Cybersecurity: What You Need to Know and Why

Ming Chow (E02, GE04)
Senior Lecturer, Department of Computer Science
mchow@cs.tufts.edu
Twitter: @0xmchow
Tufts Faculty Webinar Series, March 13, 2019

What is Cybersecurity?

- “The science and practice of protecting information and information processing components from misuse during their design, creation, transmission, storage, transformation, use, and disposal.” [1]
- A very broad field that encompasses many disciplines: Economics, Psychology, Mathematics, International Relations, Political Science, Law, Business, etc.

Why Cybersecurity?

- Our lives and the global economy are so dependent on technology and connected systems.
- We are still facing the same problems from decades ago.
- An international crisis.

How I Got Into Cybersecurity

- USENIX Annual Conference **2004** in Boston, MA
  - The USENIX Association is the Advanced Computing Systems Association
- I didn’t know cybersecurity was a thing
- Gary McGraw and Ed Felten
- The message from Gary and Ed: *“We (the computing and scientific communities) need to step up to the plate and educate people on technological issues. The goal can be accomplished by being more involved, by being partisan, and by talking to anyone who is curious.”* [2]

Cybersecurity Now

- Old attacking techniques still very successful
- Throwing money at the problem
- Many software developers still do not know basic security
- Growing complexity [3]
- Disenfranchisement of women, very low female participation of all Computer Science disciplines
- Disconnect between security folks and business stakeholders; not understanding tradeoffs
- Not educating government / federal government not asking hard questions

A Dossier of Sobering Reality

Summary of Results

The data set includes 100 separate internal penetration test engagements spanning 75 unique organizations.

The top four attack vectors are based on utilizing stolen credentials. This is a serious problem because credential theft will always work as long as the credentials are valid. Credential theft is highly reliable, repeatable, and has a low likelihood of negative impact for an attacker.

The last finding in our list is insufficient network segmentation. Attackers can use credentials wherever they are allowed, even in places the users might not need or know about. This is why it is important to restrict access at the network level based on business requirements.

The five identified issues are "root causes" of a compromise, which we define as security weaknesses that were used to achieve a network compromise or engagement objective, such as access to sensitive information (e.g. cardholder data, PII, and PHI).

The Approach

The following table represents the top five attack vectors used by Praetorian between 2013 and 2016 as part of a complete corporate network compromise kill chain. This list was last updated in June 2016 and is based on a review of 100 reports.

RANK	FINDING	PERCENTAGE
1	Weak Domain User Passwords	66%
2	Broadcast Name Resolution Poisoning (aka WPAD)	64%
3	Local Administrator Attacks (aka Pass the Hash)	61%
4	Cleartext Passwords Stored in Memory (aka Mimikatz)	59%
5	Insufficient Network Access Controls	52%

Table 1: Praetorian's top internal findings based on frequency of occurrence in kill chain

Credentials. Source: https://p16.praetorian.com/downloads/report/How%20to%20Dramatically%20Improve%20Corporate%20IT%20Security%20Without%20Spending%20Millions%20-%20Praetorian.pdf

Dropbox employee's password reuse led to theft of 60M+ user credentials

Kate Conger, Matthew Lynley 3 years ago

Comment

Source: https://techcrunch.com/2016/08/30/dropbox-employees-password-reuse-led-to-theft-of-60m-user-credentials/

How the NSA Gets You

In the world of advanced persistent threat actors (APT) like the NSA, credentials are king for gaining access to systems. Not the login credentials of your organization's VIPs, but the credentials of network administrators and others with high levels of network access and privileges that can open the kingdom to intruders. Per the words of a recently leaked NSA document, the NSA hunts sysadmins.

The NSA is also keen to find any hardcoded passwords in software or passwords that are transmitted in the clear—especially by old, legacy protocols—that can help them move laterally through a network once inside.

https://twitter.com/ncweaver/status/692518696808353793

And no vulnerability is too insignificant for the NSA to exploit.

"Don't assume a crack is too small to be noticed, or too small to be exploited," he said. If you do a penetration test of your

Source:
https://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/

CSO FROM IDG

Default usernames and passwords have always been a massive problem in IT. These days, the consumer technology that envelops the Internet of Things (IoT) has only made the problem larger.

Default credentials, which are ignored or too difficult for some people to change, behind the development of a botnet that took part in the largest DDoS attack on record.

The usernames and passwords below were used to enable the Mirai botnet, which is powered by IoT technology. The botnet hit Brian Krebs with traffic topping out at 620Gbps, but it's also been linked to a DDoS against OVH (799Gbps).

USER:	PASS:	USER:	PASS:
root	xc3511	admin1	password
root	vizxv	administrator	1234
root	admin	666666	666666
admin	admin	888888	888888
root	888888	ubnt	ubnt
root	xmhdipc	root	klv1234
root	default	root	Zte521
root	juantech	root	hi3518
root	123456	root	jvbzd
root	54321	root	anko
support	support	root	zlxx.
root	(none)	root	7ujMko0vizxv
admin	password	root	7ujMko0admin
root	root	root	system
root	12345	root	ikwb
user	user	root	dreambox
admin	(none)	root	user
root	pass	root	realtek
admin	admin1234	root	00000000
root	1111	admin	1111111
admin	smcadmin	admin	1234
admin	1111	admin	12345
root	666666	admin	54321
root	password	admin	123456
root	1234	admin	7ujMko0admin
root	klv123	admin	1234
Administrator	admin	admin	pass
service	service	admin	meinsm
supervisor	supervisor	tech	tech
guest	guest	mother	fucker
guest	12345		
guest	12345		

Mirai: https://www.csoonline.com/article/3126924/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html

1. Developers aren’t trained in secure coding.

Traditionally, the focus for developers is creating functional, rather than secure code. Veracode research shows that the pass rate of applications against standards like the OWASP Top 10 hasn’t budged in recent years, with applications failing policy consistently around 70 percent of the time on the initial scan. When we looked at the prevalence of major vulnerability categories like SQL injection in initial application scans, we see a similar consistency over time. If SQL injection, and other flaws like credentials management, are continuing to show up at the same rate during development, that indicates developer education programs still aren’t providing secure coding training.

Developers just don’t know:
https://www.veracode.com/blog/secure-development/what-developers-need-know-about-state-software-security-today

The simple and stupid mistakes still being made:
https://arstechnica.com/tech-policy/2019/02/plain-wrong-millions-of-utility-customers-passwords-stored-in-plain-text/

VULNERABILITIES / THREATS

4/7/2016
11:00 AM

Kelly Jackson Higgins
News

Connect Directly

0 COMMENTS
COMMENT NOW

Login

50% 50%

Like

Tweet

Top US Undergraduate Computer Science Programs Skip Cybersecurity Classes

New study reveals that none of the top 10 US university computer science and engineering program degrees requires students take a cybersecurity course.

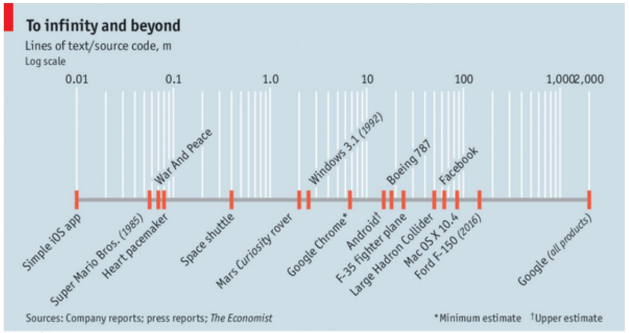
There's the cybersecurity skills gap, but a new study shows there's also a major cybersecurity education gap -- in the top US undergraduate computer science and engineering programs.

An analysis of the top 121 US university computer science and engineering programs found that none of the top 10 requires students take a cybersecurity class for their degree in computer science, and three of the top 10 don't offer any cybersecurity courses at all. The higher-education gap in cybersecurity comes amid the backdrop of some 200,000 unfilled IT security jobs in the US, and an increasing sense of urgency for organizations to hire security talent as cybercrime and cyber espionage threats escalate.

Robert Thomas, CEO of CloudPassage, whose company conducted the study, says the security gap in traditional computer science programs is worrisome, albeit not too surprising. "The results were pretty profound," Thomas says. "When we tested the top universities' computer science degrees, it was disturbing to find that very few require any kind of cybersecurity [instruction] as part of the curriculum to graduate" with a computer science degree, he says.

The education problem. Source:
https://www.darkreading.com/vulnerabilities---threats/top-us-undergraduate-computer-science-programs-skip-cybersecurity-classes/d/d-id/1325024

Android, the most popular smartphone operating system, is 12m.



Getting each of those lines to interact properly with the rest of the program they are in, and with whatever other pieces of software and hardware that program might need to talk to, is a task that no one can get right first time. An oft-cited estimate made by Steve McConnell, a programming guru, is that people writing source code—the instructions that are compiled, inside a machine, into executable programs—make between ten and 50 errors in every 1,000 lines. Careful checking at big software companies, he says, can push that down to 0.5 per 1,000 or so. But even this error rate implies thousands of bugs in a modern program, any one of which could offer the possibility of exploitation. "The attackers only have to find one weakness," says Kathleen Fisher, a computer scientist at Tufts University in Massachusetts. "The defenders have to plug every single hole, including ones they don't know about."

The complexity problem: https://www.economist.com/science-and-technology/2017/04/08/computer-security-is-broken-from-top-to-bottom

Security pros at hacker conference: Be more boring

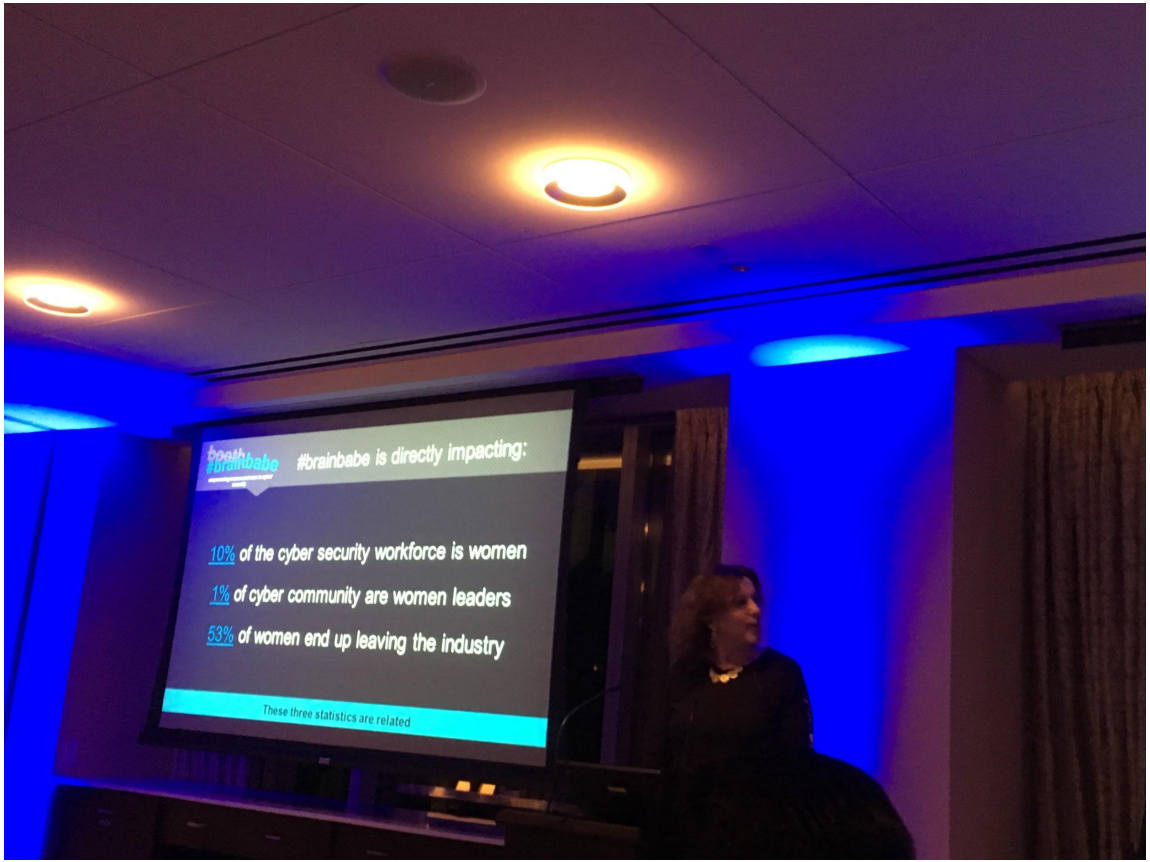
BY JOE UCHILL - 07/29/17 12:10 PM EDT

4 COMMENTS

The fundamental flaw exploited in WannaCry–ransomware that infected hundreds of thousands of machines in under a week in May –had already been patched by Microsoft at the time of the attack. The infected machines had all put off updating their systems. NotPetya, which spread about three weeks later, used the same flaw.

Most high-profile research is in novel attacks, previously unseen security flaws in software and large –sometimes nation-driven –political actors. ***But most attacks use well-worn techniques like phishing and other forms of fraud and security vulnerabilities that have long since been patched.***

Source: https://thehill.com/policy/cybersecurity/344460-security-pros-at-hacker-conference-aspire-to-be-more-boring



From November 15, 2016 in Boston, MA

Throwing money at the problem: https://twitter.com/jeremiahg/status/866783974311444480

BLEEPINGCOMPUTER

Search Site

NEWS | DOWNLOADS | VIRUS REMOVAL GUIDES | TUTORIALS | DEALS

Home > News > Security > 12,449 Data Breaches Confirmed in 2018, a 424% Increase Over the Previous Year

12,449 Data Breaches Confirmed in 2018, a 424% Increase Over the Previous Year

By Sergiu Gatlan

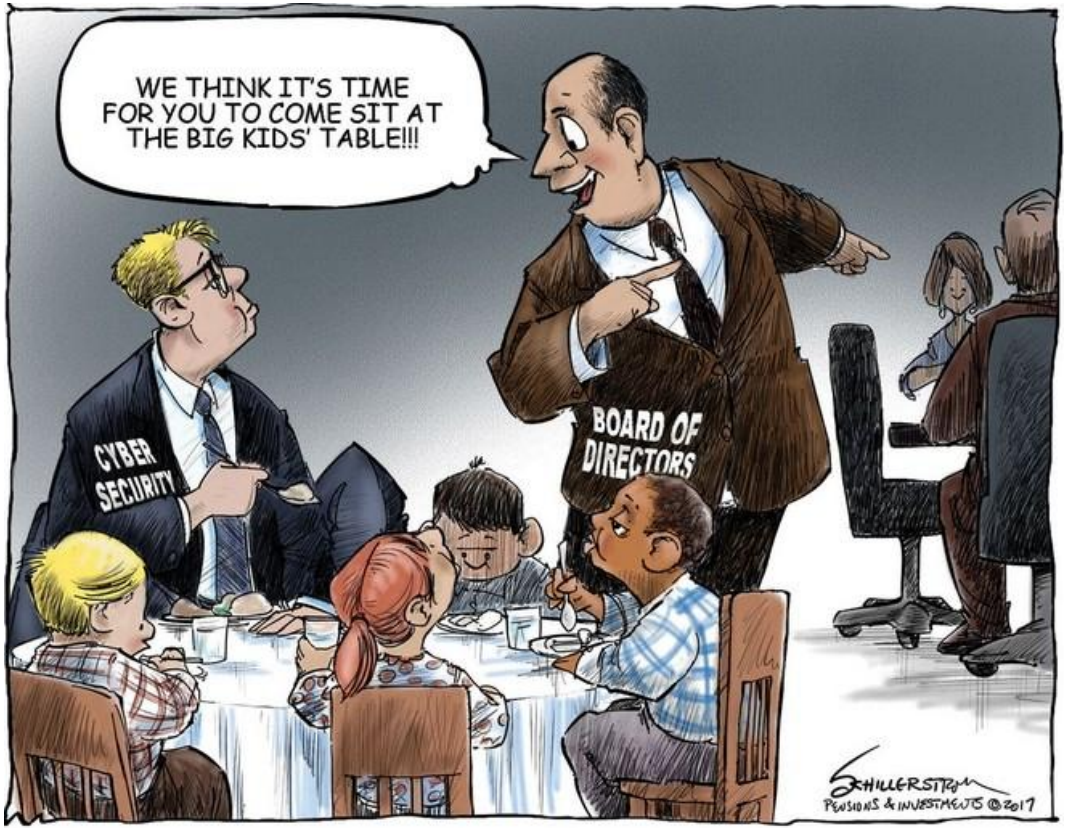
March 6, 2019 08:36 PM 0

The number of confirmed data breaches during 2018 reached 12,449, a 424% increase when compared with 2017, 47% of all compromised identity records having been exposed in breaches experienced by organizations from the United States and China.

4IQ, the identity intelligence company which published this report on the breached data landscape and trends, also discovered that, while the number of breaches saw a substantial boost last year, the average breach sized decreased to 216,884 records, a value 4.7 times smaller than the year before.

The company defines data breaches as confirmed incidents "where credentials, personal, medical, financial or other records with sensitive data have been accessed or disclosed due to being hacked or

And here we are in 2019!
https://www.bleepingcomputer.com/news/security/12-449-data-breaches-confirmed-in-2018-a-424-percent-increase-over-the-previous-year/



On the relationship between security folks and business stakeholders

Some Of The Most Common Problems Are Very Difficult to Solve

- Phishing and social engineering
- Data-driven attacks (e.g., SQL injection)
- Password reuse
- Distributed Denial of Service (DDoS)
- Attribution
- Writing secure code --“that does what people want at the end of the day”
- *Connecting and communicating with non-technical folks and the policymakers (policy)*

Cyber Security and Policy at Tufts

Why Policy?

Policy and legislation play a heavy hand.

Sources: https://twitter.com/gdead/status/892547412308480003 and https://www.extremetech.com/internet/281991-australia-becomes-first-western-nation-to-ban-secure-encryption

Why Cyber Security and Policy at Tufts?

- *Leveraging our existing strengths in International Relations, Law, Political Science, Computer Science, and Active Citizenship.*
- The Fletcher School's 2015 strategic plan "To the Know the World" identified Cyber Security and Cyber Warfare as potential growth areas for faculty research and teaching.
- Also in School of Engineering's strategic plan: "educating engineers committed to the innovative and ethical application of science and technology in addressing the most pressing societal needs."
- *Provide leadership*

What Have We Done in Cyber Security and Policy?

- (2017) Hired Susan Landau as Bridge Professor in Cyber Security and Policy, a bridge appointment between The Fletcher School and the School of Engineering.
- New courses:
  - (2017) Cyber Security and Cyber Warfare, a joint course between Computer Science and Political Science Departments
  - (2017) Privacy in the Digital Age, cross-listed between School of Engineering and The Fletcher School
  - (2018) Cyberlaw and Cyberpolicy, cross-listed between School of Engineering and The Fletcher School
  - (2018) Cyber in the Civil Sector, cross-listed between School of Engineering and The Fletcher School
  - (2019) Reverse Engineering
- (2017) Computer System Security (Introduction to Cyber Security) now offered as an online course during the summer; classroom course in fall semester
- (2018) Program Website: Cyber Security and Policy at Tufts https://sites.tufts.edu/cybersecurity/
- (2018) Inaugural Conference: Protecting Civilian Institutions and Infrastructure from Cyber Operations: Designing International Law and Organizations
- (2018) Career Panel in Cybersecurity Policy
- (2019) Cyber Security Focus Area in the Computer Science Department
  - https://engineering.tufts.edu/cs/current-students/ba-and-bs/undergraduate-focus-area-cyber-security
- (2019) NEW: Hired new Assistant Professor in Cybersecurity Policy at The Fletcher School
- (2019) Three summer fellowships for students in cybersecurity policy at civil-society organizations
- Two Atlantic Council Cyber 9/12 Student Competition teams placed semi-finals (2017, 2018)
- Two teams placed in MITRE Embedded Capture The Flag Competition (2016, 2018)

Current Research at Tufts Pertaining to Cyber Security and Policy

- Twice-a-month research meetings and informal talks in Cyber Security and Policy across Fletcher, SoE, and Political Science
- Privacy and metadata research with a Cybersecurity Policy Fellow
- Developing trust in security protocols
- Android security

The Future of Cyber Security and Policy at Tufts

- Student Symposium in Cybersecurity Policy, April 5th-6th, 2019
- New course: Computer Science for Future Presidents will be offered in fall 2019
- In process of hiring another Computer Science faculty focusing on Security and Systems

Personal Tips

So What Can You (Personally) Do?

- Credentials management
  - Two-factor authentication (2FA)
  - Password managers
  - Universal 2nd Factor (U2F), FIDO key
- Update software and systems --if you have the ability to do so
- Understand your own threat model, know who you are and what's important to you [4]
- Question everything, especially any electronic information
- Ask yourself: *do you really need that smart TV, or that touchscreen refrigerator, or the pair of sneakers that require an update?*

Q&A / AmA

References and Acknowledgements

1. https://spaf.cerias.purdue.edu/presents/rethink.pdf
2. https://www.usenix.org/legacy/event/usenix04/usenix04reports.pdf
3. https://freedom-to-tinker.com/2006/02/15/software-security-trinity-trouble/
4. https://the-parallax.com/2019/02/27/simple-nomad-opsec-tips-qa/
5. https://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/
6. https://www.economist.com/science-and-technology/2017/04/08/computer-security-is-broken-from-top-to-bottom
7. https://p16.praetorian.com/downloads/report/How%20to%20Dramatically%20Improve%20Corporate%20IT%20Security%20Without%20Spending%20Millions%20-%20Praetorian.pdf
8. https://www.darkreading.com/vulnerabilities---threats/top-us-undergraduate-computer-science-programs-skip-cybersecurity-classes/d/d-id/1325024
9. https://twitter.com/jeremiahg/status/866783974311444480
10. https://twitter.com/gdead/status/892547412308480003
11. https://techcrunch.com/2016/08/30/dropbox-employees-password-reuse-led-to-theft-of-60m-user-credentials/
12. https://www.veracode.com/blog/secure-development/what-developers-need-know-about-state-software-security-today
13. https://arstechnica.com/tech-policy/2019/02/plain-wrong-millions-of-utility-customers-passwords-stored-in-plain-text/
14. https://thehill.com/policy/cybersecurity/344460-security-pros-at-hacker-conference-aspire-to-be-more-boring
15. https://www.csoonline.com/article/3126924/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html
16. https://www.bleepingcomputer.com/news/security/12-449-data-breaches-confirmed-in-2018-a-424-percent-increase-over-the-previous-year/
17. https://www.extremetech.com/internet/281991-australia-becomes-first-western-nation-to-ban-secure-encryption

18. Special thanks to Dan Farmer, Russell Butturini, Simple Nomad, Seth Rosenblatt