

Regular standard deviation
Lower chance of massive, unexpected events

Variance not bounded
*Far* higher chance for surprise
Measuring Defensibility

- Verizon Data Breach Investigations Report
  - “Detection deficit ... is getting worse”
  - “Attackers are getting even quicker at compromising their victims”
  - Slight improvements in how quickly defenders detect compromises
- Commerce: 45 percent of US online households have stopped some sensitive online transactions
- Index of Cyber Security
For a More Defensible Cyberspace
And a $120 Trillion Payoff

• **Advantage:** Dollar of defense must buy more than a dollar of attack

• **Scale:** Dollar of defense should give 10x, 100x, or even 1,000,000x the benefits – hyperscale
THANK YOU

@Jason_Healey