

Global Deep Scans – Measuring vulnerability levels across organizations, industries, and countries

Fabian Bräunlein <fabian@srlabs.de>
Luca Melette <luca@srlabs.de>



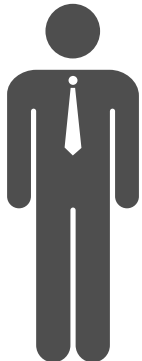
**Security
Research
Labs**

Motivation for this talk

- We often get asked: **How secure is my company compared to other companies?**
 - As researchers we can't usually say much about a single company. Until now.
 - We conducted a massive internet-wide scan to answer these questions:
 - How common are security issues on the Internet?
 - Where are issues least and most common?
 - Which organizations/industries/regions can we still learn from?
 - Today, we make our research data public to
 - Encourage your further research
 - Help different industries to start interacting and learning from each other
-

Our goal: Enable a constructive conversation between companies and researchers

Our research motivation



Security Officer

Our vulnerability scan shows 23 different issue types for my organization. Is that really bad? **How do I compare to others?**



Researcher



No Idea. All I know is that the one vulnerability I research affects 42,000 IPs including one of yours.

Defense View

Offense View

The two views are hard to compare, which inhibits a constructive exchange between the two communities. This presentation discusses a Global Deep scan, which hopefully helps bridge the gap.

Companies and researchers look at very different vulnerability statistics

	Defense view 	Offense view 																
Methodology	Deep Scan	Global Scan																
Objective	Find many vulnerabilities for the IPs of a single company	Find the prevalence of a single issue across the Internet																
Tooling	Nessus, Qualys, Nexpose, ...	Shodan, Censys, Masscan, ...																
Typical result example	<table border="0"><tr><td>Active IPs:</td><td>2,000</td></tr><tr><td>▪ Vulnerable Coldfusion</td><td>4</td></tr><tr><td>▪ Exposed VMWare ESXi</td><td>3</td></tr><tr><td>▪ Weak password</td><td>3</td></tr><tr><td>▪ Heartbleed</td><td>1</td></tr><tr><td>▪ Minor TLS/SSL config issues</td><td>500</td></tr></table>	Active IPs:	2,000	▪ Vulnerable Coldfusion	4	▪ Exposed VMWare ESXi	3	▪ Weak password	3	▪ Heartbleed	1	▪ Minor TLS/SSL config issues	500	<table border="0"><tr><td>Scanned IPs:</td><td>20,000,000</td></tr><tr><td>▪ Heartbleed</td><td>2,500</td></tr></table>	Scanned IPs:	20,000,000	▪ Heartbleed	2,500
Active IPs:	2,000																	
▪ Vulnerable Coldfusion	4																	
▪ Exposed VMWare ESXi	3																	
▪ Weak password	3																	
▪ Heartbleed	1																	
▪ Minor TLS/SSL config issues	500																	
Scanned IPs:	20,000,000																	
▪ Heartbleed	2,500																	

These two views are hard to compare. To compare security level across companies, we instead need scans that are **Global & Deep**

-
- Research motivation

- ▶ **Measuring hackability**

- Global deep scan results
 - Data for security evolution
-

Generic security issue types are prevalent across the internet

Research scope: **827k active IPs** – of 270 million IPs belonging to companies that we scanned

	Authentication and credential issues	Unnecessary exposure	Hardening gaps	Missing patches
Example issues [Issues per million active IPs]	Weak password 297	Exposed VMWare ESXi 2.154	Accessible .git 3.369	Heartbleed 1.080
	HTTP default credentials 129	Exposed Cisco SmartInstall 412	Accessible Linux home folder 898	RDP vulnerability 183
	Unauthenticated Redis 54	Exposed HP Remote Console 376	Writable anon FTP 548	Vulnerable Coldfusion 103
	Unauthenticated MQTT 30	Exposed Lantronix config 151	HTTP path traversal 307	Vulnerable Struts2 30

- Researchers focus on novel bug classes, while most issues found on the Internet are well-known issues
- The vast majority of Internet-exposed security issues would be addressed by basic security practices: Change default passwords, use a firewall well, harden your servers, and patch them regularly
- The fact that most companies we scanned seem to miss these practices shows a big gap between cutting-edge security research and tools, and issues responsible for most actual hacking

Security issues from four best practice areas are summarized in a Hackability Score

1. Scan to find issues					2. Compute Hackability Score	
Hackability sub-scores	Authentication and credential issues	Unnecessary exposure	Hardening gaps	Missing patches or end-of-life software		
Best practice	Use strong credentials	Expose only minimal set of services to hackers	Configure assets securely, fix programming bugs	Regularly install security updates		
Issue examples	Severity 4 – Exploit	<ul style="list-style-type: none"> Tomcat with default or weak credentials NFS share mountable 	<ul style="list-style-type: none"> Cisco Smart Install exposed Java Debug Wire protocol exposed 	<ul style="list-style-type: none"> CMS backup files can be downloaded Directory traversal 	<ul style="list-style-type: none"> Apache Struts vulnerability HP iLO 4 vulnerability 	x 8
	Severity 3 – Exploit fragment	<ul style="list-style-type: none"> Printer with default credentials Weak SNMP pass w/ write access 	<ul style="list-style-type: none"> Java RMI exposed Industrial control system protocol exposed 	<ul style="list-style-type: none"> .git accessible Home directory exposed in web root 	<ul style="list-style-type: none"> Oracle TNS poison attack Cisco iOS older than 3 years 	x 4
	Severity 2 – Best practice deviation	<ul style="list-style-type: none"> Known leaked TLS private key used Weak SNMP pass w/ read access 	<ul style="list-style-type: none"> Database exposed Server management interface exposed 	<ul style="list-style-type: none"> Open SMTP relay DNS server allows zone transfers 	<ul style="list-style-type: none"> EOL IIS EOL OpenSSH 	x 1
						Hackability score

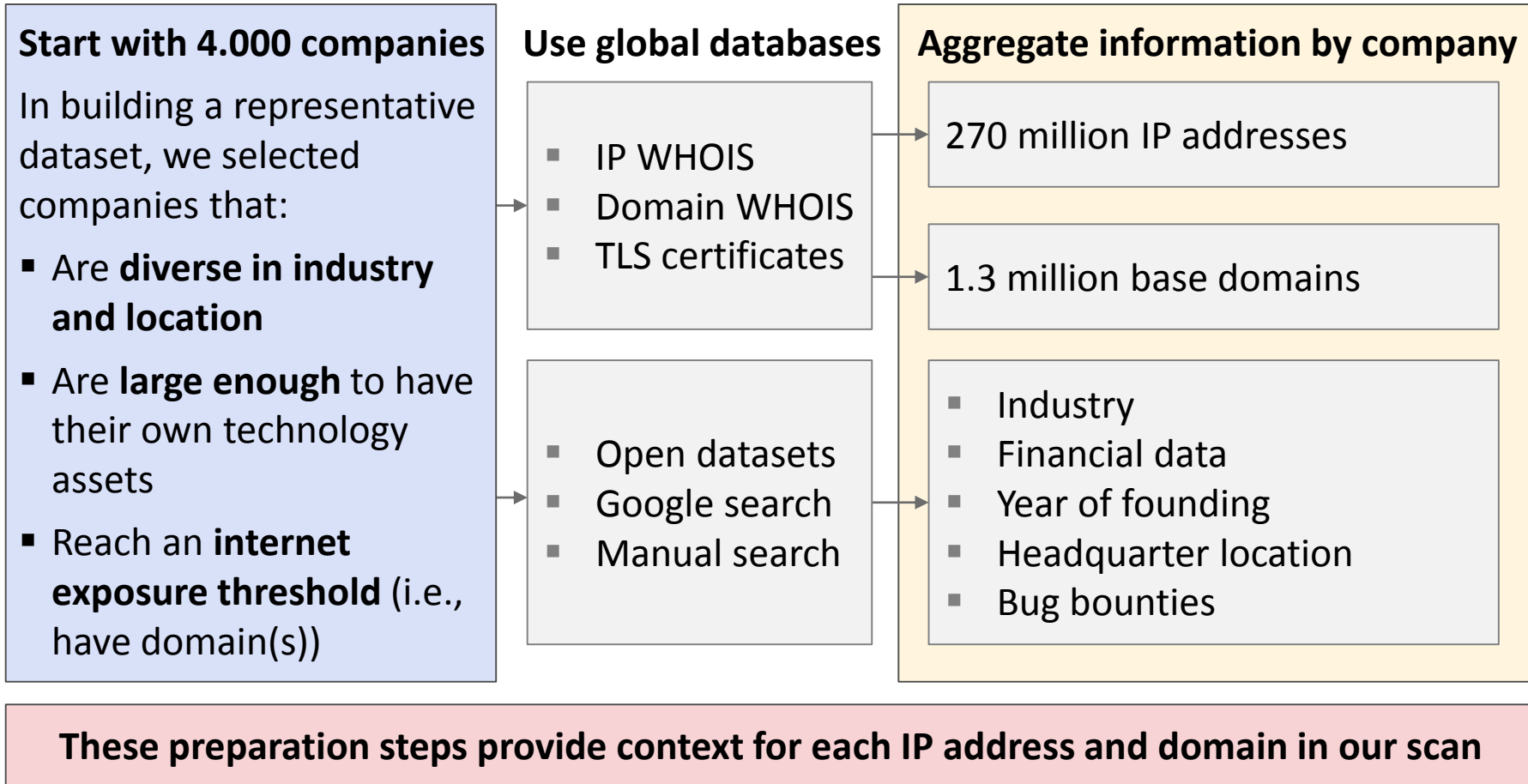
- Definition: The hackability score is the sum over Internet-exposed issues, multiplied by their severity class.
- If one issue type is present multiple times, each additional occurrence is weighted less to account for the diminishing return to the hacker

Hackability Score example

1. Scan to find issues		
	Server 1	Server 2
Severity 4	-	-
Severity 3	-	▪ .git accessible
Severity 2	▪ MySQL exposed	▪ MySQL exposed

2. Compute Hackability Score			
	Weight		
No issues	x 8	=	-
1 issue	x 4	=	4
2 times the same issue -> Count as: 1.8 issues	x 1	=	1.8
Hackability score	Σ		5.8

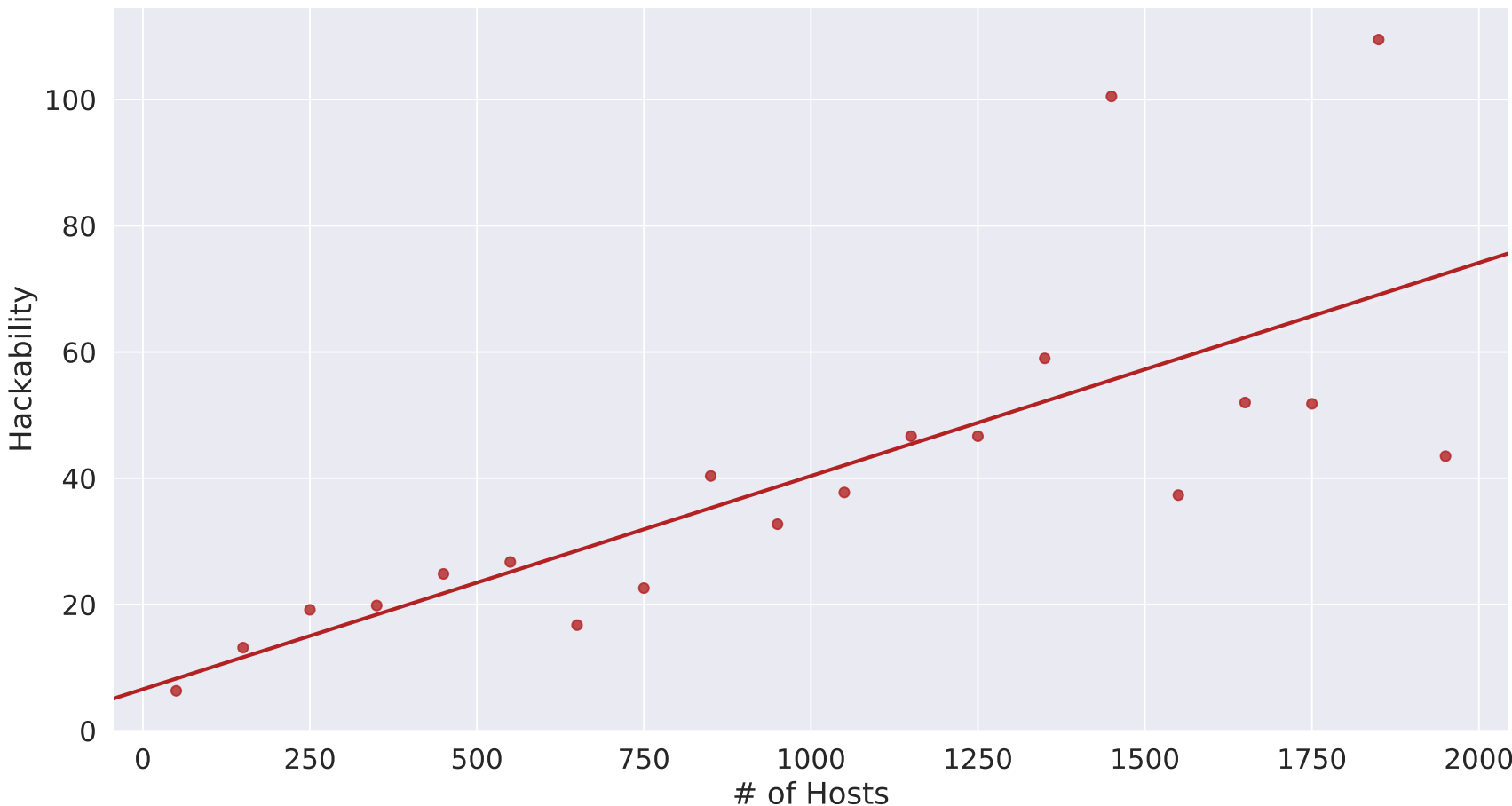
Our scan sample is composed of thousands of organizations globally



-
- Research motivation
 - Measuring hackability
 - ▶ **Global deep scan results**
 - Data for security evolution
-

The hackability of a company grows with the number of hosts it exposes to the Internet

Analysis

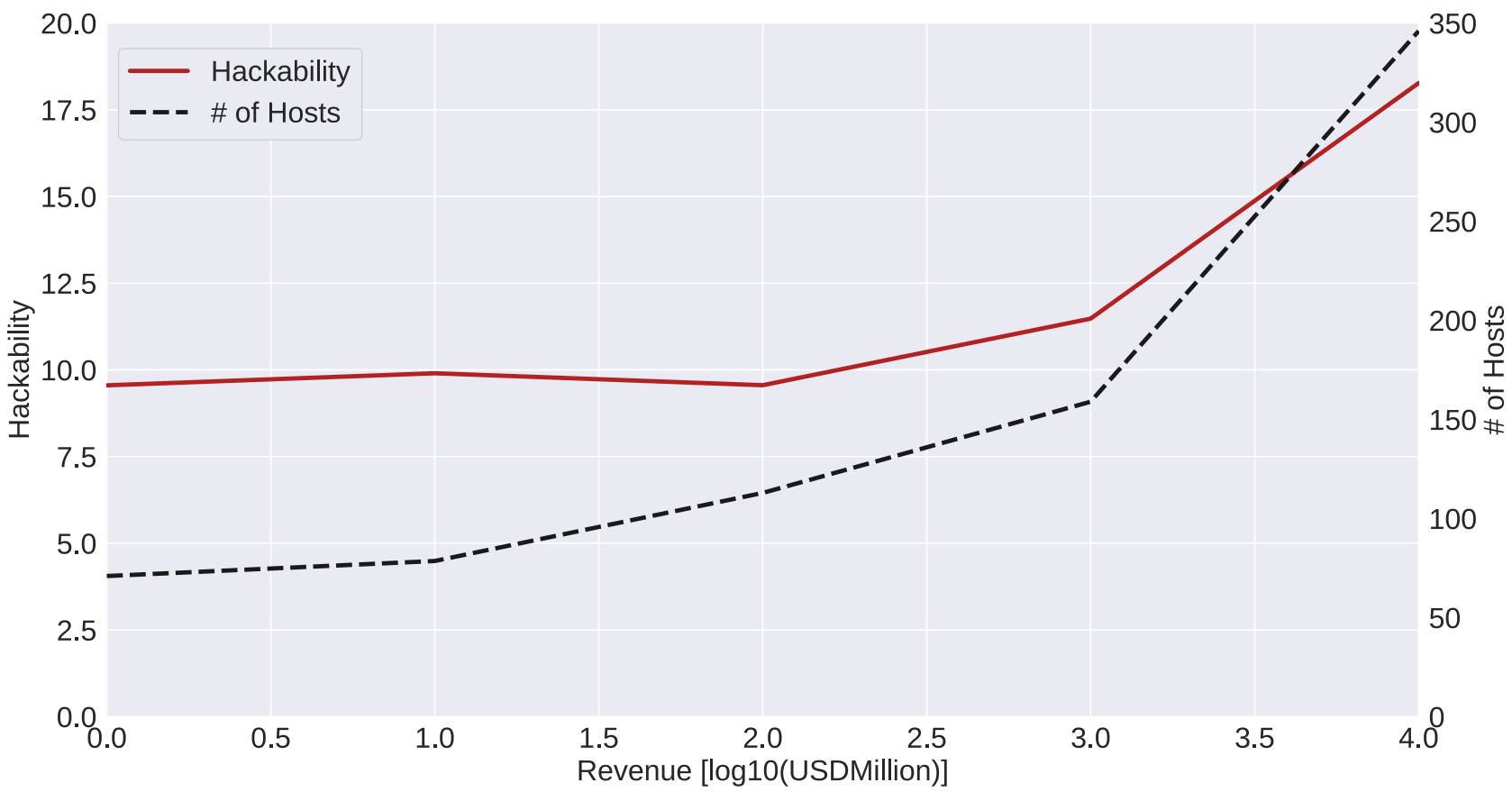


Interpretation

- The more hosts a company has exposed on the internet, the higher its hackability score
- This is intuitive as having a higher number of hosts exposed means more room for errors

Hackability grows slower than company size

Analysis




Interpretation

- Both the number of exposed hosts and the hackability score of a company increases with its revenue
- But it increases a lot slower than the revenue (logarithmic scale!)
- This is reassuring given the much larger investment into information security by large companies, and additional synergies of large security programs

Hackability varies widely across industries

Research questions

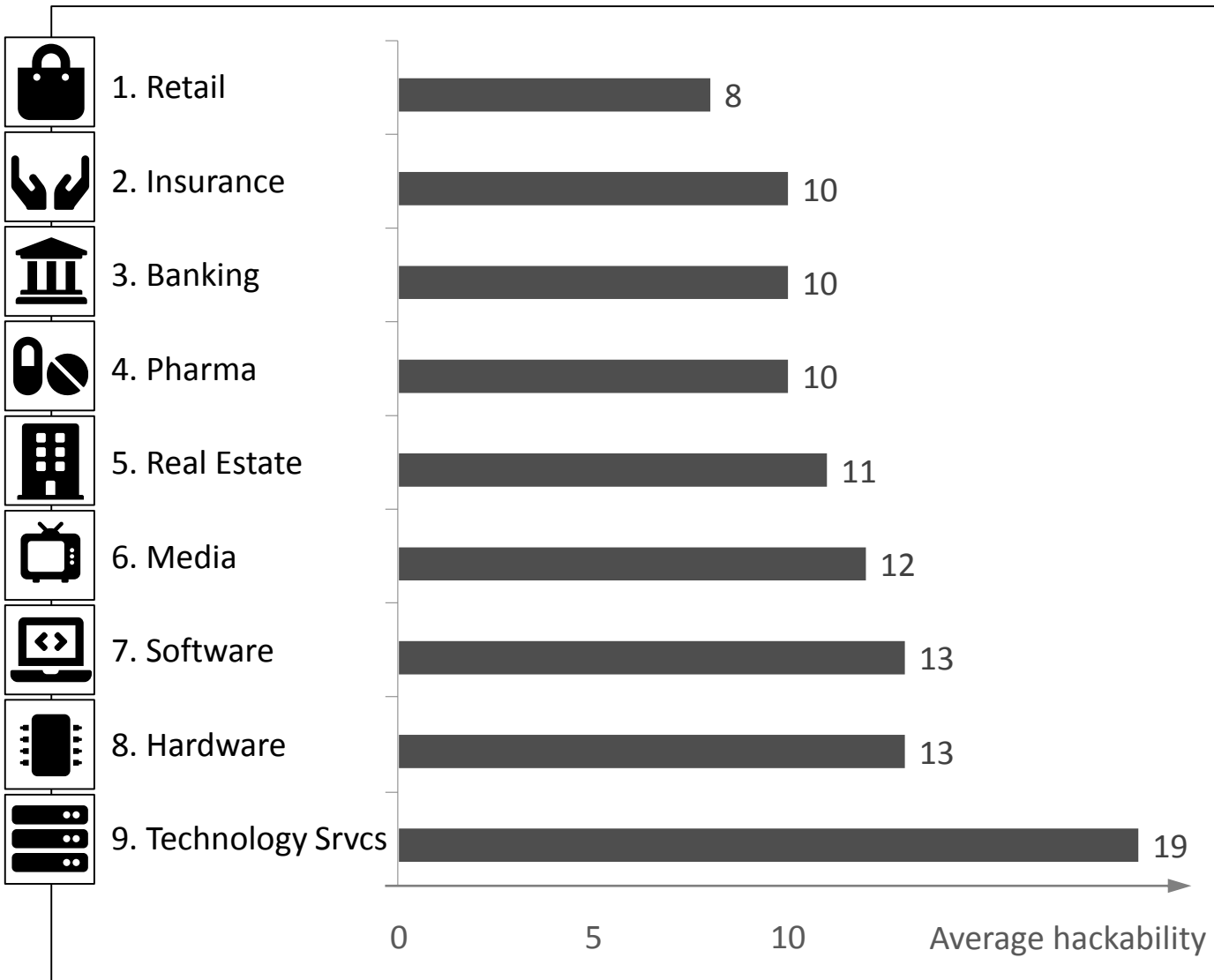
Defense view 

Which industries can I learn from?

Offense view 

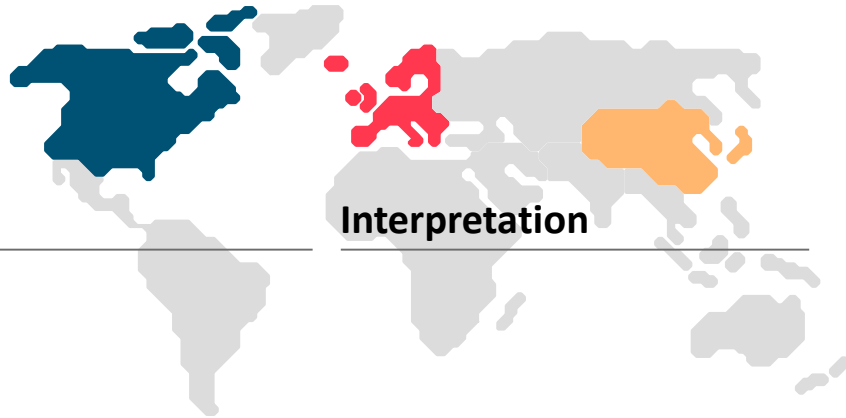
Which industries are the easiest targets?

Analysis



Cloud providers, telcos, and ISPs are excluded from our analysis because their IP ranges are typically shared with their customers.
(IP allocations for telco/ISP enterprise customers show a very high vulnerability count.)

Europe is significantly more hackable per exposed host



Research questions

Defense view

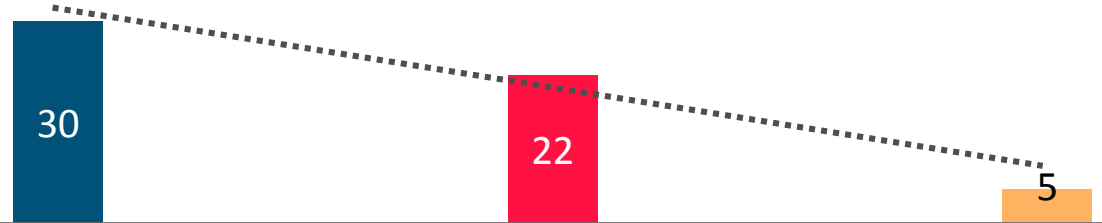
Peers from which regions can still teach us something?

Offense view

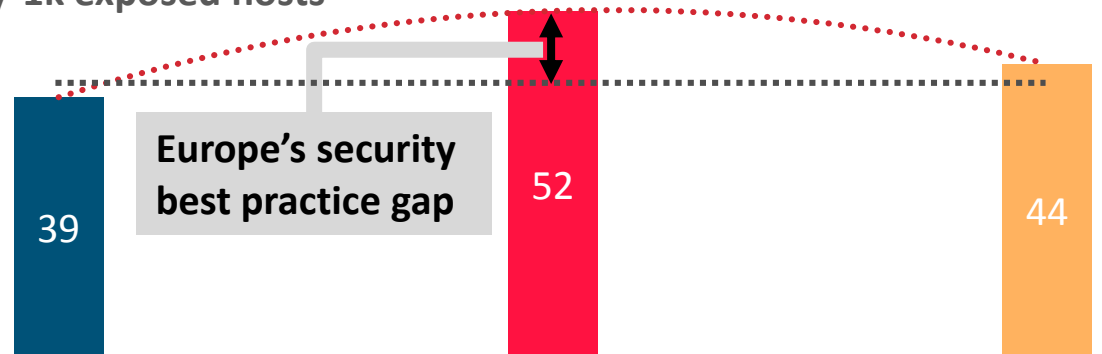
Which regions have the most low-hanging fruit targets?

Analysis

of 1k exposed hosts / USD 1b revenue



Hackability / 1k exposed hosts



North America

Europe

East Asia

Technology progressive.
Lots exposed, secured to an above-average level

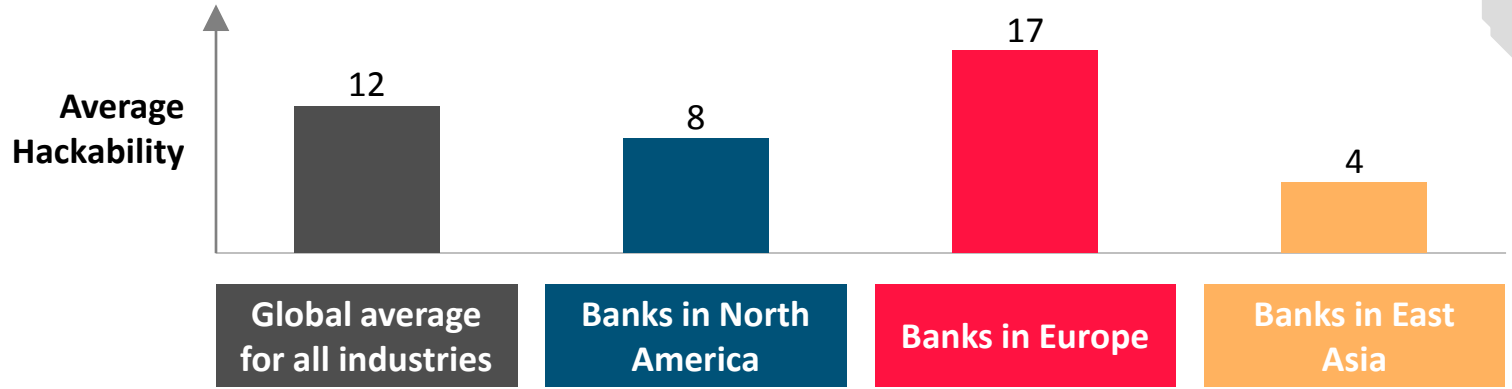
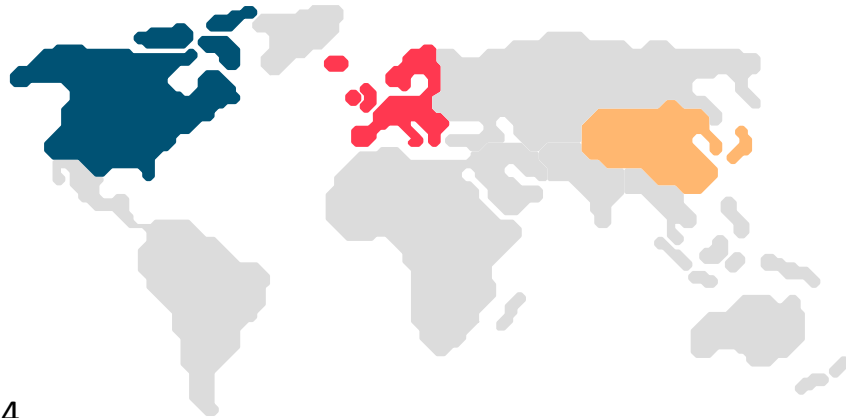
The worst of both worlds.
Less technology exposed, but more hackable on average

Technology conservative.
Less exposed technology, thereby less hackable

Interpretation

- **Hackability** typically grows with the number of technology assets exposed to the Internet
- **Europe is an exception** – fewer assets are exposed per company, but they are more hackable on average

Banks' hackability mostly arises from missing patches, and is worst in Europe



	Global average for all industries	Banks in North America	Banks in Europe	Banks in East Asia
Authentication and credential issues	11%	6%	6%	6%
Unnecessary exposure	32%	37%	34%	27%
Hardening gaps	37%	16%	20%	14%
Missing patches	20%	41%	40%	53%

Contribution of different issue types to overall Hackability

Offense view

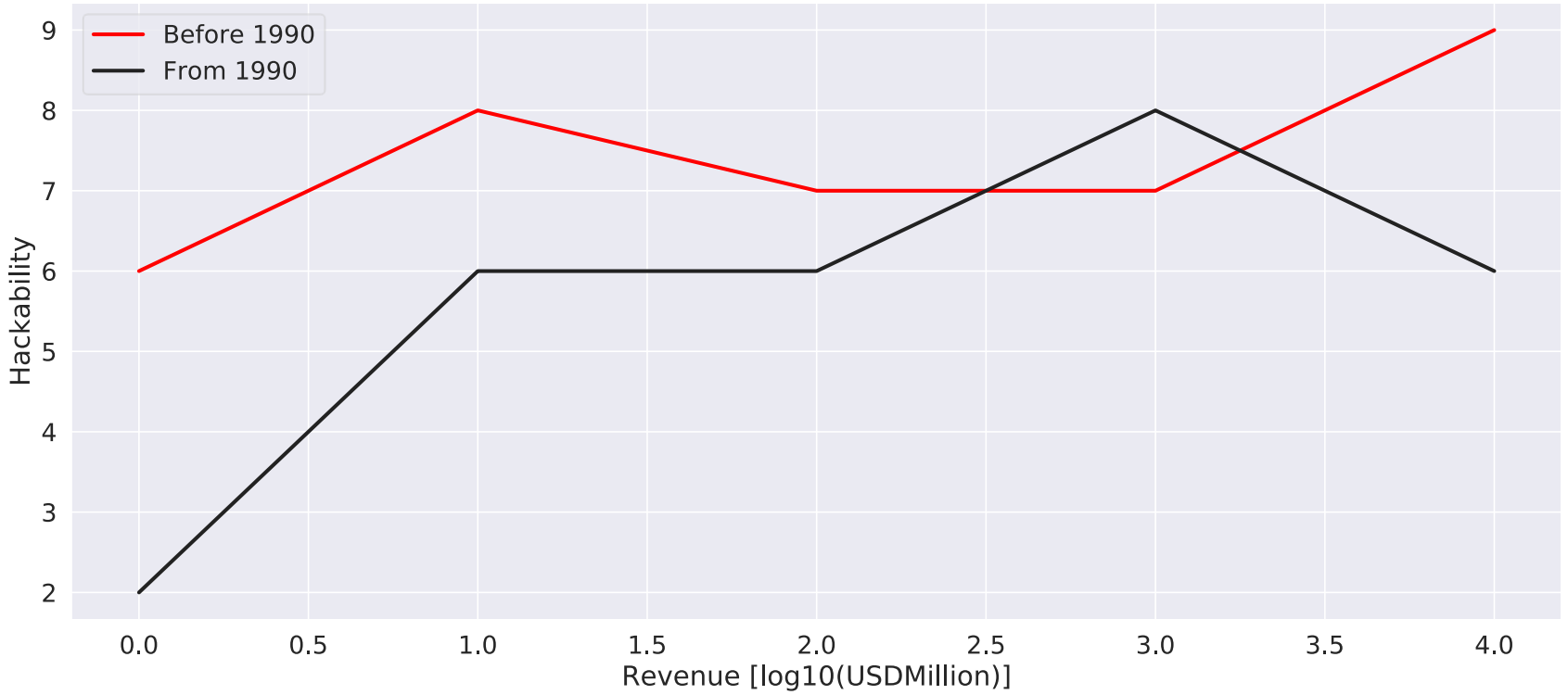
If your goal is to hack a bank, you would look for missing patches on unnecessarily exposed hosts, starting in Europe

Defense view

If you want to secure a bank in Europe, you should focus on patching, and then learn on authentication and hardening from your peers in other regions

Older companies are slightly more hackable

Analysis

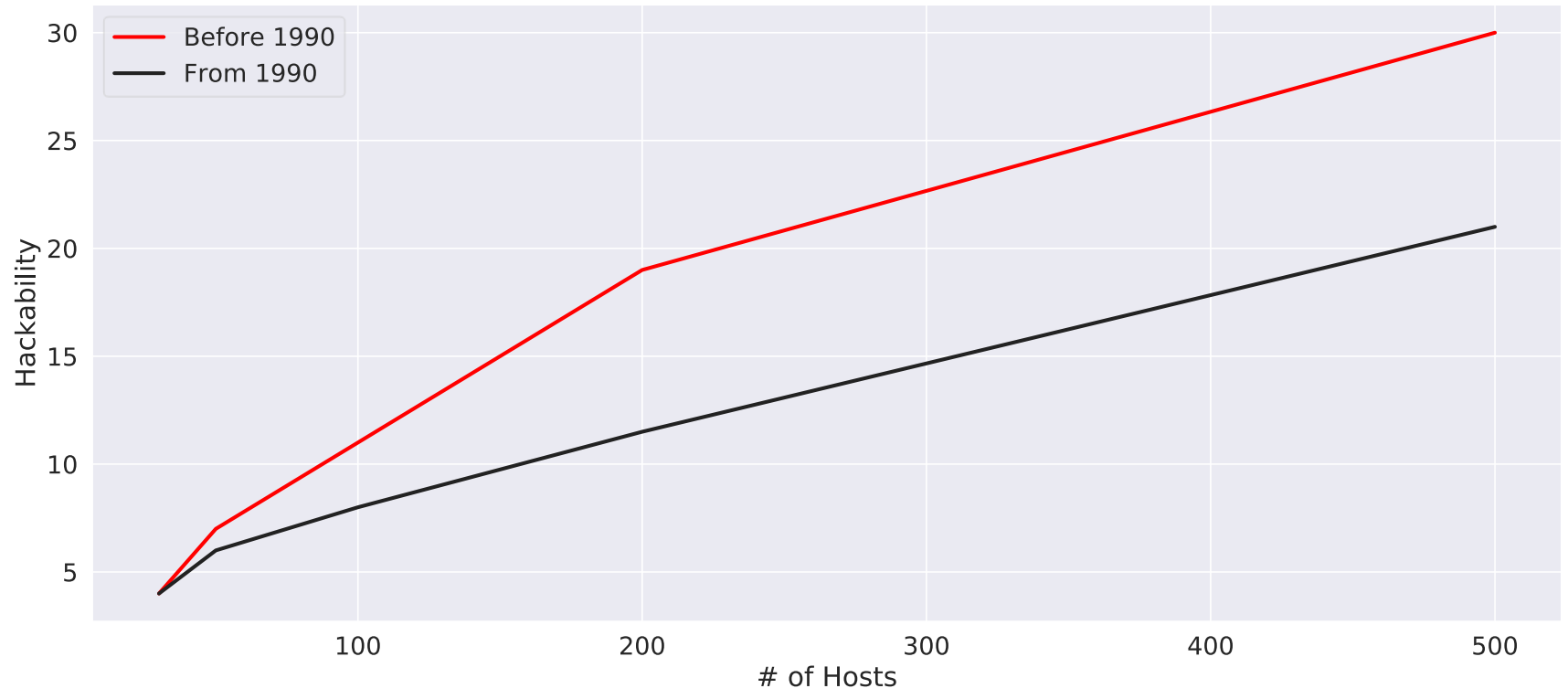


Interpretation

Companies that were founded pre-Internet are slightly more hackable than companies with similar revenue founded later

Older companies expose fewer hosts, but those hosts are significantly more hackable

Analysis

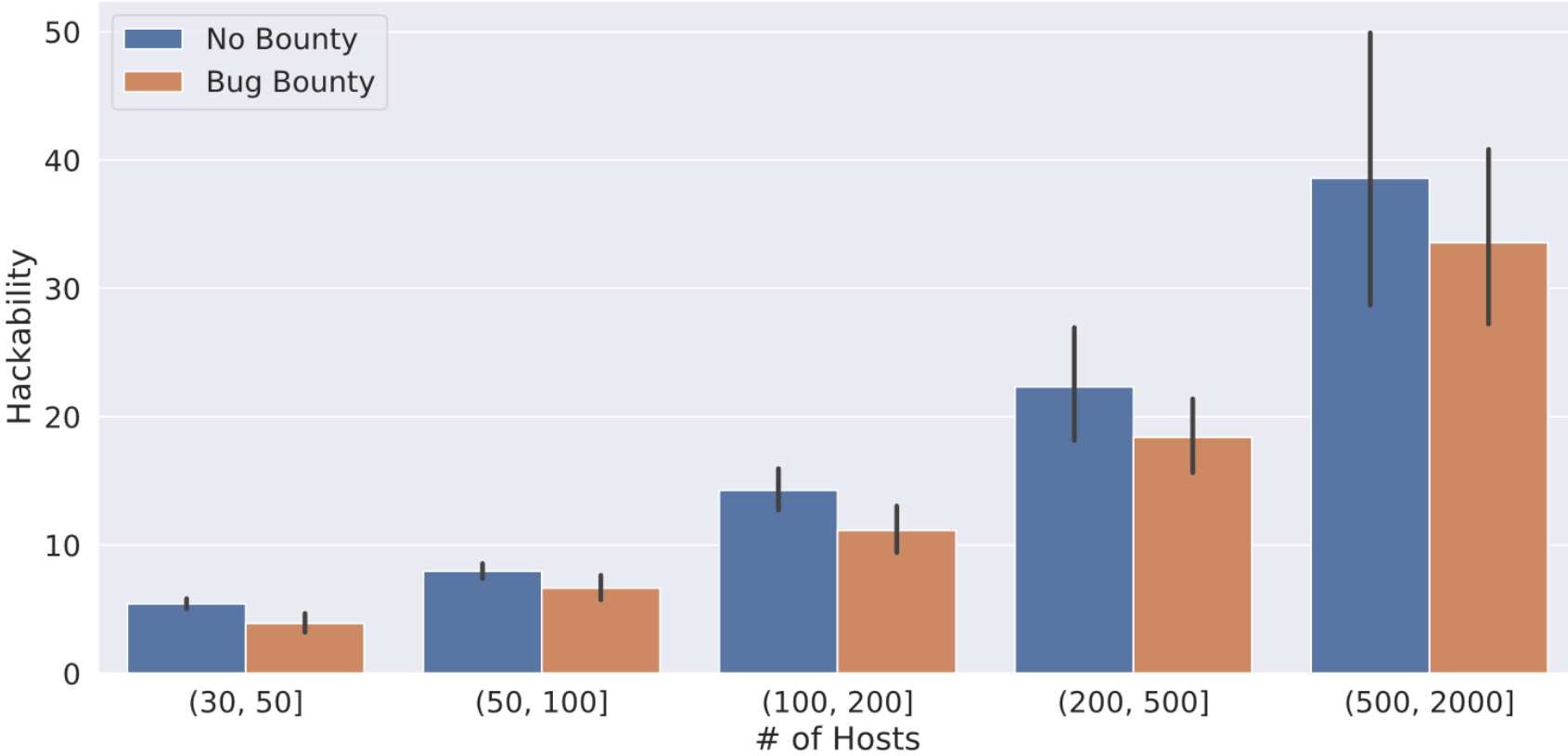


Interpretation

- Comparing companies with the same number of hosts, shows a much clearer picture
- This means that pre-Internet companies with the same revenue on average expose less hosts on the Internet, but the exposed hosts are much more hackable
- This suggests that pre-Internet companies are less experienced or skilled in applying security best practices

Companies with a bug bounty are less hackable than similarly exposed peers without a bounty

Analysis

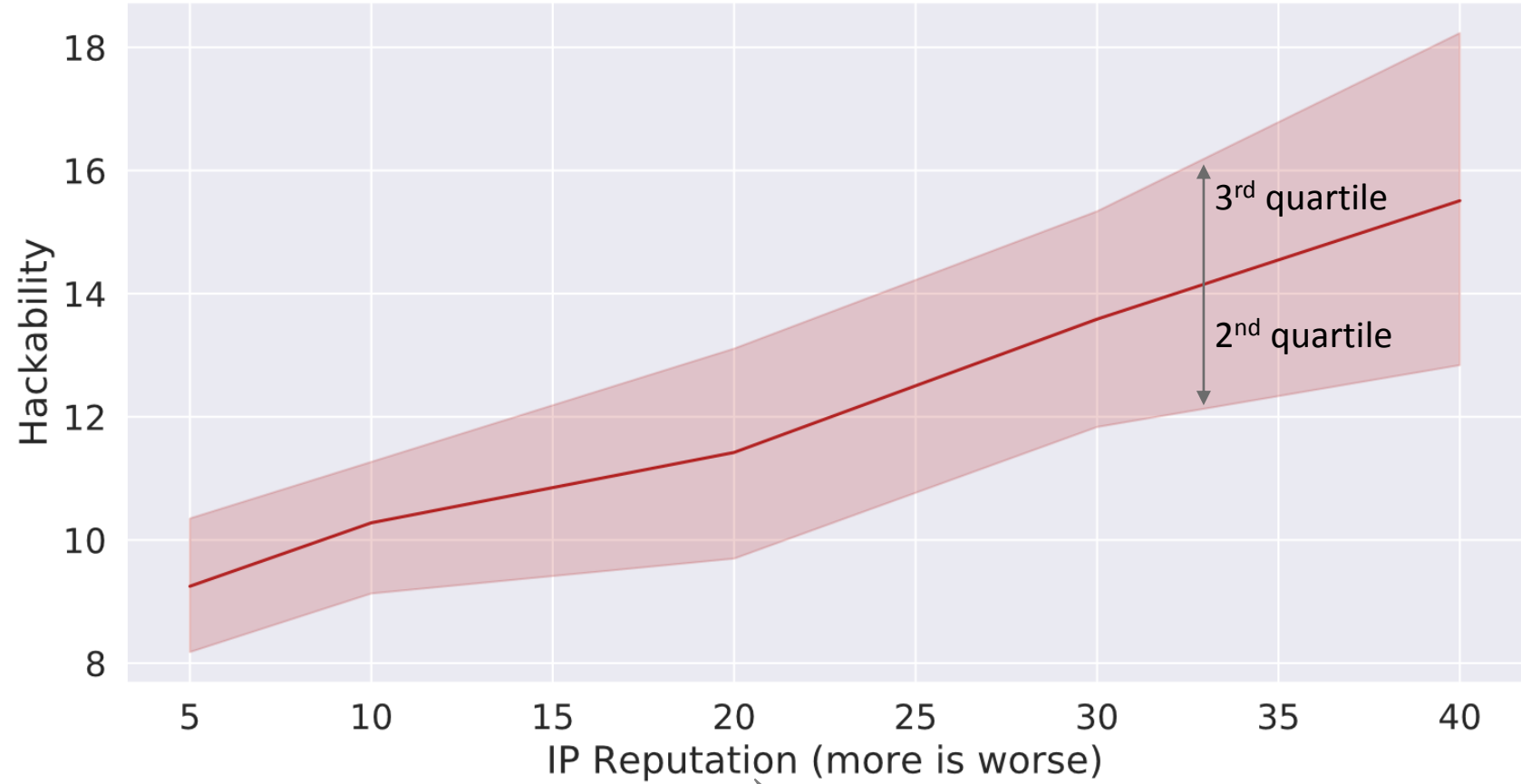


Interpretation

- (Not shown here:) On average, having a bug bounty program correlates with higher hackability (across all industries)
- However, larger, more exposed companies gravitate towards bug bounties
- As shown on here, for equally exposed companies **bounties correlate with less hackability**, suggesting that either bounties have a positive effect or companies start bounty programs after reaching above-average security, or a mix of these factors

More hackable companies have already been hacked in the past

Analysis

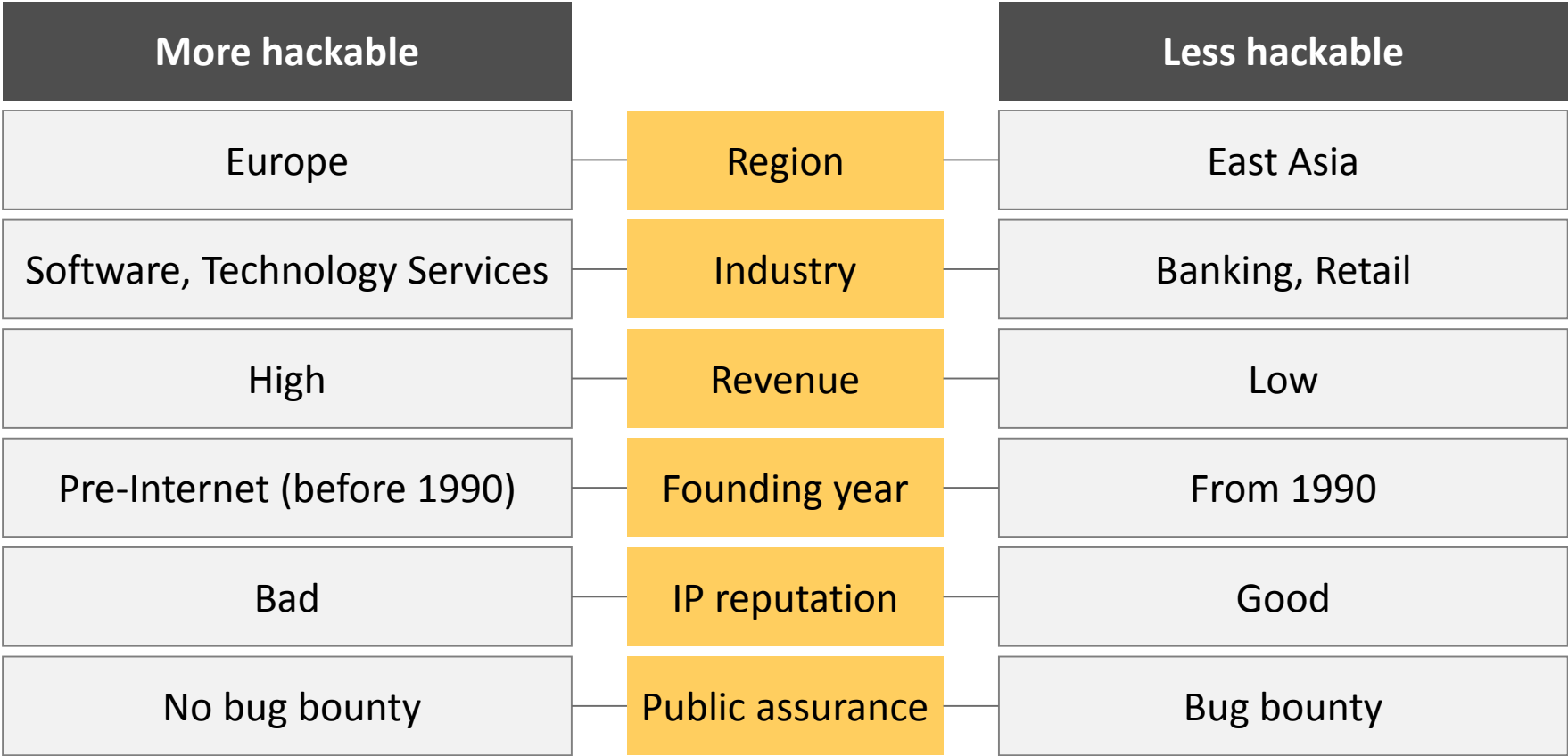


The IP reputation score grows as more IPs of a company appear on various bad-IP lists that indicate past hacking

Interpretation

- Companies who got hacked in the past, and consequently have IPs with bad reputation, are still more likely to be hacked today
- Validation: A higher hackability score correlates with higher real-life hackability

Many factors indicate the average hackability of a company

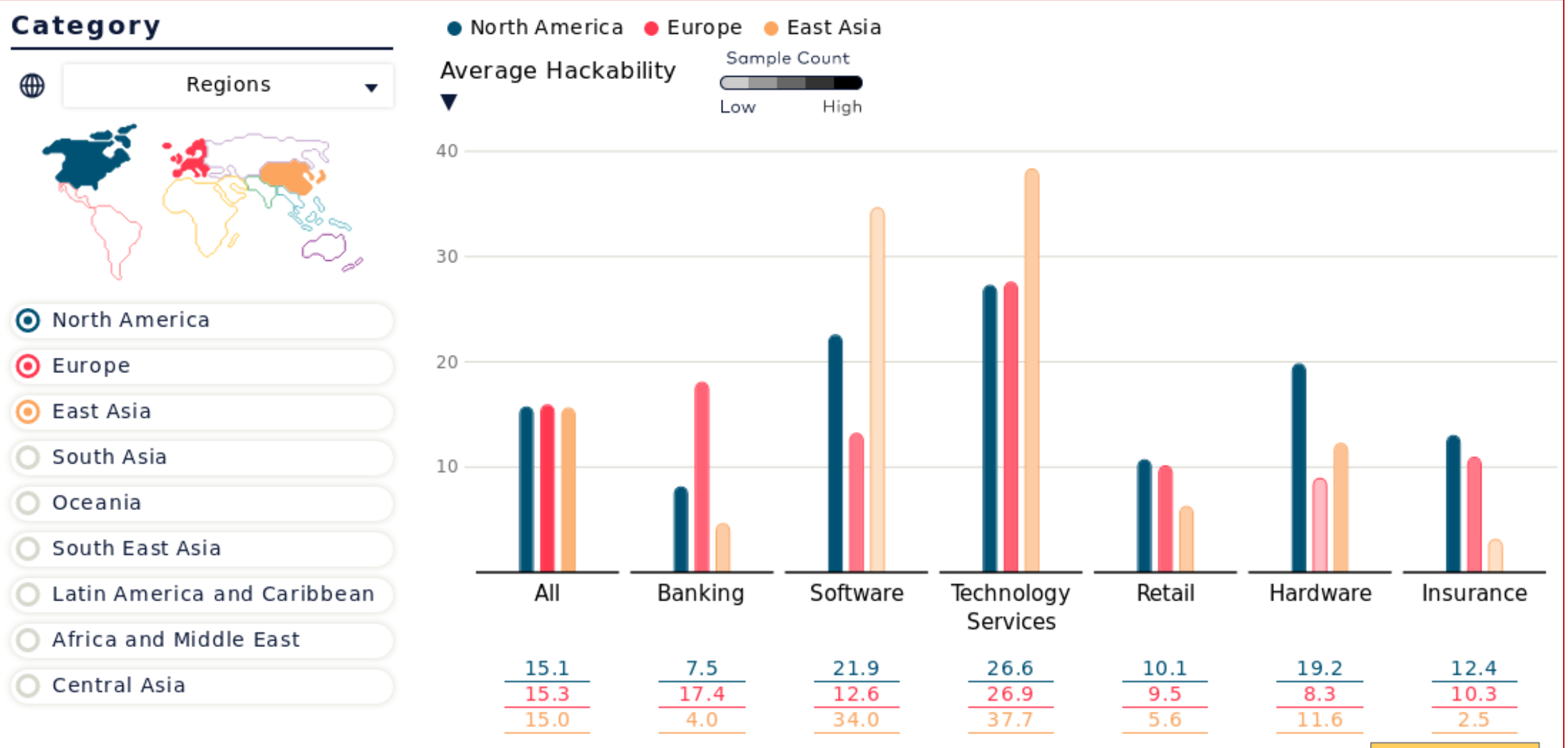


-
- Research motivation
 - Measuring hackability
 - Global deep scan results

 **Data for security evolution**

How hackable is my region or industry?

Find all the statistics discussed in this talk and a lot more at srlabs.de



+ Demo

How hackable is my company?

Get your company's report at <https://autobahn.security>

Delete Rescan

Example scan

Revision 1

Vulnerability Results

Systems By Severity Level

IPs 238 Domains 423

■ Major ■ Noteworthy ■ Minor ■ Negligible

Underlying Root Causes

Total Hackability Score 61

Security Architecture

Is our main weakness

Security Maintenance

Is worse than average

Next Actions

Short-term / Technical

- Investigate and close the major issues unauth_mqtt and aws_full_control_bucket affecting 2 hosts
- Patch and harden exposed software, starting with: git_directory, writable_snmp, rfi
- Block internal services at border firewall, starting with: 14 minor issues

Long-term / Strategic

- Rescan regularly to measure



Scans	Revision		IPs	Major	Noteworthy	Minor	Actions
AWS Infrastructure	1	🕒 37 mins to go	<div style="width: 72%; background-color: #00a651; height: 10px;"></div>		72% complete		⌛ Cancel Scan
All company assets +	4	🔍 Nov 15, 2018	3781	7	114	710	Download XLSX Email Rescan Delete
	3	🔍 Nov 13, 2018	3870	15	160	950	Download XLSX Email Rescan Delete

Take aways

- We defined a metric to compare hackability of organizations: The most common hackability drivers are still weak credentials, unnecessary exposure, config gaps, and missing patches
- **If you change default passwords, use a firewall well, harden your servers, and patch them regularly, you are easily in the global top 10%**
- Different industries can still learn a lot from each other on these most basic secure operations practices, as can different regions
- The research data is available on *srlabs.de*, for you to find further insights

Questions?

Fabian Bräunlein <fabian@srlabs.de>
Luca Melette <luca@srlabs.de>